PIER

PUEY UNGPHAKORN INSTITUTE FOR ECONOMIC RESEARCH

A DeFi Bank Run: Iron Finance, IRON Stablecoin, and the Fall of TITAN

by

Kanis Saengchote

July 2021

Discussion Paper

No. 155

A DeFi Bank Run: Iron Finance, IRON Stablecoin, and the Fall of TITAN

Kanis Saengchote*

Chulalongkorn Business School

This version: 19 July 2021

ABSTRACT

Bank runs are a natural phenomenon for financial institutions that issue fixed value liabilities (e.g. money) that are backed by assets with uncertain value. I analyze Iron Finance, a decentralized finance (DeFi) protocol that issues stablecoin (a token with fixed nominal exchange rate: IRON) liabilities in exchange for a basket of other tokens (including a token issued by the protocol itself: TITAN). A combination of mathematical algorithms and incentive to arbitrage is used to maintain the exchange rate peg, but a shock to the protocol sent it into a downward spiral – much like a bank run. The incentives built into the protocol to defend the peg exacerbated its unravelling, raising the challenge of how DeFi protocols can address this vulnerability while remaining decentralized.

Key words: DeFi, stablecoin, bank run, self-fulfilling panic

---

* Corresponding author. Chulalongkorn Business School, Chulalongkorn University, Phayathai Road, Pathumwan, Bangkok 10330, Thailand. (email: kanis@cbs.chula.ac.th). I would like to thank Unnawut Leepaisalsuwanna for helping me understand how smart contracts and blockchain work and how to make sense of blockchain data.

1. Introduction

The term decentralized finance (DeFi) carries a very a specific meaning: it generally refers to an alternative financial system built on a blockchain-based infrastructure (often public) that promises openness, efficiency, transparency, interoperability, and decentralization (for example, Harvey et al., 2021; Schär, 2021). It is a system of computer algorithms, often referred to as a "protocol" of "smart contracts", that replicates traditional financial services such as lending, exchange, and asset management and structured via a series of tokens, a process typically referred to as "tokenization".[1] This allows any token, including pre-existing cryptocurrencies, that belongs to the blockchain to be part of the protocol.

One of the problems for a tradeable tokenized system that relies on token price is price instability, as evident in many cryptocurrencies (for example, Bouri et al., 2019), so many sponsors provide tokens with fixed nominal exchange rate to national currency such as the US dollar. Such tokens are referred to as "stablecoins" and, as the name suggests, provides stability in the volatile world. There are many ways of creating and ensure price stability of stablecoins, but they share the insights from the international finance literature on exchange rate mechanisms and their defenses. Trust in the value of collateral (e.g. gold and foreign exchange reserves) and arbitrage activities are what keep exchange rates stable.

There are three main ways of collateralizing a stablecoin using on-chain tokens: first, by using external tokens not part of the protocol, such as Ethereum (ETH); second, by using internal [native] tokens that are issued [minted] by the protocol; third, by a mixture of both. The first type is often referred to as a "collateralized" stablecoin, while the latter two as "algorithmic" stablecoin. This is semantics, as all stablecoins must be collateralized by something.[2] In this paper, I analyze Iron Finance – an algorithmic DeFi stablecoin (IRON) protocol collateralized by a combination of

[1] On blockchains capable of smart contracts such as Ethereum, a token [cryptocurrency] is one type of smart contract, which means a smart contract can also be a tradeable token with a set of instructions embedded in it. A token can be imbued with rights, such as voting or cash flow rights, making it more like a security; with ability to exchange for goods and services, making it more like an IOU; or with nothing at all, making it more like an informational commodity. It is important to note that it is the imbued rights that define the nature of the token, and smart contracts are simply algorithms that automate certain calculations that can be used to replicate financial services via transfers of information.

[2] Another type of stablecoin is "national-currency-backed", which is issued by sending US dollars to a sponsor in exchange for a fixed price token such as Tether (USDT) and USD Coin (USDC). These stablecoins are not considered DeFi since they require users to trust sponsors to safekeep their collateral rather than smart contracts. See Lyons and Viswanath-Natraj (2020) for an overview of stablecoins and Kozhan and Viswanath-Natraj (2021) for a detailed analysis of MakerDAO, the world's first decentralized stablecoin that uses collateralized debt position mechanism (a collateralized stablecoin), and how collateral stability increases peg stability.

another stablecoin (USDC) and its native token (TITAN) that runs on the Polygon blockchain – and how its mechanism design and collateral choice makes it susceptible to a run.[3]

The general process of minting stablecoins involves exchanging something under pre-specified rules. For USDC, it involves sending US dollars, which is not native to blockchain, to Circle – USDC's sponsor – and they will send an equivalent amount of USDC in return, thus USDC is not a decentralized [DeFi] stablecoin. For IRON, it involves sending USDC and TITAN. Since both USDC and TITAN are native to the Polygon chain, IRON is considered a DeFi stablecoin. The ratio of USDC to $1 worth of IRON minted is referred to as Target Collateral Ratio (TCR). The rest will be made whole by the appropriate number of TITAN tokens at the prevailing price, so if TITAN price is high, fewer tokens are required to complete the minting. Users can send [redeem/burn] IRON to receive USDC and TITAN, and the ratio of USDC to $1 worth of IRON redeemed is referred to as Effective Collateral Ratio (ECR). The two ratios can be different, depending on whether the price of IRON is off the $1 peg and how much USDC there is in the protocol's reserve. In other words, IRON is backed by the *value* of USDC and TITAN but the number of USDC and TITAN tokens required to make up the value will depend on their prices. A graphical overview, see Figure A1 in the appendix.

TITAN – a native token minted by Iron Finance and not imbued with any specific right – has two uses: first, TITAN is required to mint IRON, so users need to purchase it. Second, TITAN can be entered [staked] along with a companion token into "liquidity pools" that make market for traders who are looking to buy and sell tokens.[4] Iron Finance has 4 pools in 3 token pairs: USDC-IRON (two pools), TITAN-IRON and TITAN-MATIC. Users who stake tokens in these pools to

