12-2022

Bank error in whose favor? A case study of decentralized finance misgovernance

Ping Fan KE
Singapore Management University, pfke@smu.edu.sg

Ka Chung Boris NG

Dec 12th, 12:00 AM

Bank Error in Whose Favor? A Case Study of Decentralized Finance Misgovernance

Ping Fan Ke
Singapore Management University, pfke@smu.edu.sg

Ka Chung Boris Ng
Hong Kong Polytechnic University, kc-boris.ng@polyu.edu.hk

Bank Error in Whose Favor? A Case Study of Decentralized Finance Misgovernance

Short Paper

Ping Fan Ke
Singapore Management University
80 Stamford Rd, Singapore 178902
pfke@smu.edu.sg

Ka Chung Ng
The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong
kc-boris.ng@polyu.edu.hk

Abstract

Decentralized Finance (DeFi) emerged rapidly in recent years and provided open and transparent financial services to the public. Due to its popularity, it is not uncommon to see cybersecurity incidents in the DeFi landscape, yet the impact of such incidents is under-studied. In this paper, we examine two incidents in DeFi protocol that are mainly caused by misgovernance and mistake in the smart contract. By using the synthetic control method, we found that the incident in Alchemix did not have a significant effect on the total value locked (TVL) in the protocol, whereas the incident in Compound caused a 6.13% decrease in TVL. One factor that contributed to the difference in the result could be the incident response in social media platforms, and further study should investigate the possible moderating or mediating effects of public opinions and sentiment.

Keywords: DeFi, misgovernance, fat-finger error, total value locked, synthetic control, incident response

Introduction

In response to Web3 and the future evolution of finance, decentralized finance (DeFi) emerged in recent years, growing from around 700 million USD in total value locked (TVL) in January 2020 to over 100 billion USD in September 2021 (Werner, et al., 2021). Compared to traditional finance, DeFi aims to offer financial services to the public without the need for centralized intermediaries by leveraging technologies like artificial intelligence, Blockchain, cloud computing, and big data (Zetzsche, Arner, & Buckley, 2020). DeFi also enables financial inclusion, as DeFi provides accessible, efficient, and affordable financial services to the public with the aid of novel financial technologies (Popescu, 2022). For example, a recent report shows that many DeFi users are in an underprivileged situation, such as an Afghan who was restricted from creating a GoFundMe campaign (Resnick, 2022). They often seek advice on social media platforms like Twitter, where some influencers on these platforms will produce free educational content for the DeFi community.

Despite the DeFi community growing rapidly, cybersecurity remains a big challenge. As of 1st September 2022, there are 104 cybersecurity incidents in DeFi documented by CryptoSec[1] since 2020, with total lost funds of about 3.6 billion USD. Although many of these incidents happen in protocols with unaudited smart contracts, some incidents also happened in DeFi protocols audited by professional cybersecurity firms.[2] This means the cybersecurity issue could be easily overlooked, probably due to the complex nature of the technology. For example, by exploiting a race condition vulnerability, an attacker could repeatedly execute a function in a smart contract and drain the fund inside. This is also known as reentrancy vulnerability

[1] https://cryptosec.info/defi-hacks/

[2] https://rekt.news/leaderboard/

(Samreen & Alalfi, 2020), and it affected many smart contracts, from the infamous DAO hack that caused a hard fork in Ethereum to the recent Cream Finance hack that caused an 18.8 million USD loss in the DeFi landscape.

While many of these incidents are initiated by hackers with a deep understanding of sophisticated smart contract vulnerabilities like reentrancy and flash loan attacks, surprising, some of these incidents are triggered by ordinary users who accidentally discovered a bug in the smart contract. Typically, this kind of incident is caused by careless mistakes from the developers and smart contract users. For instance, a non-fungible token (NFT) holder accidentally listed an NFT token for 444 Wei (less than a penny) instead of 444 Ether (around 1.2 million USD), which was immediately bought by a bot (Hall, 2022). This type of mistake not only happens in an individual user but also occurs in large-scale DeFi protocols with a proper governance body. In particular, a DeFi protocol will usually issue tradable tokens to active developers and users based on certain criteria, and the token holders could propose changes to the smart contract and vote with the tokens, similar to the concept of shares of stock in the context of a company.

