منتدى الشراكة في مواجهة غسل الأموال
وتمويل الإرهاب
AML/CFT Partnership Forum

اللجنة الوطنية لمواجهة غسل الأموال ومكافحة
تمويل الإرهاب وتمويل التنظيمات غير المشروعة
National Anti Money Laundering and Combatting Financing
of Terrorism and Financing of Illegal Organizations Committee
General Secretariat الأمانة العامة

Virtual Assets and DeFi:
Risks and Mitigation

Digital Working Group

Table of Contents

Understanding And Mitigating risks – Virtual Assets And Decentralised Finance Landscape

In the last few years, the adoption of virtual assets ("VAs") and decentralised finance ("DeFi") has seen significant growth, driven by increasing institutional interest, regulatory clarity, and technological advancements.

Key Trends – UAE

Increased Ownership

According to research reports, the Middle East experienced a 166% surge in crypto adoption in 2024, with the number of daily active crypto traders soaring to over 700,000[1]. The UAE leads this growth, accounting for 7.5% of global transaction volume, with its daily trader count reaching around 500,000[2].

Institution Investment

There is a notable rise in institutional investors allocating larger portions of their portfolios to VAs, driven by high-net-worth individuals and venture capital firms[3]. Financial institutions are becoming more open to crypto, with 44% willing to offer bank accounts to crypto businesses and 21% already active in the space[4].

Against this backdrop and the evolving regulatory landscape to provide greater stability and legitimacy to the crypto market, banks, fintechs and payment providers are accelerating plans around VAs to tap new market opportunities. Many are developing strategies to integrate crypto into their services, focusing on compliance, risk management, and customer demand.

As UAE financial institutions look to expand and offer their financial services to VA service providers ("VASPs"), so too should their understanding of underlying and prevalent risks events that can materialize in VA and DeFi ecosystems. To take advantage of new market opportunities in the VA and DeFi space, it is essential for financial institutions to integrate sound risk appreciation and assessment into their operational and compliance processes and systems which will enable them to scale. This can be built from multiple sources, such as from reported risk events, industry standards, and publications from international standard setting bodies.

This paper discusses several approaches and tools that financial institutions or other institutions seeking to undertake VA and DeFi activities could consider in deepening their understanding of the risks inherent in the fast-evolving VA and DeFi ecosystems, and put in place appropriate risk management and compliance systems to mitigate impact from adverse events.

Event-Driven Analyses

Known risk events that have occurred in VA and DeFi ecosystems can serve as an effective reference to guide the appropriate risk mitigation measures that financial institutions may adopt. In this respect, a structured approach to extracting meaningful insights may involve aggregating an extensive database of hacking incidents, standardising classifications, followed by refining categorizations to ensure consistency and clarity of analyses.

[1] https://www.prnewswire.com/news-releases/bitget-report-middle-east-crypto-market-surges-daily-traders-up-166-in-year-302123303.html

[2] https://www.chainalysis.com/blog/middle-east-north-africa-mena-cryptocurrency-adoption/

[3] https://www.ainvest.com/news/institutional-investors-plan-83-increase-crypto-holdings-2025-2503-44/

[4] Elliptic_Report_State_of_Crypto_2025.pdf

A financial institution may start by gathering a dataset of historical hacking incidents from multiple sources[5] [6] [7] [8] including security reports, on-chain forensic analyses, and publicly available breach disclosures.

Given the diversity of security incidents in VA and DeFi ecosystems, such a dataset may contain a wide range of attack types, including blockchain protocol vulnerabilities, rug pulls[9], smart contract exploits, phishing scams, wallet breaches, and governance attacks.

To make sense of such diverse sets of information, it is important to start off with a system of classifying the various security events.

Event Labelling

Each security event can be classified under a label that captures the core nature of the attack. Labels comprising similar or related attack types can be further grouped into broader categories. For instance, multiple smart contract exploits — such as re-entrancy attacks[10], logic vulnerabilities, and unchecked input validation errors — can be grouped under a general smart contract vulnerability category.

