PUBLISHED JULY 2023

Digital Assets and Their Current Roles Within Cybercrime

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Digital Assets and Their Current Roles Within Cybercrime

Published July 2023

Scope of paper

As demonstrated by the following discussion, digital assets and their roles in cybercrime continue to increase. The purpose of this paper is to:

1. provide insurance practitioners (both actuaries and non-actuaries) with a high-level overview of digital assets;
2. outline the use of digital assets within ransomware;
3. highlight recent United States sanctions and enforcement actions against entities in the digital asset ecosystem; and
4. detail trends surrounding the theft of digital assets from exchanges and decentralized finance (DeFi) platforms.

There are numerous other topics to be explored regarding cybercrime and digital assets. However, this paper seeks to provide a baseline understanding of digital assets for insurance industry practitioners whose lines of business may interact with digital assets and highlight recent trends surrounding their use within cybercrime.

What are digital assets?

According to the U.S. Securities and Exchange Commission (SEC), a digital asset is defined as:

> *An asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens."*[1]

There are different subtypes of digital assets, and they are not a monolith when it comes to various use cases. Each subtype has unique attributes for different uses. While the common types are shown in Table 1, most digital assets utilized in the ransomware ecosystem are related to crypto assets.

1 "Joint proposed rules"; Release No. IA-6083; File No. S7-22-22; Securities and Exchange Commission; *Federal Register*; Sept. 7, 2022.

Table 1. Common Types of Digital Assets[2]

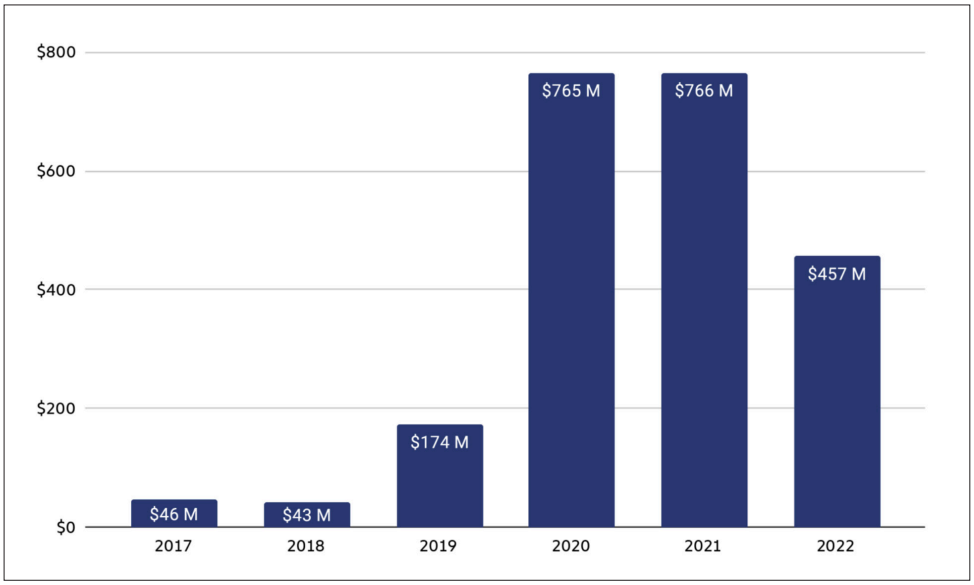
Type	Definition	Common Uses
Crypto assets	Any digital store of value or medium of exchange (currency) that's stored on the blockchain.	• Investments • Payments • Creating a coin to fund a project
Stablecoins	A cryptocurrency designed for price stability. The prices associated with stablecoins are linked to fiat currencies, commodities, or other crypto assets.	• Payments • Foreign exchange • Cross-border payments and transfers
Non-fungible tokens (NFTs)	A token that represents ownership of a unique digital item (examples: a work of art, a government ID, a specific unit of production). An NFT certifies that the holder owns the underlying digital asset and can sell, trade, or redeem it.	• Proving your identity and granting access (to either a virtual or physical space) • Ownership of virtual items (games, avatars, virtual land) • Tokenizing your supply chain to track inventory movement and ownership
Central bank digital currencies (CBDCs)	A type of digital asset that represents a nation's fiat currency and is backed by its central bank. Not all nations issue CBDCs.	• Payments • Cross-border payments and transfers
Security tokens	Digital assets that meet the definition of a security or financial investment, like stocks and bonds.	• Tokenized versions of stocks (equity) and bonds • Tokenized versions of real-world assets (real estate, property, plant, and equipment, etc.)

