



Adversarial Actions in Digital Asset Payment Technologies (AADAPT)™

MITRE™ AADAPT™ Framework:
Protecting Crypto Ecosystems

Digital Trust, Financial Services

November 2025

KPMG. Make the Difference.





Table of Contents

01 Introduction

02 Overview of Adversarial Actions in Digital Asset Payment Technologies enterprise tactics

03 Enterprise tactics and attack techniques against digital assets

04 Way forward

Introduction

Adversarial Actions in Digital Asset Payment Technologies

Adversarial Actions in Digital Asset Payment Technologies (AADAPT™), developed by MITRE Corporation™, is a cyber threat framework tailored for digital asset systems. It empowers users to analyse, secure, and manage digital assets by offering a structured approach to identifying and mitigating vulnerabilities. AADAPT™ complements the widely adopted MITRE™ ATT&CK™ framework and is designed to support a global community of cyber defenders. AADAPT™ provides a standardised methodology for understanding adversarial behaviors, enhancing threat intelligence, and guiding secure system design.

OBJECTIVES

- Enhances cybersecurity for digital asset systems by identifying and mitigating adversarial threats.
- Support secure system design, inform threat intelligence, and enable proactive defense strategies.
- Assist developers design secure platforms, support threat intelligence and detection, guide red and blue teams in simulating and defending against attacks.
- Enables regulators and policymakers to understand emerging risks and shape effective security policies.

ADVANTAGES

- Assist cybersecurity teams detect and respond to threats in digital asset systems, supports developers in building secure platforms, and guides red/blue teams in simulating and defending against attacks.
- Enables regulators to shape informed policies and assists organizations in assessing and improving their security posture.
- Facilitate collaboration across stakeholders to keep threat models current and relevant.

APPLICABILITY

- Consensus algorithms
- Smart contracts
- Quantum computing
- Distributed ledger technology (DLT) systems

