DeFi Attack Analysis[*]

My subtitle if needed

Jack McKay

24 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 DEFIYIELD'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://github.com/jmacattack27

DEFIYIELD 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

2.1 Data Source

The data used in this report was collected by DEFIYIELD in their public Rekt Database, a database containing information on all recorded DeFi scams, hacks and exploits, including the total funds lost in each event, as well as a breakdown of the technical issues that led to the hack. Data on the 200 costliest attacks was then scraped from the DEFIYIELD's website via Octoparse, an a visual web data extraction software, before being downloaded into a .csv file, at which point it was uploaded to R, cleaned, and made ready for analysis.

2.2 Data Collection

The dataset used in this report contains information on the 200 costliest attacks in the DeFi space since the inception of cryptocurrency, with data on attacks as early as the Bitcoin Savings and Trust Ponzi scheme in July 2012, and as recently as the Elephant Money attack 2 weeks ago. The term 'attack' is used as a catch-all term to encompass any sort of malicious event occuring in the greater decentralized finance space in which funds were lost, with such events including hacks, rug pulls, exploits, dubious projects and exit scams.

This dataset is a subset of the greater Rekt Database, which at the time of writing holds information on 2780 attacks. Data was collected and recorded manually by the team at DEFIYIELD over the course of multiple months, before the database was published in August 30, 2021, from which point it has been continuously updated. While DEFIYIELD is constantly recording new attacks and updating their database themselves, individuals can also report a claim if they have been affected by an attack themselves, at which point an engineer at DEFIYIELD will work to verify the report. If the claim is corroborated, the engineer will then analyze activity on whichever chain the attack is reported to have occurred, and if the claim is proven to be valid, the attack is then added to the database. Each entry in the database contains the following details:

- The name of the exploited project & its associated URL
- The chain on which the attack occurred
- The date on which the attack occurred
- The type of malicious event: (Exit Scam, Flash Loan, Exploit, Abandoned, Bank Run, Honeypot, Access Control)
- The total funds lost in the attack

Malicious events are further defined as follows:

- Exit Scam: When promoters of a cryptocurrency or DeFi protocol vanish during or soon after the initial coin offering (ICO) for their product. Promoters will market and promote the currency or concept in order to raise money from investors, before abandoning the project and disappearing with said money.
- Flash Loan: A flash loan attack occurs when a bad actor manipulates the smart contract executing the flash loan in order to siphon funds to their own wallet. For example, a flash loan attack might involve the malicious party changing the values of the currencies being traded, in order to trick the smart contract into thinking the loan has been repaid when it hasn't.
- Exploit: Any sort of hostile attack on a DeFi service that exploits a vulnerability or oversight in the protocol code. Exploits can take many forms.
- Abandoned: When a project is abandoned by its developers. Abandoned coins are referred to as 'dead coins'.

- Bank Run: Similar to with traditional banks, a bank run in DeFi refers to when holders of a token rapidly withdraw their assets, causing the token price to drop and leading to a negative feedback loop wherein other holders panic-sell their tokens, further lowering the price, causing even more users to sell their tokens, and so forth. The most recent example of a DeFi bank run occurred with Iron Finance's TITAN token, which dropped from US$65 to US$0.000000035 over the course of a single day. Stablecoins, particularly algorithmically backed stablecoins, are especially vulnerable to bank runs.
- Honeypot: An attack in which attackers create and send out smart contracts that have an apparent vulnerability, but contain a hidden trap, such that when an unsuspecting user goes to exploit the apparent vulnerability in the contract, the trap activates and allows the attacker to siphon the victims funds to themselves.
- Access Control: A scam in which the attacker obtains access to a targets digital wallet or authentication keys.

2.3 Data Analysis

This dataset scraped from DEFIYIELD's public Rekt Database via the data extraction software Octoparse (Team (2022)), before being imported to JupyterHub. Data was then processed and analyzed using the R programming language (R Core Team (2020)), as well as tidyverse (Wickham et al. (2019)), tidyr (Wickham (2022)) and dplyr (Wickham et al. (2021)) programming packages. The package janitor (Firke (2021)) was used to clean column names.