Similarly, wallet-related breaches, including private key leakage, mnemonic phrase theft, and phishing-based wallet compromise, can be classified under a broader wallet security category.

Having a structured taxonomy facilitates the tiered application of a baseline suite of risk management measures across a common category of risk events, and a more granular set of measures catering to specific attack mechanisms within each category as appropriate.

FSRA Data Analysis

The Financial Services Regulatory Authority ("FSRA") of Abu Dhabi Global Market ("ADGM") collected and analysed over 1,800 unique hacking events that occurred between 2014 and 2024, and identified four broad categories.

Technology	Governance	Financial	Operational
Attacks that exploit weaknesses in blockchain protocols, smart contracts, cryptographic mechanisms, and software infrastructure	Real-world corporate changes, manipulations in voting mechanisms, protocol governance exploits, and decision-making vulnerabilities within decentralized autonomous organizations (DAOs)	Traditional risk domains such as credit, liquidity, as well as market-based exploits, including price manipulation, oracle attacks, and liquidity crises triggered by security weaknesses	Human errors, insider manipulation, and other off-chain / real-world events that may impact a VA or DeFi project

The following are examples of events noted from the data sources as categorised according to the above classification.

[5] REKT database, https://rekt.news/

[6] Slowmist event database, https://hacked.slowmist.io/en/

[7] Cointelegraph hacks news, https://cointelegraph.com/tags/hacks

[8] Chainalysis crypto crime reports, https://www.chainalysis.com/blog/category/crime/

[9] A rug pull is when a cryptocurrency project developer(s) abandons the project and abscond with investors' funds

[10] A re-entrancy attack occurs when attackers exploit weak coding in smart contracts that enable actions that should only occur once to be repeated. Such attacks allow attackers to drain funds as the smart contract does not complete a balance check before allowing the attacker to make a subsequent withdrawal

Technology Events

On-chain events

- Protocol upgrades, hard forks[11], that significantly alter network operation, security, or economics
- Exploitation of smart contract or protocol vulnerabilities, e.g., underlying bugs or loopholes in the smart contract's or protocol's code
- Attacks on the blockchain protocol, e.g., network congestion attack[12], random number attack[13]
- Impersonation on the blockchain, e.g., sleepminting[14]

Off-chain events

- Cyberattacks, e.g., DDoS attack[15], DNS attack[16], malware attacks, etc.
- Phishing and social engineering attacks leading to compromise of user accounts and private keys, e.g., pig butchering scams[17]

Governance Events

- Corporate restructuring – Changes in shareholders, takeovers, leadership changes, e.g., resignation of founders or key developers
- Changes of whitepaper or roadmap – Delays / cancellations / changes to feature releases
- On-chain governance attacks – Malicious governance proposals by attackers who gain access to majority voting tokens
- Regulatory actions / legal proceedings – Regulatory acceptance of the VA for payments, enforcement actions on the project / project team
- Underlying protocol changes affecting VA / DeFi projects – Significant changes to the protocol, e.g., switch from proof of work to proof of stake consensus mechanism

Financial Events

- Credit risk events arising from the project's inability to fulfil its debt obligations
- Liquidity risk events arising from significant changes in token supply
- Counterparty risk events typically arising from AML / CTF sanctions
- Market risk events, e.g., price volatility, delisting, etc.
- Stablecoin peg breaks resulting in significant devaluation and price volatility

[11] Hard forks are significant changes in programming that branches the blockchain and users have to choose between validating the existing branch or the new branch

[12] A network congestion attack arises when a large number of spam and false transactions are submitted to the network thereby preventing legitimate transactions from being validated

[13] An attacker can exploit weak code in smart contracts to reverse-engineer the random number generated that grants rewards for block validation through a random number attack

