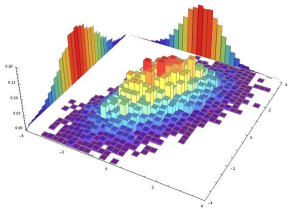
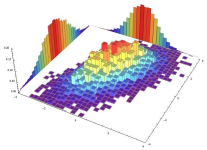
Thinking Through Economic Security

fmrmf
@SmolQuants

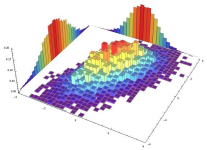


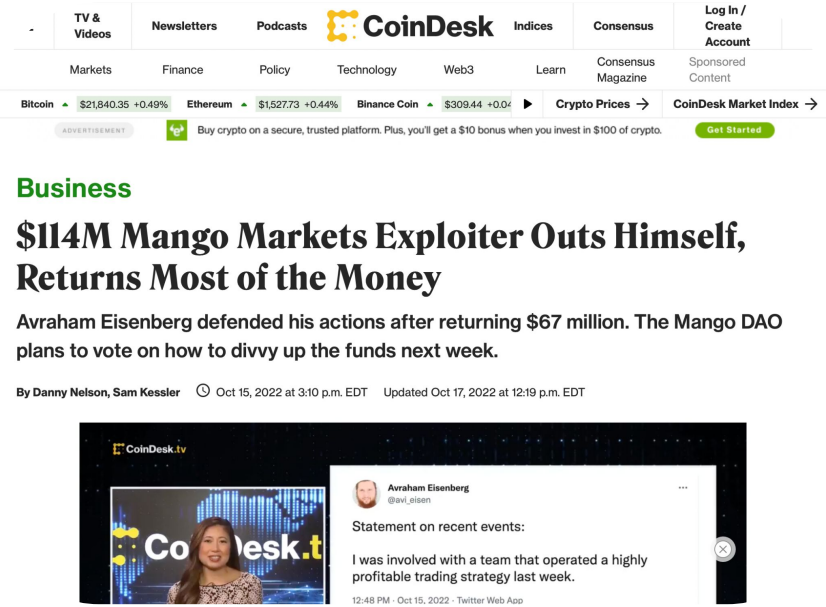
Who am I?

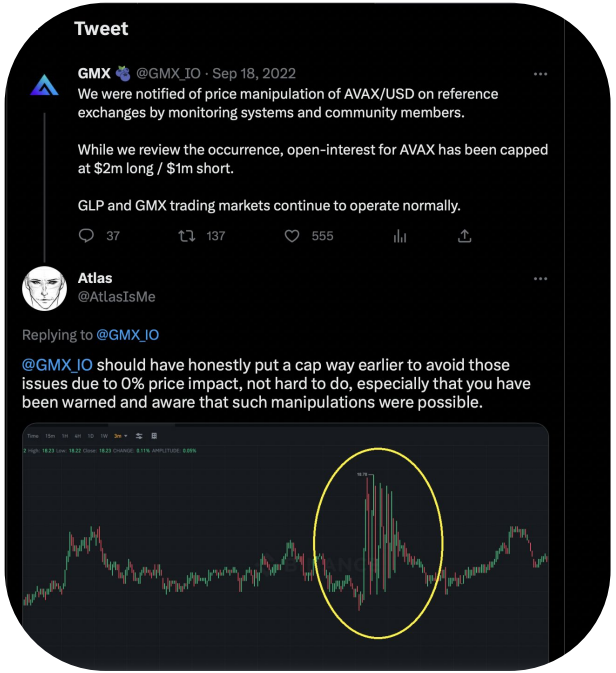


- Researcher and technical lead at SmolQuants
- Previously, formulated risk framework/spec for DeFi derivatives protocol
- Quant/physics background from a prior life

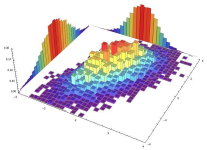
Why worry about economic security? (1/n)

