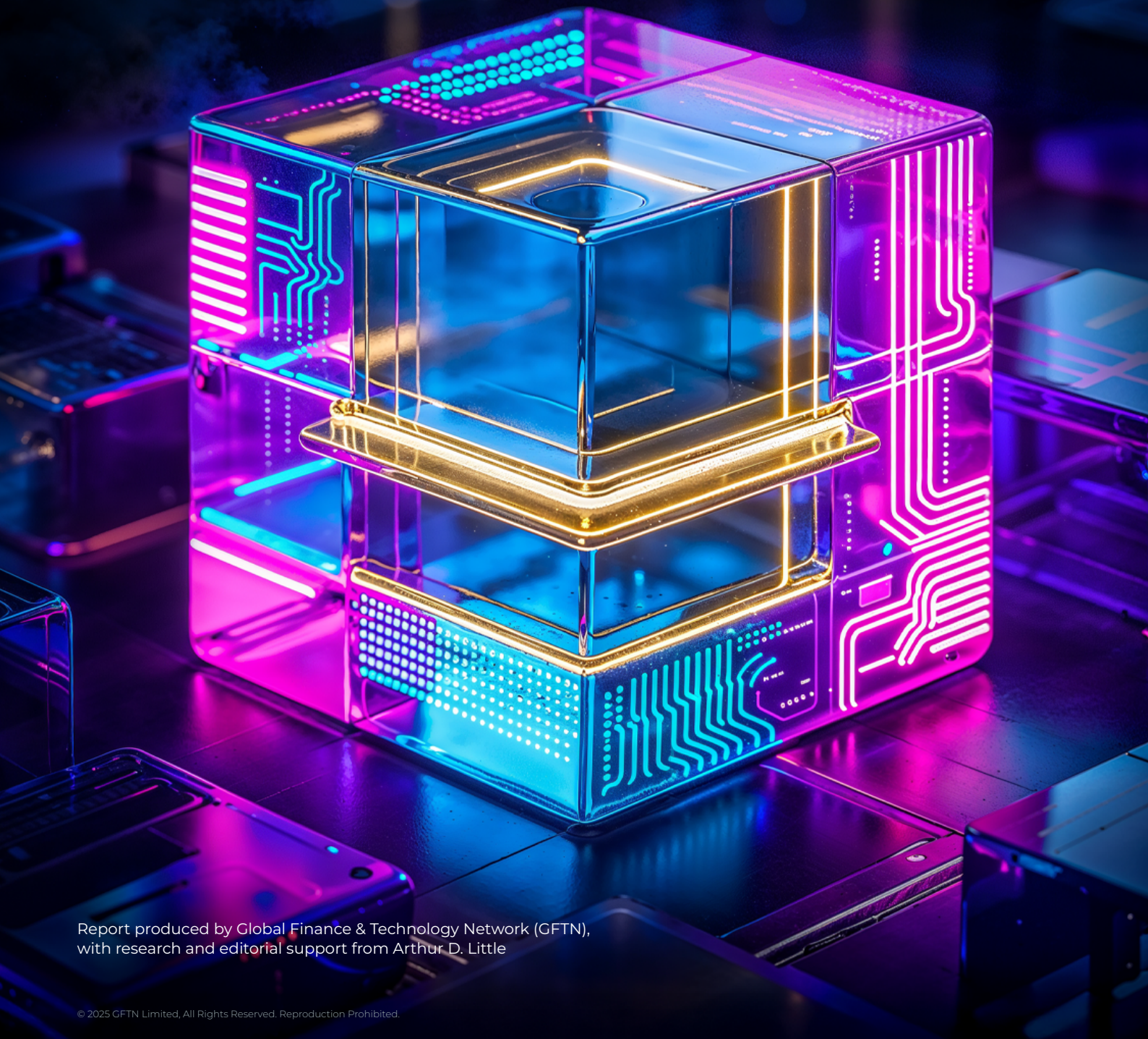
FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN

GFTN Global Digital Assets Report

Policy Evolution Market Development Future Pathways



Report produced by Global Finance & Technology Network (GFTN), with research and editorial support from Arthur D. Little

Contents

Acknowledgements

Global Finance & Technology Network (GFTN) would like to express deep gratitude to our members Amazon, Binance, ByBit, Circle, Coinbase, Digit9, OKX, Paxos, Ripple, Solana, Temasek, and Visa whose support and partnership made this report possible.

GFTN wishes also to extend special thanks to Arthur D. Little and Whitesight for their invaluable contribution in providing research support and editorial services for this comprehensive report.

We further extend our sincere thanks to the policymakers, regulators, and financial authorities, including the Bank of England, European Commission, Banque de France, Hong Kong Monetary Authority, Interpol Financial Crime and Anti-corruption Centre, Financial Services Agency Japan, Qatar Financial Centre, Monetary Authority of Singapore, Swiss Financial Market Supervisory Authority, Bank of Thailand, and the many industry leaders listed below; whose generous contribution of their insights and time were instrumental to the development of this report.

Contributors

Pradyumna Agrawal
Managing Director,
Investment, Temasek

Maha Al-Saadi
Head – Regulatory Affairs,
Financial Services Sector, Qatar Financial Centre

Niki Ariyasinghe
Head of Business Development,
Asia-Pacific and Middle East,
Chainlink Labs

Isadora Arredondo
Global Policy Director,
Hedera

Bruno Batavia
Principal & Director of Emerging Tech,
Valor Capital

Lee Brenner
Head of Public Policy,
Digital Assets, Goldman Sachs

Arnaud Caudoux
Deputy Chief Executive Officer,
BPI France

Clinton Chen
Senior Managing Counsel,
Regulatory Affairs, Visa

Joseph Cleetus
Vice President Business Transformation,
LuLu Financial Holdings

Ezechiel Copic
Director, Digital Currency Policy,
Visa

Lex Fisun
CEO & Co-Founder,
Global Ledger

Frederik Gregaard
CEO,
Cardano Foundation

Walter Hessert
Head of Strategy,
Paxos

David Hui
Chief Commercial Officer,
DBS Digital Exchange

Yip Kah Kit
Executive Director,
Head of Blockchain and Digital Assets,
UOB

Sungyong Kang
Criminal Intelligence Officer,
Interpol Financial Crime and Anti-corruption Centre

Peter Kerstens
Advisor for Financial Sector Digitalisation and Cybersecurity,
European Commission

Yam Ki Chan
Vice President,
Asia Pacific, Circle

Joe Kohler
Chief Legal and Chief Operating Officer,
Nethermind

Bjørn Krog Andersen
Chief Compliance Officer,
Banking Circle

Park Kwan Hoon
Executive Director, Group Strategic Planning Office, OCBC

Deng Chao
CEO,
HashKey Capital

Rosemary Lim
Executive Director,
Payments Department,
Monetary Authority of Singapore

Fernando Luis Vasquez Cao
Senior Advisor,
SBI Digital Asset Holdings

Robert MacDonald
Chief Legal & Compliance Officer,
Bybit

Naveen Mallela
Global Co-Head, Kinexys by J.P. Morgan

Jesse McWaters
Executive Vice President,
Head of Global Government Affairs,
Mastercard

Audrey Metzger
Director,
Innovation and Financial Markets Infrastructures, Banque de France

Terk Ming Kwong
Executive Director,
Government Affairs, Goldman Sachs

Katie Mitchell
Head of APAC and Middle East Policy,
Coinbase

Fiona Murray
Managing Director APAC,
Ripple

Tom Mutton
Director of Fintech,
Bank of England

Matthias Obrecht
Head,
Market Analysis, FINMA
(Swiss Financial Market Supervisory Authority)

Karen Ottoni
Sr. Director of Ecosystem & Strategic Initiatives, Linux Foundation Decentralized Trust

Haseeb Qureshi
Managing Partner,
Dragonfly

Ari Redbord
Global Head of Policy and Government Affairs, TRM Labs

Jason Rozovsky
Head of Legal & Policy,
InterOp Labs

Dr Daranee Saeju
Assistant Governor,
Bank of Thailand

Richard Teng
CEO,
Binance

Pucktada Treeratpituk
Director,
Fintech Office, Bank of Thailand

Ryosuke Ushida
(then) Chief Fintech Officer,
Financial Services Agency, Japan (JFSA)

Roeland Van Der Stappen
Head of E.U. Policy,
Coinbase

Masashi Watanabe
Managing Director,
Head of Digital Asset, Mitsubishi UFJ Financial Group

Tang Wei
Head of Public Policy,
Southeast Asia and Greater China,
Stripe

Star Xu
Founder and CEO,
OKX

Lu Yin
APAC Lead,
Solana Foundation

GFTN Contributors

Aanault Lee

Kaitlyn Thinn

Gabriel Lee

Bernice Neo

Chek Tchung Foo

Akanksha Rath

Rafat Kapadia

Princeton Ang

Production

Carol Ann Christy

Regina Mok

Shanell Chia

Loo Pooi Joo

Abbreviations

Acronym	Description	Acronym	Description	Acronym	Description
ADGM	Abu Dhabi Global Market	**CBDC**	Central Bank Digital Currency	**dApps**	Decentralized Applications
AED	Arab Emirates Dirham (currency of U.A.E.)	**CBU.A.E.**	Central Bank of the United Arab Emirates	**DDEx**	DBS Digital Exchange
AFM	Authority for the Financial Markets (Dutch)	**CCIP**	Cross-Chain Interoperability Protocol	**DeFi**	Decentralized Finance
AI	Artificial Intelligence	**CCTP**	Cross-Chain Transfer Protocol	**DEX**	Decentralized Exchange
AML	Anti-Money Laundering	**CDD**	Customer Due Diligence	**DFSA**	Dubai Financial Services Authority
AMLA	Anti-Money Laundering Act	**CDN**	Content Delivery Network	**DID**	Decentralized Identity
AMLO	AML Ordinance	**CeDeFi**	Centralized–Decentralized Finance	**DIF**	Decentralized Identity Foundation
AMLR	Anti-Money Laundering Regulation	**CeFi**	Centralized Finance	**DIFC**	Dubai International Financial Centre
AMM	Automated Market Maker	**CEXs**	Centralized Exchanges	**DINO**	Decentralized in Name Only
API	Application Programming Interface	**CFT**	Counter-Terrorist Financing	**DLD**	Dubai Land Department
APR	Annual Percentage Rate	**CFTC**	Commodity Futures Trading Commission	**DLT**	Distributed Ledger Technology
APTCP	Act on Prevention of Transfer of Criminal Proceeds	**CIS**	Collective Investment Scheme	**DNB**	De Nederlandsche Bank
ARTs	Asset-Referenced Tokens	**CMTA**	Capital Markets and Technology Association	**DOJ**	Department of Justice (U.S.)
ATS	Alternative Trading System	**CNAD**	National Commission of Digital Assets	**DPoS**	Delegated Proof of Stake
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Germany)	**CNY**	Chinese Yuan (RMB) / Digital Yuan (e-CNY)	**DPT**	Digital Payment Token (used in Singapore regulatory framework)
BIS	Bank for International Settlements	**CSAO**	Central & Southern Asia and Oceania	**DSA**	Digital Settlement Asset (term used by U.K. regulators for stablecoin frameworks)
BMA	Bermuda Monetary Authority	**CSDs**	Central Securities Depositories	**DSS**	Digital Securities Sandbox
BUIDL	BlackRock's USD Institutional Digital Liquidity	**CSSF**	Commission de Surveillance du Secteur Financier	**DTCC**	The Depository Trust and Clearing Corporation
CaaS	Crypto-as-a-Service	**CVM**	Comissão de Valores Mobiliários (Brazil's Securities and Exchange Commission)	**DTSP**	Digital Token Service Provider
CAGR	Compound Annual Growth Rate	**CySEC**	Cyprus Securities and Exchange Commission	**DVNs**	Decentralized Verifier Networks
CAISP	Crypto-Asset Intermediary Service Provider	**DAI**	Decentralized Stablecoin (issued by MakerDAO)	**DvP**	Delivery versus Payment
CASP	Crypto-Asset Service Provider	**DAO**	Decentralized Autonomous Organisation	**EBA**	European Banking Authority

Acronym	Description	Acronym	Description	Acronym	Description
ECB	European Central Bank	**FSA**	Financial Services Agency (Japan)	**JFSA**	Financial Services Agency, Japan
EDD	Enhanced Due Diligence	**FSMA**	Financial Services and Markets Act (U.K.)	**JVCEA**	Japan Virtual and Crypto Assets Exchange Association
EDSSI	European Digital Identity and Services Infrastructure	**FSRA**	The Financial Services Regulatory Authority (Abu Dhabi, U.A.E.)	**KYC**	Know Your Customer
EMI	Electronic Money Institutions	**FSTB**	Financial Services and the Treasury Bureau (Hong Kong)	**LATAM**	Latin America
EMIR	European Market Infrastructure Regulation	**FX**	Foreign Exchange	**LST**	Liquid Staking Token
EMTs	E-Money Tokens	**GDPR**	General Data Protection Regulation (E.U.)	**MAS**	Monetary Authority of Singapore
ERC	Ethereum Request for Comments	**GENIUS Act**	The Guiding and Establishing National Innovation for U.S. Stablecoins Act	**MENA**	Middle East and North Africa
ESMA	European Securities and Markets Authority	**GFTN**	Global Finance & Technology Network	**MFSA**	Malta Financial Services Authority
ETF	Exchange-Traded Fund	**GIFT**	Gujarat International Finance Tec-City (India)	**MiCA**	Markets in Crypto-Assets Regulation
ETH	Ethereum	**HKD**	Hong Kong Dollar	**MiFID**	Markets in Financial Instruments Directive (E.U.)
ETPs	Exchange-traded Products	**HKMA**	Hong Kong Monetary Authority	**MMF**	Money Market Funds
E.U.	European Union	**HNWI**	High Net Worth Individual	**MoU**	Memorandum of Understanding
EUDI	European Digital Identity	**HQLA**	High-Quality Liquid Assets	**MPC**	Multi-Party Computation
FATF	Financial Action Task Force	**IDB**	Inter-American Development Bank	**MSB**	Money Services Business
FBI	Federal Bureau of Investigation	**IDO**	Initial DEX Offering	**MTLs**	Money Transmitter Licences
FCA	The Financial Conduct Authority (U.K.)	**IFSCA**	International Financial Services Centres Authority (India)	**MUFG**	Mitsubishi UFJ Financial Group
FDIC	Federal Deposit Insurance Corporation (U.S.)	**IMF**	International Monetary Fund	**NYDFS**	New York Department of Financial Services
FHE	Fully Homomorphic Encryption	**IMG**	Implementation Monitoring Group	**OCC**	Office of the Comptroller of the Currency
FIEA	Financial Instruments and Exchange Act (Japan)	**IOSCO**	International Organisation of Securities Commissions	**OFAC**	Office of Foreign Assets Control (U.S.)
FINMA	Swiss Financial Market Supervisory Authority	**IP**	Intellectual Property	**OFT**	Omnichain Fungible Token
FIU	Financial Intelligence Unit	**IRS-CI**	Internal Revenue Service – Criminal Investigation	**OTC**	Over-the-Counter
FSB	Financial Stability Board	**ITL**	Innovation Testing Licence	**P2P**	Peer-to-peer

Acronym	Description
PBM	Purpose Bound Money
PBOC	People's Bank of China
PDPA	Personal Data Protection Act
PEP	Politically Exposed Person
PII	Personally Identifiable Information
PMLA	Prevention of Money Laundering Act (India)
PoS	Proof-of-Stake
PoSL	Proof-of-Staking Liquidity
PoW	Proof-of-Work
PQC	Post-Quantum Cryptography
PRA	Prudential Regulation Authority (U.K.)
PSA	Payment Services Act
PSPs	Payment Service Providers
PTSR	Payment Token Services Regulation
QFC	Qatar Financial Centre
QFCRA	Qatar Financial Centre Regulatory Authority
RAO	Regulated Activities Order
RBA	Reserve Bank of Australia
RBI	Reserve Bank of India
RWA	Real-World Asset
SAMA	Saudi Central Bank
SAR	Suspicious Activity Reporting
SCS	Single-Currency Stablecoin
SEC	Securities and Exchange Commission (U.S.)
SEPA	Single Euro Payments Area
SFA	Securities and Futures Act (Singapore)
SFC	Securities and Futures Commission (Hong Kong)
SFO	Securities and Futures Ordinance
SIM	Subscriber Identity Module
SMB	Small and Medium-sized Business
SME	Small and Medium-sized Enterprise
SRO	Self-Regulatory Organisation
SSI	Self-Sovereign Identity
StaaS	Staking-as-a-Service
STABLE Act	Stablecoin Transparency and Accountability for a Better Ledger Economy Act
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFZ	Tbilisi Free Zone
TPRM	Third-Party Risk Management
TradFi	Traditional Finance
TVL	Total Value Locked
U.A.E.	United Arab Emirates
U.K.	United Kingdom
UOB	United Overseas Bank
U.S.	United States
VA	Virtual Asset
VARA	Virtual Assets Regulatory Authority (Dubai, U.A.E.)
VASP	Virtual Asset Service Provider
VATP	Virtual Asset Trading Platform
VCs	Verifiable Credentials
VDASP	Virtual Digital Asset Service Provider
YoY	Year on Year
ZKPs	Zero-Knowledge Proofs

Foreword

Sopnendu Mohanty
Group Chief Executive Officer, GFTN

The evolution of digital assets marks one of the most profound shifts in modern finance, a shift that redefines how money, markets, and trust intersect. What began with Bitcoin's launch in 2009 as an experiment of decentralized currency has trodden two paths – one path engaged in risky, speculative activities and the other in responsible, use-cases driven experiment and real economy-based application. The latter path has now matured into a complex ecosystem of digital money, tokenized assets, exchanges, custodians, wallets, and decentralized protocols that increasingly touch the lives of consumers and enterprises alike. The question is no longer whether digital assets matter, but how they can be integrated responsibly into financial systems in a way that enhances trust, resilience, and inclusion.

This report, prepared by the Global Finance & Technology Network, addresses that question. It goes beyond short-term risky and speculative market sentiment to examine the fundamentals shaping the digital asset ecosystem around the world. We examine regulatory developments across major jurisdictions, assess the evolution of market infrastructure, and analyse the innovation and adoption trends shaping digital money and stablecoins, tokenization, exchanges, staking, and decentralized finance. The report also explores the inherent risks of digital assets, including AML/CFT concerns, privacy and security vulnerabilities, and real-world incidents of fraud, scams, and cyberattacks, and highlights how regulators and industry participants are responding to these challenges with strengthened safeguards and collaborative frameworks.

Our findings are grounded in a global evidence base. The report draws on more than 40 in-depth interviews with senior leaders across the public and private sectors, complemented by a global survey conducted by GFTN. The interviewees and survey respondents include policymakers from central banks and financial regulators, executives from leading banks, digital asset firms, payment networks, investors and Fintechs, as well as experts from international bodies. Representation spans Asia, Europe, the Middle East, and the Americas, providing a cross-jurisdictional perspective on how digital assets are evolving across diverse market contexts.

Several insights stand out. Consumer adoption of digital assets is expanding steadily, particularly in the use of stablecoins, crypto exchanges, and crypto wallets. Enterprises are exploring tokenized deposits, stablecoins, and asset tokenization as part of their business strategies. Fintechs, which once focused primarily on distribution and user experience, are now leveraging partnerships with digital asset firms to reimagine financial products from the ground up and scale the distribution of crypto products. Market infrastructure players, from exchanges to custodians, are building platforms designed for institutional scale. And critically, regulators are working hand-in-hand with innovators, using sandboxes to test new ideas and engaging with standard-setting bodies on harmonisation efforts for interoperable regulatory frameworks. They are also closely tracking consumer adoption trends to ensure frameworks support responsible growth and remain aligned with how markets and users are evolving.

This report highlights that digital assets are no longer an isolated experiment but are fast becoming a part of the next chapter of financial modernisation. We extend our appreciation to the regulators, innovators, and industry leaders who contributed their perspectives. We invite the wider policy and financial industry community to use these insights to guide a future where digital assets are engines of growth, inclusion, and trust.

Introduction

This inaugural GFTN Global Digital Assets Report provides a comprehensive cross-jurisdictional analysis of the evolving digital asset ecosystem, focusing on market developments, regulatory trends, and forward-looking policy implications. The report is designed to serve as a practical reference for policymakers, central banks, industry participants, and international standard-setting bodies navigating the rapid transformation of digital money, tokenization, and decentralized finance.

Objective

The primary objective is to map the global state of digital asset regulation and market adoption, highlight best practices, and provide actionable recommendations for aligning innovation with financial stability, consumer protection, and business resilience. The report addresses eight verticals, spanning market themes such as Digital Money & Stablecoins, Asset Tokenization, Crypto Exchanges, Staking, and DeFi. The report also highlights cross-cutting risk themes such as AML/KYC & Illicit Finance, Privacy & Security, alongside Emerging Technologies such as AI, quantum, and zero-knowledge proofs.

Jurisdictional Scope of Analysis

For this report, we have selected 12 jurisdictions worldwide as a representative set to capture the diversity of regulatory and market developments in digital assets. The selection reflects a balance of:

- **Advanced economies** that are setting global benchmarks for digital asset regulation and market standards (such as the U.S., E.U., U.K., Switzerland, and Japan).
- **Innovation hubs** in Asia and the Middle East, where regulatory frameworks are already well established and where smaller, agile economies have positioned themselves as fast movers in digital asset adoption (including Singapore, Hong Kong, Qatar, and the U.A.E.).
- **Large and fast-growing markets,** where consumer adoption is accelerating and shaping new models of innovation (such as Brazil, India, and Saudi Arabia).

By including jurisdictions of different sizes and levels of market maturity, the analysis also highlights how the complexity of digital asset regulation and adoption can vary significantly between large economies and smaller, more nimble markets. For consistency, the order of countries in the regulatory framework comparison tables across chapters is presented according to 2024 annual GDP rankings[1], arranged from highest to lowest.

Report Coverage and Cut-off Period

The report primarily captures regulatory and market developments up to July 2025, reflecting the most significant announcements and initiatives shaping the digital asset landscape during this period. The coverage includes updates on new regulatory frameworks, market trends, institutional initiatives, and technological pilots across major jurisdictions.

Where possible, we have also integrated select updates from August and September 2025 to ensure the analysis reflects the latest developments. However, coverage of these recent announcements is constrained by the time required for consolidation, verification, and review in the reporting process. The focus therefore remains on presenting a reliable snapshot of the state of digital assets in 2025, while acknowledging the fast-moving nature of this space.

Data sources for this report include official publications from regulators and central banks, press releases, industry announcements, and disclosures by financial institutions and market participants.

Methodology

This report applies a multi-layered research approach designed to capture both strategic perspectives and practical insights on the evolution of the digital asset ecosystem. By combining first-hand inputs from global decision-makers with structured analysis of market activity and regulatory frameworks, the methodology provides a comprehensive and forward-looking assessment of the industry.

Primary Research

The foundation of this report is built on extensive primary research, combining executive interviews and a global survey.

- **Executive Interviews:** Over 40 in-depth interviews were conducted with senior leaders across the digital asset ecosystem, spanning key regions and major markets worldwide. 16 of these interviews were conducted

[1] Countryeconomy, 2024

in person with delegates at the Point Zero Forum, alongside scheduled virtual meetings and bilateral discussions, providing unique access to senior decision-makers. Interviewees included:

  - Assistant Governors, Executive Directors, and Directors from central banks and regulatory authorities.
  - Managing Directors, Group Executives, and Heads of Digital Assets from global banks and payment networks.
  - Chief Executive Officers, Chief Legal and Compliance Officers, and Policy Heads from digital asset firms, Fintechs and infrastructure providers.
  - Senior representatives from international coordination bodies and law enforcement agencies.
  - Managing Partners and senior leaders from sovereign wealth funds and venture capital firms.