2.3.1 Exploitation Rates by Chain

The first aspect of the data that I analyzed was which chains were being exploited most frequently. Summing the number of exploits on each chain into a new data frame, Figure 1 shows the distribution of attacks across all recorded chains. Here we see that the vast majority of attacks occur on either Ethereum (ETH) or Binance Smart Chain (BSC); 50.5% and 30.5% respectively. The remaining 19% of attacks are spread more evenly across the other chains, with Polygon, Solana, Fantom and Avalanche (AVAX) accounting for a combined 12.5% of total attacks. The remaining 6.5% is distributed evenly across the remaining chains.

Just looking at the number of attacks per chain doesn't give us the full picture on their security. There are numerous factors that would affect the number of attacks attempted on a given chain. One such factor is the varying total value locked (TVL) in each chain. The more value locked in a chain, the more liquidity exists to be exploited; as such, larger chains like Ethereum are naturally subject to more attacks. Using data from DeFi Llama (DefiLlama (2022)) on the total value locked across each chain, Figure 2 shows the distribution of the number of exploits on each chain, divided by the TVL (in billions) in that chain. This gives us a more realistic picture of the rate at which each chain is being targeted. Note that this figure includes two graphs: one containing data on Polkadot, and one without data on Polkadot. Due to the relatively tiny amount of value locked in the Polkadot chain (about $3.84 million), the exploits to TVL ratio for Polkadot was more than 31x greater than the next highest ratio. As a result, the scale of the graph is disproportionately affected making it far less interpretable. As such, a second graph is included that omits data on Polkadot. Here we see a wildly different distribution than in the previous figure, with Ethereum going from the by far the most exploited chain to the third least exploited, while chains such as Algorand (ALGO), Heco, RONIN and EOS all saw substantial increases in their adjusted attack rates. Cronos and Tron remain the least exploited, while Avalanche (AVAX) also saw a noticeable decrease in exploit rates relative to the other chains.

