

Flash in the pan?: Analyzing flash loan attacks on the DeFi ecosystem

Tim Hall 

*Department of Policing, Criminology and Forensics,
University of Winchester, Winchester, UK, and*

Remo Stieger

SyntiFi GmbH, Zug, Switzerland

429

Abstract

Purpose – This paper aims to explore attacks on the decentralized finance (DeFi) ecosystem through the case of flash loan attacks (FLAs). FLAs use flash loans, a novel form of lending developed in the DeFi ecosystem, to steal cryptocurrency assets. FLAs have been identified as serious emergent threats to the DeFi ecosystem with the potential to cause significant financial losses.

Design/methodology/approach – The paper used data from a massive on-chain analysis to identify all FLAs on seven major blockchains between February 2020 and July 2024, an analysis of public discussions of FLAs and an interview with a victimized platform.

Findings – The paper identified 254 successful attacks on the DeFi ecosystem resulting in losses of US\$ 6.568bn. 72 of these were FLAs, resulting in losses of US\$ 1.211bn. It identified 14 different types of FLA that either ‘manipulated price feeds’ (MPF attacks) or ‘exploited (flaws in) the underlying protocol logic’ of platforms in various ways (EUPL attacks). The analysis revealed distinctive temporal patterns of FLA activity.

Originality/value – Crimes targeting the DeFi ecosystem have grown significantly, producing a growing literature primarily from cybersecurity and cognate perspectives. This is true of the limited FLA literature to date. Despite an emergent interest in cryptocurrencies and the advocacy of criminological contributions, very little is known about attacks on the DeFi ecosystem from a criminological perspective. This paper aimed to extend understandings of FLAs specifically, and crimes targeting the DeFi ecosystem more generally, by applying a criminological lens for the first time to FLAs.

Keywords Cryptocurrencies, DeFi ecosystem, Crime, Cybersecurity, Criminology, Flash loan attacks

Paper type Research paper

Introduction

The decentralized finance (DeFi) ecosystem, built on blockchain technologies and utilizing smart contracts to offer peer-to-peer financial services, has grown significantly in recent years. Fundamental to the DeFi ecosystem are cryptocurrencies, digital assets that are traded and act as currencies in this ecosystem. The first cryptocurrency, Bitcoin, appeared in 2009, and by September 2025, the global market capitalization of all cryptocurrencies was estimated at over US\$ 4tn (Coingecko, 2025). The rapid growth of cryptocurrency use and value, the pseudonymity inherent in blockchain technologies and the lack of regulation of the DeFi ecosystem have raised concerns that cryptocurrencies offer extensive and diverse opportunities for criminality (Mackenzie, 2022; Trozze *et al.*, 2022).



Funding: This work was supported by funding from the Higher Education Innovation Funding, Innovation Accelerator Support Fund (2023–2024) and University of Winchester internal QR funding (2024–2025).

Cryptocurrencies have been associated with crime in three broad ways: as the focus of investment scams, where victims are lured into investing in, for example, fake cryptocurrencies (Habila Garba *et al.*, 2024; Kamps and Kleinberg, 2018; Mackenzie, 2022; Nizzoli *et al.*, 2020), through their use in illegal markets including drug dealing, money laundering, blackmail and extortion (Aldridge and Askew, 2017; Childs, 2023; Campbell-Verduyn, 2018; Desmond *et al.*, 2019; Holt *et al.*, 2023) and as the targets themselves of attacks on the DeFi ecosystem that have resulted in the loss of many billions of USD worth of cryptocurrency assets (Carpentier-Desjardins *et al.*, 2025; Zhou *et al.*, 2023). The largest cryptocurrency theft, for example, is believed to have occurred in February 2025 when hackers, thought to be from North Korea, stole an estimated US\$ 1.5bn in Ethereum tokens from the cryptocurrency exchange Bybit (Masud, 2025).

Crimes that steal cryptocurrencies target either human vulnerabilities, such as when victims are conned into revealing security details, or technical vulnerabilities, for example, in the exploitation of undetected bugs [1] in the code of platforms. Attacks that exploit technical vulnerabilities in the DeFi ecosystem are numerically more significant and account for greater financial losses than DeFi attacks that exploit human vulnerabilities (Carpentier-Desjardins *et al.*, 2025). Cryptocurrencies now represent major cybersecurity concerns and emergent areas of criminological research. While cryptocurrency investment scams and the use of cryptocurrencies in illegal markets have been the subject primarily of criminological research, studies of crimes targeting the DeFi ecosystem have emerged mainly from a cybersecurity perspective.

This paper explores crimes targeting the DeFi ecosystem through the case of flash loan attacks (FLAs). FLAs are crimes that use flash loans, a novel form of lending developed on the DeFi ecosystem, to steal cryptocurrency assets by exploiting technical vulnerabilities in this ecosystem. Flash loans are a form of uncollateralized lending, where assets are borrowed from liquidity pools and returned within the same blockchain transaction in return for a fee. If the borrower fails to repay the loan within the same transaction, the loan reverts. Flash loans are executed by smart contracts that run as code on a blockchain. Flash loans were introduced on the Ethereum blockchain in 2018 and have grown rapidly since (Figures 1 and 2). They have a number of legal uses including arbitrage, liquidations, collateral swaps and creating leveraged positions (Coinbase, 2024).

Flash loans have proven controversial, however, as they have also been used to fund attacks on the DeFi ecosystem. Some studies have identified the use of flash loans “as a vehicle to significantly amplify attack profit” (Carpentier-Desjardins *et al.*, 2025: 3; see also Chen *et al.*, 2024; Gan *et al.*, 2023; Gudgeon *et al.*, 2020; Oosthoek, 2021; Qin *et al.*, 2021). FLAs are executed in various ways [our analysis identified 14 specific types of FLAs (types of FLA)]. These can be divided into Two broad types: FLAs that ‘manipulate price feeds’ [2] (MPF attacks), or FLAs that ‘exploit (flaws in) the underlying protocol logic’ of platforms in various ways (EUPL attacks). The specific techniques used within FLAs vary considerably, but what is common to all FLAs is the use of flash loans by attackers to access the, often considerable, collateral needed to execute these attacks. The techniques used within different types of FLA are outlined below.

Manipulating price feeds/creating price or stake imbalances (MPF):

- *Price oracle attack*: An attacker uses the borrowed assets to manipulate the feed into the protocol’s price oracle.
- *Governance attack*: An attacker gains a substantial, albeit temporary, share of voting power in the protocol’s governance.

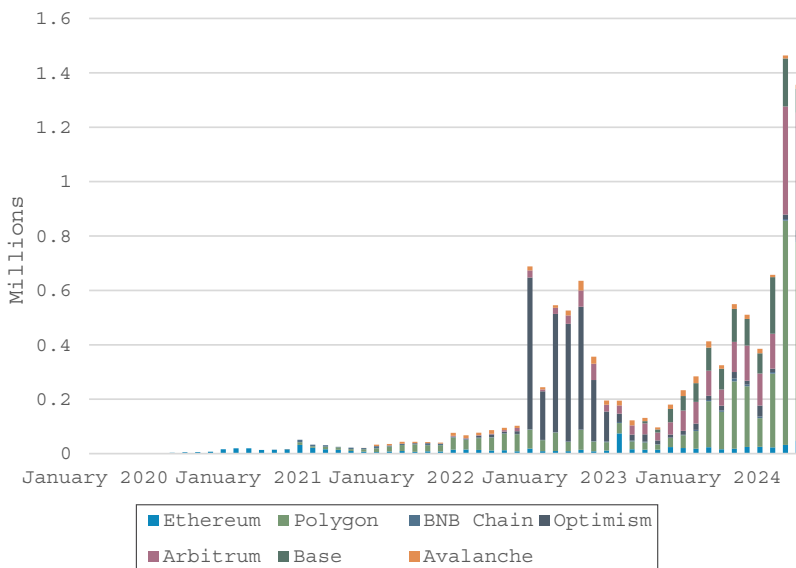


Figure 1. Number of flash loans. Monthly flash loans, by blockchain

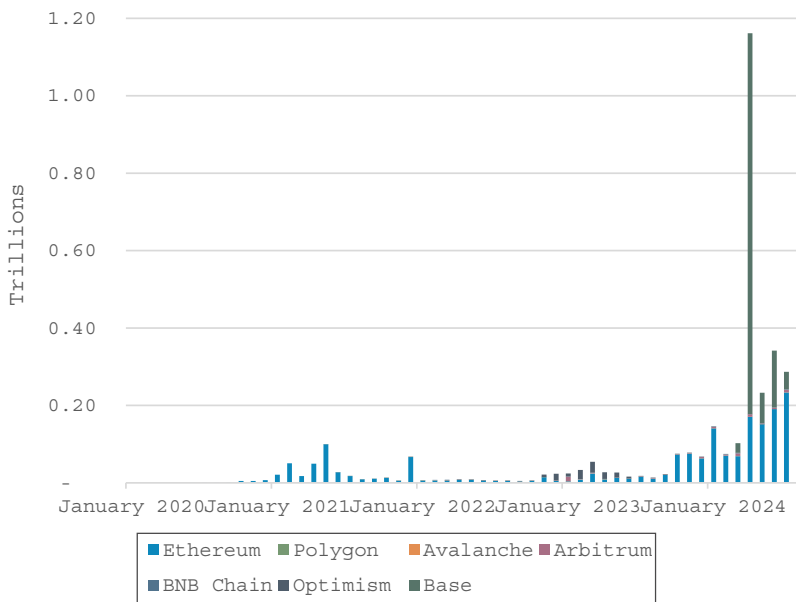


Figure 2. Value borrowed US\$, monthly flash loans by blockchain

- *Swap logic exploit*: An attacker uses the borrowed tokens to execute large trades on one or more liquidity pools. By swapping a large amount of one asset for another, they create a significant price imbalance in the targeted pool.
- *Incentive rewards exploit*: An attacker uses a flash loan to temporarily manipulate their stake or activity within a protocol to capture an outsized share of incentive rewards.
- *Price manipulation attack*: An attacker uses the borrowed funds to cause an imbalance in the token reserves. This reserve imbalance skews the automated market maker mechanism, temporarily inflating or deflating the price of the asset within the pool.
- *Slippage attack*: An attacker uses the borrowed funds to make a large trade within a liquidity pool or decentralized exchange. The trade is designed to cause a price slippage, where the price of an asset moves unfavorably due to insufficient liquidity.
- *New market exploit*: An attacker takes advantage of the initial conditions in the market (such as price discovery, low liquidity or flawed incentive mechanisms) to make a profit at the expense of other users or the protocol.
- *Burn function exploit*: An attacker manipulates the protocol's burn function.