ENTERPRISE TACTICS

Reconnaissance

Impact

Initial Access

Execution

Privilege Escalation

Defense Evasion

Credential Access

Lateral Movement

Collection

Resource Development

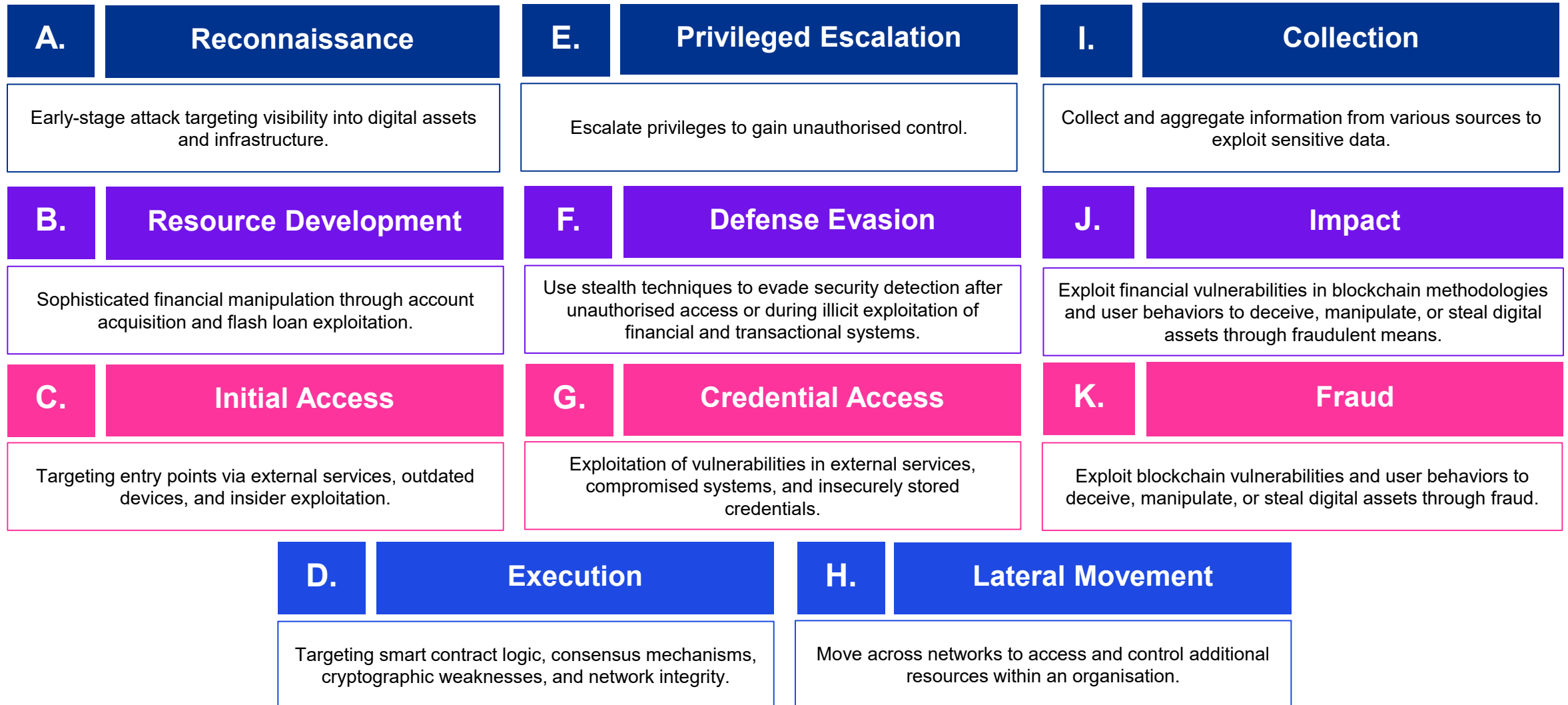
Fraud

Discovery

Command and Control

Exfiltration

Overview of AADAPT enterprise tactics



Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

A. Reconnaissance

#	Techniques/Sub-techniques	Description	Risks Identified • Data Leakage • Smart Contract Logic Exposure • Identity Compromise • Oracle Manipulation • Timestamp Exploitation Our Mitigation Strategies • Enforce strong access controls • Apply secure coding practices • Conduct thorough smart contract audits • Design resilient infrastructure • Implement zero-trust frameworks • Follow least privilege principle
1	Channel Worm-holing	A threat actor inside a private group on Hyperledger Fabric can secretly connect to outsiders and leak sensitive data from everyone in the group without them knowing.	
2	Default Visibility Abuse	A threat actor may analyse unintentionally exposed functions and variables in smart contracts to gather information for potential attacks.	
3	Endorser Identity Exposure	A threat actor may identify endorser identities in Hyperledger Fabric endorsement policies to launch attacks compromising privacy, network integrity, and availability.	
4	Non-deterministic Component Analysis	A threat actor may analyse nondeterministic components in smart contracts to identify exploitable vulnerabilities and manipulate contract behavior.	
5	Oracle Analysis	A threat actor may identify the specific oracles utilised by a target smart contract to compromise the contract's intended functionality.	
6	Timestamp Dependence Analysis	A threat actor may examine transaction timestamps to predict the timing and sequence of events within a smart contract. Smart contracts often rely on timestamps to execute critical logic, functions at specific times, or to enforce conditional triggers.	

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

B. Resource Development

#	Techniques/Sub-techniques	Description
1	Acquire Accounts	A threat actor may create valid digital asset system accounts to facilitate siphoning stolen funds.
2	Default Visibility Abuse	A threat actor may analyse unintentionally exposed functions and variables in smart contracts to gather information for potential attacks.

- Risks Identified**
 - Unauthorised access
 - Abuse of flash loans
 - Market manipulation
- Our Mitigation Strategies**
 - Enforce strong identification verification
 - Monitor account behavior for anomalies
 - Apply transaction limits
 - Use circuit breakers
 - Embed safeguards in smart contract logic

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

C. Initial Access			Risks Identified • Unauthorised access via vulnerable third-party services. • Exploitation of unpatched or obsolete devices. • Insider-assisted breaches compromising system integrity. Our Mitigation Strategies • Secure integrations with regular vulnerability assessments. • Decommission legacy systems and enforce patch management. • Monitor user behavior and apply role-based access controls.
#	Techniques/Sub-techniques	Description	
1	Exploit External Services	A threat actor may exploit the vulnerabilities in external services to gain unauthorised access to connected digital asset systems.	
2	Exploit Obsolete Device	A threat actor may leverage unpatched vulnerabilities in an obsolete device to steal value-form from digital asset wallets or inflict reputational damage.	
3	Insider - Assisted Access	A threat actor may exploit an insider to gain unauthorised access to the digital asset system.	