The token-based voting process is also referred to as governance in the Blockchain context. In general, governance in a corporate setting is the "system by which companies are directed or controlled" (Cadbury, 1992), and typically involves the participation of the board of directors to fulfill the objectives of the stakeholders. The use of the term "governance" in the Blockchain context is originated from the concept of Decentralized Autonomous Organizations, where "decisions are governed by proposals and voting to ensure everyone in the organization has a voice."[3] Besides the most adopted token-based governance, Blockchain governance also includes share-based governance, which requires prospective members to submit a proposal to gain a share from other shareholders to participate in governance, and reputation-based governance, where the voting power is solely gained from participation and cannot be bought, transferred or delegated.

The concept of Blockchain governance is used vaguely in various articles, such as the process of arriving at consensus-relevant changes in the software used in the Blockchain ecosystem (Curran, 2020), the system used by developers and mining nodes for managing and implementing changes to Blockchain (Frankenfield, 2021), or the collective like council and committee who can execute privileged functions to affect the outcome in the Blockchain (Petrowski, 2020). A recent review summarized the concept of Blockchain governance broadly as the "integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organization" (Fischer & Valiente, 2021). In this research, we focus on the most important aspect of Blockchain governance for DeFi protocols – smart contract versioning – that allows the protocol to introduce or modify the features provided. Blockchain misgovernance presents when the smart contract versioning process is not properly conducted; for example, the token holders did not review the code before voting, which could lead to security incidents.

Our research examines how misgovernance or poor management in smart contract versioning affects the valuation of the DeFi protocol in terms of TVL. We will also discuss how other factors in the management process, particularly incident response and public relations management, may help in damage control. To answer the research question, we will discuss two DeFi protocol incidents that are caused by misgovernance and mistake in the smart contract, namely the Alchemix incident and the Compound incident. These two incidents share a similarity in which the vulnerability in the smart contract allows users to claim the asset in the smart contract for free. This type of incident may have a competing effect on the valuation of the DeFi protocol. On the one hand, users may obtain extra assets, just like bank error in their favor. On the other hand, the circulating asset in the market may increase and dilute the users' existing asset value. The incident itself may also affect the reputation of the protocol and damage the valuation. To assess this research question, we apply the synthetic control method to reveal the causal impact of DeFi incidents due to misgovernance on the yielding market, realized by the TVL of the protocol. Our preliminary results suggest that the loss from Compound is more significant than that from Alchemix after the incident occurred.

Our work is expected to contribute to the literature on Blockchain and DeFi, where the aspect of cybersecurity and incident response is still under-studied. We also plan to apply sentiment analysis and word embedding approach to extract useful information from posts and comments about DeFi incidents on social media platforms and conduct econometric analysis to reveal the causality of social media discussions

[3] https://ethereum.org/en/dao/

on the overall health of DeFi and the yielding market. The results from the further analysis will guide the DeFi protocol governance body on how to manage the protocol and respond to an incident properly.

Literature Review

Traditional vs. Decentralized Finance

Traditional finance relies on intermediaries that bring together multiple parties who have resources and who seek resources. The intermediaries, such as government and financial institutions, are regarded as the central point as they aggregate financial resources, perform financial functions, and offer financial services all in a centralized way. A fundamental issue of this centralized structure is about the trust and confidence of the intermediaries, while these can be established through setting up a lot of laws and regulations. However, traditional finance can be very vulnerable and fail significantly, as we witnessed during the financial crisis in 2008 and the censorship in Russia this year (Lalljee, 2022).