Exploitation of issue with underlying protocol logic (EUPL):

- *Donate function logic exploit*: An attacker uses the borrowed tokens to make a 'donation' to the target contract. This contract might have a logic flaw where rewards or benefits are calculated based on the total balance of tokens in the contract or the relative contribution of the sender.
- *Reentrancy attack*: An attack takes advantage of a contract's inability to update its internal state before a function completes, which the attacker repeatedly calls in rapid succession using borrowed funds.
- *Pool shares exploit*: The attacker uses a flash loan to manipulate their share in a liquidity pool temporarily, allowing them to extract an outsized profit.
- *Misconfiguration exploit*: An attacker takes advantage of errors or oversights in a DeFi protocol's configuration.
- *Withdraw logic exploit*: An attacker uses a flash loan to exploit vulnerabilities in a protocol's withdrawal or redemption logic.
- *Rounding donation attack*: An attack takes advantage of how small fractional values are rounded off in the protocol, typically when performing operations like donations, distributions or reward allocations.

While FLAs constitute criminal conduct, the specific offences engaged and the applicable legal framework will depend on the jurisdiction and the factual context in which the attack occurs. FLAs, whether MPF or EUPL attacks, can constitute criminal conduct because they intentionally distort or abuse a system to obtain assets without legitimate entitlement. From a legal perspective, these actions typically fall under fraud, unlawful appropriation and computer misuse and can constitute hacking-related offences (or unauthorized interference with data processing), under, for example, the UK's Computer Misuse Act 1990 and the Swiss Criminal Code (e.g. Art. 146 fraud, Art. 147 computer fraud). Liability arises where a person intentionally manipulates or exploits digital systems or data to cause financial loss or secure an unjust enrichment. Accordingly, FLAs can fall within established criminal

offences even when executed through permitted protocol interactions, provided the elements of manipulation, intent and economic harm are met. Furthermore, FLAs can also trigger regulatory implications, particularly where they distort markets or harm investors.

The massive growth of flash loans, their potential to amplify attack profits and the greater significance of attacks that exploit technical vulnerabilities, suggest that FLAs represent a potentially serious emerging threat within the DeFi ecosystem. All of the specific analysis of FLAs to date has emerged within the disciplines of cybersecurity, digital forensics and cryptography (Gudgeon *et al.*, 2020; Chen *et al.*, 2024; Gan *et al.*, 2023; Oosthoek, 2021; Qin *et al.*, 2021). While offering invaluable insights into this emerging threat, this literature has tended to be highly technical in nature, somewhat limited in its empirical scope and exclusively focused either on the internal dynamics of attacks (Cao *et al.*, 2021; Qin *et al.*, 2021; Xu and Feng, 2022) or on cybersecurity detection or prevention systems (Chen *et al.*, 2024; Deng *et al.*, 2023; Wang *et al.*, 2021; Wang *et al.*, 2022) and has largely lacked analysis of the external, contextual dimensions of FLAs.

This paper aims to extend this previous research and is organized around the following research question: what patterns of FLA activity can we identify, and what do these tell us about the nature of FLAs, their significance and impacts, the perpetrators of FLAs and responses to them? The paper makes four primary contributions. Empirically, it offers the first extensive analysis of FLAs. It explores the nature, patterns and extent of FLAs across seven major blockchains between February 2020 and July 2024. This analysis uses data from over 20 billion cryptocurrency transactions obtained using a specialist on-chain risk intelligence (ORI) engine. Our analysis is more outward-looking than is typical of the FLA literature, and FLAs are here contextualized within the growth of the DeFi ecosystem generally, flash loans specifically and the wider DeFi attack landscape, in ways that have not been done previously. Further, we complement the technical data obtained from the ORI engine with an analysis of public discussions of 35 FLAs and an interview with a cryptocurrency platform that suffered a major FLA. The paper considers what social dimensions of FLAs these data reveal. This combination of data offers some methodological innovation. The paper also considers the theoretical contributions of this analysis for criminological, rather than cybersecurity, analysis of cryptocurrency crimes. Finally, it also highlights applied contributions of this analysis for the DeFi community, the cybersecurity sector, law enforcement agencies, regulators and policymakers. The research for this paper was conducted through a partnership between an academic criminology researcher and SyntiFi, a DeFi risk intelligence company.

Literature review

There is now an extensive and rapidly growing cybersecurity literature exploring attacks on the DeFi ecosystem that has emerged and grown in step with the growth of this sector (for a detailed review see Carpentier-Desjardins *et al.* (2025: 2–3). This literature considers issues such as the inherent vulnerabilities of the DeFi ecosystem, the nature and extent of attacks and the challenges of identifying, preventing and responding to malicious activity targeting this sector. Studies have identified significant losses through attacks on the DeFi ecosystem. Zhou *et al.* (2023), for example, identified losses to the DeFi ecosystem of US\$ 3.24bn between 30 April 2018 and 30 April 2022, while Carpentier-Desjardins *et al.* (2025) reported a figure of US\$ 10bn in DeFi losses to attacks of various types between 2017 and 2022. Within the literature that has explored attacks on the DeFi ecosystem, though, there has been only limited attention given to FLAs.

A literature specific to FLAs began to emerge in 2021 with Qin *et al.* (2021) claiming to produce the first paper to specifically explore the implications of FLAs for the DeFi

ecosystem. This paper analyses two FLAs from February 2020. Such an intensive empirical focus is not unusual within the FLA literature. Other studies, for example, provide analysis of two (Cao *et al.*, 2021; Qin *et al.*, 2021), three (Xu and Feng, 2022) and six (Wang *et al.*, 2022) FLAs. More extensive empirical analysis of FLAs is available in studies that explore cybersecurity systems designed to detect or prevent FLAs (Chen *et al.*, 2024; Deng *et al.*, 2023). These studies include analysis of 16 and 24 FLAs, respectively. Here, though the emphasis is primarily on testing the efficacy of cybersecurity systems. Prominent themes with the FLA literature are FLA detection, security and technical responses (Cao *et al.*, 2021; Chen *et al.*, 2024; Deng *et al.*, 2023; Gan *et al.*, 2023; Wang *et al.*, 2021; Wang *et al.*, 2022; Xu and Feng, 2022). This literature provides invaluable forensic detail on the technical vulnerabilities exploited in FLAs, their operations and nascent responses to them. However, in addition to the need for more extensive and accessible studies of FLAs, we see the need for analyses that look beyond the technicalities of individual attacks to provide more contextual analysis.

The literature specific to FLAs has emerged, to date, exclusively within cybersecurity and its cognate fields. This is largely true also of the wider literature exploring crimes targeting the DeFi ecosystem (see Carpentier-Desjardins *et al.*, 2025: 2–3). However, there has been a small but growing literature from criminology concerned with analyzing the implications of cryptocurrencies within criminal activity and advocacy for the value of a criminological contribution to DeFi-focused crimes. Dearden and Tucker (2023: 257), for example, argue that: “While cybersecurity, information technology, accounting and other disciplines can examine the financial data itself, we believe that criminologists can provide additional benefits in pattern analysis and organizing the context and theory around the transactions” (see also Mackenzie, 2022: 1537; Maimon and Louderback, 2019: 193). However, this criminological contribution remains, so far, limited and at best only partially realized.

Criminology’s cryptocurrency crime literature has primarily examined the implication of cryptocurrencies within a range of crimes including studies of fraudulent cryptocurrency investment, pump and dump and Ponzi scams (Habila Garba *et al.*, 2024; Kamps and Kleinberg, 2018; Mackenzie, 2022; Nizzoli *et al.*, 2020), drug and other illicit cryptocurrency markets (Aldridge and Askew, 2017; Childs, 2023) and cryptocurrency based money laundering (Campbell-Verduyn, 2018; Desmond *et al.*, 2019; Holt *et al.*, 2023). There has been very little specifically criminological research to date that has explored the theft of cryptocurrencies through attacks on the DeFi ecosystem. We identified only one, broadly, criminological study of crimes targeting the DeFi infrastructure to steal cryptocurrencies. Carpentier-Desjardins *et al.* (2025) offered a “mapping of the DeFi crime landscape” which includes analysis of an extensive database of DeFi crimes over a five-year period compiled from aggregator databases and which offers a rich analysis of the patterning of these crimes. Here, our technical data analysis follows a broadly comparable approach to that of Carpentier-Desjardins *et al.* (2025). Even in this case, though, the methods employed, the disciplinary orientations of the majority of authors and the publication outlet suggest a significant cybersecurity rather than criminological orientation within this study.

The methods and data employed in the majority of criminological studies of cryptocurrency crimes tend to be more qualitative and limited than those from cybersecurity studies. Examples from this literature have included online ethnographies and discourse analyses (Dearden and Tucker, 2023: 257), including advertising strategies of vendors of illicit services (Holt *et al.*, 2023) and interactions between participants in illicit markets, online forums and on social media (Childs, 2023; Mackenzie, 2022; Nizzoli *et al.*, 2020). Direct empirical observation of cryptocurrency crimes and the use of blockchain data is almost entirely absent from this criminological literature of cryptocurrency crimes (though

see [Dearden and Tucker, 2023](#); [Kamps and Kleinberg, 2018](#)). Consequently, in eschewing the incorporation of blockchain data, much criminological literature on cryptocurrency crimes embodies [Maimon and Louderback's \(2019: 208\)](#) concerns about “serious data limitations” in relying, with a small number of exceptions, on convenience samples and “small samples of publicly available posts from online markets”. While illuminating some of the social dimensions of cryptocurrency crimes, such studies say relatively little about “the progression of criminal events” ([Maimon and Louderback, 2019: 208](#)) and their technical operations.

