Incident Analysis of Decentralized Finance

Cheng-Chieh Lin[1], Chia-Cheng Tsai[2] and Shih-Wei Liao[2*]
[1]Department of Computer Science and Information Engineering, National Cheng Kung University
[2]Department of Computer Science and Information Engineering, National Taiwan University
Email: f74076027@gs.ncku.edu.tw, b09902052@csie.ntu.edu.tw, liao@csie.ntu.edu.tw

***Abstract*—Decentralized Finance (DeFi) has emerged as a transformative force in the financial landscape, bringing about challenges in ensuring blockchain security. This paper systematically examines prominent DeFi incidents from June 2022 to May 2023. Our findings underscore the significance of continuous vigilance in DeFi operations.**

***Index Terms*—Decentralized Finance, DeFi, Flash loan, Oracle, Reentrancy**

I. Analysis of Incidents

There is no widely accepted standard for classifying blockchain vulnerabilities. After a thorough review of papers [1]–[5], the 5-layer framework proposed by [1] presents the most comprehensive coverage of vulnerabilities in DeFi. We have opted to utilize this framework to categorize the vulnerabilities.

The scope of this paper is limited to DeFi incidents that occurred from June 2022 to May 2023, involving direct or indirect losses of 1 million USD or more. The incident data sources[1] primarily rely on (i) Rekt News; (ii) DeFiHackLabs; (iii) Slowmist, and official post-mortem reports. Any incidents involving CeFis (e.g. FTX, Binance), DAOs, or NFTs will not be included.

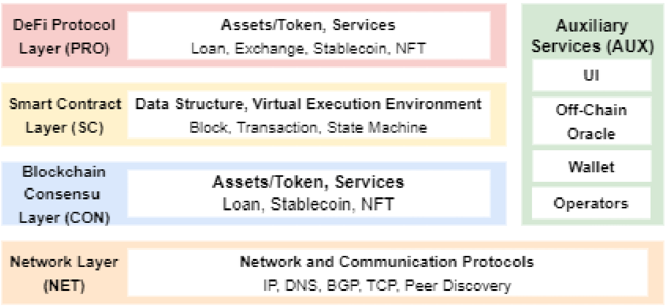
DeFi Protocol Layer (PRO)
Assets/Token, Services
Loan, Exchange, Stablecoin, NFT
Smart Contract Layer (SC)
Data Structure, Virtual Execution Environment
Block, Transaction, State Machine
Blockchain Consensu Layer (CON)
Assets/Token, Services
Loan, Stablecoin, NFT
Network Layer (NET)
Network and Communication Protocols
IP, DNS, BGP, TCP, Peer Discovery
Auxiliary Services (AUX)
UI
Off-Chain Oracle
Wallet
Operators

Fig. 1. The 5-layer framework proposed by [1]

Table I reveals the 35 real-world incidents, where 33 victims had professional audits in place. Upon an in-depth investigation, we identified that some incidents stem from the following human errors:

- **Leave Audited Risks Unresolved:** Quantstamp audit suggested Nomad Bridge validate the `_leaf` input of the `Replica.sol:prove`, with QSP-19 Proving With An Empty Leaf. But the Nomad team seemed to misunderstand the issue an leave it unresolved.
- **Deploy New Code Without Audit:** Gym Network releases new features without being extensively audited.
- **Partially Audit:** Euler Finance introduced vulnerable code `EToken.sol:donateToReserve` [16], however, Omniscia only performed an audit of the Chainlink integration component.
- **Use Unsafe Vanity Address:** Wintermute used the Profanity tool to generate addresses with multiple leading zeros. The private keys were compromised by brute force.
- **Rug Pull:** A member of Hope Finance deployed a fake router and deceived the other three owners into approving a multi-signature wallet, thereby siphoning off the funds.

The practical value of an audit becomes limited when a project is unable to effectively prevent human errors. This highlights the need for rigorous processes to prevent human errors and oversights.