Apart from intermediaries, decentralized finance differs from traditional finance in the following eight properties: Public Verifiability, Custody, Privacy, Atomicity, Execution Order Malleability, Transaction Costs, Non-stop Market Hours, and Anonymous Development and Deployment (Qin et al., 2021). Public verifiability enables users to inspect the states and transaction records, and therefore it is more common to see incidents in DeFi on the news than in traditional finance. The verifiability nature also helps researchers conduct scientific research on the financial market, which may not be feasible in the context of traditional finance. Custody allows any user to create a wallet, which is similar to a bank account, at any time at no cost. These two properties lead to a unique feature in privacy, where all transaction records could be attributed to a pseudonym, but it is difficult to link the pseudonym to an entity in real life. Our case study in the Compound incident suggests that managing users based on real-life properties like tax accounts in the world of DeFi may result in a backlash from the community.

The unique way of transaction order handling in DeFi (i.e., Atomicity, Execution Order Malleability, and Transaction Costs) also leads to a unique cybersecurity threat compared to traditional finance. In particular, the transaction execution order in traditional finance is typically first-come-first-served due to regulatory requirements, whereas the transaction execution order in DeFi is influenced by the transaction fee offered to the Blockchain validators. For example, Ke et al. (2021) discussed an attack on DeFi auctions called a Block-stuffing attack, which allows the attacker to drive out all other possible auction participants by spamming transactions with sufficiently high transaction fees and win the auction with a nearly zero bid. The complexity of DeFi also highlights the importance of cybersecurity management in DeFi, which is under-researched. Moreover, a governance body with a development and deployment team should actively maintain the DeFi smart contracts, and the deployment decision will be finalized by token-weighted voting anonymously. Our study investigates the impact when the above governance process is flawed and causes a cyber-incident.

Financial Impact of Cyber-Incident

Prior research also examined the impact of cyber-incidents on the traditional financial market. For example, Telang and Wattal (2007) found that a software vulnerability report will decrease the stock price of the software vendor by 0.6% on average, and the decrement is more severe if the market is competitive or the vendor is small. Similarly, Goel and Shawky (2009) found that a security breach will decrease the market value of a firm by 1% on average during the days surrounding the event. A meta-analysis of 45 studies on this topic suggests that 75.6% of these studies report a statistically significant effect of cybersecurity events on stock price (Spanos & Angelis, 2016). Our study also investigated the impact of cyber-incidents on DeFi.

However, apart from the context difference, there are still two major differences between our study and the related studies from the IS literature. First, prior studies mainly use stock market data to estimate the market value of a company before and after the cyber-incident. In our study, we use TVL to estimate the value of the DeFi protocol. Unlike the token market data that mainly captures the investors' perception of the protocol valuation, TVL mainly captures the protocol valuation based on users' adoption and continuance of the protocol. Second, prior studies often analyze the event of news announcements about the cyber-incident, rather than the actual occurrence of the incident. Our study could examine the event of

the actual incident occurrence, thanks to the verifiability of Blockchain that allows us to verify when did the incident occur exactly.

In the traditional finance market, it is also common to see cyber-incidents mainly caused by typos from keyboard input error, which is also referred to as fat-finger error. For example, the stock price of Cebu Air suddenly dropped by 37% due to a major broker entering a sell order at 58 Philippine pesos instead of 98 Philippine pesos (Shane, 2019). A study found that Samsung Security, which mistakenly distributed shares worth more than 100 billion USD to its employees, lost 12.17% (428 million USD) of its market capitalization due to the fat-finger error (Ahn, 2019). The incidents we examine in this study also involve over-compensating assets to users due to misgovernance, yet the expected effect may differ in the context of DeFi. First, it is common to see cryptocurrency protocols distributing free tokens to users, which is also known as airdrop, and users may prefer this and continue to use and invest in the protocol. Indeed, research found that promotional airdrop increases the investment probability of potential investors during initial coin offerings by 2.3 times (Li et al, 2021). Second, the over-distributed token may not be diluted because the total supply of the token is fixed by the protocol, unlike the case of traditional finance where the total outstanding shares are often increased after stock issuance. For instance, the total supply of the governance token of Compound, COMP, is always 10 million units. Therefore, it is important to examine the impact of cyber-incidents on the DeFi market due to its unique features.

Background

In this study, we examine two DeFi protocols: Alchemix and Compound, which have a similar nature in their incidents. Both incidents were caused by the mistakes in the smart contract implemented by the governance body, which was discovered and exploited by ordinary users afterward.

