ENIGMA SECURITIES

MAKOR

De-Coding Crypto

Enigma Weekly

23rd June 2021

Written by Joseph Edwards, Head of Research at Enigma Securities.

Our Market View

May you live in interesting times. A dreadful week, with a brief kindling of optimism on Thursday being thoroughly distinguished by another crash in the wake of a number of new anti-crypto pronouncements coming out of China (the most crypto-friendly jurisdiction in Sichuan expelling miners, re-issuance of central bank guidance disallowing banks from dealing in crypto or with crypto holders, etc.), which ended up seeing us briefly mark new lows below $30,000 on Tuesday.

There are some reasons for short-term optimism ahead – quarterly expiry should, in theory, relieve some pressure on markets, and we only have one round of Grayscale unlocks left (July 16th) so the backlog there is likely close to being worked through entirely. However, upwards momentum for now remains extremely weak, and while we saw a bounce for now, it does feel like we're one bad headline away from a fall straight from $32,000 to the low-20s at this point.

On alts: most have continued to lose ground against BTC on the way down. ETHBTC ratio is down to 0.059, which is the lowest mark since May 2nd, but still substantially above the breakout point it started moving from at 0.045; expect further downside there in coming weeks. No assets really able to fully buck the trend with respects to the broader bear market, though SOL in particular is moving interestingly (suffered among the most severely in Tuesday's crash, but bounced far harder than anything else today).

Major

Ticker	Price	7D	1M	6M	12M	Cap
BTC	33711	-13.7%	-13.1%	27.6%	274.9%	631.8B
ETH	1990.87	-18.0%	-24.8%	212.6%	801.4%	231.8B
LTC	128.64	-23.2%	-30.3%	-0.6%	213.8%	8.59B
BCH	468.39	-21.8%	-37.6%	44.8%	116.4%	8.79B
EOS	3.676	-25.5%	-34.6%	40.7%	57.7%	3.52B

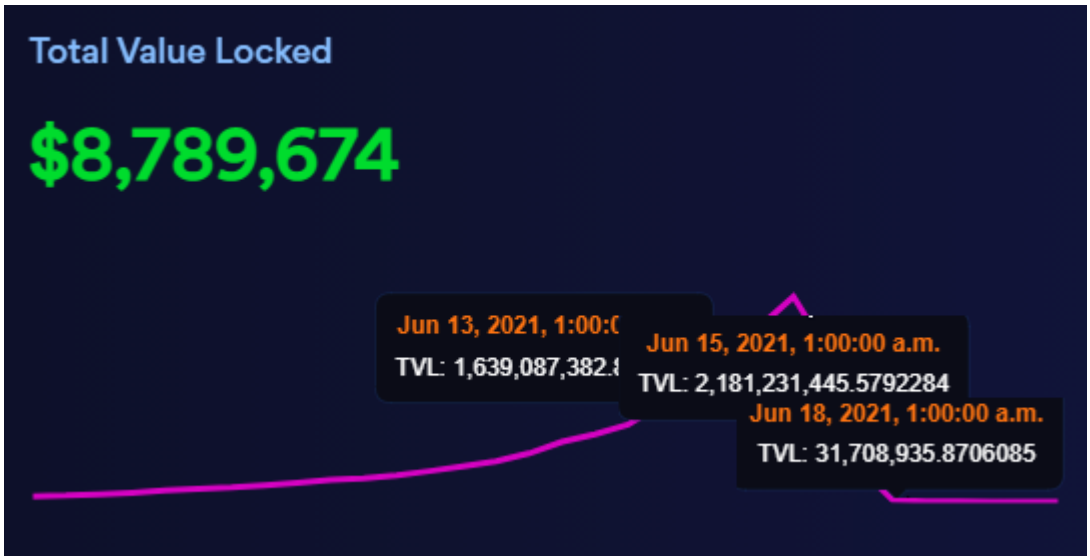
Selected

Ticker	Price	7D	1M	6M	12M	Cap
ADA	1.259	-17.4%	-19.0%	690.5%	1516.0%	40.29B
DOT	16.11	-30.5%	-31.0%	209.1%	451.3%	15.37B
LINK	18.35	-21.5%	-30.3%	67.7%	317.7%	7.95B

Please direct all enquiries about this week's research to jedwards@enigma-securities.io.

Components of a collapse: DeFi and Iron Finance

Last week, the Iron Finance stablecoin protocol collapsed overnight.



Via Iron Finance.