II. Analysis of Layers, Loss, and Occurrences

Table II presents the losses, occurrence frequencies, and average losses of individual layer attack events. It is noteworthy that neither NET Layer nor CON Layer was involved in the 35 incidents. The most common incident causes belong to SC Layer, accounting for 22 out of 35 cases (62%).

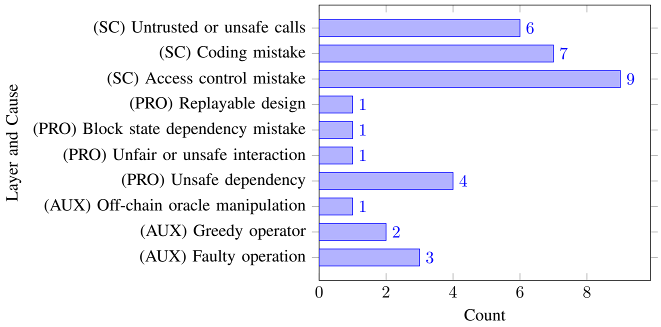

Fig. 2. Occurrences of Incident Causes

Figure 2 shows the frequency of incident causes. In SC Layer, Access Control Mistake is the most common incident cause, by which most of the victims deployed flawed authentication logic. In PRO Layer, Unsafe Dependency is the most common incident cause, which implies that DeFi projects should not blindly trust external data sources, such as oracles. In AUX Layer, Faulty Operation and Greedy Operation are

*Corresponding author

[1] Links: https://rekt.news, https://github.com/SunWeb3Sec/DeFiHackLabs, https://www.slowmist.com

TABLE I
DeFi Incidents that lost over 1 million USD occurred from June 2022 to May 2023.

Project	Loss	Layer	Incident Type	Attack Event	Date	Report
Jimbos Protocol	7.5M	PRO	Unfair slippage protection	Flash loan	May 29, 2023	[6]
Swaprum	3.0M	AUX	Authority control or breach of promise	Rug pull	May 18, 2023	[7]
Level Finance	1.1M	SC	Absence of coding logic or sanity check	Flash loan	May 02, 2023	[8]
0vix	2.0M	PRO	On-chain oracle manipulation	Flash loan, Oracle attack	Apr 28, 2023	[9]
Merlin DEX	1.8M	AUX	Authority control or breach of promise	Rug pull	Apr 26, 2023	[10]
Hundred Finance	7.4M	SC	Absence of coding logic or sanity check	Flash loan	Apr 15, 2023	[11]
Yearn	11.6M	SC	Absence of coding logic or sanity check	Attacks related to contract	Apr 13, 2023	[12]
Sushi	3.3M	SC	Visibility error and unrestricted action	Attacks related to contract	Apr 09, 2023	[13]
SafeMoon	8.9M	SC	Visibility error and unrestricted action	Attacks related to contract	Mar 28, 2023	[14]
Kokomo Finance	4.0M	SC	Direct call to untrusted contract	Attacks related to contract	Mar 27, 2023	[15]
Euler Finance	197.0M	SC	Absence of coding logic or sanity check	Flash loan	Mar 13, 2023	[16]
Hedera	12.2M	SC	Inconsistent access control	Attacks related to contract	Mar 09, 2023	[17]
Hope Finance	1.9M	AUX	Deployment mistake	Rug pull	Feb 20, 2023	[18]
Dexible	2.0M	SC	Direct call to untrusted contract	Attacks related to contract	Feb 17, 2023	[19]
Platypus Finance	8.5M	SC	Absence of coding logic or sanity check	Flash loan	Feb 16, 2023	[20]
dForce Network	3.6M	SC	Reentrancy	Flash loan, Reentrancy	Feb 09, 2023	[21]
Orion Protocol	3.0M	SC	Reentrancy	Flash loan, Reentrancy	Feb 04, 2023	[22]
Rubic	1.5M	SC	Direct call to untrusted contract	Attacks related to contract	Dec 25, 2022	[23]
Raydium	4.4M	AUX	Compromised private key / wallet	Private key leakage	Dec 16, 2022	[24]
Lodestar Finance	6.5M	PRO	On-chain oracle manipulation	Oracle attack	Dec 10, 2022	[25]
DFXFinance	4.0M	SC	Reentrancy	Flash loan, Reentrancy	Nov 10, 2022	[26]
Skyward Finance	3.2M	SC	Visibility error and unrestricted action	Attacks related to contract	Nov 02, 2022	[27]
Team Finance	15.8M	SC	Inconsistent access control	Attacks related to contract	Oct 27, 2022	[28]
Mango Markets	115.0M	AUX	External market manipulation	Oracle attack	Oct 12, 2022	[29]
Transit Swap	21.0M	SC	Visibility error and unrestricted action	Attacks related to contract	Oct 02, 2022	[30]
Wintermute	162.0M	PRO	Randomness	Attacks related to contract	Sep 20, 2022	[31]
Acala Network	1.6M	SC	Arithmetic mistakes	Attacks related to contract	Aug 14, 2022	[32]
Nomad Bridge	190.0M	SC	Absence of coding logic or sanity check	Attacks related to contract	Aug 02, 2022	[33]
Reaper.Farm	1.7M	SC	Inconsistent access control	Attacks related to contract	Aug 01, 2022	[34]
Nirvana Finance	3.5M	PRO	Liquidity borrow, purchase, mint, deposit	Flash loan	Jul 29, 2022	[35]
Crema Finance	8.8M	SC	Visibility error and unrestricted action	Attacks related to contract	Jul 03, 2022	[36]
Harmony Bridge	100.0M	AUX	Compromised private key / wallet	Private key leakage	Jun 24, 2022	[37]
Inverse Finance	5.8M	PRO	On-chain oracle manipulation	Flash loan, Oracle attack	Jun 16, 2022	[38]
Gym Network	2.1M	SC	Visibility error and unrestricted action	Attacks related to contract	Jun 08, 2022	[39]
Wintermute	27.6M	PRO	Transaction / strategy replay	Attacks related to contract	Jun 05, 2022	[40]