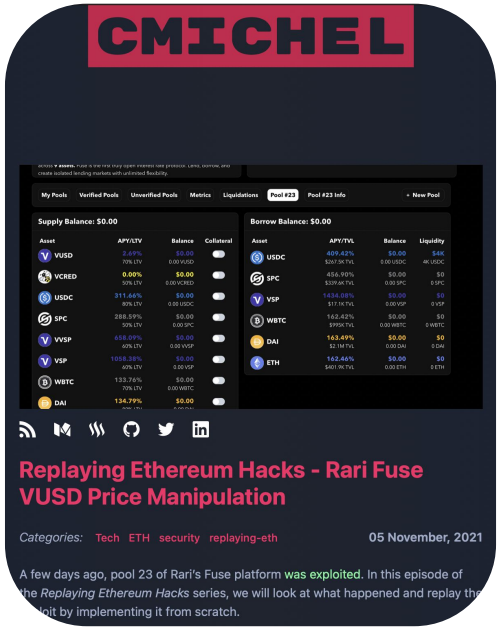




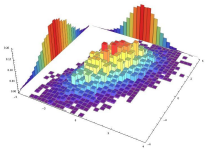


Why worry about economic security? (2/n)





Why worry about economic security? (3/n)



AAVE Sign Up Log In

Discussion: Reducing Long Tail Asset Risk

Governance General

monet-supply Nov '22

Hi all,

Many of you may be aware of Avi Eisenberg's "highly profitable trading strategy" on Mango Markets. In the aftermath of this manipulation attack, Aave froze reserves of several low liquidity assets including BAL, REN, and CVX.

However, the CRV market was not frozen and it seems that the protocol is now at risk of accumulating significant bad debt due to a tactical short position that Avi entered with the intention of precipitating a short squeeze. This has so far resulted in his initial position accumulating around $1.5 million of CRV denominated bad debt 103 . In a worst case scenario, continued price action could lift CRV far above fair market value and allow users to withdraw excessive liquidity from other assets based on inflated collateral value (although CRV liquidation threshold is only 61% so this risk is relatively lower).

I'd like to open discussion on potential mitigation measures to reduce imminent risk to the protocol from manipulation of low liquidity assets. While these parameters could be optimized, I think it's best to avoid analysis paralysis and implement some common sense changes as soon as possible.

Some initial suggestions:

- Reduce liquidation threshold to 80% for any assets that currently have a higher value (DAI, USDC, TUSD, ETH, stETH)
- Reduce max LTV to 75% for any assets that currently have a higher value
- Freeze reserves (prevent new deposits and borrows) and set max LTV (initial margin) to 0% for low liquidity assets at risk of similar short squeezes that are listed as collateral (BAT, CRV, DPI, ENJ, ENS, MANA, MKR, SNX, xSUSHI, YFI, ZRX)

I believe the above changes will significantly reduce risk to the Aave v2 ETH market while further optimizing changes can be considered through governance. Aave v3 includes significant improvements to risk management options, which could allow for greater capital efficiency and wider asset listings once launched on mainnet.

Nov 2022

1 / 19
Nov 2022

Back

Dec 2022

Thread

Inverse+
@InverseFinance

This morning Inverse Finance's money market, Anchor, was subject to a capital-intensive manipulation of the INV/ETH price oracle on Sushiswap, resulting in a sharp rise in the price of INV which subsequently enabled the attacker to borrow $15.6 million in DOLA, ETH, WBTC, & YFI

11:44 AM · Apr 2, 2022

63 Retweets **38** Quote Tweets **281** Likes

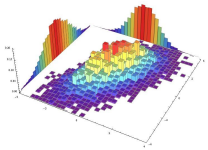
Inverse+ @InverseFinance · Apr 2, 2022
Replying to @InverseFinance
The manipulation was not a flash loan attack and was un-related to Inverse's smart contract or front end code. All future borrows on Anchor are temporarily paused. Some additional updates:

1 3 53

Inverse+ @InverseFinance · Apr 2, 2022
1. The plan to be proposed to governance is to ensure all wallets impacted by the price manipulation are repaid 100%. We have multiple avenues for accomplishing this and will provide updates as the DAO discusses our options.

5 12 86

What is "economic security"?

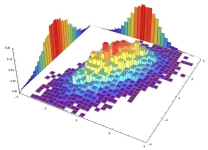


Economic security is concerned with:

- How much capital will it take to break your protocol?
- Are the economic mechanisms behind your protocol sound?