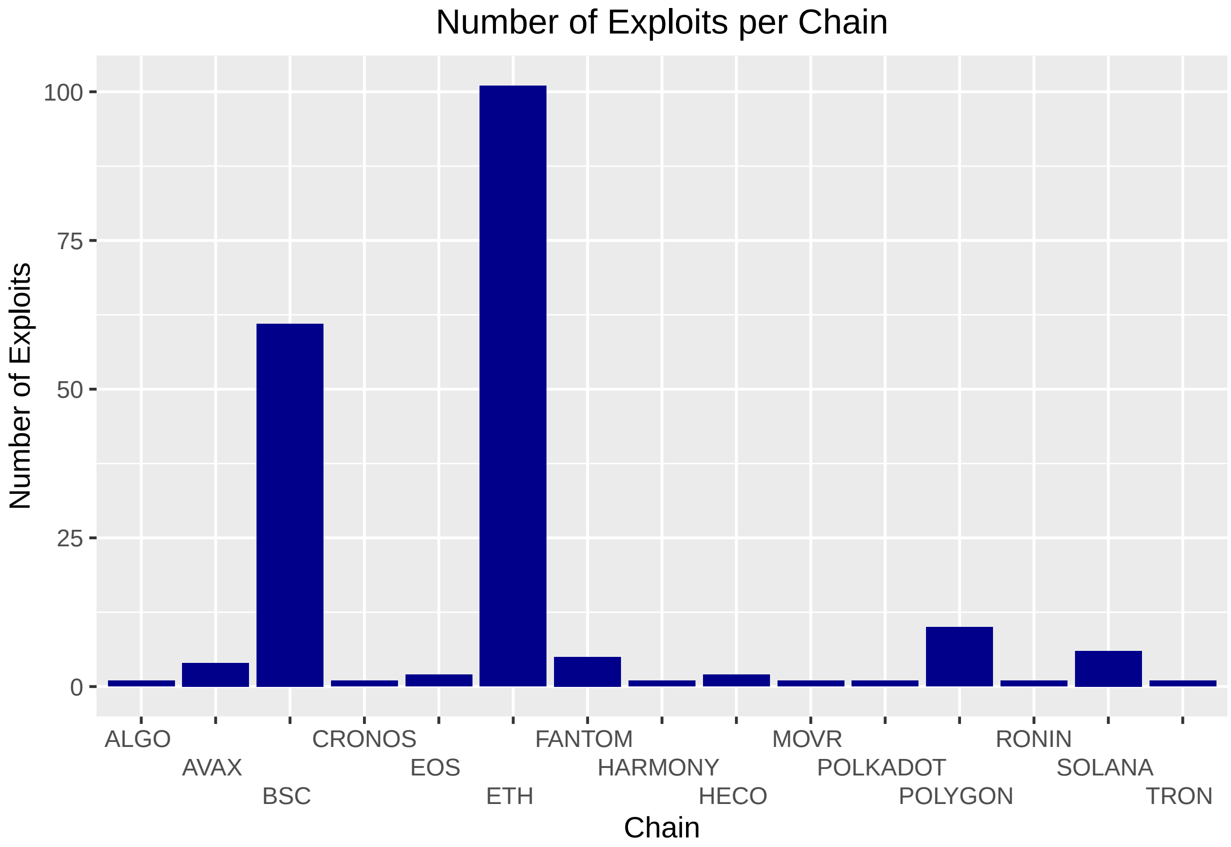
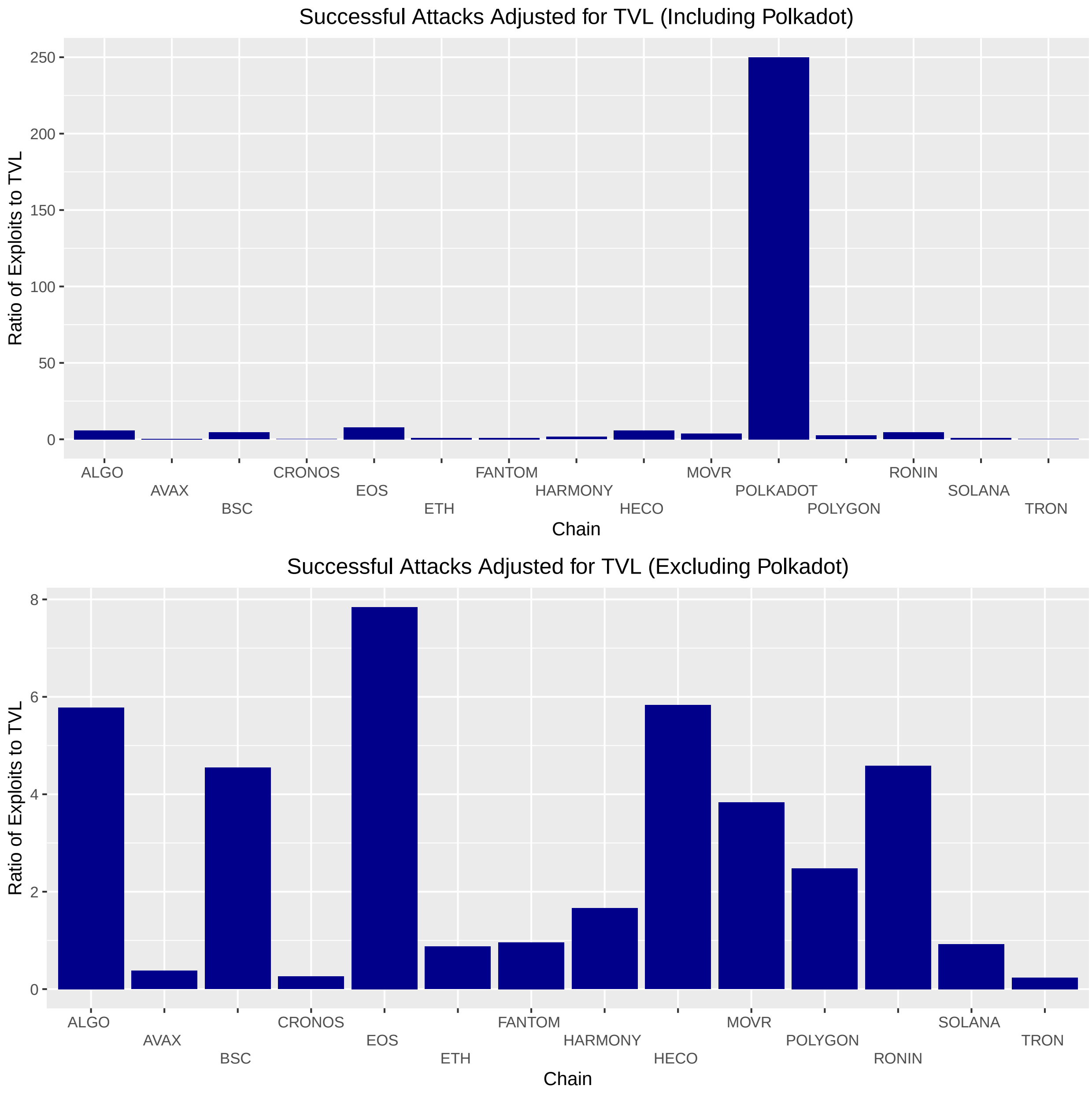