[14] Sleepminting occurs when an attacker leverages on code vulnerabilities in non-fungible token (NFT) smart contracts to impersonate artists and mint NFTs which would then be artificially sold back to the attacker

[15] A Distributed Denial of Service (DDoS) attack is the overwhelming of a target system with a flood of malicious internet traffic

[16] An attacker can redirect network traffic from a legitimate site to a malicious site under their control by compromising the domain name server (DNS) records or spoofing the DNS server via cache poisoning

[17] Pig butchering scams lure victims into making incremental monetary transfers to scammers for the purpose of investing in fraudulent schemes

- Tokenomics risk events arising from flaws in the economic design of a protocol / project, e.g., deficient lock-ups[18]
- Market misconduct e.g., arbitrage attack[19], oracle attack[20], flash loan attack[21]

Operational Events

- Acceptance of the VA for payments by major merchants / corporations / e-commerce platforms
- Human error in the development and deployment of the project / protocol
- Insider manipulation token activity / price
- Data leakage leading to reputational concerns
- Adverse events affecting hardware wallets, e.g., theft, loss, damage, etc.
- Real world adverse events, e.g., natural disasters

The insights drawn from the known risk events that have occurred may help inform the financial institution on the development of internal frameworks, policies and controls to address or mitigate adverse impact arising from such events.

Industry-Driven Views

Industry-driven resources are another rich source of information on approaches that can help financial institutions navigate the risks in VA and DeFi ecosystems. One such approach is described in the Decentralized Finance Risk Assessment Guidelines ("DeFi Guidelines")[22] established by a working group under the Enterprise Ethereum Alliance ("EEA")[23]. The EEA is a member-led industry organization that promotes the use of blockchain technology. While the EEA's work is primarily focused on promoting a specific blockchain platform, the DeFi Guidelines can be adapted to other blockchain technologies and DeFi platforms.

The DeFi Guidelines describes seven areas of risk that are inherent in DeFi, the key sets of information that would facilitate assessment of these risks, and mitigation strategies to address the risks. The DeFi Guidelines also provide metrics that can be used to measure risk factors in a risk assessment.

Software	Governance	Credit	Counterparty	Market	Compliance	Standards

Software Risks

- Smart Contracts – Bugs, exploits, and functional vulnerabilities causing asset theft, price manipulation, and liquidity issues
- Blockchain – Downtime, transaction delays, or malicious attacks like 51% attacks impacting network integrity

[18] Lock-ups, or vesting periods, refer to time periods where specific tokens cannot be traded or transacted, e.g., founder tokens locked up for some time immediately after an initial coin offering to increase confidence in the project

[19] Arbitrage attacks exploit inefficiencies in token prices across different exchanges and platforms

[20] Attackers can compromise the data source the Oracle relies on or the Oracle itself to provide false pricing data. Oracles provide real-world data (e.g., currency prices, weather information, etc.) to smart contracts and decentralized applications on blockchain networks

[21] An attacker takes an uncollateralized loan and exploits vulnerabilities in cryptocurrencies to manipulate prices and profit from artificially induced volatility

[22] EEA DeFi Risk Assessment Guidelines - Version 1, 17 July 2024, https://entethalliance.org/specs/defi-risks/

[23] Ethereum Enterprise Alliance, https://entethalliance.org/about-enterprise-ethereum-alliance/

- User Interface – Security flaws in user interfaces leading to user errors, malicious redirections, and financial loss
- Oracles – Exploits using manipulated data sources causing financial loss (e.g., flash loans, arbitrage manipulations)
- Bridges – Asset theft and systemic vulnerabilities across blockchain bridges
- Malicious Extracted Value – Manipulation of transactions causing user losses (e.g., front-running, sandwich attacks)

Governance Risks

- Governance – Malicious proposals or fund theft due to concentrated governance power
- Custodial – Loss or theft of private keys leading to asset loss or unauthorized transactions
- Tokenomics – Flawed economic designs that destabilize token value (e.g., inflationary or speculative)