Crazy things like this happen in the DeFi space on a distressingly regular basis, but for the most part, nobody not involved tends to hear about it. There is, however, a good chance that you have heard about this one, even if you're not big on DeFi, or even if you're not big on crypto full stop. Why? Well, because of one Mr. Mark Cuban:

Via blogmaverick.com.

If you're not familiar with Mark Cuban: tech billionare-cum-media personality. You're now mostly familiar. Cuban has long been crypto-curious, but rarely a full-on evangelist, so when he came out with a post on 13th June extolling the virtues of yield and liquidity farming, including a reference to Iron Finance's TITAN token, it turned some heads.

Now, we should point out here that Mark Cuban absolutely did not cause either the rise or fall of Iron Finance. He did, however, draw significant attention to it, both at the time and in the aftermath, and his involvement has inevitably meant that it's now a story that's increasingly reverberating outside of crypto circles.

However, even if you are actively involved in crypto, there is a not inconsiderable chance that you have no idea what went on, even after reading about it, so we thought we'd take a slightly different approach. This isn't a technical post-mortem on Iron Finance; there are better pieces already written in that regard, with this one from DeFi news site The Defiant being our favourite.

Rather, this is an attempt to explain the component parts behind the collapse, and in doing so, explain (as briefly as possible) a number of the concepts and terms key to a lot of what goes on in DeFi that still remain unfamiliar to most.

Yield farming

This is the big thing to understand, because it's a large part of what underpins almost everything going on in DeFi. The short version is this: with the advent of decentralised exchanges, two of the things that were mainstays of most upstart cryptocurrency projects for years and years go away:

1) **Having an automatic system for new issuance** (because there's no mining system automatically bootstrapped to random ETH/BSC/etc.-based tokens).
2) **The ability to bring in liquidity and volumes immediately early on** (because nobody owns the exchanges and, for the most part, everything is on-chain and therefore transparent).

Yield farming is essentially how you address these absences. Participants put X amount of a certain token - either a native crypto token like ETH, or a stablecoin - into a pool, and that pool is used to provide liquidity for a decentralised exchange. In return, depositors receive (typically on a hourly or daily basis) a certain quantity of new issuance of a certain token. Due to the specifics of how this liquidity provision works, the depositors in the pool face no risk to their assets as part of the market making process.

Even in crypto terms, this is a fairly new development. Compound kicked off the trend in June 2020 by using it for issuance on their governance token COMP, and this was followed by a frenzy of projects jumping on the trend over the course of DeFi summer last year. The reason that incidentally it's referred to as 'farming' is because a huge number of the initial wave of tokens were named after food – PICKLE, YAM, CREAM, and countless others. If you've ever wondered why SushiSwap is called SushiSwap - this is literally why. The trend cooled off for a bit in the back half of 2020, but was revived with the start-of-year crypto boom and the success of Binance Smart Chain and the like, and has in all been the biggest part that you've never heard of in this crypto cycle.

It all sounds very safe. What's the catch? There are several. The first big one is of course **that there is no guarantee that the asset that you'll receive in the end will be worth anything.** (There are platforms where you CAN do that, but they're built on peer-to-peer lending, not printing money out of thin air). As to prove the point, STEEL and TITAN, the rewards for most Iron Finance pools, are basically worthless now and likely to stay worthless, for reasons we'll discuss later on.

