Operational risks in cryptocurrency-based ventures

Andrej Kolchin

Tether/Bitfinex

Tether [1] is firm which provides USDT, a cryptocurrency "stable coin", which was pegged 1-to-1 to dollar. It maintained this peg by only exchanging one USDT for one dollar[1], and redeeming USDT[2] at the same rate.

---

[1]Until 2019, when the dollars were replaced with "reserves", which include commercial paper [2], [3].

[2]Technically, the terms of service stated that redemption could be denied for arbitrary reasons, but that was the promise.

Banking issues

Tether resisted auditing [4] and, at the same time, could not bank with the major US banks due to governmental regulations.

This caused them to deposit up to 80% with Crypto Capital [5], a Panama bank [6][3]

[3] Which was implicated in money laundering, with its accounts seized [5], but that's a whole other story.

Insolvency

These banking issues eventually caused an insolvency for Tether, during which it lacked the necessary cash reserves to back all of their USDT coins. During this time they also had to undergo an attestation, as a way to reassure investors that their funds were safe.

To account for that, Tether had to commingle funds with their sister firm, an exchange Bitfinex, which had to urgently come up with additional funds in order to complete the attestation. Bitfinex transferred $382 million [7] to Tether on September 15th, 2017.

Bitfinex losses

To come up with that sum of money, Bitfinex most likely had to sell off their Bitcoin reserves. Prior to the attestation the Bitcoin price fell by 40% [8].

Speculatively, Bitfinex might've been to blame for that fall. If we suppose that it was a linear fall in price, Bitfinex might've lost around:

$$382 \cdot \left(1 - \frac{3637}{\frac{4901+3166}{2}}\right) \approx 37$$

Meaning Bitfinex might've lost $30-$40 million.

Factors

The Bitfinex/Tether pair struggled from the following issues:

- Lack of financial audits. Attestations were not able to highlight impending liquidity issues, arising from financial obligations.
- Lack of collateralization.

Alleviation strategies

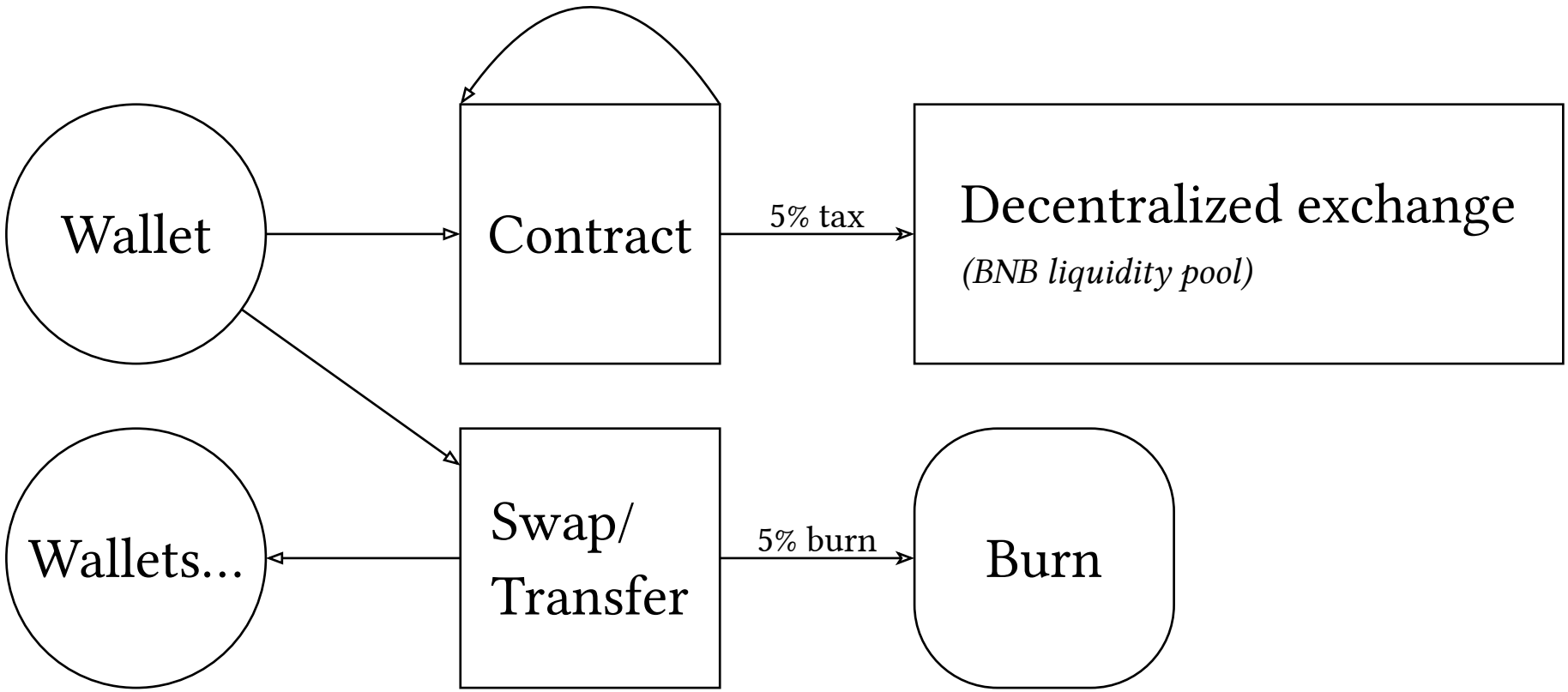
Financial audits a thorough financial audit can highlight management issues and warn the organization of potential liquidity risks ahead of time. A simple attestation cannot do that.

