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. Digital assets have enhanced the capabilities of financial systems by reducing transaction times and costs, increasing transparency, and expanding access to banking services globally. This growth in digital assets has also unfortunately 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 susceptible to cyber risk. Reliance of individuals and organizations on cryptocurrencies creates a risk for attacks resulting in financial loss. As the financial landscape continues to shift towards digitalization, it is essential to maintain the integrity, confidentiality, and availability of the overall financial ecosystem, which is crucial for managing the risks associated with adopting new, less proven technologies and their related financial models.

AADAPT™: What and why?

MITRE's Adversarial Actions in Digital Asset Payment Technologies™ (AADAPT™) is a cyber threat framework for digital asset management systems designed to be complementary to MITRE ATT&CK®. AADAPT allows users to analyze and secure digital assets. It provides a structured approach to identifying, assessing, and mitigating potential vulnerabilities and risks which can help inform the engineering and implementation of these systems. In addition, it serves as a resource to assist in ongoing cyber defense once systems are operational. The framework supports a range of critical use cases: it helps cyber defenders develop analytics to detect adversarial techniques, enables threat intelligence analysts to structure and compare insights using a common language, guides red teams in emulating specific threats and planning operations, and assists organizations in assessing their security capabilities and prioritizing engineering decisions. AADAPT can assist a wide range of stakeholders, including developers, policymakers, and users, in adopting best practices and robust security measures.

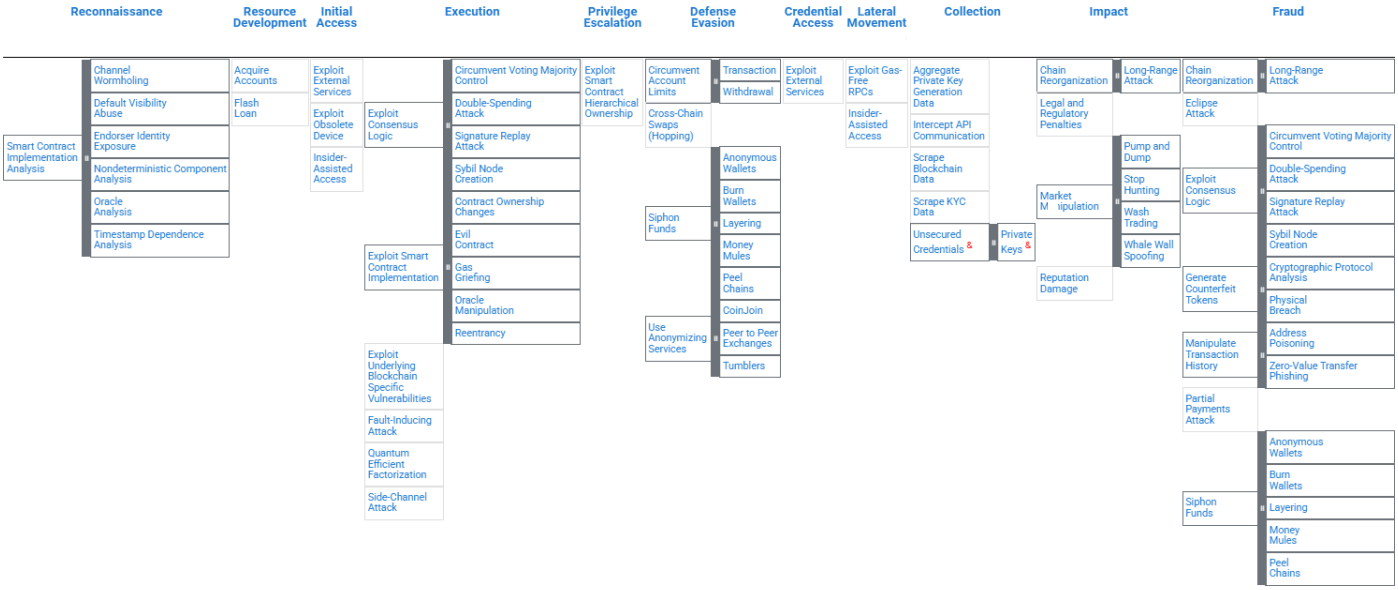
The Tactics, Techniques, and Procedures (TTPs) that comprise the AADAPT framework are derived from a comprehensive analysis of real-world attacks on digital currencies and related technologies. The analysis included in-depth review of underlying technologies used to implement digital assets, focusing on credible attack methods and vulnerabilities that have been published, hypothesized, or explored in laboratory settings. Technologies AADAPT examined have limited real-world implementations and documented attacks to date, such as consensus algorithms, smart contracts, quantum computing, and distributed ledger technology (DLT) systems. Our analysis took a predictive approach, anticipating potential threats arising from vulnerabilities in these complex technologies. This enables users and issuers to develop secure digital asset systems that preemptively address novel threats and vulnerabilities before attacks materialize. AADAPT addresses the complex landscape of digital asset security.

