Talk: Platform Building With Fake Consumers: On Double Dippers and Airdrop Farmers

Hanna Hałaburda[1][0000-0002-2438-4972], Benjamin Livshits[2][0000-0002-4921-8452], and Aviv Yaish[3,4,5][0000-0002-7971-2494]

[1] New York University Stern School of Business, New York, NY, USA
hh66@stern.nyu.edu
[2] Imperial College London, London, UK
livshits@ic.ac.uk
[3] Yale University, New Haven, CT, USA
aviv.yaish@yale.edu
[4] Complexity Science Hub, Vienna
[5] IC3

Abstract. We study the strategic choice faced by platforms wishing to increase market coverage via reward issuance to pseudonymous consumers. This practice, also known as an airdrop, is commonly used in blockchains. However, prior work finds that despite platforms' best efforts, airdrops are commonly gamed by *farmers* who specialize in creating multiple "fake" accounts to receive an outsize share of rewards, and who thereafter exit the platforms. To understand how to design airdrops in this adversarial setting, we analyze a market inhabited by real users and farmers, where the latter may costlessly create an arbitrary amount of fake accounts. We show that by correctly aligning incentives, a platform that cannot detect even a single fake account can still harness farmers to increase both its appeal to real users, and its revenue. While motivated by airdrops, our work applies to other reward schemes.

Keywords: Platforms, Decentralized Finance, Tokens, Network Effects.

1 Introduction

Platforms may *airdrop* (i.e., distribute) rewards to consumers to attract them, both in the blockchain setting [16], and also in traditional ones [17]. Generally, the amount of rewards one can receive is limited and eligibility is conditional, e.g., on performing tasks or proof-of-humanity (PoH) procedures.

Unfortunately, airdrops attract the attention of *farmers* who employ sophisticated tactics such as creating multiple "fake" accounts to increase their rewards and even paying others to circumvent PoH measures [15]. To curtail reward farming, some issue *retroactive* airdrops that are not announced in advance. Instead, reward eligibility is based on consumers' past interactions with the platform, also allowing to screen those exhibiting farmer-esque behavior. Despite such countermeasures, empirical work shows that farmers still receive a large share of

rewards [6,14]. Given the persistence of farmers and as platforms continue to issue airdrops that are not farmer-proof, a question is raised:

Can farmers be used to a platform's benefit?

2 This Work

We initiate the study of the aforementioned question. Our main contribution is an economic analysis of airdrops in an adversarial setting, where farmers would use a platform solely to receive rewards.

In particular, our analysis accounts for farmers' impact on *network effects*, a phenomenon in which an individual's utility from a service depends on the size of its userbase, highlighted by previous work highlights as crucial for airdrops [13,1]. Our work emphasizes that effective airdrop design requires both a tolerance for a certain level of farming and a strategic selection of rewarded activities. Activities should be chosen carefully, e.g., rewarding liquidity provision is preferred to rewarding trading, as the latter may devolve into wash-trading [4] while the former more robustly benefits the ecosystem. Thus, correctly setting the incentive structure results in limiting farmers' negative impact, and can even harness them for the platform's benefit.

We present a model which builds on empirical findings based on data from several notable airdrops, and addresses limitations of previous work on related settings, e.g., digital piracy [2,11,12]. In particular, we consider the ability of farmers to perform "Sybil attacks", that is, cheaply create new identities under false names. In contrast, the digital piracy literature considers consumers who may obtain services or products for free (e.g., by pirating video games), but relies on assumptions that do not account for the risks inherent in airdrops, e.g., 1. firms do not bear a direct cost for each pirated copy (while airdrops may result in issuing costly rewards to farmers), 2. some consumers consider pirated products as imperfect substitutes for original ones (in contrast, the value of two equal amounts of rewards received in an airdrop of fungible assets is identical), and, 3. the pirate market segment has limited consumption (while farmers' consumption is potentially unbounded). These assumptions limit the potential harm of pirates to revenue, while the threat posed by farmers may be greater.

By addressing these limitations, our work contributes to several lines of work beyond those on platform economics in adversarial markets. Thus, our work complements the literature on mechanisms robust to false-names [20,8,18], and the literature on pseudonymity in digital settings [7,5,3].

Having laid out the model, we proceed to solve it via a series of results outlining how various market factors influence platforms' optimal airdrop strategies. To demonstrate the impact of farmers and highlight differences with prior art, we show that when considering a fixed reward for each eligible user (à la Worldcoin's 25 tokens per incoming user [9]), farmers may significantly harm revenue irrespective of the strength of network effects.

Although this may seem bleak, we consider another design: a proportional airdrop, where a predefined reward amount is split equally among eligible users.

We prove that this scheme naturally leads farmers to limit the amount of Sybil accounts that they create. Thus, while an airdrop issuer would give rewards to farmers, the latter's contribution to network effects can outweigh the bounded revenue losses. Then, we prove that under certain market conditions, this implies that issuers do not need to curtail farming and can even profit from letting farmers roam free. We continue by deriving the optimal strategies for platforms, and characterizing the conditions under farmers are beneficial. To do so, we compare a market in which farmers are present with another one without farmers.

Our results paint a "love-hate" triangle, if you will, due to the tension between: 1. platforms and farmers, 2. honest users and farmers, 3. platforms and users.

