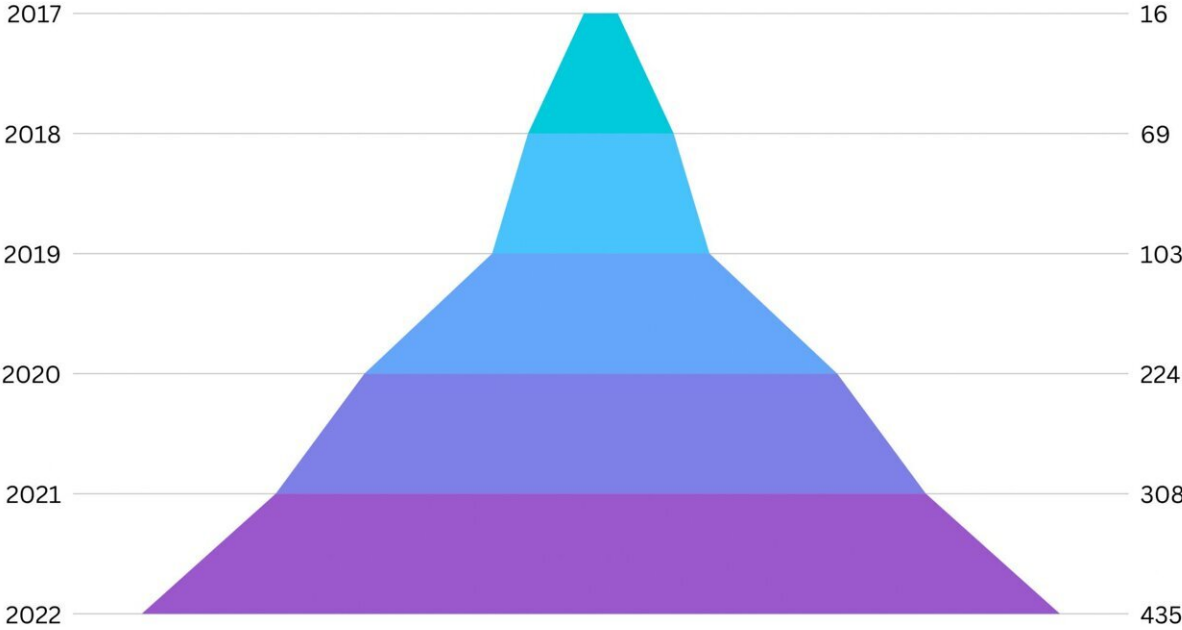


Researchers: Criminal activities caused losses of \$30 billion in the crypto sector from 2017 to 2022

October 16 2023



While only 16 criminal activities were documented in 2017, there were 308 reported crimes in 2021 and 435 in 2022. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2310.04356

Digital financial products are increasingly coming under the crosshairs of cyberattacks. However, evidence-based results are not yet available regarding the actual magnitude of this threat. Researchers from the

Complexity Science Hub and the University of Montreal have now, for the first time, shown that the global damage amounts to at least \$30 billion and is on the rise. A preprint of the study was recently published on *arXiv*.

Decentralized Finance (DeFi) represents a new financial paradigm where [financial services](#), such as lending, are offered through decentralized computer programs running on so-called blockchains. It's well-known that numerous criminal attacks occur in this space. However, "since there is no central point of contact for criminal cases, evidence-based statements about the total damage could not be made until now," explains Bernhard Haslhofer, head of the Cryptofinance research group at the Complexity Science Hub.

At least 1,155 criminal incidents

Therefore, the researchers have now compiled documented criminal incidents in the crypto sector from various databases for the first time. In doing so, they identified a total of 1,155 criminal events from 2017 to 2022. "But this doesn't mean there couldn't be more cases. Accordingly, all our results are minimum values," emphasizes Haslhofer. The resulting total damage: \$30 billion, roughly equivalent to Luxembourg's state revenue in 2022.