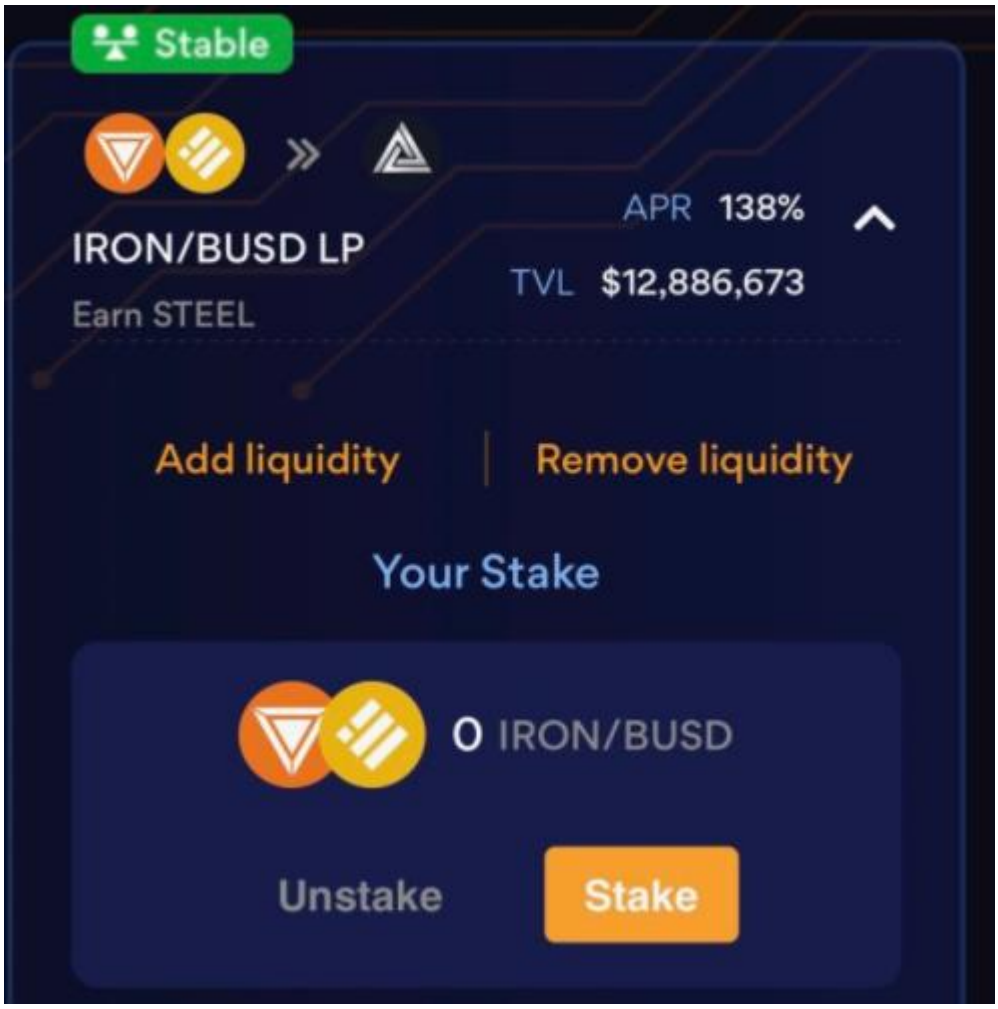
Next, a large amount of the trick with these pools is that, because they start out with barely anybody invested, and with reward assets that are themselves initially illiquid (i.e. overpriced), **they are able to quote incredibly misleading figures with regards to APR% returns.** Most long-term pools do settle

down to anywhere between 5% and 50%, but in the short-term, they are able to quote thousands or millions of % APR (because a 1% daily return compounds to a 3678% annual return).

There are further complications with regards to high APR pools generally requiring one to hold crypto-native assets rather than stablecoins (thus being exposed to their risk), the highest-APR pools requiring one to hold tokens from that same pool (the DeFi sector as a whole has been higher-beta than ETH and most altcoins in both the run up and the run down), the potential for pool rugs and exploits (more on that later), and a million other things. There is, in short, enough risk baked in here to give a level 2 CFA a case of the vapors.

Nonetheless, this isn't all a fiction or a Ponzi; there is a thread of logic that runs through the entire system, and there is absolutely something there to yield farming as a premise. Iron Finance was the latest in a long line of projects to look to take advantage of that general system. You had IRON, an algorithmic stablecoin that formed the core of the project, that we'll discuss in the next section; and you had STEEL and TITAN, which were the native tokens that allowed said system to operate.

Again, we don't want to go too complex here, but short version: the protocol had its own coins, it needed a way to issue them, and hence you had farming pools set up wherein one could stake assets for liquidity provision (mainly on Binance Smart Chain exchange QuickSwap) and in return get a share of that regular new issuance. Crucially, APRs on these were extremely high, especially (relatively speaking) on the stablecoin pools; a post on a Japanese personal blog showed a 138% nominal APR on a pool where one deposited IRON or BUSD and received STEEL on June 13th:



Via awajifishing.com.