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

D. Execution		
#	Techniques/Sub-techniques	Description
1	Exploit Blockchain Technology Specific Vulnerabilities	A threat actor can exploit vulnerabilities specific to the underlying blockchain technology of a digital asset system.
2	Circumvent Voting Majority Control	A threat actor may seize control over more than 51 per cent of a network's hash rate and add new blocks to the chain at a rate faster than all other validators on the network.
3	Double - Spending Attack	A threat actor may exploit the consensus logic to spend the same digital assets multiple times to create fraudulent transactions.
4	Sybil Node Creation	A threat actor may create numerous fake nodes, or Sybil nodes, on a blockchain to manipulate the network's honest protocol behavior and gain undue influence.
5	Fault-Injection Attacks	A threat actor may place a device under external stress to deduce key values by comparing faulty program output against expected program behavior.
6	Quantum Efficient Factorization	A threat actor may utilise quantum efficient factorization algorithms to circumvent obsolete encryption implementations.
7	Side-Channel Attack	A threat actor may create valid digital asset system accounts to facilitate siphoning stolen funds.

Risks Identified

- Signature replay across chains
- Blockchain and consensus logic flaw
- Sybil Node abuse and 51 per cent attacks
- Quantum or side-channel cryptographic breaches
- Malicious smart contracts and oracle manipulation

Our Mitigation Strategies

- Deploy reentrancy guards, validate execution flow, and audit smart contracts
- Enforce chain-specific signature checks and adopt quantum-resistant encryption

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

D. Execution		
#	Techniques/Sub-techniques	Description
8	Evil Contract	A threat actor may develop and deploy a malicious smart contract designed to exploit blockchain vulnerabilities and execute unauthorised or deceptive functions.
9	Gas Griefing	A threat actor may manipulate how much gas is sent to a smart contract so that sub-calls and external communications for a given transaction cannot execute to induce unpredictable behavior and block future transactions from taking place.
10	Oracle Manipulation	A threat actor may alter external data feeds to deceive smart contracts into executing unauthorised actions.
11	Contract Ownership Changes	A threat actor can exploit weak access controls to execute malicious functions.
12	Reentrancy	A threat actor may exploit a reentrancy vulnerability in a smart contract to repeatedly call a function before the previous call has completed.
13	Signature Replay Attack	A threat actor may reuse another entity's digital signature obtained from one blockchain to carry out a transaction on another blockchain, causing the victim to incur financial losses without their knowledge or consent.

Risks Identified

- Signature replay across chains
- Blockchain and consensus logic flaw
- Sybil Node abuse and 51 per cent attacks
- Quantum or side-channel cryptographic breaches
- Malicious smart contracts and oracle manipulation

Our Mitigation Strategies

- Deploy reentrancy guards, validate execution flow, and audit smart contracts
- Enforce chain-specific signature checks and adopt quantum-resistant encryption

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

E. Privilege Escalation		
#	Techniques/Sub-techniques	Description
1	Exploit Smart Contract Hierarchical Ownership	A threat actor can exploit vulnerabilities in the hierarchical ownership structure of a smart contract, allowing them to gain unauthorised control or privileges within the contract.

Risks Identified

- Signature replay across chains
- Blockchain and consensus logic flaw
- Sybil Node abuse and 51 per cent attacks
- Quantum or side-channel cryptographic breaches
- Malicious smart contracts and oracle manipulation

Our Mitigation Strategies

- Deploy reentrancy guards, validate execution flow, and audit smart contracts
- Enforce chain-specific signature checks and adopt quantum-resistant encryption

