

**Université de Montréal**

**Crime Opportunities in the Decentralized Finance (DeFi) Industry: Do DeFi Actors'  
Attributes Influence Target Attractiveness?**

Par

Catherine Carpentier-Desjardins

École de criminologie, Faculté des arts et des sciences

Travail dirigé présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention  
du grade de Maître ès sciences (M.Sc.) en Criminologie, Option Criminalistique et Information

Septembre 2025

© Catherine Carpentier-Desjardins, 2025

Université de Montréal

## Abstract

Decentralized finance (DeFi) platforms have gained in popularity over the last few years, as they offer a wide range of accessible, innovative and complex financial services. Because they evolve quickly under little regulations, it is easy for malicious parties to target them for profit when they notice a vulnerability in these emergent protocols. Existing work has focused on understanding typical attack flows and securing the technology to alleviate crime. However, little is known about what other attributes, beyond technical vulnerabilities, may put DeFi actors at risk. Drawing on Cook (1986)'s framework on target attractiveness, this study investigates what makes DeFi actors likely to be targeted by comparing key features (propinquity, vulnerability, potential payoff, areas of operation and self-protecting activities) of actors attacked in 2022 with those that were not. Results suggest that providing lending services, listing tokens on popular centralized exchanges (CEX), and past victimizations influenced the likelihood of being victimized in 2022. Ultimately, this study finds that the dimensions of target attractiveness discussed by Cook (1986) are relevant in DeFi, but not necessarily in the same direction as for traditional crimes. Notably, past victimization, unlike in traditional crime, appears to reduce the chance of revictimization in DeFi. Such insights are complementary to existing knowledge on technical vulnerabilities to better protect DeFi actors at risk of external attacks.

Key words: decentralized finance, cryptocurrency, cryptoassets, crime, target attractiveness, victimization

## Résumé

Les plateformes de finance décentralisée (DeFi) ont gagné en popularité au cours des dernières années, car elles offrent une large gamme de services financiers accessibles, innovants et complexes. Parce qu'elles évoluent rapidement sous peu de réglementation, il est facile pour des parties malveillantes de les cibler à des fins lucratives lorsqu'elles remarquent une vulnérabilité dans ces protocoles émergents. Les travaux existants se sont concentrés sur la compréhension des flux d'attaque typiques et la sécurisation de la technologie pour prévenir la criminalité. Cependant, mis à part les vulnérabilités techniques, il y a peu de connaissances sur les autres attributs susceptibles de représenter un risque pour les acteurs DeFi. À travers le cadre théorique de Cook

(1986) sur les cibles attrayantes, cette étude examine ce qui rend certains acteurs DeFi plus susceptibles d'être ciblés en analysant et en comparant les caractéristiques clés (proximité, vulnérabilité, gain potentiel, services financiers offerts et activités d'autoprotection) des acteurs attaqués en 2022 par rapport à celles de ceux qui ne l'ont pas été. Les résultats suggèrent qu'offrir des services de prêts, rendre disponibles ses jetons sur les plateformes d'échange centralisées (CEX) populaires et le nombre de victimisations passées influencent la probabilité d'être victime en 2022. Cette étude révèle donc que les dimensions d'une cible intéressante évoquées par Cook (1986) sont pertinentes dans l'écosystème DeFi, mais pas nécessairement dans la même direction que pour les crimes traditionnels : plutôt que d'accroître la vulnérabilité des acteurs DeFi, les victimisations passées réduiraient leurs chances d'être à nouveau victimisé. Ces informations s'avèrent complémentaires aux connaissances existantes sur les vulnérabilités techniques pour permettre de mieux protéger les acteurs DeFi exposés aux risques d'attaques externes.

Mots clés: finance décentralisée, cryptomonnaie, cryptoactif, criminalité, cible intéressante, victimisation

# Table of contents

<b>ABSTRACT</b> .....	<b>2</b>
<b>RÉSUMÉ</b> .....	<b>2</b>
<b>LIST OF TABLES</b> .....	<b>6</b>
<b>LIST OF FIGURES</b> .....	<b>7</b>
<b>GLOSSARY</b> .....	<b>8</b>
<b>REMERCIEMENTS</b> .....	<b>9</b>
<b>INTRODUCTION</b> .....	<b>10</b>
<b>REVIEW OF THE LITERATURE</b> .....	<b>14</b>
THE DECENTRALIZED FINANCE INDUSTRY AND ITS ACTORS .....	14
<i>Figure 1: DeFi Stack Reference Model from Carpentier-Desjardins et al. (2025)</i> .....	16
<i>Table 1: Technical Areas of Operation of DeFi Actors as Developed by Carpentier-Desjardins et al. (2025)</i> .....	17
TARGET ATTRACTIVENESS AND ITS DIMENSIONS .....	18
<i>Figure 2: Dimensions of Target Attractiveness as Developed by Cook (1986)</i> .....	20
TARGET ATTRACTIVENESS IN THE DeFi SPACE .....	24
<i>Figure 3: Dimensions of Target Attractiveness in the DeFi Space and Their Attributes</i> .....	26
Propinquity .....	26
Vulnerability .....	28
Potential Payoff .....	29
Main Area of Operation .....	30
Self-protection Activities .....	31
<b>THIS STUDY</b> .....	<b>33</b>
<b>DATA AND METHOD</b> .....	<b>35</b>
DATA COLLECTION .....	35
<i>Table 2: Tactics Used to Target DeFi Actors as Developed by Carpentier-Desjardins et al., (2025)</i> .....	35
DATASET CREATION AND DESCRIPTIVE STATISTICS .....	37
<i>Table 3: Variables and Definitions</i> .....	38
<i>Table 4 : Descriptive Statistics (N=388)</i> .....	39
LOGISTIC REGRESSION ANALYSIS .....	43
METHOD LIMITS .....	45
ETHICS .....	47
<b>RESULTS</b> .....	<b>48</b>
TABLE 5. LOGISTIC REGRESSION MODELS PREDICTING THE LIKELIHOOD OF VICTIMIZATION OF DeFi ACTORS ....	49
<b>DISCUSSION</b> .....	<b>53</b>
PAST VICTIMIZATIONS PREVENTING SUBSEQUENT VICTIMIZATIONS .....	53

THE NEGATIVE SIDE TO INCREASED EXPOSURE .....	55
LENDING SERVICES AS ATTRACTIVE TARGETS FOR CRIME IN DeFi.....	56
THE ROLE OF COMMUNITY ENGAGEMENT IN THE CREATION OF DeFi CRIME OPPORTUNITIES.....	58
THE EFFECTIVENESS OF SELF-PROTECTION ACTIVITIES IN DeFi.....	60
<b>BRIDGING DISCIPLINES: INTEGRATIVE DIMENSIONS OF CRIMINOLOGY AND FORENSIC SCIENCE.....</b>	<b>62</b>
<b>CONCLUSION .....</b>	<b>66</b>
<b>BIBLIOGRAPHY .....</b>	<b>68</b>
<b>ANNEX 1 .....</b>	<b>73</b>
TABLE 6 : BIVARIATE CORRELATIONS OF VARIABLES INCLUDED IN LOGISTIC REGRESSION MODELS .....	73

## List of Tables

Table 1: Technical Areas of Operation of DeFi Actors as Developed by Carpentier-Desjardins et al. (2025) .....	17
Table 2 : Tactics Used to Target DeFi Actors as Developed by Carpentier-Desjardins et al., (2025) .....	35
Table 3 : Variables and Definitions.....	38
Table 4 : Descriptive Statistics (N=388) .....	39
Table 5 : Logistic Regression Models Predicting the Likelihood of Victimization of DeFi Actors .....	49
Table 6 : Bivariate Correlations of Variables Included in Logistic Regression Models.....	73

## List of Figures

Figure 1 : DeFi Stack Reference Model from Carpentier-Desjardins et al. (2025) .....	16
Figure 2 : Dimensions of Target Attractiveness as Developed by Cook (1986) .....	20
Figure 3 : Dimensions of Target Attractiveness in the DeFi Space and Their Attributes .....	26

# Glossary

AML Anti Money Laundering

API Application Programming Interface

ATM Automated Teller Machine

CeFi Centralized finance

CEX Centralized Exchange

CI Confidence interval

DAO Decentralized Autonomous Organization

Dapp Decentralized Application

DeFi Decentralized finance

DEX Decentralized Exchange

DSR DeFi Stack Reference

EVM Ethereum Virtual Machine

FT Fungible token

KYC Know Your Customer

NFT Non-fungible token

OR Odds ratio

PoW Proof of Work

PoS Proof of Stake

TradFi Traditional finance

TVL Total Value Locked

## Remerciements

Je tiens particulièrement à remercier ma directrice de recherche, Masarah, dont l'enthousiasme, l'implication, le soutien et l'écoute attentive ont grandement facilité la réalisation de ce travail. Merci de m'avoir fait découvrir le monde des finances décentralisées et de m'avoir transmis ta passion pour la recherche. Travailler ensemble a manifestement embelli mon expérience universitaire, et je suis reconnaissante de la confiance que tu m'as accordée en m'intégrant au EconCrime Lab, où j'ai pu développer mes compétences et participer à multiples projets des plus enrichissants au fil des années.

Je souhaite également remercier David pour sa contribution essentielle à ce travail, notamment en rédigeant le script qui a permis la collecte des données. Merci aussi pour tes précieux conseils à propos de la session d'échange en Suisse, et pour avoir été le premier à me faire confiance en tant qu'auxiliaire de recherche au DARC Lab.

De plus, je tiens à souligner mon appréciation pour la Chaire de recherche en prévention de la cybercriminalité (CRPC), la Clinique de cyber-criminologie, ainsi que l'Université de Lausanne et ses professeurs associés pour toutes les opportunités et l'expérience que ces organisations m'ont apportées.

Finalement, je tiens à remercier tous les gens qui partagent ma vie pour leur soutien émotionnel. Mention spéciale à ma maman; la personne la plus fière de mon projet malgré sa compréhension limitée du sujet et de l'anglais!

## Introduction

Monetary gains have always been one of the main incentives for crime (Uggen & Thompson, 2003). However, it would not be fair to say that economic crime is static; it has greatly evolved over the years. In this sense, the arrival of new technologies has not only facilitated the commission of certain crimes, but also led to the development of new *modi operandi* to achieve them (Trozze et al., 2022). Namely, the recent emergence of distributed ledger technology, also known as blockchain, together with smart contract technology has made it possible to revisit the world of traditional finance. Blockchains are distributed ledgers that record transactions across multiple computers in a decentralized, immutable and transparent manner, ensuring data integrity and security (Qin et al., 2021). Hence, through this technology, users can send and receive cryptocurrencies. Smart contracts, on the other hand, are digital agreements that are created using programming languages, such as Solidity<sup>1</sup> (Auer et al., 2023). They self-execute when the predetermined conditions programmed in their code are met. Smart contracts allow for more complex transaction patterns than sending and receiving assets. Creating tokens and building various DeFi services like exchange and lending are possible through smart contracts, which are then deployed on blockchains for users to interact with. In summary, by developing and deploying smart contracts on blockchains, entities are able to provide innovative financial services in a decentralized manner. The concept of DeFi actors is employed in this study to designate entities that provide DeFi services. Note that some DeFi services can be launched by formal entities, such as foundations or companies (Dotan et al., 2023). One example is Uniswap Labs, a U.S.-based company that developed the DeFi exchange protocol Uniswap<sup>2</sup>. However, once the protocol is deployed on a blockchain, it is common for its control to be transferred to a Decentralized Autonomous Organization (DAO) (Dotan et al., 2023). Consequently, DeFi protocols themselves are often not tied to employees, a headquarters, or even a legal entity. In that sense, the governance structure of the protocol is decentralized and run by smart contracts. Governance tokens are distributed to users of the platform, granting them voting rights in the platform's governance

---

<sup>1</sup> Solidity is a high-level, contract-oriented programming language designed for implementing smart contracts on Ethereum Virtual Machine (EVM) compatible blockchains. Influenced by C++, Python, and JavaScript, it allows for creating various decentralized applications including voting systems, crowdfunding, blind auctions, and multi-signature wallets (Hegedűs, 2018).

<sup>2</sup> According to Uniswap Labs' company profile on <https://www.crunchbase.com/organization/uniswap-labs>

protocol (Dotan et al., 2023). In the case of Uniswap, no single entity or company controls the actual protocol; it is governed by UNI token holders (Uniswap Labs, 2023). Hence, we refer to all entities that provide DeFi services, whether such services were developed by companies, foundations or DAOs, as DeFi actors. It is also important to note that this excludes services like centralized exchanges (CEX) and crypto ATMs, as these are rather part of the centralized finance (CeFi) ecosystem, where entities are typically subject to more regulations such as anti-money laundering (AML) and know your customer (KYC) because they allow converting fiat money to cryptocurrencies and vice versa.

The technologies leveraged by DeFi actors are relatively recent and operate without clear regulations; our understanding of criminal activity in the DeFi ecosystem is therefore still limited. It is known, however, that malicious actors are constantly seeking to exploit innovative DeFi services for illicit purposes (Carpentier-Desjardins et al., 2025; Zhou et al., 2022). Mainly, various studies have demonstrated that profit-driven malicious users target DeFi actors by exploiting vulnerabilities in their smart contracts or their protocol infrastructure for illicit gains (Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022). This has quickly become an alarming preoccupation in the world of decentralized finance, as stolen funds from DeFi actors reached an all-time high at \$2.2B USD in 2024, an increase of approximately 21.07% from the previous year (Chainalysis, 2025). It is also important to note that the number of attacks is also on the rise, as it increased from 282 in 2023 to 303 in 2024 (Chainalysis, 2025). Consequently, studies have focused on developing vulnerability typologies which aim to secure these technologies and prevent crime (Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022).

Other studies have rather illustrated how DeFi actors themselves can be malicious and exploit users through a variety of scams, like rug pulls, honeypots and Ponzi schemes (Xia et al., 2020; Phillips & Wilder, 2020; Puggioni 2022). These studies then provide fraudulent DeFi actors' detection and scam prevention tools. Chainalysis (2025) revealed that crypto addresses which had been reported to be fraudulent received in total around \$9.9B USD in 2024.

Finally, some have shown how malicious users also impersonate legitimate DeFi actors to defraud other users with different deceptive techniques leveraging ads, social media, emails and airdrops

(Matakovic, 2022; Andryukhin, 2019; Shukla et al., 2022). DeFi users' attributes, such as their level of exposure to crypto spaces, overconfidence, cognitive bias and past victimizations are increasingly being studied to better identify scam victimization risk factors and equip vulnerable users in the DeFi space (Luoma et al., 2025). Hence, existing work has thoroughly investigated how both DeFi users and DeFi actors can fall victim to attacks in this ecosystem. However, only attributes of DeFi users that relate to the likelihood of victimization have been considered; attributes of DeFi actors, beyond technical vulnerabilities, are currently overlooked. Consequently, there is a need to identify relevant attributes of DeFi actors and assess if they relate to the likelihood of victimization to highlight attributes that can act as indicators of a greater risk of victimization.

To identify relevant attributes of DeFi actors, we leverage the theoretical framework presented by Cook (1986) in his work on the demand and supply of crime opportunities. This framework introduces five dimensions related to the concept of target attractiveness: propinquity, vulnerability, potential payoff, access to law enforcement and self-protecting activities. DeFi actor attributes that relate to these dimensions are therefore susceptible to relate to the risk of victimization, as they are indicators of an attractive target. We identified these attributes through existing literature on crime in DeFi. They include, namely, the number and types of blockchains, markets and social media the DeFi actor is operating on, the type of DeFi service the actor offers, the market value and trading volume of its main token, the presence of self-protecting activities on its smart contracts, like audits and bug bounty programs, as well as its number of past victimizations as a vulnerability indicator. We then collected the associated data on the cryptocurrency aggregator CoinGecko for a set of DeFi actors who have been victimized and a set of DeFi actors who haven't. Ultimately, we compare the two sets of actors to identify if dimensions of target attractiveness and their attributes played a role in the outcome of victimization. A series of logistic regression models were computed with these variables to better understand to what extent dimensions of target attractiveness and their specific attributes statistically influence the risk of victimization of DeFi actors. In other words, this study provides a first comprehensive assessment of profit-driven crimes in the DeFi industry, focusing on how specific attributes of DeFi actors influence their attractiveness as targets and contribute to their likelihood of victimization by malicious external parties.

The sections below begin with a literature review that examines the size and scope of the DeFi industry, as well as how DeFi actors are usually victimized. This is followed by an analysis of the relevant dimensions of a suitable target based on Cook's theory, and later how these dimensions can apply to modern targets, like DeFi actors. The relevance of the study is then outlined, followed by a detailed explanation of the data collection process, variable operationalization, the application of logistic regression, methodological limits and ethics concerns. We present the results of seven logistic regression models: one for each dimension of suitable targets, one overarching model encompassing all variables, and a parsimonious model. The results are discussed with a focus on five key takeaways. Finally, we explore how integrating criminology together with forensic science enriched our study and discuss the practical implications of the results for DeFi crime prevention and future research.

## Review of the Literature

The three following sections respectively discuss the DeFi industry landscape, target attractiveness and its dimensions according to Cook (1986), and current knowledge of target attractiveness in the DeFi Space. Each section clarifies some concepts that are central to our research objective, such as “DeFi actors” and “target attractiveness”. Altogether, the sections also help understand the relevant theoretical framework and insights behind the variable selection for the statistical models that were computed in this study.

### The Decentralized Finance Industry and Its Actors

DeFi services are financial products arising from the emergence of blockchain technology and smart contracts. “Decentralized” means that the finances are not managed by a central entity such as a bank, but rather by the individuals holding the funds. DeFi is distinguished from traditional finance (TradFi), by its resistance to censorship, its transparency, immutability, scope, and system of governance (Qin et al., 2021). In fact, as no single entity oversees the transactions, they cannot be disputed nor reverted, making them immutable. Instead, governance is distributed across users through consensus mechanisms to validate transactions and achieve an agreement on the state of the network, the two most common ones being Proof of Work<sup>3</sup> (PoW) and Proof of Stake<sup>4</sup> (PoS). As transparency on the state of the network is necessary to reach consensus, historical data of all transactions remains public.

These inherent characteristics of blockchain technology, paired with an ecosystem that hosts an impressive amount of financial assets, will logically attract some malicious users. However, while the DeFi actors operating within the ecosystem all leverage blockchain technology, they also hold various attributes unique to their protocols and smart contracts, like the type of DeFi service they

---

<sup>3</sup> Proof of Work: Participants wishing to create and validate transaction blocks to earn financial rewards must compete to solve a mathematical puzzle that enables the creation of the next block. This requires powerful devices in terms of computing power, as well as significant electricity consumption. When a participant finds the solution, they broadcast their block to the rest of the network. The others then test the solution and validate the authenticity of the block, after which the competition for the subsequent block begins (Nair et al., 2021).

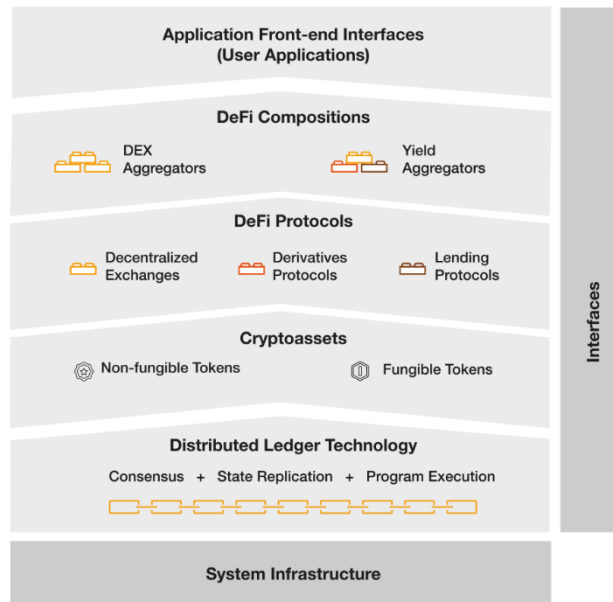
<sup>4</sup> Proof of Stake: To reduce the reliance on computing power, participants are instead chosen to create and validate blocks based on the amount of assets they hold and are willing to freeze as collateral. In principle, those who hold the most assets have a vested interest in ensuring the security and proper functioning of the blockchain. A validator attempting to create a malicious block will be detected by others, their block will not be accepted, and they will lose a portion of the assets provided as collateral (Nair et al., 2021).

provide, the market value and circulating supply of their tokens, the blockchains and markets they decide to operate on and the security measures they invest in to prevent external attacks. These characteristics are the ones that are overlooked in existing work on DeFi crime opportunities. In fact, blockchain and smart contract characteristics have been thoroughly investigated. As a result, many risk factors and vulnerabilities within the technology have been identified and linked to the likelihood of attacks (Ghaleb, 2022; Zhou et al., 2022; Qian et al., 2022; Werner et al., 2022; Carpentier-Desjardins et al., 2025).

The same effort has not been put into investigating DeFi actors' attributes to identify what makes a DeFi actor an attractive target, placing it at greater risk of victimization. Our study takes a first step to bridge this gap. It is first necessary to review what is currently known about DeFi actors and the crime opportunities surrounding them, to define the concept of target attractiveness and explore its dimensions (propinquity, vulnerability, potential payoff, access to law enforcement and self-protecting activities), and finally to link what we know about DeFi actors to these dimensions, which ultimately guides us on the relevant variables to include in our analysis when investigating which DeFi actors' attributes influence the likelihood of victimization.

To date, DeFi actors have replicated and offered all TradFi services like exchange, asset management, lending, insurance, and contracts, but they also offer innovative services and other concepts, not achievable through TradFi, such as non-fungible tokens (NFT), synthetic assets, flash loans, yield farming and liquidity mining, automated market making and other decentralized applications (Dapp) (Jensen et al., 2021; Auer et al, 2023). In fact, smart contracts make DeFi protocols highly composable, meaning they can interact seamlessly with one another, allowing for flexible and innovative financial strategies. The system infrastructure of DeFi can be better understood through a DeFi stack reference Model (DSR), as presented in Figure 1. This stack is derived from Carpentier-Desjardins et al. (2025), who augmented the DSR previously introduced by Auer et al. (2023).

Figure 1: DeFi Stack Reference Model from Carpentier-Desjardins et al. (2025)



The stack shows the distributed ledger technology (DLT) at the bottom, followed by layers that can be built on the technology through smart contracts in ascending order of complexity. Hence, some DeFi actors simply offer cryptoassets like fungible (FT) or non-fungible tokens (NFT), some offer simple protocols like the ones TradFi offers, but in a decentralized manner (e.g., exchange and lending), and others, rather offer composition protocols (e.g., yield and DEX aggregators), which merge different services due to composability to create unique applications. The top layer represents the tangible interfaces users interact with to engage with the services offered by DeFi actors. Finally, the interface layer on the side represents DeFi actors like oracles and bridges that increase composability and allow smart contracts to fetch information they need from outside the blockchain to better conduct their operations (such as the current market value of a fiat currency). From this stack, Carpentier-Desjardins et al. (2025) suggested 12 categories (defined in Table 1) to represent relevant technical areas of operation for DeFi actors: blockchain, fungible tokens (FT), non-fungible tokens (NFT), exchanges, lending, derivatives, Dapps, yield, staking, bridges, oracles, and others. Thus, DeFi actors can offer a broad variety of financial services, some more complex than others. It is also important to note that some categories are more popular, as fungible tokens and exchange services are typically the most interacted with by users (Auer et al., 2023).

Table 1: Technical Areas of Operation of DeFi Actors as Developed by Carpentier-Desjardins et al. (2025)

<b>DeFi actor areas of operation</b>	<b>Definition</b>
<b>Blockchain</b>	Actors that offer a decentralized digital ledger that records transactions in a secure, transparent, and tamper-proof way
<b>Fungible Token (FT)</b>	Actors that offer a digital asset that is interchangeable with others of the same kind
<b>Non-Fungible Token (NFT)</b>	Actors that offer a unique digital asset that represents ownership of a specific item or content and that is not interchangeable
<b>Exchange</b>	Actors that facilitate the trading of tokens
<b>Lending</b>	Actors that allow the lending and borrowing of tokens
<b>Derivatives</b>	Actors offering insurance services and platforms that allow the issuing and trading of synthetic positions that track the value of underlying tokens or real-world assets.
<b>Dapp</b>	Actors that offer a blockchain-based app that does not fall under other protocol categories (e.g., gaming, storage and social platforms)
<b>Yield</b>	Actors comparing the returns of diversified financial services across multiple DeFi protocols to maximize the value of users' portfolio
<b>Staking</b>	Actors that offer locking up tokens to earn rewards
<b>Bridge</b>	Actors that allow the moving of tokens or data between different blockchains
<b>Oracle</b>	Actors that supply real-world data to smart contracts
<b>Others</b>	Actors that offer services which fall under the user application layer of the DSR model (e.g., markets, wallets)

According to the service they offer, vectors of attacks to victimize DeFi actors can vary. For example, lending platforms are more susceptible to flash loan attacks (Oosthoek, 2021). Consequently, most studies focused on how DeFi actors can be victimized, mainly by identifying loopholes in the protocols, smart contracts and infrastructure of different DeFi services (Zhou et al., 2022; Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022). Relevant insights resulting from

these investigations include smart contract and consensus mechanism vulnerabilities, as well as types of attack typologies. Most frequently mentioned types of attack revolve around technical vulnerabilities such as smart contract exploitations through re-entrancy vulnerabilities, access control flaws or logical bugs, governance issues like 51% attacks, or oracle manipulation and flash loan funded attacks (Qian et al., 2022; Caldarelli & Ellul, 2021; Wang et al., 2021; Oosthoek, 2021; Qin et al., 2021). It is also mentioned how a lack of internal security and infrastructure vulnerabilities can lead to private key leakages, precipitating both internal and external attacks. Beyond technical vulnerabilities, some studies have also demonstrated that malicious users can target DeFi actors by exploiting human risks, for example socially engineering a team member to access sensitive data like private keys and wallets (Carpentier-Desjardins et al., 2025; Li et al., 2022).

Consequently, a lot is known about how DeFi actors get victimized, but significantly less work has focused on why certain actors are more victimized than others, or what places them at greater risk of being attacked successfully. To date, two studies have reviewed a large amount of mediatized DeFi crime events in the last few years and shown that some layers of the DSR do, in fact, face more attacks, as well as greater financial losses than others (Carpentier-Desjardins et al., 2025; Zhou et al., 2023). This suggests that, just like for traditional crimes, victimization is not distributed equally in the DeFi ecosystem. In fact, some DeFi actors seem to attract offenders more. Consequently, it is relevant to revisit the concept of target attractiveness and apply it to the DeFi ecosystem, as no previous work sought to explain why some DeFi actors are more targeted than others, nor to identify circumstances increasing the chance of being targeted outside of coding mistakes and technical vulnerabilities. To that end, we first define the concept of target attractiveness along with its dimensions (propinquity, vulnerability, potential payoff, access to law enforcement and self-protecting activities) based on Cook's (1986) theory in the next section. We then present which attributes of DeFi actors relate to those dimensions to identify the relevant variables to investigate in our analysis.

## Target Attractiveness and Its Dimensions

Our study is inspired by concepts discussed by Cook (1986) in his work “The Supply and Demand of Crime Opportunities”, as the author also prefaces that the role of victims and potential victims

in determining the volume and distribution of crime is often neglected, insisting that victims' attributes and behaviors do influence the likelihood and nature of crimes. His opportunity theory employs the economic theory of markets with the analogy of supply and demand to describe and predict how criminals and victims interact: "*If crime rates are influenced by the quality and quantity of criminal opportunities, and vice versa, then the aggregate crime rate is determined by the interaction between the public, as 'providers' of crime opportunities and potential criminals*"<sup>5</sup> (Cook, 1986). In addition, Cook argues that criminals tend to be selective when choosing a target; they would be more attracted to targets that appear to offer a high payoff with little effort or risk of legal consequences. Simultaneously, potential victims respond to the crime threat by reducing their exposure and engaging in self-protection efforts to appear less vulnerable. This statement suggests that several specific attributes of potential targets will be salient to the criminal: propinquity, payoff, vulnerability, access to law enforcement and self-protection activities. Relative target attractiveness to criminals would then help understand the differences in victimization rates for different potential target groups. In fact, others have also demonstrated that victimization rates and distributions for crimes of theft and violence differ widely among different groups of people (Meier & Miethe, 1993). To that end, Cook insists that an understanding of crime volume and distribution requires a complete characterization of both potential criminals and potential victims, as well as their interactions. As mentioned above, DeFi studies have prioritized characterizing malicious actors' actions and types of attacks over victimized parties' attributes and behaviors to explain crime. There is a need to bridge this imbalance by shifting the focus from attackers to targets. A righteous first step is to investigate to what extent DeFi actors' attributes related to propinquity, payoff, vulnerability, access to law enforcement and self-protection activities influence their likelihood of victimization, which is the main objective of this study. The next section further defines the dimensions of target attractiveness according to Cook (1986), as illustrated in Figure 2.

---

<sup>5</sup> Note that while victimized parties are given an important role in the understanding of crime rates and opportunities in this theory, Cook discusses perceived target attractiveness by offenders rather than the objective attractiveness of potential victims. This approach thus attributes responsibility to offenders and solely aims at understanding crime patterns, never implying that victims should be blamed for the outcome of events.

Figure 2: Dimensions of Target Attractiveness as Developed by Cook (1986)



In his work, Cook (1986) claims that dimensions of target attractiveness, as seen in Figure 2, are applicable to common crimes of theft and violence, such as assault, burglary, personal larceny and robbery. He explains that other authors studying target attractiveness share this idea (Conklin, 1972; Cohen et al., 1981; Sparks, 1981; Gottfredson, 1981). However, to remain consistent and concise throughout his speech, Cook limits his examples to robbery. Hence, he introduces the five dimensions of target attractiveness by relating propinquity, vulnerability, potential payoff, access to law enforcement and self-protection activities to offenders and victims involved in robberies. The concept of **propinquity** encompasses two important elements: exposure and proximity. The former refers to the physical visibility and accessibility of individuals or objects to potential offenders at any given time or space, while the latter refers to the physical distance between areas where potential targets reside and areas where motivated offenders are typically found (Cook, 1986; Cohen et al., 1981). Thus, according to Cook (1986), propinquity revolves around offenders wanting to spare time spent selecting a suitable target. Consequently, targets that are visible and situated in a location that is easily accessible will tend to suffer a higher victimization rate. Hence, the risk of suffering victimization can increase simply by being more exposed to offenders, who frequently perceive looking further as time consuming and unnecessary efforts. In addition, Cook

argues that targets who present characteristics that offenders associate with **vulnerability** can be at greater risk of suffering victimization. In fact, offenders do not wish to deploy efforts into countering resistance attempts from the victim or protest from bystanders (Cook, 1986). In the eyes of the offender, the necessary power and the probability of success will depend on the vulnerability of its victim. Potential targets that appear to be in a vulnerable state, incapable or unwilling to defend themselves, will therefore appear as more attractive. In that respect, groups of people, including women, elderly people, intoxicated people or already victimized people, can appear relatively vulnerable (Cook, 1986). Next, as monetary gains are often the main incentive for crime, Cook argues that offenders, like robbers, will generally select a target that offers a higher **potential payoff**. Hence, individuals or businesses who appear to be carrying a lot of money or material valuables will be considered more attractive targets than others. A great example is banks; these locations are known to carry a lot of money, ensuring a high payoff in the eyes of the robbers if they are successful (Cook, 1986). However, more lucrative targets will typically put effort into reducing their propinquity and vulnerability. In fact, knowing they appear as an attractive target because of the assets they hold, Cook anticipates that such targets will attempt to compensate by reducing their attractiveness elsewhere. Another dimension mentioned by Cook is having **access to law enforcement**, as offenders typically seek to minimize the probability and severity of punishment. This reinforces the attractiveness of vulnerable victims, as quicker and easier robberies without resistance are unlikely to lead to an on-scene arrest or a visual identification by witnesses (Cook, 1986). Other groups of potential targets that have limited law enforcement access would include individuals that are themselves part taking in illicit activities and individuals who are unlikely to report their victimization, for example, because of past negative experiences with the authorities or the lack of support they expect to receive (Cook, 1986). On the contrary, individuals or entities that actively engage in **self-protecting activities** have chances of decreasing their risk of victimization. Cook (1986) regroups self-protection activities under three categories. The first one aims at increasing the difficulty of a successful crime, like hiding valuables in concealed spaces or staying at locations with guards, dogs, and other situational means of protection to help reduce target vulnerability. The second one rather aims at increasing the likelihood of arrest and punishment, for example, with alarm systems or marked goods. The third category includes actions to minimize potential losses or discourage criminals by reducing the

potential payoff. Such actions relate to limiting the usual number of valuables on hand, as well as keeping weapons for deterrence and self-defence purposes (Cook, 1986).