Figure 1: The Distribution of Attacks by Chain

2.3.2 Attack Rates by Type of Attack

The next aspect of the data I analyzed was the distribution of attack data, in terms of what types of attacks are most common, which types have historically resulted in the most damage, and which types are most damaging on average. Figure 3 shows the distribution of attack types, based on frequency, total damage and average damage. Here we see that exploits are by far the most prevalent types of attacks across all metrics, being more than twice as common as any other attack, and almost 3 times more costly on average. We also notice that despite being the second most common attack, exit scams are only the 4th costliest attacks on average, with both access control and flash loan attacks costing more on average. Abandoned projects are by far the least common attack, and are only slightly less costly than honeypot attacks, the second least damaging attack.

Continuing my analysis into attack rates, the next aspect of the data I analyzed is how the frequency of each type of attack is changing over time. Figure **??** shows the number of each type of attack year over year since 2016. Here we see that the every type of attack increased in frequency in 2021, with exploits experiencing by far the greatest spike.



Successful Attacks Adjusted for TVL (Including Polkadot)

Successful Attacks Adjusted for TVL (Excluding Polkadot)

Figure 2: The Distribution of Attacks Adjusted for Total Value Locked

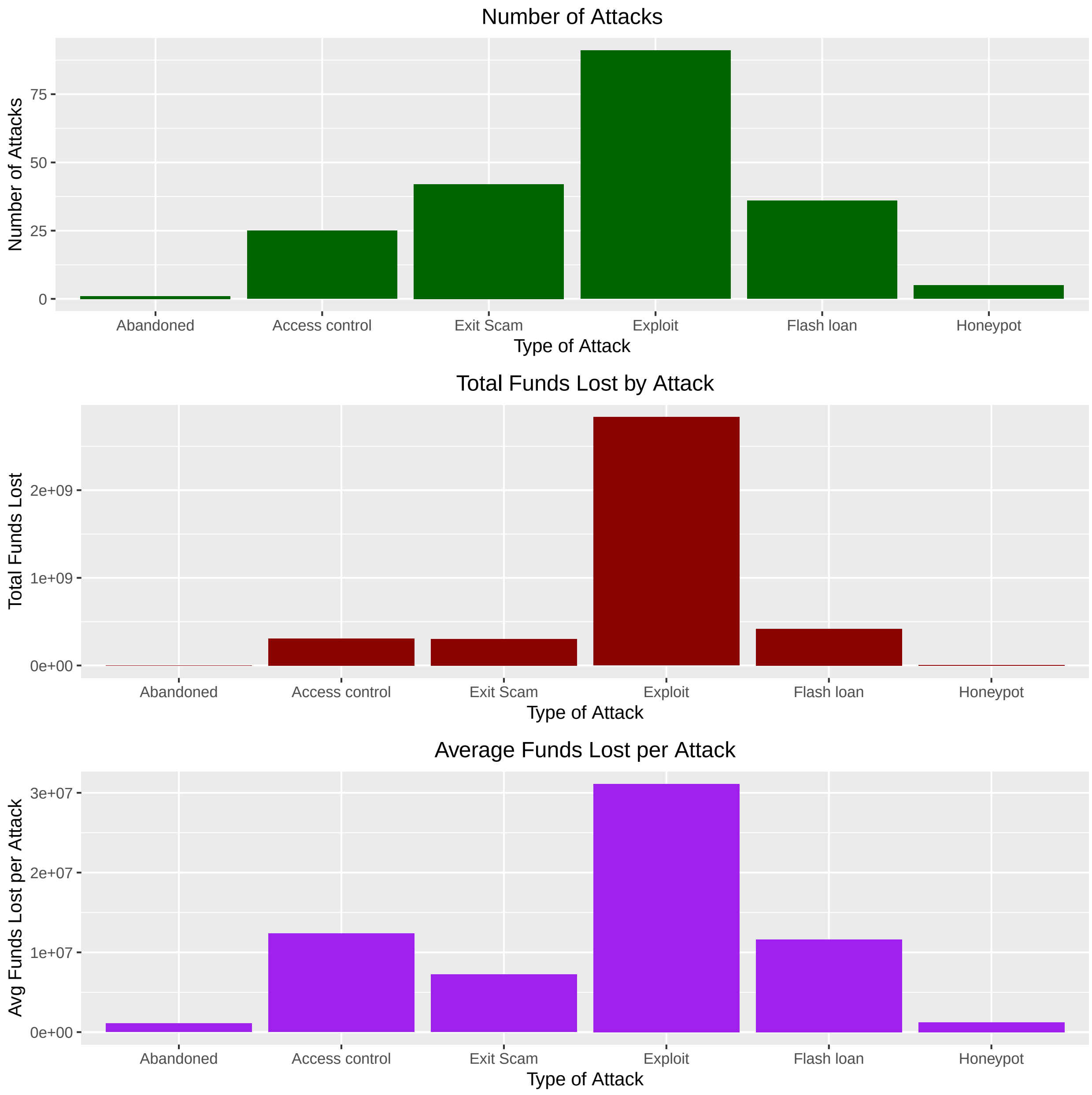
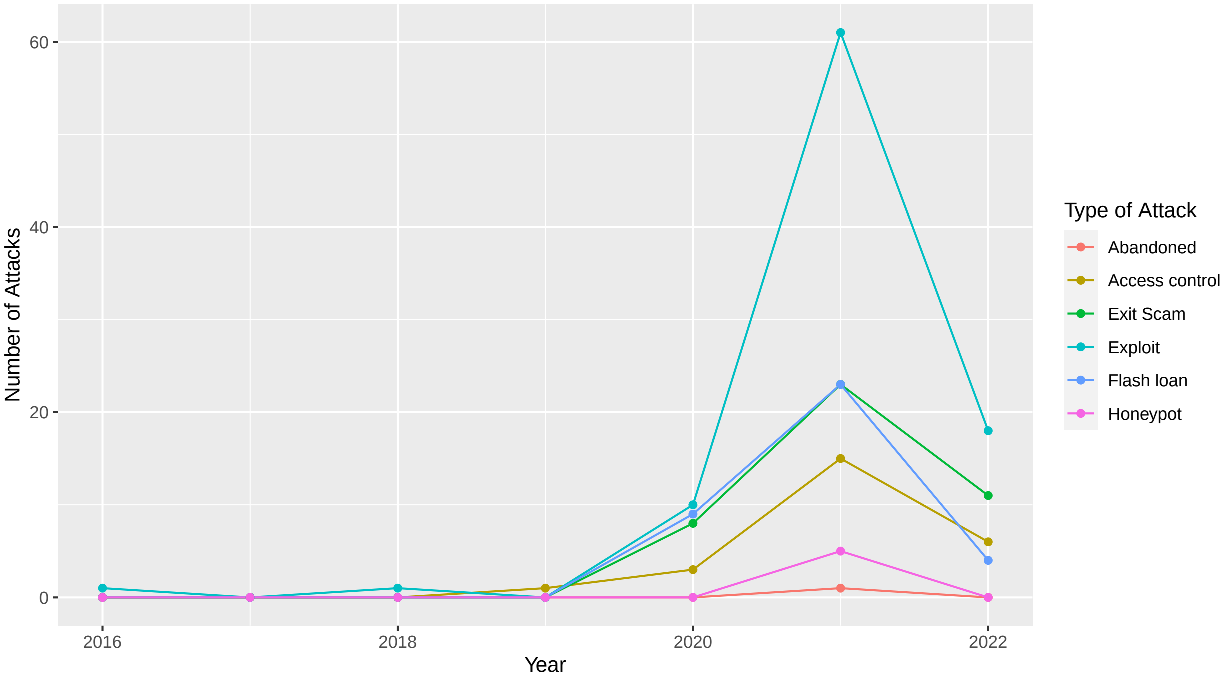