Since 2021, there have been 1000+ documented hacks targeting cryptocurrency and decentralized finance platforms, resulting in total losses of $12.5 billion.

Chainalysis 2025 Crypto Crime Report[1] and FBI report on the February 2025 ByBit Hack[2].

For access to AADAPT™ email us at:
aadapt@mitre.org

MITRE



How do you use AADAPT™?

The AADAPT framework, modeled after MITRE's ATT&CK framework, is designed to help users understand and counteract cyber threats targeting digital asset systems. By categorizing adversarial actions into tactics, techniques, and subtechniques, AADAPT provides valuable insights into the short-term objectives and fundamental actions adversaries may employ. This understanding allows users to anticipate, intercept, and shut down attacks more effectively, enhancing the security of digital financial infrastructures.

The framework's value is evidenced by the interest it has garnered from multiple banks and regulatory agencies in the digital assets community, who are looking to use AADAPT to predict and address threats during the design phase rather than after implementation. This proactive approach has the potential to improve financial integrity and reduce costs. Additionally, initial validation results have shown that forward-looking threats can be identified in representative digital asset systems, further demonstrating the framework's effectiveness.

AADAPT also fosters ongoing engagement from stakeholders, who contribute feedback and new content, ensuring the framework remains relevant and robust. With AADAPT, MITRE is at the forefront of research in securing digital assets and infrastructure, aiding the community in understanding, securing, and crafting policy for the latest digital asset technologies.

What is MITRE ATT&CK®?

The MITRE ATT&CK knowledge base[3] is a worldwide de-facto standard for modeling adversarial behaviors, published and maintained by MITRE for over 10 years. ATT&CK provides implementation-level detail about threat behaviors in three domains: Enterprise, Mobile, and Industrial Control Systems (ICS). Its content is based solely upon adversary activity that has been observed in real-world use, as documented by either public or privately shared Cyber Threat Intelligence (CTI).

Most digital payment systems are built upon standard enterprise information technology and mobile components that process financial transactions. The TTPs documented in the MITRE ATT&CK framework are thus highly relevant to digital asset use cases where these technologies are involved. AADAPT expands upon ATT&CK, providing threat behaviors specific to digital asset implementations. Incorporating threats from both these complementary frameworks provides a comprehensive approach to identify and mitigate threats in digital asset systems.

MITRE's related experience and products

Over the past several years, MITRE has empowered multiple federal agencies and U.S. policymakers to anticipate and respond to technological opportunities and threats across the full spectrum of digital assets, from cryptocurrencies to stablecoins to centralized exchanges. MITRE also has extensive experience with cybersecurity, both in general and with regards to the financial sector. Several of our related publications and outreach 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
- System-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
- SEC Crypto Task Force meets with Saylor, CCI, and MITRE to discuss regulation, CryptoSlate, Feb 24, 2025, https://cryptoslate.com/sec-crypto-task-force-meets-with-saylor-cci-and-mitre-to-discuss-regulation/

---

[1] Chainalysis, "The 2025 Crypto Crime Report," Feb. 2025. Accessed: Mar. 14, 2025. [Online]. Available: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

[2] FBI, "Internet Crime Complaint Center (IC3) | North Korea Responsible for $1.5 Billion Bybit Hack," Feb. 2025. Accessed: Mar. 14, 2025. [Online]. Available: https://www.ic3.gov/PSA/2025/PSA250226

[3] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, "MITRE ATT&CK®: Design and Philosophy," Mar. 2020. Accessed: Apr. 11, 2025. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf