# AADAPT™: A cyber threat framework for digital assets

## Digital Asset Threat Landscape

Since the invention of Bitcoin in 2008, digital forms of trade and currency have seen increasing usage. Unfortunately, this growth in digital currencies has brought about new forms of cyber threats and attacks, impacting individuals, businesses, and governments alike. Some of the common cyber-attacks against digital asset systems include double-spending, 51% attacks, phishing attacks, Sybil attacks, and smart contract vulnerability exploitation. A surge in cryptocurrency-fueled ransomware attacks has also affected various sectors of commerce and government, making them increasingly reliant on cyber insurance coverage to manage and reduce cyber risk. This coverage helps organizations respond to ransomware attacks, pay crypto ransoms, cover direct costs of restoration and recovery, and protect against potential third-party liability. However, the growing frequency and costs of ransomware attacks have put the insurance industry under pressure, leading to higher prices and reduced coverage, particularly impacting small- to medium-sized businesses, state and local governments, and small towns and municipalities that may be unable to afford the necessary preventive measures to reduce their vulnerabilities. As the financial landscape continues to shift towards digitalization, it is essential to maintain the integrity, confidentiality, and availability of these digital assets. This is crucial for managing the risks associated with new, less-proven technologies and their related financial models. Ensuring this is key to building trust, mitigating identified risks, and safely advancing the future of digital finance.

## AADAPT™: What and Why?

MITRE's Adversarial Actions in Digital Asset Payment Technologies (AADAPT) is a preliminary cyber threat framework for digital asset management systems designed to be complementary to MITRE ATT&CK®. AADAPT aims to facilitate efforts to analyze and secure digital assets by providing a structured approach to identifying, assessing, and mitigating potential vulnerabilities and risks. It seeks to contribute to the ongoing discourse on digital asset security and help guide stakeholders, including developers, policymakers, and users, in adopting best practices and robust security measures.

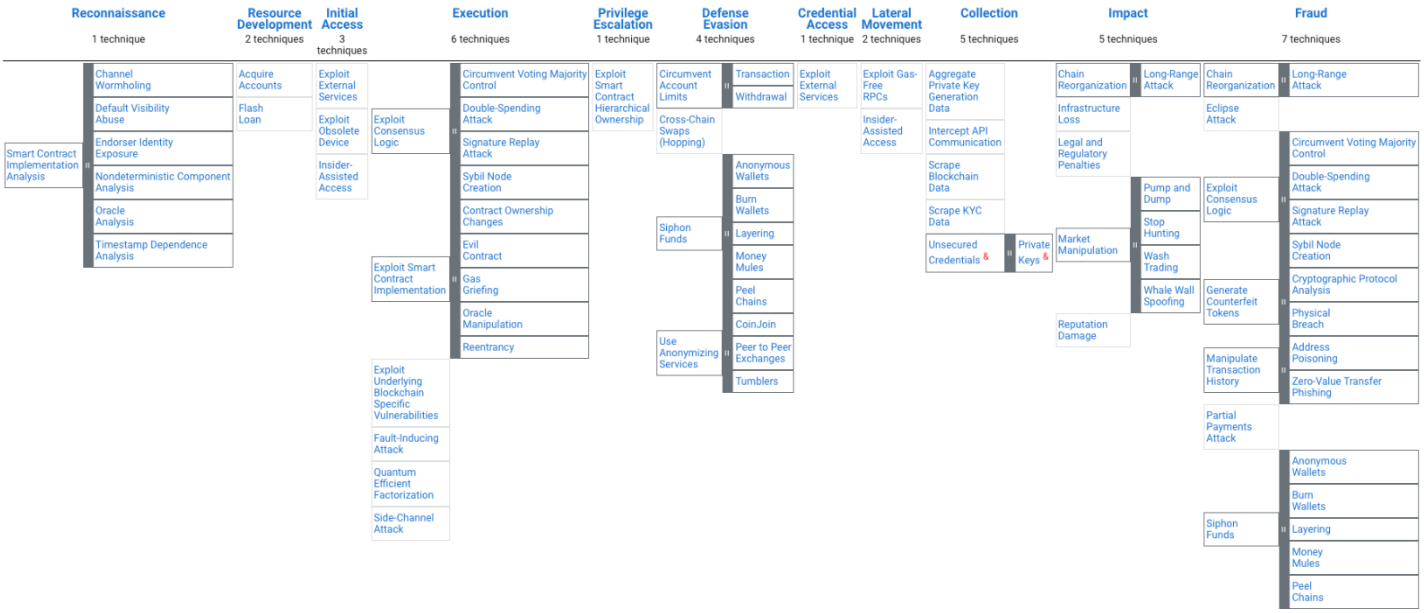
The methodology to identify Techniques Tactics and Procedures (TTPs) captured in the AADAPT framework involved analyzing known real-world attacks on digital assets and related technologies. This included several examples of digital-asset underlying technologies in connection with credible attack methods and vulnerabilities that have been published, hypothesized, or explored in laboratory settings. The focus was also on comparing consensus algorithms, smart contracts, and digital asset implementations to understand and identify common elements and themes. These insights were incorporated into the framework to ensure that it remains up-to-date and relevant in addressing the complex and evolving landscape of digital asset security.