Digital assets and their use in ransomware

As noted elsewhere in the Cyber Risk Toolkit, digital assets such as Bitcoin and Monero have been utilized by threat actors when demanding ransom payments associated with ransomware and other extortion incidents. In particular, the increased use of digital assets for ransom payments increased as ransomware activity spiked over the course of the 2020 and 2021 calendar years. In fact, according to the blockchain research firm Chainalysis, the total value of digital assets received by cryptocurrency addresses *known* to be controlled by cyber threat actors was $765 million in 2020 and $766 million in 2021.[3] Surprisingly, the value associated with the 2022 calendar year dropped to $457 million as shown in Chart 1 from Chainalysis' 2023 *Crypto Crime Report*. It's important to note that these figures are subject to change as research analysts uncover cryptocurrency addresses associated with these cyber threat actors.

2 "Demystifying cryptocurrency and digital assets"; PwC.
3 "Ransomware Revenue Down As More Victims Refuse to Pay"; Chainalysis; Jan. 19, 2023.

Chart 1. Total value received by ransomware attackers, 2017–2022



Chainalysis

In calendar year 2022, Chainalysis concluded that the total value received dropped primarily due to a decrease in the victims' willingness to pay the ransom demand. Based on an analysis by Coveware, ransomware victims' payment of ransoms decreased in 2022 to the lowest level from 2019 to 2022:

Table 2. Share of Companies That Paid a Ransom[4]

Year	Paid Ransom	Did Not Pay
2019	76%	24%
2020	70%	30%
2021	50%	50%
2022	41%	59%

There are a few potential reasons for the decrease in victims' payment of ransoms shown above, according to Chainalysis. As cyber insurers have tightened underwriting standards, insureds are incentivized to strengthen controls and backup measures. An improvement across insureds' cybersecurity posture as well as an increased focus on backups, business continuity, and disaster recovery may mean that victims are less reliant on paying the ransom. Another reason is an increase in sanctions from governmental entities has made paying demands legally riskier for the impacted victims.

4 "Improved Security and Backups Result in Record Low Number of Ransomware Payments"; Coveware; Jan. 20, 2023.

Ecosystem sanctions by the U.S. Department of Treasury

Since digital assets have such a strong use within ransomware attacks, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) have been monitoring virtual currency exchanges. In particular, OFAC and FinCEN have sanctioned entities due to violations associated with the Bank Secrecy Act's anti-money laundering (AML) and suspicious activity report (SAR) reporting requirements. Listed in Table 3 is a sampling of notable sanctions and enforcements against entities participating in the digital asset ecosystem over the course of 2021 and 2022.

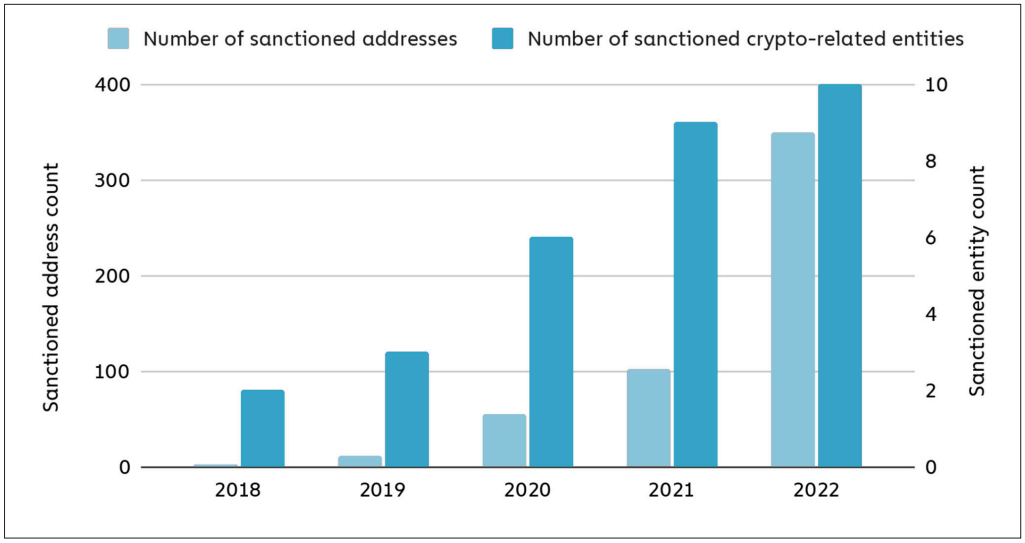
Table 3. Notable Sanctions and Enforcements