---

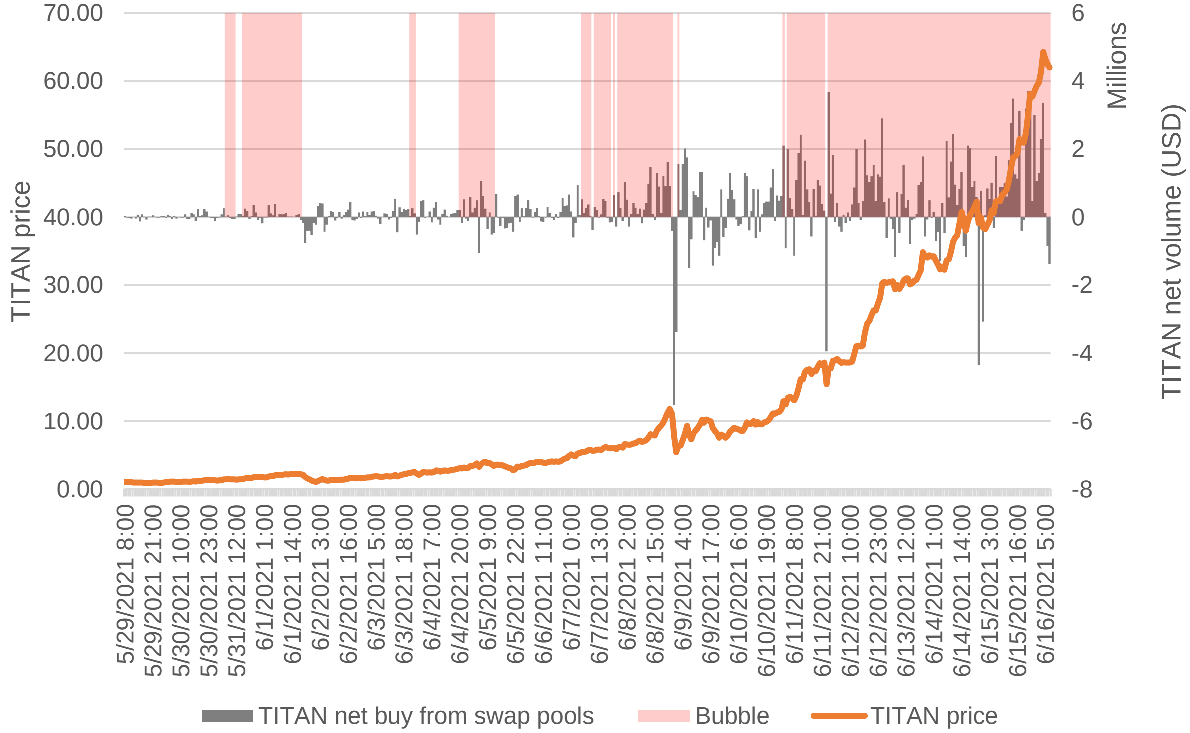
[3] Polygon is an alternative blockchain to the Ethereum blockchain that is also capable of smart contracts. The Ether (ETH) equivalent on Polygon is MATIC. There are two universes of the Iron Finance protocol: the first is the Polygon version, where the stablecoin is IRON and native token TITAN (for titanium), and the second is the Binance Smart Chain version (another smart contract blockchain), where the stablecoin is also IRON and native token STEEL. Both operate independently, but protocols that allow a token on one chain to convert to an equivalent one on another exist.

[4] Liquidity pools often comprise pairs of tokens, and market making mechanism is done via a "bonding curve" that algorithmically determines the exchange ratio (hence, price) based on the relative number of tokens in the pool. It generally works as follows: send x units of token A to receive y units of token B. The popular algorithm is $xy = k$, where the exchange ratio is the ratio of two token quantities. When x increases and y decreases, the price changes, so large changes in x and y lead to large fluctuations in price. The larger the pool (deeper liquidity), the less price slippage, so protocols incentivize staking by providing rewards (see Harvey et al., 2021), often distributed in native tokens. More complex versions that involve more than two tokens also exist. For a technical explanation, see Xu et al. (2021). The main protocols used by Iron Finance are SushiSwap and QuickSwap.

provide liquidity earn TITAN as incentives.[5] The protocol launched on May 18, 2021, but all its smart contracts were operational on May 29, 2021. At that point, it was emitting 735,158 TITAN per day. Iron Finance envisioned total emission of 1 billion TITAN in total, with 700 million emitted as rewards over 36 months and 300 million for protocol sponsors, to be vested linearly over 12 months.

Figure 1: TITAN (native token) price and bubble stamping, pre-run.

This figure plots the hourly closing prices of TITAN, obtained from Iron Finance's swap pools between 8:00am UTC of May 29, 2021, to 8:00am UTC of June 16, 2021. The value of net buy transactions (in $ million) in each hourly bucket is reported as bars on the secondary axis. The shaded regions are buckets which are stamped as bubble using the methodology of Phillips et al. (2015), also used by Bouri et al. (2019). During the 3-week window, there are multiple episodes of bubble-like price runups.



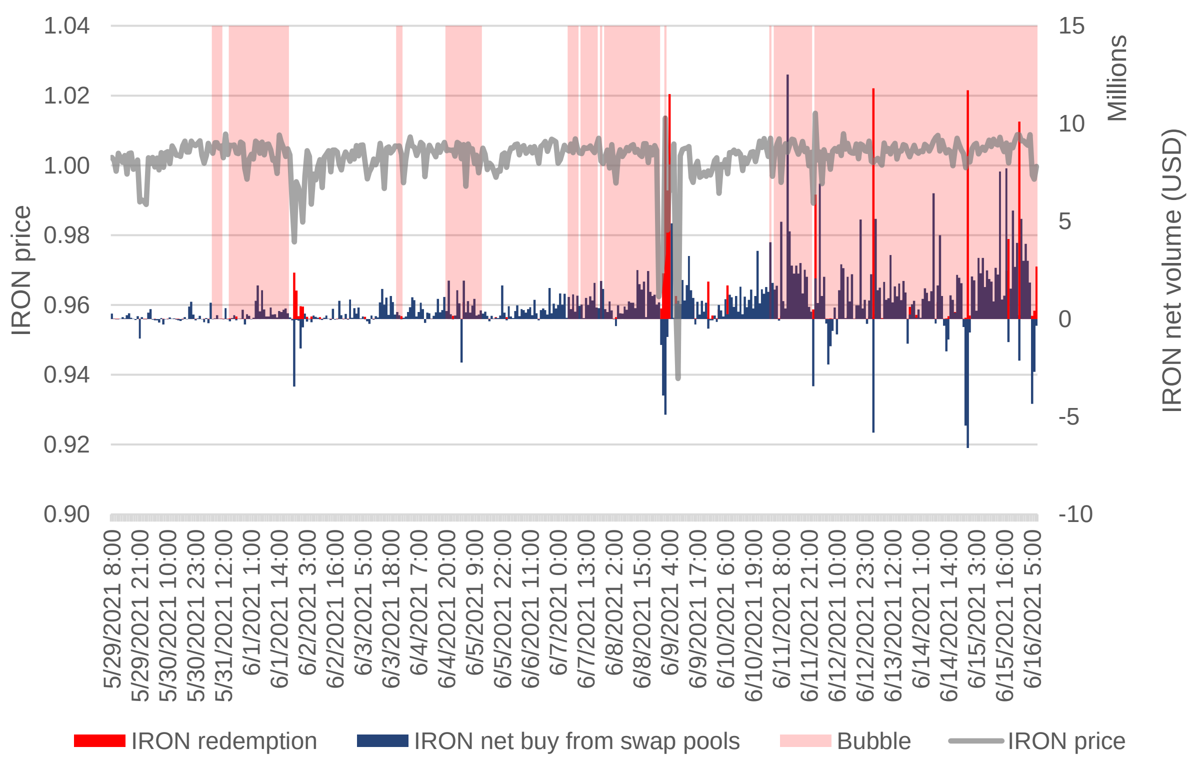
I use visualizations of transaction-level blockchain data (to be further described) to illustrate how Iron Finance works. In Figure 1, the hourly closing prices of TITAN between 8:00am UTC of May 29 to 8:00am UTC of June 16 is plotted with the net dollar volume of TITAN bought. I also highlight periods identified as bubbles using the methodology of Philips et al. (2015). Like many cryptocurrencies analyzed by Bouri et al. (2019), TITAN also experienced