When considering a monopolist, in some parameter regimes an airdrop can be used to harness farmers to the platform's benefit. In such cases, there is a give-and-take relationship between the monopolist and farmers, where a properly designed airdrop essentially serves as a mechanism for the issuing platform to outsource the costly task of improving the platform's utility in the eyes of honest users to farmers, who, due to competitive entry, would do so efficiently. In our results, we highlight that a monopolist's optimal airdrop strategy may, in fact, entail setting eligibility conditions that are only profitable for well-oiled operations, resulting in honest-users being "crowded-out" of the airdrop by farmers. While that may be, the outcome is still a better platform for honest users. In turn, this enables the monopolist to both cover a larger part of the market and charge higher fees, thus profits can *increase* when farmers are present.

On the other hand, a different dynamic emerges for a duopoly. The tug-of-war between the two platforms operates on two levels: service fees and airdrop rewards. Any income made from service fees is funneled to an "airdrop war" of sorts, where the platforms compete away their profits. As we show, the symmetric equilibrium in this case is for both platforms to refrain from issuing airdrops.

Our full results and the corresponding analysis are provided in [10].

Acknowledgments. A preliminary version of this paper was written while Aviv Yaish and Benjamin Livshits were working at Matter Labs (see [19]). This research article is a work of scholarship and reflects the authors' own views and opinions. It does not necessarily reflect the views or opinions of any other person or organization, including the authors' past or present employer(s). Readers should not rely on this article for making strategic or commercial decisions, and the authors are not responsible for any losses that may result from such use.

References

1. Allen, D.W., Berg, C., Lane, A.M.: Why airdrop cryptocurrency tokens? Journal of Business Research **163**, 113945 (2023). https://doi.org/10.1016/j.jbusres.2023.113945
2. Besen, S.M., Kirby, S.N.: Private Copying, Appropriability, and Optimal Copying Royalties. The Journal of Law & Economics **32**(2), 255–280 (1989). https://doi.org/10.1086/467177

3. Chemaya, N., Yaish, A., Yacouel, S., Malkhi, D., Cong, L.W.: Quantifying inequality in blockchain networks (Sep 2025). https://doi.org/p957
4. Cong, L.W., Li, X., Tang, K., Yang, Y.: Crypto Wash Trading. Management Science **69**(11), 6427–6454 (Nov 2023). https://doi.org/10.1287/mnsc.2021.02709
5. Conitzer, V., Yokoo, M.: Using Mechanism Design to Prevent False-Name Manipulations. AI Magazine **31**(4), 65–78 (Sep 2010). https://doi.org/10.1609/aimag.v31i4.2315
6. Fan, S., Min, T., Wu, X., Cai, W.: Altruistic and profit-oriented: Making sense of roles in web3 community from airdrop perspective. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, NY, NY, USA (2023). https://doi.org/10.1145/3544548.3581173
7. Friedman, E.J., Resnick, P.: The social cost of cheap pseudonyms. Journal of Economics & Management Strategy **10**(2), 173–199 (Jun 2001). https://doi.org/10.1111/j.1430-9134.2001.00173.x
8. Gafni, Y., Yaish, A.: Transaction Fee Mechanisms Robust to Welfare-Increasing Collusion (Mar 2025). https://doi.org/10.2139/ssrn.5165100
9. Gent, E.: A cryptocurrency for the masses or a universal id?: Worldcoin aims to scan all the world's eyeballs. IEEE Spectrum **60**(1), 42–57 (1 2023). https://doi.org/10.1109/MSPEC.2023.10006664
10. Hałaburda, H., Livshits, B., Yaish, A.: Platform building with fake consumers: On double dippers and airdrop farmers (Jul 2025). https://doi.org/g9z6tg
11. Hui, K.L., Png, I.: Piracy and the Legitimate Demand for Recorded Music. Contributions in Economic Analysis & Policy **2**(1), 1–22 (Sep 2003). https://doi.org/10.2202/1538-0645.1160
12. Jain, S.: Digital piracy: A competitive analysis. Marketing Science **27**(4), 610–626 (2008). https://doi.org/10.1287/mksc.1070.0313
13. Makridis, C.A., Fröwis, M., Sridhar, K., Böhme, R.: The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. Journal of Corporate Finance **79**, 102358 (2023). https://doi.org/10.1016/j.jcorpfin.2023.102358
14. Messias, J., Yaish, A., Livshits, B.: Airdrops: Giving money away is harder than it seems (2023). https://doi.org/10.48550/arXiv.2312.02752
15. Ohlhaver, P., Nikulin, M., Berman, P.: Compressed to 0: The silent strings of proof of personhood (2024). https://doi.org/10.2139/ssrn.4749892
16. Wahby, R.S., Boneh, D., Jeffrey, C., Poon, J.: An airdrop that preserves recipient privacy. In: Bonneau, J., Heninger, N. (eds.) Financial Cryptography and Data Security. pp. 444–463. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-51280-4_24
17. Wignall, D.: How Churners Earn Money By Regularly Signing Up for Credit Cards. The New York Times (Oct 2025), https://www.nytimes.com/2025/10/11/business/credit-cards-churners.html
18. Yaish, A., Chemaya, N., Malkhi, D., Cong, L.W.: Inequality in the age of pseudonymity. In: Proceedings of the Fortieth AAAI Conference on Artificial Intelligence and Fortieth Conference on Innovative Applications of Artificial Intelligence and Eighteenth Symposium on Educational Advances in Artificial Intelligence. AAAI'26/IAAI'26/EAAI'26, AAAI Press (2026)
19. Yaish, A., Livshits, B.: Tierdrop: Harnessing airdrop farmers for user growth (2024), https://arxiv.org/abs/2407.01176v1
20. Yokoo, M.: False-name bids in combinatorial auctions. SIGecom Exch. **7**(1), 48–51 (Dec 2007). https://doi.org/10.1145/1345037.1345049