While Cook's opportunity theory was developed regarding more traditional crimes with an emphasis on robberies, the dimensions of a suitable target were later applied to the online space and deemed relevant to understand the distribution and risk factors of cybervictimizations as well (Kshetri, 2009; Bossler & Holt, 2009; Leukfeldt & Yar, 2016). For example, different studies found that **propinquity** and **vulnerability** also play an important role in online crime victimization (Bossler & Holt, 2009; Leukfeldt & Yar, 2016; Mikkola et al., 2024). In fact, it was found that, through the amount of time they spent online, the types of websites they visit and the types of activities they engage in online, individuals could increase their exposure to cybercriminals, appear more vulnerable and thus be perceived as more attractive targets (Leukfeldt & Yar, 2016). Like physical locations, virtual spaces can harbour a higher victimization rate, as the configuration of the space can change or influence the dynamics between offenders and victims (Miró-Llinares et al., 2020). Other studies examining online crime through an economic lens also showed how the low probability of cybercriminals being caught, prosecuted and punished, together with the increased financial incentives, grants them highly positive economic feedback, meaning they associate online targets with greater **potential payoff** (Kshetri, 2009). Another study focusing on the attractiveness of companies as potential targets for cyber-attacks showed that companies who display a strong overall financial status, namely high annual earnings, growth trends and historical earnings stability, were perceived as more attractive targets by cyberoffenders (Awan & Dahabiyeh, 2018). This reinforces the belief that, like in traditional crimes, offenders look for targets who appear to be carrying more money and valuables. The dimension of a suitable target relating to **access to law enforcement** was also explored for online crimes. It was found that inefficiency and congestion in the law enforcement system for cybercrime investigation and prosecution increase perceived online target attractiveness for cybercriminals (Kshetri, 2009). In fact, the novelty of cybercrimes, low-governmental priorities, the lack of cross borders and industry-government cooperation, along with victims' reticence to report these crimes significantly decreases the power of law enforcement over cybercriminals (Kshetri, 2009). In addition, Paquet-Clouston & Garcia (2023) found evidence that a lack of deterrents resulting from lower law enforcement power correlates with cybercrime engagement. In fact, cyber offenders, in

certain regions of the world, do not perceive the threat of law enforcement (Paquet-Clouston & Garcia, 2023). Moreover, in Canada, in 2023, only one in eight businesses (13%) who suffered a cyber security incident reported it to law enforcement (Statistics Canada, 2024). Most of the security incidents related to thefts of money or demands for ransom payments. In addition, decisions not to report these incidents related to a preference for resolving the issue internally (55%), the belief that the incident was too minor (35%), or a preference for seeking help from the private sector, for example with information technology consultants or contractors (31%) (Statistics Canada, 2024). These insights suggest that access to law enforcement becomes less relevant for online victimization, as the system is perceived as inefficient in responding to these types of crimes and targets would rather solve their issues through other avenues. Finally, **self-protection activities** have also been investigated and linked to a decreased risk of being online victimized. Mainly, the usage of privacy-enhancing technologies and other techniques, like two-factor authentication and antivirus software, are prioritized amongst individuals concerned with online exposure and cyber-offenders (Leukfeldt & Yar, 2016; Ireland, 2021)

Note that these studies mainly focused on individual online behaviours, findings on propinquity, vulnerability, potential payoff, access to law enforcement and self-protecting activities can thus hardly be generalized to broader entities like businesses or DeFi actors. For example, self-protecting activity expectations might be different for individuals and broader entities, as we would expect a regular person to use basic protections, like antivirus programs, while a business could invest in audits and cybersecurity teams. Furthermore, the context of access to law enforcement within the DeFi ecosystem is distinct. First, because DeFi actors rely on decentralized governance systems like smart contracts and DAOs (which often involve pseudonymous international developers), so there is a lack of central authorities to directly cooperate with law enforcement, receive subpoenas, or freeze funds at risk (Altschuler, 2022). For that reason, CeFi actors are more likely to engage with law enforcement and report victimizations than DeFi actors. Second, after a victimization, recovery is frequently prioritized by DeFi actors over reporting the incident. In fact, victimized DeFi actors prefer to concentrate their efforts into tracking and recovering lost funds by quickly involving other entities like blockchain forensic firms and white hat hackers, engaging in negotiations with the offender and publicly informing their community of the risks related to the exploit (McDougall & Tan, 2023). For these reasons, the role of law enforcement in the context

of DeFi crime is less central than it is to other crimes; DeFi actors are often the main guardians of their activities.

Nevertheless, the findings on online target attractiveness show the relevance of Cook's target attractiveness dimensions in the online space and suggest that victimization patterns can be organized differently from one virtual space to another, thus reinforcing the relevance of investigating the unique cyberspace provided by DeFi. For instance, Dearden & Gottschalk (2024) conceive cyberspaces involving cryptoassets as criminogenic areas of the online world, much like being in a geographic region high in crime. Still, there is a need to further our understanding of target attractiveness in DeFi's specific context, which is the object of the next section.

## Target Attractiveness in the DeFi Space

This section categorizes and regroups various findings from journal and conference peer-reviewed articles, as well as relevant blogs and posts from blockchain security firms on crime in the DeFi space under the dimensions of a suitable target, namely propinquity, vulnerability, payoff, and self-protecting activities. Note that we do not develop more on access to law enforcement, as it was previously stated that DeFi actors typically favour taking means into their own hands post victimization, and that the decentralized nature of their governance systems limits instances of reporting. In fact, when a protocol is run through a DAO, it is difficult to identify who can file a report and communicate with law enforcement on behalf of the DAO, as token holders are pseudonymous, and no designated higher authority is in charge (Černá, 2024). Because reporting to law enforcement is challenging and complex in DeFi (Černá, 2024; McDougall & Tan, 2023), and because no attributes of DeFi actors can act as an indicator of their individual access to law enforcement, we chose to exclude this dimension from our analysis. While we removed this dimension, we also decided to add another one named the **main area of operation**, as seen in Figure 3. We add this dimension along the original ones presented by Cook (propinquity, vulnerability, potential payoff and self-protection activities) because findings in DeFi suggest that the financial service offered by a DeFi actor (its main area of operation) might have an influence on target attractiveness, as some offenders might perceive an area of operation as easier to attack or as potentially yielding a higher payoff (Zhou et al., 2022; Carpentier-Desjardins et al., 2025). We separate this dimension from the original ones to better account for the specific context of

DeFi and its actors in our study. The review below further details each dimension's relation to victimization in DeFi. In that sense, it allows us to better understand how fragments of existing work on DeFi can relate to the crime opportunity theory as developed by Cook (1986), which helps us identify variables of interest to accomplish the objective of this study: **assess which attributes of DeFi actors relate to the likelihood of victimization**. Figure 3 introduces the dimensions of target attractiveness in the DeFi space and their attributes, which are further discussed in the text below. Note that Figure 3 presents all attributes that could be identified through the literature review, but that only attributes in bold are featured in the models we present later, as these are the attributes for which data necessary for our analysis was available, sufficient, and could be collected online. For example, DeFi actors do not publicly disclose the smart contract security tools they utilize, hence why we do not further investigate this attribute.

Figure 3: Dimensions of Target Attractiveness in the DeFi Space and Their Attributes



### Propinquity

While Cook (1986) conceived propinquity through both proximity and exposure, we rather focus on exposure. In a specific setting, such as the DeFi ecosystem, we can account for a DeFi actor’s online exposure through visibility and accessibility, but we cannot account for its physical proximity in terms of distance from offenders. One way to account for DeFi actors’ exposure is with **social media**. In fact, DeFi actors often use social media to build an online community, which helps expand their user base and overall transaction volume. Such marketing tactics increase the online presence of DeFi actors and their visibility, further exposing them to potential malicious users. In addition, many DeFi vulnerabilities would originate from DeFi actors who focus on rapid online community growth over implementing and maintaining robust security systems (Chainalysis, 2024). Hence, prioritizing exposure over self-protecting measures could influence the likelihood of victimization in DeFi.

Other ways DeFi actors can improve their exposure are by increasing the accessibility of the service they offer, which can be done by deploying their protocols and smart contracts across different **blockchains** and listing their tokens to be available to trade on numerous **markets** (centralized (CEX) and decentralized (DEX) exchanges). As operating on different blockchains can help reach more users, it also reaches more malicious users. In addition, some chains' characteristics, like popularity and capability to execute smart contracts, were linked to the likelihood of victimization, as Ethereum Virtual Machine (EVM) based chains and Solana were amongst the most targeted chains of 2020 and 2021 (Chainalysis, 2024). Also, recently, a different class of blockchains, called *Layer-2*, has emerged to alleviate the blockchain scalability issues many chains face. In fact, as blockchains often suffer from low transaction rates and high transaction processing latencies, affecting their scalability, layer-2 blockchains were designed to improve transaction processing rates, periods, and fees by minimizing the use of underlying slow and costly blockchains (Gangwal, 2023). As these chains have quickly gained popularity in the DeFi ecosystem due to their efficacy, they share characteristics of chains that are linked to increased victimization, as stated above. For this reason, even if no study currently links these chains to the likelihood of DeFi actors being victimized, layer-2 chains should be further investigated.

As it relates to markets, it can be beneficial for a DeFi actor to expand its scope by spreading the trading of its assets across multiple decentralized exchanges, especially more reliable and established DEXs. In fact, providing accessibility to a larger pool of traders and increasing liquidity can enhance overall market efficiency. On the other hand, limiting market activity on a few DEXs or smaller ones might make an asset more susceptible to manipulation or disruptions, as it may take fewer trades to influence prices (Solidus Labs, 2023). These insights suggest a complex relation between propinquity and victimization in DeFi, as sometimes exposure can place DeFi actors at risk, while other times it could limit potential harm to their assets.

## Vulnerability

Objectively, technical vulnerabilities allowing users to exploit DeFi platforms are the most widely documented and linked to victimization. Mainly, loopholes in protocols' smart contracts or infrastructure are at cause (Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022). Coding mistakes are a primary source of vulnerability, as the exploits of smart contracts are the most prevalent types of attack observed (Carpentier-Desjardins et al., 2025). Additionally, because of the public nature and transparency of smart contracts' source code, malicious users can easily detect vulnerable contracts. Beyond coding mistakes, vulnerabilities originating from oracle choices in smart contracts are deemed some of the most significant in DeFi, as manipulating an oracle can alter the outcome of actions driven by a smart contract (Wang et al., 2021). Like smart contract coding mistakes, malicious users can also identify if smart contracts rely on vulnerable oracles. An oracle's vulnerability can be influenced by its degree of decentralization, its number and quality of data sources, its data feeder selection process, node quality and reliability, as well as frequent changes in volume and prices (Wang et al., 2021). DeFi actors can self-protect by relying on a more decentralized oracle to alleviate the risk of a single point of failure, which facilitates attacks.

Other less documented vulnerabilities susceptible to increase the likelihood of victimization are off-chain vulnerabilities relating to human risks. In fact, internal thefts have been observed on DeFi platforms, where developers or greedy operators abuse their privileged access to certain functions of the platform for personal gains (Carpentier-Desjardins et al., 2025; Zhou et al., 2022). Other human risks relate to operational mistakes or operators being socially engineered, leading to the victimization of the platform. In those cases, a team member will compromise sensitive information by mishandling it or storing it ineffectively or will be deceived into granting funds or data access to a malicious external party (Carpentier-Desjardins et al., 2023). This reinforces the relevance of considering vulnerabilities beyond technology-based ones, as they also put DeFi actors at risk of victimization.

Finally, previous victimizations can sometimes be considered as a precursor for subsequent victimization in traditional and online criminality, as a perceived target's vulnerability is increased post-victimization (Holt et al., 2017; Leukfeldt & Yar, 2016). This has yet to be confirmed in DeFi. However, some offenders have revictimized DeFi actors shortly after they targeted them, since the

technical vulnerabilities they exploit often take time to resolve, which leaves victimized DeFi actors exposed and vulnerable to subsequent attacks (Chainalysis, 2024). In that sense, **past victimizations** might contribute to perceived target attractiveness in DeFi as well. In addition, an attack on a DeFi actor can put other DeFi actors in a more vulnerable state, as a hack on another protocol might create vulnerability in theirs due to the composability of DeFi; many actors rely and build on each other. This phenomenon is called contagion (Chainalysis, 2024). Real-time attack detection and updates on the state of the market can therefore be beneficial to all DeFi actors, as identifying any attack in the ecosystem can indicate to other platforms to be particularly vigilant in the upcoming hours.

### Potential Payoff

In Cook's (1986) theory, targets who appear to carry a lot of valuables are attractive. This was reiterated by Awan & Dahabiyeh (2018), who implied that companies with strong financial status featuring high annual earnings, growth trends, historical stability and immovable and movable properties were linked to increased perceived target attractiveness. In DeFi, certain metrics can be associated with the financial status of a DeFi actor. DeFi actors each hold their share of assets, where their value can be quantified. The **Total Value Locked (TVL)**, which can be measured as follows.

$$TVL = \sum(\text{Value of Tokens Locked in DeFi Actor's Contracts})$$

represents the value in USD of the total token balance held by smart contracts of a DeFi actor. Zhou et al. (2022) explained that a high TVL was an indicator of a greater value of assets at risk of attacks. A high TVL could have indicated a higher potential payoff for attacks, but they later showed that protocols who incurred the most financial damages (yield farming and cross-chain bridges) had a lower total TVL than DEX protocols, who incurred smaller losses. This suggests that DeFi actors who carry more assets do not seem to be more victimized. This needs to be further analyzed. Other metrics that are widely used to investigate the value, evolution, and relevance of cryptoassets include token value, market capitalization, and trading volume. **Token value**, measured as:

$$\text{Token Value} = \text{Market Capitalization} / \text{Circulating Supply}$$

refers to the market value of one unit of a specific token. **Market capitalization**, on the other hand, reflects the market value of the entire circulating supply of a token, calculated as:

$$\text{Market Capitalization} = \text{Token Value} \times \text{Circulating Supply}$$

Finally, **trading volume** refers to the number of a specific token traded within the last 24 hours, multiplied by its token value. It can be expressed by the following formula:

$$\text{Trading Volume} = \text{Number of Tokens Traded (24h)} \times \text{Token Value}$$

In existing literature, no explicit findings link these metrics to the likelihood of DeFi actor victimization. In fact, empirical evidence has only linked trading volume to the likelihood of victimization of DeFi users, as it can be an indicator of pump and dump schemes (Xu & Livshits, 2019). We know that attacks targeting DeFi actors continue to occur even when the overall state of the DeFi ecosystem is not at its best, or when actors exhibit lower token values and TVLs. However, when interest towards a token rises, users become more active, which increases the trading volume and token value. More transactions involving more valuable tokens can showcase attractive opportunities for offenders, as they typically look for targets that carry out more money (Cook, 1986). Because attacks against DeFi actors are profit-driven, it is relevant to investigate if TVL, token value, market capitalization and trading volume, which can be associated with the potential payoff in the context of target attractiveness, relate to the likelihood of victimization.

### Main Area of Operation

Another element that is mentioned in the literature is the main area of operation of DeFi actors. While, this is not an original target attractiveness dimension of Cook (1986), it is relevant in the context of DeFi, as some areas have been linked to more instances of crime, while others have been linked to more financial losses. For example, Carpentier-Desjardins et al. (2025) estimated that while **DeFi protocols** (e.g., exchange, lending, Dapp) suffered more crime events (N= 298) totalizing more financial losses (\$2.6B\$) from 2017 to 2022, **DeFi compositions** and **interfaces** yielded higher average profits per incident. Specifically, the average financial gain per attack was \$522,807 for protocols, compared to \$1.3 million for compositions and \$800,000 for interfaces. Similarly, Zhou et al. (2022) investigated DeFi crime events from 2018 to 2022 and found evidence that yield farming (\$868M) bridges (\$860M), and lending (\$485M) protocols were the DeFi actors

who suffered the most financial damages, reiterating that actors involved in compositions and interfaces face greater financial damages. Here, the disparity in damages across different actors suggests that some targets might be more attractive than others, as they would ensure a greater payoff due to the nature of the financial service they offer. However, it is also suggested that the services facing the most attacks (DeFi protocols) yield, on average, a lower payoff. One might think that some DeFi actors may simply be easier to victimize due to the nature of the financial service they offer, which also attracts offenders. For this reason, we differentiate the potential payoff and areas of operation dimensions to better capture their individual influence on the likelihood of victimization.