[5] This practice is referred to as "liquidity mining" in an (inaccurate) analogy to blockchain mining and "yield farming" in an analogy to growing tokens on fertile protocols. The yield depends on how the generous the emission schedule is and how fast the token price increases.

multiple episodes of bubble-like price runups, but over a much shorter timeframe. Generous emission schedule (even for stablecoin pair) and rapid appreciation make TITAN staking rewards more valuable, which, in turn, make both IRON and TITAN more sought after, like a flywheel. I plot the hourly closing price of IRON during the same window in Figure 2. IRON had lost its peg several times due to net sales, which can be thought as an outflow from the protocol, as the only way to sell IRON is to swap it for USDC via one of the two liquidity pools. Selling pressure depressed price, so arbitrageurs could buy IRON for below $1 and profitably redeem it for $1 worth of USDC and TITAN. The red redemption bars in Figure 2 indicate that users indeed behaved as intended. Arbitrageurs play an important role in price stabilization, a conclusion also reached for other stablecoins by Lyons and Viswanath-Natraj (2020). The algorithm worked and price stabilized, until it did not on June 17, as TITAN price began falling. A DeFi bank run had occurred.

Figure 2: IRON (stablecoin) price and redemption, pre-run.

This figure plots the hourly closing prices of IRON, obtained from Iron Finance's swap pools between 8:00am UTC of May 29, 2021, to 8:00am UTC of June 16, 2021. The value of net buy transactions (in $ million) in each hourly bucket is reported as bars on the secondary axis. The shaded regions are buckets which are stamped as bubble (of TITAN's price) using the methodology of Phillips et al. (2015), also used by Bouri et al. (2019). During the 3-week window, there have been multiple episodes where IRON significantly deviates from the $1 peg.



In the rest of the article, I examine the unravelling of Iron Finance, how users behaved during the episode, and show how the protocol worked exactly as programmed, but toward an unintended outcome instead.

2. Data and Empirical Methodology

The Polygon blockchain data used in this article is obtained from Google BigQuery, which is hosted and listed the Google Cloud Marketplace. Token transfers between protocol addresses and related addresses can reveal insights about the protocol: for example, one can identify staking activities in liquidity pools (and hence relative token prices during that block in that pool), the quantities of net buys, token minting and redemption and collateral ratios between IRON and USDC (TCR and ECR).[6] The list of Iron Finance and related addresses is provided in the appendix.

In this study, I am interested in the prices of IRON and TITAN, the minting and redemption of IRON, the net buy volume of IRON and the minting of TITAN between 8:00am of May 29 to 2:00am of June 18. I divide the timeframe into overlapping windows: the first window is 8:00am of May 29 to 8:00am of June 16, used in Figure 1 and 2 to illustrate pre-run period prices in 1-hour interval; the second window is 12am of June 16 to 2am of June 18, used to illustrate prices during and after the run in 10-minute interval; the third window is 12am of June 16 to 12am of June 18, used to illustrate token minting and redemption in 10-minute interval. I omit the last 2 hours because the number of TITAN minted during those hours will reach *trillions*, making data visualization very difficult. Summary statistics are reported in Table 1.

Table 1: Summary statistics

Panel A reports the summary statistics of IRON (stablecoin) and TITAN (native token) prices during 2 windows: pre-run (May 29 to June 16) and during the run (June 16 to June 18). The frequency of prices is 1-hour during the pre-run window and 10-minute during the run window. Prices are obtained from Iron Finance's swap pools and quoted in $. Panel B reports the summary statistics of token minting, redemption and net trading activities during the run at 10-minute intervals. Units are reported in millions of tokens. Time zone is coordinated universal time (UTC).

Panel A: Token prices

Unit: $	IRON	TITAN	IRON	TITAN
Start time	May 29, 8am	May 29, 8am	June 16, 12am	June 16, 12am
End time	June 16, 8am	June 16, 8am	June 18, 2am	June 18, 2am
Frequency	Hourly	Hourly	10-minute	10-minute
Mean	1.00	18.79	0.83	12.40
Std. dev.	0.01	24.70	0.16	15.15

[6] All activities in swap pools (staking, unstaking and token swapping) can be used to infer prices, but because a blockchain transaction often involves multiple steps which may incur transaction fees, staking transactions are the simplest way to infer prices.

Median	1.00	0.00	0.75	5.57
Maximum	1.01	64.32	1.01	64.30
Minimum	0.94	0.00	0.48	0.90
Skewness	-4.81	0.79	-0.10	1.57
Kurtosis	38.00	1.90	1.43	4.53
Jarque-Bera	23,770.75	46.49	31.53	220.41
p-value	0.0000	0.0000	0.0000	0.0000
ADF	-12.74	-3.52	-1.59	2.99
p-value	0.0000	0.0075	0.4867	1.0000

Panel B: Token minting, redemption, and net purchase transactions

Unit: million tokens	Mint IRON	Redeem IRON	Net Buy IRON	Mint TITAN
Start	June 16, 12am	June 16, 12am	June 16, 12am	June 16, 12am
End	June 18, 12am	June 18, 12am	June 18, 12am	June 18, 12am
Frequency	10-minute	10-minute	10-minute	10-minute
Mean	0.57	3.59	-3.79	5,820
Std. dev.	1.61	5.47	7.32	65,000
max	13.10	30.30	17.70	781,000
p90	1.57	12.00	1.23	0.59
p75	0.25	5.01	0.45	0.06
p50	0.04	0.75	-0.61	0.00
p25	0.01	0.01	-7.13	0.00
p10	0.00	0.00	-13.70	0.00