Often criminological studies have emphasized continuities between cryptocurrency scams and earlier pre-digital crimes. [Kamps and Kleinberg \(2018: 2–3\)](#), for example, draw comparisons between cryptocurrency pump-and-dump schemes and earlier stock market ‘bubble’ scams, while [Mackenzie \(2022: 1539–1541\)](#) compares crypto scams to pre-digital cons such as fake bookmaker scams. Here, we typically see the deployment of a relatively narrow palette of criminological theory that was developed in the study of pre-digital crimes. [Dearden and Tucker \(2023: 270\)](#), for example, acknowledge the potential relevance of convenience theory and routine activity theory (RAT). There are reasons to suppose, however, that the transfer of such criminological theories to the context of crimes targeting the DeFi ecosystem is not unproblematic. [Weulen Kranenborg \(2020: 196\)](#), for example, notes the necessity for cybercriminals undertaking crimes of great technical complexity, such as those targeting the DeFi ecosystem, to acquire highly specialized, skills and to demonstrate considerable planning, investment and patience, qualities that seem unlikely to be developed in contexts that are “routine” and “convenient,” to reference those theories highlighted by [Dearden and Tucker's \(2023\)](#). Elsewhere, and following [Brown's \(2006\)](#) call for a “criminology of hybrids,” other criminological studies of cryptocurrency crimes have lent towards theories such as technosocial ([Mackenzie, 2022](#)) and assemblage ([Childs, 2023](#)) theories. These recognise cybercrimes as assemblages of social and technical actants. While offering significant theoretical innovation, these studies remain somewhat fettered by the challenges of accessing and interpreting blockchain data that reveals the technical, operational empirics of the cryptocurrency crimes. Both [Mackenzie \(2022\)](#) and [Childs \(2023\)](#), for example, draw upon extensive qualitative analysis of discussions within crypto trading forums and social networks, rather than directly scrutinizing the use of cryptocurrencies in illegal transactions. What we have here, then, are valuable social analyses of these crimes rather than wholly technosocial analyses. Transcending the technical-social binary that has run through the criminological literatures on cryptocurrency crimes has proven difficult to achieve in the absence of empirical data from the technical side. Criminology's contribution, then, to the interpretation of crimes targeting the DeFi ecosystem to steal cryptocurrency assets remains somewhat fettered by both empirical and theoretical challenges.

FLAs have been recognized as a nascent, potentially significant threat to the DeFi ecosystem that has, thus far, produced only a very limited research literature. This, like much of the literature on threats to the DeFi ecosystem, has emerged within the field of cybersecurity and its cognate disciplines. This literature, and the data that supports it, has been largely technical in nature. While criminological contributions to understanding threats facing the DeFi ecosystem and cryptocurrency focused criminal activities have been advocated ([Dearden and Tucker, 2023: 257](#); [Mackenzie, 2022: 1537](#); [Maimon and Louderback, 2019: 193](#)), they have yet to provide any substantive engagement with crimes that target the DeFi ecosystem to steal cryptocurrencies and have tended to rely on qualitative data ([Maimon and Louderback, 2019: 208](#)). There is yet to be any substantive deployment of technical quantitative blockchain data within the criminological literature of cryptocurrencies and crime. This paper aims to apply a more criminologically

informed perspective by using both technical quantitative blockchain data and social qualitative off-chain data.

Methods

Three sets of data were collected: an on-chain analysis of cryptocurrency transactions, an analysis of the cryptocurrency media and an interview with a platform victimized by a FLA. The first of these identified all FLAs during our study period and provided a range of information about each attack, while the second and third data sets provided various contextual information relating to these attacks. This paper offers the first instance of data of these kinds being brought into analytic dialogue.

The first data set comprised a massive on-chain analysis of the seven major blockchains where flash loans are available (Ethereum, Base, Optimism, Arbitrum, BNB Chain, Avalanche and Polygon) to identify all FLAs that occurred within our study period (February 2020–July 2024). No “off-the-shelf” databases of FLAs previously existed. Blockchain data is inherently vast and disorganized. Every transaction, smart contract interaction and event is stored permanently, leading to continuous data growth without any deletion or compression. Finding a specific event requires potentially scanning millions of blocks and billions of transactions. Unlike traditional databases, blockchains prioritize security and integrity over structured, queryable storage. Data is organized chronologically, not by relevance or user, and smart contracts each define their own unique, often complex storage formats. They store their internal data in low-level key-value storage and not in an organized SQL database. Additionally, redundant and failed transactions remain part of the history, increasing noise. Accessing meaningful information requires scanning and interpreting massive amounts of low-level data, making blockchain data challenging to query efficiently without specialized indexing solutions. A scalable and systematic approach involves the use of blockchain indexing, such as ORI.

Our analysis used Syntifi’s ORI engine, which scanned 20.63 billion transactions across the seven blockchains. From this, we identified 72 FLAs and 182 other attacks on the DeFi ecosystem. To enhance methodological reliability, all potential FLAs identified by the proprietary ORI engine were subjected to a multi-stage validation process. Candidate transactions were cross-checked against publicly reported incidents, protocol documentation, blockchain explorers and transaction traces where available. Attack types were assigned through manual verification of the transaction sequence and exploited vulnerability, while ambiguous cases were reviewed individually and excluded where classification could not be established with sufficient confidence. This combined automated and manual approach was adopted to minimize false positives and false negatives while ensuring consistent classification across the data set. Our sample identified 48 more FLAs than the largest previous sample within the FLA literature. The data collected here included victims, date of attack, attack type and amount stolen. These data were analyzed using a variety of descriptive statistics. Forensic details of every transaction involved in each attack were also available from this analysis. These were included in the data analysis only to classify FLAs into the 14 types we outline in Types of FLA. Our focus in this paper is primarily contextual rather than upon internal FLA dynamics.

Our on-chain data underwent extensive statistical analysis to produce a comprehensive picture of FLA activity and trends during our study period. This analysis had four aims. The first was to produce a comprehensive statistical breakdown of the 72 FLAs identified, including attack frequency, total and average losses, different types of attack (analyzed on two levels), their frequency and total and average losses attributable to different types of attack. Victimization data was also analyzed descriptively by both platform and blockchain.

A FLA typology was produced by combining data on FLA type, loss and frequency. Second, these data underwent comprehensive temporal analysis to reveal FLA trends over our study period. Third, our data was subject to contextual analysis that explored FLAs within global flash loan activity and the wider DeFi attack landscape. This again involved both descriptive statistical and temporal analysis and aimed to assess the temporally dynamic contributions of FLAs to the wider DeFi attack landscape and the threat they pose to flash loan activity. Finally, regression analysis was undertaken to explore the relationships between FLA activity and DeFi market conditions, by exploring flash loan number and value and total value locked (TVL [3]) as potential predictors of FLA activity. To explore the relationship between market activity and FLAs, ordinary least squares regression models were estimated. The dependent variables included monthly attack frequency, attack volume and FLA metrics, while the independent variables comprised TVL, total flash loan volume and the total number of flash loans. Separate models were estimated for the full observation period and for the post-emergence period beginning in January 2020. Regression diagnostics were reviewed to assess model fit, and results are reported using regression coefficients (β), R^2 , adjusted R^2 , F -statistics, t -values, p -values and sample sizes (Appendix Table A1).

The second data collection phase involved an extensive scan of the cryptocurrency media to identify public discussions of FLAs. In total, discussions of 35 FLAs were identified in this way. Media texts were scrutinized to identify empirical details of the FLAs, which were used to verify data obtained through our ORI analysis. In addition, these sources revealed several contextual details including details about the impacts of FLAs and responses to them. The final data collection phase was an interview with a representative of a victimized platform. The platform had been open and public about the FLA that had targeted them and the responses they had taken. They were contacted through private messages on social media. Anonymity was granted at their request. The respondent revealed many details beyond the technical details of the FLA and the response to it that the platform had previously published and also talked about the wider impacts of FLAs and other attacks on the DeFi ecosystem. A number of other platforms were approached to participate but no others agreed to be interviewed. The data gathered from our analysis of the cryptocurrency media and the interview with a victimized platform was subject to thematic analysis. This revealed contextual information that complemented that produced by our statistical analysis of the on-chain data. These included details of the non-financial impacts of FLAs, responses to them by affected platforms and the wider DeFi community and some, albeit limited, information about attackers.

We cannot claim representativeness or data saturation from this single interview or from our relatively limited sample of media sources. However, accessing respondents from within the cryptocurrency and DeFi sectors generally is a challenge given the pseudonymity of this sphere. Accessing those affected by DeFi attacks is particularly difficult given the challenges of identifying victims and the reputational risk associated with discussing victimization. Much remains to be done to open up this sector to academic scrutiny. This interview here acted as complementary data, highlighting a number of contextual features of the attacks identified through our ORI analysis. Given the rarity of combining social, qualitative data about crimes targeting the DeFi ecosystem alongside technical, quantitative data, within the academic literature to date, it offered empirical novelty, enhanced our findings and demonstrated the potential of bringing these two types of data into dialogue. Given these limitations, the incorporation of social data into this analysis should be considered exploratory. Its primary purpose here is to contextualize our technical on-chain data and to indicate avenues of future research.