Differs from code security in the sense that economic security assumes the protocol has been programmed to perfection, and the only way to attack the protocol *requires* some form of upfront capital.

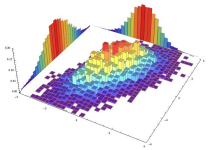
A framework for thinking about economic security



Fundamental theorem of asset pricing:

1. There's no free lunch (no-arbitrage condition)
2. Assets can be replicated as portfolios of basic financial legos (complete markets)

How can we apply this framework?

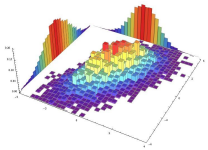


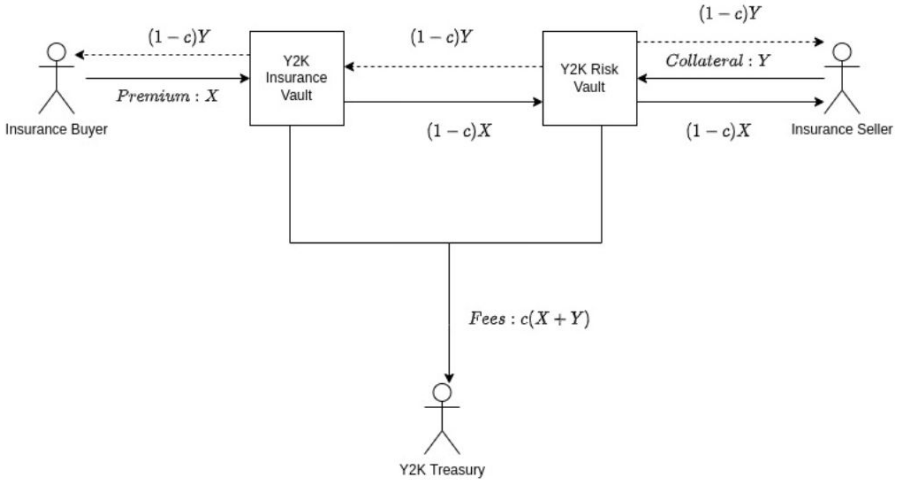
Should think through:

- Who are the counterparties involved in your system?
- Does your protocol trend toward no-arbitrage in steady state of system?
- How much capital does it take to create an “arbitrage” on your protocol (possibly via your protocol’s dependencies)?
- What types of financial assets are involved in what your protocol is offering?

A lot of the time the answers to these questions (e.g. is your protocol sound?) are *probabilistic* in nature v.s. deterministic.

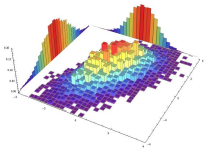
Example: Y2K Finance (1/n)



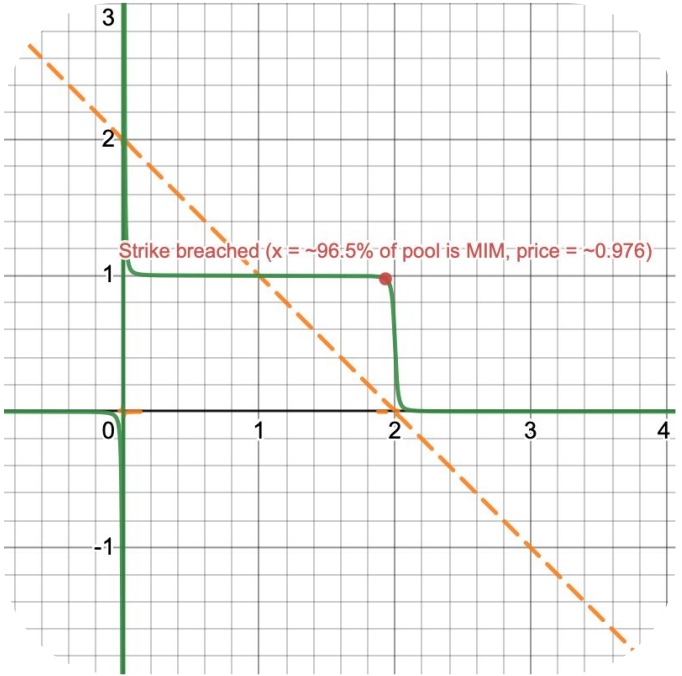


- Two-sided markets for stablecoin (and other pegged asset) insurance over pre-defined periods: MIM, USDC, USDT, FRAX, DAI, etc.
- Insurance payout in the event market price goes below a set strike price

