

Notional Labs Incident Report

Terra, May 15, 2022

Jacob Gadikian

Funded by Delegations to Notional Validators in Cosmos

WTF HAPPENED TO TERRA?

First, what was terra? It was a blockchain platform that included a price-feed based algorithmic stable coin mint mechanism.

This means that you could use terra in order to mint arbitrary algorithmic stable coins, which would follow the price of various international currencies, like USD, Korean won, euro, etc. It did this by allowing users to swap between its native currency, Luna, and the algorithmic stable coins. These swap functions used a concept, “burning”.

So, you have 100 luna, value \$10 each.

You can now mint 1000 UST, which tracks the price of the USD. Your luna is now burned, and the supply of luna has been reduced, making luna more scarce, and theoretically increasing its value.

This mechanism was designed for use by arbitrageurs. In many situations in fintech, arb seekers are our friends. These arb seekers in the terra/luna case, would balance the supply of luna/ust. So the chain was an open marketplace for the creation of price-pegged representative currencies. In other words it was a dollar printing machine with a novel mechanism to ensure that the issued dollars were always exchangeable for an equal value stake of luna.

Now, the price of a dollar fluctuates daily. As does the price of a luna. As does the price of a UST. We refer to the closeness between the price of a dollar and the price of a UST as “the peg”. The closer those are, the tighter the peg is, the better the product is performing.

UST/USD peg held well.

The founder of Luna/terra is Do Kwon.

Along the way, Do became convinced that he needed an external mechanism to try to reinforce the UST/USD peg. Basically a team of internal arbitrageurs. He is a bitcoin fan.

He started Ifg.org which was the trading org designed to reinforce the peg.

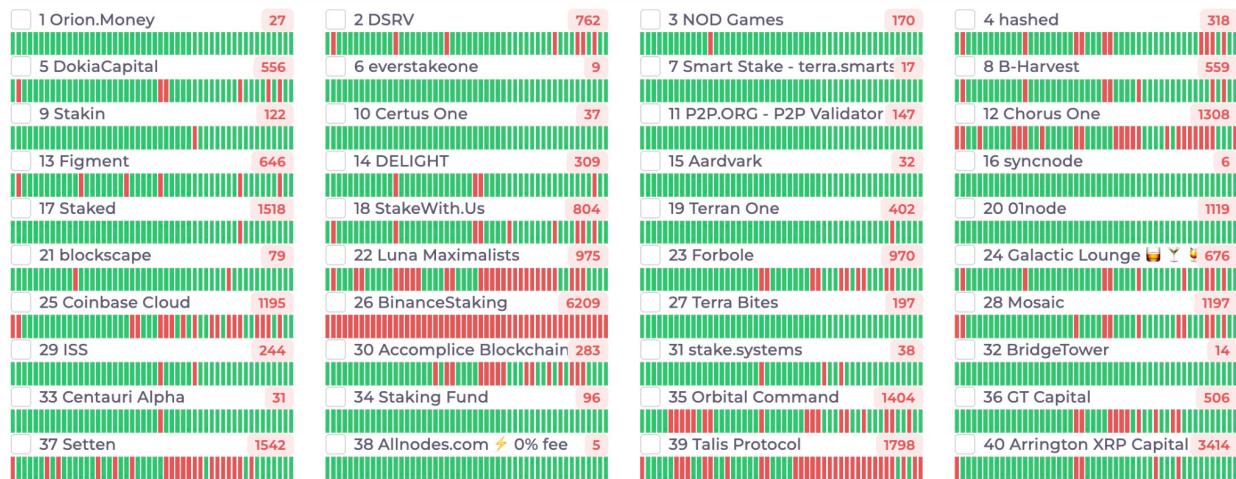
They purchased billions of dollars of btw using UST, using a TWAP mechanism provided by 3 arrows capital. This put a whole bunch of new UST on the market, likely 3 arrows betrayed Do and Ifg.org but we can't say for sure without an audit, which terraform labs says is pending.

Shortly after, the price of UST began to Deppeg, initally, by about \$.03 — it did not look like a big deal.

But the attackers had done their homework. They attacked terra both financially and on the blockchain infrastructure level.

It is my opinion that Terra validators did a really terrible job.