"These 1,155 cases might not be the whole picture, but they constitute one of the most extensive set of events analyzed to date, which represents the first step towards assessing the size and scope of the DeFi crime landscape," says Catherine Carpentier-Desjardins of the University of Montreal.

Increasing criminal activity

While only 16 cases were documented in 2017, there were 308 in 2021 and, finally, 435 reported crimes in 2022. "This entire ecosystem is still in its infancy. It's highly complex, and currently, we have little understanding of how it works. Therefore, security in this area remains a problem," explains Haslhofer.

In half of the attacks, the damage exceeded \$356,000, with the smallest "hack" amounting to just \$158, while the largest was \$3.6 billion. This significant loss was associated with Africrypt, a centralized financial platform (CeFi) from South Africa.

CeFi serves as the link between traditional finance and decentralized financial systems (DeFi). These are cryptocurrency trading exchanges where trading occurs with both fiat and cryptocurrencies through a centralized management system.

"Whether Africrypt was hacked or the administrators left with the money does not matter much: what matters is that someone could leave with clients' investments because the money was centrally managed, even if the investment was in cryptocurrency," explains Masarah-Cynthia Paquet-Clouston from the University of Montreal. These types of events are frequent in the CeFi sector, and the resulting damages are unprecedented, according to the researchers.

While the researchers observed significantly more successful attacks in the DeFi sector, with 1,050 incidents, the damages in the CeFi sector are much higher. "With only 105 documented crimes, the damages amounted to \$20 billion, which is two-thirds of the total damage," explains Haslhofer. In comparison, traditional financial sector platforms are closely monitored by [regulatory authorities](#), making such incidents less likely there.

Most common cause: Technical weaknesses

In addition to the extent, the researchers examined the types of attacks and the technical levels at which they occurred.

In 52.4% of the cases, DeFi services were targeted, and this was almost always achieved through technical vulnerabilities at the protocol level. "Hence, it is essential for stakeholders to give top priority to safeguarding their contracts and protocol designs in order to reduce external vulnerabilities," says CSH researcher Stefan Kitzler.

In 40.7% of the cases, DeFi was utilized to target users. "When this happens, over 70% of the crimes involve manipulated cryptocurrencies that have a kind of backdoor through which criminals can withdraw funds," explains Kitzler.

Security gaps and market manipulation

Knowing where an attack is most likely to occur is essential to be able to take effective countermeasures, according to the researchers. "There's no doubt that security in the DeFi sector is improving. Nevertheless, this sector remains a prime target for motivated offenders due to numerous opportunities," says Paquet-Clouston.

This is also due to the potential for market manipulation, and stolen funds are irretrievably lost. Therefore, even with robust security measures, the DeFi sector will remain a target, the researchers are certain. "It is crucial to understand the asymmetrical position between offenders and defenders: while defenders must secure every potential vulnerability, attackers need only find one," emphasizes Paquet-Clouston.

This study shows where attacks are most likely to occur and the extent of the damage. However, tracking the [money](#) trail in the DeFi sector is

currently extremely difficult. That's why the "DeFi Trace" project is currently underway at the Complexity Science Hub, led by Bernhard Haslhofer. "Over the course of two years, we aim to develop methods to automatically trace illegal payment flows in the DeFi sector, thereby containing criminal activities," says Haslhofer.

More information: Catherine Carpentier-Desjardins et al, Mapping the DeFi Crime Landscape: An Evidence-based Picture, *arXiv* (2023). [DOI: 10.48550/arxiv.2310.04356](https://doi.org/10.48550/arxiv.2310.04356)

Provided by Complexity Science Hub Vienna

Citation: Researchers: Criminal activities caused losses of \$30 billion in the crypto sector from 2017 to 2022 (2023, October 16) retrieved 27 April 2024 from <https://techxplore.com/news/2023-10-criminal-losses-billion-crypto-sector.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.