Credit Risks

- Insufficient collateral or liquidators during market crashes result in bad debt for lenders

Counterparty Risks

- Failure by transacting parties to fulfil obligations leading to defaults and financial loss

Market Risks

- Asset volatility, liquidity shortages, or manipulative practices eroding confidence and protocol value
- Fragmented liquidity pools and insufficient buyers/sellers hindering asset conversion at fair value

Compliance Risks

- Regulatory Compliance – Failure to comply with AML/KYC standards or obtain necessary licences resulting in shutdowns or legal action
- Tax – Uncertainty in reporting and recognizing taxable events that can lead to legal scrutiny or penalties

Standards Risks

- Accounting Conformance – Applying inappropriate treatment of accounting standards for DeFi transactions
- Operational Accounting – Weak internal controls and inconsistent valuations resulting in financial errors or loss of protocol value

While the DeFi Guidelines serve a useful tool for DeFi organisations and financial institutions that have DeFi offerings, they can be adopted or adapted by regulatory authorities as well. For example, the ADGM's Registration Authority ("RA") that regulates and supervises Distributed Ledger Technology ("DLT") Foundations[24] has incorporated the DeFi Guidelines into its assessment process, among other requirements, for licence applications.

Views from International Standard Setting Bodies

In recent years, international standard setting bodies ("SSBs") for financial services and markets have published research, discussion papers, consultations, and policy recommendations that regulators around the world can adopt to enhance local regulatory frameworks and guidance.

[24] DLT Foundations Framework, https://www.adgm.com/dlt-foundations

The following SSBs have issued publications that relate to risks present in VA and DeFi ecosystems.

Bank for International Settlement (BIS)

The BIS supports central banks' pursuit of monetary and financial stability through international cooperation, and to act as a bank for central banks. The BIS provides central banks with a forum for dialogue and broad international cooperation, a platform for responsible innovation and knowledge sharing, in-depth analysis and insights on core policy issues, and sound and competitive financial services[25].

International Organization for Securities Commissions (IOSCO)

The IOSCO is an international body for securities regulators and is recognized as the global standard setter for financial markets regulation. IOSCO develops, implements and promotes adherence to internationally recognized standards for financial markets regulation[26].

Financial Stability Board (FSB)

The FSB promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies[27].

A compendium of publications by these SSBs are at **Annexure**.

An Integrated View

As shown above, there are different approaches to identifying and analysing risks in the VA and DeFi ecosystems. It is important to recognise that there is no one best approach, as they are contextual and often inter-related. For example, many of the risks identified in the SSB publications could be considered under financial, governance, and technological risks.

Similarly, the industry-driven approach has multiple financial-related risks that could be consolidated. Financial institutions can benefit from an integrated approach to implementing and adapting frameworks and systems that best fit their circumstances and business models.

It is also important to integrate these frameworks with existing financial regulatory frameworks that deal with risks associated with their regulated activities.

This will ensure that prevailing risk areas such as money laundering and terrorism financing, and other conduct and prudential aspects are adequately captured within the risk universe of financial institutions.

Leveraging Technological Solutions for Risk Mitigation

The digitally native nature of VA and DeFi ecosystems presents a unique opportunity for the use of technology to effectively manage the risks inherent in the space. By leveraging advanced technologies such as blockchain analytics, smart contract auditing tools, AI-driven monitoring systems, and secure governance platforms, financial institutions, VASPs and regulators alike can significantly enhance their capacity to identify, prevent, and respond to risk events. This section outlines potential technological solutions that can aid in supervising and mitigating risks in support of a resilient and secure VA and DeFi ecosystem.

