DeFi Attack Analysis*

My subtitle if needed

Jack McKay

05 April 2022

Abstract

Decentralized finance (DeFi) describes the emerging ecosystem of financial services, protocols and applications built on and designed for public blockchains such as Ethereum and Algorand. One of the most promising applications of blockchain technology, DeFi has experienced explosive growth over the last few years. But with this growth has also come the attention of bad actors, who aim to exploit flaws in protocol security for personal gain. Using data collected by DeFi Yield's REKT Database on the 200 most costly exploits of DeFi protocols, this paper will analyze and identify trends in these exploits, with the goal of identifying the most common types of exploits, as well as other trends and patterns that may precipitate a hostile attack.

1 Introduction

Imagine a world where financial services are available to anyone, from any location, 24 hours a day, 7 days a week, without the need for any intermediaries. One where financial transactions are fully automated, eliminating the need for any intermediary financial institutions, reducing human error and lowering transactions fees. All transactions are stored on a public, open-source ledger, allowing for complete transparency. Such a world is becoming increasingly feasible by the day, and the key to achieving it lies in decentralized finance (DeFi). DeFi is a completely open source and decentralized ecosystem running on blockchain technology that offers users financial services such as loans, payments, asset management and derivatives, as well as access to decentralized crypto exchanges (DEXes). DeFi minimizes–and in many cases eliminates– the need for centralized institutions such as banks or brokerages. Interactions on DeFi are peer-to-peer and are completed via smart contracts, self-executing computer programs functioning as contracts between parties that automatically execute when certain pre-set conditions are met. As such, DeFi aims to return control over individual's finances back to the individual, restoring freedom of choice to the financial industry. The near-unlimited potential of DeFi has not gone unnoticed, with the industry as a whole experiencing incredible growth. DeFi's current market cap is $147 billion as of April 2022, up from $2 Billion two years ago (CoinGecko (2022)), an annual growth rate of 757.32%. One of the primary drivers of this growth is a design principle known as "permissionless composability", wherein developers are able to employ any combination of pre-existing DeFi protocols, without requiring any permissions, in order to fulfill specific use cases. This allows developers to create and interact with limitless combinations of protocols, without any third party controlling any aspect of the network activity, creating a seamless and frictionless innovation cycle wherein users can build off of each others work. Indeed, permissionless composability is one of the fundamental innovations that has allowed DeFi to grow so quickly. However, this growth has not been without setbacks. One of the primary drawbacks to DeFi is its vulnerability to hackers. By nature of the way composability allows applications to work on top of each other, if the base chain was to suffer an attack, all of the applications built on top of it would also be at risk. As well, as transactions are executed automatically via smart contracts and without human oversight, this means that a bug in a smart contract can be exploited by hackers and used to reroute funds from the transaction. Due to these risks, identifying and preventing possible attacks is one of the primary focuses of the DeFi community at the moment. Using data collected by

*Code and data are available at: https://defiyield.app/rekt-database

DeFi Yield and scraped by Octoparse, this paper will analyze data from the 200 costliest attacks on DeFi protocols in order to identify the sectors most vulnerable to hostile attacks, as well as the types of attacks that are most frequent, with the goal of determining where DeFi cybersecurity efforts would best be focused.

2 Data

Our data is of penguins (Figure **??**).

3 Model

$$Pr(\theta|y) = \frac{Pr(y|\theta)Pr(\theta)}{Pr(y)} \tag{1}$$

Equation (1) seems useful, eh?

Here's a dumb example of how to use some references: In paper we run our analysis in `R` (R Core Team 2020). We also use the `tidyverse` which was written by Wickham et al. (2019) If we were interested in baseball data then Friendly et al. (2020) could be useful.

We can use maths by including latex between dollar signs, for instance θ.

4 Results

5 Discussion

5.1 First discussion point

If my paper were 10 pages, then should be be at least 2.5 pages. The discussion is a chance to show off what you know and what you learnt from all this.

5.2 Second discussion point

5.3 Third discussion point

5.4 Weaknesses and next steps

Weaknesses and next steps should also be included.

Appendix

A Additional details

References

CoinGecko. 2022. *Top 100 Defi Coins by Market Capitalization*. https://www.coingecko.com/en/categories/decentralized-finance-defi.

Friendly, Michael, Chris Dalzell, Martin Monkman, and Dennis Murphy. 2020. *Lahman: Sean "Lahman" Baseball Database*. https://CRAN.R-project.org/package=Lahman.

R Core Team. 2020. *R: A Language and Environment for Statistical Computing*. Vienna, Austria: R Foundation for Statistical Computing. https://www.R-project.org/.

Wickham, Hadley, Mara Averick, Jennifer Bryan, Winston Chang, Lucy D'Agostino McGowan, Romain François, Garrett Grolemund, et al. 2019. "Welcome to the tidyverse." *Journal of Open Source Software* 4 (43): 1686. https://doi.org/10.21105/joss.01686.