- **Online Survey:** A GFTN-led online survey captured responses from 48 participants representing a broad cross-section of stakeholders. Respondents included investors, national regulators and policymakers, blockchain infrastructure providers, crypto exchanges, tokenization firms, payment networks, research and advisory institutions, and other digital asset companies. With responses spanning Africa, Europe, North America, South and Southeast Asia, North Asia, and the Middle East, the survey offered a cross-jurisdictional perspective on adoption trends, regulatory approaches, and market development.

Secondary Research

The primary research was supplemented by comprehensive secondary research covering three key dimensions: market trends, regulatory developments, and case studies.

- **Regulatory Developments:** Mapping of existing regulatory frameworks applicable to stablecoins, tokenization, exchanges, staking, and DeFi. The emphasis is on how supervisory frameworks are being formulated, rather than on the legislative processes. Only limited commentary is provided on bills or ordinances under consideration, with greater focus on enacted rules, supervisory practices, and compliance standards.
- **Market Trends:** Analysis of adoption patterns and innovation trajectories across themes, including digital money and stablecoins, tokenization of real-world assets, exchanges, staking, and decentralized finance.
- **Case Studies:** As part of this report, over 65 case studies were analysed across the major themes of digital assets to illustrate how regulation, product innovation, and industry partnerships are shaping real-world outcomes. The case studies reflect a diverse range of organisations, including incumbent financial institutions, Fintechs, crypto-native firms, infrastructure providers, regulators, and non-financial enterprises, each experimenting with and scaling a variety of use cases in the digital asset industry.

Target Audience

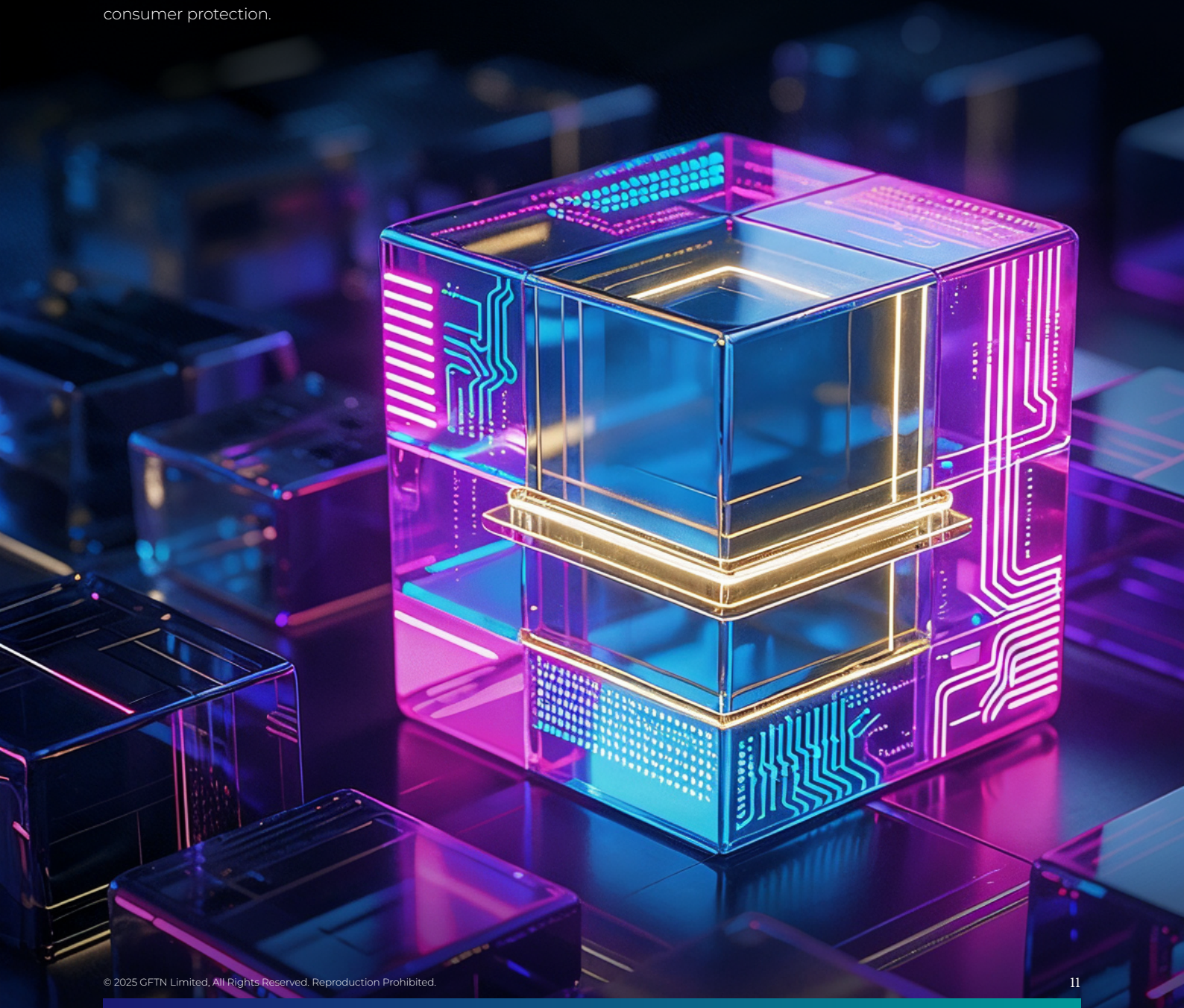
This report is designed for three primary stakeholder groups whose decisions will shape the future of digital assets:

1. **Policymakers & Regulators:** Central banks, securities regulators, and financial supervisors who are designing or refining digital asset frameworks. For this group, the report highlights market adoption trends alongside the approaches taken by regulators in key jurisdictions across major digital asset themes, including stablecoins, tokenization, exchanges, staking, and DeFi, while also addressing supervisory challenges such as AML/CFT compliance, consumer protection, and financial stability.
2. **Industry Participants:** Banks, digital asset platforms, Fintechs, custodians, and institutional investors who are embedding digital assets into their business strategies. For these stakeholders, the report provides insights into market adoption trends, the evolution of supporting infrastructure, and opportunities to innovate responsibly while aligning with emerging regulatory expectations.
3. **International Coordination Bodies:** Global standard-setters and multilateral organisations such as the BIS, FSB, IMF, and FATF, which play a critical role in harmonising cross-border rules and market standards. The report offers comparative perspectives across jurisdictions, highlighting regulatory convergence and divergence, and identifying areas where international coordination is most urgently needed.

With the combination of executive perspectives, survey insights, and data-driven analysis, this report is intended to serve as a practitioner-focused resource that bridges the market and regulatory aspects of the digital assets landscape. In addition, it also covers an analysis on the emerging technologies that are increasingly shaping and transforming the sector.

Executive Summary

This inaugural GFTN Global Digital Assets Report analyses the regulatory and market landscape for digital assets across multiple jurisdictions, highlighting diverse approaches to policy design, supervisory implementation, and private sector innovation. It captures perspectives from both regulators and industry participants to provide a balanced view of how the digital asset ecosystem is evolving. The report emphasises the urgent need for clear, consistent, and interoperable frameworks to guide the fast-growing digital asset ecosystem and ensure that responsible innovation flourishes while maintaining financial stability and consumer protection.



The regulatory landscape heatmap below highlights where clear frameworks for digital assets are already in force, where regulations are in progress, and where policy remains limited or absent.

Global Regulatory Landscape on Digital Assets

High Clear frameworks in force Medium Partial/progressing Low Limited or not specific regulation or banned completely

1. Digital Money & Stablecoins

Market Developments

As of September 2025, stablecoins have been fast scaling into a core layer of digital finance, processing more than US$263.4 trillion[2] in cumulative transaction volume since 2019, including over US$40.5 trillion[3] in the past 12 months alone.

Regulatory Frameworks

On the regulatory front, the U.S. GENIUS Act, now passed, establishes a federal regime for payment stablecoins with strict 1:1 reserve and redemption requirements, marking a watershed for market adoption. The E.U.'s MiCA offers a comprehensive, risk-based framework harmonised across member states, while Japan, Singapore and Hong Kong mandate high-quality reserve backing and redeemability as preconditions for issuance. In contrast, Saudi Arabia, Qatar, and India maintain a wait-and-see approach, with no formal frameworks yet in place.

[2] Visa, accessed on September 2, 2025
[3] Visa, accessed on September 2, 2025

2. Asset Tokenization

Market Developments

Real-world asset tokenization is scaling rapidly, with market cap (excluding stablecoins) growing from US$5 billion in 2022 to over US$24[4] billion by June 2025, representing 380% cumulative growth and 85% YoY.

Regulatory Frameworks

On regulation, multiple jurisdictions now formally recognise tokenized assets in law. The E.U. leads with MiFID/MiCA-classified digital securities and a DLT Pilot Regime; Switzerland integrates tokenized securities under its DLT Act with full legal equivalence to traditional assets. Singapore and Hong Kong regulate tokenized RWAs under existing securities frameworks, providing clear licensing pathways. Japan's FIEA regime covers tokenized instruments, while the U.S. has proposed Clarity Act (2025), which seeks to introduce a formal classification framework for digital assets and bring greater certainty to market participants. Emerging markets like Brazil have classified tokenized assets as securities under CVM guidance, and India is in a consultation phase for now.

3. Crypto Exchanges

Market Developments

Crypto exchanges remain the core gateways for digital asset adoption, serving over 750 million[5] global crypto users in 2025, a number forecast to cross 1 billion[6] by 2030. The cryptocurrency market cap stands at around US$4 trillion[7], with exchange market revenues estimated at US$63 billion in 2025, projected to almost triple to US$186 billion[8] by 2030 as institutional participation deepens and regulated trading infrastructure scales.

Regulatory Frameworks

Regulatory regimes are rapidly maturing to match this growth. The E.U.'s MiCA CASP regime, Singapore's DTSP licensing, Japan's FSA-led exchange registration, and Hong Kong's SFC trading platform licence represent some of the most comprehensive frameworks, embedding consumer protection, custody standards, and market integrity. U.A.E.'s VARA licence has positioned Dubai as a competitive global hub with clear exchange-specific supervision. Switzerland continues to integrate exchanges into its financial licensing under FINMA. In contrast, the U.S. still lacks a unified federal licence, relying on FinCEN MSB registration and state-level MTLs while new federal bills seek to clarify SEC/CFTC oversight. The U.K. is developing its exchange-specific regime through FCA consultations. Emerging markets such as Brazil have implemented VASP licensing under its 2023 crypto law, while India and Saudi Arabia remain in early stages with registration or sandbox approaches.

4. Staking

Market Developments

Staking has become a core layer of the digital asset economy, with over 42%[9] of crypto holders participating across major PoS networks and over US$800 billion[10] in combined PoS blockchain networks' market cap as of July 2025.

Regulatory Frameworks

Regulatory treatment is beginning to emerge. The E.U.'s MiCA covers staking services offered as part of licensed custody platforms, while the U.S. SEC's May 2025 guidance clarified that protocol-level solo and delegated staking does not constitute a securities offering, marking a significant step for on-chain staking clarity. Hong Kong's 2025 regulatory circular permits licensed virtual asset trading platforms to offer staking, reversing its previous prohibition. Switzerland and the U.A.E. have introduced detailed supervisory rules for custodial staking, focusing on segregation and validator transparency. Singapore allows institutional staking under risk controls and has restricted DPT service providers (like crypto exchanges) from offering staking services to their retail customers. Japan's tax reforms classify staking income, with broader regulatory consultation underway. In contrast, India, Brazil, Saudi Arabia, and Qatar have no specific frameworks, with staking rewards treated as income under general tax rules where applicable.

[4] RWA.xyz, July 2025
[5] Statista, 2025
[6] BCG, 2022
[7] Coingecko, 2025
[8] Research and Markets, 2025 Note: The same CAGR for 2025–2029, as reported by Research and Markets, has been applied to project the 2030 values.
[9] Coinlaw, 2025
[10] Coingecko, July 2025

5. Decentralized Finance

Market Developments

Decentralized Finance has expanded rapidly, reaching 312 million[11] active users across 88 countries as of Q2 2025. On-chain lending has emerged as its most systemically important use case, with US$47.4 billion[12] in active loans and nearly 346,000[13] monthly users generating close to 490 million[14] transactions annually.

Regulatory Frameworks

Regulation of DeFi is still in the early stages of development across jurisdictions. In the United States, SEC roundtables and the launch of Project Crypto in 2025 signalled a shift toward a tailored securities regime for on-chain markets. The U.K.'s FCA, through DP25/1, proposed that truly decentralized protocols remain outside the regulatory perimeter, while "DINO" (Decentralized In Name Only) projects would face proportionate oversight. In the European Union, MiCA currently excludes fully decentralized projects, but the ESMA/EBA Article 142 report published in January 2025 highlighted options for potential perimeter expansion. In Asia and the Middle East, Japan's CAISP licence was extended to cover DeFi interfaces, while Hong Kong's ASPIRe roadmap brought DeFi under SFO licensing. Singapore, through Project Guardian, continues to limit DeFi activity only to institutional pilots, whereas the U.A.E's VARA has set out strict licensing and disclosure rules for DeFi lending. Globally, progress has been slow. FATF's 2025 update found that only 9% of jurisdictions had active DeFi licensing, reflecting uneven implementation of international standards.

DeFi's systemic relevance is growing. DeFi Lending protocols are increasingly interconnected with tokenized RWAs and stablecoins, which are now increasingly used as collateral. This creates new channels of FX risk for emerging markets through exposure to USD stablecoins. At the same time, partnerships such as Coinbase–Morpho are expanding DeFi's reach, enabling retail access at scale.

6. AML/KYC, Privacy, and Security Risks in Digital Assets

Market Developments

AML/KYC non-compliance penalties reached US$5.1 billion in 2024, marking a 39% YoY increase, with fines surpassing US$1.3 billion in the first quarter of 2025 alone.[15] In addition to this, privacy risks have also intensified. 69,000[16] Coinbase user records were leaked due to insider malfeasance, while over 18 million[17] U.S. exchange user records surfaced on the dark web in a major data breach in 2025.

Security breaches continue to remain a defining risk for digital assets. Between January and November 2024, 43.8% of stolen funds stemmed from private key compromises, highlighting persistent weaknesses in hot wallet infrastructures and insufficient multi-signature or hardware protections. Additional attack vectors included phishing and insider leaks (11.2%), smart contract vulnerabilities (8.5%), market manipulation via oracles and flash loans (4.7%), and technical misconfigurations such as weak access controls (6.3%).[18] In the first half of 2025, US$2.1 billion was stolen across approximately 75 exploits and hacks, nearly matching the entire-year loss totals for 2024.[19]

Regulatory Frameworks

While FATF has provided the blueprint of AML/CFT obligations and Travel Rule compliance requirements for digital assets, domestic regulators vary in how far they translate guidance into regulatory frameworks. Jurisdictions such as the E.U., Singapore, Japan, Hong Kong, Switzerland, U.A.E., and Brazil have rolled out full-spectrum, crypto-specific AML regimes requiring VASPs to be licensed, apply CDD/EDD protocols, monitor transactions, and file suspicious transaction reports. The E.U. (via MiCA) and Singapore (via PSN02) stand out for their detailed compliance expectations. By contrast, countries such as the U.S., U.K., India, Saudi Arabia, and Qatar still rely on traditional financial crime statutes like the U.S. Bank Secrecy Act or India's PMLA, without a dedicated crypto-specific framework.

[11] Coinlaw, 2025
[12] Token Terminal, September 2025
[13] Token Terminal, September 2025
[14] Token Terminal, September 2025
[15] Coinlaw, 2025
[16] CCN, 2025
[17] Mitrade, 2025
[18] Chainalysis, 2025
[19] TRM Labs, 2025

7. Emerging Tech in Digital Assets

Market Developments

The next phase of digital assets is being shaped by technologies that combine privacy, security, and interoperability. Zero-Knowledge Proofs and Fully Homomorphic Encryption are enabling compliance checks without exposing sensitive customer data, piloted in initiatives such as Project Aurum 2.0 by HKMA and BIS, which applied ZKPs to retail CBDC issuance. Verifiable Credentials and Self-Sovereign Identity are advancing in the E.U. (via the EUDI Wallet) and in Latin America (through the IDB's LACChain project), reducing onboarding costs and improving financial inclusion. On the custody side, Multi-Party Computation is becoming the industry standard, used by custodians to eliminate single points of failure, while Quantum-Resistant Cryptography is being tested in projects like QANplatform, anticipating future systemic risks from quantum computing. In supervision and intelligence, AI is being piloted by central banks (e.g. BIS Project AISE) and by industry players such as Kraken in M&A due diligence, while Blockchain Analytics tools (e.g. Chainalysis, TRM Labs) are now mainstream in law enforcement, supporting AML monitoring and fraud investigations. Cross-chain messaging protocols (e.g. Circle's CCTP, LayerZero) and Oracles (e.g. Chainlink integrations on Solana) are underpinning interoperability, enabling secure value transfer, compliance data portability, and resilience against market manipulation.

Regulatory Frameworks

For regulators, these technologies are not just enablers of innovation but tools to monitor and manage systemic risks and improve compliance. ZKPs and FHE can enable privacy-preserving supervision, where regulators verify AML/KYC compliance without bulk data collection, addressing both privacy concerns and compliance risks. VCs and SSI present pathways for portable, regulator-recognised digital identity, cutting onboarding costs and reducing fraud in cross-border contexts. AI and blockchain analytics are redefining supervisory models, allowing near real-time detection of suspicious activity and proactive market surveillance, but they also raise new risks around explainability, model bias, and governance. Cross-chain protocols and oracles are increasingly viewed as critical infrastructure for on-chain finance. For regulators, they represent a dual challenge—on the one hand, potential channels for systemic contagion, and on the other, indispensable building blocks for scaling tokenized assets, programmable money, and DeFi.

1 Digital Money & Stablecoins

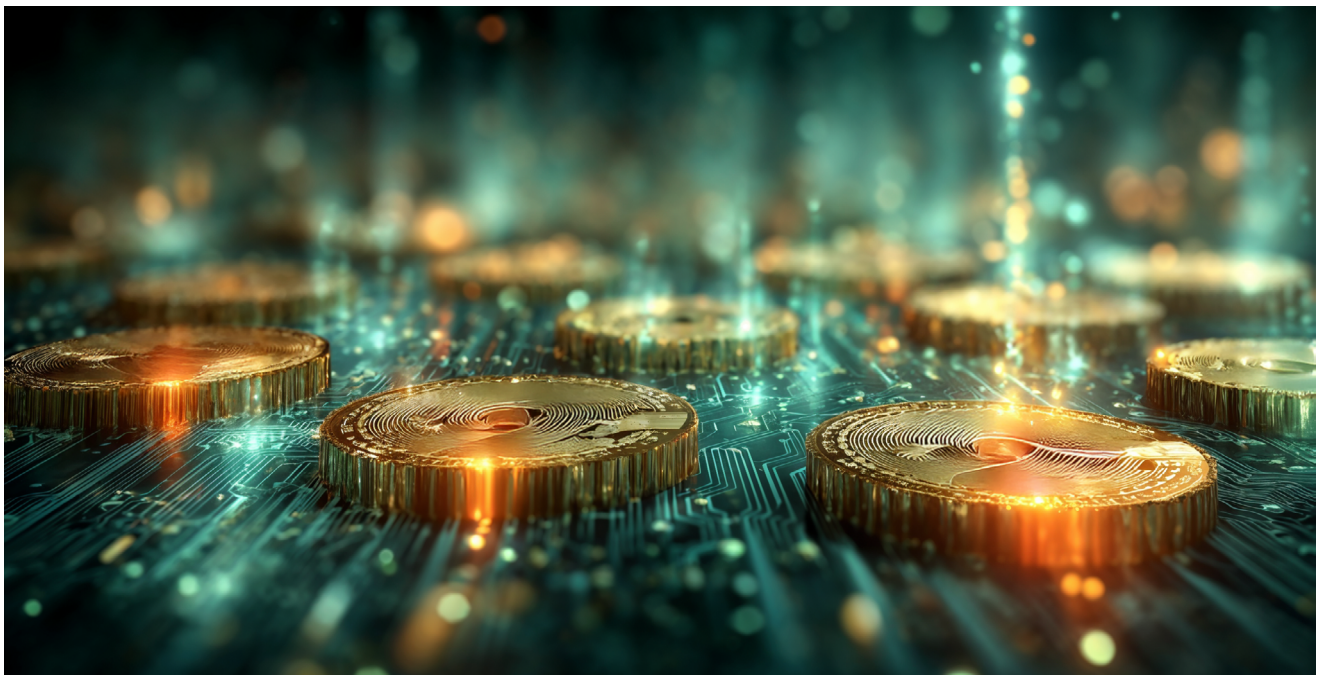
1.1 Introduction

The role of money in the financial system is entering a period of accelerated evolution. What was once confined to physical cash and account-based banking is now expanding to digital-native forms of money, designed for programmability, interoperability, and real-time settlement. This includes the emergence of stablecoins, CBDCs, and tokenized deposits, each representing a distinct approach to reimagining how value is issued, transferred, and stored in the digital age. Among these, stablecoins have seen the most widespread adoption to date. Pegged to fiat currencies and issued primarily by private institutions, stablecoins aim to combine the stability of traditional money with the efficiency and programmability of blockchain networks. Once niche instruments used largely within crypto trading ecosystems, stablecoins have grown into a US$280 billion[20] market by August 2025, used increasingly in remittances, DeFi, commerce, and treasury operations.

Following the announcement of Facebook's Libra project in 2019, several jurisdictions launched pilot programs to explore CBDCs, reflecting an initial focus on central bank-issued digital money. However, over the past two to three years, the rapid growth in stablecoin adoption has shifted regulatory attention back toward privately issued digital money, highlighting its expanding role in payments, remittances, and on-chain finance. This chapter examines the use cases, adoption levels, value-chain participants, and policy landscape surrounding these new forms of digital money.

1.1.1 Types of Digital Money

Today, three primary models of digital money have emerged: **stablecoins, tokenized deposits**, and **CBDCs**, each with distinct issuers, designs and regulatory clarity. Stablecoins, privately issued and blockchain-native, offer speed but carry medium-to-high risk due to factors such as reserve opacity, uncertain redemption rights, and vulnerabilities in governance structures. Tokenized deposits, issued by regulated commercial banks, leverage existing banking frameworks, and hence offer enhanced stability and relatively lower counterparty risk. Finally, CBDCs, direct central bank liabilities, present the lowest risk due to sovereign backing, but raise privacy concerns and adoption challenges. While most CBDCs globally remain in early stages, limited to pilots, proof-of-concept trials, or controlled rollouts, a few have achieved large-scale adoption within their respective jurisdictions. According to the Atlantic Council CBDC Tracker[21], out of 137 countries and currency unions tracked, only 3 have launched, while 49 are in pilot stage, 20 in development, and 36 in research. The Digital Euro and e-CNY (China's digital yuan) continue to undergo large-scale testing while countries like the U.K., Canada, and Singapore have narrowed their focus to wholesale CBDC applications for interbank settlement and cross-border use. A few implementations have gone live for retail CBDCs, such as the Bahamas' Sand Dollar, Nigeria's eNaira, and Jamaica's JAM-DEX, but adoption remains limited, thus far.