Technology Risk Mitigation

Pre-emptive Measures

- Pre-emptive measures form the first and most critical line of defence against technological risks within VA and DeFi ecosystems. Ensuring software and system components are continuously updated with the latest security patches and adhering to industry-standard coding practices can significantly reduce the potential attack surface. Regular smart contract audits conducted by

[25] https://www.bis.org/

[26] https://www.iosco.org/

[27] https://www.fsb.org/

reputable, independent auditors, combined with structured bug bounty programs, further strengthen critical systems by proactively identifying and remediating vulnerabilities before exploitation

- To ensure compliance, financial institutions can implement periodic technology audits, regular security assessments, and advanced security measures, such as formal verification for critical smart contracts[28]. Employing automated vulnerability scanning, penetration testing, and continuous monitoring further enhances the detection and mitigation of potential exploits

Detection and Monitoring Measures

- Financial institutions should consider employing blockchain analytics tools capable of tracking on-chain transactions, identifying anomalous behaviours, and detecting early warning signs of potential attacks, such as unusual transaction patterns or smart contract interactions indicative of exploitation attempts. Additionally, leveraging security event monitoring solutions, log monitoring, and automated alerting tools, enhances visibility into emerging threats.

Governance Risk Mitigation

Pre-emptive Measures

- The prevention of governance risk falls into the design and implementation of robust governance frameworks and voting mechanisms. Platforms such as Aragon[29], Snapshot[30], Tally[31], and others, facilitate the creation of customizable governance models, enabling DAOs to define roles, voting mechanisms, and proposal processes that align with their specific needs and robust governance controls.

Detection and Monitoring Measures

- Continuous monitoring of governance activities is vital to detect anomalous or malicious actions promptly. For example, DeepDAO[32] provides analytics dashboards that track proposal submissions, voting patterns, and participant engagement. By integrating both on-chain voting and off-chain activities (e.g. discussions in web forum), these platforms can offer real-time insights into the DAO's governance health.

Financial Risk Mitigation

Pre-emptive Measures

- With a spectrum of financial-related risks, it is crucial that VA and DeFi projects are designed well and with strong tokenomics considerations. Additionally, VA and DeFi projects can consider utilising multiple robust oracles to reduce price manipulation via oracle attacks, utilising private mempools[33] to mitigate front-running and arbitrage attacks, and adopt tools such as Machinations.io[34] for designing, simulating, and testing robust tokenomics models.

Detection and Monitoring Measures

- Effective financial risk monitoring should involve multiple specialized tools. While there are customised solutions available to firms, the common blockchain analytics platforms like

[28] Formal verification of smart contracts is a process that determines if the smart contract is functioning as intended and meets desired specifications. This is typically done using mathematical proofs to verify the logic coded into the smart contract

[29] Aragon,

[30] Snapshot, https://snapshot.box/

[31] Tally, https://www.tally.xyz/

[32] DeepDao, https://deepdao.io/

[33] Inside the private mempools where Ethereum traders hide from running bots, https://www.coindesk.com/tech/2024/01/31/inside-the-private-mempools-where-ethereum-traders-hide-from-front-running-bots

[34] Machinations, https://machinations.io/

Chainalysis[35], Elliptic[36] and TRM Labs[37] help reduce counterparty risks by identifying illicit transactions. Platforms such as Gauntlet[38] provide on-chain risk analytics and stress testing to optimize DeFi protocol parameters and dashboards such as Dune[39] and DeFiLlama[40] offer real-time insights into stablecoin health, liquidity conditions, and overall market stability. Certain financial risks can be monitored by processing raw data from these platforms or directly utilising the metrics provided.

Operational Risk Mitigation

Pre-emptive Measures

- Operational risks can be reduced by conducting comprehensive training programs that enhance team members' understanding of VA and DeFi risks, security best practices, and regulatory requirements. Firms should also establish robust internal controls including clear operational procedures, segregation of duties, and multi-signature authorisation for critical transactions. The major wallet service providers, such as Fireblocks[41], Ledger[42], and Safe[43], offer secure configurations on their platforms that can be incorporated into a firms' operational processes.