The Amount column is expressed in millions (M) of US dollars. The Incident Type column indicates the type proposed by [1].

TABLE II
Losses and Occurrence of Layers

Layer	Loss	Count	Loss / Count
NET	0	0	-
CON	0	0	-
SC	512.3M	22	23.3M
PRO	214.9M	7	30.7M
AUX	226.0M	6	37.7M
Total	953.3M	35	27.2M

common causes. Preventing the leakage of private keys and guarding against rug pulls are critical in this context.

Figure 3 shows that the losses incurred due to Coding Mistake in SC Layer significantly outweigh those caused by other factors. The losses in the AUX Layer are also substantial. The losses incurred by these vulnerabilities are exceptionally costly. Even a single occurrence of such a vulnerability event could result in the flourishing project's bankruptcy.

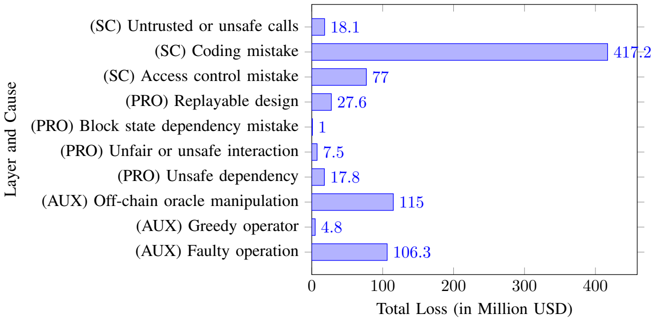

Fig. 3. Total Loss of Incident Causes

III. Security Strategy and Conclusion

SmartBugs [41] incorporates 19 open-source static code analyzers. We selectively utilized four tools Mythril, Manticore, Slither, and Solhint to evaluate the capability of identifying vulnerabilities. Unfortunately, none of these tools successfully detected the vulnerabilities causing the incidents. Hence, there is still substantial room for improvement in existing code analysis tools.