Alchemix

Alchemix is a decentralized lending protocol (DLP) that allows users to collateralize cryptocurrency to borrow synthetic derivative tokens from the protocol. The first version of Alchemix was launched in late February 2021 and introduced the derivative token "alUSD," where users could mint it by depositing DAI.[4] A special feature of this protocol is that the smart contract will re-invest the collateral fund from the users and automatically pay back the debt. The protocol was listed on the leaderboard of DeFi Pulse,[5] a website that shows popular DeFi projects, with a ranking at #24 and $465.5 million TVL on 21st May 2021.

Given the success of the favorable feature of self-repaying loans, Alchemix planned to launch the second version in early June 2021 with the derivative token "alETH," which is valued based on collaterals in ETH. The governance body proposed the initial parameters of the new alETH token on 27th May 2021, and the majority agreed on the proposal with about 28,300 votes in ALCX,[6] the governance token of Alchemix.

However, right before the planned launching date, a bug in the smart contract for rewarding the liquidity pool stake providers was discovered, and 60 ALCX (approximately $50,000) was over-rewarded.[7] The development team of Alchemix had to fix this issue first, causing a delay in the launch of the version two protocol. This minor incident is not reported by major DeFi incident news websites like rekt.news, yet the protocol still decided to compensate by doubling the reward in the affected liquidity pool until 13th June 2021, which is the new launching date of the version two protocol with the new alETH token.

Unfortunately, the mistake of over-rewarding appears again on a much larger scale. On 16th June 2021, the Alchemix team found that the alETH smart contract was vulnerable and paused the contract.[8] Yet, many users have already found that the collateralized ETH for minting alETH could be withdrawn immediately, while the minted alETH could still be used. This means any user could mint any amount of alETH with negligible cost. Despite the version two contract being modified based on the original contracts audited by

[4] https://alchemixfi.medium.com/introducing-alchemix-9e7054de54d6

[5] https://twitter.com/defipulse/status/1392217222991470598

[6] https://snapshot.org/#/alchemixstakers.eth/proposal/QmVja9Wvn4H30VWZ4rDh9mCinGgRsauCTwApEdBq9VauvN

[7] https://alchemixfi.medium.com/alchemix-farm-migration-post-mortem-and-aleth-update-78c6dd98e3f5

[8] https://twitter.com/AlchemixFi/status/1405187348678148101

a professional Blockchain security consulting firm called CertiK, it still did not function as expected because of the mistake from the modification by the developer. In particular, the new contract referred to the vault using a wrong array index, which caused the debt to be considered as fully paid off.[9] The vulnerability was exploited by users and caused about 2,700 ETH (approximately $6.5 million) lost in collateral of alETH.[10]

Compound

Compound is one of the leading DLP that facilitates investors to borrow and lend different types of crypto assets. Investors can first supply assets to the liquidity pool in exchange for a corresponding cToken. For example, if an investor locks ETH in the liquidity pool, they will receive an equal amount in cETH. The investor can further collateralize the cToken to borrow a crypto asset. The protocol reached $10 billion TVL in April 2021, which is about $2 billion more than the first collateral-based DLP, Maker.

Compound has a mature governance process where the changes in the smart contract are often reviewed and tested by members of the community before making a change proposal. Once the proposal is made, users who own the governance token COMP could vote for or against the proposal. If the proposal is supported by the majority, the change could be executed one week after the decision is made.

Unfortunately, mistakes could still occur with such a mature process. On 22nd September 2021, a user called Tyler Loewen made a proposal to change the common reward rate for COMP distribution to a borrower-only and a supplier-only reward rate, and the proposed smart contract codes are uploaded to the Ethereum Blockchain for review as well.[11] Nevertheless, nobody discovered the bug inside the proposed smart contract, and the proposal was executed on 29th September 2021. There are already users who exploited the vulnerability after 2 hours from the proposal execution and claimed about 29,665 COMP (approximately $8.9 million),[12] while some users could only claim about 0.0055 COMP (approximately $1.73)[13] after 17 hours from the proposal execution.