Figure 3: Distribution of Attack Type by Quantity, Net Loss and Average Loss per Attack


Number of Attacks
60
40
20
0
2016
2018
2020
2022
Year
Type of Attack
Abandoned
Access control
Exit Scam
Exploit
Flash loan
Honeypot

2.3.3 Attack Data by Chain

The final aspect of the data I will analyze is the attack data for individual chains. Of the chains in our data set, only Ethereum, BSC and Polygon have witnessed enough attacks for the data to be statistically significant and interesting. Figure 4 shows the number of attacks on these chains, broken down by type of attack, so that we may see if certain chains are particularly vulnerable to certain types of attacks. Here we see that exit scams account for a noticeably smaller proportion of attacks on Ethereum compared to other chains, with BSC experiencing 38% more exit scam attacks in total than Ethereum, despite experiencing 39.6% less attacks in total. Exit scams accounted for 50%, 42.9% and 29.5% of the attacks on Solana, Polygon and BSC respectively, compared to only 13% of attacks on Ethereum, indicating that Ethereum is particularly secure against exit scams. On the other hand, we see that Ethereum is disproportionately affected by access control attacks, which account for 16.2% of attacks on ETH, compared to only 6.9% of attacks on BSC, and 0% of the attacks on Solana or Polygon. As well, ETH is the only chain to have experienced a honeypot exploit, which account for 5.1% of ETH attacks. Interestingly, flash loans account for a very similar proportion of attacks on ETH, BSC and Polygon, at 19.2%, , 21.3% and 28.6% respectively, while not Solana did not experience any such attacks.