[20] Defillama, August 2025
[21] Atlantic Council, September 2025

Table 1.1:

Types of Digital Money: Stablecoins, Tokenized Deposits, and CBDCs

Key Parameters	Stablecoins	Tokenized Deposits	CBDCs
Issuer	Private sector (Non-banks, Banks)	Private sector (Commercial banks)	Public sector (Central banks)
Backing & Stability	Fiat currency, short-term securities, or commodities	Bank deposits, which are the basis of tokenized deposits, are directly insured by regulators	Direct central bank liabilities, fully sovereign-backed
Use Cases	Cross-border payments, trading, merchant payments	Institutional settlements, treasury management, commercial payments	Domestic retail payments, wholesale payments, monetary policy tools
Regulatory Clarity	Varies (Developing regulatory frameworks)	High (Established banking regulatory environment)	High (Clearly defined by central banks and regulators)
Risk Profile	Medium-High (Issuer credibility, Proof of Reserve, cybersecurity)	Medium-Low (Bank solvency, operational risks)	Low (Sovereign-backed, but privacy and disintermediation risks remain)
Programmability & Innovation	High (Smart contracts, programmable payments)	High (Blockchain-based banking operations)	Medium (Programmable money in controlled environments)
Market Adoption & Maturity	High (Adoption in crypto and Fintech, rapidly expanding)	Emerging (Adoption mainly in institutional and commercial banking)	Various phases of implementation stages
Examples	Circle (USDC), Ripple (RLUSD), Paxos (USDP)	Kinexys by J.P.Morgan, Citi Tokenized Deposits	Digital Euro, Singapore's Project Orchid

Industry Perspectives on the Evolving Landscape of Digital Money

"Stablecoins are no longer just crypto infrastructure — they're solving real payment problems. Cross-border trade, retail merchant payments, and treasury operations are now leveraging our euro stablecoin. In Europe, SEPA Instant isn't yet universal across all countries, and stablecoins can fill that gap. With MiCA, we've shown banks that compliant issuance is not only possible but practical. And as markets evolve, tokenized deposits will emerge alongside stablecoins, offering yield and programmability within a regulated framework."

Bjørn Krog Andersen - Chief Compliance Officer, Banking Circle

"The ideal structure is a unified ledger built on a two-tier model. Central bank money interacting directly with private deposits. Deposits remain essential for credit creation, while sovereign money underpins monetary policy and government financing. Stablecoins may serve as an intermediate step, but they are essentially stabilised by deposits. For commercial banks, diverting deposits to issue stablecoins raises fundamental questions. The path should lead to unified ledgers, though it can be a heavy lift and may take years."

Masashi Watanabe - Managing Director, Head of Digital Asset, MUFG

1.1.2 Digital Money Progress Across the Core Characteristics

The rise and progress of digital money is rooted in longstanding frictions in the traditional financial system, i.e. slow cross-border payments, high transaction costs, limited access to dollar-based assets in emerging markets, and the lack of programmable financial infrastructure. These limitations have led to the development of new forms of money that are faster, more accessible, and tailored to the digital economy.

Across the core functions of money, medium of exchange, store of value, and unit of account, digital currencies demonstrate varied levels of maturity:

- Stablecoins have rapidly matured as a medium of exchange, particularly in cross-border transactions and DeFi. In several emerging markets, they are also used as a store of value, offering a dollar-denominated alternative in high-inflation environments.
- Tokenized deposits, issued by regulated commercial banks, are gaining traction as a medium of exchange for institutional payments, securities settlement, and treasury flows, benefiting from integration with the traditional banking system.
- CBDCs remain in various phases of implementation, ranging from pilots and limited rollouts to full-scale launches in select jurisdictions. Due to their status as sovereign liabilities, they are uniquely positioned among digital money models to comprehensively fulfil all three core functions of money, serving as a medium of exchange, store of value, and potentially, a new unit of account within national economies.

Industry Perspectives on Stablecoins as a Catalyst for Financial Innovation

"The form of digital money that gains traction depends on regulatory clarity. Stablecoins benefit from clearer rules such as MiCA in Europe, GENIUS Act in the US and the Stablecoin Regulatory Framework in Singapore. Tokenized deposits are promising, but mostly confined to intra-bank networks for now. CBDCs are the safest form of settlement assets but are mostly still in pilot mode. While stablecoins are more likely to scale in cross-border payments for now, tokenized deposits and CBDCs are likely to follow suit in the future, each finding their own product-market fit and co-existing with stablecoins and other TradiFi rails."

Yip Kah Kit - Executive Director, Head of Blockchain and Digital Assets, UOB

"The approval of Bitcoin ETFs in the U.S. was a turning point. It persuaded regulators to accept crypto's place in mainstream finance. Now we are seeing stablecoin acts and self-custody recognition emerge, protecting customers while enabling innovation. Stablecoins, in particular, are already tokenized U.S. national debt, making them one of the most impactful applications of blockchain."

Star Xu - Founder & CEO, OKX

"Stablecoin demand is growing from two vectors: organic ecosystem growth and institutional product maturity. More people discover and use stablecoins across crypto platforms and in markets where holding dollars is difficult. Meanwhile, large enterprises like Stripe, PayPal, and Mastercard come to us to power stablecoin infrastructure as part of broader financial product strategies. They want solutions that meet regulatory standards and integrate with their distribution models. The regulatory clarity now emerging globally is enabling these firms to proceed with real use cases, from settlement to B2B flows."

Walter Hessert - Head of Strategy, Paxos

"Stablecoins perform several distinct functions across digital asset markets — facilitating payments, enabling trading, and providing liquidity. This complexity makes it essential for regulation to be flexible enough to accommodate multiple use cases."

Roeland Van Der Stappen - Head of E.U. Policy, Coinbase

Table 1.2:

Digital Money Progresses Across the Core Characteristics of Money

Money characteristics	Stablecoins	Tokenized Deposits	CBDCs
Medium of Exchange	**Advanced** Widely adopted for cross-border and online payments. **Example:** Shopify merchants in 34 countries[22] can accept USDC through Shopify Payments (powered by Stripe and Coinbase) via the Base blockchain. Merchants can receive funds in either local currency or USDC and benefit from 0.5% cashback incentives and near-zero fees.	**Moderate** Mostly used within specific banking ecosystems. **Example:** J.P. Morgan's Kinexys platform recently enabled a cross-chain DvP settlement using tokenized deposits on its permissioned blockchain network, in collaboration with Ondo Finance and Chainlink. Kinexys processes over US$2 billion[23] in daily volume and has handled more than US$1.5 trillion in cumulative transactions since inception.	**Emerging** Limited pilots and retail acceptance in early stages. **Example:** The PBOC has piloted the digital yuan extensively for domestic retail payments. As of July 2024, over 180 million[24] individual wallets had been opened, facilitating more than 7.3 trillion yuan (approximately US$1 trillion) in cumulative transaction volume across pilot regions.
Store of Value	**Moderate** Stable value backed by assets like fiat currency or treasury bonds. **Example:** Through a partnership between Circle and Nubank, over 100 million[25] customer accounts in Brazil have access to USDC via the bank's app. This collaboration enables users to buy, hold, and transfer USDC alongside their existing banking services.	**Emerging** Subject to banking system risks; backed directly by regulated bank deposits. **Example:** Citi's Token Services for Cash has transitioned from pilot to commercial launch, facilitating multimillion-dollar transactions for institutional clients such as Mars. The service enables 24/7 cross-border liquidity and settlement between Citi branches via a permissioned blockchain network managed by the bank.	**Advanced** Stability tied directly to central bank policy, not market-tested widely yet. **Example:** eNaira was launched in Nigeria in October 2021. Within a year, just 0.5% of the population used the eNaira, and the IMF reported that 98.5%[26] wallets were inactive during that period.
Unit of Account	**Emerging** Limited mainstream adoption as a primary unit for pricing, though gaining ground in crypto markets. **Example:** In inflation-prone countries, contract workers denominate their salaries in USDC via platforms like Bitwage, effectively using stablecoins as a unit of account. Bitwage has processed over US$400M[27] in payrolls till August 2025, serving more than 90,000 registered workers and 4,500 companies across 200 countries.	**Emerging** Currently restricted to bank-specific or institutional usage, with limited broader pricing usage. **Example:** Citi's Token Services for Trade is being piloted by global shipping firms CB Fenton and GAC Panama Shipping to digitise trade settlement processes. In this setup, the tokenized deposit serves as the unit of account, with trade contracts and obligations denominated directly in the tokenized form of money.	**Moderate** Planned usage by central banks to mirror fiat currency precisely. **Example:** Jamaica's JAM-DEX, launched in July 2022, acts as a digital alternative to cash and a store of value for users. Over 260,000[28] consumer wallets had been opened by early 2024, about 9% of Jamaica's 2.8 million population.

[22] Stripe Shopify Partnership, 2025
[23] Kinexys by J.P. Morgan, 2024
[24] Digital Pound Foundation, 2024
[25] Nubank, 2024
[26] The Cable, 2023
[27] Bitwage Payroll, 2025
[28] SSRN Library, 2025

Expert Insights on Stablecoin Use-cases

"Stablecoins are the easiest way for institutions to get on-chain. They offer stability, traceability, and real-time settlement. For corporates, this unlocks better treasury operations — you can sweep capital across entities, avoid liquidity fragmentation, and manage working capital more effectively. That's why we built our own stablecoin — to bridge fiat and crypto in a secure, compliant way."

Fiona Murray - Managing Director APAC, Ripple

"Stablecoins are being used by multinational companies for treasury management and by HR platforms for global payroll. These are not speculative experiments; they are real businesses solving real-world problems. One of the most compelling use cases is enabling global contractors to be paid in stablecoins where payment preferences are shifting. This demand comes directly from businesses seeking to access global talent without the friction of legacy payment rails."

Tang Wei - Head of Public Policy for Southeast Asia and Greater China, Stripe

"Stablecoins will not take over all of payments, but they can unlock specific corridors where traditional rails are inefficient, particularly for cross-border commerce and USD exposure in emerging markets. Their programmability also makes them adaptable to future needs such as AI-driven commerce."

Ezechiel Copic - Director, Digital Currency Policy, Visa

"The programmability of tokenized money opens fascinating new use cases that our current financial infrastructure cannot easily support. Tokenization allows us to reimagine access, liquidity, and product design in ways that could be transformational."

Jesse McWaters - Executive Vice President, Head of Global Government Affairs, Mastercard

The following case studies illustrate the growing acceptance of stablecoins as a medium of exchange and as a store of value, where adoption is most evident within the digital asset ecosystem. In contrast, there is limited evidence of stablecoins serving as a unit of account, as they are not recognised as legal tender and prices continue to be denominated in fiat currencies, even where stablecoins are accepted by merchants or service providers.

Table 1.3:

Case Studies: Stablecoins as a Functional Medium of Exchange

A. Visa & Bridge: Stablecoin-Linked Visa Cards	
Entities Involved:	Visa, Bridge (a Stripe company), Lead Bank
Use Case Title:	Enabling everyday purchases with stablecoins
Target Customers:	Consumers and remittance users in Latin America
Use Case Description:	• In April 2025, Visa partnered with Bridge to launch stablecoin-linked Visa cards across six Latin American countries - Argentina, Colombia, Ecuador, Mexico, Peru, and Chile. • These cards allow users to make purchases everywhere Visa is accepted (around 150 million merchant locations globally) by converting USDC from their balance into local currency at the point of sale. • Bridge handles real-time conversion and settlement via its API and Lead Bank integration.
Value Proposition:	• Consumers can hold and spend stablecoins like USDC, shielding them from domestic inflation. • Bridge's API allows Fintechs to spin up stablecoin card programs programmatically across multiple regions with one integration.

Future Outlook:	Plans to expand the program to Europe, Africa, and Asia, broadening the reach of stablecoin usage in daily transactions.

Source: Visa, 2025

B. Mastercard & MoonPay: Mainstreaming Stablecoin Payments

Entities Involved:	Mastercard, MoonPay
Use Case Title:	Manage payouts and disbursements more efficiently, improving cross-border money transfer
Target Customers:	Business-to-business (B2B clients such as enterprises, neobanks, Fintechs)
Use Case Description:	• Mastercard and MoonPay have collaborated to enable stablecoin-powered payments for businesses. It enables businesses, neobanks, and payment participants to easily manage payouts and disbursements more efficiently, improving cross-border money transfers. • It also allows businesses to offer stablecoin-based payouts to gig workers, contractors and creators. • MoonPay's extensive network, with integrations across over 500 leading crypto platforms, including major wallets and exchanges, provides a combined reach of over 100 million active crypto users.
Value Proposition:	• Offers real-time, low-cost cross-border payout infrastructure. • Enables new crypto-native financial products for gig economy firms. • Reduces reliance on traditional correspondent banking networks, enhancing liquidity and speed for global settlements.
Future Outlook:	Mastercard aims to extend stablecoin settlement to more corridors, potentially replacing legacy rails for disbursement-heavy sectors like creator economy platforms and payroll services. Aims to reach 150 million merchants globally, integrating stablecoin payments into mainstream commerce.

Source: Mastercard, 2025

Table 1.4:

Stablecoins Becoming a Reliable Store of Value

A. Stripe: Stablecoin Financial Accounts in 101 Countries

Entities Involved:	Stripe, Bridge
Use Case Title:	Providing businesses with stablecoin-based financial accounts
Target Customers:	Business-to-business (Businesses in emerging markets)
Use Case Description:	• Stripe has launched stablecoin financial accounts across 101 countries, enabling businesses to hold and transact in stablecoins like USDC as well as in fiat currencies like USD and EUR. This offering provides a modern alternative to traditional banking, allowing for efficient international transactions and fund management. • Since January 2025, stablecoin transactions on Stripe have grown at a compound rate of 30% month-over-month, signalling robust and accelerating demand. • Customers using stablecoins are 2x more likely to be net-new than those using traditional payment methods, expanding the addressable market for global merchants. • A Stripe survey found that businesses processing over US$1M in monthly cross-border volume are 92% more likely to use stablecoins, indicating adoption is no longer limited to crypto-native firms or niche use cases.

Value Proposition:	• Offers businesses in regions with unstable financial infrastructure a reliable method to manage funds, access USD-pegged assets, and engage in global trade, without the friction of legacy banking rails. • Reduces FX exposure and enhances liquidity access for SMBs and tech-native companies.
Future Outlook:	As stablecoin financial infrastructure matures, features like multi-currency account access and real-time cross-border payments will no longer be premium offerings; they will become baseline expectations for SMBs operating in global markets.

Sources: Stripe, 2025; Stripe Survey

B. Circle & Nubank: USDC Savings with Rewards

Entities Involved:	Circle, Nubank
Use Case Title:	Integrating digital dollars into everyday banking
Target Customers:	Brazilian consumers
Use Case Description:	• In December 2023, Circle and Nubank partnered to extend access to USDC, a digital dollar stablecoin, to Nubank's customers in Brazil. This integration allows users to hold and transact in USDC within the Nubank app, offering a stable store of value amidst local currency volatility. • After initially piloting its USDC rewards program with a small group of users, Nubank expanded the offering to all Nubank Cripto users in Brazil as of January 14, 2025. • The program offers a fixed 4% annual interest rate, paid daily, for any wallet balance of at least 10 USDC. Users can toggle participation at will and maintain instant liquidity in their wallets. • In 2024, the amount of USDC held by Nubank customers increased tenfold. More than 50% of new **Nubank Cripto** users chose USDC as their first digital asset.
Value Proposition:	• Offers users in high-inflation environments a safer alternative to traditional savings, with consistent returns. • Daily interest and easy eligibility enhance user stickiness. • Over half of new crypto users start with USDC, demonstrating its role as an entry point into the digital assets ecosystem.
Future Outlook:	With a strong user base (over 100 million in Brazil) and initial success, Nubank is poised to further integrate USDC into features like crypto swaps, enabling seamless conversion between digital assets and local currencies. This positions the stablecoin-backed savings product as a new norm in retail banking in Latin America.

Sources: Circle, 2023; Nubank, 2025

C. Banking Circle: Euro Stablecoins Becoming a Core Settlement Asset

Entities Involved:	Banking Circle, Fireblocks, Binance
Use Case Title:	Enabling 24/7 euro settlements via bank-issued stablecoin
Target Customers:	PSPs, Fintechs, Remittance Platforms
Use Case Description:	• In August 2024, Banking Circle launched EURI, the first euro-pegged stablecoin issued by a regulated bank under MiCA. • EURI is deployed on Ethereum and BNB Smart Chain through integration with Fireblocks, supporting minting, burning, and transfers around the clock. • Designed to offer instant settlement capabilities for PSPs and Fintech firms, eliminating reliance on traditional banking rails like SWIFT and SEPA. • The solution was built to address demand for compliant, euro-denominated digital settlement options in Europe's financial infrastructure.

Value Proposition:	• Reduces FX friction and settlement lags in cross-border euro payments. • Offers MiCA-compliant digital money infrastructure backed by a regulated banking entity. • Supports liquidity management and 24/7 operations for PSPs and Fintechs. • Acts as an alternative to commercial bank money for B2B settlements.
Future Outlook:	Serves as a reference model for other banks seeking to issue stablecoins under the MiCA regime.

Source: Banking Circle, 2024

1.1.3 Digital Money Risk Assessment Profile

Despite rising adoption, risks differ markedly by type of digital money. Stablecoins entail substantial cybersecurity and counterparty risks, stemming from private issuance and less established regulatory oversight. Tokenized deposits carry moderate operational risks tied to legacy bank integration. CBDCs present minimal credit risk yet face significant privacy and potential disintermediation concerns, given their central bank issuance and wide-ranging impacts on monetary policy.

Table 1.5:

Risk Metrics for Stablecoins, Tokenized Deposits, and CBDCs

Assessment Parameter	Stablecoins	Tokenized Deposits	CBDCs
Regulatory & Legal Uncertainty	**Medium** Example: Global regulatory challenges faced by Tether and other stablecoins.	**Medium** Example: Regulatory clarity needed for bank-issued deposit tokens.	**Low** Example: Clear regulatory oversight established by ECB's Digital Euro project.
Credit & Counterparty Risk	**Medium** Example: Transparency concerns regarding stablecoin reserves (e.g. TerraUSD).	**Medium** Example: Tokenized deposits vulnerable to issuer-bank insolvency risks.	**Low** Example: Central bank-backed assets minimise credit risk in CBDCs.
Cybersecurity & Fraud Vulnerability	**Medium** Example: Security vulnerabilities such as compromised smart contracts or custodial breaches.	**Medium** Example: Security threats due to integration with legacy banking systems.	**Medium** Example: Cybersecurity concerns influencing the design of central bank digital currencies.
Operational Complexity & Integration Risks	**High** Example: Network congestion causing delays in stablecoin transactions (Ethereum).	**Medium** Example: Complex integration processes with traditional banking infrastructure (Citi Token Services for Cash and Citi Token Services for Trade).	**Medium** Example: Challenges anticipated in integrating CBDCs with existing payment systems.
Privacy & Surveillance Concerns	**Medium** Example: Public transparency on blockchain ledgers for stablecoins.	**Medium** Example: Privacy balanced with regulatory transparency requirements.	**High** Example: Significant public concerns regarding potential surveillance by central banks (e.g. digital Yuan).

Source: GFTN Analysis

Having established the foundations and distinct features of digital money, it becomes clear that stablecoins warrant a deeper exploration. Unlike CBDCs, which are directly issued by central banks, and tokenized deposits managed within the highly regulated framework of commercial banks, stablecoins are predominantly created and managed by private-sector non-bank entities. This structural difference significantly amplifies their risk exposure, particularly because stablecoin regulation remains fragmented and often lacks clarity across jurisdictions.

1.2 Stablecoins: Rapid Adoption Amid Increasing Regulatory Clarity

The GFTN survey highlights how regulators and industry participants perceive the opportunities and challenges around stablecoins. The findings underline the dual narrative shaping stablecoins today: while they promise faster cross-border payments, programmability, and broader access, they also raise critical questions for monetary policy, financial stability, and supervisory frameworks.

GFTN Survey Insights: Digital Money & Stablecoins

Survey Insight 1.1

Regulatory Attention on Stablecoins

31%

Stablecoin Issuers were identified by 31% of respondents as requiring the most regulatory attention in their jurisdiction, making it the second-highest concern after centralized crypto exchanges.

Survey Insight 1.2

Perceived Benefits of Stablecoins

47%

"Faster, cheaper cross-border payments" (47%) and "programmable and automated financial services" (36%) were the top two benefits cited by the respondents. Both of these are core value propositions of stablecoins and tokenized money.

Survey Insight 1.3

Monetary Policy Risks from Stablecoins

40%

The impact of stablecoins on FX and monetary policy was chosen by 40% of respondents, making it the top-ranked emerging area needing immediate regulatory clarity.

Survey Insight 1.4

Stablecoins & Tokenized Deposits Drive Programmable Finance

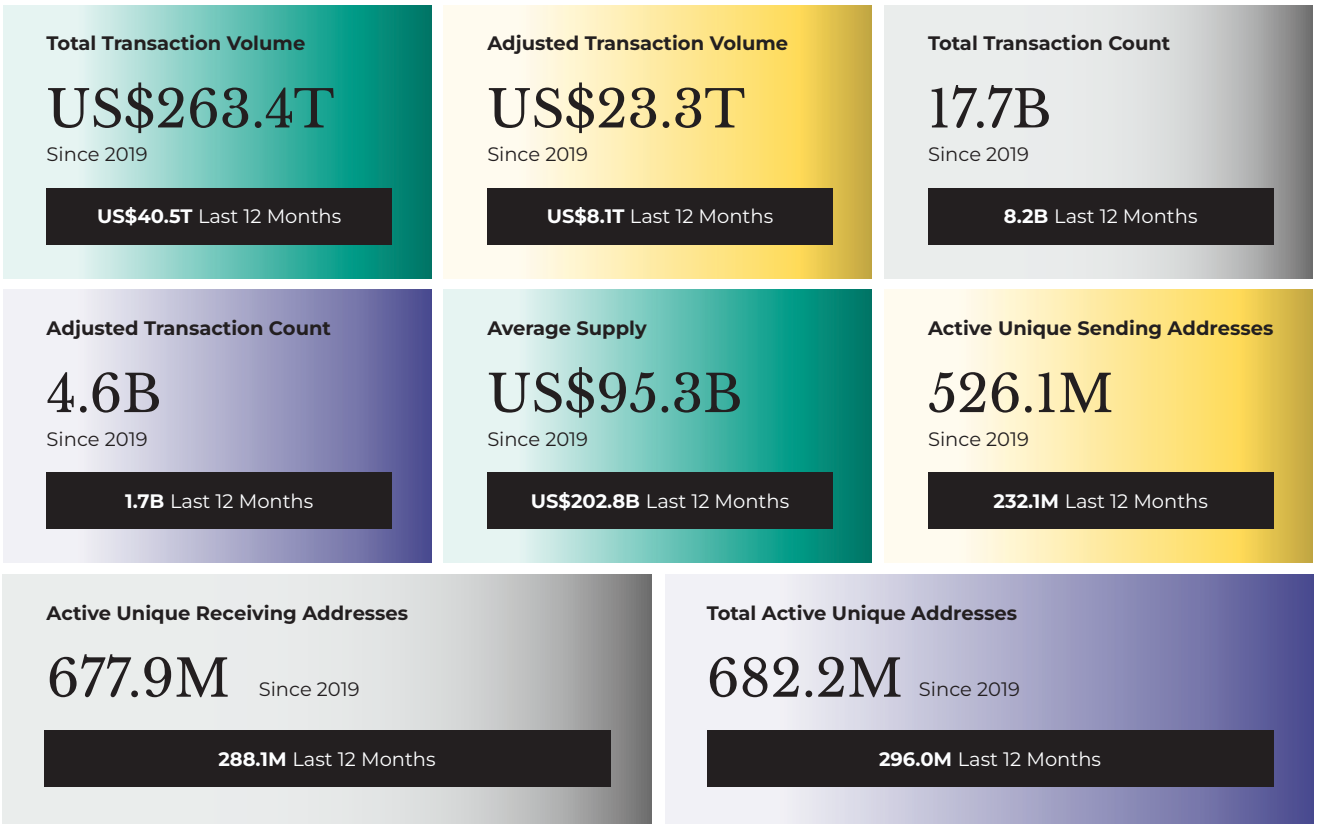
46%

Programmable money and smart contracts were cited by 46% of respondents as the biggest opportunity for digital assets over the next 3 years, underscoring the potential of stablecoins and tokenized deposits as programmable financial primitives.

1.2.1 Rapid Adoption of Stablecoin

Figure 1.1:

Stablecoin Metrics At A Glance



Source: Visa Onchain dashboard (powered by Allium), accessed on September 2, 2025

Stablecoins have swiftly evolved from a crypto-native innovation into a cornerstone of the digital finance industry. As documented in the 2025 BCG Stablecoin report, their adoption is not only accelerating in scale but also diversifying across use cases.[29] In 2024, 88% of total stablecoin transaction value, amounting to US$23 trillion, was attributed to crypto trading pairings, highlighting their continued role in exchange arbitrage and liquidity routing. However, a growing share of flows is now associated with more diverse use cases: US$1 trillion (4%) supported on/off-ramping, bridging exchanges and wallets; US$0.8 trillion (3%) was linked to tokenized RWA settlements, driven by pilot programs in tokenized treasuries; and US$1.3 trillion (5%) was distributed across P2P payments (remittances), B2C/C2B payments (retail spending on commerce platforms), and B2B payments (Institutional payments involving treasury, FX, and invoice settlement).

Visa Onchain metrics as of September 2025 further reinforce the accelerating adoption of stablecoins. Since 2019, stablecoins have facilitated over US$263.4 trillion in total transaction volume, with US$40.5 trillion recorded in the last 12 months alone, signalling their robust integration into both institutional and retail financial flows. When adjusted to exclude intra-exchange transfers, bots, and high-frequency trading, the adjusted cumulative volume stands at US$23.3 trillion, with US$8.1 trillion attributed to the past year—highlighting meaningful, organic usage. The number of transactions also underscores scale: 17.7 billion total transactions since 2019, of which 8.2 billion occurred in the past year. Adjusted for non-economic activity, 4.6 billion transactions (and 1.7 billion over the last 12 months) represent genuine economic engagement.

The active user base has expanded significantly. Since 2019, there have been 526.1 million unique sending addresses and 677.9 million receiving addresses. Over just the past 12 months, 232.1 million users sent, and 288.1 million users received stablecoins, reflecting growing traction across wallets, apps, and platforms. Driven by growing demand, the average stablecoin supply over the past 12 months has reached US$202.8 billion, reflecting a sharp increase in issuance and adoption in 2025. This is more than double the long-term average supply of US$95.3 billion since 2019, which includes the early years of limited market activity.

[29] BCG, 2025

Table 1.6:

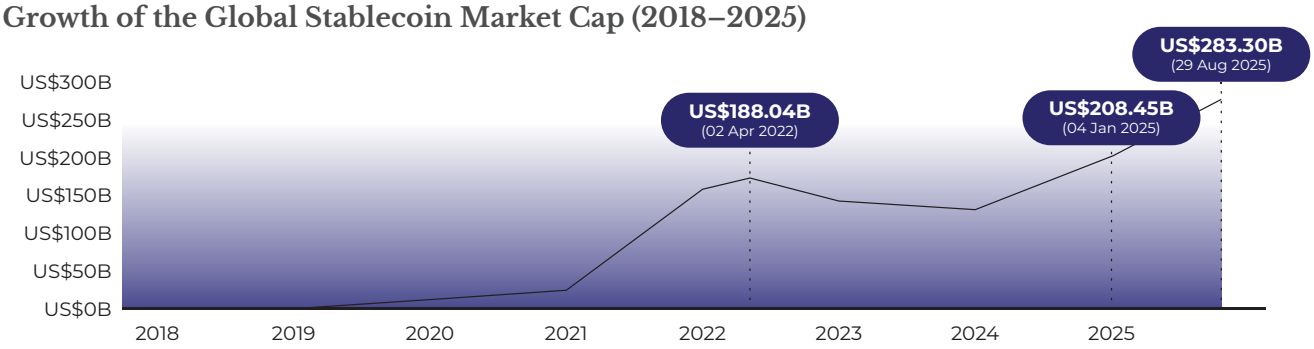
Top 10 Stablecoins by Market Capitalisation (September 2, 2025)

Rank	Issuer	Stablecoin Symbol	Market Cap
1	Tether	USDT	US$168.03B
2	Circle	USDC	US$71.77B
3	Ethena	USDe	US$12.44B
4	MakerDAO	DAI	US$5.36B
5	World Liberty Financial	USD1	US$2.67B
6	First Digital	FDUSD	US$1.45B
7	PayPal	PYUSD	US$1.19B
8	Ripple	RLUSD	US$701M
9	True	TUSD	US$492M
10	TRON DAO	USDD	US$446M

Source: Coinmarketcap, accessed on September 2, 2025

Figure 1.2:

Growth of the Global Stablecoin Market Cap (2018–2025)



Source: Defillama, accessed on September 2, 2025

This adoption wave is being matched by the market cap of stablecoin issuers. Between January 2025 and August 2025, the total stablecoin market capitalisation grew from US$208.4 billion to US$283.3 billion, representing an increase of nearly 36% in just eight months (see Figure 1.2). This expansion reflects growing confidence in the utility and safety of stablecoins, especially those with high transparency and regulatory alignment. Market leaders like USDT (Tether) and USDC (Circle) continue to dominate due to their large liquidity bases, trusted reserves, and alignment with emerging regulatory frameworks. The emergence of players like Ethena's USDe (backed mainly by crypto assets and stabilised through a delta hedging strategy[30]) and World Liberty's USD1 (U.S.-regulated, fully reserved model) reflects experimentation with different approaches to achieving price stability and market trust. Their entry demonstrates that the stablecoin market is not confined to a single design template (e.g. fiat-backed), but is evolving with competing models of collateralization, governance, and regulatory engagement. This diversity signals openness to innovation while fostering competitive differentiation as issuers seek to balance efficiency, compliance, and resilience. These dynamics illustrate a maturing ecosystem: increasingly consolidated around trusted issuers, yet still flexible enough to welcome alternative architectures. As regulatory clarity deepens across key jurisdictions, the momentum behind stablecoin usage is expected to accelerate further.

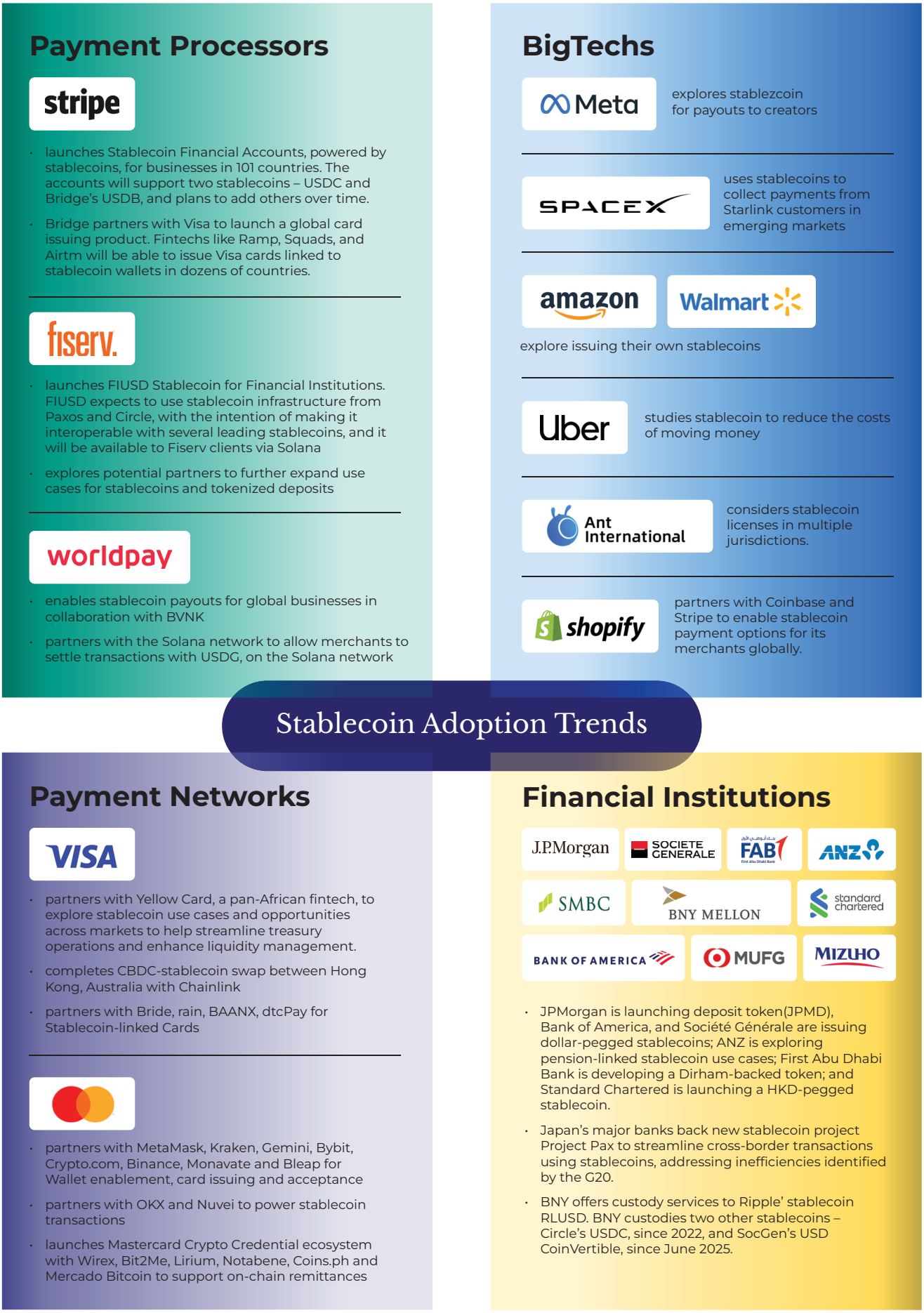
"We've seen US$3.7 trillion in USDC volume on Solana in a single quarter. This isn't speculative. Payment companies are building stablecoin strategies because regulations are finally giving them permission to enter. The floodgates have opened."

Lu Yin - APAC Lead, Solana Foundation

[30] Ethena, 2025

1.2.2 TradFi Embraces Stablecoins: From Experimentation to Integration

Figure 1.3:



Source: Public disclosures and corporate media statements

Stablecoins are no longer peripheral instruments limited to crypto-native firms; they are becoming integral to global financial and payment ecosystems. These past two years have witnessed a remarkable uptick in institutional and corporate participation across a wide spectrum of industries. Financial institutions such as JPMorgan, Société Générale, and Bank of America have either launched or are exploring dollar-pegged stablecoins, while Standard Chartered is developing an HKD-pegged variant and First Abu Dhabi Bank is piloting a Dirham-backed stablecoin. Custodians like BNY Mellon are expanding their digital asset custody offerings to support stablecoins such as Ripple's RLUSD and Circle's USDC, signalling deepening integration into traditional banking services.

At the same time, major payment networks like Visa and Mastercard are actively shaping stablecoin utility. From card-linked stablecoin wallets to global remittance infrastructure, partnerships with players such as Chainlink, OKX, and Nuvei demonstrate the increasing convergence between digital asset platforms and incumbent payment rails.

Payment processors are also moving aggressively: Stripe now supports stablecoin financial accounts in over 100 countries, and Fiserv is developing interoperability layers for institutions using Solana-based infrastructure.

Big Tech firms are equally active, with Meta exploring creator payouts, SpaceX trialling stablecoin payments in emerging markets, and Shopify integrating stablecoin payment options for merchants globally. Retail and e-commerce giants like Amazon and Walmart are reportedly assessing issuance models, while Uber and Ant International are studying deployment strategies to enhance cross-border efficiency.

Together, these developments cement stablecoins as a high-scale, high-velocity component of the modern financial stack, no longer experimental, but increasingly foundational. As adoption accelerates across banking, payments, and platform ecosystems, stablecoins are steadily converging with mainstream finance.

1.2.3 Mapping the Stablecoin Stack: Functions, Risks, and Regulatory Touchpoints

Figure 1.4:

The Stablecoin Stack

	Examples	Ecosystem Role	Regulatory Scrutiny Level	Key Regulatory Considerations
Applications & Interfaces	SlingMoney, Bitso, Strike, DolarApp, Lemon	Deliver real-world use cases (e.g., remittances, savings, payments), often abstracting stablecoin usage from the user	High	AML/KYC obligations, consumer protection, licensing as PSP or EMI
Orchestrators & Infrastructure Providers	BVNK, Walapay, Conduit, Fireblocks, Paxos	Coordinate the movement, compliance, custody, and interoperability of stablecoins across chains and jurisdictions	Medium	AML compliance infrastructure, API-based transfer tracking, Travel Rule support
Liquidity Providers & Market Makers	Wintermute, Keyrock, Cumberland, Flowdesk, FalconX	Ensure on-chain/off-chain liquidity, arbitrage, and pricing efficiency for stablecoins-Fiat transactions	Medium	Market abuse risk, exchange registration, cross-border capital flow regulation
Issuers	Tether, Circle, Ripple, Binance, PayPal	Mint and redeem stablecoins, maintain reserves, ensure peg stability	High	Reserve transparency, prudential oversight, systemic importance thresholds
Blockchains	Ethereum, Solana, Tron, Base, Stellar, Avalanche	Provide transaction finality, smart contract execution, and decentralised transparency for stablecoin activity	Low	Jurisdictional control, compliance tooling, public chain risk assessments
Custodians & Trust Structures	BNY Mellon, Anchorage, Zodia, BitGo, Paxos Trust	Safekeep reserve assets, offer attestations, provide bankruptcy-remote structures	High	Audit & reserve regulation, fiduciary responsibility, legal segregation of funds
Governance & Attestation Providers	Chainlink (PoR), Armanino, Deloitte, OpenZeppelin, Notabene	Provide smart contract audit, real-time reserve verification, off-chain/on-chain data bridges	Low	Attestation standards, smart contract liability, oracles and systemic reliance

Source: GFTN Analysis

As stablecoins scale rapidly and move closer to mainstream finance, the complexity of their underlying ecosystem has grown in parallel. The stablecoin market is no longer limited to issuers and users. It now spans a full-stack architecture that includes interfaces, liquidity providers, custodians, governance frameworks, and technical infrastructure providers. Understanding this stack is important for regulators, industry participants, and financial system coordinators alike, as it helps delineate responsibilities, risks, and regulatory focus areas across the value chain.

At the top of this stack are Applications and Interfaces, such as SlingMoney, Bitso, or DolarApp, which provide users with direct access to stablecoin use cases, ranging from remittances to savings products. These entities typically face high regulatory scrutiny, particularly around licensing, AML/KYC obligations, and consumer protection.

Infrastructure providers like BVNK and Fireblocks play a foundational role, enabling stablecoin movement and interoperability across platforms and jurisdictions. As orchestrators of cross-chain activity, they must support AML compliance infrastructure, Travel Rule integration, and secure custody. While their role is primarily technical, supporting applications or stablecoin issuers, their position at the heart of transaction routing and interoperability makes them critical to system integrity. As a result, they often face medium regulatory scrutiny, either directly or indirectly through oversight of their institutional clients.

The Liquidity Providers and Market Makers, including firms like Wintermute and Flowdesk, maintain pricing efficiency and enable stablecoin-to-fiat conversion at scale. Their exposure to market abuse risks and capital flow regulation places them under a similar medium regulatory scrutiny.

At the core of the ecosystem are the Issuers, i.e. Tether, Circle, Ripple, and others, who are responsible for minting, redemption, reserve management, and peg stability. Given their systemic importance and financial responsibilities, these entities face the highest levels of scrutiny focused on reserve transparency, systemic thresholds, and prudential oversight.

Beneath these operational layers lie the blockchains, public infrastructure such as Ethereum, Solana, and Base, which ensure transaction finality and smart contract execution. While essential to the ecosystem, they are subject to relatively low regulatory scrutiny, though concerns around jurisdictional control, transparency and compliance tooling persist.

Custodians and Trust Structures such as BNY Mellon and Anchorage hold and secure reserves, offering legal segregation and bankruptcy-remote mechanisms. These functions draw high regulatory attention due to fiduciary obligations and the need for robust audit frameworks. These entities are already regulated within the traditional financial system, as they operate as licensed banks, trust companies, or qualified custodians subject to stringent oversight across jurisdictions.

Finally, Governance and Attestation Providers, ranging from Chainlink to Deloitte, are emerging as key players in ensuring real-time transparency and smart contract integrity. Though less visible to end-users, they are integral to operational assurance and systemic reliability. As they primarily deliver services to regulated issuers and custodians, their operations are increasingly subject to indirect oversight through client compliance requirements, especially in areas like audit quality, data attestation standards, and smart contract liability.

This multi-layered structure highlights that regulating stablecoins cannot be reduced to regulating issuers alone. Each layer of the ecosystem, ranging from wallets and applications to custodians, infrastructure providers, and attestation services, carries distinct operational roles and risk profiles. As such, they require differentiated forms of oversight: some rooted in financial conduct and prudential regulation, others focused on technological assurance, operational resilience, and data integrity. To address this complexity, policymakers may need to adopt a more holistic supervisory approach. This may include not only direct regulation of Stablecoin Issuers and Custodians, but also indirect oversight through TPRM obligations imposed on regulated entities for technology, infrastructure, and professional service providers. In parallel, regulators may develop guidance, minimum compliance standards, or certification programs for key service providers supporting stablecoin ecosystems.

1.2.4 Drivers and Inhibitors for Stablecoin Adoption Across the World

Stablecoin adoption varies significantly across regions, influenced by distinct economic needs and regulatory concerns. The U.S. has become the most active market for stablecoin innovation, with regulated offerings such as USDC gaining traction across payment platforms, trading venues, and treasury applications. Pilot projects increasingly link stablecoins with cross-border payment use cases, drawing participation from both Fintechs and traditional financial institutions.

In contrast, stablecoin adoption in the E.U. and U.K. has been more measured. While there are regulated offerings such as EUR CoinVertible and pilot projects around tokenized commercial payments, authorities have generally taken a cautious stance. The E.U.'s MiCA framework provides an overarching regulatory structure but limits room for rapid growth, and the Bank of England has proposed caps[31] on stablecoin holdings for systemic payment systems

[31] The Paypers, 2025

to mitigate financial stability risks. Regulatory concerns centre on monetary sovereignty, consumer protection, and systemic oversight, reflecting a more conservative approach compared to the U.S.

In Asia-Pacific, developed economies are leveraging stablecoins and tokenized deposits as catalysts for Fintech advancement by embedding them into digital banking infrastructure, cross-border payment corridors, and government-led initiatives such as Japan's licensed stablecoin trust frameworks and Hong Kong's regulatory sandbox for stablecoin issuance. While these efforts are unlocking new models for programmable money and institutional settlement, they are also driving the evolution of regulatory frameworks across jurisdictions. In contrast, emerging economies in Latin America pursue stablecoins to mitigate currency volatility and promote financial inclusion by enabling access to dollar-backed digital assets through mobile wallets and crypto platforms, particularly in regions with limited banking penetration or inflationary local currencies. However, these benefits come with potential risks to capital controls and monetary policy transmission, prompting regulators to tread carefully.

"The biggest inhibitor for stablecoin adoption is the lack of a scale model that enterprises can adopt. Companies with large distribution networks of consumers want to adopt stablecoin infrastructure but don't see value in today's models where the economic benefits go to the issuer. These firms want white-label infrastructure that integrates with their systems and allows them to retain user economics. Our role is to offer "stablecoin-as-a-service" with regulatory clarity and operational flexibility. We've done this with Binance, PayPal, and are in discussions with other major players looking for similar models."

Walter Hessert - Head of Strategy, Paxos

"Sound stablecoin regulation should prioritize solvency, segregation of client assets, and mechanisms for cross-border supervision. These elements together help safeguard users, maintain trust, and support market integrity in both normal and stressed conditions."

Roeland Van Der Stappen - Head of E.U. Policy, Coinbase

Table 1.7:

Stablecoins Drivers and Inhibitors Across Regions

1. United States (Developed Economy)	
Drivers	**Inhibitors/Risks**
✅ Promote and maintain USD dominance globally.	⚠️ High market concentration.
✅ Enhance financial innovation and technology leadership.	⚠️ Opaque reserve practices.
✅ Facilitate efficient and cost-effective payments.	⚠️ Fraud, and redemption failures.

2. Europe & United Kingdom (Developed Economies)	
Drivers	**Inhibitors/Risks**
✅ Foster innovation in digital finance.	⚠️ Monetary policy sovereignty concerns.
✅ Support faster and cheaper intra-European payments.	⚠️ Financial stability and systemic risk.
✅ Strengthen global competitiveness in Fintech.	⚠️ AML/KYC risks and consumer protection.
Example: **United Kingdom, Germany, France, Italy**	

3. Asia-Pacific (Developed Economies)

Drivers	Inhibitors/Risks
✅ Strengthen position as global Fintech and innovation hubs.	⚠️ Regulatory complexity and fragmentation.
✅ Enhance regional financial integration and payment efficiency.	⚠️ Risk of financial disintermediation.
✅ Attract global digital asset companies.	⚠️ Concerns over illicit financial activities.
Example: **Singapore, Australia, Japan, Hong Kong**	

4. Major Emerging Economies (BRICS and others)

Drivers	Inhibitors/Risks
✅ Address currency volatility and inflation.	⚠️ Capital flight and exchange control concerns.
✅ Reduce cross-border payment fees.	⚠️ Monetary policy disruption.
✅ Promote financial inclusion.	⚠️ Risks related to dollar dominance.
✅ Provide alternative financial infrastructure.	
Example: **Brazil, Russia, India, China, South Africa**	

5. Developing Economies (Africa, Latin America)

Drivers	Inhibitors/Risks
✅ Mitigate severe currency instability.	⚠️ Limited regulatory capacity.
✅ Reduce dependency on inefficient traditional banking.	⚠️ Potential financial instability.
✅ Facilitate remittances and cross-border payments.	⚠️ Risk of illicit transactions (AML issues).
Example: **Nigeria, Kenya, Ghana, Argentina, Venezuela**	

6. Frontier Economies (Small developing states, Island nations)

Drivers	Inhibitors/Risks
✅ Enhance financial inclusion and access.	⚠️ Regulatory inexperience and uncertainty.
✅ Reduce high remittance fees.	⚠️ Limited technical and financial infrastructure.
✅ Improve resilience to external economic shocks.	
Example: **Bahamas, El Salvador, Fiji, Barbados**	

Source: GFTN Analysis

1.2.5 Stablecoins in Action: Key Regulatory Developments (Q1–Q3 2025)

In the first three quarters of 2025, the stablecoin sector has seen a slew of dynamic developments on the regulatory fronts. Governments and financial regulators across the globe are rapidly formalising rules to ensure stablecoin safety, transparency, and alignment with monetary and financial stability objectives. Table 1.8 highlights selected regulatory initiatives shaping the digital money and stablecoin landscape.