The analysis of the incident by rekt.news[14] suggested that the vulnerability is caused by a minor typo in the logical comparison: a greater than or equal sign should be used instead of just a greater than sign. The missing equal sign caused Compound of about $80 million lost. The governance body wanted to pause the contract and fix the bug, but they had to wait for the new proposal to be passed and executed. The situation worsens when someone refills the fund in the vulnerable contract with the reserved fund. By calling the *drip* function in the reservoir contract, 202,472.5 COMP (approximately $66.2 million) was sent to the vulnerable contract on 3rd October 2021. The bug-fix proposal was executed on 9th October 2021, but the fund, in total about $147 million in COMP[15], was already drained by the users.

Analysis

To examine the impact of the two incidents on the yielding market, we collected data from Defi Pulse, which comprises daily data on the token locked in BTC, ETH, and DAI, as well as the total value locked in terms of USD for the DeFi projects under the lending category from 1st April 2021 to 31st March 2022. Among the 34 listed DeFi lending projects, 26 of them (including Alchemix and Compound) are within the sample period. Table 1 shows the summary statistics of the dataset. Note that some protocols may also have tokens locked in a particular cryptocurrency as zero because the protocols did not support that cryptocurrency.

We conduct a panel regression on the dataset to estimate the impact of the incidents. To indicate the incident, we create a treatment dummy variable with a value equal to one if the subject is Alchemix and the time is after 16th June 2021, or the subject is Compound and the time is after 30th September 2021, and zero

[9] https://forum.alchemix.fi/public/d/137-incident-report-06162021

[10] https://rekt.news/alchemix-rekt/

[11] https://compound.finance/governance/proposals/62

[12] https://etherscan.io/tx/0xbc246c878326f2c128462d08a0b74048b1dbee733adde8863f569c949c06422a

[13] https://etherscan.io/tx/0xed77e2c4c5573392cfe680fed6201c8b052b5a9d19203fcd28539911ab798679

[14] https://rekt.news/overcompensated/

[15] https://rekt.news/compound-rekt/

otherwise. We also transform the variable by $y' = \ln(1 + y)$ for estimating the impact in terms of the percentage change. The two-way fixed-effect econometric model is specified as follows:

$$y' = \beta x + \mu_i + \tau_t + \varepsilon_{it},$$

where y' is one of the transformed value-lock variables, x is the treatment dummy, μ_i is the project fixed effect, τ_t is the time fixed-effect, and ε_{it} is the error term. The regression results were shown in Table 2, and none of them has a statistically significant effect, meaning the incidents may not have a long-term effect.

Variable	**Mean**	**Std. Dev.**	**Min**	**Max**
Token Locked in BTC	4523.253	12280.15	0	94314.59
Token Locked in ETH	266474.3	648055.2	0	3135476
Token Locked in DAI	1.99e+08	7.33e+08	0	5.58e+09
TVL in USD	1.87e+09	4.32e+09	1386	1.99e+10

Table 1. Summary Statistics (N = 9490)

Variable	(1) Value Locked in BTC	(2) Value Locked in ETH	(3) Value Locked in DAI	(4) Total Value Locked (USD)
Post-incident period	-0.2990 (0.3339)	0.6368 (1.5551)	-0.9507 (0.5673)	0.2248 (0.2540)
Observations	9490	9490	9490	9490
R-squared	0.9180	0.8802	0.9051	0.9456
Adjusted R-squared	0.9145	0.8751	0.9011	0.9432

Notes: 26 project fixed-effects and 365 time fixed-effects are not shown in the table. Clustered robust standard errors by projects in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

Table 2. Panel Regression Results

The result from the above econometric model could be biased because the control groups may have different characteristics that are not captured. To address this limitation, we conduct an analysis with the synthetic control method, using the 30 days prior to the incident as the matching period. We optimize with all available characteristics (Token locked in BTC, ETH, DAI, and TVL in USD) to construct the synthetic control.