*Since 2021, there have been a dozen cyber-attacks on cryptocurrency and decentralized finance platforms, resulting in total losses of $1.34 billion, according to the Carnegie Endowment for International Peace's report on cyber incidents involving financial institutions*[1]

*Through our public-private partnerships and federally funded R&D centers, MITRE works across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.*

*For further inquiries, please reach out to us at aadapt@mitre.org*

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®




## How Do You Use AADAPT™?

Following a similar structure to MITRE's ATT&CK framework, the AADAPT framework includes techniques and sub-techniques outlining actions adversaries may employ to achieve specific objectives. These goals are sorted into tactical groups, giving a broader picture of why these actions happen. The correlation among tactics, techniques, and sub-techniques is visualized through the AADAPT matrix pictured above.

Tactics represent the short-term objectives behind adversarial behaviors, providing the rationale for why an adversary may perform a given action. Each technique in a cyber threat framework is associated with at least one tactic. Although adversaries employ a series of behaviors to achieve campaign-level objectives, tactics help to contextualize these behaviors within the broader attack lifecycle.

Techniques represent the fundamental actions that an adversary may undertake when targeting a digital asset management system. Within the proposed AADAPT framework, there are three primary categories of techniques and sub-techniques:

- Techniques that are exclusive to the AADAPT framework.
- Sub-techniques to an AADAPT or existing ATT&CK technique.
- Addendums (indicated by &) – annotations to existing ATT&CK techniques or sub-techniques that provide crucial information about adversary behavior in the context of a digital asset management system.

## What Is MITRE ATT&CK®?

The MITRE ATT&CK knowledge base[2] has been published and maintained by MITRE for over ten years and is a de-facto standard for modeling adversarial behaviors at an implementation level of abstraction. ATT&CK covers three domains: Enterprise, Mobile, and Industrial Control Systems (ICS). Its content is solely based upon real-world adversary activity, as documented by either public Cyber Threat Intelligence (CTI) or private sharing of such information.

The dependency of digital payment systems on standard enterprise information technology and mobile components renders the tactics, techniques, and procedures (TTPs) documented in the ATT&CK framework somewhat applicable[3].

## MITRE's Related Experience and Products

Over the past several years, MITRE has provided unbiased, trusted advice to multiple federal agencies and U.S. policymakers who seek to better understand rapidly changing technology developments across the full spectrum of digital assets, e.g., cryptocurrencies, stablecoins, CBDCs, and non-fungible tokens. MITRE also has extensive experience with cyber security, both in general and with regards to financial institutions. Several of our recent publications include:

- Enhanced Cyber Threat Model for Financial Services Sector Institutions, https://www.mitre.org/news-insights/publication/enhanced-cyber-threat-model-financial-services-sector-institutions
- Enterprise Threat Model Technical Report-Cyber Threat Model for a Notional Financial Services Sector Institution, https://www.mitre.org/news-insights/publication/enterprise-threat-model-technical-report-cyber-threat-model-financial
- Systems of Systems Threat Model, https://www.mitre.org/news-insights/publication/system-systems-threat-model
- Stablecoin Regulatory Design: A Logic Model-Based Approach to Drive Public-Private Collaboration, https://www.mitre.org/news-insights/publication/stablecoin-regulatory-design-logic-model-based-approach
- Securing Web3 and Winning the Battle for the Future of the Internet, https://www.mitre.org/news-insights/publication/securing-web3-and-winning-battle-future-internet
- MITRE's Response to the OSTP RFI Supporting a National Digital Assets R&D Agenda, https://www.mitre.org/news-insights/publication/mitre-ostp-supporting-national-digital-assets-rd-agenda

---

[1] Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," 2022. [Online]. Available: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[2] The MITRE Corporation, "MITRE ATT&CK," March 2020. [Online]: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[3] Bank for International Settlements, "Project Polaris Part 3: Closing the CBDC cyber threat modeling gaps," July 2023. https://www.bis.org/publ/othp71.pdf

MITRE