To examine behavior during the run, I regress log of IRON minting and redemption quantities (y_{it}) on proxies for arbitrage profits.[7] The first proxy is an indicator variable which takes value of one when it is profitable to buy IRON and redeem for TITAN and USDC. The second proxy is the arbitrage profit of the transaction, quoted in cents. I assume that the arbitrageur will pay a 0.3% fee buying IRON and another 0.3% for swapping TITAN (to, for example, USDC) and hold USDC as it is.[8] I also control for movements in prices of TITAN and IRON. To address potential autocorrelation, I use the Newey-West standard error with lag of 1 period (10-minute block).

$$y_t = \alpha + \beta_1 Profit_t + \beta_2 \ln(TITAN)_t + \beta_3 \ln(IRON)_t + \varepsilon_t$$

[7] There are several arbitrage strategies available. Details are provided in the appendix.

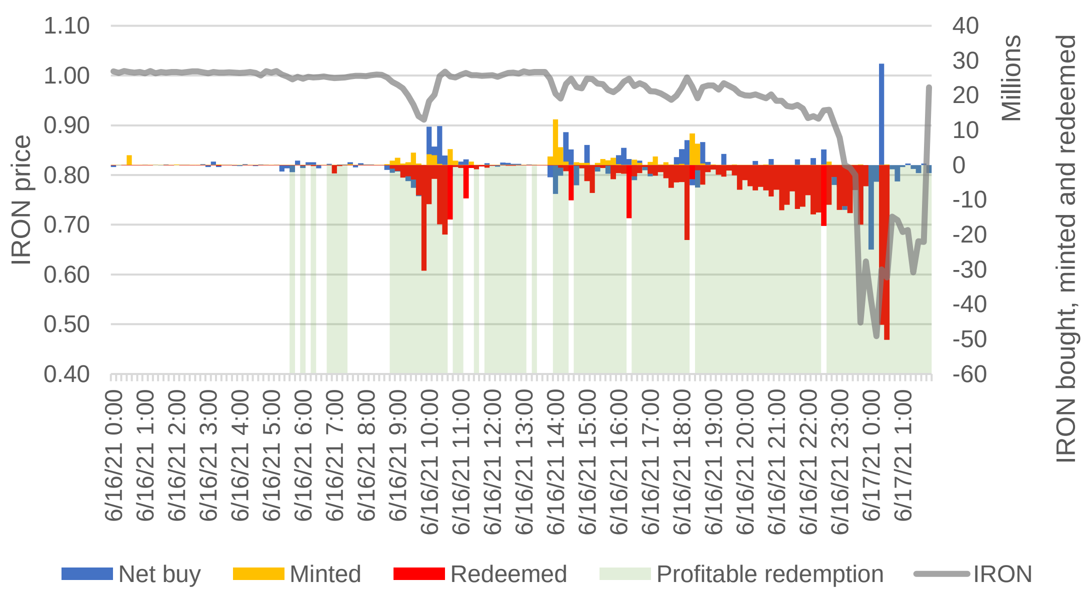
[8] The alternative to buying IRON on the open market is to use the Zap function of Iron Finance, where users can send USDC and get IRON at a fixed price of 1.003 USDC (in other words, $1 plus 0.3% fee). I calculate the arbitrage profit from the minimum cost of the two methods. 0.3% is the typical DeFi fee for using liquidity pools to swap tokens.

3. Results

I begin this section by visualizing the data. Figure 3 plots IRON price at 10-minute intervals. Around 8:40am of June 17, large amount of TITAN and IRON was unstaked from all 4 liquidity pools and swapped out of the protocol via the pools, causing both TITAN and IRON prices to drop. It is important to note that the magnitude of liquidity leaving the protocol was significant: across the two stablecoin (USDC-IRON) pools, a net amount of 100 million IRON was unstaked – tens of times greater than the usual amount – and executed by large users (referred to as "whales"). IRON lost its peg, falling to $0.911 by 10:00am and began to recover as arbitrageurs bought IRON to redeem. I highlight the buckets where buy-to-redeem is profitable in green (see details of arbitrage strategies in the appendix). The fall in TITAN price is more pronounced, dropping from the all-time-high price of $63.78 at 5:10am to $30.58 by 10:10am, as illustrated in Figure 4.

Figure 3: IRON price off-the-peg and the run.

This figure plots the 10-minute closing prices of IRON, obtained from Iron Finance's swap pools between 12:00am UTC of June 16, 2021, to 2:00am UTC of June 18, 2021. The number of IRON tokens traded in swap pools, minted, redeemed in each 10-minute bucket is reported as bars on the secondary axis. The shaded regions are buckets where buying IRON to redeem for USDC and TITAN, net of fees, is profitable (hence, arbitrage profit), increasing the incentive to buy IRON to redeem.



Let us turn to the regression results, reported in Table 2, which show that users indeed redeem IRON more when arbitrage opportunity exists. Readers may be perplexed as to why users also seem to mint IRON more, but this is also a rational behavior. It turns out that the price data used to calculate how many TITAN tokens are provided along with USDC depends on a time-weighted average price (TWAP) over the past 10 minutes, so there exists conditions where it is profitable to mint IRON to burn – specifically when IRON price is below $1 and TITAN price is falling. This helps explain the negative coefficient on lagged log IRON price in model 3.[9] For both discrete and continuous definitions of arbitrage profit, the propensity to redeem IRON is greater when it is profitable to do so. A 1-cent increase in arbitrage profit is associated with a 117.6% increase in minting and a 62.9% increase in redemption (mean: 0.92 cent, standard deviation: 1.54 cent per IRON).

Table 2: Minting and redemption

This table reports the result from the regressions of log IRON minting and redemption on proxies for arbitrage profits. Profitable arbitrage (model 1 to 4) is an indicator variable which takes value of one when it is profitable to buy IRON and redeem for TITAN and USDC. Arbitrage profit (model 5 and 6) is the numerical value of the profit, quoted in cent, assuming the user will pay a 0.3% fee buying IRON (or Zap USDC to IRON for 1.003 USDC each) and another 0.3% for swapping TITAN (to, for example, USDC) and hold USDC as it is. Model 3 to 6 control for lagged log prices of TITAN and IRON. Standard errors are computed using the Newey-West procedure with one-bucket lag and reported in parenthesis. Stars correspond to statistical significance level, with *, ** and *** representing 10 percent, 5 percent and 1 percent level respectively.