### Self-protection Activities

Cook (1986) explains that potential targets can engage in self-protection activities that aim at increasing the difficulty of a successful crime, minimizing potential losses or increasing the likelihood of arrest and punishment. The two formers are prioritized by DeFi actors, as they actively aim to secure the smart contracts they deploy and the funds they hold. In fact, it was previously mentioned that coding mistakes and oracle issues can be singled out and exploited by malicious actors. Conversely, it is possible for DeFi actors along with professionals to identify and resolve such vulnerabilities before, which alleviates the risk of attacks. In that sense, DeFi actors can seek blockchain security firms' help to conduct **audits** on their contracts to detect potential vulnerabilities and obtain a security score prior to deploying their contracts to all users. To that end, Zhou et al. (2022) found evidence that a security audit can decrease the average probability of an exploit on a DeFi actor by a factor of four. However, they explain that this result is derived from a small sample (N=56), which calls for further research. Chainalysis (2024) also stated that when they investigated DeFi hacks, a large proportion of the affected contracts they examined had either not undergone any audit or had been audited inadequately. This suggests that a lack of self-protecting behaviours from DeFi actors can increase their risk of victimization.

Apart from audits performed by security firms, researchers have developed **security tools** to enhance developers' ability to program and deploy secure smart contracts. Some examples include Mythril, DEFINERY, EthBMC, ContractFuzzer and ContractWard (Zhang et al., 2024). While

these tools, along with audits, can be very efficient to reduce the risks of deploying a vulnerable contract, they won't prevent attacks, hence why other tools have focused on real-time transaction management, as well as patching tools to better post-deployment security. SODA, Ægis and EVM-Shield are tools that use real-time analysis via enhanced EVM to protect after deployment, and EVMPatch and SolSaviour assist developers in upgrading smart contracts when vulnerabilities are discovered post deployment (Zhang et al., 2024). Finally, BLOCKEYE deployed a real-time attack detection system that identifies vulnerable DeFi projects according to the oracles they use, and whether it allows for prices to be externally manipulated (Wang et al., 2021). Leveraging these self-protection tools could therefore reduce a target's attractiveness in the DeFi space, as they ultimately help deploy and manage safer smart contracts.

Finally, some DeFi actors include the entire DeFi community in self-protective activities, by part taking in **bug bounty programs**, which are popular tools to help prevent software exploits. These programs offer monetary rewards for users that report vulnerabilities before they can be exploited by malicious parties (Breidenbach et al., 2018). Such initiatives sometimes prevent large-scale attacks, as DeFi actors benefit from the entire community's scrutiny, and users are incentivized by financial gains. Hence, audits, contract security tools and bug bounty programs are self-protection activities which DeFi actors may engage with to both increase the difficulty of attack for offenders and minimize potential losses caused by attacks.

In summary, findings in DeFi's existing work indicate how Cook's target attractiveness dimensions (propinquity, vulnerability, potential payoff and self-protection activities), as well as the novel dimension of the main area of operation, all relate, to some extent, to victimization in DeFi. In fact, all dimensions encompass DeFi actor attributes, such as chains, markets, past victimizations, token values, trading volume and audits, which are susceptible to relate to the likelihood of being victimized. Attributes that are featured in bold in Figure 3 will be investigated in our models, others were discarded due to insufficient data availability. In the next section, we further explain the necessity and relevance of developing models assessing which attributes of DeFi actors relate to the likelihood of victimization and introduce the method we employ to reach this objective.

## This Study

Research on crime in DeFi has mostly focused on how assets can be stolen but has failed to investigate victimized parties as thoroughly as malicious ones. In fact, there exist many technical studies that, from blockchain malicious transaction patterns, detail possible attack methods and flows (Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022), but less effort has been put into developing explanations regarding victimization patterns in the DeFi space. The lack of studies exploring to what extent traditional opportunity theory concepts can be applied to the DeFi space can partially be explained by the fact that research in DeFi and cryptoassets has been dominated by the computer science field. In fact, research questions and objectives aim at better understanding and improving DeFi technologies (Zhou et al., 2022; Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022). In addition, methods often rely on programming skills and tools to interpret digital traces like malicious transaction patterns, cryptoasset flows and technical vulnerabilities.

We suggest that the DeFi community could benefit from different approaches rooted in social sciences to interpret data. In fact, computer sciences facilitate the understanding of technical vulnerabilities and attacks, while social science like criminology can provide interesting frameworks to explain why we observe such crime opportunities and patterns in DeFi. In that sense, criminology theories can be leveraged, like programming knowledge, to interpret the digital traces surrounding DeFi actors and crime events. Dimensions of target attractiveness have been studied regarding online targets and deemed relevant to explain the likelihood of victimization, but no work has focused on the context of DeFi. We thus estimate that this novel way of analyzing data on DeFi crime events would be complementary to existing work and facilitate the identification and understanding of attributes relating to the likelihood of victimization for DeFi actors. A first step towards this goal is to verify to what extent traditional opportunity theory concepts are relevant in the DeFi space. The unicity of this ecosystem is an opportunity to further the understanding of “target attractiveness”, as modern targets like DeFi actors now offer new financial services and operate through a technology that has not been considered in the development of those crime theories.

As DeFi can be further disaggregated into different categories of DeFi actors, each hosting their tokens, which have value, market capitalization and trading volume of their own, we consider DeFi

actors and their respective tokens the two components of a target in the DeFi space. It is therefore relevant to collect data on both the actors themselves as well as their tokens to assess what might influence the likelihood of victimization.

Drawing from Cook's (1986) framework on target attractiveness, **the main objective of this study is to assess which attributes of DeFi actors relate to the likelihood of victimization.** To achieve this, we 1) select variables that reflect the dimensions of propinquity, vulnerability, potential payoff, area of operation and self-protecting activities in DeFi as discussed in the literature review, and 2) compute logistic regression models to assess to what extent the different dimensions and their variables influence the likelihood of victimization of DeFi actors. The latter was achieved with logistic regression statistical analysis comparing a sample of targeted and non-targeted actors in 2022 (N=388).

# Data and Method

## Data collection

This study requires the comparison of a set of DeFi actors who have been victimized with a set of actors who haven't. The list of victimized DeFi actors is derived from a previous dataset that includes all crime events reported online by three aggregators (De.Fi<sup>6</sup>, Slowmist<sup>7</sup> and CryptoSec<sup>8</sup>). The dataset was created in the context of Carpentier-Desjardins et al. (2025)'s work, and such aggregators have previously been used in other studies, like Zhou et al. (2022), as they also considered these platforms the most extensive aggregators for DeFi crime events to this day. This dataset encompasses crime events in which DeFi actors were targets, fraudsters and intermediaries. We only retained DeFi actors that have been targeted in 2022. For precision purposes, Table 2 discloses the types of attack that relate to targeted DeFi actors that are featured in this dataset.

Table 2: Tactics Used to Target DeFi Actors as Developed by Carpentier-Desjardins et al., (2025)

Type of attack	Definition	Examples
Contract vulnerability	A vulnerability in a smart contract's code is exploited for theft purposes	Reentrancy, access control flaw, logical bug, rollback
Hacked/exploited infrastructure	A vulnerability in the infrastructure of the DeFi actor is exploited	Accessing private keys, ransomware
Interconnected actor flaws	A loophole in a financial service implicating multiple DeFi actors leads to a vulnerability being exploited	Flash loan arbitrage, oracle manipulation
Transaction attack	Blockchain's transaction order process is exploited	Replay, front-running, transaction congestion
Decentralization issue	The governance or consensus mechanism or a DeFi actor is exploited	51% attack, vote manipulation
Internal theft	An insider takes advantage of their strategic position in the DeFi actor's organization for personal gains	Unauthorized use of private keys, contract exploits, backdoors and malicious code injection
External factors	A DeFi actor's team member is socially engineered or commits an operational mistake that can be exploited	Exploiting operational mistakes, deceiving personnel

<sup>6</sup> <https://de.fi/rekt-database>

<sup>7</sup> <https://hacked.slowmist.io/en/>

<sup>8</sup> <https://cryptosec.com/>

For the set of actors who have not been targeted, 500 random actors listed on DeFi actor aggregator DeFi Llama<sup>9</sup> were considered. We researched these 500 actors on the crime event aggregators introduced above to make sure we retained a set of DeFi actors who had no victimization reported for 2022. Note that we verified that DeFi actors encompassed in our first set (victimized actors) were also listed on the DeFi actor aggregator DeFi Llama leveraged for the second set. This is important, as it reinforces the idea that we compare two sets of relatively similar actors, apart from the fact that some have been victimized and some have not, since all of them successfully registered as DeFi actors on a notable aggregator: DeFi Llama.

Ultimately, we kept victimized (N=113) and non-victimized (N=275) DeFi actors that were also listed on CoinGecko, as this is the cryptocurrency aggregator we leverage to fetch data on DeFi actors. Therefore, DeFi actors who did not appear on CoinGecko were excluded. The final sample thus comprises 388 DeFi actors, for which different attributes could be fetched on CoinGecko.

CoinGecko is an open-source data platform aggregating information that provides an in-depth analysis of the crypto market. Precisely, most active cryptocurrencies are listed on their platform, where various metrics of these assets are displayed, such as their price charts, trading volume, market capitalization, and other relevant information about the protocols these cryptocurrencies are associated with. The platform does so by continuously tracking data from across over 100 different blockchains (e.g., Ethereum, Solana, Avalanche) and over 900 crypto exchanges (e.g., Binance, Kraken) to ensure up-to-date pricing information (*Cryptocurrency Prices, Charts, and Crypto Market Cap*, CoinGecko). To this date and according to the website, data for over 13, 000 cryptocurrencies is available on the platform. CoinGecko also displays retroactive metrics to better understand an asset's evolution, as they keep historical data for all cryptocurrencies. A DeFi actor's search on CoinGecko outputs all assets issued by this actor, like native or utility tokens, governance tokens, or other ERC-20 tokens. However, the most relevant token associated with their protocol will be the first result. While most actors only had one cryptocurrency listed, the first result was prioritized for other actors, as the most relevant token of a protocol is typically tied to the success of the platform.

---

<sup>9</sup> <https://defillama.com/>

Data was collected using CoinGecko’s application programming interface (API) key from a paid plan subscription. Using unique coin API IDs, different endpoints were leveraged with a PHP script to collect the token value, market capitalization, trading volume, chains and markets where the token is available as well as audits and bug bounty programs related to the DeFi actor. For the three former variables, the script indicated to collect daily historical data of 2022. To ensure data accuracy, a sample of 50 random cryptocurrency IDs were reviewed. These IDs were manually searched in CoinGecko, and the information listed on the page had to match the data collected for a given actor. Because this verification demonstrated that the data for 50 tokens was accurately collected, we assume this is the case for the entire sample. The data was then processed to create variables fitting the relevant attributes of target attractiveness. In addition, we collected the main area of operation of the DeFi actor by relying on DeFi Llama’s categorization, as well as manual searches directly on DeFi actors’ websites. This method was previously used by Carpentier-Desjardins et al. (2025) to build the dataset we draw from in this study for victimized DeFi actors. The same categorization as introduced in Table 1 is therefore used for this study. The next section further explains how we created relevant variables in our study from this collected data.

## Dataset Creation and Descriptive Statistics

This section introduces the process behind the creation of each variable we use in our logistic regression models and their relation to the appropriate dimension of target attractiveness. To that end, Table 3 summarizes all variables and definitions, while Table 4 displays their descriptive statistics. We offer below a more detailed explanation of all variables, regrouped under their respective dimensions.

Table 3: Variables and Definitions

Dimension	Variable	Type	Definition
<b>Dependent</b>	Victimized 2022	Binary	The DeFi actor suffered an attack and was victimized in 2022
<b>Propinquity</b>	Chains	Discrete	The number of blockchains the DeFi actor is operating on
	Is on Layer 2	Binary	Is the DeFi actor available on a layer-2 blockchain
	Markets	Discrete	The number of markets the DeFi actor's token is available on
	Is on Main CEX	Binary	Is the DeFi actor listed on the most popular CEX in the dataset
	Is on Main DEX	Binary	Is the DeFi actor's token listed on the most popular DEX in the dataset
	Social media	Discrete	The number of social media the DeFi actor is registered on (e.g., Instagram, Twitter, Medium)
<b>Vulnerability</b>	Past Victimization	Discrete	The number of recorded victimization instances of a DeFi actor prior to 2022
<b>Payoff</b>	Market Capitalization	Continuous	The total market value of a token's circulating supply
	Trading Volume	Continuous	The traded amount of a token in the last 24h
	Token value	Continuous	The market value of a token
<b>Area of operation</b>	Exchange	Binary	The DeFi actor's main area of operation is exchange services
	Lending	Binary	The DeFi actor's main area of operation is lending services
	Dapp	Binary	The DeFi actor's main area of operation is Dapp services
	Composition	Binary	The DeFi actor's main area of operation is composition services
<b>Self-protecting activities</b>	Audits	Discrete	The number of audits conducted on the token prior to 2022
	Has a Bug Bounty	Binary	Is there an active bug bounty program associated with the DeFi actor prior to 2022

As seen in Table 3, we include propinquity, vulnerability, payoff and self-protecting activities as discussed by Cook (1986) for relevant dimensions of target attractiveness in DeFi. We also decided

to add the dimension main area of operation, referring to the main financial service provided by a DeFi actor, as our literature review showed how this attribute can be linked to victimization.

Table 4 : Descriptive Statistics (N=388)

Variables	Min	Max	Mean	Median	SD	%
<b>Victimized 2022</b>						17.99
<b>Propinquity</b>						
Chains	1.00	29.00	2.22	1.00	2.65	
Is on Layer 2						19.21
Markets	1.00	296.00	15.51	3.00	36.34	
Is on Main CEX						43.30
Is on Main DEX						35.67
Social media	0.00	7.00	3.00	3.00	1.61	
<b>Vulnerability</b>						
Past Victimizations	0.00	5.00	0.27	1.00	0.63	
<b>Potential Payoff</b>						
Token Value (USD)	$3.13 \times 10^{-11}$	$2.82 \times 10^4$	$1.72 \times 10^2$	$1.95 \times 10^{-1}$	$1.79 \times 10^3$	
Trading Volume (USD)	$2.32 \times 10^1$	$4.98 \times 10^{10}$	$2.92 \times 10^8$	$1.73 \times 10^5$	$3.20 \times 10^9$	
<b>Area of Operation</b>						
Exchange						33.21
Lending						10.98
Dapp						10.06
Composition						23.17
<b>Self-protection activities</b>						
Audits	0.00	3.00	0.36	0.00	1.62	
Has a Bug Bounty						10.36

The preexisting dataset on crime events allowed to create the binary dependent variable *Victimized 2022*, indicating if the DeFi actor suffered an attack in 2022 or not. Table 4 shows that 17.99% of the total sample (N=388) encompasses DeFi actors who have been victimized in 2022. The rest of the sample is composed of actors who have not suffered a victimization this year.

Independent variables associated with the different target attractiveness dimensions were then created, as summarized in Table 3. For the concept of **propinquity**, we started by collecting, from CoinGecko’s data, the chains the actor was operating on, the markets its token could be bought or traded on and social media platforms the actor was active on. We estimate this data is useful to reflect propinquity, as an actor who operates on various blockchains, markets and social media would be more accessible and visible in the community, consequently reaching more DeFi users and possible offenders. We thus created variables that quantified the number of blockchains, markets and social media each DeFi actor is operating on with discrete variables. The `Chains` and `Markets` variables suggest that certain actors have a weaker presence in the DeFi ecosystem, as the minimum number of blockchains and markets an actor is operating on is one, while the maximum for these variables goes to 29 for chains and rises as high as 296 for markets. The means and medians of these variables stay low, suggesting the average actor is closer to the minimum value. Similarly, the `Social Media` variable also suggests a disparity in terms of propinquity, as the minimum social media platform a DeFi actor is present on is zero, while the maximum is seven. However, the mean and median being 3.00 (std: 1.61) suggests the online presence of actors does not fluctuate as much.

We then considered the qualitative aspect of chains and markets, as smart contract friendly chains seemed at greater risk of victimization, and listings on more reliable and established markets could help protect tokens from market manipulation and disruptions (Chainalysis 2024; Solidus Labs 2023). We thus created three binary variables. The first one `Is on Layer 2`, is a binary variable that indicates if the actor’s token is available on a layer-2 blockchain, which is designed to increase smart contract friendliness. While the `Chain` variable shows that the number of chains an actor is listed on greatly varies, Table 4 demonstrates that only 19.21% are listed on a layer-2 type blockchain. For the second and third variables, we determined the most popular CEX and DEX by identifying the most recurrent market listings in our dataset, and created the binary variables `Is on Main CEX` and `Is on Main DEX`. The former indicates if the token is available to trade on the most popular CEX found in our dataset, and the latest applies the same logic to the most popular DEX. Table 4 informs that a higher proportion of DeFi actors (43.30%) are available on the most popular CEX than on the most popular DEX (35.67%).