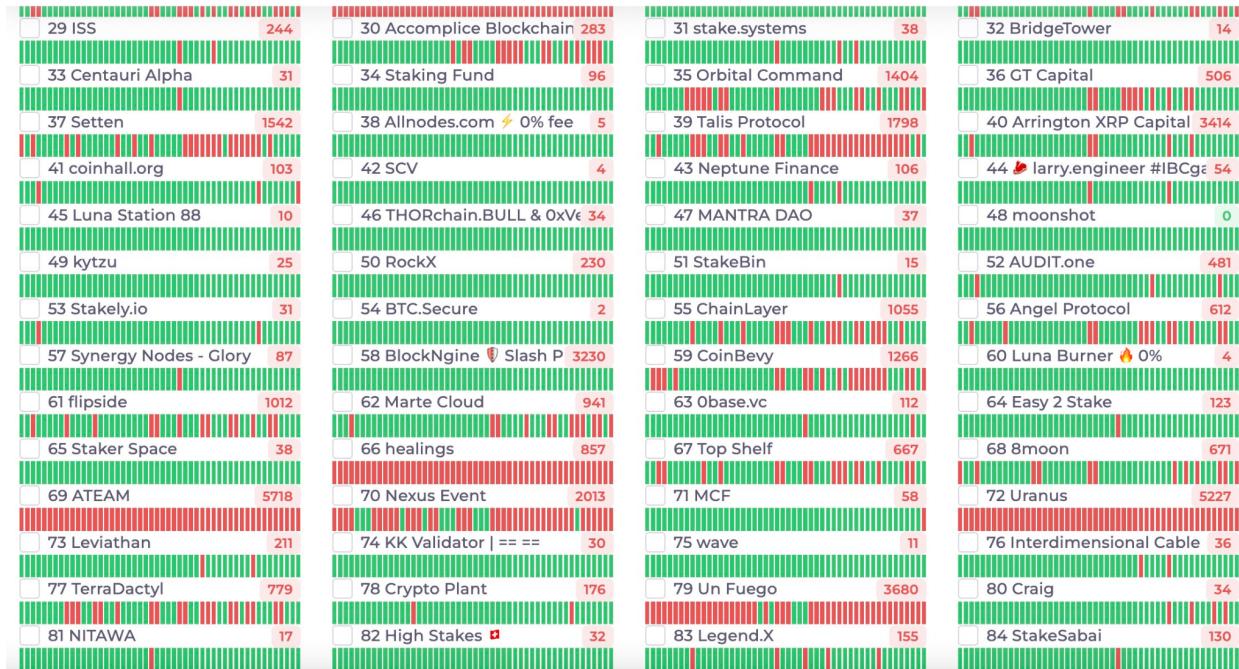
I recommend that you delegate away from those printing red streaks. Missing a couple of blocks while the chain is under stress is totally understandable. More than that is very bad, because the chain relies on validators to continue to exist, and to process user txns.



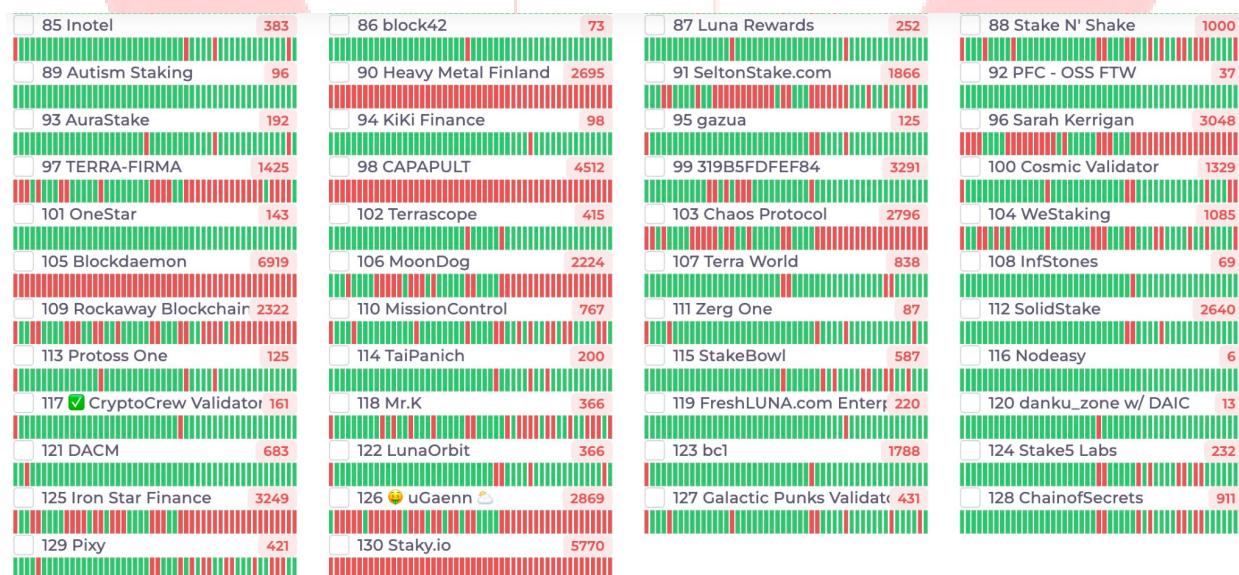
Let's call out quality, instead of attacking:

- Syncnode
- Bridgetower
- Allnodes
- Orion.money
- Everstakeone
- Aardvark
- Certus One

NOTIONAL



- Moonshot
- Scv
- Btc.secure
- Stakely.io
- Luna station 88
- Craig
- Wave
- NITAWA



- Nodeeasy
- Danku
- Autism Staking
- PFC Validator

Validators I've mentioned above, did notably well during the attack on Terra.

The chain was flooded with transactions. This caused a series of cascading failures on the chain:

- leveraged positions were wiped out as prices fluctuated, "liquidated"
- the chain wasn't highly available. Users could not transact because it was being flooded.
- On external markets, the adversary was working to lower the price of UST. This reduced confidence. People began to swap to luna.
- At some point, the total value of issued UST exceeded the total value of luna.
- The attacker knew that Ifg.org had bitcoin. They used capital to reduce the price of bitcoin all over the internet. Every market.
- Ifg.org could not **effectively** use its bitcoin to reinforce the peg on external markets anymore. It was no longer capital-efficient. There also may be fraud involved. Surely the wallet is now empty. Notional Labs is explicitly not accusing the Terra team of fraud, and advises that they release as much information as possible about the disposition of the Ifg.org bitcoin.
- People began to move more and more ust into luna, to get the par value back.
- The supply of luna began to spiral upwards. Zaki Manian, suggested that the chain may become consensus unstable because of this.
- the validators took the chain down to address consensus instability by disabling staking.
- Galois capital has claimed responsibility for the attack:

https://twitter.com/Galois_Capital/status/1524365468752138241

BUT IT GETS WORSE

NOTIONAL

The chain was brought back up in a way that protected consensus, but did not disable the stable coin redemption mechanism.

The value of luna dropped. This chain was aware of its prices externally through a price feed.

As the prices dropped, more and more Luna was minted.

Currently there's 6.9 trillion luna.

A week ago there were about 90 million luna, and each was worth \$100.

Terra had three stages:

0) **Original state**, which became consensus unstable

1) **Zombie stage 1**, which had ibc connections to other chains, unrestricted minting, and staking disabled and this protected only Terra's consensus mechanism but didn't protect pools or exchanges connected to terra, or users from themselves or others. Various fraud occurred in zombie stage 1. If you're in the osmo-luna pool, this is where stuff got bad for you. Previous to zombie stage 1, I recorded "[Euthanize Terra](#)". I don't take the idea of killing a chain lightly, but it was already undead.

After everyone shat their pants the chain was taken down a second time.

2) **Zombie Stage 2**, terra is brought back to life a second time with some IBC channels to external dexes turned off. Those who did not have their channels turned off, every chain connected them with liquidity saw that liquidity taken from its pools. Foreign assets are sitting ducks. The chain has a native token supply thousands of times higher than its norm. We are here now.

What should the user community do?

- You should take care of your mental health. You can twitter DM me 24/7 at twitter.com/gadikian if you feel suicidal or unwell. I will straight up call you if you need. I will tell you how far down I've fallen before and how high I managed to climb up afterwards. The only thing that separates you from an improved future, is the notion of harming yourself.
- You should not buy Luna
- You should not buy UST
- You should remove all foriegn assets from Luna as quickly as possible
- You may have lost IBC assets. There's little anyone can do about it.
- To some extent, you should be understanding: the terra engineering team is going through an absolute nightmare scenario. You should demand clarity on the Bitcoin.

Is this document authoritative?

No. This is a best-effort, firsthand account that I put together with the information that I have available to me as a scaled cosmos infrastructure provider. I could easily have missed important information.