	(1)	(2)	(3)	(4)	(5)	(6)
VARIABLES	Ln(Mint)	Ln(Redeem)	Ln(Mint)	Ln(Redeem)	Ln(Mint)	Ln(Redeem)
Profitable arbitrage	1.140**	6.022***	1.297**	3.986***		
	(0.443)	(0.639)	(0.589)	(0.676)		
Arbitrage profit					1.176***	0.629**
(unit: 1 cent)					(0.326)	(0.267)
Lagged ln(TITAN)			1.383***	-0.561*	0.950**	-0.976*
			(0.394)	(0.330)	(0.479)	(0.495)
Lagged ln(IRON)			-34.52**	-52.74***	26.90	-56.49**
			(16.363)	(11.623)	(24.144)	(24.011)
Constant	10.09***	8.20***	4.67***	10.60***	6.73***	13.77***
	(0.279)	(0.560)	(1.587)	(1.588)	(1.905)	(2.013)

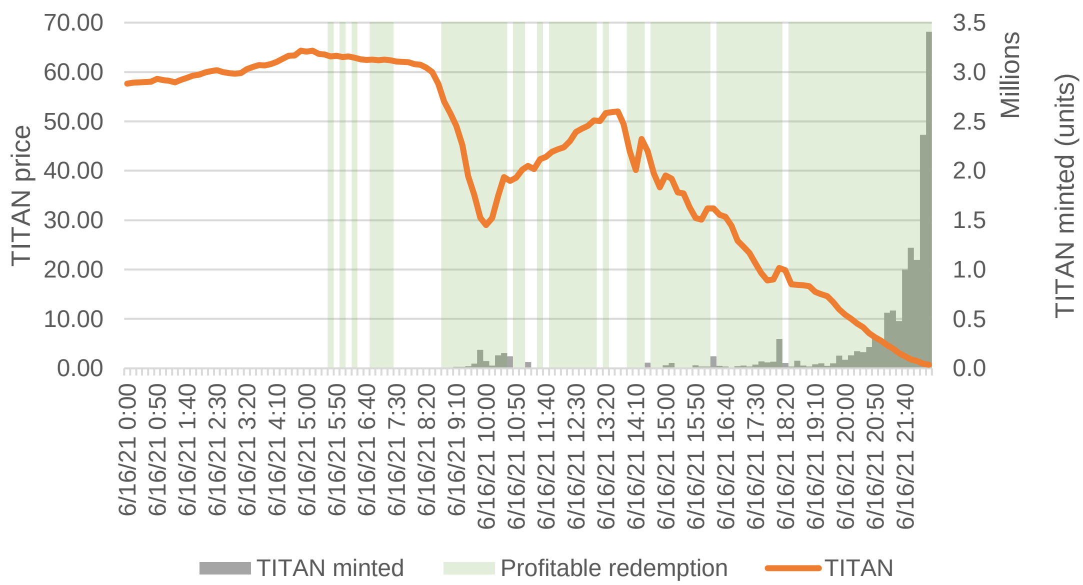
The negative coefficient of lagged log TITAN price in model 4 and 6 also seems perplexing: why would users be more likely to redeem IRON when TITAN price is falling? It turns out this result highlights the susceptibility of Iron Finance to a panic and thus a self-fulfilling run.

[9] In an unreported regression which I omit for brevity, I find that the minting is more likely to occur when both arbitrage opportunities exist. The moral of the story is the same: people respond to incentives, and arbitrageurs will execute all profitable strategies they could find. For the protocol, however, minting rather than buying IRON is problematic for both IRON and TITAN price, as it does not increase demand for IRON but still increases supply of TITAN.

While the profitable redemption of IRON is supposed to increase the demand for IRON and thus stabilize price, redemption leads to new creation of TITAN. As users sell TITAN to realize profit, TITAN price is further suppressed, making the redemption mint even more TITAN per IRON redeemed. Quantities of TITAN that were emitted in days were now being minted in just an hour. Around 2:00pm, another round of unstaking and selling occurred. As the prices of *both* TITAN and IRON continued falling for unknown reason, users who observed this situation unfold may have lost their confidence in the protocol, turning this into a self-fulfilling panic in the fashion of Diamond and Dybvig (1983). Capital flight from the protocol ensued.

Figure 4: TITAN (native token) minted from redemption of IRON.

This figure plots the 10-minute closing prices of TITAN, obtained from Iron Finance's swap pools between 12:00am UTC of June 16, 2021, to 2:00am UTC of June 18, 2021. The number of TITAN minted from IRON redemption in each 10-minute bucket is reported as bars on the secondary axis. The shaded regions are buckets where buying IRON to redeem for USDC and TITAN, net of fees, is profitable (hence, arbitrage profit), increasing the incentive to buy IRON to redeem, which in turn increases the supply of TITAN. As TITAN price falls, even more TITAN is minted when IRON is redeemed.



Between 8:40am of June 16 to 12:40am of June 17, more than 612 million IRON were redeemed, resulting in over 25.3 trillion TITAN minted (remember, there were supposed to be 1 billion to be emitted over 3 years), 24.5 trillion of which were minted in just 20 minutes. Iron Finance halted operation until 5:00pm of June 17. Once it reopened, waves of redemptions resumed as IRON continued to trade below or close to \$0.7467, the ECR that determines how many USDC a redeemed IRON will receive. At that point, it would be profitable to buy IRON and redeem just get USDC, and while TITAN price was low, users would get trillions of TITAN whose

value would still make up the full dollar, but users seemed disinterested.[10] TITAN continued to trade at around 6×10^{-8} as trillions more were minted from redemption.

4. Conclusion

In this article, I document the rise and fall of TITAN, the native token of Iron Finance, and how the rapid price decline contributed the protocol run, highlighting the risk of stablecoins collateralized by native tokens. Bank runs are a natural phenomenon for financial institutions that issue fixed value liabilities (e.g. money) that are backed by assets with uncertain value. Under this definition, many entities can be considered a bank, for example, a money market mutual fund, or even Iron Finance.[11] In September 2008, a single money market mutual fund "broke the buck" and triggered a market-wide run that eventually unfolded into the global financial crisis (Schmidt et al., 2016). For Iron Finance, its fall did not spillover to other protocols (popular stablecoins are unaffected by this episode), but IRON was on Polygon, and it was largely unconnected to other protocols (see Figure A3 in appendix). Had it been on more proliferated chains such as Ethereum, interoperability can make tethered DeFi protocols vulnerable to contagion.