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

F. Defense Evasion

#	Techniques/Sub-techniques	Description
1	Transaction Limit	A threat actor may circumvent the transaction limit to evade identification during exfiltration.
2	Withdrawal Limit	A threat actor may circumvent the withdrawal limit to exfiltrate large amounts of stolen funds.
3	Cross-Chain Swaps (Hopping)	A threat actor may exchange illicitly acquired digital assets across multiple blockchains to obscure their origin and evade detection.
4	Anonymous Wallets	A threat actor may transfer stolen or illicit funds to anonymous wallets, which are designed to protect the privacy and confidentiality of their users.
5	Money Mules	A threat actor may leverage money mules – willing or deluded agents to launder stolen digital assets, obscuring the financial trail and evading detection within a digital asset system.
6	Layering	A threat actor may obscure the origin of illicit funds through multiple complex transactions and processes, effectively "layering" the digital assets to make them difficult to trace.
7	Tumblers	A threat actor can conduct illicit transactions utilizing mixers or tumblers to pool their illicit cryptocurrency with other users in an online service and send "clean" cryptocurrency in different sums.

Risks Identified

- Evading transactional and withdrawal limits
- Obfuscation of asset origin via cross-chain swaps and layering
- Use of anonymous wallets and money mules to hide ownership and laundering via tumblers, mixers, and peel chains anonymously
- Exploiting peer-to-peer (P2P) exchanges lacking regulatory oversight

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

F. Defense Evasion

#	Techniques/Sub-techniques	Description
8	Peer to Peer Exchanges	A threat actor can utilise peer-to-peer exchanges to buy, sell, and trade cryptocurrencies without the regulatory supervision and protections of a commercial exchange.
9	Peel Chains	A threat actor can utilise peel chains to launder a large amount of cryptocurrency through a sequence of minor transactions.
10	CoinJoin	A threat actor can utilise a CoinJoin for Bitcoin transactions to combine inputs from different users and return multiple outputs with identical values.

Our Mitigation Strategies

- Enforce transaction and withdrawal limits with anomaly detection
- Monitor cross - chain and P2P activity for suspicious behavior
- Restrict access to anonymous wallets and unverified entities
- Detect and block mule networks using behavioral analytics
- Apply forensic tracing and pattern recognition to complex laundering methods
- Analyse and flag anonymization tools like CoinJoin, tumblers, and peel chains

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

G. Credential Access			
#	Techniques/Sub-techniques	Description	
1	Exploit External Services	A threat actor may exploit the vulnerabilities in external services to gain unauthorised access to connected digital asset systems.	Risks Identified • Exploitation of vulnerabilities in external services • Unauthorised access to connected digital asset systems • Searching for private key certificate files on compromised systems • Full asset compromise due to insecure credential storage Our Mitigation Strategies • Regularly patch and update external services • Enforce strong authentication and Securely store private keys and sensitive credentials • Perform regular security audits and assessments
2	Private Keys	A threat actor may search for private key certificate files on compromised systems for insecurely stored credentials to gain complete control over their assets.	

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

H. Lateral Movement		
#	Techniques/Sub-techniques	Description
1	Exploit Gas Free RPCs	A threat actor may abuse gas-free RPCs to gain unauthorised access to additional resources.
2	Insider Assisted Access	A threat actor may exploit an insider to gain unauthorised access to the digital asset system.

Risks Identified

- Abuse of gas - free RPCs for unauthorised access
- Exploitation of insider assistance to breach systems

Our Mitigation Strategies

- Enforce strict access controls and monitor RPC activity
- Conduct regular employee security training and background checks
- Apply multi-factor authentication and least privilege access

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

I. Collection

#	Techniques/Sub-techniques	Description
1	Aggregate Private Key Generation Data	A threat actor can collect and aggregate information concerning how private keys are generated in a digital asset system.
2	Intercept API Communication	A threat actor may intercept API communication to steal sensitive data.
3	Scrape Blockchain Data	A threat actor may scrape blockchain data to reveal sensitive information for exploitation.
4	Scrape KYC Data	A threat actor may scrape Know Your Customer (KYC) data to expose user identities.