Entity	Enforcement/ Sanctioned Date	Press Release
SUEX	09/21/2021	Treasury Takes Robust Actions to Counter Ransomware
Chatex	11/08/2021	Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange
Garantex	04/05/2022	Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex
Hydra	04/05/2022	Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex
Blender	05/06/2022	U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats
Tornado Cash	08/08/2022	U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash
Bittrex	10/11/2022	Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.
Kraken	11/28/2022	Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Payward, Inc. ('Kraken')

This is not an exhaustive list of investigations and sanctions into digital asset exchanges, but it does represent a sampling of the actions undertaken by U.S. regulators when it comes to utilizing regulatory authority to curb ransomware activity. In fact, the overall number of entities and corresponding cryptocurrency addresses sanctioned by the U.S. Department of Treasury's OFAC continues to increase as shown in Chart 2 from Chainalysis.[5]

5 "How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime"; Chainalysis; Jan. 9, 2023.

Chart 2. Sanctioned Crypto-related Entities and Number of Sanctions-related Addresses by Year Added, 2018–2022



Chainalysis

Trends in theft of digital assets

Due to their ability to be transferred via distributed ledger technology, digital assets are attractive to cyber threat actors not only through their use when demanding payment from a ransomware/extortion incident from victims, but also through the theft of the assets directly from digital asset exchanges and DeFi platforms.

Before describing the trends associated with the theft of digital asset exchanges and DeFi platforms, it's important to define these two financial intermediaries as well as note the key similarities and differences between them.

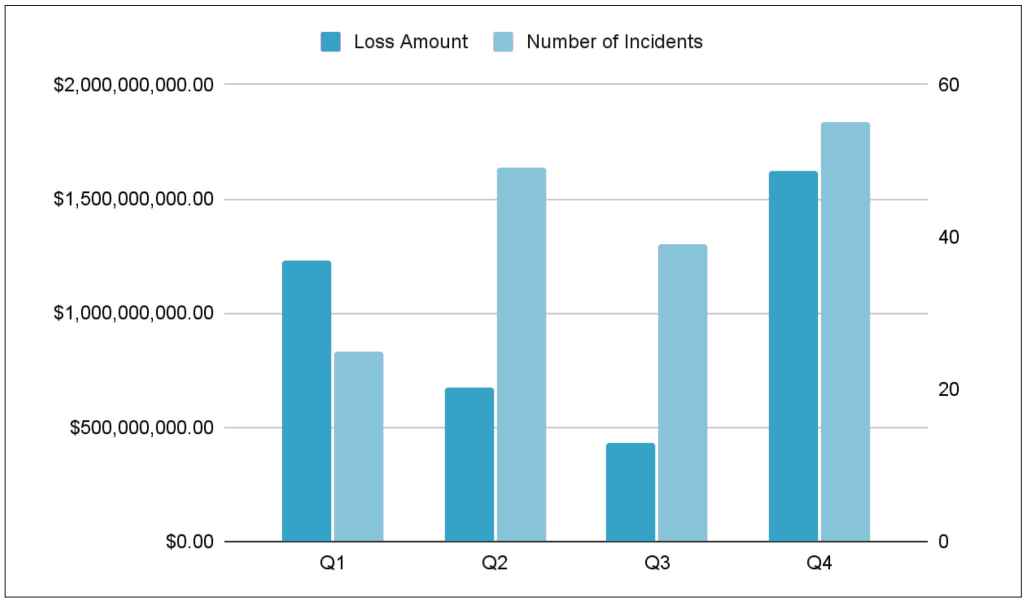
- *Centralized Digital Asset Exchanges*[6]
  In general, centralized digital asset platforms or exchanges allow users to trade various digital assets and often require users to perform a user verification. While their main purpose is primarily trading of digital assets, they may also offer other services surrounding stablecoins and even trading / purchasing of other financial instruments such as stocks and bonds. Within the U.S., these centralized exchanges have AML and know-your-customer (KYC) requirements.

6 *Crypto-Assets: Implications for Consumers, Investors, and Businesses*; U.S. Department of the Treasury; September 2022.