Trust is the cornerstone of the financial system, and beliefs play a crucial role: even rumors can trigger runs on the financial system (He and Manela, 2016), and institutional arrangements or government interventions are often the solution to this instability. Thus, it remains to be seen how DeFi – the promise of an alternative financial system with transparency and openness, free of institutional intervention – will address this vulnerability inherent in every financial system.

[10] One reason why there is little such arbitrage could be due to how IRON tokens can be acquired at that price. Users must swap USDC for IRON in one of the 2 USDC-IRON pools (other choices are TITAN-IRON and IRON-MATIC, but not as deep as the stablecoin pools), but the same pools are also exit routes as they swap IRON for USDC. The arbitrage requires users to lean against the wind, but they may be too busy fleeing the protocol.

[11] In the post-mortem blog post, Iron Finance reminds readers that it "…is a partially collateralized stablecoin, which is similar to the fractional reserve banking of the modern world. When people panic and run over to the bank to withdraw their money in a short period, the bank may and will collapse." (https://ironfinance.medium.com/iron-finance-post-mortem-17-june-2021-6a4e9ccf23f5)

REFERENCES

Bouri, E., Shahzad, S. J. H., & Roubaud, D. (2019). Co-explosivity in the cryptocurrency market. *Finance Research Letters*, 29, 178-183.

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy*, 91(3), 401-419.

Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). DeFi and the Future of Finance. Available at SSRN 3711777.

He, Z., & Manela, A. (2016). Information acquisition in rumor ‐ based bank runs. *The Journal of Finance*, 71(3), 1113-1158.

Kozhan, R., & Viswanath-Natraj, G. (2021). Decentralized Stablecoins and Collateral Risk. *WBS Finance Group Research Paper*.

Lyons, R. K., & Viswanath-Natraj, G. (2020). What keeps stablecoins stable? (No. w27136). *National Bureau of Economic Research*.

Phillips, P. C., Shi, S., & Yu, J. (2015). Testing for multiple bubbles: Historical episodes of exuberance and collapse in the S&P 500. *International Economic Review*, 56(4), 1043-1078.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review*.

Schmidt, L., Timmermann, A., & Wermers, R. (2016). Runs on money market mutual funds. *American Economic Review*, 106(9), 2625-57.

Xu, J., Vavryk, N., Paruch, K., & Cousaert, S. (2021). SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols. arXiv preprint arXiv:2103.12732.

APPENDIX

Iron Finance Smart Contracts

Name	Polygon Address	Description
IRON token	0xd86b5923f3ad7b585ed81b448170ae026c65ae9a	Iron Finance's stablecoin.
TITAN token	0xaaa5b9e6c589642f98a1cda99b9d024b8407285a	Iron Finance's native token.
USDC-IRON SushiSwap	0x85de135ff062df790a5f20b79120f17d3da63b2d	Liquidity pool to support market making. Eligible for TITAN reward.
USDC-IRON QuickSwap pool	0x099ce8f12d9824f7441950759d2999022b717ff2	Liquidity pool to support market making. Eligible for TITAN reward.
USDC-IRON QuickSwap token	0x2bbe0f728f4d5821f84eee0432d2a4be7c0cb7fc	QuickSwap administers LP token and pool separately.
TITAN-IRON SushiSwap	0x35c1895dac1e2432b320e2927b4f71a0d995602f	Liquidity pool to support market making. Eligible for TITAN reward.
TITAN-MATIC SushiSwap	0xa79983daf2a92c2c902cd74217efe3d8af9fba2a	Liquidity pool to support market making. Eligible for TITAN reward.
MasterChef0	0x65430393358e55a658bcde6ff69ab28cf1cbb77a	Accounting system for TITAN-MATIC and USDC-IRON staking.
MasterChef1	0xb444d596273c66ac269c33c30fbb245f4ba8a79d	Accounting system for TITAN-IRON staking.
MasterChef2	0xa37dd1f62661eb18c338f18cf797cff8b5102d8e	Accounting system for TITAN staking (minor part of protocol).
ZapPool	0xc7b1f244397e2157036a89ce0d58f3a467a7ed2f	Exchanges USDC to IRON for 1.003 USDC per IRON.
CollateralReserve	0xec12b5d70a84895f819fe037dc4eabdbd24707f2	Processes minting and redemption of IRON for USDC and TITAN.
TITAN reward emitter 1	0xf622a4e83ecbcfb7d8cb3007a3c6b03bcda8666b	Sends TITAN reward for TITAN-MATIC and USDC-IRON staking.
TITAN reward emitter 2	0xe07f9242a58f59dc585eef0620ca88940aa86205	Sends TITAN reward for TITAN-IRON staking.

Related Smart Contracts

Name	Polygon Address	Description
Mint/burn address	0x0000000000000000000000000000000000000000	Polygon-based tokens (e.g. TITAN, IRON) minted and burned here.
USDC token	0x2791bca1f2de4661ed88a30c99a7a9449aa84174	Circle's USD Coin on Polygon blockchain.
MATIC token	0x0d500b1d8e8ef31e21c99d1db9a6444d3adf1270	Polygon chain's native token, used to pay gas.
WETH token	0x7ceb23fd6bc0add59e62ac25578270cff1b9f619	Wrapped Ether (WETH) token on Polygon chain.
TITAN-WETH SushiSwap	0x95ad49c07a50da43770a85bc4a1f4abf7e58b1af	Liquidity pool to support market making. Not eligible for reward.
TITAN-USDC SushiSwap	0xe4984fc367ab9a8c9dc6978d5c0d22c6626c6c54	Liquidity pool to support market making. Not eligible for reward.
IRON-MATIC SushiSwap	0xe600c9c1a0faa03b055924eead9498adb3e63fef	Liquidity pool to support market making. Not eligible for reward.
TITAN-IRON QuickSwap	0xa3a91979fb88561886577fc85ce84cb44f625262	Liquidity pool to support market making. Not eligible for reward.
TITAN-WETH QuickSwap	0xe600c9c1a0faa03b055924eead9498adb3e63fef	Liquidity pool to support market making. Not eligible for reward.
TITAN-MATIC QuickSwap	0x1b29d2af57e90111aebc69b2f757a7263cb54932	Liquidity pool to support market making. Not eligible for reward.
TITAN-USDC QuickSwap	0x8af511761c74af631258d8ee6096679ff4838cde	Liquidity pool to support market making. Not eligible for reward.
Polycat Finance Contract 1	0x83e6250c35617869a1e91ede86702be21f1933e8	Yield aggregator protocol that optimizes yield farming rewards.
Polycat Finance Contract 2	0xbda1f897e851c7ef22cd490d2cf2dace4645a904	Yield aggregator protocol that optimizes yield farming rewards.
Polycat Finance Contract 3	0x8cfd1b9b7478e7b0422916b72d1db6a9d513d734	Yield aggregator protocol that optimizes yield farming rewards.
Polycat Finance Contract 4	0xfe9156d1efa7d24ae31da2eee05b124d3be01327	Yield aggregator protocol that optimizes yield farming rewards.