Findings

Our analysis confirms the findings of previous research that identified significant financial losses caused by attacks on the DeFi ecosystem. We identified 254 successful attacks on the DeFi ecosystem during our study period. Total losses from these attacks were US\$ 6.568bn. They resulted in an average loss of US\$ 1.459bn per annum. Previously [Zhou *et al.* \(2023: 1\)](#) have reported DeFi attack losses of US\$ 3.24bn between April 2018 and April 2022, giving an average loss of US\$ 0.810bn per annum, while [Carpentier-Desjardins *et al.* \(2025\)](#) reported a DeFi attack loss figure of US\$ 10bn between 2017 and 2022, giving an annual DeFi attack loss of US\$ 2bn. Our findings sit between those of these two previous studies. The differences between these findings reflect the inherent difficulties of identifying attacks on and quantifying losses in the DeFi ecosystem, as well as differences in calculation methods and sources of data. While our findings, in the context of these earlier studies, are unable to point categorically to a rising or falling profile of DeFi attack losses, they do confirm that attacks on the DeFi ecosystem continue to pose a major financial threat.

Our analysis has also confirmed the findings of previous research that FLAs can cause considerable financial losses to the DeFi ecosystem ([Cao *et al.*, 2021](#); [Gan *et al.*, 2023](#); [Xu and Feng, 2022](#)). Of the attacks that we identified, 72 were FLAs that resulted in total losses of US\$ 1.211bn. FLAs represented 28.35% of all detected DeFi attacks and 18.44% of all DeFi attack losses. The average loss per FLA was US\$ 16.83m, while average losses from other forms of DeFi attack were US\$ 29.43m. FLA losses ranged from US\$ 0.08 to US\$ 197m. While over 65% of FLAs ($n=47$) resulted in losses of under US\$ 10m, FLAs that resulted in losses of US\$ 10m or more ($n=25$) accounted for over 88% of all FLA losses ([Table 1](#)). The potential for such high levels of loss variance is reflective of the vast sums circulating within the DeFi ecosystem and the range of platform vulnerabilities. Both are significant motivations for criminals and major challenges for affected platforms.

Within our population, EUPL attacks were less frequent than MPF attacks but resulted in higher average losses. Of the FLAs we identified, 42 were MPF attacks and 30 were EUPL attacks. US\$ 695.05m (57.37%) was lost to MPF attacks, with an average loss of US\$ 16.55m, and US\$ 516.45m (42.63%) to EUPL attacks, with an average loss of US\$ 17.22m. EUPL attacks are seen as more technically sophisticated than MPF attacks. A pool shares (EUPL) exploit on Spartan Protocol, for example, involved more than 500 separate transactions. Further, our interviewee spoke of the skill levels the perpetrator required to successfully execute an EUPL attack on their platform:

I would say in particular of the analysis and discovering the exploit, he must certainly, must have had some very very good skills, right. This bug passed, you know, ourselves and several of the auditors, all of the auditors looked at it, some of them very well regarded, and of course, you know, it was unnoticed on the chain for over a year, right. So yeah, absolutely like it's definitely something and it's real insight in this one instance at least.

Table 1. Categories of FLAs by loss (February 2020–July 2024)

Losses	No.	Total losses (US\$ million)	Percent of total FLA losses
US\$ 100–300m	3	508.00	41.93
US\$ 20–99.99m	13	436.20	36.01
US\$ 10–19.99m	9	126.34	10.43
US\$ 1–9.99m	31	133.06	10.98
Less than US\$ 1m	16	7.91	0.65

Note(s): All data in tables and figures are from SyntiFi ORI (2024), unless otherwise stated

Losses were dominated by four specific FLA types that collectively accounted for 63.89% of all FLAs by number and 81.75% of all FLA losses (Table 2): price oracle attacks (MPF); donate function logic exploits (EUPL); a governance attack (MPF); and reentrancy attacks (EUPL).

FLA types varied considerably in terms of their frequency and average loss per attack. The typology in Table 3 categorises FLAs according to whether their attack frequency is above the median frequency value (2) or equal to or below the median frequency value, and whether their average loss per attack is above or below the median average loss per attack value (US\$ 11.347m).

The most quantitatively significant FLA loss categories (ranks 1 and 2) include three MPF types and four EUPL types. Both vulnerabilities associated with price feeds and underlying protocol logics, then, represent significant FLA vulnerabilities.

FLA activity, measured both in terms of number and average loss, varied considerably over time during our study period (Figure 3), displaying a series of phases of growth and decline.

A diversity of attack types was typical across our study period (Table 4). Each six month period contained at least two FLA types, while most contain between three to six attack types, six being the modal class. Different FLA types demonstrated distinct temporal patterns. Three FLA types (price oracle attacks, reentrancy attacks and, albeit to a lesser extent, pool shares exploits) demonstrated frequent, enduring temporal distributions, occurring across much of our study period. The first price oracle attack, for example, occurred in February 2020 and the last in June 2024 and they were present in all but two six month periods. Six attack types demonstrated either more ephemeral, isolated temporal distributions, occurring as one-off events or in small numbers in close temporal proximity (a governance attack, incentive rewards exploits, a withdraw logic exploit and a burn function exploit), or ephemeral but recurring temporal distributions across more dispersed time periods (swap logic exploits and slippage attacks). Finally, five attack types (donate function logic exploits, misconfiguration exploits, price manipulation attacks, new market exploits and a rounding donation attack) displayed emergent profiles, all appearing only in the last eighteen months of our study period.

The ranks of FLA threats identified in the typology in Table 3 also show some temporal dynamism. Table 4, below, highlights that the dominance of rank 1 attack types is in part residual. While rank 1 FLA types accounted for at least 65.00%, and in two periods over 80%, of all FLA losses between February 2020 and January 2022, they only accounted for the majority of FLA losses in two of the subsequent five six month periods. The significance of rank 1 FLA types remains, but as more sporadic threats than previously. Broadly, the threats posed by different FLA types in Table 5 have been less predictable after February 2022 than was the case previously. Predicting FLA threats, then, became potentially more challenging over our study period.

We analyzed the number of novel FLA types that emerged across our study period. Due to the small number of FLA types we divided our study period into 12 rather than six monthly periods. From this, we tentatively propose that FLA activity displayed the following phases during our study period:

- February 2020–January 2021: Emergence: 3 novel FLA types;
- February 2021–January 2022: Growth/innovation: 5 novel FLA types;
- February 2022–January 2023: Consolidation: 1 novel FLA type;
- February 2023–January 2024: Growth/innovation: 5 novel FLA types; and
- February 2024–July 2024: Consolidation: 0 novel FLA types.

Table 2. Numbers and losses per FLA type

Type of FLA	No. of attacks	Percent total FLAs	Total losses (US\$ million)	Percent of total FLA losses	Average loss per attack (US\$ million)
Price oracle attack (MPF)	25	34.722	403.770	33.314	16.151
Donate function logic exploit (EURL)	5	6.944	228.100	18.820	45.620
Governance attack (MPF)	1	1.389	181.000	14.934	181.000
Reentrancy attack (EURL)	16	22.222	177.990	14.686	11.124
Pool shares exploit (EURL)	5	6.944	68.757	5.673	13.751
Swap logic exploit (MPF)	2	2.778	59.000	4.868	29.500
Incentive rewards exploit (MPF)	5	6.944	24.406	2.014	4.881
Misconfiguration exploit (EURL)	2	2.778	23.139	1.909	11.570
Withdraw logic exploit (EURL)	1	1.389	18.000	1.485	18.000
Price manipulation attack (MPF)	4	5.556	9.100	0.751	2.275
Slippage attack (MPF)	2	2.778	7.85	0.648	3.925
New market exploit (MPF)	2	2.778	4.750	0.392	2.375
Burn function exploit (MPF)	1	1.389	4.500	0.371	4.500
Rounding donation attack (EURL)	1	1.389	0.464	0.038	0.464

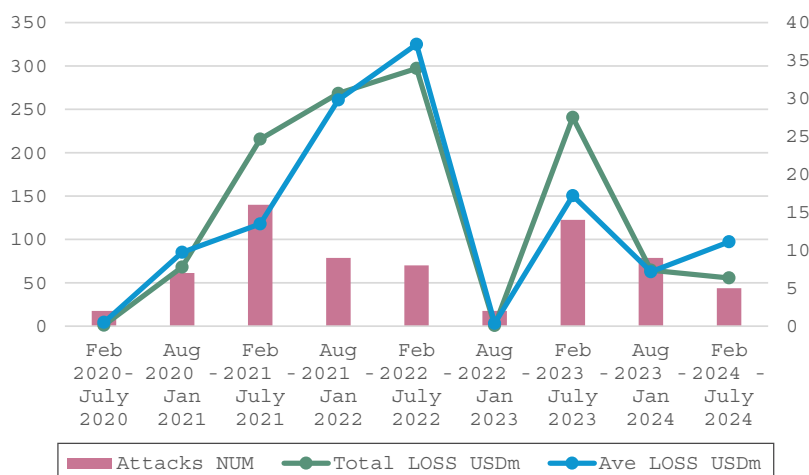


Figure 3. FLA number, total and average loss, February 2020–July 2024

Broadly speaking, FLA activity showed a bimodal temporal distribution across our study period with phases of growth and innovation being followed by periods of consolidation and, in some periods, decline. This pattern suggests that platforms enhanced resilience following FLAs by successfully patching up exploited vulnerabilities and upgrading or modifying their cybersecurity. One example of this is Euler Finance who modularized their protocol following the FLA that successfully targeted them (Euler Labs, 2024b). Following actions such as these, perpetrators were required to innovate, typically through scanning platforms for other vulnerabilities and/or developing novel forms of FLA. This periodic tension between platform security and criminal innovation was outlined by our interviewee following the attack on their platform:

Yeah, I think things have gotten more secure. People have learned lessons and practises have improved, but like I said before is that it's very dynamic, right and that people are always coming up with new things to do on it (the DeFi ecosystem) and sometimes those interact in a weird way with existing products so even something that was secure yesterday, given the new changing conditions, may no longer be secure.