Risks Identified

- Aggregation of private key generation data
- Interception of API communications
- Scraping of blockchain and KYC data for sensitive insights and to expose user identities

Our Mitigation Strategies

- Monitor anomalies and apply techniques to preserve privacy

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

J. Impact		
#	Techniques/Sub-techniques	Description
1	Induce Legal Regulatory Penalties	A threat actor may exploit vulnerabilities to induce legal and regulatory violations for the digital asset system or organization.
2	Long – Range Attack	A threat actor validator in a blockchain using Proof-of-Stake (PoS) consensus may create an illegitimate branch with at least the same length and genesis block as the original chain.
3	Burn Wallets	A threat actor can transfer stolen or illicit funds to burn wallets, wallets that have been abandoned or have lost their private keys, to make it impossible for anyone to recover the assets.

Risks Identified

- Inducing legal and regulatory violations
- Executing long - range attacks on pos blockchains
- Transferring funds to unrecoverable burn wallets
- Manipulating markets via pump and dump and related market spoofing schemes
- Damaging reputation and public trust in the system

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

J. Impact		
#	Techniques/Sub-techniques	Description
4	Pump and Dump	A threat actor may artificially inflate an asset's price to sell at a profit, causing the price to crash and leaving others with losses.
5	Wash Trading	A threat actor may rapidly buy and sell the same digital asset to create the illusion of market activity, misleading traders and manipulating the price of the digital asset for personal gain.
6	Stop Hunting	A threat actor may intentionally manipulate an asset's price to trigger stop-loss orders, causing a cascade of automatic selling and allowing them to buy the asset at a lower price for profit.
7	Whale Wall Spoofing	Whale wall spoofing is a market manipulation tactic where attackers place large fake buy/sell orders to create false demand or supply signals. This misleads traders into reacting, allowing the attacker to profit from the induced price movement by canceling the spoofed orders and trading at favorable prices.
8	Reputation Damage	Reputation damage involves adversaries spreading misinformation, disrupting operations, leaking sensitive data, or impersonating official accounts to erode trust in a digital asset system. This can lead to user distrust, regulatory scrutiny, financial losses, and increased vulnerability to future attacks.

Our Mitigation Strategies

- Enforce compliance with legal and regulatory standards
- Strengthen pos consensus mechanisms and validate chain integrity
- Flag transactions to burn wallets
- Implement surveillance tools to identify wash trading patterns

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

K. Fraud			Risks Identified • Long - range attacks to rewrite blockchain history • Exploiting partial payments to mislead recipients • Circumventing voting majority to validate unauthorised transactions • Double - spending via consensus manipulation • Cryptographic key interception and reverse engineering • Physical breaches of offline storage devices
#	Techniques/Sub-techniques	Description	
1	Long – Range Attack	An adversary can create a longer, fake blockchain to replace the real one, manipulating transaction history, erasing evidence, or gaining financial advantage especially dangerous in PoS systems where it requires minimal resources.	
2	Partial Payments Attack	A threat actor may exploit the partial payments feature on the XRP ledger platform to deceive the receiving party about the actual amount delivered.	
3	Circumvent Voting Majority Control	An adversary can exploit flaws in blockchain consensus mechanisms like gaining majority control to validate unauthorised transactions, disrupt operations, and compromise network integrity.	
4	Double-Spending Attack	A threat actor may exploit the consensus logic to spend the same digital assets multiple times to create fraudulent transactions. Different variants of this attack include race attacks, Finney attacks, and 51 per cent attacks.	

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

K. Fraud		
#	Techniques/Sub-techniques	Description
5	Cryptographic Protocol Analysis	A threat actor can capture cryptographic keys during the transfer of a digital asset value-form between purses to reverse engineer them.
6	Physical Breach	A threat actor may seize control of user devices used to store offline digital value-form and use invasive physical attacks (e.g. micro-probing, chip modification) to clone or manipulate this value-form.
7	Zero-Value Transfer Phishing	A threat actor can send fake zero-value transactions from lookalike addresses to trick users into sending money to the wrong wallet.

Risks Identified

- Phishing via zero - value transfers and address poisoning
- Node isolation through eclipse attacks
- Laundering via anonymous wallets, layering, money mules, and peel chains

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

K. Fraud		
#	Techniques/Sub-techniques	Description
8	Address Poisoning	A threat actor can send tiny fake transactions from lookalike addresses to trick users into copying and sending money to the wrong wallet.
9	Eclipse Attack	A threat actor isolates a target node in a decentralized network using a botnet and bandwidth constraints, enabling the threat actor to feed false data and manipulate the node for malicious purposes.
10	Anonymous Wallets	A threat actor may transfer stolen or illicit funds to anonymous wallets, which are designed to protect the privacy and confidentiality of their users.