In sum, this paper summarizes 35 real-world DeFi incidents. While most DeFi projects undergo professional audits, certain key issues, such as human error and oracle manipulation, still lead to security incidents. This underscores the need to maintain vigilance throughout the operational phases of DeFi and elevate the reliability of audits.

References

[1] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, “Sok: Decentralized finance (defi) attacks,” 2023.

[2] W. Li, J. Bu, X. Li, and X. Chen, “Security analysis of defi: Vulnerabilities, attacks and advances,” 2022.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17318332

[4] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, “Systematic review of security vulnerabilities in ethereum blockchain smart contract,” *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[5] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, “Blockchain-enabled smart contracts: Architecture, applications, and future trends,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[6] “Decoding Jimbo’s Protocol $7.5M Exploit — QuillAudits — quillaudits.medium.com,” https://quillaudits.medium.com/decoding-jimbos-protocol-7-5m-exploit-quillaudits-772ad1db6c07, Jun 2023, [Accessed 14-10-2023].

[7] “Decoding Swaprum Finance $3 Million Rug Pull — QuillAudits — quillaudits.medium.com,” https://quillaudits.medium.com/decoding-swaprum-finance-3-million-rug-pull-quillaudits-2c6f9527b589, May 2023, [Accessed 14-10-2023].

[8] “Rekt - Level Finance - REKT — rekt.news,” https://rekt.news/level-finance-rekt/, May 2023, [Accessed 14-10-2023].

[9] “Decoding Ovix Protocol’s $2 Million Exploit — QuillAudits — quillaudits.medium.com,” https://quillaudits.medium.com/decoding-ovix-protocols-2-million-exploit-quillaudits-92befc250e7c, Apr 2023, [Accessed 14-10-2023].

[10] “Rekt - Merlin DEX - REKT — rekt.news,” https://rekt.news/merlin-dex-rekt/, Apr 2023, [Accessed 14-10-2023].

[11] “Rekt - Hundred Finance - REKT 2 — rekt.news,” https://rekt.news/hundred-rekt2/, Apr 2023, [Accessed 14-10-2023].

[12] “Rekt - Yearn - REKT 2 — rekt.news,” https://rekt.news/yearn2-rekt/, Apr 2023, [Accessed 14-10-2023].

[13] “Rekt - SushiSwap - REKT — rekt.news,” https://rekt.news/sushi-yoink-rekt/, Apr 2023, [Accessed 14-10-2023].

[14] “Rekt - Safemoon - REKT — rekt.news,” https://rekt.news/safemoon-rekt/, Mar 2023, [Accessed 14-10-2023].

[15] “Rekt - Kokomo Finance - REKT — rekt.news,” https://rekt.news/kokomo-finance-rekt/, Mar 2023, [Accessed 14-10-2023].

[16] “Euler Finance Incident Post-Mortem — omniscia.io,” https://medium.com/@omniscia.io/euler-finance-incident-post-mortem-1ce077c28454, Mar 2023, [Accessed 14-10-2023].

[17] A. P. Joe Blanchard, “Analysis & Remediation of the Precompile Attack on the Hedera Network — Hedera — hedera.com,” https://hedera.com/blog/analysis-remediation-of-the-precompile-attack-on-the-hedera-network, Mar 2023, [Accessed 14-10-2023].

[18] “Rekt - Hope Finance - REKT — rekt.news,” https://rekt.news/hope-finance-rekt/, Feb 2023, [Accessed 14-10-2023].

[19] “Rekt - Dexible - REKT — rekt.news,” https://rekt.news/dexible-rekt/, Feb 2023, [Accessed 14-10-2023].

[20] “Rekt - Platypus Finance - REKT — rekt.news,” https://rekt.news/platypus-finance-rekt/, Feb 2023, [Accessed 14-10-2023].

[21] “Rekt - dForce Network - REKT — rekt.news,” https://rekt.news/dforce-network-rekt/, Feb 2023, [Accessed 14-10-2023].

[22] “Rekt - Orion Protocol - REKT — rekt.news,” https://rekt.news/orion-protocol-rekt/, Feb 2023, [Accessed 14-10-2023].