Our analysis also revealed a shift over time in the relative threats of MPF and EUPL attacks. Between February 2020 and January 2022 25 MPF attacks (73.53%) and nine (26.47%) EUPL attacks occurred. By contrast, between February 2022 and July 2024 17 MPF attacks (44.74%) and 21 (55.26%) EUPL attacks occurred. US\$ 396.99m (71.79%) of all FLA losses between February 2020 and January 2022 were due to MPF attacks and US\$ 156.00m (28.21%) to EUPL attacks, whereas between February 2022 and July 2024 USD 298.07m (45.27%) of all FLA losses were due to MPF attacks and US\$ 360.45m (54.74%) to EUPL attacks. EUPL attacks, then, grew as a threat over the course of our study period. This suggests an increasing technical sophistication of FLAs over time and the potential efficacy of cybersecurity responses, such as bug bounties (Sridhar and Ng, 2021), that specifically aim to address these vulnerabilities.

FLAs also caused significant reputational damage to affected platforms (Immunebytes, 2022a) and generated instability in the value of cryptocurrencies. For example, a FLA on the Elephant Money platform in April 2022, which resulted in direct financial losses of US\$

Table 3. FLA Typology based on interactions of attack frequency and average loss

Attack frequency	Average losses above median value	Average losses below median value
Attack frequency above median value	Price oracle attacks (MPF) Donate function logic exploits (EUPL) Pool shares exploits (EUPL) — Total FLA Losses = US\$ 700.64 m Percent FLA Losses = 57.81 Losses Rank = 1 Governance attacks (MPF) Swap logic exploits (MPF) Misconfiguration exploits (EUPL) Withdraw logic exploits (EUPL) — Total FLA Losses = US\$ 281.14 m Percent FLA Losses = 23.20 Losses Rank = 2	Reentrancy attacks (EUPL) Incentive rewards exploits (MPF) Price manipulation attacks (MPF) — Total FLA Losses = US\$ 211.50 m Percent FLA Losses = 17.45 Losses Rank = 3 Slippage attacks (MPF) New market exploits (MPF) Burn function exploits (MPF) Rounding donation attacks (EUPL) — Total FLA Losses = US\$ 17.56 m Percent FLA Losses = 1.45 Losses Rank = 4
Attack frequency on or below median value		

Table 4. FLA type, number and losses February 2020–July 2024

FLA type	Feb 20–Jul 20	Aug 20–Jan 21	Feb 21–Jul 21	Aug 21–Jan 22	Feb 22–Jul 22	Aug 22–Jan 23	Feb 23–Jul 23	Aug 23–Jan 24	Feb 24–Jul 24
Price oracle attack (MPF)	1	5	7	4	3		3		2
Donate function logic exploit (EURL)							3	1	1
Governance attack (MPF)					1				
Reentrancy attack (EURL)		2	1	3	4	1	5		
Pool shares exploit (EURL)			2			1	1	1	
Swap logic exploit (MPF)				1				1	
Incentive rewards exploit (MPF)			4	1					
Misconfiguration exploit (EURL)							1		1
Withdraw logic exploit (EURL)			1						
Price manipulation attack (MPF)							1	4	
Slippage attack (MPF)	1								
New market exploit (MPF)								1	1
Burn function exploit (MPF)			1						
Rounding donation attack (EURL)								1	
Total FLAs in period	2	7	16	9	8	2	14	9	5
Total FLA types in period	2	2	6	4	3	2	6	6	4
Total MPF attacks in period (%)	2 (100)	5 (71)	12 (75)	6 (67)	4 (50)	0 (0)	4 (29)	6 (67)	3 (60)
Total EURL attacks in period (%)	0 (0)	2 (29)	4 (25)	3 (33)	4 (50)	2 (100)	10 (71)	3 (33)	2 (40)
Total loss (US\$m) in period	1.00	68.10	215.585	268.3	297.1	0.74	240.639	64.491	55.55
Average loss (US\$m) in period	0.500	9.729	13.474	29.811	37.138	0.37	17.189	7.166	11.10

Table 5. FLA Rank types, temporal analysis

FLA ranks and losses	Feb 20–Jul 20	Aug 20–Jan 21	Feb 21–Jul 21	Aug 21–Jan 22	Feb 22–Jul 22	Aug 22–Jan 23	Feb 23–Jul 23	Aug 23–Jan 24	Feb 24–Jul 24
Rank 1 FLAs	1	5	9	4	3	1	7	2	3
Rank 1 FLAs	0.65	58.10	180.80	184.5	22.70	0.08	207.67	2.43	43.70
Loss (US\$m)									
Percent of all	65.00	85.32	83.86	68.77	7.64	10.81	86.30	3.77	78.67
FLA losses in Period = Cat 1									
Rank 2 FLAs	0	0	1	1	1	0	1	1	1
Rank 2 FLAs	0	0	18.00	11.00	181.00	0	11.54	48.00	11.60
Loss (US\$m)									
Percent of all	0	0	8.35	4.10	60.92	0	4.80	74.43	20.88
FLA losses in Period = Cat 2									
Rank 3 FLAs	0	2	5	4	4	1	5	4	0
Rank 3 FLAs	0	10.00	12.29	72.80	93.40	0.66	13.93	9.10	0
Loss (US\$m)									
Percent of all	0	14.68	5.70	27.13	31.44	89.19	5.79	14.11	0
FLA losses in Period = Cat 3									
Rank 4 FLAs	1	0	1	0	0	0	1	2	1
Rank 4 FLAs	0.35	0	4.50	0	0	0	7.50	4.96	0.25
Loss (US\$m)									
Percent of all	35.00	0	2.09	0	0	0	3.12	7.69	0.45
FLA losses in Period = Cat 4									
Total FLA losses (US\$m) in period	1.00	68.10	215.585	268.3	297.1	0.74	240.639	64.491	55.55

22.2m, also caused their \$ELEPHANT tokens to lose 75% of their value, while their TRUNK stablecoins lost 40% of their value (Immunebytes, 2022b, 2022c). In addition to financial losses and instability, FLAs may also generate damaging social tensions within platform teams as outlined by our interviewee:

I've seen this happen to like many other teams. Watching teams right, like sadly too many, and most often it ends up fracturing them and destroying them, even if they do [...] recover funds, it's usually not the same, right, and it's difficult to restore trust and especially even inside the team there [...] is a lot of tension and sometimes it boils over publicly.

Losses to FLAs as a percentage of all flash loan activity remained small throughout our study period. In only one six month period (February 2022 to July 2022) did FLA losses exceed 0.5% of flash loan value borrowed. This is accounted for by the coincidence of a sharp fall in the flash loan value borrowed and the end of the initial growth phase of FLAs where total and average FLA losses were at the highest recorded during our study period. Despite the significance of FLA losses they did not negatively impact the growth of flash loan activity during our study period and have not posed an existential threat to flash loan activity, which continued to grow rapidly. [Table 6](#)

Our analysis of the relationships between FLA activity and wider DeFi market conditions produced two statistically significant results. First was a weak positive linear relationship between the number of FLAs per month and TVL/month from April 2018. Here approximately 4.7% of the variance in the FLAs per month was explained by market size (TVL). Second was a moderate positive relationship between the FLA volume/month and TVL/month from April 2018. Here approximately 9.8% of the variance in FLA volume per month was explained by market size (TVL). None of the remaining regression analyses produced statistically significant results. Thus, we found some weak/moderate relationships between TVL and FLA activity where TVL data is taken from April 2018, but no significant relationships between FLA activity and TVL when TVL is taken from January 2020, or with flash loan number and volume. The full TVL data set includes a period between April 2018 and January 2020 when flash loans were technically available but were not sufficiently established to be exploited. TVL, then, predicts variation in FLA activity less successfully after January 2020. Including the pre-FLA period (months with zero FLAs) helps the regression capture a rising trend between market size and the emergence of FLAs by providing more signal or smoothing out volatility. Our results suggest FLAs show only very limited market sensitivity.

FLAs declined in significance within the wider DeFi attack landscape across our study period ([Table 7](#)). Between February 2020 and July 2021, FLAs accounted for 47.17% of all DeFi attacks by number and 41.10% of all detected DeFi attack losses. However, after this they represented less than 30% of all DeFi attacks by number in all six month periods, within a broadly declining profile, and only accounted for more than 20% of DeFi attack losses in one six month period (February 2023–July 2023), during which the Euler Finance attack, the single biggest FLA by loss, occurred. The exceptional scale of this attack distorted somewhat the impact of FLAs within the context of all significant DeFi attacks during this period. In the last two years of our study FLAs generally accounted for lower proportions of DeFi attack numbers and particularly DeFi attack losses than previously. Between August 2023 and July 2024, for example, FLAs accounted for 17.28% of all DeFi attacks by number and 7.1% of all DeFi attack losses.

In sum, then, following this analysis of FLA activity between February 2020 and July 2024 and their contextualization within wider DeFi market conditions and attack activity, we characterize FLAs as significant, dynamic, innovative, increasingly sophisticated,

Table 6. FLA losses as percentage of flash loan value borrowed, February 2020–July 2024

Period	Flash loan value borrowed (US\$m)	No. of flash loans	FLA losses (US\$m)	Loss as percent of flash loan value borrowed
Feb 2020–July 2020	1 884.950	9 199	1.000	0.050
Aug 2020–Jan 2021	41 057.790	72 848	68.100	0.170
Feb 2021–July 2021	262 922.140	159 163	215.590	0.080
Aug 2021–Jan 2022	114 898.220	179 558	268.300	0.230
Feb 2022–July 2022	45 028.000	347 766	297.100	0.660
Aug 2022–Jan 2023	85 760.190	1 762 469	0.74	0.001
Feb 2023–July 2023	175 717.750	2 029 663	240.640	0.140
Aug 2023–Jan 2024	401 470.850	1 338 186	64.490	0.01
Feb 2024–July 2024	2 199 342.880	3 891 154	55.550	0.002
Total	3 328 082.72	9 790 006	1 211.51	0.036

Table 7. FLAs as the percentage of all DeFi hacks, February 2020–September 2024

FLA and DeFi hacks, numbers and losses	Feb 20–Jul 20	Aug 20–Jul 21	Feb 21–Jul 21	Aug 21–Jul 22	Feb 22–Jul 22	Aug 22–Jul 23	Feb 23–Jul 23	Aug 23–Jul 24	Feb 24–Jul 24
Total FLAs	2	7	16	9	8	2	14	9	5
Total FLAs loss (US\$m)	1.00	68.1	215,585	268.3	297.1	0.74	240,639	64,491	55.55
Total all DeFi hacks	5	11	37	33	27	10	50	47	34
Total all DeFi hacks loss (US\$m)	29,550	154,200	508,913	1913,790	1523,310	209,406	538,417	776,895	913,944
% Total all DeFi hacks = FLAs	40.00	63.64	43.24	27.27	29.63	20.00	28.00	19.15	14.71
% Total all DeFi hacks loss = FLAs	3.38	44.16	42.36	14.02	19.50	0.35	44.69	8.30	6.08

unpredictable and potentially market sensitive, but not existential, threats to the DeFi ecosystem.

FLA victimization was highly concentrated by blockchain (Table 8). The overwhelming majority of FLAs and FLA losses occurred on the Ethereum blockchain. These both proportionately exceeded the number and value of flash loans on this blockchain, especially so in the case of the number of flash loans. Only one other blockchain (BNB Chain) accounted for more than 3% of FLAs by number and 4% of FLAs by value. Both Ethereum and BNB Chain were over-victimised by FLAs. All five remaining blockchains suffered proportionately less FLA victimization by number than the proportionate number of flash loans transacted on these chains. Three of these five (Base, Optimism and Arbitrum) suffered proportionately less FLA victimization by value than the proportionate value of flash loan transactions on these chains, whilst Avalanche and Polygon suffered proportionately slightly more FLAs by value than the proportionate value of the flash loan transactions on these blockchains.

The two over-victimised blockchains were the first two to introduce flash loans. It would appear FLAs were initially innovated and practiced largely on these two blockchains. There have been journalistic observations, for example, that suggest extensive illicit activities occurred on BNB Chain in the early years of its existence (Berwick and Wilson, 2022). Base was the only blockchain to suffer no recorded FLAs. Base is a newer blockchain which was launched in August 2023 and was developed by Coinbase, a regulated US cryptocurrency exchange. Patterns of blockchain victimization, then, seem to reflect patterns of flash loan innovation and avoidance of regulation.

The DeFi ecosystem is both pseudonymous and public. While perpetrators of DeFi attacks assume pseudonymous identities, every detail of their crimes is permanently and publicly recorded on blockchains. While this record is immensely valuable, it tells us nothing about the identities of perpetrators of FLAs. The social media identities of perpetrators do sometimes emerge through interactions on these channels following successful DeFi attacks. Our interviewee indicated that the perpetrator who targeted their platform: “had started like, I guess you could say, taunting us or negotiating, I guess, in public”. In some cases specific social media accounts are able to be linked to specific DeFi attacks through discussions of wallet addresses associated with these attacks. This occurred in a number of the FLAs included in our sample of 35 publicly discussed FLAs. Here it was common for platforms to publicly appeal to the perpetrator for the partial or full return of stolen funds (Rekt, 2020; Haqshanas, 2023). Such dialogues tended to be carefully scripted and included acknowledgements of hackers’ skills and explicit statements that perpetrators’ identities would not be released (doxing). These public communications, typically through social media channels such as X, Discord and Telegram or through blockchains, sometimes also

Table 8. FLA victimization by blockchain

Blockchain	% Num flash loans	% Num FLAs	% Value flash loans	% FLA losses
Ethereum	7.63	63.89	60.26	80.56
Base	10.03	0.00	34.21	0.00
Optimism	24.63	2.78	3.22	2.23
Arbitrum	18.51	6.94	1.57	1.48
BNB chain	1.42	20.83	0.36	12.01
Avalanche	4.08	2.78	0.20	3.51
Polygon	33.97	2.78	0.18	0.22

sought to enrol other members of the cryptocurrency community. It was through such post-event communications that requests for the return of funds and financial incentives to the perpetrator, or others with information about the attack, were made (Haqshanas, 2023). The X (then Twitter) outputs from Harvest Finance following a successful FLA in October 2020 exemplified such perpetrator- and community-centred responses:

Harvest Finance @harvest_finance · 7h.

In addition to the BTC addresses which hold the funds, there is now a significant amount of personally identifiable information on the attacker, who is well-known in the crypto community.

We are putting out a 100k bounty for the first person or team to reach out to the attacker.

[...].

Harvest Finance @harvest_finance · 7h.

and help the attacker return the funds to the deployer address.

[...].

Harvest Finance @harvest_finance · 7h.

We are not interested in doxxing the attacker, your skill and ingenuity is respected, just return the funds to the users" (in Rekt, 2020).

Our interviewee became aware of the identity of the perpetrator who successfully exploited their platform following his arrest by law enforcement and provided some insights into this specific perpetrator and also into their perceptions of the wider landscape of perpetrators who target the DeFi ecosystem. They characterized this as being split between 'hobbyist individual researchers' and 'professionals'. They described the former as primarily motivated by curiosity, a desire for notoriety or to demonstrate their skills, rather than purely financial rewards. Indeed, in the case of our interviewee's platform, the perpetrator returned all of the stolen assets:

Yes, we did end up recovering the funds. The attacker voluntarily sent them back to us, you know, for a variety of reasons, one of which was obviously he was afraid of being revealed and arrested and so on, and also he did, at some level, seem to have some remorse about the fact that some people could have lost a lot of money, like important money for them [...] He actually did some back and forth [with] the community and he did what one person kind of backed him like [into]. [Victim saying to the attacker] 'Can you please give it back to me and for such reasons I need it'. And he did actually refund that user, right, so it was a very like positive side for us that that we're not dealing with North Korea.

This reference to North Korea, is an allusion to DeFi attackers that our interviewee referred to as professionals. Here the main motivation for attacks is financial. These perpetrators, he indicated, tended to launch less technically sophisticated attacks and also acted in very different ways to hobbyist researchers following a successful attack:

Yeah, one interesting thing is that when the hack was happening he did some behaviour that would be very unusual if this was a conventional attacker [...] like, for example North Korea, and these like professional actors [...] typically when they hack, the silence is just gone and you'll never hear from them again right [...] Yeah for sure I have a good categorisation. It's like the professionals state level or organized crime versus the sort of like, I guess you could say, more individual or like research focused. On the professional ones like North Korea typically their attacks are not at all advanced, right, like from the perspective of blockchain security, right. Actually, they do not have, you know, quite sophisticated conventional attacking methods [...]

Typically they're not doing the kind of research that would be required to perform smart contract exploits right, yeah, so most the time the really advanced exploits I would say they are kind of this kind are like the hobbyist individual researchers.

Currently, insights into the perpetrators of attacks on the DeFi ecosystem generally and FLAs specifically remain very scant. Perpetrator focused analysis and the identification of perpetrators of DeFi attacks remains a priority for future research.

Discussion

This paper provides the first extensive, contextual analysis of FLAs which combines technical and social data and is informed by criminological, rather than purely cybersecurity, methods and theory. The potentials for flash loans to be used to access finance that can be used for criminal activities has been previously acknowledged ([Aramonte et al., 2021](#); [Carpentier-Desjardins et al., 2025](#); [Gudgeon et al., 2020](#); [Oosthoek, 2021](#); [Qin et al., 2021](#); [Zhou et al., 2023](#)) and has been confirmed by our analysis. In addition, cryptocurrencies have become associated with extensive, innovative forms of financial crime ([Trozze et al., 2022](#)). This combination might suggest flash loans represent an untrammelled opportunity for criminality. However, our analysis of FLAs tells a somewhat different story. While it is one of FLA growth and innovation, it is also one of consolidation and absolute and relative decline at times, of the avoidance of regulation, of different perpetrator motivations and profiles and victimization patterns, and of evolving resilience and counter initiatives within the DeFi ecosystem. This analysis of FLAs, then, suggests a more nuanced story of this emergent form of criminality and highlights the need for further criminological scrutiny of cryptocurrency crime and the DeFi ecosystem.

In addition to the empirical contributions discussed in the previous section, the paper makes a number of theoretical and applied contributions. Previous studies, as we have noted earlier, have highlighted continuities between cryptocurrency crimes and pre-digital forms of criminality ([Kamps and Kleinberg, 2018](#); [Mackenzie, 2022](#)). This has informed their deployment of criminological theories such as RAT and convenience theory in their interpretation of these crimes. We, however, see few equivalent continuities between FLAs and earlier forms of offline crime. Rather, our analysis emphasizes the novelty, technical sophistication and challenges of FLAs. This suggests practices reflective of “patience and investment” ([Weulen Kranenbarg, 2020](#): 197), skill development and innovation by perpetrators, confirming [Weulen Kranenbarg's \(2020\)](#) reservations about the transferability of criminological theories such as RAT and convenience theory to the interpretation of cybercrimes of great technical sophistication and perhaps point to the potential of technosocial theories to inform criminological enquiry into crimes targeting the DeFi ecosystem.

Following this, we see the flaws within price feed mechanisms and underlying protocol logics that are exploited within FLAs not as mere technical ‘glitches’ that can be exploited and which need patching, but rather as socially produced. By this we mean that they emerge, like all cryptocurrency technological configurations, out of a series of social contexts. These include the cultures and social practices of hardware engineering, software coding, cybersecurity, cryptocurrency investment and speculation, DeFi industry working practices and community cultures, and regulatory contexts. Equally, we see the exploitation of these vulnerabilities through FLAs as socially produced and similarly emerging out of multiple contexts. These include contexts, which might be on- and/or offline, where knowledge of potential DeFi vulnerabilities and the hacking skills to exploit them are acquired, developed and shared, contexts within which these skills and their execution are legitimized and celebrated ([Foxley, 2020](#)) and wider contexts out of which the motivations for these criminal activities emerge. Further, we view aspects that had previously been seen as purely technical

as having agency within the technosocial networks of FLAs, as with the nature of specific vulnerabilities which profoundly shapes the nature of different types of attack and their characteristics, such as their frequency and the losses they generate, which, as we note above, vary wildly. They, in turn, are active in shaping the various chains of social and technical responses following successful FLAs.