Table 1.8:

Stablecoin: Regulatory Initiatives

Quarter	Entities	Activity	Description
Q1 2025 (Jan-Mar)	**U.S. Government**	Draft bill	The GENIUS Act and the STABLE Act were introduced in the U.S.
	DFSA	Approval	Dubai approved Circle's stablecoins USDC and EURC for use in DIFC.
	JFSA, SBI VC Trade	Approval	SBI VC Trade secured regulatory approval to list and distribute USDC in Japan.
	OCC (U.S.)	Guidance	OCC announced that federally regulated banks can engage in certain stablecoin activities without prior approval.
	Thailand SEC	Approval	Thailand's SEC added USDC and USDT stablecoins to approved cryptocurrencies.
	U.S. Government	Draft bill	The latest draft of the GENIUS Act proposed to split stablecoin regulation between state and federal authorities.
	U.S. Government	Draft bill	The U.S. Senate Banking Committee advanced the GENIUS Act toward the Senate floor.
	Australia Government	Guidance	Australia's government announced plans to introduce crypto regulations targeting custody and stablecoin issuance.
	U.S. Government	Draft bill	The U.S. Congress released the text version of the STABLE Act.
Q2 2025 (Apr-Jun)	**SEC (U.S.)**	Guidance	SEC clarified that some stablecoins aren't securities and are marketed solely for use in commerce.
	Kenya's National Treasury	Draft bill	Kenya proposed the first crypto bill to regulate ICOs, stablecoins, exchanges.
	U.K. Government	Draft bill	The U.K.'s new crypto rules to subject U.K.-based stablecoin issuers to regulation.
	HKMA	Bill passed	Hong Kong's legislature passed a stablecoin bill that establishes a licensing regime for fiat-referenced stablecoin issuers.
	U.S. Government	Bill passed	The U.S. Senate advances stablecoin bill, formally titled the GENIUS Act.
	JFSA	Draft bill	JFSA introduced a new Bill to update the Payment Services Act, the legislation that governs stablecoins and cryptocurrencies.
	Ripple	Approval	Ripple's RLUSD stablecoin has received regulatory approval from the DIFC.

	U.S. Senate	Draft bill	The U.S. Senate passed the GENIUS Act to regulate stablecoins.
	Circle	Approval	Circle received in-principle regulatory approval from Abu Dhabi Global Market's Financial Services Regulatory Authority to expand its operations in the Middle East.
	U.K. Government	Consultation	The U.K. government released consultation papers on stablecoin issuance.
	SEC, PayPal	Investigation	SEC concluded its investigation into PayPal's stablecoin, PYUSD, and would not take any enforcement actions.
	FCA (U.K.)	Consultation	The FCA announced that it is seeking additional views on its upcoming stablecoins regime.
Q3 2025 (Jul-Sep)	**SEC, Ripple**	Lawsuit	The U.S. Securities and Exchange Commission's 2020 lawsuit against Ripple Labs is officially over, after the two parties informed the Second Circuit Court of Appeals that they were voluntarily dismissing their respective appeals of a 2023 ruling in the case.
	HKMA	Launch	Hong Kong's rules for licensing stablecoin issuers came into effect.
	HKMA	Guidance	HKMA released guidelines on capital, reserve and governance standards for stablecoin issuers wanting to get licensed.
	U.S. Government	Laws	U.S. President Donald Trump signed the GENIUS Act, the Senate's stablecoin bill, passed by the House of Representatives, into law.
	Ripple, OCC	Licence	Ripple applied for a national banking licence from the Office of the Comptroller of the Currency.
	The Commodity Futures Trading Commission (U.S.)	Announcement	The Commodity Futures Trading Commission, as part of its ongoing "crypto sprint," is advising firms that felt pressured to leave the U.S. that they can still do business domestically as "foreign boards of trade."
	BMA, Haycen	Licence	Haycen secured a stablecoin issuance licence from the Bermuda Monetary Authority.
	JFSA	Approval	Japan's Financial Services Agency will approve the first yen-denominated stablecoin by the end of 2025.

Table 1.9:

Regulatory Clarity Fuels Digital Money Innovation

A. Singapore – Purpose Bound Money (PBM) by MAS

Authority : MAS

Framework: PBM under Project Orchid

Key Developments:

- In 2022–2023, the MAS released a technical whitepaper introducing PBM, a programmable form of digital money that enables restricted usage conditions, such as specific merchants, timeframes, or purposes.
- This form of programmable digital money is designed to provide greater control over how tokenized currency is spent, enabling more targeted fiscal interventions or subsidy programs.
- PBM allows the digital money to be embedded with logic such that it can only be spent if predefined conditions are met (e.g. location-based usage, merchant acceptance, time-bound disbursement). This provides granular control while preserving the fungibility and transferability of digital currency.
- The pilot deployments of PBM were conducted in partnership with major commercial and technology players:
- Grab tested programmable retail vouchers that could be redeemed at designated merchants.
- UOB trialled commercial payment flows with programmable disbursement logic for business clients.
- Other use cases included disbursement of government aid, merchant-specific commercial payments, and pay-per-use infrastructure transactions.

Objectives:

- Build foundational infrastructure to support a tokenized Singapore dollar ecosystem, enabling digital currency adoption for both retail and institutional use cases.
- Enable programmable payment conditions that can support specific policy objectives (e.g. stimulus control, grant disbursement, or conditional subsidies).
- Ensure continued financial control and regulatory oversight by allowing authorities to program monetary flows without issuing a CBDC directly, maintaining the two-tier monetary system.

Industry Implications:

- Singapore's PBM initiative stands out as a CBDC alternative that leverages tokenized commercial bank money and e-money structures to offer programmable features. It reflects MAS's broader "minimum viable central bank digital infrastructure" strategy to empower the private sector to innovate within a controlled, interoperable framework.
- Unlike CBDCs that are centrally issued and often more rigid, PBM provides a flexible regulatory model that enables innovation while maintaining compliance and stability. It also offers a viable pathway for cross-border interoperability by integrating with tokenized deposits and stablecoins.

Sources: MAS, 2023; The Straits Times, 2023; Project Orchid Overview, 2022

B. European Union – MiCA

Authority : European Commission, supervised by ESMA & EBA

Framework: MiCA Regulation (entered into force in 2023, full implementation in 2024)

Key Developments:

- Following MiCA's phased rollout, stablecoin provisions from June 30, 2024, and crypto-asset service providers from December 30, 2024, significant momentum has followed in 2025.
- Around 73% of stablecoin issuers began compliance ahead of the deadline, with over 40 projects seeking MiCA authorisation. The E.U. market is projected to grow 37% in 2025, with stablecoin assets reaching approximately €450 billion.
- Within the first 100 days of full enforcement, 11 EMT-issuer licences were granted, spanning six countries, including Germany and Malta. These issuers produced 10 euro-pegged tokens and 6 dollar-pegged tokens. Notable institutional entrants, such as Société Générale, BBVA, and Circle, have positioned themselves firmly within the MiCA framework, signalling mainstream banking engagement.

- Consumer protection and stability measures are already reshaping market dynamics: Tether's USDT has been delisted by some E.U. exchanges due to non-compliance, while Circle's USDC, built with MiCA standards in mind, has gained regulatory acceptance.

Objectives:

- Establish a harmonised E.U.-wide regulatory framework for crypto assets, particularly stablecoins, to reduce legal fragmentation across member states.
- Enhance financial stability and consumer protection through strict reserve backing, redemption rights, and prudential oversight of stablecoin issuers.
- Support innovation by providing regulatory certainty, enabling legitimate projects to scale across the E.U. via a single "passporting" licence.

Industry Implications:

- Stablecoins like Tether's USDT face reduced access or outright delisting in MiCA-compliant jurisdictions due to opaque reserve structures and lack of licensing, pushing market share toward regulated alternatives such as Circle's USDC and Société Générale's EURCV.
- CEXs operating in the E.U. must ensure that stablecoins they list are MiCA-compliant, impacting token selection, custody design, and disclosure obligations.
- Regulatory clarity encourages banks, payment firms, and Fintechs to develop MiCA-aligned euro- and dollar-pegged stablecoins, with at least 11 issuers already licensed across 6 countries.
- MiCA's stablecoin regime is influencing policy debates in jurisdictions like the U.K., Hong Kong, and the U.S., acting as a blueprint for aligning innovation with financial safeguards.

Sources: ESMA, accessed Sep 2025; Coinlaw, 2025; Cryptopolitan, 2025

C. Japan – Institutional-Led Innovation with MUFG's Progmat Stablecoin Platform

Authority : Japan's FSA

Framework: Regulated issuance framework under the Payment Services Act (2023) that restricts stablecoin issuance to banks, trust companies, and licensed money transfer agents, with mandatory 1:1 fiat backing and redeemability guarantees.

Key Developments:

- Following Japan's June 2023 implementation of stablecoin regulations that restrict issuance to licensed financial institutions, MUFG has advanced its Progmat Coin platform to issue and manage bank-backed stablecoins.
- In April 2025, MUFG Trust prepared to launch Japan's first compliant stablecoin, built on Progmat infrastructure, with planned usability across multiple public blockchains such as Ethereum, Avalanche, Polygon, and Cosmos.
- In May 2025, Japan's FSA proposed amendments to the Payment Services Act that expand reserve flexibility for trust-type stablecoins, allowing up to 50% of reserves to be held in low-risk instruments such as short-term government bonds and time deposits, provided a 1:1 reserve ratio is maintained.

Objectives:

- Support institutional-grade, bank-backed stablecoin issuance that complies with the Payment Services Act.
- Build a domestic digital currency infrastructure with cross-chain interoperability for yen and foreign currency tokenized money.
- Promote digital assets integration by enabling financial institutions to issue stablecoins, pilot trade settlement use cases, and connect with global stablecoin networks.

Industry Implications:

- MUFG's Progmat-led initiatives have spawned wallet providers (Ginco), settlement systems (STANDAGE), custodians, and global partnerships (e.g. Binance Japan).
- Institutional leadership and regulatory backing position Japan as a credible hub for stablecoin innovation and cross-border tokenized money flows.
- Japan stands out as a model for cautious, bank-led stablecoin issuance under comprehensive regulatory supervision, offering a blueprint for jurisdictions seeking to introduce stablecoins through a conservative and institutionally anchored approach.

Sources: Cryptonomist, 2025; MUFG, 2024; Law.Asia, 2025

D. Hong Kong – Stablecoin Regulatory Regime by HKMA & FSTB

Authority : HKMA & FSTB

Framework: Stablecoin Issuers Ordinance

Key Developments:

- In January 2022, the HKMA published a Discussion Paper on Crypto assets and Stablecoins, signalling its intention to establish a dedicated regulatory framework for stablecoin issuance and operations.
- In December 2023, the HKMA and FSTB jointly launched a Public Consultation on the legislative proposal to implement a comprehensive regime for stablecoin issuers. The framework closely reflects the FSB's July 2023 high-level recommendations on global stablecoin arrangements, emphasising prudential standards, reserve management, and operational resilience.
- The framework applies consistently to both single- and multi-jurisdictional issuers, ensuring uniform standards. Stablecoins must be fully backed at all times, with reserve assets held by an HKMA-licensed bank or HKMA-approved custodian.
- Only Hong Kong-incorporated entities or licensed banks incorporated outside Hong Kong are eligible to obtain a licence, ensuring strong local oversight and alignment with international norms.

Objectives:

- Safeguard financial stability and monetary sovereignty by ensuring stablecoins used in Hong Kong are fully backed and properly regulated.
- Promote market integrity and investor protection through stringent licensing, disclosure, and reserve asset requirements.
- Support the responsible development of digital assets, positioning Hong Kong as a trusted hub for regulated stablecoin activities.

Industry Implications:

- Hong Kong's regime provides regulatory clarity and uniformity by applying the same standards to both local and global stablecoin issuers. This addresses cross-border challenges while aligning with FSB recommendations.
- The framework sets strict eligibility and reserve requirements, ensuring that only well-capitalised and prudentially managed entities can issue stablecoins in Hong Kong.
- By embedding international standards into local law, Hong Kong strengthens its role as a regional leader in digital asset regulation, balancing innovation with systemic safeguards.

Sources: HKMA, 2022; FSTB & HKMA Consultation, 2023; HKMA, 2024; FSB, 2023

1.2.6 Stablecoin Regulatory Landscape: Comparing Major Jurisdictions

As stablecoins continue to evolve from speculative instruments to core components of digital financial infrastructure, several jurisdictions have moved decisively toward implementing structured regulatory frameworks. In 2025, jurisdictions such as the European Union, Japan, Singapore, Switzerland, Hong Kong, the U.A.E., and the United States, via the GENIUS Act, represent a cohort of markets where stablecoin regulation has either already been passed or is progressing rapidly. These jurisdictions reflect a spectrum of approaches, from the E.U.'s harmonised and risk-based MiCA framework to Switzerland's principle-based integration within existing financial law, and Singapore's high-bar regulatory architecture focused on reserve quality and financial stability. This wave of regulatory momentum reflects growing consensus around the need to align stablecoin systems with broader monetary, prudential, and consumer protection mandates. According to the FSB's 2025 peer review report[32], relatively few jurisdictions have actually finalised comprehensive regulatory frameworks for global stablecoin arrangements, and even those fall short of full alignment with the FSB's high-level recommendations. In practice, this patchy implementation has led to gaps and inconsistencies. A situation the FSB warns could enable regulatory arbitrage and complicate effective oversight of stablecoin arrangements operating across borders. Strengthening and harmonising stablecoin rules internationally is thus still very much a work in progress in 2025, despite the growing consensus on their importance.

[32] FSB, 2025

Table 1.10:

Overview of Global Stablecoin Regulatory Frameworks and Underlying Principles

Jurisdiction	Stablecoin Regulatory Status	Relevant Regulatory Framework	Regulatory Approach / Principle Toward Stablecoins
U.S.	Passed	GENIUS Act, STABLE Act, FinCEN MSB regime	**Risk-based,** focused on financial stability and consumer protection.
E.U.	Passed	Markets in Crypto Assets Regulation	**Comprehensive risk-based**, harmonized across E.U.
Japan	Passed	Revised Payment Services Act	**Pro-stability,** banking-led issuance only by licensed banks and Trust companies.
India	Not initiated	RBI + Ministry of Finance (Discussion paper upcoming)	**Wait-and-see** approach.
U.K.	In Development	Financial Services and Market Act, FCA Discussion Papers	**Functional approach**: stablecoins as e-money, with systemic token focus.
Brazil	Early Stages	Brazil Crypto Law (Law No. 14,478/22)	**Capital flow protection**, evolving toward prudential oversight.
K.S.A	Not initiated	SAMA & CMA Innovation Sandbox (no named framework yet)	**Wait-and-see** approach.
Switzerland	Passed	FINMA ICO Guidelines, DLT Act, banking licences for issuers	**Technology-neutral, principle-based**, integrated into existing financial law.
Singapore	Passed	MAS Stablecoin Regulatory Framework (2023)	**High-quality reserve backing, redeemability,** and **financial stability focus.**
U.A.E.	Passed	VARA Regulatory Framework; ADGM DLT Regime	**Commercial permissiveness** with supervision, aligned to **economic diversification goals.**
Hong Kong	Passed	VASP Licensing Regime (under SFC/ FSTB), Stablecoin Consultation Paper.	**High-quality reserve backing, redeemability,** and **financial stability focus.**
Qatar	Not initiated	QFC Digital Assets Framework (2024)	**Restrictive**; stablecoins seen as incompatible with current Digital Assets Framework.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

The following sections will provide a comparative deep dive across these jurisdictions, focusing on key regulatory dimensions such as legal classification, issuer requirements, reserve asset rules, custody, redemption rights, and AML/ CFT obligations. The aim is to highlight both areas of convergence and jurisdiction-specific approaches that shape the evolution of compliant stablecoin ecosystems.

Jurisdictions like Saudi Arabia, Brazil, India, and Qatar are excluded from this comparison, as stablecoin regulation in these markets is either in very early stages with no public announcements or is explicitly excluded from the current digital asset regulatory framework.

1.2.6.1 Stablecoin Regulatory Landscape: Legal Definition & Classification

Table 1.11:

Legal Definition & Classification

Jurisdiction	Definition / Classification
U.S.	Payment stablecoins (GENIUS Act).
E.U.	E-Money Tokens or Assets-Referenced Tokens.
Japan	Electronic payment instruments.
U.K.	Digital Settlement Assets.
Switzerland	Providing a means of payment aimed at reducing price volatility.
Singapore	Single-Currency Stablecoins.
U.A.E.	Stablecoins regulated as Payment Token.
Hong Kong	Flat-referenced stablecoins (excludes algorithmic types).

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

Across leading jurisdictions, the legal classification of stablecoins has evolved toward a functional and payment-oriented lens. The United States, under the GENIUS Act, defines stablecoins as "payment stablecoins" issued by regulated financial institutions.

The European Union offers one of the clearest taxonomies through the MiCA regulation, classifying stablecoins as either EMTs or ARTs, depending on their pegging mechanism. EMTs are stablecoins that aim to maintain a stable value by referencing the value of a single official currency, such as the euro or the U.S. dollar. EMTs are explicitly treated in parallel with traditional electronic money under existing E.U. payment laws. On the other hand, ARTs are stablecoins whose value is pegged to a basket of assets, which may include multiple fiat currencies, commodities, or other crypto assets. ARTs are subject to a differentiated regulatory regime under MiCA due to their more complex structure and potentially broader use cases, including as investment instruments or stores of value. This two-pronged classification under MiCA allows the E.U. to distinguish between stablecoins designed for payments and monetary use (EMTs) and those oriented toward investment or alternative financial utility (ARTs). Japan categorises stablecoins under the broader umbrella of electronic payment instruments, reflecting its commitment to integrate them within existing payment laws. The United Kingdom refers to them as DSAs, positioning them within a systemic payments framework.

Singapore defines a SCS with specific criteria tied to fiat-pegged instruments. In contrast, Switzerland defines value-stable tokens more broadly as instruments aimed at providing a means of payment that reduces price volatility. The U.A.E. defines stablecoins as "payment tokens" under the Central Bank's 2024 regulation. The regulation treats stablecoins as a form of stored value for payment and remittance services, explicitly excluding their use as investment or speculative instruments. Hong Kong identifies only fiat-referenced stablecoins as eligible, explicitly excluding algorithmic designs. This variety of legal classifications reflects each jurisdiction's underlying regulatory philosophy and risk assessment toward integrating stablecoins into its monetary and financial systems.

Expert Perspectives on Jurisdictions Shaping Stablecoin Policy

"Stablecoins, like digital payment tokens in general, give rise to concerns regarding money laundering/terrorist financing threats and consumer protection. The critical risk for stablecoins however, is value stability. Holders must have confidence that reserve assets are properly set aside and disclosed. More broadly, we are mindful of the potential financial stability issues as digital assets and stablecoins grow more interconnected with traditional markets."

Rosemary Lim - Executive Director, Payments Department, Monetary Authority of Singapore

"Regulatory clarity on stablecoins is emerging but globally we see variations. Singapore and Hong Kong are balanced, Europe is structured under MiCA and the US is catching up with the GENIUS Act. All regulators align on financial stability and consumer protection, but lack of harmonised definitions and requirements adds complexity and poses a challenge to industry players."

Yip Kah Kit - Executive Director, Head of Blockchain and Digital Assets, UOB

"Regulators globally are giving closer attention to how stablecoins fit within payments and settlement frameworks. From initiatives such as MAS's BLOOM, which explores tokenized liabilities and stablecoins for real-world settlement, to the CFTC's work on tokenized collateral, we're seeing a shift toward practical experimentation. These efforts — focused on operational resilience, asset backing, and interoperability — are essential to building confidence as tokenization moves from pilots to production."

Katie Mitchell - Head of APAC and Middle East Policy, Coinbase

1.2.6.2 Stablecoin Regulatory Landscape: Issuance Licensing & Entity Type

Table 1.12:

Issuance Licensing & Entity Type

Jurisdiction	Who Can Issue?
U.S.	Bank subsidiary Non-bank issuer (Fed or State regulated if less than US$10B market cap).
E.U.	Electronic money instituitions or credit instituitions.
Japan	Banks, Fund Transfer Service Providers, and Trust Companies.
U.K.	FCA-regulated firms under DSA regime.
Switzerland	Entities holding a banking licence or exempted from deposit-taking rules under strict conditions. (e.g. full reserce backing, daily redeemability, segregation of funds).
Singapore	MAS-approved issuers; Can be approved as a Non-bank entity (subject to market cap requirements).
U.A.E.	VARA/ADGM-licensed entities; The PTSR licence by CBUAE across the U.A.E. except in the Dubai International Financial Centre and the Abu Dhabi Global Market.
Hong Kong	HKMA-licensed issuers.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

The regulatory frameworks governing who can issue stablecoins vary significantly across jurisdictions, though many are converging toward models that prioritise institutional oversight and financial integrity. In the United States, the proposed framework under the GENIUS Act distinguishes between bank subsidiaries and non-bank issuers, with the latter required to be federally or state-regulated unless their market capitalisation falls below US$10 billion. Collectively, these licensing structures signal a global regulatory preference for bringing stablecoin issuance under the purview of prudential regulators, while allowing limited flexibility for innovation through non-bank licensing models.

In the European Union, issuance is restricted to EMIs or credit institutions under the MiCA regime, aligning stablecoins closely with traditional e-money models. Japan permits issuance by a broader set of regulated entities, including banks, fund transfer service providers, and trust companies, reflecting a flexible yet tightly supervised model. The United Kingdom authorises stablecoin issuance under its DSA regime, with oversight by the FCA. In Switzerland, issuers must either hold a banking licence or be explicitly exempted from deposit-taking rules, provided they meet strict conditions including full reserve backing, daily redeemability, and asset segregation.

Singapore allows MAS-approved issuers, including non-bank entities, provided they meet specific conditions such as market capitalisation thresholds. The U.A.E. offers a dual-regulatory structure. Issuance is permitted by entities licensed under the VARA in Dubai or the ADGM, while the CBU.A.E. enforces a separate PTSR regime that applies across the mainland U.A.E. Under the PTSR framework, the CBU.A.E. recognises and regulates two types of stablecoins used for payments: Dirham Payment Tokens and Foreign Payment Tokens. A Dirham Payment Token is a token denominated in AED, or pegged to the value of another token that is AED-denominated, and must be issued by a licensed Dirham Payment Token Issuer. In contrast, a Foreign Payment Token is denominated in or referenced to a foreign currency and may be issued by foreign entities, including those in the U.A.E. Financial Free Zones, upon registration with the CBU.A.E. In Hong Kong, only entities licensed by the HKMA are permitted to issue fiat-referenced stablecoins, reinforcing a banking-centric approach to market stability.

1.2.6.3 Stablecoin Regulatory Landscape: Reserve Asset Requirements

Table 1.13:

Reserve Asset Requirements

Jurisdiction	Reserve Requirements
U.S.	100% backed by cash, demand deposits (up to FDIC insurance limit), Treasuries or repurchase agreements.
E.U.	100% in liquid, low-risk assets.
Japan	Required to manage all reserves as demand deposits (bank deposits). The New Bill (2025) allows up to 50% of reserves to be held in term deposits and/or government bonds, provided the on-to-one backing is maintained.
U.K.	100% backing by fiat reserves or HQLA expected, details evolving.
Switzerland	100% backing with segregated, bankruptcy-remote, liquid assets; no reinvestment allowed; daily redeemability required for exemption from banking licence.
Singapore	100% HQLA with mark-to-market.
U.A.E.	Hold reserve assets as cash in a separate escrow account that is: 1. In the same currency as the payment tokens. 2. In the issuer's name with a U.A.E.-licensed bank, not part of the issuer's group. 3. Clearly marked for safeguarding reserve assets as regulations. 4. Used only holding the issuer's reserve assets. 5. If the issuer is a wholly-owned subsidiary or a bank, it can hold at least 50% of its reserve assets as cash.
Hong Kong	Fully backed by fiat reserves.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

Stablecoin reserve requirements across jurisdictions emphasise full backing with high-quality, liquid assets to ensure stability, redemption certainty, and financial soundness. In the United States, reserves must be held in cash, demand deposits (up to FDIC insurance limits), treasuries, or repurchase agreements under the proposed regulatory regime. The European Union mandates 100% reserves in liquid, low-risk assets under the MiCA framework. Japan requires reserves to be held as demand deposits with licensed banks. A new legislative bill (2025) introduces some flexibility, allowing up to 50% of reserves to be placed in term deposits or government bonds, provided that the one-to-one backing principle is upheld. The United Kingdom expects 100% backing with fiat currency or HQLA, with further details still being finalised. Switzerland mandates 100% reserve backing with segregated, bankruptcy-remote, and liquid assets. Reinvestment is not permitted, and daily redemption is required to qualify for exemption from banking licensing requirements.