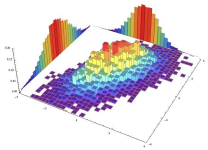
Example: Y2K Finance (2/n)



- ~62% of MIM circulating supply and the majority of liquidity for MIM was in the MIM Curve metapool at time of econ audit
- Attacker could:
  - Purchase Y2K insurance on MIM
  - Mint MIM through Abracadabra
  - Sell into the Curve pool to trigger a depeg
  - Collect on Y2K
  - Swap back through the Curve pool
  - Repay the MIM loan
- Cost of attack to execute profitably required ~47M MIM mint

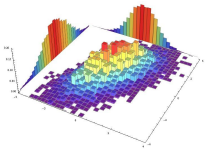


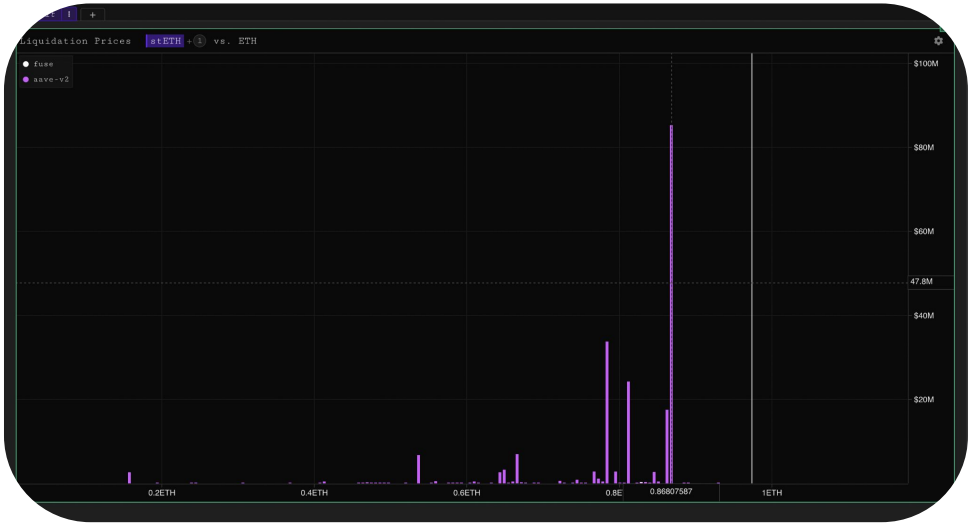
Example: Y2K Finance (3/n)



- Insurance product analogous to binary put options
- Pro-rata payout structure in V1 caused some issues at the extremes; V2 improving on this
- Two player extreme example (ignoring fees):
  - Seller deposits 1000 ETH in the risk vault for MIM
  - Buyer deposits 0.000001 ETH in the hedge vault for MIM
  - If depeg occurs, buyer receives 1000 ETH and seller receives 0.000001 ETH
- First binary put buyer is able to specify their own price through depositing whatever amount they desire
  - Meaning, initial round of sellers depositing into the risk vault are effectively quoting the ask for the binary put at a price of 0
  - Unlikely risk sellers actually are pricing the binary put at this value
- In practice with V1, however, steady state for system seems to be pricing close to market's expectations for probability of depeg.