For example, while reiterating that we cannot claim representativeness or data saturation from our single interview with a victimized platform, it does suggest the emergence of promising technosocial stories with potential cybersecurity applications. Our interviewee, for example, spoke of the social fracturing that they had observed in platform teams following large successful DeFi attacks. This is not something that has been noted in the previous FLA research and is not something that is captured in any technical empirics related to these attacks. Rather, technosocial stories like this emerge through engagement with the social networks of the DeFi ecosystem. This points to cybersecurity being thought of as more than a technical practice, one that draws upon both the technical and social resources of the DeFi ecosystem. The fracturing of platform teams following an attack is likely to compromise or weaken cybersecurity responses. Anticipating and preventing this social fracturing, within the context of cybersecurity, is likely to enhance the resilience of the DeFi ecosystem. This suggests that the technosocial perspective that we have begun to explore here has potential application in both the interpretation of and response to crimes targeting the DeFi ecosystem such as FLAs. However, noting such observations is only the first step in developing a technosocial, criminological perspective on crimes targeting the DeFi ecosystem. Much remains to be done to more fully engage with the social dimensions of the DeFi ecosystem and the crimes that target it and to successfully marry this analysis with the technical analysis typical of cybersecurity and its cognate disciplines.

The analysis within this paper has a number of potential applications. For example, it offers the DeFi community, cybersecurity firms, law enforcement agencies, regulators and policymakers a novel framework for understanding and responding to FLAs. Beyond technical descriptions, this analysis situates FLAs within broader patterns of offender behaviour, opportunity structures and system vulnerabilities – providing a richer, context-aware perspective often absent in purely technological assessments. The exploration of both victims and perpetrators facilitates more nuanced approaches to platform liability, enforcement prioritization and consumer protection. By highlighting the technosocial dynamics of DeFi-based crime, this research equips regulators with an evidence-based foundation to craft adaptive, forward-looking policies that address not only the symptoms but also the structural conditions enabling this new form of cybercrime.

For the DeFi community and cryptocurrency project developers, the identification of 14 distinct types of FLAs and their temporal patterns presents a foundation for building more secure protocols and improving smart contract design. Our findings allow developers to rethink system design not only in terms of technical robustness but also in terms of crime opportunity structures, leading to more criminologically informed risk management practices, targeted audits and the implementation of environmental and procedural safeguards that reduce the likelihood of exploitation. Cybersecurity firms benefit from the empirical mapping of attack behaviours, which supports the use and development of on-chain threat detection tools (such as SyntiFi ORI), incident response systems and risk profiling services. The insights into attacker strategies and the dynamics of exploit execution contribute to more effective monitoring and early-warning frameworks tailored to DeFi environments.

For law enforcement agencies, the empirical tracking of FLA incidents, methods and financial impact offers a foundation for forensic investigation, crime attribution and inter-

jurisdictional cooperation. The differentiation between types of attacks also supports clearer categorization within legal and enforcement frameworks, helping authorities understand the complexities of these novel digital crimes. From a regulatory and policy-making perspective, the application of a criminological lens represents a significant contribution to the understanding of cybercrime in DeFi systems. This research goes beyond technical analysis by examining offender behaviour, systemic vulnerabilities and the technosocial conditions that enable exploitation. Such contextualization allows for the development of informed, proportionate regulatory responses. The findings offer guidance for setting smart contract standards, improving DeFi platform accountability and shaping cross-chain oversight mechanisms. In sum, this paper bridges a critical gap between technology, criminology and practice. It equips developers, regulators, law enforcement and cybersecurity professionals with the conceptual and empirical tools necessary to better prevent, investigate and respond to FLAs, while contributing to a more secure and accountable DeFi ecosystem.

Cryptocurrencies and the DeFi ecosystem have shown remarkable growth in recent years. There is little sign of this growth stalling. However, they currently face three major challenges: becoming more environmentally sustainable, more secure and reducing criminal activity in the DeFi ecosystem. The findings and applications of this paper contribute to the second and third of these challenges. Inevitably, however, given the novelty of this analysis, there remain many avenues of further criminological research into FLAs and DeFi attacks of all types. For example, due to constraints of space, this paper has said little about the range of responses to FLAs from affected platforms, cybersecurity companies, the DeFi community, law enforcement agencies and perpetrators of FLAs, nor about the money laundering practices that follow successful FLAs. Also, it remains a priority for researchers to engage more fully and directly with the various social actants enrolled within the networks of the DeFi ecosystem and the crimes that target it, including the perpetrators of these crimes, notwithstanding the challenges associated with this, and in doing so to develop more fully rounded technosocial analyses of these crimes.

Finally, the analysis within this paper was made possible by an innovative partnership between a criminologist and a cryptocurrency risk intelligence company, exemplifying a unique collaboration between academia and the private sector, that was able to combine a contextual criminological perspective with technically sophisticated on-chain data analysis. We believe this model of co-production has the potential to be replicated elsewhere and, in being so, to advance significantly our understanding of and responses to crimes targeting the DeFi ecosystem.

Acknowledgements

The authors would like to thank Gina Kallis for her excellent work as a research assistant on this project and their interviewee from a victimized platform for their valuable insights. The authors would also like to thank Ian Mills for arranging the contact between the two authors.

Notes

- [1.] Bugs in the code are errors, flaws or unintended mistakes in software that cause the program to behave differently from what its developers intended.
- [2.] Price feeds are automated, real time feeds of market data that applications on the DeFi ecosystem use to execute smart contracts accurately.
- [3.] TVL represents the combined value of all funds locked in smart contracts for various use cases such as lending, staking, liquidity pools and yield farming. The majority of FLAs occurred

within these applications. TVL provides a potentially appropriate measure of any relationship between FLAs and wider market conditions as it reflects the volume of outside money entering the DeFi ecosystem. Whilst this is in part a reflection of the degree of external trust placed in the system, it also reflects potential opportunities for attackers. Larger TVL suggests more platforms and protocols are being built within the DeFi ecosystem, which represent more potential education, skills development and attack opportunities. Growth in TVL also, potentially, increases the financial rewards for attackers. Flash loans were first introduced in April 2018 but were only made available on the Ethereum network in January 2020. This gave us two potential sets of TVL data: a full set from April 2018 with data for 86 months and a smaller set that captured the introduction of flash loans on Ethereum, which gave us TVL data for 65 months. We ran a series of regression analyses exploring the relationships between FLA number and volume and both of these TVL samples, as well as with flash loan number and volume.

References

- Aldridge, J. and Askew, R. (2017), "Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement", *International Journal of Drug Policy*, Vol. 41, pp. 101-109, doi: [10.1016/j.drugpo.2016.10.010](https://doi.org/10.1016/j.drugpo.2016.10.010).
- Aramonte, S., Huang, W. and Schrimpf, A. (2021), "DeFi risks and the decentralisation illusion", *BIS Quarterly Review*, pp. 21-36.
- Berwick, A. and Wilson, T. (2022), "How crypto giant Binance became a hub for hackers, fraudsters and drug traffickers", Reuters, available at: www.reuters.com/investigates/special-report/fintech-crypto-binance-dirty-money/ (accessed 10 April 2025).
- Brown, S. (2006), "The criminology of hybrids: rethinking crime and law in technosocial networks", *Theoretical Criminology*, Vol. 10 No. 2, pp. 223-244, doi: [10.1177/1362480606063140](https://doi.org/10.1177/1362480606063140).
- Campbell-Verduyn, M. (2018), "Bitcoin, crypto-coins, and global anti-money laundering governance", *Crime, Law and Social Change*, Vol. 69 No. 2, pp. 283-305, doi: [10.1007/s10611-017-9756-5](https://doi.org/10.1007/s10611-017-9756-5).
- Cao, Y., Zou, C. and Cheng, X. (2021), "Flashot: a snapshot of flash loan attack on the DeFi ecosystem", arXiv:2102.00626, doi: [10.48550/arXiv.2102.00626](https://doi.org/10.48550/arXiv.2102.00626).
- Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S. and Haslhofer, B. (2025), "Mapping the DeFi crime landscape: an evidence-based picture", *Journal of Cybersecurity*, Vol. 11 No. 1, doi: [10.1093/cybsec/tyae029](https://doi.org/10.1093/cybsec/tyae029).
- Chen, Z., Mohamed Beillahi, S. and Long, F. (2024), "FlashSyn: flash loan attack synthesis via counter example driven approximation", *ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, doi: [10.1145/3597503.3639190](https://doi.org/10.1145/3597503.3639190).
- Childs, A. (2023), "How cryptomarket communities navigate marketplace structures, risk perceptions and ideologies amid evolving cryptocurrency practices", *Criminology and Criminal Justice*, Vol. 25 No. 5, doi: [10.1177/17488958231213012](https://doi.org/10.1177/17488958231213012).
- Coinbase (2024), "What is a flash loan?", Coinbase, available at: www.coinbase.com/en-gb/learn/advanced-trading/what-is-a-flash-loan (accessed 20 November 2024).
- CoinGecko (2025), "Global cryptocurrency market cap charts", CoinGecko, Crypto Market Cap Charts CoinGecko (accessed 18 September 2025).
- Dearden, T.E. and Tucker, S.E. (2023), "Follow the money: analyzing Darknet activity using cryptocurrency and Bitcoin blockchain", *Journal of Contemporary Criminal Justice*, Vol. 39 No. 2, pp. 257-275, doi: [10.1177/10439862231157521](https://doi.org/10.1177/10439862231157521).
- Deng, X., Zhao, Z., Mohamed Beillahi, S., Du, H., Minwalla, C., Nelaturu, K., Veneris, A. and Long, F. (2023), "A robust front-running methodology for malicious flash-loan DeFi attacks", *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, doi: [10.1109/DAPPS57946.2023.00015](https://doi.org/10.1109/DAPPS57946.2023.00015).