Singapore similarly requires 100% backing with HQLA that are marked to market. The U.A.E. sets out detailed reserve conditions under its PTSR. Reserve assets must be held in cash in an escrow account under the issuer's name at a U.A.E.-licensed bank that is not part of the issuer's corporate group. These assets must be clearly designated for safeguarding purposes, used solely to back the issuer's liabilities, and maintained in the same currency as the

issued stablecoin. If the issuer is a wholly owned bank subsidiary, it is permitted to hold at least 50% of reserves in cash. Hong Kong enforces full fiat reserve backing for all licensed stablecoin issuers.

1.2.6.4 Stablecoin Regulatory Landscape: Redemption Rights & Consumer Protections

Redemption rights are a core element of stablecoin regulation, ensuring users can reliably convert tokens back into fiat value. The European Union requires that redemptions be carried out in a "timely manner" but does not impose a specific time limit. Japan follows a similar approach, requiring redemptions to be processed "without delay," again without defining a fixed redemption window. Singapore provides a more concrete standard, mandating redemption at par within five business days. The United States adopts a stricter timeline under its proposed framework, requiring that redemptions be fulfilled no later than one business day after a customer request.

In the United Kingdom, stablecoins recognised under the regulatory framework must be promptly redeemable at par value by any holder. Hong Kong guarantees unconditional, fair, and transparent redemption rights without delay as a standard part of its licensing framework. The U.A.E.'s rules specify that redemptions must be completed, or at least initiated, for foreign-denominated payment tokens by the end of the next business day, unless otherwise allowed by the Central Bank. Switzerland enforces daily redemption at par value as a condition for exemption from banking licence requirements. This focus on speed, fairness, and transparency in redemption processes reflects a broader global consensus on the importance of safeguarding end-user confidence in stablecoin ecosystems.

1.2.6.5 Stablecoin Regulatory Landscape: Anti-Money Laundering and Travel Rule Obligations

As stablecoins move further into mainstream financial ecosystems, their alignment with global AML and CFT frameworks has become a foundational regulatory priority. Most jurisdictions that have introduced or are finalising stablecoin regulations in 2025 have explicitly incorporated AML/CFT obligations that mirror the FATF standards. These typically include CDD, suspicious transaction reporting, and specific rules for VASPs. In the European Union, the AML Directives (notably AMLD5 and AMLD6), reinforced by Title VI of the MiCA regulation, establish mandatory safeguards for crypto asset issuers and service providers. Similarly, the United States imposes AML obligations on stablecoin issuers through FinCEN's MSB regime, while Singapore and Japan enforce oversight via MAS notices and the Act on Prevention of Transfer of Criminal Proceeds, respectively.

A key cross-jurisdictional harmonising tool is the Travel Rule, originally developed for wire transfers and extended by the FATF to cover digital asset transfers. The rule requires the collection and transmission of originator and beneficiary information by VASPs during crypto transfers above a certain threshold. The goal is to make stablecoin transactions traceable across borders, aiding law enforcement and regulatory monitoring. Every jurisdiction covered in Table 1.11 has now embedded Travel Rule compliance into its frameworks for digital assets, including stablecoins. The E.U., U.K., and Switzerland have no minimum thresholds, while the U.A.E. applies the rule from AED 3,500 (approximately US$ 950). In Hong Kong, AMLO-compliant entities are obligated to apply the Travel Rule under their new VASP licensing framework, while Japan's implementation came into effect in mid-2023.

This near-universal convergence on AML/CFT measures and Travel Rule obligations reflects growing international alignment on digital asset oversight. Jurisdictions are not only enforcing baseline FATF rules but also tailoring them to stablecoin risks, particularly around illicit finance, anonymity, and cross-border flows, without undermining innovation. While implementation timelines and technical standards may vary slightly, the underlying principles are now consistent across most advanced regulatory regimes. This harmonisation is particularly important for fostering global interoperability and reducing regulatory arbitrage in the stablecoin sector.

Industry Perspectives on Regulatory Compliance Challenges

"The most pressing challenges for digital assets are balancing privacy with AML/KYC, ensuring interoperability without compromising sovereignty, and addressing settlement risks. Stablecoins highlight all three dilemmas in real-time, requiring careful regulation to maintain safety while enabling innovation."

Ezechiel Copic - Director, Digital Currency Policy, Visa

"The biggest is balancing privacy with AML/KYC obligations. Other challenges include settlement finality on blockchains, travel rule compliance, and ensuring new entrants meet the same standards as regulated financial institutions. True compliance requires constant investment in technology and monitoring, not just policies on paper."

Jesse McWaters - Executive Vice President, Head of Global Government Affairs, Mastercard

1.2.7 Stablecoins in Action: Key Market Developments (Q1–Q3 2025)

The pace and direction of stablecoin market activity are increasingly shaped by evolving regulatory frameworks.

Against this backdrop, Q1–Q3 2025 witnessed a surge in market activity, with banks, Fintechs, and global exchanges aligning new stablecoin initiatives with emerging regulatory clarity and associated compliance requirements. Table 1.14 highlights key market developments during this period.

Table 1.14:

Stablecoin: Market Activities

Quarter	Entities	Activity	Description
Q1 2025 (Jan-Mar)	Ripple, Chainlink	Partnership	Ripple partnered with Chainlink to integrate real-time price oracles, enhancing the utility and adoption of its RLUSD stablecoin across DeFi markets.
	Circle, Hashnote	Acquisition	Circle acquires Hashnote.
	ABN AMRO, 21X	Partnership	ABN AMRO and 21X conducted on-chain trade of tokenized assets against stablecoins.
	Tether	Launch	Tether launched the USDT stablecoin on the Bitcoin and Lightning Networks.
	Stripe, Bridge	Acquisition	Stripe acquired ED Bridge, a stablecoin API platform, for US$1.1B.
	Standard Chartered Bank (Hong Kong), Animoca Brands, and HKT	Announcement	Standard Chartered Bank (Hong Kong) Limited, Animoca Brands, and HKT announced plans to issue a stablecoin backed by the Hong Kong dollar.
	Mansa	Funding	Mansa raised US$10M to expand stablecoin-based cross-border payments.
	Société Générale Forge, Stellar	Launch	Société Générale Forge launched a EUR-backed stablecoin on the Stellar network.
	Ethena	Funding	USDe Stablecoin Developer Ethena Raises US$100M.
	Bank of America	Announcement	Bank of America announced plans to launch its own dollar-backed stablecoin.
	Mesh	Funding	Mesh raised US$82M to expand its stablecoin-based payments settlement network.
	Fidelity Investments	Announcement	Fidelity Investments announced plans to launch its own dollar-pegged stablecoin.
	Ripple	Integrate	Ripple integrates RLUSD Stablecoin into its cross-border payments system.
	Sony	Launch	Sony began accepting USDC payments in its Singapore online store.
	Bitso Business	Launch	Bitso Business introduced euro-denominated payment ramps utilising SEPA and stablecoins.

	Visa	Partnership	Visa joined the Global Dollar Network (USDG) stablecoin consortium.
	Circle	Launch	Circle launched a new payments and cross-border remittance network.
	ING	Development	ING announced that it is working on a stablecoin project with other banks and crypto firms.
	Mastercard	Launch	Mastercard partnered with Nuvei and Circle to enable merchants to settle transactions in stablecoins.
	ADQ, IHC, First Abu Dhabi Bank	Partnership	ADQ, IHC, and First Abu Dhabi Bank partnered to launch a new stablecoin backed by dirhams.
	BVNK, LianLian	Partnership	BVNK partnered with LianLian to convert merchant stablecoin deposits to USD.
	Deutsche Bank	Exploration	Deutsche Bank announced that it is exploring stablecoins and tokenized deposits as part of its digital assets strategy.
	SG Forge	Exploration	SG Forge, the cryptocurrency division of Société Générale, announced plans to introduce a dollar-backed stablecoin on
	PayPal	Exploration	PayPal announced plans to bring its PYUSD stablecoin to the Stellar blockchain network.
	Shopify	Launch	Shopify enabled stablecoin payments for its merchants over Base, Coinbase's Ethereum layer-2 network.
	Walmart, Amazon	Exploration	Walmart and Amazon are considering issuing their own stablecoins in the U.S., as per WSJ.
	Coinbase	Launch	Coinbase launched Coinbase Payments to allow merchants to accept stablecoin USDC payments 24/7 without blockchain expertise.
	Visa	Expansion	Visa expanded its stablecoin capabilities across the Central and Eastern Europe, Middle East, and Africa (CEMEA) region.
	Fiserv	Launch	Fiserv announced plans to launch a new digital asset platform and FIUSD stablecoin on Solana.
	Mastercard	Launch	Mastercard integrated PayPal's PYUSD, the Paxos-led Global Dollar (USDG) and Fiserv's FIUSD into its global network.
Q2 2025 (Apr-Jun)	SoFi	Launch	SoFi announced plans to launch international remittances through blockchain networks and stablecoins.
	Taurus	Launch	Taurus rolled out a zero-knowledge proofs (ZKP) privacy layer for stablecoins, starting with Circle's USDC.
	World Liberty Financial, Re7 Labs	Partnership	World Liberty Financial partnered with Re7 Labs to set up a USD1 stablecoin vault on DeFi lending platforms Euler and Lista.
	Bolt	Launch	Bolt introduced stablecoin payments to streamline cross-border commerce for merchants and marketplaces.

Mastercard, Nuvei, Circle, and Paxos	Partnership	Mastercard partnered with Nuvei, Circle, and Paxos to enable merchants to settle transactions directly in stablecoins.
Ripple, Circle	Acquisition	According to Bloomberg, Ripple offered US$4B-US$5B to acquire stablecoin issuer Circle.
Baanx, Visa	Partnership	Baanx partnered with Visa to launch stablecoin payment cards tied to self-custodial wallets.
Visa, BVNK	Investment	Visa invested in BVNK, a startup focused on stablecoin-based payment infrastructure for businesses.
Stripe	Launch	Stripe launched stablecoin financial accounts to enable businesses to hold a balance in stablecoins and distribute them anywhere in the world.
StraitsX	Launch	StraitsX launched its Singapore dollar-pegged stablecoin, XSGD, on the XRP Ledger.
JPMorgan Chase, Bank of America, Citi, and Wells Fargo	Exploration	JPMorgan Chase, Bank of America, Citi, and Wells Fargo are weighing launching a joint stablecoin as per WSJ.
Circle	IPO	Circle Internet Group filed for an IPO on the New York Stock Exchange.
Stripe	Partnership	Stripe held early discussions with banks about integrating stablecoins into their core service.
Matera, Circle	Partnership	Matera partnered with Circle to accelerate the adoption of stablecoins as a mainstream payment method.
Stripe, Shopify	Partnership	Stripe partnered with Shopify to help Shopify merchants accept stablecoin payments.
OpenPayd, Circle	Partnership	OpenPayd partnered with Circle to deliver a unified fiat and stablecoin infrastructure layer for global businesses.
Highnote, BVNK	Partnership	Highnote partnered with BVNK to introduce real-time, 24/7 stablecoin-based funding for card programs.
Fiserv, PayPal	Partnership	Fiserv partnered with PayPal to build future interoperability between FIUSD and PYUSD.
Animoca Brands, Standard Chartered, and HKT	Partnership	Animoca Brands, Standard Chartered, and HKT formed a stablecoin joint venture called Anchorpoint to build a business model for the issuance of licensed stablecoins.
Ripple, Rail	Acquisition	Ripple announced plans to acquire Rail, a stablecoin payments platform, for US$200M.
KakaoBank	Exploration	KakaoBank announced plans to enter into the South Korean stablecoin sector.
Slash, Stripe	Partnership	Slash, a San Francisco-based neobank for businesses, launched a payments and treasury platform powered by a new U.S. dollar stablecoin issued by Stripe's Bridge.

Q3 2025 (Jul-Sep)	Visa, Paxos	Partnership	Visa is expanding its stablecoin settlement platform to include PayPal USD and Global Dollar through a partnership with Paxos. It also added Circle's euro token, EURC.
	Stable	Funding	Tether-focused blockchain Stable raised US$28M to power stablecoin payments.
	AllUnity	Launch	AllUnity, a joint venture between DWS, Galaxy and Flow Traders, has launched EURAU, a euro-denominated stablecoin approved under Germany's new crypto regulations.
	Ethena, Anchorage Digital	Partnership	Ethena partnered with Anchorage Digital to issue its US$1.5B stablecoin, USDtb, in the U.S. under the new stablecoin laws.
	Bank of America	Exploration	Bank of America revealed that it has been working on stablecoin development and expects to move forward.
	Citi	Exploration	Citigroup announced that it is exploring plans to launch its own stablecoin.
	Ant Group	Integration	Ant Group's international arm announced plans to integrate Circle's USDC stablecoin onto its proprietary blockchain.
	Ripple, OpenPayd	Partnership	Ripple partnered with OpenPayd to build a stablecoin and payments infrastructure for businesses.
	Banca Sella, Fireblocks	Partnership	Banca Sella conducted an internal trial of crypto custody services for a small group of employees in partnership with Fireblocks.
	Finastra, Circle	Partnership	Finastra announced plans to integrate Circle's USDC stablecoin into its payments hub, allowing banks to settle cross-border transfers with the token.
	SBI Group, Chainlink	Partnership	SBI Group teamed up with Chainlink to develop stablecoin solutions in Japan.
	Ripple and SBI Holdings	Partnership	Ripple and SBI Holdings plan to introduce Ripple USD (RLUSD) in Japan to capitalise on the country's evolving stablecoin market.
	Metamask	Launch	MetaMask announced plans to launch a proprietary stablecoin mUSD in partnership with Bridge (now part of Stripe) and stablecoin platform M0.
	Circle, Malachite	Acquisition	Circle acquired consensus engine Malachite from development firm Informal Systems to support its new stablecoin-focused blockchain Arc.
	SWIFT	Partnership	SWIFT, in collaboration with over 30 financial institutions and ConsenSys, is developing a shared blockchain-based digital ledger with an initial focus on real-time 24/7 cross-border payments.

Table 1.15:

Stablecoin Issuers Expanding into Payment Infrastructure

A. Circle Payments Network (CPN): Real-Time Cross-Border Settlements

Entities Involved:	Circle
Use Case Title:	Streamlining global money movement with stablecoins
Target Customers:	B2B (Financial Institutions, Payment Service Providers)
Use Case Description:	Circle's CPN connects financial institutions globally, enabling 24/7 real-time settlement using stablecoins like USDC and EURC. This network reduces inefficiencies in cross-border payments by eliminating bilateral agreements and settlement delays, offering a faster, more transparent alternative to traditional methods.
Value Proposition:	Enhances liquidity and reduces operational and compliance costs for financial institutions engaged in international transactions.
Future Outlook:	Expected to expand its network of partners, including support for more stablecoins, further simplifying the global payments infrastructure.

Source: Circle, 2025

B. Coinbase x402: Internet-Native Stablecoin Payments

Entities Involved:	Coinbase
Use Case Title:	Enabling instant stablecoin payments over HTTP
Target Customers:	B2B (Developers, API Providers, AI Agents)
Use Case Description:	Coinbase has introduced x402, a payment protocol that facilitates instant stablecoin payments directly over HTTP. This innovation allows APIs, applications, and AI agents to transact seamlessly, unlocking faster, automated internet economies without the need for traditional payment intermediaries.
Value Proposition:	Simplifies the integration of payment functionalities into web services, reducing complexity and enhancing user experience.
Future Outlook:	Potential to become a standard for web-based micropayments and automated transactions for agentic commerce.

Source: Coinbase Developer Documentation, 2025

Stablecoins and the Future of Payments: Voices from Industry Leaders

"We're not here to disrupt the dollar. USDC is an internet-native digital asset pegged to the U.S. dollar. It can settle near-instantly, is programmable by design, and moves globally without the friction associated with traditional banking. This is not about speculation, it's about building trusted infrastructure for global commerce."

Yam Ki Chan - Vice President, Asia Pacific, Circle

"We have three main areas of focus: stablecoin settlement between issuers and acquirers, stablecoin-linked cards that allow customers to spend directly from stablecoin wallets, and cross-border money movement using stablecoins, such as our partnership with Yellowcard in Africa. Through these pilots, we are expanding settlement hours, improving conversion in challenging currency corridors, and connecting digital wallets to Visa's global merchant network."

Ezechiel Copic - Director, Digital Currency Policy, Visa

"The Multi-Token Network is not a new global settlement system, but an orchestration layer across chains. Its purpose is to provide certainty, rules, and compliance standards for transactions involving stablecoins, tokenized deposits, or CBDCs. It's about building trust across multiple blockchains rather than replacing them."

Jesse McWaters - Executive Vice President, Head of Global Government Affairs, Mastercard

---

1.2.8 Global Alignment, Local Nuance: Stakeholder Perspectives on Regulatory Convergence

As stablecoins scale globally, the need for regulatory clarity and coordination across jurisdictions has become increasingly important. Yet full harmonisation may not be practical or even necessary. Stakeholders from industry and government agree that what matters most is alignment on core principles: reserve quality, redemption rights, licensing standards, and supervisory accountability.

"Harmonisation might not be the right word. In some areas, convergence or mutual recognition may be enough. Whether we need global harmonisation on digital assets — and what exactly that would entail — is still under discussion. What matters is achieving aligned outcomes without stifling innovation."

Tom Mutton - Director of Fintech, Bank of England

"With EMIR 3.0, we're seeing a progressive shift from national to European supervision. ESMA, EBA, and other central authorities are playing a growing role in harmonising practices. The move from directives to direct regulations reduces fragmentation and enables more consistent rule application across the E.U.."

Audrey Metzger - Director, Innovation and Financial Markets Infrastructures, Banque de France

"We do not need perfect harmonisation — that's never happened even in traditional finance. What we need is regulatory alignment. If jurisdictions can agree on principles — like transparency, capital reserves, and licensing standards — then companies like Ripple can build consistent infrastructure that meets those requirements flexibly."

Fiona Murray - Managing Director APAC, Ripple

"We operate in 22 regulated markets. But each one is different — different KYC rules, different custody standards, different trading disclosures. It's exhausting and expensive. What's needed is global regulatory harmonisation — a core set of rules that jurisdictions can adapt, rather than reinventing the wheel every time."

Richard Teng - CEO, Binance

1.3 The Next Phase of Digital Money

The evolution of digital money is moving from experimentation to systemic relevance. Stablecoins, tokenized deposits, and CBDCs are laying the foundations for a programmable monetary layer that could redefine global finance. As adoption accelerates, the distinction between "crypto" and "mainstream finance" will blur, with stablecoins embedded in merchant payments, CBDCs powering interbank settlements, and tokenized deposits underpinning corporate treasury operations. Regulators face the challenge of balancing innovation with monetary stability, especially as stablecoins begin to influence foreign exchange dynamics and challenge the autonomy of national monetary policy. For banks and payment institutions, the opportunity lies in harnessing programmability, which enables conditional transfers, event-driven logic, and real-time settlements. Globally, competitive dynamics are emerging. Jurisdictions that establish clear, interoperable regimes could position themselves as hubs for digital money issuance and adoption. Over the next five years, the convergence of private and public forms of digital money may reshape not only payment systems but also the structure of capital markets, driving toward a more integrated, efficient, and inclusive financial ecosystem.

2 Tokenization of Real-World Assets

2.1 Introduction

Asset tokenization refers to the issuance or representation of assets in the form of digital tokens using technologies such as distributed ledgers, as defined by the FSB. It involves converting rights to an asset class, such as a bond, equity, real estate, or commodities, into a digital token recorded on a blockchain. These tokens represent ownership or claim on the underlying asset and can be held, transferred, or traded much like traditional securities or records of title. Tokenization is increasingly moving from proof-of-concept to production, spanning a wide range of use cases across both regulated capital markets (e.g. tokenized treasury funds and bonds) and non-capital market domains, such as private credit, supply chain financing, real estate, art, and even carbon credits. As such, tokenization is emerging as a foundational infrastructure layer for the future of digital ownership, liquidity, and programmable finance across the broader financial and real economy.

Industry Perspectives on the Future Potential of Tokenization

> "We see tremendous potential in RWA tokenization, especially for treasury operations. Real-time settlement, increased liquidity, and programmatic governance are game-changers. But legal frameworks, standardisation, and tech rails still need to evolve before RWAs can move from pilots to scale."

Richard Teng - CEO, Binance

> "Our digital assets journey began in 2016, and we have made significant progress since then, having launched our enterprise blockchain and built in-house expertise. For example, Global Transaction Banking focused on conditional payments and improving payment capabilities and Global Markets launched an asset tokenization platform, availing bespoke tokenized bonds to corporate accredited investors. We are scaling up the tokenization capabilities across geographies and asset classes. Today, we are also working towards future-proofing our core capabilities through a group-wide digital assets strategy."

Park Kwan Hoon - Executive Director, Group Strategic Planning Office, OCBC

> "We see this as the third wave of disruption in financial infrastructure. The first was RTGS systems in the 1980s, the second was instant payment rails like Pix starting in 2010, and now the third is blockchain settlement systems. With programmability, atomic settlement, and composability, these new rails are not just about efficiency — they are about rewiring financial markets for the next generation."

Bruno Batavia - Principal & Director of Emerging Tech, Valor Capital

As described in the previous chapter, the tokenization of money, such as stablecoins or tokenized deposits, primarily serves as a medium of exchange or store of value within blockchain-based financial systems. In contrast, tokenization represents more than a digital wrapper—it signals the emergence of programmable financial infrastructure. Market participants increasingly view tokenization as a path to frictionless issuance, continuous settlement, and automated compliance. Firms like Mastercard and Binance see potential in unlocking entirely new models, such as fractionalized sovereign debt, real-time treasury operations, and programmable yield instruments. However, this promise depends on parallel evolution in legal frameworks, infrastructure standards, and cross-border interoperability. According to projections from Standard Chartered and Synpulse, the global tokenized asset market could scale to US$30 trillion[33] by 2034, underscoring its systemic significance.

[33] Standard Chartered, 2024

2.1.1 Evolution of Asset Tokenization

The timeline below charts the pivotal moments shaping the evolution of asset tokenization, from early innovations in financial structuring to the emergence of blockchain-based models. Beginning with the launch of ETFs in 1990, which introduced fractionalized, tradable exposure to traditional assets, the journey accelerated with the conceptualisation of smart contracts in 1994 and the launch of Bitcoin in 2009, marking the advent of programmable digital value.

The introduction of Ethereum in 2015 enabled token standards such as ERC-20, establishing the technical rails for asset tokenization at scale. Institutional momentum has grown steadily since 2018, with landmark projects such as the tokenization of real estate, the launch of tokenized funds by asset managers like BlackRock, and regulatory pilots including MAS's Project Guardian. As of 2025, tokenized assets are entering mainstream institutional portfolios, cross-border settlement frameworks are being tested by central banks, and regulated trading of digital securities is moving from pilot to production in key jurisdictions. Together, these milestones signal a structural shift toward programmable finance and digitally-native capital markets.