Iron Finance Arbitrage Strategies

Arbitrage strategies involve exploiting the discrepancy between alternative ways of acquiring and disposing of IRON. There are three strategies available:

1. **Buy-to-redeem.**

This involves buying IRON, either from swap pools or from its Zap function that allow users to send 1.003 USDC for 1 IRON without exerting any price pressure on the pools. Then, IRON is redeemed for USDC and TITAN, which is minted, adding to its circulating supply. I assume that the arbitrageur will want to exit the TITAN position but keep USDC on hand, so the transaction fee is only applicable to TITAN. The arbitrage profit is calculated as redemption value minus acquisition price, defined per unit of TITAN below:

$$Acquire = \min\{P_{IRON} \times (1 + 0.3\%), 1.003USDC\}$$

$$Redeem = ECR \times P_{USDC}Q_{USDC} + (1 - ECR) \times (1 - 0.3\%)P_{TITAN}Q_{TITAN}$$

Effective Collateral Ratio (ECR) determines how much each TITAN is collateralized by the *values* of USDC and TITAN. If TITAN price falls, TITAN quantity minted increases. It turns out Iron Finance does not use the spot TITAN price in the calculation, but instead uses a 10-minute time-weighted average price (TWAP) obtained via its price oracle that processes prices from its liquidity pools to prevent price manipulation from large transactions that could push the exchange ratio too far along the bonding curve. Let P_{TITAN}^{O} be the oracle price, and P_{TITAN}^{S} be the spot price, the value of TITAN sent by the protocol is only worth $k = P_{TITAN}^{S} \,/\, P_{TITAN}^{O}$ of the intended amount. Since redemption of each IRON is pegged to $1, we can express $Redeem$ in terms of dollar value, so:

$$Redeem = ECR \times \$USDC + (1 - ECR) \times (1 - 0.3\%)\$TITAN \times k$$

To see this, let us consider the parameters at 8:50am on June 16. In that bucket, the spot TITAN price was $54.75, and the oracle price was $56.25 (in the previous bucket, the spot price was $57.79). IRON was trading at $0.987, so it was better to buy than Zap an IRON. ECR was 74.57%. Now, suppose the oracle used real-time data, the arbitrage would be 74.57% ($1) + (1 – 74.57%) ($1) (0.997) – (1.003) (0.987) = $0.0094 per IRON since k = 1. With the delayed TWAP price, k = 54.75 / 56.25 = 0.9732, so arbitrage profit falls to 74.57% ($1) + (1 – 74.57%) ($1) (0.9732) (0.997) – (1.003) (0.987) = $0.0025 per IRON – significantly lower but still positive – so arbitrageurs still have an incentive to buy IRON. Combine this demand for IRON with the reduction in circulating supply of IRON via redemption, IRON price should adjust back to the $1 peg. The shaded regions in Figure 3 and 4 are calculated this algorithm.

2. **Mint-to-redeem.**

This involves minting IRON using USDC and TITAN, then burning it for USDC and TITAN again. The ratio of USDC used to mint IRON is governed by Target Collateral Ratio (TCR), which evolves according to the price paths of IRON. If the 60-minute TWAP of IRON is above $1, it will be adjusted downward to make IRON minting increasingly less reliant on USDC (signaling more confidence in TITAN), increasing the circulating supply of IRON, hence lowering its price. The dual collateral ratio (TCR and ECR) is a departure from Frax Finance, a mixed collateral (“fractional-algorithmic”) stablecoin protocol that is the progenitor of Iron Finance. Because IRON prices have often traded above its peg, TCR had trended down from around 90%

(at launch, it was close to 99%) to just 70% by June 16, while ECR was 75.57% (see Figure A2). Again, I assume that the transaction fee is only applicable to TITAN. The arbitrage profit is calculated as redemption value minus minting price, defined in $ per unit of TITAN below:

$$Mint = TCR \times \$USDC + (1 - TCR) \times (1 + 0.3\%)\$TITAN \times k$$

$$Redeem = ECR \times \$USDC + (1 - ECR) \times (1 - 0.3\%)\$TITAN \times k$$

It is straightforward to see that if TCR = ECR and k = 1, this arbitrage cannot exist. However, given how Iron Finance works, it does. Let us consider the parameters at 10:30pm on June 16. In that bucket, the spot TITAN price was $0.3546, and the oracle price was $0.5329 (in the previous bucket, the spot price was $0.7903). IRON was trading at $0.930, while TCR was 72.10% and ECR 73.54%. The arbitrage profit for this transaction is [73.54% ($1) + (1 – 73.54%) ($1) (0.997) (0.6655)] – [72.10% ($1) + (1 – 72.10%) ($1) (1.003) (0.6655)] = $0.0038 per IRON. Now, let us consider the buy-to-redeem arbitrage using the same parameters. The profit would be 73.54% ($1) + (1 – 73.54%) ($1) (0.6655) (0.997) – (1.003) (0.930) = -$0.0219! So, arbitrageurs no longer have an incentive to buy IRON to stabilize price. They will still redeem IRON, but this will have no effect on circulating supply as they redeem the minted tokens. The increased demand for IRON to stabilize the peg is no longer there.

Arbitrageurs can also use the minted TITAN to mint IRON again, and again in a loop, and in the process acquire more USDC via the TCR-ECR spread. Under normal circumstances, users may deem $1 of USDC and $1 of TITAN at a given point in time equivalent in value, but in an environment where TITAN price is rapidly declining, users may prefer to hold USDC rather than TITAN (and, by virtue of their connection, IRON).

3. Mint-to-sell.

The last arbitrage is the reverse mechanism to restore IRON price when it appreciates. It involves minting IRON using USDC and TITAN to sell, in turn reducing IRON price. We can use the equations already defined above. Let us consider the parameters at 4:30am on June 16. In that bucket, the spot TITAN price was $62.94, and the oracle price was $63.13 (in the previous bucket, the spot price was $62.27). IRON was trading at $1.006 (so Iron Finance would want to see this arbitraged down), while TCR was 70.19% and ECR 74.66%. Again, I assume that the transaction fee is only applicable to TITAN. The arbitrage profit for this transaction is ($1.005) (0.997) – [70.19% ($1) + (1 – 70.19%) ($1) (1.003) (1.0132)] = -$0.0028! Again, arbitrageurs do not have any incentive to keep IRON price down.

In fact, the TITAN yield farming rewards are for pools that accept IRON and TITAN. The generous emission schedule for stablecoin pair (USDC-IRON) may be the driving force behind the rapid appreciation of TITAN (as users buy TITAN to mint IRON) and the IRON premium above the $1 peg that persisted for a very long time, in turn suppressing TCR, as observed in Figure A2.

Figure A1: How IRON stablecoins are minted and redeemed.

Users send the smart contract a basket of tokens under the pre-specified rule to receive a stablecoin, which is minted by the smart contract. The smart contract can also redeem the stablecoin for a basket of tokens (potentially different from those sent). The process is often referred to as burning. Stablecoins (and tokens in general) can only be minted and burned in the originating smart contract. For Iron Finance, users are required to send USDC (another stablecoin) and TITAN (Iron Finance's native token) to receive IRON (Iron Finance's stablecoin), and the ratio of USDC to $1 worth of IRON minted is referred to as Target Collateral Ratio (TCR). Users can send IRON to receive USDC and TITAN, and the ratio of USDC to $1 worth of IRON redeemed is referred to as Effective Collateral Ratio (ECR). Creation and redemption price of IRON is fixed at $1 in smart contract calculation, and users can price discrepancy to gain arbitrage profits.

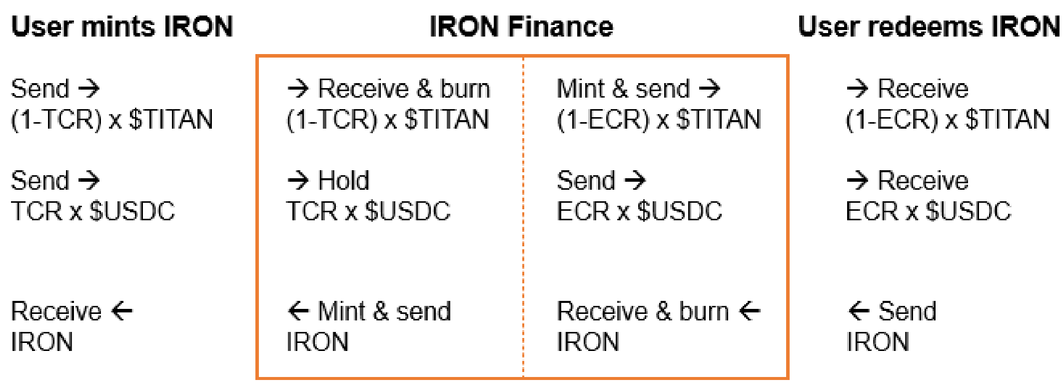


Figure A2: Dual collateral ratios over the entire period.

This figure plots the Target Collateral Ratio (TCR) and Effective Collateral Ratio (TCR) between 8:00am UTC of May 29, 2021, to 2:00am UTC of June 18, 2021. TCR determines the proportion of USDC necessary to mint IRON, while ECR determines the proportion of USDC users will receive for IRON redemption. TCR is reduced if the time-weighted average price of IRON over the last hour is greater than $1, and vice versa. ECR depends on the ratio of USDC in the protocol to outstanding IRON. The shaded regions are buckets where the price of IRON is less than $1, likely to trigger a reduction in TCR (labeled TCR drop). If TCR < ECR, a user who mints IRON and immediately redeems it will end up with more units of USDC and fewer units of TITAN on hand (arbitrage #2).

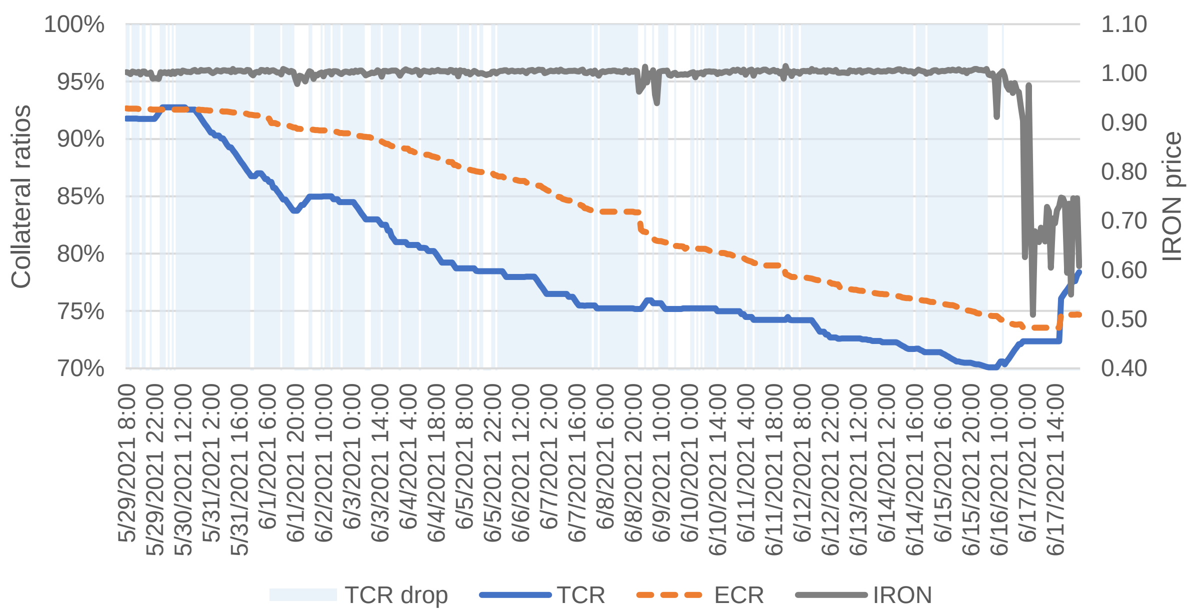


Figure A3: Network diagram of Iron Finance.

This figure plots the token flows between Polygon addresses listed in the appendix ((Iron Finance smart contracts and related smart contracts). Other contracts such as liquidity pools and unknown wallets and smart contracts that are the top 50 list of most active addresses are manually inspected, identified to the best effort, and plotted. To be included in the diagram, addresses must have at least 100 transfers between May 29, 2021, and June 18, 2021. Addresses colored in orange are part of Iron Finance, while addresses colored in pink are liquidity pools. To reduce diagram complexity, only flows of tokens directly related to the protocol (TITAN, IRON, USDC, USDC-IRON SushiSwap LP token, USDC-IRON QuickSwap LP token, TITAN-IRON SushiSwap LP token, and TITAN-MATIC SushiSwap LP token) are plotted. Polycat Finance is a yield aggregator protocol that helps users find liquidity pools that earn the highest staking rewards available.