- *Decentralized Platforms and Protocols (DeFi platforms/protocols)*[7]
  DeFi platforms are highly utilized within the digital asset ecosystem and are decentralized to the extent that they leverage distributed ledger technology to eliminate the need for centralized financial institutions and intermediaries. Unlike centralized digital asset exchanges, decentralized platforms and protocols do not manage the same customer verification, AML, and KYC processes. They are also not registered with U.S. regulators such as the SEC or Commodity Futures Trading Commission (CFTC), which means they may or may not be complying with appropriate U.S. laws and regulations.

The number of thefts impacting digital asset exchanges and DeFi platforms decreased slightly in 2022 compared to 2021. However, the overall monetary loss values in 2022 exceeded the total value stolen in 2021, per Chainalysis. Chart 3 and Table 4 show the quarterly activity in terms of incidents and financial value stolen from digital asset exchanges and DeFi platforms over 2022 per blockchain research company Immunefi.

Chart 3. 2022 Digital Asset Theft Losses by Quarter[8]



7 Ibid.
8 *Crypto Losses in 2022*; Immunefi.

Table 4. 2022 Digital Asset Theft Incidents by Quarter[9]

Q1 2022		Q2 2022	
Ronin Bridge	$625,000,000	Beanstalk	$182,000,000
Wormhole	$326,000,000	Harmony	$100,000,000
Qubit	$80,000,000	Mirror Protocol	$90,000,000
Cashio	$50,000,000	TribeDAO	$80,340,000
IRA Financial	$36,000,000	Fantom Scream	$35,000,000
crypto.com	$30,000,000	Optimism	$35,000,000
Lympo	$18,700,000	Akutars	$33,000,000
Superfluid	$13,000,000	Deus Finance	$13,400,000
Arbix Finance	$10,000,000	Elephant Money	$11,200,000
Dego Finance	$10,000,000	Venus Protocol	$11,200,00

Q3 2022		Q4 2022	
Nomad Bridge	$190,000,000	FTX	$650,000,000
Wintermute	$160,000,000	BNB Chain	$570,000,000
Racoon Network and Freedom Protocol*	$ 20,000,000	Mango Markets**	$100,000,000
Impermax Finance	$7,451,118	mgnr*	$52,000,000
Audius	$6,000,000	DeFiAI	$40,000,000
The Bribe Protocol	$5,500,000	Transit Swap	$28,900,000
ZB	$4,800,000	Deribit	$28,000,000
Teddy Doge*	$4,500,000	UXD Protocol**	$20,000,000
Slope Mobile Wallet	$4,500,000	Flare	$18,500,000
Nirvana	$3,500,000	Helio	$15,000,000

* The teams behind Raccoon Network and Freedom Protocol, Teddy Doge, and mgnr allegedly performed a rug pull.
** Mango Markets later recovered $67 million of the stolen funds. UXD Protocol later recovered over $19 million of the stolen funds.

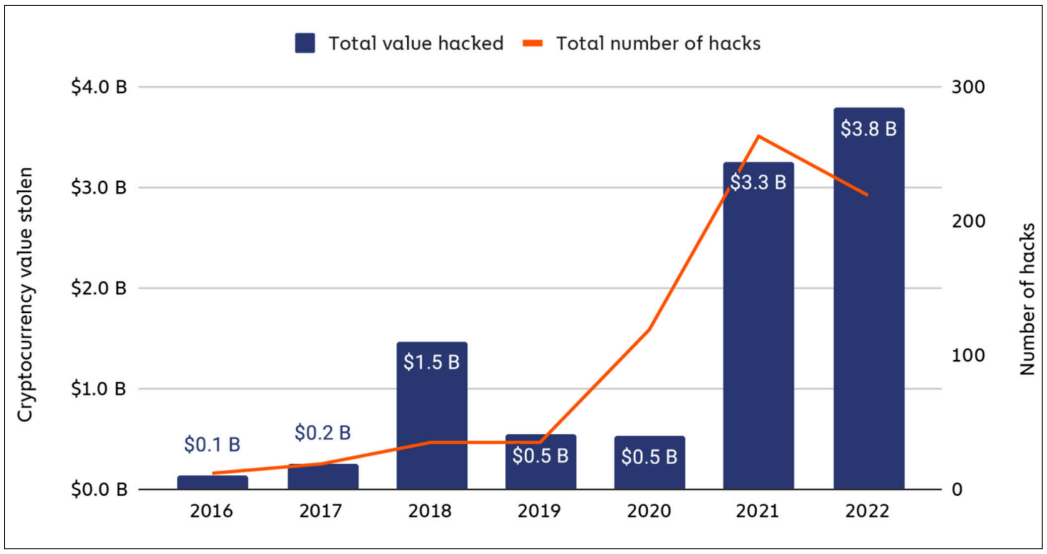
It is important to note that the use and tracking of digital assets are not fully anonymous. In fact, authorities have been able to track and seize digital assets linked to prior hacks. For example, in February 2022, the U.S. Department of Justice (DOJ) was able to seize $3.6 billion of cryptocurrency related to the 2016 Bitfinex digital asset exchange hack.[10] The DOJ also announced a seizure of $3.36 billion of cryptocurrency in conjunction with fraud surrounding the Silk Road Dark Web market in November 2022.[11] Authorities are continuing to monitor blockchain traffic to track down cyber threat actors who are involved with these hacks of digital asset exchanges and DeFi platforms.