Table 2.1:

Milestones in the Evolution of Asset Tokenization

Year	Milestone	Description
1990	Introduction of ETFs	The Toronto 35 Index Participation Fund (TIP) launched on the Toronto Stock Exchange.
1994	Concept of Smart Contracts	Nick Szabo introduced the idea of self-executing contracts, foundational for blockchain applications.
2009	Emergence of Bitcoin	Marked the beginning of blockchain technology and digital assets.
2015	Ethereum and Smart Contracts	Ethereum launched, enabling token standards like ERC-20, catalysing tokenization.
2018	Tokenization of Aspen St. Regis Resort	First major digital tokenization of a commercial real estate asset.
2022	MAS Project Guardian	Singapore's MAS launched Project Guardian to explore tokenization of financial assets with industry partners.
2023	BlackRock's Tokenized Fund	Launch of BUIDL Fund on Ethereum.
2024	MAS's Project Guardian Expansion	MAS expanded Project Guardian to include tokenized securities pilots.
2024	MAS Global Layer 1 (GL1) Initiative	MAS introduced the Global Layer 1 (GL1), proposing a public-private infrastructure to create an interoperable and unified settlement layer for digital assets.
2024	MUFG Tokenizes Osaka Skyscraper	MUFG launched a blockchain-based tokenization of a ¥100 billion (US$681M) Osaka skyscraper.

Sources: Investopedia, accessed Sep 2025; Satoshi Nakamoto Institute, accessed Sep 2025; Bitcoin Whitepaper, 2008; Ethereum, accessed Sep 2025; Venture Beat, 2018; Securitize, 2024; Project Guardian launch, 2022; Global Layer 1, 2024; Project Guardian Expansion, 2024; MUFG Real Estate, 2025

2.1.2 Anatomy of Tokenized Assets

RWA tokenization has the potential to expand a comprehensive range of asset types, beyond traditional financial instruments to include real assets, intangible rights, and emerging alternative categories. The framework below categorises RWAs into five broad buckets: financial instruments, receivables and cash flows, real assets, intangible assets, and alternative/emerging asset classes.

This diversity reflects the growing maturity of tokenization infrastructure and the increasing legal clarity across jurisdictions are encouraging signs that bode well for broader adoption, as more markets move toward enabling efficient, transparent, and programmable asset exposure.

Figure 2.1:

Emerging Landscape of Real-World Asset Tokenization - Illustrative Asset Class Categories

Note: This table outlines the broad potential of RWA tokenization. Some categories already have live examples in the market, while others represent emerging or future possibilities as infrastructure, legal clarity, and market demand evolve.

Source: GFTN Analysis

Table 2.2 highlights representative use cases across key tokenized asset classes, showcasing how tokenization is being applied to enable programmable finance, fractional ownership, and enhanced collateral utility across a range of asset classes. Real-world deployments, ranging from tokenized government bonds and commercial real estate to small and medium enterprise (SME) credit pools and structured products, demonstrate both the breadth of application and growing institutional engagement across geographies.

"Tokenization is not a fringe experiment. It is about integrating distributed ledger technology into traditional finance. Our digital asset platform was designed to manage the lifecycle of this process, including tokenized bonds, money market funds, and other instruments. Over the next three to five years, we expect these products to become integrated into capital markets in a seamless way so clients may no longer need to distinguish between a 'blockchain product' and a traditional one."

Lee Brenner - Head of Public Policy, Digital Assets, Goldman Sachs

Table 2.2:

Representative Use Cases of Tokenized Asset Classes

(Ordered by Asset Liquidity, from Most Liquid to Least Liquid)

Asset Class	Tokenization Use Case	Notable Examples
Treasuries & Funds	Tokenized MMFs and T-Bills used as on-chain collateral.	BlackRock USD Institutional Digital Liquidity Fund (BUIDL), Franklin Templeton OnChain U.S. Government Money Fund (FOBXX), Fidelity Digital Interest Token (FDIT) have raised over US$3B in AUM.
Sovereign Bonds	Programmable coupon payments, real-time distribution.	HKMA has issued two batches of tokenized green bonds worth HK$6.8B. HKMA also plans to regularise the issuance of tokenized Government bonds in 2025.
Structured Products	Custom risk-return exposure delivered via programmable tokens.	DBS is tokenizing structured notes on the Ethereum public blockchain.
Equity & Debt	Equity fundraising, tokenized convertibles.	Taurus & CMTA live deals in Switzerland include tokenized share issuances by firms such as the Audacia Group, QoQa Brew, and CODE41.
Private Credit	Collateralized SME loans, tokenized real-world credit pools.	Maple Finance, Centrifuge: Tokenized credit pools for SME lending and structured private debt funding.
Commercial Real Estate	Fractional ownership, democratised investing.	MUFG, has acquired a high-rise office building in Osaka valued at over ¥100 billion (approximately US$681M) and plans to tokenize the property using its Progmat platform.

Sources: Financial Times, 2025; HKMA Green Bonds, 2025; HKMA Government Bonds, 2025; DBS, 2025; Taurus, 2022; Maple, 2024; and Portalcripto, 2025

2.2 Technology Foundations and Token Standards in the Tokenization Lifecycle

2.2.1 Building Blocks of Tokenization Infrastructure

The architecture of tokenized systems is composed of multiple interlocking layers that define how assets are represented, governed, and transacted. Each layer is functionally distinct but must integrate securely and seamlessly with the others. The choice of architecture—modular vs. integrated will dictate the degree of customisation, scalability, and regulatory control possible for different financial use cases.

Table 2.3:

Tokenization Tech Stack Overview

Layer	Functional Role
Application Layer	Interfaces for end-users such as custodial wallets, trading dashboards, and marketplaces.

Smart Contract Layer	Encodes business logic, lifecycle events, asset servicing, and compliance automation.
Protocol/ Middleware Layer	Token standardisation (e.g. ERC-20, ERC-1400), lifecycle orchestration, interoperability bridges.
Ledger Layer (DLT)	Distributed ledger platforms where tokens reside and transactions are recorded. (e.g. Ethereum, Hyperledger Fabric, Corda, Avalanche, Solana).

Sources: BCG, 2025; Ripple, 2025; Ethereum, accessed Sep 2025; LCX, 2024; Federal Reserve, 2024

2.2.2 Technology Models and Deployment Approaches

The choice of **ledger architecture** plays a critical role in determining how tokenized assets, such as those outlined in the previous section, are issued, held, and transacted. As tokenization use cases evolve across asset classes, institutions must align technical infrastructure with regulatory and operational needs.

- **Public permissionless blockchains** (e.g. Ethereum, Solana, Avalanche) offer openness, programmability, and composability with the broader Web3 ecosystem. These networks support a wide range of smart contracts and decentralized applications, making them attractive for innovation. However, they also raise important concerns around transaction privacy, legal finality, and compliance assurance, which are increasingly under the scrutiny of financial regulators.
- In contrast, **private permissioned networks** (e.g. Hyperledger Fabric, R3 Corda) are favoured by many regulated institutions. These networks allow controlled participation, customisable privacy settings, and greater scalability, making them more suitable for enterprise-grade deployments.

The divide between public and private blockchains is increasingly blurring, with institutions leveraging hybrid architectures to balance composability with compliance. Platforms such as Cardano have demonstrated on-chain transparency by anchoring their entire balance sheets to public networks, while players like Paxos emphasise regulated issuance on permissioned rails. Crypto-native institutions argue that tokenization must go beyond pilots and instead activate full-stack utility, including on-chain custody, cash leg settlement, collateralization, and programmability, if it is to truly transform capital markets. These hybrid models are also gaining traction as regulators seek architectures that balance open access and interoperability with compliance, control, and governance.

"Our code powers real tokenized assets — not just test cases or proofs of concept. Japan's clearing house is issuing commodities such as rubber on Besu. Brazil's Drex has transformed its blockchain landscape from supply chain to finance. The RBI's CBDC is built on Hyperledger Fabric. These are in production. Our tech isn't theoretical — it's operating the rails of tokenized finance today."

Karen Ottoni - Sr. Director of Ecosystem & Strategic Initiatives, Linux Foundation Decentralized Trust

2.2.3 Interoperability and Programmability

Token standards play a critical role in enabling interoperability by ensuring consistency in how digital assets are created, transferred, and managed across different blockchain platforms and applications. Key standards include:

Table 2.4:

Key Token Standards for Interoperable and Programmable Digital Assets

Token Standard	Blockchain	Use Cases	Feature Highlights
ERC-20	Ethereum	Fungible tokens (e.g. cash equivalents, bonds)	Transferable, fungible, supports approval and burn operations.
ERC-721	Ethereum	Non-fungible assets (e.g. art, collectables)	Unique asset representation with individual ownership.

ERC-1400	Ethereum	Security tokens, regulated instruments	Partitioned ownership, compliance checks, and modular design.
FA2	Tezos	Multi-asset support (fungible, NFTs, and hybrids)	Unified standard, composable and extensible framework.
XRC-20 (not "XDC Token Standard")	XinFin Network	RWAs, trade finance tokens	EVM-compatible, hybrid deployment, supports smart contract logic.

Sources: Ethereum ERC 20, Ethereum ERC 721, Polymath, XDC, and Chainlink, accessed Sep 2025

2.2.4 The Tokenization Process

Tokenization is a structured process that transforms ownership rights of real-world or financial assets into programmable, transferable digital representations on blockchain. This process spans multiple operational and legal stages, each designed to preserve the enforceability of rights while enabling digital efficiency.

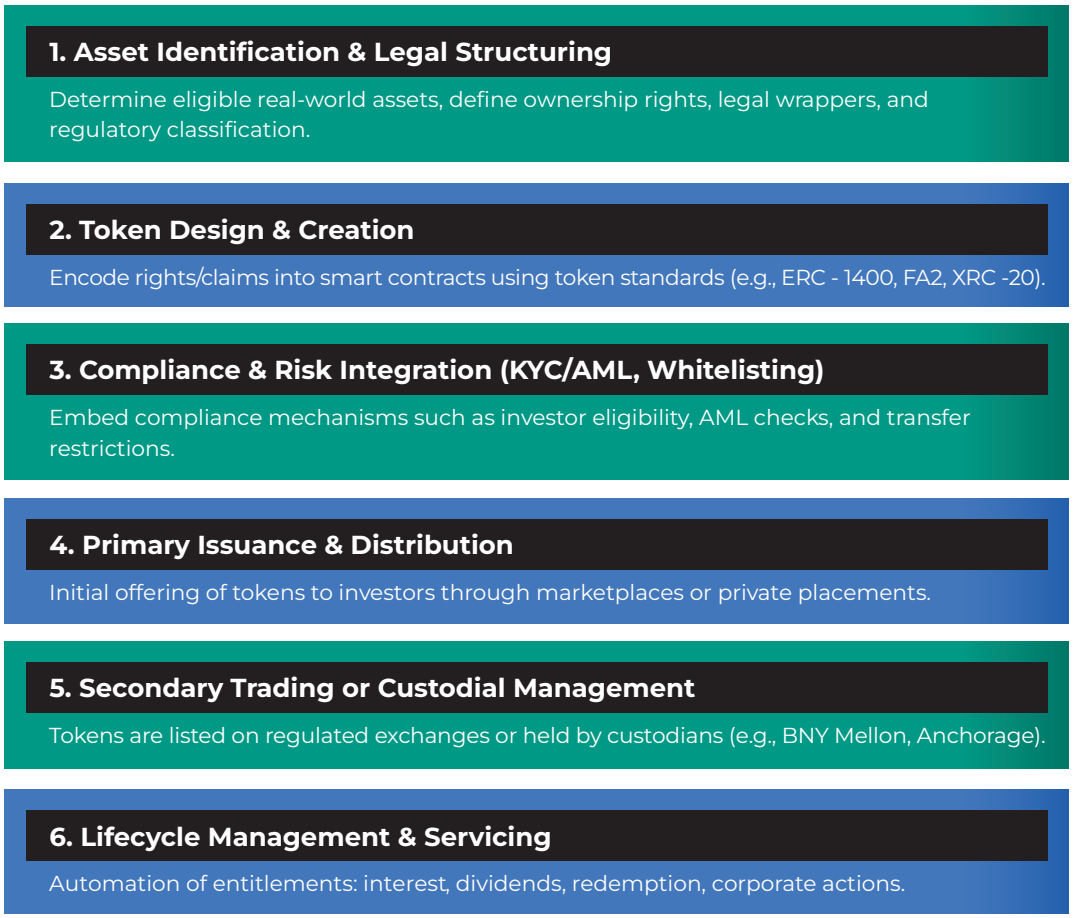
> "There is a lot of discussion around tokenization of real-world assets, but in practice, legal structures like residential property deeds do not support fractionalization. In contrast, we see more concrete use cases in financial instruments — like repo or investment funds — where tokenization could reduce friction and improve settlement."

Tom Mutton - Director of Fintech, Bank of England

The lifecycle begins well before any token is minted. It involves legal analysis, technology configuration, compliance integration, and post-issuance governance. The following flowchart provides a high-level overview of this lifecycle.

Figure 2.2:

Tokenization Value Chain



Source: GFTN Analysis

The tokenization process can take different forms depending on how the asset is represented and enforced, with each of these models existing along a continuum:

Table 2.5:

Continuum of Tokenization Models

Model	Legal Basis of Ownership	Value Transfer Mechanism	Token Role	Examples
Traditional Fractionalization	Off-chain contracts or certificates	Manual off-chain recordkeeping	Informational only; not legally binding	Real estate REITs using share certificates; art co-ownership agreements
On-Chain Representation	Off-chain legal agreements (mirrored on-chain)	Legal ownership updated off-chain	Token represents economic interest	Tokenized Treasuries via private blockchains (e.g. Franklin Templeton)
On-Chain Integration	Off-chain contracts referencing tokenized assets	Hybrid (on-chain token and legal registry update)	Token is partially enforceable	Digital bonds with automated settlement (e.g. Euroclear's DLT pilot)
On-Chain Enforcement	Token is the legal record of ownership	Fully digital settlement	Token is the authoritative legal record	Smart legal contracts on DLT; tokenized equity with full legal standing
Fully On-Chain	Native digital asset with embedded legal and functional logic	Fully digital; native blockchain transfer	Token operates autonomously (DeFi-like logic)	Stablecoins or DeFi tokens (e.g. DAI, AAVE); fully decentralized NFTs

Sources: BIS, 2023; Federal Reserve, 2023; Kaleido, 2025

2.3 The Regulatory Landscape of Tokenization

Tokenization, while technologically transformative, exists within a legal and regulatory environment that remains highly fragmented. For regulators and financial institutions, the challenge is twofold: to enable innovation without compromising the integrity of financial systems, and to do so in a manner that accommodates diverse legal traditions and market structures. The four pillars of effective token regulation include:

1. **Personal Property Rights:** Tokens must be legally recognised as assets that confer enforceable ownership rights.
2. **Cross-Border Compliance:** Legal recognition and rights associated with a token should be preserved across jurisdictions.
3. **Enforcement Clarity:** Stakeholders need access to legal remedies, including in cases of fraud or smart contract malfunction.
4. **Jurisdictional Certainty:** Blockchain requires rules on which jurisdiction's law applies, especially when transactions span borders.

GFTN Survey Insights: Asset Tokenization

Survey Insight 2.1

Regulatory Attention on Tokenization Platforms

31%

Tokenization platforms were identified by 31% of respondents as requiring the most regulatory attention in their jurisdiction, on par with stablecoin issuers and just behind centralized exchanges.

Survey Insight 2.2

Tokenization as a Capital Markets Efficiency Driver

56%

Capital market efficiencies via tokenization were identified by 56% of respondents as the biggest opportunity for digital assets over the next three years. This highlights strong industry optimism about tokenization's potential to streamline issuance, settlement, and asset servicing processes, particularly for traditional instruments like bonds, funds, and private assets.

2.3.1 Regulatory Maturity and Framework Development Across Jurisdictions

The rapid expansion of tokenization is increasingly being shaped by regulatory oversight. Authorities across major jurisdictions are moving from pilot discussions to concrete actions, ranging from registrations and approvals to warnings and exploratory initiatives. Table 2.6 captures some of the recent regulatory initiatives that illustrate this shift.

Table 2.6:

Tokenization: Regulatory Initiatives

Quarter	Entities	Geography	Activity	Product	Description
Q1 2025 (Jan-Mar)	**Fidelity Investments, SEC**	U.S.	Registration	Treasury	Asset manager Fidelity Investments has filed paperwork to register a blockchain-based, tokenized version of its U.S. dollar money market fund, aiming to join the tokenized asset race.
	Dubai Land Department	U.A.E.	Launch	Real estate	DLD began a pilot for real estate tokenization, using blockchain technology for property title deeds.
Q2 2025 (Apr-Jun)	**Coinbase**	U.S.	Approval	Stocks	Coinbase is seeking approval from the U.S. SEC to launch tokenized stock trading.
	BPX Exchange, FCA	U.S.	Registration	RWA	Tokenization platform, the BPX Exchange, was added to the U.K.'s crypto register, the first new addition since April and only the third this year, according to the FCA.
	Robinhood	U.S.	Registration	RWA	Robinhood has formally submitted a regulatory proposal to the U.S. SEC seeking the creation of a federal framework for the tokenization of real-world assets.
	VARA, DLD	U.S.	Warning	Real estate	Dubai's crypto regulator has issued an alert, warning of firms falsely claiming to be part of the city's high-profile real estate tokenization pilot, saying that such

					misrepresentation may violate the emirate's virtual asset laws.
Q3 2025 (Jul-Sep)	**The Reserve Bank of Australia**	Australia	Explore	RWA	RBA announced plans to explore the development of wholesale tokenized asset markets alongside an array of industry participants.

Table 2.7: Regulatory Approaches to Tokenization

Asset Tokenization Regulatory Comparison

Jurisdiction	Regulatory Status	Key Framework(s)
U.S.	Development / In Progress	SEC and CFTC evolving guidance on tokenized securities.
E.U.	In Force	MiCA; DLT Pilot Regime under MiFID II.
Japan	Development / In Progress	FSA Security Token Offering guidelines.
India	Development / In Progress	IFSCA Real-World Asset Tokenization paper.
U.K.	Development / In Progress	FCA DP23/2; PRA Clarification Letter (Nov 2023)
Brazil	Development / In Progress	Brazil Crypto Law (Law No. 14,478/2022)
Switzerland	In Force	DLT Act (Aug 2021), FINMA token types & licensing guidance.
Singapore	Advanced / Active Pilots	Project Guardian, Global Layer One (GL1).
U.A.E.	Advanced / Active Pilots	ADGM Tokenization Framework; VARA Regulations.
Hong Kong	Advanced / Active Pilots	SFC-HKMA tokenized securities framework (June 2023).
Qatar	Development / In Progress	QFC Digital Assets Framework.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

The evolution of tokenization regulation across major jurisdictions reveals a varied yet increasingly harmonised global landscape. In the European Union, regulation is now in force under the Markets in Crypto Assets Regulation (MiCA), supplemented by the DLT Pilot Regime under the MiFID II. This framework establishes a comprehensive and binding legal basis for tokenized financial instruments and market infrastructures, making the E.U. one of the first jurisdictions to offer full legal certainty for the use of distributed ledger technology in capital markets.

Singapore has similarly established itself as a leader in tokenization regulation through the MAS Project Guardian initiative. Singapore's role is evolving from a pilot hub to an institutional tokenization platform. Local banks like DBS and OCBC are advancing from tokenized bonds to more scalable instruments such as tokenized ETFs, certificates of deposit, and commercial papers, offering structured entry points for regulated adoption. Singapore's regulatory regime is considered highly advanced and interoperable, actively engaging in real-world pilots with major financial institutions to test tokenization use cases across fixed income, foreign exchange, and fund distribution.

"Tokenization of financial markets and real-world assets can enhance efficiency, enable fractional ownership, and reduce costs by minimising intermediaries. These benefits support a more efficient financial system overall. MAS does not pick winners in terms of assets or tokens – this should be driven by the industry. However, if there is industry demand for tokens with inherently higher risk, then MAS will investigate the reason for it."

Rosemary Lim - Executive Director, Payments Department, Monetary Authority of Singapore

Switzerland, another forerunner, enforces its own DLT Act passed in 2021, alongside granular guidance from the Swiss FINMA on token classification, licensing, and custody obligations.

"We have the legal framework, and we've seen proof-of-concept projects such as NFTs of Picasso, tokenized sneakers, and luxury cars. But none of these gained huge market adoption. Institutional investors, like pension funds, demand deep due diligence and professional structures. It's difficult for startups to meet those standards, particularly in markets like real estate where access and relationships matter."

Matthias Obrecht - Head, Market Analysis, FINMA

In contrast, countries like Brazil and India remain in the developmental stages. Brazil's framework is grounded in the Crypto Law No. 14.478/2022, but further guidance for tokenized securities is still under development. India is engaged in a consultation phase via the IFSCA's paper on RWA tokenization, aiming to integrate tokenization within GIFT City's regulatory sandbox.

Meanwhile, the United Kingdom, the United States, Japan, and Hong Kong offer a mixed bag of regulatory clarity. The U.K. is still in the consultation phase, with frameworks such as the FCA's DP23/2 and the PRA's November 2023 clarification letter offering high-level policy direction but lacking enforceable detail. Historically, the U.S. regulatory regime for tokenized assets has been shaped by overlapping guidance and enforcement from agencies like the SEC and CFTC. The CLARITY Act of 2025[34] marks a significant step toward establishing a unified regulatory framework. The Act introduces a formal classification system for digital assets, notably defining a "digital commodity" as a token whose value is derived from the use of its associated blockchain network. This category excludes securities, derivatives, payment stablecoins, and tokenized real-world assets, which remain under the oversight of other regulatory bodies. The Act also clarifies that digital collectables and representations of physical goods fall outside the scope of both securities and commodities regulation. However, as of writing in September 2025, the CLARITY Act has only passed the House and is still awaiting Senate approval before it becomes law. Until then, regulatory uncertainty continues in areas such as asset classification, decentralization thresholds, and agency jurisdiction. Hong Kong has implemented an active licensing regime based on its tokenized securities framework introduced in June 2023, while Japan continues to build upon its FSA Security Token Offering guidelines.

Taken together, these examples highlight that while the pace of regulatory maturity differs, jurisdictions are increasingly converging on shared pillars such as issuer licensing, investor protection, and asset segregation. Bringing these strands together, the emerging pattern is one of gradual harmonisation, echoing the earlier point on a global landscape moving toward interoperability.

2.3.2 Legal Classification and Token Types

Jurisdictions vary significantly in how they legally classify tokenized assets, though common themes are beginning to emerge. In the European Union, tokenized assets are legally recognised either as financial instruments or as e-money, depending on their structure and function, under the provisions of MiFID and MiCA. This dual classification allows for a flexible yet comprehensive regulatory treatment of tokenized assets.

"The tokenization of financial assets, equities, debt, funds, derivatives is where the real potential lies. If this scales, the traditional crypto market will be dwarfed. But we'll need three things: central bank money on the ledger, regulatory adaptation to support tokenized activity, and acceptance of tokenized assets as collateral. These conditions are beginning to emerge."

Peter Kerstens - Advisor for Financial Sector Digitalisation and Cybersecurity, European Commission

[34] Clarity Act Overview, 2025

Singapore has taken a more pragmatic route by treating tokenized assets under its existing securities laws. MAS has clarified that tokenized assets, especially when backed by RWAs or structured as investment products, fall under the jurisdiction of the SFA. Japan also applies its FIEA to security tokens, ensuring that tokenized instruments are subject to the same safeguards as traditional securities.

In the U.S., the proposed CLARITY Act 2025 seeks to bring greater certainty by introducing a classification framework for digital assets, distinguishing between securities (under SEC), commodities (under CFTC), and stablecoins (under separate frameworks like the GENIUS Act).