- Desmond, D.B., Lacey, D. and Salmon, P. (2019), "Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review", *Journal of Money Laundering Control*, Vol. 22 No. 3, pp. 480-497, doi: [10.1108/JMLC-10-2018-0063](https://doi.org/10.1108/JMLC-10-2018-0063).
- Euler Labs (2024b), "Securing Euler", Euler Blog, 12 August, Securing Euler – Euler Finance (accessed 18 March 2025).
- Foxley, W. (2020), "Harvest finance: \$24M attack triggers \$570M 'bank run' in latest DeFi exploit", *CoinDesk.com*, 26 October, Harvest Finance: \$24M Attack Triggers \$570M 'Bank Run' in Latest DeFi Exploit – CoinDesk (accessed 9 July 2024).
- Gan, R., Wang, L., Ruan, X. and Lin, X. (2023), "Understanding flash loan-based wash trading", *AFT '22: Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pp. 74-88, doi: [10.1145/3558535.3559793](https://doi.org/10.1145/3558535.3559793).
- Gudgeon, L., Perez, D., Harz, D., Livshits, B. and Gervais, A. (2020), "The decentralized financial crisis", *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Rotkreuz, Switzerland, pp. 1-15, doi: [10.1109/CVCBT50464.2020.00005](https://doi.org/10.1109/CVCBT50464.2020.00005).
- Habila Garba, K., Lazarus, S. and Button, M. (2024), "An assessment of convicted cryptocurrency fraudsters", *Current Issues in Criminal Justice*, Vol. 38 No. 1, doi: [10.1080/10345329.2024.2403294](https://doi.org/10.1080/10345329.2024.2403294).
- Haqshanas, R. (2023), "Platypus DeFi platform hit by \$8.5 M flash loan attack with unexpected twist – here's what happened", *Cryptonews*, 23 October, Platypus DeFi Platform Hit by \$8.5M Flash Loan Attack with Unexpected Twist – Here's What Happened (cryptonews.com), (accessed 3 July 2024).
- Holt, T.J., Lee, J.R. and Griffith, E. (2023), "An assessment of cryptomixing services in online illicit markets", *Journal of Contemporary Criminal Justice*, Vol. 39 No. 2, pp. 222-238, doi: [10.1177/10439862231158004](https://doi.org/10.1177/10439862231158004).
- Immunebytes (2022a), "Top 10 flash loan attacks", Immunebytes, 29 December, Top 10 Flash Loan Attacks - ImmuneBytes (accessed 4 July 2024).
- Immunebytes (2022b), "Elephant money hack – April 12, 2022 – detailed analysis", Immunebytes.com, 11 April, Elephant Money Hack–April 12, 2022–Detailed Analysis – ImmuneBytes (accessed 4 July 2024).
- Immunebytes (2022c), "Top 10 flash loan attacks", Immunebytes.com, 29 December, Top 10 Flash Loan Attacks - ImmuneBytes (accessed 9 July 2024).
- Kamps, J. and Kleinberg, B. (2018), "To the moon: defining and detecting cryptocurrency pump-and-dumps", *Crime Science*, Vol. 7 No. 1, pp. 1-18, doi: [10.1186/s40163-018-0093-5](https://doi.org/10.1186/s40163-018-0093-5).
- Mackenzie, S. (2022), "Criminology towards the metaverse: cryptocurrency scams, grey economy and the technosocial", *The British Journal of Criminology*, Vol. 62 No. 6, pp. 1537-1552, doi: [10.1093/bjc/azab118](https://doi.org/10.1093/bjc/azab118).
- Maimon, D. and Louderback, E.R. (2019), "Cyber-dependent crimes: an interdisciplinary review", *Annual Review of Criminology*, Vol. 2 No. 1, pp. 191-216, doi: [10.1146/annurev-criminol-032317-092057](https://doi.org/10.1146/annurev-criminol-032317-092057).
- Masud, F. (2025), "Cryptocurrency theft of £1.1bn could be biggest ever", *BBC News*, Cryptocurrency theft of £1.1bn could be biggest ever, says Bybit - BBC News (accessed 18 September 2025).
- Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M. and Ferrara, E. (2020), "Charting the landscape of online cryptocurrency manipulation", *IEEE Access*, Vol. 8, doi: [10.1109/ACCESS.2020.3003370](https://doi.org/10.1109/ACCESS.2020.3003370).
- Oosthoek, K. (2021), "Flash crash for cash: cyber threats in decentralized finance", *arXiv:2106.10740*, doi: [10.48550/arXiv.2106.10740](https://doi.org/10.48550/arXiv.2106.10740).
- Qin, K., Zhou, L., Livshits, B. and Gervais, A. (2021), "Attacking the DeFi ecosystem with flash loans for fun and profit", *International Conference on Financial Cryptography and Data Security*, *arXiv:2003.03810*.
- Rekt (2020), "Harvest Finance - Rekt", *Rekt.news*, 26 October Rekt - Harvest Finance - REKT (accessed 9 July 2024).

- Sridhar, K. and Ng, M. (2021), "Hacking for good: leveraging HackerOne data to develop and economic model of bug bounties", *Journal of Cybersecurity*, Vol. 7 No. 1, pp. 1-9, doi: [10.1093/cybsec/tyab007](https://doi.org/10.1093/cybsec/tyab007).
- Trozze, A., Kamps, J., Arda Akartuna, E., Hetzel, F.J., Kleinberg, B., Davies, T. and Johnson, S.D. (2022), "Cryptocurrencies and future financial crime", *Crime Science*, Vol. 11 No. 1, pp. 1-35, doi: [10.1186/s40163-021-00163-8](https://doi.org/10.1186/s40163-021-00163-8).
- Wang, S.H., Wu, C.C., Liang, Y.C., Hsieh, L.H. and Hsiao, H.C. (2021), "ProMutator: detecting vulnerable price oracles in DeFi by mutated transactions", *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, doi: [10.1109/EuroSPW54576.2021.00047](https://doi.org/10.1109/EuroSPW54576.2021.00047).
- Wang, B., Yuan, X., Duan, L., Ma, H., Wang, B., Su, C. and Wang, W. (2022), "DeFiScanner: spotting DeFi attacks exploiting logic vulnerabilities on blockchain", *IEEE Transactions on Computational Social Systems*, Vol. 11 No. 2, pp. 1577-1588, doi: [10.1109/TCSS.2022.3228122](https://doi.org/10.1109/TCSS.2022.3228122).
- Weulen Kranenbarg, M. (2020), "Contrasting cyber-dependent and traditional offenders: a comparison on criminological explanations and potential prevention methods", in Leukfeldt, R. and Holt, T. J., (Eds), *The Human Factor of Cybercrime*, Abingdon, Routledge, pp. 194-215.
- Xu, J. and Feng, Y. (2022), "Reap the harvest on blockchain: a survey of yield farming protocols", *IEEE Transactions on Network and Service Management*, Vol. 20 No. 1, pp. 858-869, doi: [10.1109/TNSM.2022.3222815](https://doi.org/10.1109/TNSM.2022.3222815).
- Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D. and Gervias, A. (2023), "SoK: Decentralized finance (DeFi) attacks", *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, pp. 2444-2461, doi: [10.1109/SP46215.2023.10179435](https://doi.org/10.1109/SP46215.2023.10179435).

Further reading

- Behnke, R. (2021), "Explained: the spartan protocol hack", Halborn, available at: www.halborn.com/blog/post/explained-the-spartan-protocol-hack-may-2021 (accessed 19 November 2024).
- Certik (2023), "Zunami protocol incidence analysis", Certik, 16 August, CertiK - Zunami Protocol Incident Analysis (accessed 13 November 2024).
- Coinbase Ventures (2026), "Around the block #3: analysis on the bZx attack, DeFi vulnerabilities and the state of debit cards in crypto", Coinbase Ventures, Around the Block #3: Analysis on the bZx attack, DeFi vulnerabilities and the state of debit cards in crypto Coinbase (accessed 3 July 2024).
- Euler Labs (2024a), "War and peace: behind the scenes of euler's \$240M exploit recovery", Euler Blog, 10 January, War and Peace: Behind the Scenes of Euler's \$240M Exploit Recovery - Euler Finance (accessed 15 March 2025).
- Nnamaka, N. (2024), "Learning from the biggest DeFi hacks of 2024", Medium, 6 February, Learning From The Biggest DeFi Hacks of January 2024 by Natachi Nnamaka | Web3 Writers Guild | Medium, (accessed 3 July 2024).
- Pirus, B. (2020), "Cheese bank's multi-million-dollar hack explained by security firm", cointelegraph.com, 16 November, Cheese Bank's multi-million-dollar hack explained by security firm (cointelegraph.com) (accessed 3 July 2024).
- Reynolds, K. (2021), "Belt finance victim of flash loan attack in latest exploit of a BSC DeFi protocol", Coindesk, 30 May, Belt Finance Victim of Flash Loan Attack in Latest Exploit of a BSC DeFi Protocol - CoinDesk (accessed 4 July 2024).

Corresponding author

Tim Hall can be contacted at: tim.hall@winchester.ac.uk

Table A1. Results of regression analysis between market activity and FLAs

Model	Dependent variable	Predictor	Sample	n	β (predictor)	t	p	R ²	Adj. R ²	F	Result
1	Number of hacks/month	TVL/month	Apr 2018–	86	6.10×10^{112}	2.03	0.045	0.047	0.036	4.13	Significant (+)
2	Volume of hacks/month	TVL/month	Apr 2018–	86	0.000237	3.02	0.003	0.098	0.087	9.12	Significant (+)
3	Number of hacks/month	TVL/month	Jan 2020–	65	1.31×10^{112}	0.31	0.756	0.002	−0.014	0.1	Not significant
4	Volume of hacks/month	TVL/month	Jan 2020–	65	255.43	1.92	0.059	0.055	0.04	3.7	Marginal