After, to operationalize the dimension of **vulnerability**, we once again leveraged the crime events dataset and created the discrete variable `Past Victimization`s. This variable represents the sum of mediatized victimization occurrences of a DeFi actor prior to 2022. From the dataset, victimizations that took place in 2021 and 2020 were summed up. Earlier victimizations were not considered, as not all studied DeFi actors were in operation yet. While most DeFi actors have not been victimized prior to 2022, Table 4 still shows that certain actors have been victimized up to five times between 2020 and 2021.

Related to the target's **payoff** dimension, we relied on CoinGecko's daily financial historical data of 2022, which we collected for market capitalization, token value and trading volume. We estimate the value of a token represents an easy indicator for an offender to approach the cost-benefit calculation of a crime opportunity. While token value is greatly correlated to market capitalization, we created a different variable with this metric, as it includes the total circulating supply, which indicates the broader value of the DeFi actor. Trading volume operationalizes payoff in a less direct way; it indicates if the asset is traded a lot daily, which demonstrates users' interest in the asset and its potential value. The formulas associated with these concepts were presented when discussing potential payoff in the section on target attractiveness in DeFi earlier. For the study, we created the continuous variables `Token Value`, `Trading Volume` and `Market Capitalization`. Each variable indicates the 2022 annual mean of the metric of interest, based on daily 2022 historical data. As seen in Table 4, payoff variables have a relatively high standard deviation (`Token value`:  $1.79 \times 10^3$  and `Trading Volume`:  $3.20 \times 10^9$ ), which shows the token value and trading volume can fluctuate a lot from one DeFi actor to another. In addition, the `Token Value` median of  $1.95 \times 10^{-1}$  suggests that most tokens studied had a relatively low market value throughout 2022, as it represents only \$0.20 USD. It is also important to note that a logarithmic transformation was performed on both variables prior to computing the logistic regression models to reduce skewness and stabilize their distribution. Variables from other dimensions did not undergo this transformation, as their distributions were not highly asymmetrical. As for the `Market Capitalization`, note that it strongly correlated with the `Token Value` (0.84) when computing bivariate correlations. Therefore, we decided to remove one of these variables from further analysis to mitigate multicollinearity; we chose to exclude `Market Capitalization` because it had more missing values (N=147) than `Token Value`

(N=50). In addition, Market Capitalization had a VIF superior to the critical value of five when attempts to include it in logistic regression models were made. Hence, because of its correlation with another variable, its number of missing values, and its VIF score, it was more beneficial not to include it in our model. Bivariate correlations of all variables that are included in our models can be viewed in Annex 1.

The next dimension is the **main area of operation** of the DeFi actor, for which we collected the category of DeFi service the actor was providing on DeFi Llama and determined the main area of operation by conducting subsequent manual searches on the DeFi actor's website. We leverage the same categories introduced in Carpentier-Desjardins et al. (2025), which were summarized earlier in Table 1. Table 1 shows how 12 categories were originally created: blockchain, fungible tokens (FT), non-fungible tokens (NFT), exchanges, lending, derivatives, Dapps, yield, staking, bridges, oracles, and others. For this study, we aggregated some of the categories and excluded others, as it better represented our smaller dataset. In fact, blockchain, FT, NFT, bridges and oracles were all merged into "others", as all these categories had fewer than 30 observations. We then excluded this category from our analysis because it regroups services that are very different from one another. In addition, the yield and staking categories also had fewer than 30 observations individually; they were merged to create the category "composition", as these DeFi services are similar and grouped under the DeFi composition layer of the technical stack. Consequently, we created binary variables of the remaining relevant categories of *Exchange*, *Lending*, *Dapp* and *Composition* to identify the main area of operation of each DeFi actor in our dataset. Table 4 demonstrates that a greater proportion of DeFi actors offer exchange services (33.21%), followed by composition services such as yield and staking (23.17%), then lending (10.98%) and Dapp (10.06%). This distribution is representative of the ecosystem, as exchange and staking services are known to be amongst the most popular and interacted with by users (Auer et al., 2023).

Finally, regarding the **self-protection activities** dimension, data on audits and bug bounties were collected in the "security" section of each token on CoinGecko for all DeFi actors. In fact, these verifications and programs were portrayed as important attack prevention tools in the literature review (Zhou et al., 2022; Chainalysis, 2024). We thus collected the number of audits and the presence of active bug bounty listed on CoinGecko for all actors, as well as the date the audit was

conducted, or the bounty program entered into function. This allowed us to create the discrete variable `Audits` and the binary variable `Has a Bug Bounty`, where the former indicates the number of reported audits that were conducted on the DeFi actor token's smart contract prior to 2022, and the latter whether there was an active bug bounty program associated with the DeFi actor's protocol prior to 2022. Table 2 indicates a low proportion of actors who had an active bug bounty program prior to 2022 (10.36%), and a relatively low mean for `Audits` (0.36) demonstrates that few DeFi actors engaged in visible self-protection activities throughout 2020 and 2021.

## Logistic Regression Analysis

All variables, except for market capitalization, were then used in logistic regression models. This method tests whether independent variables can predict a dichotomous dependent variable's outcome (Desjardins, 2005; El Sanharawi & Naudet, 2013). Hence, logistic regression allows to compute the impact of each selected independent variable on the odds ratio (OR) of an event's occurrence (Sperandei, 2014). The dependent variable is represented by the event as it is binary; the event occurs or does not occur. In our case, the event of interest is victimization in 2022, so our model assesses the influence of all variables encompassed in our DeFi target attractiveness dimensions on the likelihood of a DeFi actor being victimized in 2022.

The variable selection process can be difficult when building a logistic model; it is tempting to collect as many variables as possible and try to identify which ones have a statistically significant relation with the dependent variable (Sperandei, 2014). However, this approach may cause issues. In fact, while more variables can appear statistically significant, researchers need theories and realistic hypotheses to link or explain the influence of those variables on the outcome of the event. Also, a model that contains all possible explanatory variables might hold less statistical power. In that case, some associations between an explanatory variable and the occurrence of an event can be overlooked, as saturated models are not sensible enough to detect them (Sperandei, 2014). To address these concerns, we first base our variable selection process on both crime opportunity theory and existing work on DeFi. Second, we adopt an approach in which we start our regression using a null (empty) model rather than a full (saturated) model.

This means that, instead of including all selected explanatory variables at once, we proceed by testing our dimensions of target attractiveness individually, before computing a model that encompasses everything. Therefore, we start by computing 5 distinct models for each dimension (Model 1: propinquity; Model 2 vulnerability; Model 3: payoff; Model 4: area of operation; Model 5: self-protection activities). These models include the respective independent variables associated with their dimensions (see Table 3 and 4). Afterwards, Model 6 includes all dimensions and their variables, and finally, Model 7 only variables that showed a significant statistical relation to the dependent variable in Model 6. In other words, Model 6 is a full model, while Model 7 is a parsimonious model. We estimate this approach limits the risk of overlooking associations between an explanatory variable and the occurrence of an event. Also, this approach allows us to account for the explanatory power of dimensions individually, which helps us better understand how and to what extent the overall concept of target attractiveness is relevant in DeFi. Finally, a parsimonious model allows us to identify variables that persist, indicating their practical relation to the likelihood of victimization might be the strongest.

All selected variables met the basic logistic regression assumptions, such as the independence of observations, a linear relationship between the natural logarithm of the odds ratio and all continuous explanatory variables, a minimal variance between observations and at least 10 observations per variable, no outlier observations, and the absence of multicollinearity (Desjardins, 2005; El Sanharawi & Naudet, 2013). For the latter, note that all recorded VIF were under the threshold of five, rejecting the presence of multicollinearity in our models. It is also important to note that logistic regression does not require that independent variables be normally distributed or have equal variance between observations (Desjardins, 2005).

Regarding the interpretation of our models, we adhere to a significance threshold of 0.05 ( $p < 0.05$ ). Also, because logistic regression outputs coefficients from which odds ratios (OR) are then calculated for interpretation, it is relevant to discuss the distinction between odds and probabilities, as these terms are often used as synonymous, but are not the same. Probability is the chance of a favorable outcome divided by all possible outcomes (Sperandei, 2014). Odds compare the probability of success to the probability of failure. While probability ranges from 0 to 1, odds range from 0 to infinity. The odds ratio (OR) thus compares two sets of odds. Note that a large OR can still correspond to a small probability, and vice versa (Sperandei, 2014)

Finally, the explanatory power and adequacy of our models are assessed through the McFadden's  $R^2$  (pseudo- $R^2$ ) and Chi2 (chi-square) measures. The McFadden's  $R^2$  compares the result of the likelihood function defined by the model with explanatory variables with the likelihood function found in a model without any explanatory variables (Desjardins, 2005). It ranges from 0 to 1, with higher values indicating a better model. McFadden's pseudo- $R^2$  can also be used to compare different models for the same dataset, which is useful to interpret our seven models and compare the explanatory power of target attractiveness dimensions. On the other hand, the Chi2 measures the difference between the null deviance and the residual deviance to calculate a chi-square test statistic with a p-value, which assesses whether adding explanatory variables to the null model significantly improves the model's fit (Alavi et al., 2020). Ultimately, if the chi-square test statistic is large and statistically significant, it suggests that the model with the explanatory variables provides a better fit compared to the null model.

## Method Limits

Of course, our approach is not devoid of limits. In this section, we introduce three limits that relate to our variables in the context of this study. Understanding these limits early on allows for a better interpretation of the results obtained through our logistic regression models later.

A first limit to this approach is that our model sometimes lacks visibility on elements that were deemed relevant to the probability of being victimized in the literature review. As displayed in Figure 3, all attributes which are not featured in bold were not included in our model. For example, the use of smart contract security tools by DeFi actors' developers and the vulnerability of DeFi actors that can arise from human risks could not be captured and included in the model. In fact, it is impossible to know which security tools are used by DeFi actors to monitor suspicious interactions with their smart contracts, or to know which DeFi actor presents more human risks, as these aspects are not visible to the public. Nevertheless, such omitted variables might influence the Pseudo- $R^2$  score. Subsequent research should seek to collect data on these elements and create variables that could be included in logistic regression models.

The second limit concerns a lack of visibility on descriptive information related to our variables of interest. For example, one variable we use to operationalize the propinquity dimension is social media; we measure the exposure of DeFi actors via the number of social media they have an active account on. Hence, we suggest that an actor who is active on many social media platforms is more exposed to DeFi users. However, we do not account for elements like the number of followers, posts, and engagement, such as likes, comments and views the DeFi actors have on their accounts, which increases their exposure to the DeFi community, as their content directly reaches more users. In fact, through our approach, we risk mistaking a DeFi actor who has five social media accounts with zero followers and no engagement as more exposed than a DeFi actor who has two social media accounts with thousands of followers and a lot of engagement.

A third limit relates to operations behind the creation of payoff variables. In fact, we collected daily historical data of token value and trading volume but ultimately decided to only rely on the annual 2022 mean of these metrics. While this allows us to capture the overall financial performance of the DeFi actor throughout 2022, it could also potentially introduce bias in our results. In reality, tokens are especially known to be volatile, as the crypto market fluctuates frequently. Because of that, DeFi actors might experience a lot of highs and lows over an extended period. Therefore, an annual mean is not necessarily representative of a constant financial state of 2022. For example, DeFi actors who had short periods of impressively high token values might display a higher 2022 annual mean than other actors. Furthermore, when looking at DeFi actors who have been victimized, this approach also captures the state of the actor post-victimization, when a token's value often plummets and its trading volume decreases. It is important to understand and highlight these limits when interpreting payoff variable results, as well as to nuance our statements in the discussion regarding the relation between token value, trading volume and the likelihood of victimization.

Finally, our model does not include control variables. The one attribute that has been widely investigated in DeFi and that is linked to victimization is the presence of technical vulnerabilities. While we assume that DeFi actors that engage in self-protection activities are less likely to have technical vulnerabilities in their protocols, this cannot be verified. There is a possibility that propinquity, payoff and self-protection activities are not as relevant in DeFi as they are in

traditional or regular cybercrime because target attractiveness is rather contingent on technical vulnerabilities, hence the presence of flaws in the DeFi actor's protocol, like coding mistakes in a smart contract. Possibly, tokens smart contracts' code could eventually be scanned in a vulnerability detection tool to distinguish actors whose code appears more secure than actors whose code displays potential vulnerabilities.

## Ethics

The present study entirely relies on open sources, such as cryptocurrency and crime event aggregators, which feed on public data displayed by blockchains. Because blockchain technology is rooted in transparency and decentralization, the accessibility of historical data, transactions, smart contracts, audits and other digital traces is highly facilitated and promoted. In fact, the end goal is to ensure that users have full visibility into how the DeFi actors operate, how their funds are being used, and how rewards are distributed. This transparency is a key reason why DeFi is perceived as more trustworthy than TradFi, which often operates with limited public insight. All DeFi community users are free to actively participate in monitoring the state of the ecosystem. On the other hand, the ecosystem also favors privacy for all users through their pseudo-anonymity. Therefore, all data necessary for this study were gathered in accordance with the ecosystem's principles; we used only public data that exists due to the ecosystem's transparency principle. Other sources consulted to achieve our objectives include DeFi actor websites and blockchain security firm reports that are also of a public nature. We did not seek to deanonymize any DeFi users, nor acquire information on any DeFi actors' individual team members. For these reasons, an ethics certificate was not necessary in the context of this work. Nevertheless, ethics principles have been considered throughout this study. For example, we do not disclose the names of any DeFi actors in our dataset, and we anonymize blockchains and markets present in our variables. Hence, we refer to a variable named `Is on Main CEX` instead of the actual name of the most popular CEX in our dataset. We do the same for the variable `Is on Main DEX`. Similarly, we refer to layer 2 blockchains as `Is on Layer 2` instead of disclosing the name of the blockchains behind this variable. We estimate this ensures that our findings cannot be associated, favour, nor negatively impact specific DeFi actors, blockchains and DeFi markets.

## Results

This section first presents findings from all logistic regression models in Table 5 below. The first five models account for each target attractiveness dimension individually; they each encompass the selected variables that relate to the model's dimension. Model 6 then accounts for variables of all dimensions simultaneously, and Model 7 only retains variables that were statistically significant in Model 6 to present a parsimonious model. In the end, we further describe the results displayed in Table 5 with an emphasis on the evolution of statistically significant variables throughout the models.