9 Ibid.
10 "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency"; U.S. Department of Justice press release; Feb. 8, 2022.
11 "U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud"; U.S. Department of Justice press release; Nov. 7, 2022.

In addition to viewing the quarterly activity over 2022, it's important to note that these thefts have been ongoing, with significant frequency increases in 2021 and 2022. Given that Chainalysis and Immunefi conduct their own independent research of the blockchain, the specific frequencies and total value stolen may differ slightly between the two research firms. However, the overall trends around cyber threat actors leveraging retail consumer and institutional financial platforms for theft of digital assets remain.

Understanding the theft of digital assets is important for both general consumers of these financial services as well as for insurers who provide insurance policies (for example: crime and specie insurance, a specialized coverage for priceless items) to these financial institutions and platforms.

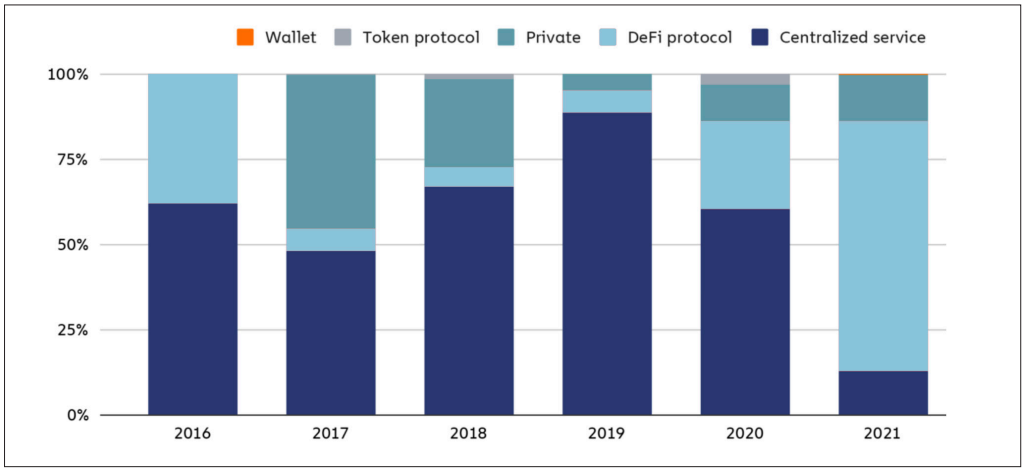
Chart 4. Total Value Stolen in Crypto Hacks and Number of Hacks, 2016–2022[12]



Chainalysis

12 "2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers"; Chainalysis; Feb. 1, 2023.

Chart 5. Cryptocurrency Stolen by Victim Platform Type, 2016–2022[13]



Chainalysis

Specific impact to actuaries

While a deep technical knowledge of digital assets is not required by actuaries interacting with cyber, crime, or specie insurance, it is important for actuaries to have a baseline understanding of the role digital assets play in facilitating cybercrime such as ransomware or in their attractiveness when it comes to the theft of digital asset exchanges or DeFi platforms. The increased digitization of our global economy will likely continue to find uses for digital assets, and actuaries should be aware of how existing and future digital assets could be utilized by threat actors. Additionally, governmental regulators both within and outside the United States are likely to continue their oversight in this area and levy sanctions where appropriate to minimize how criminals can utilize digital asset exchanges and services to transfer digital assets.

13 Ibid.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**