We first examine the case of the Alchemix incident, and Figure 1a shows the TVL comparison between Alchemix and synthetic Alchemix, where the time series shows the period 30 days prior to the incident and 14 days after the incident. The vertical dotted line indicates the date of the incident occurrence. The difference between the two series before the incident is statistically insignificant (t = 0.93849, df = 29, p-value = 0.3557, mean = 6831715), despite there being a sharp increase starting on 11th June 2021, probably due to the double reward as a compensation of the minor incident. Interestingly, the difference between the two series after the incident is also statistically insignificant (t = 1.3041, df = 13, p-value = 0.2148, mean = 23530448). Based on the figure, it visually appears that the incident offset the abnormal gain from the sharp increase since 11th June 2021, and the level of TVL remains similar to a comparable alternative in the market, which is about 64% of Idle Finance plus 33% of TrueFi plus 3% of Instadapp.

Similarly, the TVL comparison between Compound and synthetic Compound is shown in Figure 1b. The difference between the two series before the incident is statistically insignificant (t = 0.00012023, df = 29, p-value = 0.9999, mean = 4396.146), and visually the two series match perfectly. Moreover, the difference between the two series after the incident is statistically significant (t = -7.1155, df = 13, p-value = 7.869e-06, mean = -592217523). Using the TVL one day before the incident as the baseline (9663386501), the incident caused the TVL of Compound to decrease by 6.13% on average. Based on the figure, it also visually

appears that the TVL after the incident is consistently lower than its synthetic counterpart, which is about 11% of Maker plus 47% of Aave plus 16% of Instadapp, plus the remaining controls at around 1.3% each.

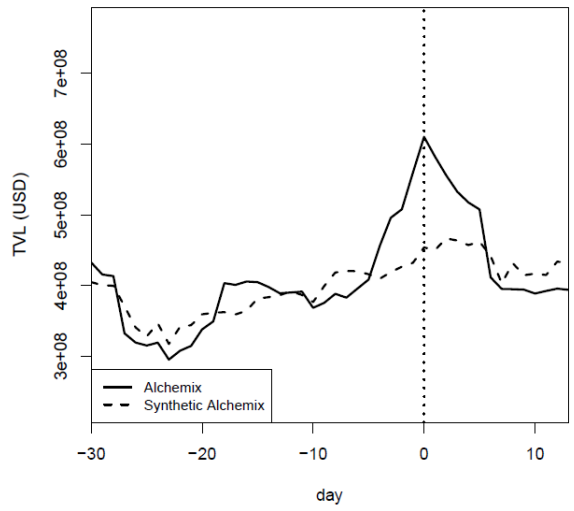

Figure 1a. TVL Comparison of Alchemix and Synthetic Alchemix

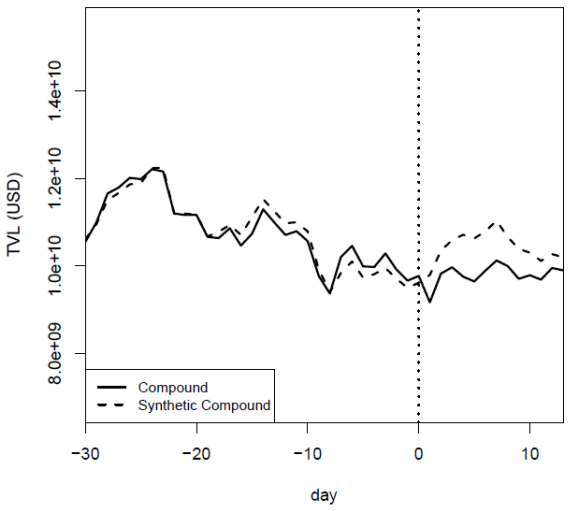

Figure 1b. TVL Comparison of Compound and Synthetic Compound

Discussion

In this research, we compared the impact of two DeFi incidents due to misgovernance using the case of Alchemix and Compound. Using the synthetic control method, we found no significant impact for the Alchemix incident, but a significant impact with a 6.13% decrease in TVL for the Compound incident.