Table 5. Logistic Regression Models Predicting the Likelihood of Victimization of DeFi Actors

	<b>Model 1</b>	<b>Model 2</b>	<b>Model 3</b>	<b>Model 4</b>	<b>Model 5</b>	<b>Model 6</b>	<b>Model 7</b>
	<b>OR [CI]</b>	<b>OR [CI]</b>	<b>OR [CI]</b>	<b>OR [CI]</b>	<b>OR [CI]</b>	<b>OR [CI]</b>	<b>OR [CI]</b>
<b>Intercept</b>	0.14*** [0.06-0.27]	0.25*** [0.19-0.34]	0.05*** [0.02-0.16]	0.35*** [0.20-0.57]	0.23*** [0.18-0.34]	0.02*** [0.01-0.135]	0.04*** [0.01-0.14]
<b>Propinquity</b>							
Chains (N)	0.92 [0.74-1.09]					0.85 [0.66-1.05]	
Is on layer 2 (1/0)	1.72 [0.90-3.32]					<b>2.68*</b> [1.28-5.82]	1.41 [0.88-2.22]
Markets (N)	1.00 [0.99-1.01]					0.99 [0.97-1.00]	
Is on main CEX (1/0)	<b>2.63**</b> [1.39-5.06]					<b>2.38*</b> [1.14-5.04]	<b>2.07*</b> [1.00-4.32]
Is on main DEX (1/0)	0.66 [0.33-1.28]					0.64 [0.30-1.33]	
Social media (N)	1.06 [0.88-1.27]					1.00 [0.83-1.22]	
<b>Vulnerability</b>							
Past victimizations (N)		0.484 [0.21-0.92]				<b>0.40*</b> [0.15-0.83]	<b>0.31*</b> [0.12-0.63]
<b>Potential Payoff</b>							
Trading volume (N)			<b>1.12*</b> [1.03-1.23]			<b>1.25**</b> [1.07-1.49]	1.11 [1.00-1.23]
Token value (N)			0.99 [0.81-1.18]			1.02 [0.79-1.27]	
<b>Area of Operation</b>							
Exchange (1/0)				0.50 [0.23-1.05]		0.56 [0.24-1.31]	
Lending (1/0)				1.84 [0.78-4.32]		<b>3.27*</b> [1.25-8.85]	<b>5.10***</b> [2.25-11.65]
Dapp (1/0)				0.29 [0.06-0.94]		<b>0.23*</b> [0.05-0.83]	0.39 [0.09-1.23]
Composition (1/0)				<b>0.29*</b> [0.11-0.72]		0.37 [0.13-1.00]	
<b>Self-Protection activities</b>							
Audits (N)					0.77 [0.44-1.27]	0.80 [0.42-1.41]	
Has a bug bounty (1/0)					0.68 [0.19-1.89]	0.74 [0.18-2.46]	
Pseudo-R <sup>2</sup>	0.04	0.02	0.02	0.06	0.01	0.17	0.12
Chi2	12.11	5.22*	7.15*	18.94***	2.09	51.59***	36.66***

\*: p<0.05, \*\*: p<0.01, \*\*\*: p<0.001, OR: Odds ratio, CI: Confidence interval 95%

The first five logistic regression models show that individually, variables from all target attractiveness dimensions do not seem to significantly influence the likelihood of victimization. In

fact, in **Model 1** relating to propinquity, only `Is on Main CEX` showed a statistically significant relation to being victimized in 2022 ( $p < 0.01$ ; CI [1.39-5.06]). It suggests that the odds of being targeted are about 2.63 [1.39-5.06] times higher for those listed on the most popular CEX in the dataset. However, model adequacy measures (Pseudo-R<sup>2</sup>: 0.04; Chi2:  $p > 0.05$ ) indicate a small explanatory power. Variables from the vulnerability dimension showed no influence on being victimized in 2022, as **Model 2** displays that `Past Victimitizations` was not statistically significant. **Model 3** on the potential payoff dimension shows that the `Trading Volume` is statistically significant ( $p < 0.05$ ; CI [1.03-1.23]), but not the `Token Value` variable. It indicates that for an increase in one unit of trading volume, the chances of being victimized are 1.12 [1.03-1.23] times higher. Once again, the model's adequacy shows, however, little explanatory power (Pseudo-R<sup>2</sup>: 0.02; Chi2:  $p < 0.05$ ). **Model 4** on the added main area of operation dimension displays a little higher explanatory power (Pseudo-R<sup>2</sup>: 0.06; Chi2:  $p < 0.001$ ), but only one variable accounts for this statistical relation; the DeFi actor being a `Composition` ( $p < 0.05$ ; CI [0.11-0.72]). It translates into DeFi actors offering composition services being 71% [0.11-0.72] less likely to be victimized. Other areas of operation, like `Exchange`, `Lending` and `Dapp` showed no significant statistical relation to the likelihood of victimization. Finally, variables from **Model 5** on self-protection activities, like `Model 2` on vulnerability, showed no influence on victimization, as both `Audits` and `Has a Bug Bounty` were not statistically significant.

When assessing all variables together in **Model 6**, at least one variable from each dimension, except the self-protection dimension, is significant. Specifically, both `Audits` and `Has a Bug Bounty` from the self-protection dimension remain non statistically significant. However, `Past Victimitizations`, from the vulnerability dimension is statistically significant ( $p < 0.05$ ; CI [0.15-0.83]). Here, each past victimization occurrence decreases the chances of being revictimized by 60% [0.15-0.83]. Similarly, `Is on layer 2` ( $p < 0.05$ ; CI [1.28-5.82]) is significant, as being accessible on a layer 2 blockchain now increases the chances of being victimized by 2.68 [1.28-5.82]. The same is observed for two variables in the main area of operation dimension: `Lending` ( $p < 0.05$ ; CI [1.25-8.85]) and `Dapp` ( $p < 0.05$ ; CI [0.05-0.83]). In those cases, offering lending services would increase the chances of being victimized by 3.27 [1.25-8.85], while providing Dapp services would decrease the chances of being victimized by 77% [0.05-0.83]. Note, however, that

Composition, which was statistically significant in Model 4 (main area of operation) is not statistically significant in Model 6. Finally, this model also features variables that were previously statistically significant in individual models and still are in Model 6: *Is on Main CEX* ( $p < 0.05$ ; CI [1.14-5.04]) and *Trading Volume* ( $p < 0.01$ ; CI [1.07-1.49]). In this model, the odds of being targeted are about 2.38 [1.14-5.04] times higher for those listed on the most popular CEX, while an increase in one unit of trading volume increases the chances of being victimized by 1.25 [1.07-1.49]. Overall, Model 6 presents a better Model adequacy than the previous individual ones (Pseudo- $R^2$ : 0.17; Chi2:  $p < 0.001$ ), indicating that when accounted for altogether, variables from dimensions of target attractiveness do contribute to explaining the likelihood of DeFi actors being victimized in 2022.

When computing the parsimonious **Model 7**, only three variables keep their significant statistical relation to being victimized in 2022: *Is on Main CEX* ( $p < 0.05$ ; CI [1.00-4.32]), *Past Victimitizations* ( $p < 0.05$ ; CI [0.12-0.63]) and *Lending* ( $p < 0.01$ ; CI [2.25-11.65]). The significance of *Trading Volume* and *Dapp* disappears. The parsimonious model therefore indicates that *Is on Main CEX*, *Lending* and *Past Victimitizations* had an influence on the chances of victimization of DeFi actors in 2022. In fact, the odds of being targeted are about 2.07 [1.00-4.32] times higher for those listed on the most popular CEX in the dataset. As for categories of DeFi services, the odds of being targeted are more than 5 [2.25-11.65] times higher for those providing lending services. Finally, for each past victimization occurrence a DeFi actor experienced in 2021 and 2020, the chances of being victimized in 2022 decrease by 69% [0.12-0.63]. While this model has less explanatory power (Pseudo-  $R^2$ : 0.12; Chi2:  $p < 0.001$ ) than Model 6, and a Pseudo- $R^2$  lower than the common desired threshold of 0.2-0.4, Model 7 allows us to single out which variables have the most stable influence on the likelihood of victimization. The lower Pseudo- $R^2$  score could partially be explained by omitted variables, which are further discussed in the next section.

Overall, variables from the propinquity, vulnerability and area of operation dimensions appear to be the most related to the likelihood of victimization. Variables from the payoff dimension cannot totally be overlooked, as *Trading Volume* was relevant in both Model 3 and 6. On the contrary, variables from the self-protection activities dimension appear the less related, as they were the

only ones found not statistically correlated to being victimized in 2022 across all models. The section below further discusses the practical implications of these findings. Note that the key takeaways we discuss are rooted in results obtained in Model 7, and sometimes in Model 6 presented in Table 5 above. We focus on Model 7 as we estimate it reflects which variables have the most stable influence on the likelihood of victimization, and consider findings from Model 6 as it offers the best model fit with a Pseudo-R<sup>2</sup> of 0.17. While a Pseudo-R<sup>2</sup> between 0.2 and 0.4 is typically favorable, we deem that findings from both Model 6 and 7 are relevant and can be interpreted to further the understanding of DeFi crime opportunities, as the primary goal of studies with a social science approach is not to predict a precise behavior, but rather to assess whether specific predictors have a statistically significant effect on an outcome variable (Ozili, 2023). Hence, a pseudo-R<sup>2</sup> value around 0.1, such as Model 7's Pseudo-R<sup>2</sup> score of 0.12, can still be considered acceptable if multiple predictors are statistically significant and the model aligns well with theoretical expectations (Ozili, 2023).

## Discussion

Previous studies which took an interest in DeFi crime opportunities have focused on understanding how attacks unfold. In that sense, they sought to identify all possible technical vulnerabilities, different types of attacks and malicious transaction patterns in the DeFi space (Zhou et al., 2022; Ghaleb, 2022; Qian et al., 2022; Werner et al., 2022). To move beyond how attacks unfold, this study involves the theoretical framework of target attractiveness developed in the field of criminology to better understand the distribution of victimizations amongst DeFi actors. The application of target attractiveness dimensions to DeFi actors, combined with statistical results obtained from logistic regression models, provides a first comprehensive and informative assessment of what makes a DeFi actor an attractive target within the DeFi ecosystem. We present below the key takeaways from this study, how they are embedded with previous studies, and how they practically impact DeFi actors. In order, we discuss how past victimizations can prevent subsequent victimizations in the DeFi ecosystem, how increased exposure can negatively impact DeFi actors, how lending services can be considered more attractive to offenders, how community engagement can contribute to the creation of DeFi crime opportunities, and finally, how DeFi self-protection activities can fail to be effective given certain circumstances.

### Past Victimizations Preventing Subsequent Victimizations

Our results show that in the DeFi ecosystem, DeFi actors who were previously victimized in 2020 or 2021 were less likely to be revictimized in 2022. In fact, one past victimization decreases the chances of victimization in 2022 by 69% ( $p < 0.05$ ; CI [0.12-0.63]). This result is contradictory to existing work, as Holt et al. (2017) suggested that prior victimizations could put a target in a vulnerable state, which offenders would take advantage of, facilitating revictimization. This was also discussed by Chainalysis (2024) regarding DeFi specific crimes, as the firm observed some DeFi actors being revictimized shortly after they were attacked because offenders could exploit unresolved vulnerabilities multiple times. Similar challenges were observed in the form of contagion, as victimizations of some DeFi actors can subsequently put other DeFi actors at risk of victimization due to protocol composability between these actors (Chainalysis, 2024). One could then expect that past victimizations would increase the likelihood of victimization, which is not what our results indicate. One explanation could be that post victimization, DeFi actors are

incentivized to quickly engage in self-protection activities to patch vulnerabilities and reinforce their contracts' security to stop or alleviate further financial losses. Consequently, while revictimization shortly after an attack is an undeniable risk for DeFi actors during the timeframe vulnerabilities or loopholes are being fixed, the self-protection activities they must engage in to fix the current issues probably contribute to the mitigation of revictimization in the following year, explaining why a victimization occurrence would decrease the likelihood of being revictimized in the long term. This would also explain why past victimizations prevent subsequent victimizations in DeFi, but not necessarily in more traditional crimes like robberies; there is a form of urgency to patch smart contracts with known technical vulnerabilities, while victims of robberies might perceive self-protection measures as optional or non-urgent if no specific vulnerability is identified as the cause of their victimization. In addition, DeFi actors have a sense of responsibility towards their community of users, as they provide financial services and sometimes host large sums of assets in their contracts; it is in their best interest to take all necessary precautions to avoid other attacks and maintain the trust of their user base. To verify the link between past victimizations and self-protection activities, it would be relevant to investigate how DeFi actors publicly reacted to their attack, as many of them, for the sake of transparency, publish detailed mortem analysis as well as social media posts to update their user base on what they did to secure the services they offer and what steps will be taken next. These sources might provide valuable data to assess if the self-protection measures adopted post victimizations are a contributing factor to preventing revictimization in the following year.

Finally, this dynamic relation between vulnerability and self-protection activities would also suggest that offenders are rather opportunistic; they quickly move on to targets who display active vulnerabilities or loopholes in their protocols, dismissing actors who effectively secured their protocols post victimization. Hence, the other attributes beyond past victimization that are encompassed in the vulnerability dimension, like technical vulnerabilities and human risks, as shown in Figure 3, might be important omitted variables in this study. In that sense, an opportunistic offender would also take advantage of overlooked technical vulnerabilities of DeFi actors that have not yet been victimized, or take advantage of a team member's operational mistake or security negligence. Consequently, increasing visibility on smart contract source codes and teams behind DeFi actors might help better understand to what extent offenders in the DeFi space

are opportunistic. Scanning smart contract source codes with vulnerability detection tools to uncover the presence of potential vulnerable code lines should be prioritized in future research to account for technical vulnerabilities in statistical models. In addition, human risks could potentially be explored and accounted for by collecting information on DeFi actors' team members when possible. For example, a singular developer might not represent the same level of human risks as a team of multiple developers, contractors and stakeholders.

## The Negative Side to Increased Exposure

Our results also show that DeFi actors who listed their token on the most popular CEX found in the dataset had 2.07 [1.00-4.32] more chances of being victimized in 2022. This is in accordance with previous work on cybercrime which has linked increased visibility and accessibility to being an attractive target in online spaces, as it increases exposure to offenders (Holt & Bossler, 2015; Leukfeldt & Yar, 2016). Therefore, while providing accessibility to a larger pool of traders and increasing liquidity can enhance overall market efficiency (Chainalysis, 2024), our results suggest that the exposure associated with tokens being listed on the most popular CEX also increases the likelihood of victimization for DeFi actors. Note, however, that the same effect was not observed in our results regarding the most popular DEX in the dataset. The exposure gained by listing tokens on a popular DEX does not seem to affect the likelihood of being victimized, as listing tokens on a popular CEX does. We suppose this difference could be explained by the inherent characteristics of DeFi, which differ from CeFi's. In fact, CeFi platforms such as CEXs are necessary intermediaries between TradFi and DeFi. Therefore, CeFi actors and their services are amongst the most interacted with; most cryptocurrency trading happens off chain on CEX, which could explain the higher level of visibility and exposure they bring to DeFi actors' token listings (Auer et al., 2023). In addition, the CeFi industry often suffers from their centralized structure, as hackers can focus on a single point of failure to target them, which has led to more financial losses (\$19.5B USD) than DeFi (\$10B USD) between 2017 and 2022 (Carpentier-Desjardins et al., 2025). These characteristics reinforce the idea that more exposure is gained with CEX listings as opposed to DEX listings, which could partially explain why we observe a relation between a token being listed on the most popular CEX and the likelihood of victimization, but no relation when it comes to the most popular DEX. It is important to note, however, that our study does not consider which markets were leveraged to conduct the attacks. In fact, we only considered which markets the token

was accessible on, but this does not imply that these entities were involved in or facilitated the attack. For example, a DeFi actor's token could be available to trade on the most popular CEX, but have been targeted through a different market. Further investigations could include more qualitative variables such as the type of attack to better understand the relation between CEXs and the likelihood of being victimized. In fact, some attacks, like infrastructure hacks and price manipulations, are more likely to involve CEXs, while others, like smart contract exploits and transaction front-running, rather concern DEXs (Hägele, 2024). Considering types of attacks might help clarify how exposure gained from CEXs or DEXs influences the likelihood of victimization.

Similarly, our results also indicate, in Model 6, that being listed on a layer 2 blockchain increases the chances of being victimized by 2.68 [1.28-5.82]. While this result does not hold in the parsimonious model, it still provides insight into the likelihood of being victimized, as Model 6's adequacy and explanatory power are the highest. This result is also in accordance with the literature, as characteristics of specific chains, especially popularity and smart contract friendliness, were linked to victimization (Chainalysis 2024; Solidus Labs 2023). As Layer 2 chains are designed to better accommodate smart contracts, and are particularly popular because of their cost-efficiency approach, it was expected that they could contribute to the likelihood of being victimized. In that sense, the exposure and user base DeFi actors gain from being present on a Layer-2 blockchain might contribute to also increasing their perceived attractiveness through the eyes of offenders, which then increases their likelihood of being victimized. Our study considered if DeFi actors were listed on a layer 2 blockchain, but did not consider which specific chain or if the attack occurred on this chain. For this reason, and the fact that this variable was only statistically significant in Model 6, more research should be conducted on layer 2 blockchains to better understand the relation between these chains and the likelihood of victimization.