[23] Neptune Mutual, “How Was Rubic Protocol Hacked? — neptunemutual.com,” https://neptunemutual.com/blog/how-was-rubic-protocol-hacked/, Dec 2022, [Accessed 14-10-2023].

[24] “Rekt - Raydium - REKT — rekt.news,” https://rekt.news/raydium-rekt/, Dec 2022, [Accessed 14-10-2023].

[25] Waffle, “Post Mortem Summary — blog.lodestarfinance.io,” https://blog.lodestarfinance.io/post-mortem-summary-13f5fe0bb336, Dec 2022, [Accessed 14-10-2023].

[26] “V2 Vulnerability Post Mortem — dfxfinance,” https://medium.com/@dfxfinance/v2-vulnerability-post-mortem-b05232bc6550, Nov 2022, [Accessed 15-10-2023].

[27] Neptune Mutual, “Decoding Skyward Finance Smart Contract Vulnerability — medium.com,” https://medium.com/neptune-mutual/decoding-skyward-finance-smart-contract-vulnerability-3e38c5d0e312, Nov 2022, [Accessed 15-10-2023].

[28] “Rekt - Team Finance - REKT — rekt.news,” https://rekt.news/teamfinance-rekt/, Oct 2022, [Accessed 15-10-2023].

[29] “Rekt - Mango Markets - REKT — rekt.news,” https://rekt.news/mango-markets-rekt/, Oct 2022, [Accessed 15-10-2023].

[30] “Rekt - Transit Swap - REKT — rekt.news,” https://rekt.news/transit-swap-rekt/, Oct 2022, [Accessed 15-10-2023].

[31] “Rekt - Wintermute - REKT 2 — rekt.news,” https://rekt.news/wintermute-rekt-2/, Sep 2022, [Accessed 15-10-2023].

[32] “Rekt - Acala Network - REKT — rekt.news,” https://rekt.news/acala-network-rekt/, Aug 2022, [Accessed 15-10-2023].

[33] Sm4rty, “Nomad Bridge’s $200 Million Exploit Postmortem — sm4rty.medium.com,” https://sm4rty.medium.com/nomad-bridges-200-million-exploit-postmortem-9d1cd83db1f7, Aug 2022, [Accessed 15-10-2023].

[34] Gabriel Sieng, “Reaper Farm Just Lost US$1.7 Million From Exploit - ChainDebrief — chaindebrief.com,” https://chaindebrief.com/reaper-farm-got-hacked/, Aug 2022, [Accessed 15-10-2023].

[35] “Nirvana Finance Incident Analysis — certik.com,” https://www.certik.com/resources/blog/1UBzEHHu35dJdJOGsuf85D-nirvana-finance-incident-analysis, Jul 2022, [Accessed 15-10-2023].

[36] “Crema Finance Exploit — certik.com,” https://www.certik.com/resources/blog/4XzSJEeWC2bRppR9CeBckw-crema-finance-exploit, Jul 2022, [Accessed 15-10-2023].

[37] “Harmony Incident Analysis — certik.com,” https://www.certik.com/resources/blog/2QRuMEEZAWHx0f16kz43uC-harmony-incident-analysis, Jun 2022, [Accessed 15-10-2023].

[38] “Inverse Finance Incident Analysis — certik.com,” https://www.certik.com/resources/blog/6LbL57WA3iMNm8zd7q111R-inverse-finance-incident-analysis, Jun 2022, [Accessed 15-10-2023].

[39] “Rekt - Gym Network - REKT — rekt.news,” https://rekt.news/gymnet-rekt/, Jun 2022, [Accessed 15-10-2023].

[40] “Rekt - Wintermute - REKT — rekt.news,” https://rekt.news/wintermute-rekt/, Jun 2022, [Accessed 15-10-2023].

[41] J. F. Ferreira, P. Cruz, T. Durieux, and R. Abreu, “Smartbugs: A framework to analyze solidity smart contracts,” in *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, 2020, pp. 1349–1352.