Our Mitigation Strategies

- Strengthen consensus mechanisms and validate blockchain integrity
- Enforce transparency and verification in payment systems
- Monitor and secure voting mechanisms in blockchain governance
- Detect and block double - spending attempts with real - time consensus checks
- Secure cryptographic protocols and key exchanges
- Harden physical device security and offline storage practices
- Educate users on phishing tactics and verify wallet addresses

Enterprise tactics and attack techniques against digital assets

Tactic, Risks and Mitigation

K. Fraud		
#	Techniques/Sub-techniques	Description
11	Layering	A threat actor may use layering to obscure the origin of illicit funds by breaking them into smaller transactions and moving them through various platforms, making the trail complex and difficult to trace.
12	Money Mules	A threat actor may leverage money mules – willing or deluded agents to launder stolen digital assets, obscuring the financial trail and evading detection within a digital asset system.
13	Peel Chains	A threat actor may use peel chains — Small-step crypto laundering — to launder cryptocurrency by gradually transferring small amounts through multiple wallets to avoid detection and obscure the asset trail.

Our Mitigation Strategies

- Protect nodes from isolation with network diversity and monitoring
- Track laundering patterns using forensic analytics and compliance tools

Way Forward for Organizations – AADAPT Implementation Phases

Defining Scope

- **Identify key blockchain assets** such as smart contracts, wallets, bridges, and validators.
- **Identify digital asset exposure**, high-risk threat vectors, vulnerabilities, and past exploit cases.
- **Review business units**, handling blockchain assets to understand the associated processes, architecture, up streams and down streams.
- **Scope in SDLC and Incident Management Practices.**

Gap Assessment

- **Assess detection, response, and mitigation maturity.**
- **Perform gap assessment against existing controls to AADAPT™ techniques** across SOC and blockchain assets.
- **Highlight missing detection techniques** and unlinked response workflows.
- **Evaluate potential for anomaly detection** and automated attack response for missing techniques.

Align with AADAPT

- **Identify relevant AADAPT™ tactics** which apply to your business model.
- **Align existing SOC blockchain detection rules/security mechanisms** aligned with relevant AADAPT™ techniques.
- **Tag each technique with current detection coverage** and monitoring tools.
- **Document existing controls and preventive measures** for each technique.

Build and Implement

- **Build detection, playbooks, and conduct simulation training exercises** for AADAPT™ threats
- **Build response workflows** for high-risk scenarios like contract exploits.
- **Align resources for tabletop and red team drills** to test AADAPT™ readiness.
- **Align teams to Train** on AADAPT™ threats, tactics, and mitigation strategies.
- **Align performance indicators with threat coverage** and response efficiency.

How KPMG in India can help?

- **Review and Update Asset Catalogue.**
- **Review people, processes, technology aligned to the blockchain asset** to map out the threat exposure.

- **Identify missing Detection Techniques.**
- **Review existing controls for AADAPT™ Techniques.**

- **Test AADAPT™ Detection coverage in SOC.**
- **Review and Update AADAPT™ Control Mapping Document.**

- **Conduct Tabletop and Red Team Exercises**
- **Review and update Playbooks, KPIs.**

Contributors

- Aakansha Gupta
- Advait Khair
- Jay Goyal
- Vedant Paul

KPMG in India contacts:

Akhilesh Tuteja

Partner and Global Head – Cyber Security
T: +91 9871025500
E: atuteja@kpmg.com

Atul Gupta

Partner and Head of Function,
Digital Trust and Cyber
T: +91 98100 81050
E: atulgupta@kpmg.com

Kunal Pande

Partner, Co-Head - Digital Risk and
Cyber, Leader - Digital Trust for FS
T: +91 98926 00676
E: kpande@kpmg.com

Romharsh Razdan

Partner, Digital Trust
T: +91 99755 96366
E: romharsh@kpmg.com

Pratiksha Doshi

Partner, Digital Trust
T: +91 9967228986
E: pratikshadoshi@kpmg.com



Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.