Over-collateralization due to volatility of financial markets, and the cryptocurrency markets in particular, 100% collateralization might often prove insufficient. As such, higher reserves should be required.

Summary

Firm	Tether Limited Inc/iFinex Inc (Bitfinex)
Category	Cryptocurrency firm/cryptocurrency exchange
Event type	External fraud
Events	A collapse of the external bank due to money laundering charges locked up customers funds, preventing Tether from processing withdrawals. This forced the sister exchange to funnel money to Tether.
Losses	~$30-40 million
Outcome	Large monetary losses, loss of customer trust
Alleviation	Additional attestations, shift of the collateralization structure from cash-based to commercial-paper based.

SafeMoon infrastructure [9]



Liquidity pool

SafeMoon used a PancakeSwap liquidity pool [10]. It allows to trade BEP-20 tokens (like SafeMoon) for SafeMoon and visa versa. The price is determined using their relative quantities. So, if there's L_b of BNB in the pool and L_s of SafeMoon, the prices are:

$$p^b = \frac{L^s}{L^b}$$

$$p^s = \frac{L^b}{L^s}$$

Embezzlement

Against the advice of the auditors [11], the liquidity was not locked. This allowed Kyle, the creator of the project, to embezzle the stored funds with 17 (out of 27 total withdrawals) transactions [12], totaling over $10 million [13].

Example transaction: on May 5th 2021 Kyle removes 66 billion SafeMoon tokens, netting him $81 thousand. In total, Kyle removed 54 trillion SafeMoon tokens, decreasing the amounts as the coin's price went up.

v2 migration

To fix the reputation damages, caused by embezzlement, Kyle stepped down from the project and a new CEO took his place. Under his management SafeMoon started a migration to a second version of the SafeMoon protocol. In order to finalize it, the both SafeMoon and BNB from the v1 liquidity pool had to be moved to the v2 one.

This migration of M^s and M^b must be carried out with $\frac{M^s}{L_1^s} = \frac{M^b}{L_1^b}$. This ensures that the $\frac{L_2^s}{L_2^b}$ coefficient (and price) won't spike due to a sudden liquidity move.

Market manipulation

This process was manipulated by the new CEO. In their transactions, instead of moving both M^s and M^b over, They only moved M^b and delayed the deposit of M^s. This caused the v2 price to spike each time, because:

$$\frac{L_2^s + M^s}{L_2^b} > \frac{L_2^s + M^s}{L_2^b + M^b}$$

Manipulation profit and losses

Given the v1 and v2 price similarity ($\frac{L_1^s}{L_1^b} \approx \frac{L_2^s}{L_2^b}$) and the fact that $\frac{M^s}{M^b} \approx p_1^s$, this amounted to a profit of:

$$\left(\frac{L_2^s + M^s}{L_2^b} - \frac{L_2^s + M^s}{L_2^b + M^b} \right) \cdot M^s = \frac{M^b (L_2^s + M^s)}{L_2^b \left(L_2^b + M^b \right)} \cdot M^s \approx$$

$$\approx M^b \cdot M^s \cdot \frac{M^b}{M^s} \cdot \frac{1}{L_2^b} = \frac{\left(M^b \right)^2}{L_2^b}$$

Manipulation profit and losses, 2

This way, the new CEO withheld $143 million, profiting around $64 after the resale [14].

The losses inflicted by those actions are harder to estimate due to market volatility [15] and the fact SafeMoon price crashed soon after due to another case of embezzlement by another CEO. But the total losses must be more than $64 million profited by the CEO and could be more than $100 million.

Factors

Lack of control over the organization's financial system Audits were ignored and the core functions weren't secured against the abuse.

Arbitrage fraud Lack of clear protocols for v1 to v2 migration allowed the CEO, who was controlling the funds, to abuse the market.

Alleviation strategies

Signal amplification mechanisms fixing lack of information about the SafeMoon company's transactions.

Clear economic guidelines strict protocols for all interactions with outside financial markets, mimicking those of supply contracts.

Summary

Firm	SafeMoon LLC
Category	Cryptocurrency company
Event type	Internal fraud/Clients, Products, and Business Practice
Events	Access to internal funds allowed two subsequent CEOs to commit embezzlement, first by plain withdrawals, and then via market manipulation.
Losses	~$200 million
Outcome	Collapse of the cryptocurrency value and the company
Alleviation	Greater transparency, strict market interactions controls

Bibliography

[1] [Online]. Available: https://tether.to/

[2] "Tether website in 2018." [Online]. Available: https://web.archive.org/web/20180203045501/https://tether.to/

[3] "Tether website in 2019." [Online]. Available: https://web.archive.org/web/20191108122055/tether.to

[4] Liam Kelly, "Tether's CEO just told us why the Big Four won't audit reserves backing 108bn stablecoin". [Online]. Available:

https://www.dlnews.com/articles/markets/tether-ceo-just-told-us-why-the-big-4-wont-audit-its-books/

[5] New York State Attorney General, [Online]. Available: https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company

[6] Tim Copeland, [Online]. Available: https://decrypt.co/6759/crypto-capital-quadrigacx-bitfinex

[7] [Online]. Available: https://casetext.com/case/ifinex-inc-v-state

[8] [Online]. Available: https://finance.yahoo.com/quote/BTC-USD/history/?period1=1501545600&period2=1505520000&interval=1wk&filter=history&frequency=1d

[9] "SafeMoon: A Deflationary Reflection Token with Automated Liquidity Acquisition." [Online]. Available: https://web.archive.org/web/20220827043657/https://safemoon.com/whitepaper.pdf

[10] Mike Antolin, "What Are Liquidity Pools?." [Online]. Available: https://www.coindesk.com/learn/what-are-liquidity-pools/

[11] "SafeMoon Audit." [Online]. Available: https://skynet.certik.com/projects/safemoon

[12] “Kyle's transactions.” [Online]. Available: https://bscscan.com/txs?a=0xC95063D946242F26074A76C8A2E94C9D735DFC78

[13] “SafeMoon v1 price chart.” [Online]. Available: https://www.livecoinwatch.com/price/SafeMoonV1-SAFEMOON

[14] [OnlineVideo]. Available: https://www.youtube.com/watch?v=CzbBi0agLNg&list=PLOL7dZiFCN0KHgmUQLQpz4hSwMb70u_1_&index=4

[15] “SafeMoon v2 price chart.” [Online]. Available: https://coinmarketcap.com/currencies/safemoon-v2/