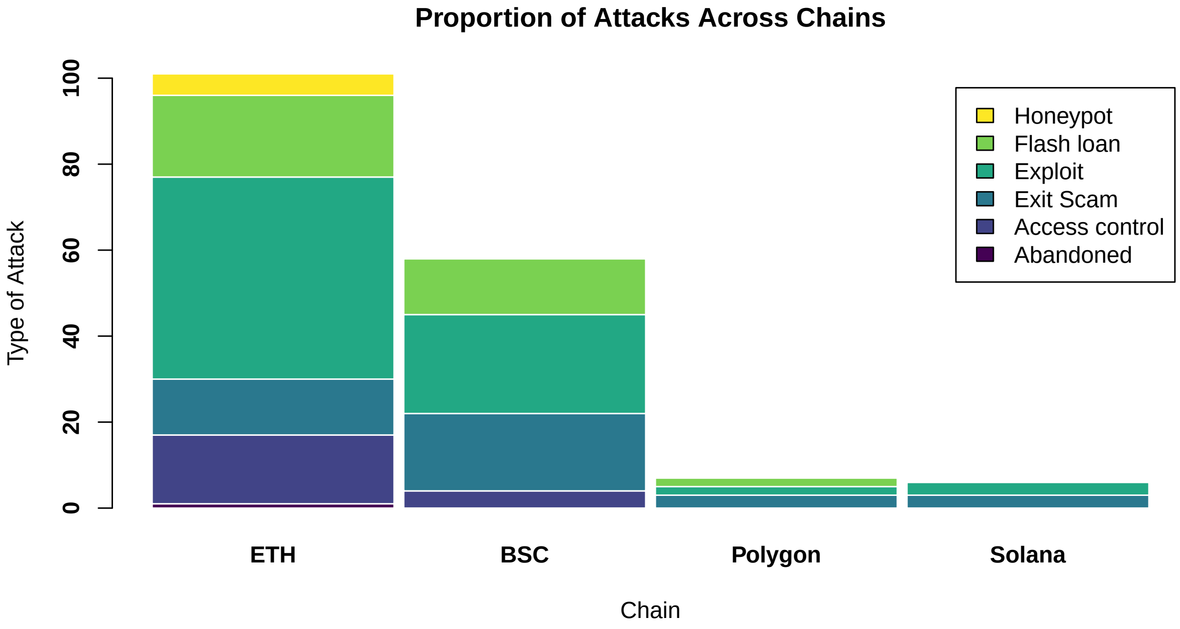


Figure 4: Number of Attacks per Chain by Attack Type

3 Results

4 Discussion

4.1 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.

4.2 Second discussion point

4.3 Third discussion point

4.4 Weaknesses and next steps

Weaknesses and next steps should also be included.

A Appendix

A.1 Key Terms

Below is a alphabetized list containing key terms used throughout this paper and their definitions.

- Bad Actor: An entity that aims to circumvent security protocols and exploit projects and/or individuals for personal gain.
- Smart Contract: A self-executing agreement, written in lines of code, that automatically executes when predetermined conditions are met. Smart contracts allow for agreements to execute instantaneously, without the involvement of intermediaries, and such that all participants can be certain of the outcome. Smart contracts are one of the fundamental building blocks of decentralized finance.
- Stablecoin: A digit asset engineered to maintain a stable value relative to some national currency or other value-based asset. A stablecoin that is designed to replicate the value of another asset is considered "pegged" to that asset. Maintaining its peg to its associated asset is one of the primary focuses of stablecoins, which can be further classified based on the method used to maintain their peg:
  - Collateralized Stablecoins: Achieve price stability through holding reserves of fiat currencies equal to or greater than the market cap of the coin. Currently the most popular type of stablecoin, with examples including Tether (USDT) and USD Coin (USDC).
  - Algorithmic Stablecoins: A stablecoin model involving 2 tokens: a stablecoin and a token that shares in the system's profits from new issuance of stablecoins. Shares in the latter token are issued to holders of the former, and allow for developers to maintain the stablecoin's price by controlling the supply, without harming holders.
- Flash Loan: A form of uncollateralized lending executed via smart contract that allows users to borrow any available amount of assets without posting any collateral. Instead, the liquidity from a flash loan must be instantly repaid to the lender within a single block transaction. If the borrower doesn't repay the capital, the transaction is instantly reversed.

B Additional details

References

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

DefiLlama. 2022. *DefiLlama - Total Value Locked All Chains.* https://defillama.com/chains.

Firke, Sam. 2021. *Janitor: Simple Tools for Examining and Cleaning Dirty Data.* https://cran.r-project.org/package=janitor.

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

Team, The Octoparse. 2022. *Octoparse: Web Scraping Tool & Free Web Crawlers.* https://www.octoparse.com/.

Wickham, Hadley. 2022. *Tidyr: Tidy Messy Data.* https://tidyr.tidyverse.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.

Wickham, Hadley, Romain François, Lionel Henry, and Kirill Müller. 2021. *Dplyr: A Grammar of Data Manipulation.* https://CRAN.R-project.org/package=dplyr.