## Lending Services as Attractive Targets for Crime in DeFi

Lending services were also shown to be related to the likelihood of victimization, as DeFi actors who offer lending services were found to have 5.10 [2.25-11.65] more chances of being victimized in our parsimonious model. This result partially aligns with that of other work, as Zhou et al. (2022) presented evidence that yield farming (\$868M) bridges (\$860M), and lending (\$485M) protocols were the areas of operation that suffered the most financial damage. Protocols who suffer more

damage, like lending services, might therefore be perceived as attractive targets in the eyes of offenders, as they associate these targets with a higher potential payoff. However, our results do not show that compositions (including yield farming) increase the likelihood of victimization, which is contradictory to what Zhou et al. (2022) presented. Also, we could not verify the relation between interfaces like bridges and oracles and the likelihood of victimization, as such services were included in the “others” category, which was excluded from the dataset due to a lack of observations. More recently, Carpentier-Desjardins et al. (2025) found that DeFi actors offering services on the protocol layer of the DeFi technical stack (e.g., exchange, lending, Dapp and derivatives) suffered more crime events (N= 298) and more total financial losses (\$2.6B\$) from 2017 to 2022. While this finding suggests that lending services are amongst the most targeted ones, it also implies that other services like Dapps and exchanges could increase the likelihood of victimization, a result which we did not observe in this study. In fact, the current study rather suggests that Dapp services would decrease the likelihood of victimization, which will be further discussed below. Nonetheless, one reason why only lending services stand out from other DeFi actors on the protocol layer (exchange and Dapp) in our study might be because of the nature of the service. In fact, when interacting with DeFi actors who offer lending services, users can leverage strategies to facilitate their operations and maximize their profit, such as flash loans (Qin et al., 2021). Flash loans allow borrowing capital without providing collateral if the assets are returned by the end of the transaction (Qin et al., 2021). Such tools are not accessible in traditional finance systems due to regulations. In the context of crime opportunities, flash loans can be leveraged to fund attacks on Defi actors, making costly attacks more accessible and ultimately more rewarding in terms of profit. In fact, while flash loans can be used to simply benefit from arbitrage opportunities, they are frequently used to distort the state of the market by artificially inflating assets’ prices, manipulating oracles, or maximizing the potential payoff of a smart contract exploit (Qin et al., 2021). Hence, flash loans were found to give adversaries instant access to billions of USD, costing them only minor upfront costs: the transaction fees (Qin et al., 2021). Flash loan funded DeFi attacks have caused a total loss of over 100M USD to victims in the year 2020 alone (Qin et al., 2021; Qin et al., 2021a). This suggests that lending services could increase the likelihood of victimization because they support operations like flash loans, which makes them more attractive through the eyes of offenders. In addition, this also suggests that in DeFi, offenders can have a more active role in the creation of crime opportunities, as they can themselves modulate

the attractiveness of a target with secondary tools like flash loans. To further develop our findings, a rightful approach would be to identify attacks that were flash loan funded and assess if they disproportionately affect DeFi actors who offer lending services, and if they individually affect the likelihood of victimization.

Another of our results concerns Dapps, as they were found to decrease the chances of being victimized by 77% [0.05-0.83] in Model 6. While this result is not maintained in the parsimonious model, it still gives relevant insight into how the main area of operation can relate to the likelihood of victimization. While Dapps are part of the protocol layer of the DeFi technical stack, which was identified as the most targeted layer by Carpentier-Desjardins et al. (2025), it is important to note that Dapps possess key differences to other DeFi protocols encompassed in this layer, such as exchange and lending. For one, Dapps typically do not focus as much on finance as other protocols do. In fact, Dapps rather leverage distributed ledger technology and tokens to deploy protocols that relate to gaming, storage, and social platforms, as described in Table 1 (Brown & Logan, 2024). While these services still require tokens and involve transactions, offenders might not perceive them as attractive targets, as they do not revolve around finances. In other words, Dapps might not be where malicious users look when searching for attractive targets; they have less exposure than common financial services, and they might not appear to offer a high potential payoff due to the nature of the services they provide. Further disaggregating Dapps into smaller categories, such as gaming, storage and media, could help us better understand if all Dapps or specific categories of Dapps decrease the likelihood of victimization.

## The role of Community engagement in the Creation of DeFi Crime Opportunities

While no variables relating to the potential payoff dimension remain in the parsimonious model, we note that the trading volume was still statistically significant ( $p < 0.01$ ; CI [1.07-1.49]) in Model 6 when assessing all variables together. This indicates that, to some extent, a higher trading volume, which relates to more transactions involving a DeFi actor's token being conducted daily, could increase the likelihood of victimization. However, confidence intervals are close to one, suggesting a small practical impact of trading volume on victimization. Also, because the relation

between this metric and the likelihood of victimization does not persist in Model 7, its effect size might be less important than that of other variables discussed above.

We did expect the potential payoff to increase target attractiveness, as Zhou et al. (2022) and Holt et al. (2017) explained a target's value was a key factor in offenders' motivation. However, in our study, only the trading volume showed a significant statistical relation to victimization, while the variable measuring the potential payoff more directly, the token value, did not show such a relation. Rather than a direct payoff measure, a high trading volume indicates strong interest and engagement from traders, while low trading volume may indicate less interest or liquidity in the market. We suggested that more trades should generate more crime opportunities for offenders, which is what our results support. This suggests that in DeFi, monitoring community engagement might be more beneficial than monitoring tokens' value to assess the likelihood of victimization. This reinforces the relevance of considering the configuration of the virtual space when investigating target attractiveness, like Miró-Llinares et al. (2020) emphasized, as dynamics between offenders and victims can change from one space to another. It also further supports the proposition that offenders in the DeFi space are rather opportunistic, as victimization seems to occur more frequently when a DeFi actor's user base is more active, and its token is being traded a lot. In fact, the trading volume reflects community engagement and interest towards an asset. This directly relates to the notion of supply and demand for crime opportunities introduced by Cook (1986), as potential offenders would seize crime opportunities where they are provided. In that case, the DeFi actor's user base would provide higher crime opportunities by raising interest and drawing attention to a specific token.

More information is needed on DeFi actor's trading volume to verify the nature of this variable's relation with the likelihood of victimization. For example, our study relied on the 2022 annual mean of the trading volume to obtain this result, which does not consider the fluctuation of the metric throughout the year, and ignores how a victimization usually negatively affects the trading volume after the event, therefore decreasing its annual mean. Subsequent analysis should aim at removing this bias by only considering the trading volume prior to the attack to better capture if the metric is linked to the outcome of the event. In addition, it could be relevant to further investigate how the broader concept of community engagement relates to target attractiveness in DeFi. Different variables reflecting the community engagement level of DeFi actors, such as the

number of followers, likes, shares, and comments on their social media channels, could provide insights into community sentiment and interest levels surrounding a token. Finally, on-chain data like the number of active addresses, transaction volume, transaction frequency, and transaction value could also provide insights into usage patterns, which would reflect community engagement.

## The Effectiveness of Self-protection Activities in DeFi

Finally, it is also important to address variables that were expected to influence the likelihood of victimization but ultimately didn't according to our result. Indeed, both variables relating to self-protection activities, such as audits and bug bounty programs, were not statistically significant in this study, meaning that they would not decrease the likelihood of victimization for DeFi actors who had implemented them. This contradicts Cook's perspective that engaging in self-protection activities would decrease target attractiveness, as well as existing work's findings on DeFi-specific self-protection activities, which indicated that smart contract security audits could decrease victimization occurrence by a factor of four, and that maintaining an active bug bounty program could contribute to mitigating external attacks (Zhou et al., 2022; Breidenbach et al., 2018).

Several explanations as to why our results differ from these statements can be considered. First, as it relates to audits, our variables only quantify them, but do not account for the quality of those measures. For example, two audits might have been conducted on a DeFi actor's smart contract, but if the firms who performed the audit are not reliable, or if the security scores obtained through said audits were poor, it would be inadequate to expect those self-protection measures to efficiently protect the DeFi actor against victimization. Complementary qualitative information on audits that were conducted could shed light on different insights. In addition, note that we have no way of assessing the quality of the developers who programmed the smart contracts; some may be inexperienced and leave vulnerabilities that are easily accessible, while others may have coded far more secure contracts. Hence, not all smart contracts that have not been audited can be considered as equally vulnerable. Some DeFi actors' contracts might still be relatively secure even if they overlooked self-protection activities like audits because they relied on experienced reliable developers. Consequently, it might not be reasonable to expect the absence of audits to always influence the likelihood of victimization. Secondly, we only recorded the presence or absence of an active bug bounty program, with no regards to its terms and conditions. For example, we do not

consider the maximum bounty that DeFi actors allocate to users reporting bugs. However, this information could be relevant, as bug bounty measures are sometimes criticized because they require impressive financial rewards to attract economically rational hackers. In fact, in cases where the program offers insufficient financial incentives, it can be more profitable for a profit-driven DeFi user to exploit the vulnerability he uncovers rather than to disclose it and collect the bounty (Breidenbach et al., 2018). For example, Allodi (2017) previously observed this situation in the context of exploits sold by vendors in underground forums, as they were priced somewhat similarly, sometimes above what is offered through bug bounty rewards. This suggests that individuals who identify vulnerabilities would gain more from participating in the cybercrime economy than moving to legitimate vulnerability reporting markets. Similarly, some bug bounty programs might very well be ineffective in decreasing a DeFi actor's perceived target attractiveness by offenders, which is something our model unfortunately cannot account for. Finally, another reason why our results show no relation between self-protection activities and the likelihood of victimization might be because our model lacks visibility on smart contract security tools, as considered in Figure 3. In fact, data on whether DeFi actors leverage smart contract security tools and which ones they rely on could not be collected. However, such tools like EVM-Shield were shown to greatly help DeFi actors manage malicious transactions in real time, facilitating attack mitigation responses (Zhang et al., 2024). In that sense, it is possible that contract security tools are more effective than other self-protection activities like audits and bug bounty programs to prevent victimization, but that our model was unable to capture this phenomenon.

Considering these explanatory avenues, subsequent research should prioritize variables like the reputation of the security firms who performed audits, the security score obtained from audits, the financial rewards allocated by bounty programs, as well as smart contract security tools leveraged by DeFi actors to better understand the effectiveness of self-protection activities in the DeFi space, and how they relate to target attractiveness and victimization.

## Bridging Disciplines: Integrative Dimensions of Criminology and Forensic Science

The integration of criminology and forensic science is beneficial to understanding and addressing criminal activities in both physical and virtual environments. By combining these fields of study, it becomes possible to develop a more comprehensive framework for analyzing crime patterns, reconstructing criminal events, and identifying attractive targets in the DeFi space. In this study, digital traces, derived from blockchains and DeFi actors' online presence, provide a wide range of data, while criminology theories offer relevant frameworks to detect and select which traces amongst said data are relevant to interpret to investigate crime opportunities and explain the dynamics of victimization within the DeFi ecosystem. Relevant traces are those which are linked to the event of interest, and which potentially provide information on their source and the activity from which they originate, hence why it is important to distinguish them from other surrounding traces (Bitzer et al., 2021). Hence, the integrative approach to this work lies in the fact that we leverage criminology insights to better locate, observe, measure and collect relevant traces in the environment of interest. In fact, the investigation of a crime scene, including the discovery of traces, as well as filtering out traces that are not relevant, is the second step of the forensic method known as the hypothetico-deductive cycle as detailed by Ribaux (2023). At this stage, different factors can influence the detection of traces, such as knowledge, experience and professional background (Ribaux, 2023). For example, authors from the computer science field deemed, in previous studies, technical vulnerabilities and transaction patterns relevant traces, but we rather selected traces associated with the dimensions of target attractiveness derived from criminology as relevant to investigate. Ultimately, this demonstrates the importance of collaboration and the exchange of information to find as many relevant traces as possible to paint a more complete picture of a given event. Our study considers both forensic science and criminology to paint a more accurate picture of crime opportunities in DeFi, as well as to better understand what makes some DeFi actors more attractive targets than others. As previously stated, existing work mainly interprets digital traces relating to DeFi crimes with computer science methodologies. While these approaches provide relevant insights, their content is often limited to identifying technical vulnerabilities and malicious transaction patterns, but fails to describe the crime opportunity landscape in DeFi and explain why some DeFi actors are more likely to fall victim to these

opportunities than others. In the next section, we further explain how integrating criminology with forensic science brings us one step closer to answering these questions.

First, criminal activities produce traces that can be analyzed to reconstruct events (Ribaux, 2023). In the DeFi space, blockchains serve as virtual environments where digital traces, such as historical transaction data, provide critical insights into criminal activities. These traces then reveal additional information on perpetrators and victims, as addresses involved in transactions are public. Traces are therefore fundamental to forensic analysis, as they provide the most direct and concrete data for reconstructing criminal activities. In the context of DeFi, the characteristics of Distributed Ledger Technology (DLT) used in blockchains enhance the potential of traces, making them particularly valuable for studying criminal behaviours. In fact, blockchain technology is notably defined by transparency, which ensures constant public access to all traces within the ledger. Also, its immutability guarantees that transactions, once recorded, cannot be altered nor deleted, preserving the integrity of traces through time. Consensus mechanisms validate transactions through algorithms that ensure the accuracy and reliability of data, which can't be tampered with by a central authority. In addition, auditability allows for a traceable and unalterable record of all transactions, facilitating audits, compliance and integrity checks. Finally, decentralization eliminates the possibility of a single point of failure, strengthening the reliability of observed traces. From a forensic perspective, these features are crucial, as they greatly limit the degradation of traces, and they prevent their pollution and contamination post crime event, which are common challenges in crime reconstruction and investigation (Weyerman & Ribaux, 2012; Margot, 2014). Ultimately, enhanced reliability of observed traces lowers the uncertainty rate in different stages of investigations and criminal reconstructions, which contributes to a more adequate interpretation of traces. In fact, forensic science deals with a continuum of uncertainties at different stages, including trace production, detection, selection and reconstruction, which can ultimately affect the overall interpretation of a crime even (Roux et al., 2022). While it is not possible to eliminate uncertainties entirely, blockchain technology alleviates some of them, as it is designed to preserve the integrity of the information it records. Hence, relying on digital traces rooted in blockchain technology, plus orienting the selection of traces with empirical data on target attractiveness in criminology, allows for a more accurate selection of traces that are relevant, and ultimately for a better interpretation of crime events.

We estimate that criminology provides the necessary theoretical frameworks to contextualize the digital traces that relate to DeFi crimes, as it typically seeks to understand dynamics surrounding criminal activities, victims and perpetrators. For example, as investigated in this study, the dimensions of an attractive target as developed by Cook (1986) are relevant to interpret the significance of digital traces that relate to victims (DeFi actors). Indeed, we can associate traces like their historical data on various financial metrics with potential payoff, traces showing activities like audits and bug bounties with self-protection, and traces of previous attacks with vulnerability. Combining disciplines then clearly leads to a more precise understanding of how offenders can perceive DeFi actors as potential victims.

Second, detecting repetitive patterns in crime events is essential for understanding phenomena like victimization distribution, which can be better achieved by relying on both forensic science and criminology. Indeed, crimes are not randomly distributed; they tend to follow patterns of offending and victimization. One of the fundamental roles of traces is to establish a connection between a criminal and a victim (Ribaux, 2014; Ribaux, 2023). In this study, we identify patterns of victimization to determine why offenders perceive some targets as more attractive. These patterns stem from the logistic regression models conducted with attributes of potential targets in the DeFi ecosystem, which were identified through relevant digital traces. In fact, from digital traces, we concluded that victimized DeFi actors tend to be accessible on popular CEX and offer lending services, while those who have previously been victimized tend not to suffer another victimization in the upcoming year. Identifying such repetitive patterns informs us on the distribution of crime within the DeFi environment. Nonetheless, the use of digital traces, joined with principles of criminology, allowed for a more structured approach to identify and interpret these patterns, ensuring that digital evidence is contextualized within broader criminological understandings of crime trends and offender decision-making.

Finally, criminology and forensic science can jointly enhance both repressive and preventive security actions against crime. In fact, identifying repetitive victimization patterns is a crucial step in developing effective preventive measures to mitigate victimization in the DeFi space. By analyzing digital traces, it becomes possible to identify which DeFi actors' attributes relate to the

likelihood of victimization, and design security interventions tailored to these specific attributes. The integration of criminology with forensic science ensures that crime prevention strategies are based on both digital empirical evidence and theoretical insights, leading to more targeted and effective responses. Our study underscores the importance of DeFi digital trace analysis in understanding crime opportunities and identifying attractive targets, which ultimately contributes to improving how we approach crime mitigation in this ecosystem. For example, while developing prevention measures was not the prime objective of this study, our results suggest that monitoring changes in digital traces behind specific attributes (accessibility on CEX, type of DeFi service offered and past victimizations) could help identify DeFi actors at risk. In addition, a DeFi actor's concerns with attack prevention, as well as self-protection, should be proportional to its exposure on CEXs and the types of service they offer to DeFi users.

## Conclusion

In this study, we applied the theoretical framework developed by Cook (1986) concerning crime opportunities and target attractiveness to victimizations occurring within the DeFi space. Our objective was to assess which attributes of DeFi actors are associated with the likelihood of victimization. Building on prior research, we argue that traditional dimensions of target attractiveness, namely propinquity, vulnerability, potential payoff, and self-protection activities, commonly used in studies of both physical and cybercrime, are also applicable in DeFi contexts. Furthermore, drawing on prior studies and adapting to the specific characteristics of DeFi ecosystems, we proposed an additional dimension, area of operation, as a determinant of target attractiveness and, consequently, of victimization.