One possible explanation for the different outcomes could be the difference in incident response. In particular, the less restricted governance process allows the Alchemix team to pause the contract immediately once the incident is discovered, whereas the Compound team needed to wait for seven days after the approval of the proposal before any change could be executed. Also, the public relations management of the Alchemix team is more favorable to the community. The Alchemix team posted a series of tweets to explain the incident transparently.[16] The team politely asked the community to return the excess ETH gained from the incident and set up a portal to handle the transactions. The team even proposed to reward the altruistic users with the governance token ALCX as well as a limited edition of NFT as a unique reward.[17] As a result, Alchemix successfully got back 55% of the lost fund due to the incident. However, the Compound team did not do well in public relations management. Specifically, Robert Leshner, the founder of Compound, threatened the users to return the illegally gained fund, or else the gain will be reported as an income to IRS.[18] Such a threat message does not sound valid in the DeFi landscape because the users can only be identified as pseudonyms unless they have interacted with centralized exchanges or projects with real-life identity verification. Therefore, the users may not want to continue to invest in the protocol.

Despite a less restricted governance process that may help during the incident response, it actually trades off the trust generated from decentralization, especially if such emergency procedures could be easily abused. For instance, after the infamous DAO hack, the Ethereum community decided to hard fork the Blockchain so that all the data on the Blockchain was restored at the point before the hacking incident and

[16] https://twitter.com/AlchemixFi/status/1405430945360998408

[17] https://twitter.com/AlchemixFi/status/1406359226126114820

[18] https://twitter.com/rleshner/status/1443730726751506432

allocated the fund from the DAO contract to a different smart contract that allows the investors to withdraw. Although the investors of the DAO are happy with such a recovery, some users believed that the principle of immutability for Blockchain is violated, and set up another Blockchain called Ethereum Classic, which did not comply with the hard forking instruction for DAO recovery. Therefore, a proper Blockchain governance should also include mechanisms to have checks and balances on emergency functions like emergency contract suspension, update, or even hard forking for protocols with their own Blockchain.

To minimize the cybersecurity threat and vulnerability during smart contract versioning, the protocol may enforce smart contract review and testing in Blockchain governance, such as deploying the new version of the contract to the testnet. If any vulnerabilities were found during the review process in the test environment, it is easier to resolve without any material impact on the actual fund in the contracts in the mainnet. However, such approaches are still not bulletproof. For instance, in the abovementioned Compound incident, the smart contract was reviewed and simulated by the developer in the test environment, yet the bug is not undiscovered because an edge case is not tested during the simulation. It is worthwhile to investigate how to design a better governance process to alleviate the possibility of smart contract vulnerabilities.

Future works are summarized as follows. First, we will comprehend our analysis by examining more DeFi incidents using the synthetic control method and other econometric analysis techniques such as the stagger difference-in-differences. The econometric models should incorporate other relevant variables such as the market data of the protocol's token, active users of the protocols, and the number of developers of the protocol. A detailed list of DeFi incidents can be found on these two sites: CryptoSec and rekt.news, where we can derive general patterns based on the commonality between these incidents to generate interesting and robust findings. This allows us to increase the generalizability of the study with a larger sample size instead of just having two cases. Also, since not all incidents are caused by misgovernance or mistakes in the smart contract (e.g., phishing attacks), it is also worthy to compare the effect of different types of incidents.

Second, our case study analysis suggests that social media can play a role during the DeFi incidents, as good control of public sentiment and emotion may significantly reduce the loss received by the DeFi platforms. In this regard, we will extend our analysis to investigate the moderating or mediating effect of public opinions and sentiment on the influence of DeFi exploits. After identifying a set of relevant and impactful DeFi incidents, we will collect social media data associated with these incidents from the Twitter platform. Natural language processing techniques and machine learning models will be applied to extract information content from social media posts and comments to construct public sentiment variables. Third, our current findings are based on data aggregated on a daily basis. Given the high-frequency nature of DeFi price and value, we plan to collect data in a much shorter time interval (i.e., hourly and even minutely) to reveal the instant impact of DeFi incidents. To obtain more granular data, we are going to reimplement the DeFi Pulse adapters for each listed DLP[19] and collect the TVL data at the block level, which has one record per 15 seconds on average. Fourth, given that there are different measures for the yield market in DeFi, we will cross-validate the value lock data with another DeFi project curating website, DeFiLlama, which uses a different way to measure TVL.