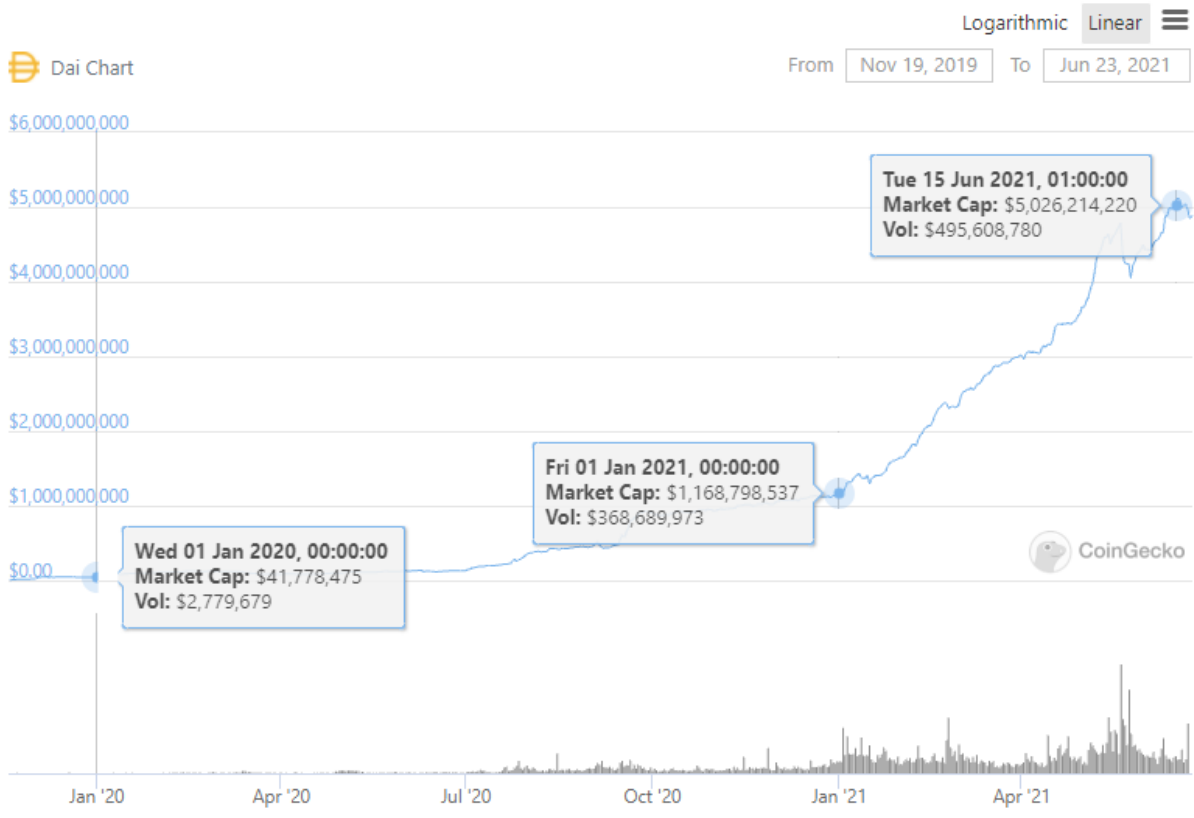
Algorithmic stablecoins

Now, so far, we have been assuming that you know what a stablecoin is. If you don't: it's a token that's intended to match the price of a fiat currency (or occasionally another external commodity like gold), most usually the US dollar. The eternal criticism of crypto over the years has of course been the fact that, because of the nature of crypto assets as naturally unpegged, anyone holding and dealing in crypto either has to deal with constant fluctuations in value (to a point that makes it difficult to use it as a means of transaction if one has anything resembling price sensitivity), or has to trust a third-party to hold fiat reserves off-chain (as both USDT and PAX-based stablecoins like USDC operate on the basis of).

While just going ahead and doing the latter has overall become a lot more palatable to even institutional actors over the last couple of years, this clearly is not exactly a good solution for systems that are supposed to be trustless above all else. So, what to do?

Stablecoins that aren't based on third-party pegs are collectively referred to as algorithmic stablecoins (or algostables). Most efforts in that regard have focused on crypto-collateralisation: you deposit crypto tokens valued at X into a system, the system gives you back Y tokens (where Y is some degree less than X) pegged to a fiat currency (almost always USD). If you want to convert back, you simply redeposit the same amount of tokens as you initially took out. **However, if your collateralisation ratio goes too low (i.e. your collateral value plummets), the system automatically liquidates some portion of your collateral; conversely, if it goes higher, you can take out more fiat tokens.**

There were a few attempts to start building systems on that basis pre-2017, but the first really successful implementation of it was MakerDAO's Sai/Dai. The initial contracts were launched at the height of the 2017 bubble, but like many similar innovations, it was stable but essentially novel for a long time, with circulation standing at around $40m as late as January 2020.



MakerDAO's implementation isn't sexy - it requires 150% minimum collateralisation, and only started adding non-ETH collateral assets at all in mid-2019 - but it's been generally effective. Circulation is now near to $5bn, and the network of systems that it essentially operates on in terms of oracles, vaults, etc. have proven robust enough that it's never lost its peg to the downside despite multiple huge drawdowns on ETH and other collateral assets.