For each dimension, we identified relevant attributes of DeFi actors, such as the blockchains and markets they are active in, their trading volume, history of past victimizations, and the presence of audits. These were translated into variables included in our statistical model. We then developed logistic regression models to test the relationship between these attributes and the likelihood of victimization, using real-world historical data from CoinGecko, as well as incident records previously collected by Carpentier-Desjardins et al., (2025), who leveraged the DeFi crime aggregators De.Fi, Slowmist, and CryptoSec.

Our results suggest that certain attributes significantly influence the probability of victimization. Specifically, listing a token on a major centralized exchange (CEX), engaging in DeFi lending services, and having a history of prior victimizations were found to influence the likelihood of being targeted. Additionally, variables such as trading volume, which can be seen as a proxy for community engagement, and operating on layer-2 blockchains, showed potential associations with victimization risk, although their effect sizes appeared more modest. These findings support the idea that criminological concepts, including exposure, repeat victimization, and areas of activity, are useful for understanding crime patterns in DeFi and should be integrated into analysis typically dominated by computer science approaches. In fact, beyond keeping an eye open for possible technical vulnerabilities, DeFi actors that have a high level of exposure on popular CEXs, and/or offer lending services should make sure they invest in self-protection measures of quality. For

example, they should prioritize relying on more reputable cybersecurity firms to conduct audits on their smart contracts.

Consequently, our study advocates for a multidisciplinary approach to DeFi-related crime research. Perspectives from criminology, computer science, and forensic science each offer valuable insights into how crime opportunities emerge and how digital traces can inform investigation and prevention strategies. Our findings emphasize that looking beyond technical vulnerabilities, mainly by incorporating socio-structural and behavioral attributes of DeFi actors, can lead to a more holistic understanding of victimization patterns in decentralized ecosystems.

Future research should also seek to expand on our findings by incorporating variables omitted from our current model and by integrating more qualitative data to better capture all dimensions of target attractiveness. As previously discussed, our model does not currently account for smart contract security tools, human behavior-related risks, or specific technical vulnerabilities. While we included quantitative measures, such as the number of audits and bug bounties, we did not assess the quality of these protections, for example, the reputation of the auditing firms, the outcomes of the audits, or the scale of financial incentives offered through bounties.

In sum, our study suggests that adopting traditional crime theories in the cryptoasset industry can help better interpret digital traces of these virtual spaces and lead to the development of more accurate DeFi-specific victimization models. Such models may not only deepen our understanding of how and why DeFi actors are targeted, but also contribute to the design of more effective attack mitigation measures. Importantly, our findings suggest that effective safeguards should go beyond identifying and securing technical vulnerabilities in DLT and smart contracts to prevent DeFi crime. Instead, they should account for broader dimensions such as propinquity, vulnerability (which includes technical vulnerabilities), potential payoff, and self-protection activities. This approach can offer a more holistic and effective framework for reducing DeFi crime opportunities, as together, these dimensions shape target attractiveness and influence the likelihood of victimization in DeFi environments.

# Bibliography

Alavi, M., Visentin, D. C., Thapa, D. K., Hunt, G. E., Watson, R., & Cleary, M. (2020). Chi-square for model fit in confirmatory factor analysis. *Journal of advanced nursing*, 76(9), 2209-2211.

Allodi, L. (2017, October). Economic factors of vulnerability trade and exploitation. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, 1483-1499.

Altschuler, S. (2022). Should centralized exchange regulations apply to cryptocurrency protocols? *Stan. J. Blockchain L. & Pol'y*, 5, 92.

Andryukhin, A. A. (2019, March). Phishing attacks and preventions in blockchain based projects. In 2019 international conference on engineering technologies and computer science (EnT) (pp. 15-19). IEEE.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2023). The technology of decentralized finance (DeFi). *Digital Finance*. <https://doi.org/10.1007/s42521-023-00088-8>

Awan, M. S. K., & Dahabiyeh, L. (2018, April). Corporate attractiveness index: A measure for assessing the potential of a cyber attack. In 2018 9th International Conference on Information and Communication Systems (ICICS) (pp. 1-6). IEEE.

Bitzer, S., O. Ribaux, E. Lock, N. Albertini et O. Delémont (2021) « La décision d'analyser une trace dans l'enquête : étude empirique des traces biologiques dans les cas de vol avec violence », *Revue internationale de criminologie et de police technique et scientifique* 75, pp. 104–126, <https://www.aiclf.net>

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection : An Examination of Routine Activities Theory. 3(1).

Breidenbach, L., Daian, P., Tramer, F., & Juels, A. (2018). Enter the Hydra : Towards Principled Bug Bounties and {Exploit-Resistant} Smart Contracts. 1335-1352. <https://www.usenix.org/conference/usenixsecurity18/presentation/breindenbach>

Brown, F., Logan, M. (2024) Decentralized Applications (dApps): Definition, Uses, Pros and Cons, *Investopedia*, <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp>

Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance—a multivocal approach. *Applied Sciences*, 11(16), 7572.

Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi crime landscape: an evidence-based picture. *Journal of Cybersecurity*, 11(1), tyae029.

Černá, M. (2024). Challenges and limitations of granting legal personality to distributed/decentralized autonomous organizations.

Chainalysis. The 2024 Crypto Crime Report. Chainalysis; 2024

Chainalysis. The 2025 Crypto Crime Report. Chainalysis; 2025

- Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American sociological review*, 505-524.
- Conklin, J. E. (1972). Robbery and the criminal justice system (p. 85). Philadelphia: Lippincott.
- Cook, P. J. (1986). The Demand and Supply of Criminal Opportunities. *Crime and Justice*, 7, 1-27. <https://doi.org/10.1086/449111>
- Cryptocurrency Prices, Charts, and Crypto Market Cap. (s. d.). CoinGecko. Consulté 15 avril 2024, à l'adresse <https://www.coingecko.com/>
- Dearden, T. E., & Gottschalk, P. (2024). Convenience Theory and Cybercrime Opportunity : An Analysis of Online Cyber Offending. *Deviant Behavior*, 45(3), 348-360. <https://doi.org/10.1080/01639625.2023.2246626>
- Desjardins, J. (2005). L'analyse de régression logistique. Tutorials in *Quantitative Methods for Psychology*, 1(1), 35–41. <https://doi.org/10.20982/tqmp.01.1.p035>
- Dotan, M., Yaish, A., Yin, H. C., Tsytkin, E., & Zohar, A. (2023, November). The vulnerable nature of decentralized governance in defi. In Proceedings of the 2023 workshop on decentralized finance and security (pp. 25-31).
- El Sanharawi, M., & Naudet, F. (2013). Comprendre la régression logistique. *Journal Français d'Ophthalmologie*, 36(8), 710–715. <https://doi.org/10.1016/j.jfo.2013.05.008>
- Gangwal, A., Gangavalli, H. R., & Thirupathi, A. (2023). A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications*, 209, 103539.
- Ghaleb, A. (2022). Towards Effective Static Analysis Approaches for Security Vulnerabilities in Smart Contracts. 37th IEEE/ACM International Conference on Automated Software Engineering, 1-5. <https://doi.org/10.1145/3551349.3559567>
- Gottfredson, M. R. (1981). On the etiology of criminal victimization. *J. Crim. L. & Criminology*, 72, 714.
- Ireland, L. (2021). Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. *Deviant Behavior*, 42(12), 1532-1548.
- Hägele, S. (2024). Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review. *Electronic Markets*, 34(1), 33.
- Hegedüs, P. (2018, May). Towards analyzing the complexity landscape of solidity based ethereum smart contracts. In Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain (pp. 35-39).
- Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. *Routledge*.
- Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice*, 33(3), 212-233. <https://doi.org/10.1177/1043986217699100>
- Jensen, J. R., Wachter, V. von, & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*, 26, Article 26. <https://doi.org/10.7250/csimq.2021-26.03>

- Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 52(12), 141-144.
- Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime : A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263-280. <https://doi.org/10.1080/01639625.2015.1012409>
- Li W, Bu J, Li X. et al. (2022). Security analysis of DeFi: vulnerabilities, attacks and advances. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain). Piscataway, NJ: IEEE, 2022, 488–93. <https://doi.org/10.1109/Blockchain55522.2022.00075>.
- Li, X., Wang, X., Kong, T., Zheng, J., & Luo, M. (2022a). From Bitcoin to Solana – Innovating Blockchain Towards Enterprise Applications. Dans K. Lee & L.-J. Zhang (Éds.), *Blockchain – ICBC 2021* (p. 74-100). *Springer International Publishing*. [https://doi.org/10.1007/978-3-030-96527-3\\_6](https://doi.org/10.1007/978-3-030-96527-3_6)
- Luoma-aho, V., Botha, J., & Hautala, M. (2025, March). Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies. In *The Proceedings of the International Conference on Cyber Warfare and Security*. Academic Conferences International Ltd.
- Mataković, C. (2022). Crypto-assets illicit activities: theoretical approach with empirical review. *International e-journal of criminal sciences*, 17.
- Margot, P. (2014). Traçologie: la trace, vecteur fondamental de la police scientifique. *Revue internationale de criminologie et de police technique et scientifique*, 67(1), 72-97.
- McDougall, A. & Tan, R. (2023). What Happens After the Hack? A Deep Dive Into DeFi Exploits and Recoveries. *Medium*. <https://medium.com/stablecorp/what-happens-after-the-hack-a-deep-dive-into-defi-exploits-and-recoveries-4aa42c3fc0b5>
- Meier, R. F., & Miethe, T. D. (1993). Understanding theories of criminal victimization. *Crime and justice*, 17, 459-499.
- Mikkola, M., Kaakinen, M., Savela, N., Oksa, R., Savolainen, I., & Oksanen, A. (2024). Cybercrime target exposure, suitability, personality, and victimization: A longitudinal approach. *Finnish Journal of Social Research*.
- Miró-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding Target Suitability in Cyberspace: An International Comparison of Cyber Victimization Processes. 14(1), 139-155.
- Nair, P. R., & Dorai, D. R. (2021, February). Evaluation of performance and security of proof of work and proof of stake using blockchain. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 279-283). IEEE.
- Oosthoek K. (2021). Flash crash for cash: cyber threats in decentralized finance. *ArXiv:2106.10740[cs]*.
- Ozili, P. K. (2023). The acceptable R-square in empirical modelling for social science research. In *Social research methodology and publishing results: A guide to non-native English speakers* (pp. 134-143). IGI global.
- Paquet-Clouston, M., & García, S. (2023). On the dynamics behind profit-driven cybercrime: from contextual factors to perceived group structures, and the workforce at the periphery. *Global Crime*, 24(2), 122-144.

Phillips, R., & Wilder, H. (2020, May). Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. In 2020 IEEE international conference on blockchain and cryptocurrency (ICBC) (pp. 1-8). IEEE.

Puggioni, V. (2022). Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it. New York, NY: *Cointelegraph*.

Qian, P., Liu, Z., He, Q., Huang, B., Tian, D., & Wang, X. (2022, septembre 13). Smart Contract Vulnerability Detection Technique : A Survey. *arXiv.Org*. <https://doi.org/10.13328/j.cnki.jos.006375>

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi—Comparing Centralized to Decentralized Finance (arXiv:2106.08157). *arXiv*. <https://doi.org/10.48550/arXiv.2106.08157>

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021a). Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit (N. Borisov & C. Diaz, Éd.s.; WOS:000712015400001; p. 3-32). *Springer Berlin Heidelberg*. [https://doi.org/10.1007/978-3-662-64322-8\\_1](https://doi.org/10.1007/978-3-662-64322-8_1)

Ribaux, O. (2014). Police scientifique: le renseignement par la trace. *EPFL Press*.

Ribaux, O. (2023). De la police scientifique à la traçologie. Le renseignement par la trace. *EPFL Press*.

Roux, C., Bucht, R., Crispino, F., De Forest, P., Lennard, C., Margot, P., ... & Willis, S. (2022). The Sydney declaration—Revisiting the essence of forensic science through its fundamental principles. *Forensic Science International*, 332, 111182.

Shukla, S., Gupta, I., & Naresh, K. (2022, August). Addressing security issues and future prospects of web 3.0. In 2022 2nd Asian Conference on Innovation in Technology (ASIANCON)(pp. 1-7). IEEE.

Solidus Labs. (2023) Market Manipulation Report – part 2 – Wash Trading; 2023

Sparks, R. F. (1981). Multiple victimization: Evidence, theory, and future research. *J. Crim. L. & Criminology*, 72, 762.

Sperandei, S. (2014). Understanding logistic regression analysis. *Biochemia Medica*, 24(1), 12-18. <https://doi.org/10.11613/BM.2014.003>

Statistics Canada (2024). Impact of cybercrime on Canadian businesses, 2023. <https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm#>

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1. <https://doi.org/10.1186/s40163-021-00163-8>

Uggen, C. & Thompson, M. (2003). The socioeconomic determinants of ill-gotten gains: within-person changes in drug use and illegal earnings. *American journal of sociology*, 109(1), 146-185 <https://doi.org/10.1086/378036>

Uniswap Labs (June 1, 2023). Uniswap 101: What is Uniswap?, *Uniswap Labs*. <https://blog.uniswap.org/what-is-uniswap>

Wang, B., Liu, H., Liu, C., Yang, Z., Ren, Q., Zheng, H., & Lei, H. (2021, mai). BLOCKEYE: Hunting for DeFi Attacks on Blockchain. 2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion). <https://doi.org/10.1109/icse-companion52605.2021.00025>

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2022). SoK : Decentralized Finance (DeFi) (arXiv:2101.08778). *arXiv*. <http://arxiv.org/abs/2101.08778>

Weyermann, C., & Ribaux, O. (2012). Situating forensic traces in time. *Science & Justice*, 52(2), 68-75.

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). Characterizing cryptocurrency exchange scams. *Computers & Security*, 98, 101993.

Xu, J., & Livshits, B. (2019). The Anatomy of a Cryptocurrency Pump-and-Dump Scheme. <https://doi.org/10.5555/3361338.3361450>

Zhang, X., Sun, W., Xu, Z., Cheng, H., Cai, C., Cui, H., & Li, Q. (2024). EVM-Shield : In-Contract State Access Control for Fast Vulnerability Detection and Prevention. *IEEE Transactions on Information Forensics and Security*, 19, 2517-2532. <https://doi.org/10.1109/TIFS.2024.3349852>

Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2022). SoK : Decentralized Finance (DeFi) Attacks (arXiv:2208.13035). *arXiv*. <https://doi.org/10.48550/arXiv.2208.13035>

# Annex 1

Table 6 : Bivariate Correlations of Variables Included in Logistic Regression Models

	Target	Chain	Layer2	Market	CEX	DEX	Social	EX	LD	DP	CP	Vol	Value	Audit	Bounty	Past Vic
<b>Target</b>	1.00															
<b>Chain</b>	0.01	1.00														
<b>Layer2</b>	0.07	0.68***	1.00													
<b>Market</b>	0.03	0.50***	0.23***	1.00												
<b>CEX</b>	0.15*	0.23***	0.11*	0.40***	1.00											
<b>DEX</b>	-0.02	0.35***	0.24***	0.23***	0.31***	1.00										
<b>Social</b>	0.04	0.04	-0.01	0.12*	0.09	0.09	1.00									
<b>EX</b>	-0.06	-0.02	-0.01	-0.08	-0.05	-0.19***	0.03	1.00								
<b>LD</b>	0.19***	-0.03	-0.07	-0.08	-0.05	-0.02	0.01	-0.25***	1.00							
<b>DP</b>	-0.08	-0.04	-0.02	0.05	0.08	0.15**	0.08	-0.24***	-0.12*	1.00						
<b>CP</b>	-0.13**	-0.08	0.00	-0.15**	-0.07	-0.06	-0.06	-0.39***	-0.19***	-0.18***	1.00					
<b>Vol</b>	0.15**	0.35***	0.12*	0.70***	0.56***	0.35***	0.17***	-0.09	-0.05	0.06	-0.16***	1.00				
<b>Value</b>	0.05	0.12*	0.08	0.38***	0.12	0.13*	0.04	-0.21***	0.04	0.09	-0.04	0.35***	1.00			
<b>Audit</b>	-0.07	0.09	0.10	0.04	0.14**	0.14**	0.01	-0.01	0.00	-0.13*	0.16***	0.06	0.00	1.00		
<b>Bounty</b>	-0.06	0.14	0.07**	0.09	0.17***	0.19***	0.01	-0.03	0.01	-0.08	0.07	0.11	0.06	0.30***	1.00	
<b>Past Vict.</b>	-0.11*	0.10	0.09	0.14**	0.14**	0.13*	-0.08	0.00	0.05	-0.04	0.00	0.14**	0.10	0.26	0.33***	1.00

\*: p<0.05, \*\*: p<0.01, \*\*\*: p<0.001