Acknowledgements

This research was supported by a research grant from the Department of Management and Marketing, Faculty of Business, Hong Kong Polytechnic University (Project ID: P0041157).

References

Ahn, Y. 2019. "The Economic Cost of a Fat Finger Mistake: A Comparative Case Study from Samsung Securities's Ghost Stock Blunder," *Journal of Operational Risk* (16:2), pp. 49-60.

Cadbury, S. A. 1992. *Committee on Financial Aspects of Corporate Governance*, The UK Cadbury Code.

Curran. 2020. *What is Blockchain Governance? Complete Beginner's Guide*. Retrieved from Blockonomi: https://blockonomi.com/blockchain-governance/

[19] https://github.com/ConcourseOpen/DeFi-Pulse-Adapters

Fischer, A., and Valiente, M.-C. 2021. "Blockchain Governance," *Internet Policy Review* (10:2), pp. 1-10.
Frankenfield, J. 2021. *What Is On-Chain Governance?* Retrieved from Investopedia: https://www.investopedia.com/terms/o/onchain-governance.asp
Goel, S., and Shawky, H. A. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information & Management* (46:7), pp. 404-410.
Hall, J. 2022. *$1 Million Rock NFT Sells for a Penny in All Ore Nothing Error*. Retrieved from Cointelegraph: https://cointelegraph.com/news/1-million-rock-nft-sells-for-a-penny-in-all-ore-nothing-error
Ke, P. F., Chen, J., and Guo, Z. 2021. "Strategic Behavior and Market Inefficiency in Blockchain-Based Auctions," *Workshop on Information Systems and Economics (WISE)*.
Lalljee, J. 2022. *Russia's Economy Already Lost $860 Million This Year Because the Government Keeps Shutting Down the Internet*. Retrieved from Business Insider: https://www.businessinsider.com/russia-internet-censorship-cost-economy-putin-ukraine-sanctions-twitter-2022-3
Li, J., Wan, X. S., Cheng, H. K., and Zhao, X. 2021. "Operation Dumbo Drop: To Airdrop or Not to Airdrop for Initial Coin Offering Success?," *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3929815
Petrowski, J. 2020. *Polkadot Governance*. Retrieved from Polkadot: https://polkadot.network/blog/polkadot-governance/
Popescu, A. D. 2022. "Understanding FinTech and Decentralized Finance (DeFi) for Financial Inclusion," in *FinTech Development for Financial Inclusiveness*, IGI Global, pp. 1-13.
Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., and Gervais, A. 2021. "CeFi vs. DeFi - Comparing Centralized to Decentralized Finance," *arXiv preprint*, arXiv:2106.08157.
Resnick, S. 2022. *A Deep Dive into the Mysterious Subcultures of Cryptocurrency Obsessives*. Retrieved from South China Morning Post: https://www.scmp.com/magazines/post-magazine/long-reads/article/3175053/deep-dive-mysterious-subcultures-cryptocurrency
Samreen, N. F., and Alalfi, M. H. 2020. "Reentrancy Vulnerability Identification in Ethereum Smart Contracts," in *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, IEEE, pp. 22-29.
Shane, D. 2019. *'Fat Finger' Error Sends Airline Stock on Wild Ride*. Retrieved from Financial Times: https://www.ft.com/content/56188540-a2cf-11e9-974c-ad1c6ab5efd1
Spanos, G., and Angelis, L. 2016. "The Impact of Information Security Events to the Stock Market: A Systematic Literature Review," *Computers & Security* (58), pp. 216-229.
Telang, R., and Wattal, S. 2007. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price," *IEEE Transactions on Software engineering* (33:8), pp. 544-557.
Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., and Knottenbelt, W. J. 2021. Sok: Decentralized Finance (Defi)," *arXiv preprint*, arXiv:2101.08778.
Zetzsche, D. A., Arner, D. W., and Buckley, R. P. 2020. "Decentralized Finance," *Journal of Financial Regulation* (6:2), pp. 172-203.