Importance of Anti-Money Laundering Regulations among Prosumers in Decentralized Finance: A Game Theoretical Evidence from Permissionless vs. Permissioned Decentralized Finance

Destan Kirimhan[1]

Decentralized finance (DeFi) proposes an alternative way of supplying financial services which are already offered by the traditional financial institutions with comparatively beneficial claims for investors such as financial inclusivity, absence of central authority, transaction transparency, and a degree of privacy for identities and financial transactions (Salami, 2021). However, this "trustless" state-space along with the lack of real-world identity verification can incentivize cybercriminals to attack or conduct some illicit activities. As a supportive empirical evidence, there is an increasing trend in the cybercriminal activity as of the writing of this summary paper (Makarov and Schoar, 2022; McKay, 2022).

Therefore, an important question to examine is whether the above-mentioned appealing characteristics of DeFi lead to cyber vulnerability of DeFi. To answer this question, we provide a game-theoretical model comparing the equilibrium of permissionless DeFi versus permissioned DeFi where permissionless space is open to every agent, privacy is achieved, and there is lack of anti-money laundering (AML) regulations including know-your-customer (KYC) and know-your-transactions (KYT), among many others. On the other hand, permissioned space requires to have allowlisters to onboard the agents that are compliant with the AML regulations, and therefore, privacy in identities and transactions is restricted.

The game theoretical model is backed by the cybercriminal theories of routine activity theory (Cohen and Felson, 1979), rational choice theory of crime (Becker, 1968), situational crime prevention (Clarke, 1983), and deterrence theory (Beccaria, 1963; Paternoster, 1987). Agents playing the sequential game are blocklisted ones that pursue the goal of attacking the DeFi liquidity pool either explicitly in permissionless space or implicitly in permissioned space to seize the maximum value of coins of naïve allowlisted agents who are not sophisticated enough to implement the precautionary actions against cyberattacks. Blocklisted agents move in the game first with a choice of action either to attack or not to attack. On the other hand, the benevolent and capable guardian that could be defined as allowlisters, decentralized governance, effective smart contract auditors, and law enforcement with the internal team of liquidity pool observes the choice of action of the blocklisted agent and then selects to either catch or not catch this agent to protect the value of coins kept on- and off-the-chain. While our results are robust in the simultaneous move game, solution in the permissionless space depends on the policy variable of recovered tokens ratio which is defined in line with the real-world examples of DeFi cyberattacks. According to the viable and optimal range of this variable, our policy implications are threefold.

First, AML regulations are particularly important to create a cybersecure DeFi space given that the optimal solution in permissioned DeFi does not depend on the recovered tokens ratio and the status quo of no attacks is kept. On the other hand, in permissionless DeFi space, due to the absence of AML regulations, the status quo without fully forfeiting the privacy is established if

[1] Kirimhan is affiliated with Woody L. Hunt College of Business, University of Texas at El Paso, 500 W University Ave., El Paso, TX 79902, USA. Email: dkirimhan@utep.edu, Work Phone Number: +1 (915) 747-7953.

naïve allowlisted agents are trained properly to take effective precautions against the cyberattacks, or recovered tokens ratio is very high relative to its real-world cases. To ensure this high level of recovered tokens, artificial intelligence (AI) with machine learning (ML) methods can be employed to flag, track, and recover the tokens from cybercriminals. In this regard, these methods can classify the user behavior and then detect the abnormal user behavior as well as upgrade the effectiveness of well-established methods of detecting malware, bugs, and vulnerabilities in different layers of smart contracts (see Bogner, 2017; Raje et al., 2017; Zeadally et al., 2020). Although this study is not free from limitations and assumptions, it is crucial to investigate whether the "banking the unbanked" catchline of DeFi comes with a cost of cyber vulnerability of the unbanked population.

References

Beccaria, C. (1963). *On crimes and punishments*. Bobbs-Merrill.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*, 169-217. https://doi.org/10.1007/978-1-349-62853-7_2

Bogner, A. (2017). Seeing is understanding-Anomaly detection in blockchains with visualized features. In *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers* (pp. 5-8). ACM. https://doi.org/10.1145/3123024.3123157

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, *4*, 225-256. https://doi.org/10.1086/449090

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and decentralized finance (DeFi)* (National Bureau of Economic Research Working Papers No. 30006). https://doi.org/10.3386/w30006

McKay, J. (2022). *DeFi-ing cyber attacks*. (Working Paper). https://tellingstorieswithdata.com/inputs/pdfs/final_paper-2022-jack_mckay.pdf

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, *4*(2), 173-217. https://doi.org/10.1080/07418828700089271

Raje, S., Vaderia, S., Wilson, N., & Panigrahi, R. (2017). Decentralised firewall for malware detection. In *2017 International Conference on Advances in Computing, Communication and Control* (pp. 1-5). IEEE. https://doi.org/10.1109/icac3.2017.8318755

Salami, I. (2021). Challenges and approaches to regulating decentralized finance. *American Journal of International Law*, *115*, 425-429. https://doi.org/10.1017/aju.2021.66

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817-23837. https://doi.org/10.1109/access.2020.2968045