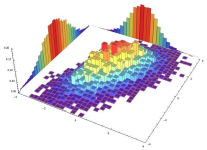
Example: Aave stETH (1/n)





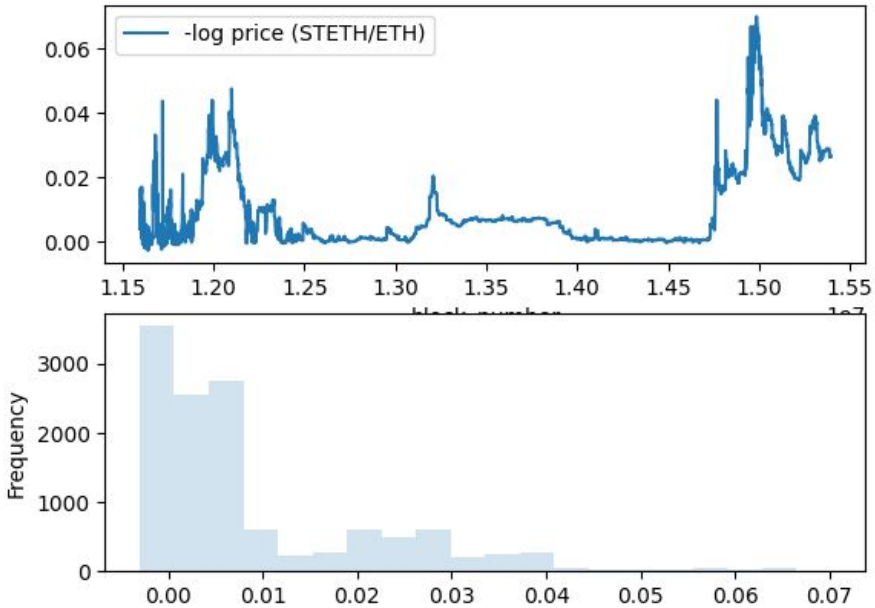
- What's the probability (roughly) stETH/ETH price decreases enough to trigger a liquidation cascade? (pre-merge analysis)
- What's the expected shortfall to the Aave insurance fund?

Example: Aave stETH (2/n)

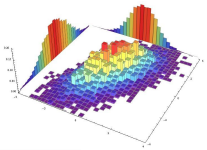


Possible way to start:

- stETH analogous to zero coupon bond, with implicit ceiling on price of 1 ETH pre-withdrawals
- Try typical TradFi model for bond:
  - Take ETH staking yield to be interest rate stochastic process
  - Cox-Ingersoll-Ross is simple enough and has implicit ceiling of 1 as rates > 0
  - Fit process via historical data
  - Use fit model with existing Aave stETH collateral amount to calculate expected loss in worst X% of price path scenarios



Where do we see this going?



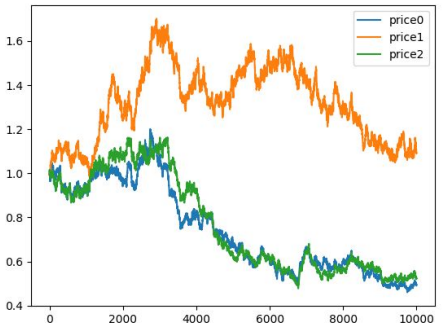
- Expect protocol devs to start using more open source risk analysis tools *that are built into their dev frameworks* to do their own pre-audit economic analyses
- Coupled with economic audits becoming a standard part of the audit process
- Why we're building tools like:
  - ape-risk – DeFi risk analysis as an ApeWorX plugin. Similar to fuzz testing, but "fuzzed params" are individual runs of Monte Carlo simulated data (e.g. price paths).
  - backtest-ape – Backtesting and forward-testing (via Monte Carlo sims) DeFi strategies

```python
import numpy as np
from ape_risk import strategies


@given(strategies.gbms(initial_value=1.0, num_points=100000, params=[0, 0.005]))
def test_gbms_param_fuzz(p):
    # strat gives a numpy.ndarray of simulated prices for each hypothesis run
    assert p.shape == (100000, 1)
    assert isinstance(p, np.ndarray)


C = np.asarray([[1, 0.5, 0.8], [0.5, 1, 0.4], [0.8, 0.4, 1]])
scale = np.linalg.cholesky(C).tolist()


@given(strategies.multi_gbms(initial_value=1.0, num_points=100000, num_rvs=3, params=[0, 0.005],
def test_multi_gbms_param_fuzz(p):
    # strat gives a numpy.ndarray of multiple simulated prices for each hypothesis run
    assert p.shape == (100000, 1, 3)
    assert isinstance(p, np.ndarray)
```



Q/A

Thanks!