Of course, if something isn't sexy, there's going to be pressure to make it sexier. There have been some truly grotesque implementations aimed at getting around collateralisation entirely (hello, Ampleforth), but this basically ends up coming down to finding ways to reduce collateralisation as much as possible.

This is the dragon that Iron Finance were chasing. IRON, the flagship feature of the product, was an algorithmic stablecoin that aimed to stay precisely 100% collateralised, no more or less, by using USDC/BUSD as backing and making the minting of new IRON (i.e. I deposit USDC, I get back IRON) more or less cheap (with STEEL or TITAN used to make up any difference) until the ratio of IRON to USDC/BUSD holdings got to 1.00 again.

The outcome

In the end, these sorts of DeFi projects as a whole tend to go one of three ways.

1) They mature - APRs come down, the system stabilises, and it finds a use in whatever niche it has.
2) They quietly fade away.
3) They get rugged or exploited.

Rugged is short for rugpulled, which in turn is a crypto neologism coming from the expression "to pull the rug from under you". This can take myriad different forms in the specifics, but they overwhelmingly come down to the same thing: somebody, somewhere wrote the smart contract that controls any given yield farm, and hence somebody, somewhere could have written some mechanism into the smart contract to divert all the funds within to themselves.

Iron Finance didn't get rugged. It also didn't get exploited in the stereotypical manner; there was no hole in the smart contract that let some entrepreneurial hacker take everything away. Iron Finance have put out their own explanation, but the short version is that the price of TITAN specifically increased to ludicrous levels due to the frenzy, some large holders started taking advantage of simple arbitrages between the IRON, TITAN, and USDC tokens, this multiplied on itself due to how the creation and redemption process for IRON works (re: printing as much TITAN as necessary to make up for any off-peg discrepancy), essentially hyperinflating the native token.

In truth, this probably still should be called an exploit; it's certainly not the system working as designed. The Iron Finance white paper states that the total planned emission of TITAN was 1 billion, and as Iron Finance's own post reveals, TITAN supply increased to 27,805 billion during this run.

We have seen characterisations of this as a bank run, with comparisons ominously drawn to other stablecoins, and that doesn't really fit what happened here; this was a technical failure more than anything else, from a development team that had seen total systems failure on at least two other recorded instance (to the point that STEEL itself was a replacement for a previous token, SIL, that had hyperinflated due to a supply bug in March). IRON itself had little to no usage outside of the project's own systems (and some apps directly connected to it); while the numbers in terms of assets locked ($2bn+ at the peak) may be eye-popping (though probably inflated by the secondary market price of TITAN), it just isn't comparable to an USDT or an USDC or even a DAI.

In a sense, there is nothing particularly special about Iron Finance; however, it is essentially a microcosm of the vast majority of what goes on in the DeFi space, both for better and for worse:

- It was an attempt to further optimise something that still remains, to some degree, unoptimised.
- It grew and grew on the basis of the promise of massive returns. It was able to offer those returns partially through sleight of hand, and partially through the fact that it was able to essentially print its own money.
- It in the end grew to the point where the prize was large enough to incentive its users to find a way to take advantage of it.
- Someone found a way to take advantage of it, and that was that.

Despite the dangers and pitfalls of the sector, DeFi and all its associated concepts are, thankfully, not going away, and ultimately, this is a rabbit hole that many in traditional finance are likely to have to dive down in coming years. It is already at a stage where the burden of knowledge for new entrants is intimidating; as we mentioned at the start, this was supposed to be as short of a piece as possible, and in only focusing on a couple of core concepts, we've still ended up at over 2000 words.

Sorry. We nonetheless hope that this note has been informative, and hopefully will play its part for many in beginning to build up a base of knowledge in an area that is still generally not well understood.

Until next week – thank you for reading.

ENIGMA SECURITIES

Subscribe on our website

www.enigma-securities.io

ABOUT US

Enigma Securities is a leading, regulated liquidity provider, offering its clients bespoke liquidity solutions through the use of a proprietary electronic trading platform and API access.

The firm was founded in 2017 as a subsidiary of Makor Partners Limited (UK), amid growing institutional demand for digital asset trading. Looking to seize the new, exciting opportunities presented by cryptocurrencies and blockchain technology, Enigma became one of the first regulated brokerage firms to set up banking relationships and custody solutions to meet institutional standards.

Since its launch, the firm has expanded its capabilities to the broader Fintech arena, leading innovation while working to bridge the gap between the traditional financial services industry and cryptocurrency markets.