Detection and Monitoring Measures

- While existing enterprise risk management tools can continue to be effective in detecting and monitoring operational risks, firms should increase the degree of automation to detect and monitor operational risk events given the digital-native nature of VA and DeFi projects.

Incident Response and Recovery

- Cutting across all risk categories are actions to be taken and tools to be deployed to support incident response and recovery. In this regard, regulators and financial institutions have a part to play, along with the VA and DeFi ecosystem partners to proactively contain, investigate, and recover from incidents.
- Regulators should develop reporting requirements for timely notification of incidents from affected firms and customers. Regulators can also facilitate awareness-building of emerging threats by disseminating alerts and advisories about emerging threats. Crucially, regulators should establish lines of communications with other regulatory bodies to potentially contain spillover risks across jurisdictions.
- Financial institutions have responsibilities to mitigate the impact and manage the technical response. Immediate actions can include activating emergency stop or "circuit breaker" functions on their platforms and smart contracts, temporarily halting asset withdrawals, utilising blockchain forensic and analytics tools, and initiating comprehensive root-cause investigations. Firms should also implement recovery procedures such as secure asset restoration (e.g. Fireblocks, Ledger, and CoinCover[44]) to restore normal operations quickly.

Finally, with the acceleration in AI technology adoption, financial institutions and regulators should explore the integration of AI into supervisory technologies to enhance compliance monitoring and risk management in the VA and DeFi space. Some case studies and explorations into the use of AI for

[35] Chainalysis, https://www.chainalysis.com/

[36] Elliptic, https://www.elliptic.co/

[37] TRM Labs, https://www.trmlabs.com/

[38] Gauntlet, https://www.gauntlet.xyz/

[39] Dune, https://dune.com/

[40] DeFiLlama, https://defillama.com/

[41] Fireblocks, https://www.fireblocks.com/

[42] Ledger, https://www.ledger.com/

[43] Safe{Wallet}, https://app.safe.global/

[44] CoinCover, https://www.coincover.com/

enhancing supervisory and regulatory technologies are set out in a recent joint publication by the ADGM Academy and the Asian Institute of Digital Finance[45] of the National University of Singapore.

Conclusion

From primary research and data-driven analyses, to industry-driven frameworks and frameworks espoused by SSBs, the different approaches offer varied perspectives on understanding risks in the VA and DeFi ecosystems. Where appropriate, an integration of these approaches and traditional regulatory frameworks may offer a comprehensive appreciation of the risks present in the fast-evolving marketplace.

As the VA and DeFi ecosystems evolve, so too have the tools that financial institutions and regulators can adopt to manage risks. Greater adoption of tools and automation of work processes will help them keep pace with industry and market developments. As the VA and DeFi ecosystems mature, a deeper understanding of associated risks will grow among financial institutions, regulators and SSBs. It is important for all parties to sustain efforts in understanding trends and evolving business models, their associated risks, and measures that can be implemented to prevent and mitigate impact from adverse events.

[45] AI Applications in Web3 SupTech and RegTech: A Regulatory Perspective, 13 February 2025, https://www.adgmacademy.com/publications/AI-Applications-in-Web3-SupTech-and-RegTech-A-Regulatory-Perspective/

Annexure

Publications by the BIS

DeFi risks and the decentralisation illusion

- Leverage
- Liquidity mismatches and run-risk in stablecoins
- Linkages with the traditional financial systems

Cryptocurrencies and Decentralised Finance[1]

- Data privacy and transparency
- Economic rents
- Transaction costs
- Governance
- Systemic risk

The Financial Stability Risks of Decentralised Finance

- Operational – Governance, Blockchain dependence, Smart contracts, Oracles and bridges
- Leverage - Automatic liquidation of collateral
- Interconnectedness – Composability, Concentration of critical functions
- Liquidity - Stablecoins and lending platforms
- Other - Market integrity, Cross-border regulatory arbitrage, "Cryptoization"

Publications by IOSCO

Report on Decentralised Finance

- Asymmetry and fraud risks
- Market integrity risks
- Front-running
- Flash loans
- Market dependencies
- Use of leverage
- Illicit activity risks
- Operational and technology-based risks
- Cybersecurity
- Governance risks
- Spillover of risks to centralised/traditional markets

Policy Recommendations for Crypto and Digital Asset Markets

- Conflicts of interest arising from vertical integration of activities and functions
- Market manipulation, insider trading and fraud
- Cross-border risks and regulatory co-operation
- Custody and client asset protection
- Operational and technological risk
- Retail access, suitability, and distribution

Policy Recommendations for Decentralised Finance Consultation Report

- Pseudonymity/anonymity
- Information asymmetries
- Cyber exploits/attacks
- Legal compliance
- Governance token proposal and voting risks
- Implementation risks
- Risks associated with leveraged strategies in DeFi
- Risks associated with liquid staking
- Liquid staking concentration validators
- Smart contract risk
- DAO governance risk
- Redemption value and counterparty risks to user
- Risks associated with other emerging derivative protocols, i.e., perpetual swaps, synthetic crypto-assets, options on crypto-assets
- Risks associated with oracles, i.e., risk of manipulation, mispricing risks
- Risks associated with the use of automated liquidation mechanisms

Publications by FSB

Assessment of Risks to Financial Stability from Crypto-assets

- Financial sector exposures
- Wealth effects
- Confidence effects
- Use in payments and settlements
- Global stablecoins

The Financial Stability Risks of Decentralised Finance

- Operational fragilities
- Liquidity and maturity mismatches
- Leverage
- Interconnectedness, concentration and complexity
- Other vulnerabilities, i.e., market integrity, cross-border regulatory arbitrage, cryptoization

Sources:

- DeFi risk and the decentralisation illusion, BIS Quarterly Review, 6 December 2021, https://www.bis.org/publ/qtrpdf/r_qt2112b.htm
- Cryptocurrencies and Decentralised Finance (DeFi), BIS Working Papers, 16 December 2022, https://www.bis.org/publ/work1061.htm
- The financial stability risks of decentralized finance, FSI Executive Summaries, 31 August 2023, https://www.bis.org/fsi/fsisummaries/defi.htm
- IOSCO Decentralised Finance Report, March 2022, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf
- Policy Recommendations for Crypto and Digital Asset Markets, 16 November 2023, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf
- Policy Recommendations for Decentralised Finance (DeFi) Consultation Report, September 2023, https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdfhttps://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf
- Assessment of Risks to Financial Stability from Crypto-assets, Reports to the G20, 16 February 2022,
- https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/
- The Financial Stability Risks of Decentralised Finance, Reports to G20, 16 February 2023, https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/

Authored by:

Wai Lum Kwok (Member, DWG)

Reviewed by:

Nishanth Nottath, Mark Newfield, David Shepherd, Nipun Srivastava, Dr Yoonus Ahammed, Bhavin Shah, Javier Pimentel, Lana Kershaw

Title: Virtual Asset and DeFi : Risks and Mitigation

Compiled by: Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti-Money Laundering and Counter Terrorism Financing in the United Arab Emirates.

Disclaimer: Despite the careful efforts made by DWG to prevent errors or omissions in this document, any unintentional mistakes or omissions are not intended. The information presented herein is solely for reference, educational, and awareness purposes and is subject to change without notice. It is important to acknowledge that DWG or any affiliates cannot be held responsible for any damage, loss, or other consequences arising from activities undertaken based on the information provided in this document.

Languages: English

Number of pages: 14 (including cover)

Edition: 1st edition

Month and year of publication: May 2025

This document is not for sale. This document shall be distributed by Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti-Money Laundering and Counter Terrorism Financing in the United Arab Emirates or their affiliates to individuals and entities as they deem fit.