While the Act does not provide specific rules for tokenized RWAs, it could influence how such assets are regulated. For instance, tokenized equities may fall under SEC oversight, whereas tokens backed by physical commodities could be regulated by the CFTC. As of September 2025, the CLARITY Act has yet to pass the Senate, and thus does not currently have legal effect.

The United Kingdom has not fully resolved its classification framework either. Depending on the use case, tokenized assets may be classified as securities or units in a collective investment scheme. Such functional classification leaves room for regulatory discretion, but may hinder institutional confidence in launching tokenization projects.

Other jurisdictions, such as the U.A.E. and Switzerland, have developed token-specific taxonomies. The U.A.E., through ADGM and DIFC, has defined security tokens within its DLT Guidance. Switzerland provides one of the most refined classifications, distinguishing between payment tokens, asset tokens, and utility tokens, each with tailored compliance and disclosure requirements.

Despite differences in terminology and scope, the global trend indicates increasing acceptance of tokenized assets as valid legal instruments, subject to appropriate financial regulation and consumer protection standards.

Table 2.8: Legal Classification of Tokenized Financial Assets by Jurisdiction

Financial Asset Tokenization Legal Classification & Token Types

Jurisdiction	Are Tokenized Financial Assets Recognised in Law?	Legal Classification
U.S.	In progress	The proposed CLARITY Act of 2025 aims to introduce a classification framework, distinguishing securities (regulated by the SEC) from commodities (regulated by the CFTC).
E.U.	Yes	Financial instruments or e-money under MiFiD/MiCA.
Japan	Yes	Regulated under Financial Instruments and Exchange Act.
India	Not yet	No legal framework currently exists for tokenized financial or real-world assets.
U.K.	Partially (depends on use case)	Likely securities or units in collective investment schemes.
Brazil	Yes	CVM classifies tokenized assets as securities.
Switzerland	Yes	Payment, asset, and utility tokens per FINMA.
Singapore	Yes	MAS treats tokenized assets under existing securities law.
U.A.E.	Yes	Security tokens under DLT Guidance (ADGM, DIFC)
Hong Kong	Yes	Regulated as securities.
Qatar	In progress	Expected to follow FATF-aligned classification.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

Note: This table specifically refers to the legal treatment of tokenized financial assets, such as tokenized securities, bonds, and funds. Jurisdictions may have different classifications for other token types, such as payment tokens, utility tokens, or asset-backed tokens (e.g. real estate, commodities).

2.3.3 Issuance, Licensing, and Regulatory Supervision

The licensing requirements for issuing tokenized assets are becoming increasingly formalised, with regulators seeking to impose conventional capital market standards on digital issuers. Within the European Union, only licensed EMI, MiFID-authorised firms, or credit institutions are permitted to issue or distribute tokenized instruments. National competent authorities are responsible for supervision, creating a harmonised yet locally administered regime.

Singapore allows issuance by regulated banks, fund managers, and insurers, with the MAS overseeing compliance under the SFA. The country's emphasis on institutional-grade participation ensures that tokenized products meet the high standards required for mainstream financial integration.

In the United States, issuance typically requires registration or exemption under SEC rules, with broker-dealers and ATS platforms forming the backbone of tokenized asset distribution. The lack of a unified framework, however, continues to be a challenge.

The U.K. permits only FCA- or PRA-regulated firms to issue tokenized assets, but ongoing consultations suggest this scope may expand in the future. In Hong Kong, only SFC-licensed brokers and intermediaries may issue tokenized securities, ensuring that only vetted entities enter the market.

Japan follows a similarly conservative approach, allowing only securities firms and financial institutions to issue such instruments. Meanwhile, Brazil and India have proposed mechanisms for licensing under the CVM and RBI, respectively, though implementation remains in early stages. Qatar, Saudi Arabia, and the U.A.E. permit issuance through regulated entities licensed under QFCRA, SAMA, and VARA or ADGM.

The global consensus is clearly shifting toward a model in which the issuance of tokenized assets is a regulated activity, with licensed financial entities playing a central role in maintaining market integrity.

Table 2.9: Issuance, Licensing, and Supervision

Asset Tokenization Issuance Licensing & Supervision

Jurisdiction	Who Can Issue/Tokenize Assets?	Regulatory Supervision
U.S.	SEC-licensed firms, broker-dealers	SEC, CFTC
E.U.	Licensed EMIs, credit instituitions, MiFID firms	National competent authorities
Japan	Securities firms and financial instituitions	FSA
India	Entities licensed under IFSCA GIFT City framework (proposed)	RBI
U.K.	FCA/PRA-regulated firms	FCA & Bank of England
Brazil	CVM and Central Bank-regulated entitites	CVM
Switzerland	FINMA-licensed DLT trading venues & custodians	FINMA
Singapore	Regulated banks, fund managers, insurers	MAS
U.A.E.	VARA/ADGM/DIFC licensed entities	Vistual Assets Regulations & FSRA
Hong Kong	SFC licensed brokers and intermediaries	SFC & HKMA
Qatar	QFC-licensed virtual asset service providers	QFCRA

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

2.3.4 Safeguarding Requirements and Custodial Mandates

The safeguarding of tokenized assets remains a key concern, especially in the context of investor protection and institutional participation. In the E.U., MiCA permits optional custody if tokenized assets are maintained on a separate DLT infrastructure, while the DLT Pilot Regime imposes segregation rules for financial instruments. Switzerland goes further, requiring that all tokenized assets be segregated under FINMA's guidelines.

In Singapore, licensed entities must comply with custodial requirements under the SFA. Japan mandates segregation under the FIEA, ensuring that client assets are not commingled. Similarly, the United States enforces segregation via the SEC Custody Rule, especially when tokens are held by broker-dealers or ATSs.

Hong Kong requires that all tokenized assets be held in trust by regulated custodians. The U.A.E. mandates that custody firms be separately licensed, and Brazil requires custody compliance under CVM's rules. The U.K. has yet to finalise its rules but recommends alignment with CIS custody practices. Qatar and Saudi Arabia remain in early development stages, with custody practices being tested in regulatory sandboxes.

While technical custody (e.g. private key storage) remains a unique challenge for digital assets, regulators are primarily focused on ensuring legal clarity, insolvency protection, and clear delineation of client ownership rights.

Table 2.10: Safeguarding and Reserve Requirements

Asset Tokenization Safeguarding & Reserve Requirements

Jurisdiction	Assets Segregation/Custody Mandate	Reserve Rules
U.S.	Yes (segregation under SEC Custody Rule)	Required by broker-dealer or ATS operator.
E.U.	Yes (under DLT Pilot Regime)	Custody optional under MiCA if separate DLT layer used.
Japan	Yes	FIEA mandates segregation.
U.K.	Pending detailed rules	Suggested alignment with existing CIS custody norms.
Brazil	Yes	Custody rules under CVM.
Switzerland	Yes, FINMA mandates custody for assets tokens	Assets token segregation required.
Singapore	Yes	Custody covered under licensing under SFA.
U.A.E.	Yes	Custody firms must be licensed separately.
Hong Kong	Yes (regulated custodians required)	Must hold client assets in trust.
Qatar	Pending	Expected to align with global custody norms.

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

2.3.5 Regulatory Sandboxes to Enable Tokenization Innovation

As tokenization use cases and adoption expand, regulatory sandboxes have emerged as key enablers of innovation. These controlled environments allow firms to test tokenized financial instruments and infrastructures under regulatory oversight. Sandboxes help regulators assess operational risks and refine supervisory frameworks. Leading examples include:

- **United Kingdom's DSS:** Launched by the FCA and Bank of England, the DSS provides a temporary legal framework for testing tokenized instruments with market infrastructure functionality, such as issuance, clearing, and settlement.
- **Singapore's Project Guardian and MAS Sandbox Plus:** These initiatives explore tokenized bonds, fund distributions, and cross-border FX settlement. They have enabled collaboration between global institutions like DBS, JP Morgan, and Standard Chartered under MAS oversight.

- **U.A.E.'s ADGM and DIFC - ITL:** These sandboxes support regulated trials of tokenized investment vehicles, enabling legal certainty around smart contract enforceability and digital custodianship.
- **European Blockchain Sandbox:** Backed by the E.U. Commission, this initiative facilitates cross-border tokenization use cases under supervisory coordination, including pilot trials involving digital identity and digital bonds.

Critically, these environments also function as **regulatory dialogue mechanisms**, helping authorities understand emerging risks, such as smart contract vulnerabilities, cross-chain transferability, and identity management in a low-risk context. Moreover, they create a feedback loop for refining taxonomy, licensing criteria, and legal interpretations before formal rulemaking.

"Our programmable payments sandbox brings together banks, e-money providers, exchanges, and tech firms. Participants are progressing from initial design stage to pilot products, demonstrating how tokenized finance can evolve under regulatory oversight."

Pucktada Treeratpituk - Director of Payment Systems and Fintech Policy, Bank of Thailand

2.4 Applications and Impacts of Tokenization on the Financial Industry

Asset tokenization represents a systemic shift in how financial products are issued, traded, and managed. As programmable ledgers redefine asset ownership and value exchange, tokenization is poised to transform the financial ecosystem by optimising operational frameworks, improving asset access, and enabling more resilient market structures.

2.4.1 Sector-Wise Application Matrix

Tokenization has been piloted and deployed across numerous sectors. The following table captures high-level sectoral use cases:

Table 2.11:

Sector-Wise Applications and Impacts of Tokenization

A. Traditional Finance Use Cases			
Sector	**Tokenization Use Cases**	**Key Impacts**	**Notable Examples**
Treasuries	Tokenized government bonds and treasury bills.	Real-time settlement, increased accessibility, and operational efficiency.	BlackRock's BUIDL Fund on Ethereum
Equities	Tokenized shares of private and public companies.	Broadened investor base, 24/7 trading, and programmable dividends.	Securitize and tZERO
Private Credit	Tokenized SME loans and private debt instruments.	Enhanced access to capital for SMEs, improved transparency, and faster settlement.	Maple Finance and Centrifuge
Commodities	Tokenization of gold, oil, and agricultural products.	Simplified trading, improved traceability, and fractional investment opportunities.	Tether Gold (XAUT) and Justoken
Real Estate	Fractional ownership of residential and commercial properties.	Increased liquidity, reduced entry barriers, and global investor access.	Aspen Digital tokenized the St. Regis Aspen Resort
Insurance	Tokenized insurance policies and automated claim processing.	Faster settlements, reduced administrative costs, and enhanced customer experience.	Etherisc and Nexus Mutual

B. Non-Financial / Alternative Use Cases

Sector	Tokenization Use Cases	Key Impacts	Notable Examples
Carbon Credits	Tokenized carbon offset credits.	Enhanced transparency, easier trading, and support for environmental initiatives.	Toucan Protocol and KlimaDAO
Healthcare	Tokenized patient records and pharmaceutical supply chains.	Enhanced data security, improved interoperability, and efficient tracking of medical products.	MediLedger and BurstIQ
Supply Chain	Tokenization of assets within supply chains for tracking and financing.	Improved transparency, reduced fraud, and streamlined operations.	IBM Food Trust and Everledger
Art & Collectibles	Fractional ownership of artworks and rare collectables.	Democratised access, improved provenance tracking, and increased liquidity.	Masterworks and Rally
Education	Tokenized academic credentials and certifications.	Simplified verification processes, reduced fraud, and increased portability of qualifications.	Blockcerts and Learning Machine
Entertainment	Tokenized music rights, film royalties, and event tickets.	New revenue streams for creators, direct fan engagement, and reduced piracy.	Royal and YellowHeart

2.4.2 Transformational Impacts on Financial Market Structure

The transition from traditional to tokenized market structures has the potential to reshape core elements of financial intermediation. Traditional markets have relied on centralized intermediaries, such as exchanges, custodians, and clearing systems, to provide trust and efficiency. While these arrangements are well established, they can involve multiple layers of intermediation, limited operating hours, and complex cross-border processes. Tokenization introduces alternative models in which distributed ledgers and smart contracts perform some of these functions directly and instantaneously. This could enable continuous settlement, enhance transparency, and lower barriers to participation. At the same time, the role of intermediaries may evolve rather than disappear, with new responsibilities emerging for both incumbent institutions and new entrants.

The table below outlines key differences between traditional market structure and emerging tokenized market structure, providing a framework to assess how market organisation and financial stability considerations may evolve.

Table 2.12:

Sector-Wise Applications and Impacts of Tokenization

Market Dimension	Traditional Market Structure	Tokenized Market Structure
Infrastructure	CSDs, clearing houses, and intermediaries manage trust and settlement.	Distributed ledgers and smart contracts enable peer-to-peer settlement, reducing reliance on central entities.
Trading Hours	Limited to regional exchange times (e.g. 9:30–4:00, weekdays).	24/7 global trading with continuous settlement.
Cross-Border Flows	Slow, costly, reliant on correspondent banking and FX intermediaries.	Seamless cross-border transfers with embedded compliance (KYC/AML).

Role of Intermediaries	Banks, brokers, and custodians act as mandatory gatekeepers.	Banks reposition as token service providers; DeFi, crypto exchanges and Fintechs provide direct market access.
Transparency	Post-trade processes; reconciliation across multiple ledgers.	Real-time, on-chain transparency with a single source of truth.
Programmability	Static back-end systems; manual corporate actions like coupon payments.	Event-driven logic: programmable bonds (automated coupon payments), automated settlements, and conditional transfers (DvP).
Products & Services	High entry barriers; access largely limited to accredited or institutional investors.	Fractional ownership of RWAs enabling democratised retail access.

"Instead of assets and cash sitting on disparate ledgers coordinated through messaging networks, shared ledgers allow atomic settlement, reduce reliance on central counterparties, unlock trapped collateral, and make assets more mobile and fungible. This can unleash liquidity, expand credit, and ultimately power GDP growth. It is not a fringe innovation — it is about rewiring the core of financial infrastructure."

Naveen Mallela - Global Co-Head, Kinexys by J.P. Morgan

2.5 Use Cases and Case Studies

2.5.1 Expanding the Spectrum of Tokenized Asset Classes

Tokenization entered a pivotal phase in 2025, shifting from experimental pilots to scaled initiatives. The year witnessed a significant rise in real-world deployments across geographies and asset classes, reinforcing tokenization's position as a cornerstone of next-generation financial infrastructure.

Industry Leaders Perspectives on the Future of Tokenization

"We began our tokenization journey with tokenized bonds and recently announced the launch of structured notes tokenized on the Ethereum public blockchain. We're also listing tokenized money market funds on our exchange. Tokenized money market funds fill a treasury gap for crypto-native firms. They are seeking yield, collateral management, and settlement efficiency. Secondary trading will be critical to unlock liqudity. The trajectory is clear — tokenization is transforming how assets are held and managed."

David Hui - Chief Commercial Officer, DBS Digital Exchange

"Tokenization is not just about crypto assets. Stablecoins themselves are essentially tokenized U.S. national debt. Beyond that, we are working with institutions on RWA applications like tokenized funds and debt instruments. These innovations will make assets more accessible and liquid while embedding compliance through verified wallets and smart contracts."

Star Xu - Founder & CEO, OKX

"We are already the issuer of the world's largest regulated gold token. Our belief is that all financial assets, i.e. fiat, commodities, equities, will move on-chain. We expect to tokenize stocks, other commodities, and eventually more fiat currencies. The challenge is aligning tokenization with real market demand and infrastructure readiness. For example, real estate could be tokenized more effectively once wealth management platforms and digital settlement tools are integrated. As adoption increases, and settlement rails mature, tokenization of fixed income, stocks, and even alternatives will follow naturally."

Walter Hessert - Head of Strategy, Paxos

"Tokenization pilots in bonds, loans, and supply chain finance show promise in improving efficiency and enabling atomic settlement. But the legal framework is not yet fully supportive — securities laws still recognise paper or electronic forms, not tokenized ones. Updating these laws is essential before tokenization can scale."

Dr Daranee Saeju - Assistant Governor, Bank of Thailand

"Banks remain anchors of trust. Customers expect safe custody, compliance and recourse when things go wrong. Fintechs and blockchain-native firms bring efficiency and innovation, but banks provide the trusted credentials and regulatory guardrails. The future will be about combining efficiency from Fintechs and blockchain-native firms with trust from banks, under clear, consistent regulation."

Yip Kah Kit - Executive Director, Head of Blockchain and Digital Assets, UOB

2.5.1.1 Tokenization by Geography

Tokenization in 2025 has seen meaningful advances globally, driven by progressive regulatory sandboxes, rising institutional involvement, and high-value real-world asset pilots. The following table outlines key activities categorised by geography.

Table 2.13:

Tokenization Use Case as per Geography

Region	Initiative	Description	Analysis
U.S.	Robinhood Regulatory Proposal	Robinhood has submitted a formal proposal to the SEC for a federal framework governing real-world asset tokenization.	Robinhood's formal proposal to the SEC reflects growing momentum in the U.S. to establish a clear federal framework for tokenizing real-world assets, indicating mainstream interest.
	BlackRock Treasury Tokenization	BlackRock is introducing a digital share class for its US$150B Treasury fund using blockchain technology from BNY Mellon.	BlackRock's blockchain-enabled Treasury product signifies increasing institutional confidence in tokenized finance, setting a benchmark for traditional asset managers entering this space.
	Custodia & Vantage Bank	Custodia Bank and Vantage Bank have successfully tokenized U.S. dollar demand deposits on the Ethereum mainnet.	Custodia and Vantage Banks' tokenization of U.S. demand deposits on Ethereum signals practical implementation of tokenization in core banking services, increasing on-chain utility.
	Fidelity and Franklin Templeton	Fidelity and Franklin Templeton launched blockchain-based versions of treasury and money market funds for global investors.	Fidelity's filing for a blockchain-based fund reveals how major financial institutions are leveraging tokenization to enhance the liquidity and accessibility of money market instruments. Franklin Templeton's expansion of its tokenized U.S. Treasury fund into Europe demonstrates growing cross-border adoption of tokenized products targeting institutional clients.
Europe	Gemini & Dinari	Gemini launched tokenized stock trading in the E.U., starting with MicroStrategy shares available on-chain.	This initiative expands access to equity markets through tokenization, highlighting Europe's openness to digital asset innovation.

Japan	Gates & Oasys	Japanese real estate firm Gates partnered with Oasys blockchain to tokenize US$75M worth of property holdings.	This initiative highlights how established firms are leveraging tokenization to unlock liquidity and expand investor access.
India	Terazo & Tokeny	Terazo partnered with Tokeny to launch Oryx, India's first regulated tokenized real estate project in GIFT City, with IFSCA approval.	This may be a pioneering step for India in regulated tokenization, demonstrating how GIFT City can serve as a hub for innovation and democratised real estate investment.
U.K.	Fasanara Capital & Polygon	U.K. asset manager Fasanara Capital launched a tokenized money market fund.	This reflects the U.K.'s growing role in tokenized finance, as regulated asset managers adopt blockchain to increase efficiency, transparency, and broaden access to institutional-grade products.
Brazil	Mercado Bitcoin & Polygon	Mercado Bitcoin is partnering with Polygon to issue over US$200M worth of tokenized real-world assets in Latin America.	The partnership between Mercado Bitcoin and Polygon Labs indicates strong momentum for tokenization in Latin America, with ambitions to scale beyond US$200M in RWAs.
Saudi Arabia	droppRWA & RAFAL Real Estate	droppRWA will conduct a comprehensive feasibility study for tokenizing properties from RAFAL's portfolio.	The milestone signals early adoption of tokenization in the Kingdom, aligning with Vision 2030 goals to diversify capital markets and expand digital economy initiatives.
Switzerland	Citi-SDX Partnership	Citi has collaborated with SDX to tokenize US$75B worth of pre-IPO shares on Switzerland's digital asset exchange.	The Citi and SDX partnership in Switzerland aims to bring tokenization to non-public shares, suggesting a maturing market for pre-IPO tokenized equities within secure infrastructures.
Singapore	Franklin Templeton	Franklin Templeton received regulatory approval to launch the first tokenized fund for retail investors in Singapore.	This marks a significant step in democratising tokenized finance in Singapore, highlighting regulatory openness and positioning the city-state as a hub for both institutional and retail digital asset innovation.
	OCBC Bank	OCBC launched its first tokenized bond in Singapore to enhance issuance and settlement efficiency.	This underscores Singapore's leadership in digital asset adoption, as major banks integrate tokenization to streamline capital markets and attract broader investor participation.
	Giants Protocol & The Assembly Place	Giants Protocol is powering the tokenization of real estate for The Assembly Place, backed by Singapore's sovereign wealth fund.	This initiative demonstrates how tokenization is being applied to institutional-grade real estate, supported by sovereign capital.
	Dubai Land Department Real Estate Platform	The Dubai Land Department has launched a tokenized real estate platform on the XRP Ledger.	This initiative highlights the Dubai government's commitment to advancing blockchain-based real estate platforms, underscoring a regulatory push toward asset digitisation.

U.A.E.	DLD Tokenization Pilot & VARA Alerts	Dubai has initiated a pilot for tokenized property title deeds and issued alerts about fraudulent claims of participation in tokenization programs.	The pilot and associated regulatory alerts demonstrate Dubai's proactive stance in testing and safeguarding real estate tokenization projects within a structured framework.
	ADGM & Chainlink Framework	The Abu Dhabi Global Market has partnered with Chainlink to develop compliant frameworks for tokenized assets.	The partnership between ADGM and Chainlink reflects Abu Dhabi's ambition to craft robust, compliant frameworks for tokenized assets, underscoring its commitment to regulatory innovation.
Hong Kong	Ant International & HSBC Collaboration	Ant International has partnered with HSBC to enable tokenized deposits on the bank's Hong Kong platform.	HSBC's collaboration with Ant International in Hong Kong showcases the role of established banks in spearheading tokenized deposit offerings under a regulated environment.
	Hong Kong Exchanges and Clearing	HKEX launched a digital issuance platform, enabling tokenization of securities such as bonds and structured products.	This provides a regulated infrastructure for capital markets to adopt tokenization at scale.
	HashKey & Bosera	HashKey Group and Bosera Asset Management launched a tokenized money market ETF, combining traditional fund structures with blockchain-based distribution.	This reflects Hong Kong's positioning the city at the forefront of tokenized fund innovation and expanding investor access to on-chain assets.
Qatar	Qatar Financial Centre	QFC unveiled an initiative to tokenize high-rise real estate assets worth more than US$500M.	QFC's regulatory clarity and sandbox approach for tokenization may encourage broader blockchain adoption for real-world assets, particularly in real estate.

"Qatar's selling point is that we do not want speculation. And as we assess the learning and best practice from international standard setters and jurisdictions, we want tokenization that unlocks liquidity, provides access to wealth in untapped areas, and creates sustainable value. That is why we are prioritising real estate, sukuk, funds, and carbon credits over cryptocurrencies or purely speculative assets."

Maha Al-Saadi, Head - Regulatory Affairs, Financial Services Sector, Qatar Financial Centre (QFC)

Tokenization Case Studies

Table 2.14:

A. BlackRock – Tokenized Money Market Fund BUIDL	
Entities Involved:	BlackRock, Securitize, BNY Mellon, Anchorage, BitGo, Coinbase, Fireblocks
Use Case Title:	BlackRock's USD Institutional Digital Liquidity Fund
Target Customers:	Accredited institutional investors and clients seeking high-liquidity, short-duration token investments.

Use Case Description:	• Launched March 20, 2024, BUIDL tokens represent holdings in a traditional USD MMF comprised of Treasuries and repos. • Built on ERC-20 (Ethereum), the fund offers real-time token transfers among accredited investors, automated daily dividend distributions, and cross-chain interoperability. • As of July 2024, AUM exceeded US$500M, making it one of the largest-tokenized funds.
Value Proposition:	It enables 24/7 atomic settlement and peer-to-peer transfers, improves capital efficiency with on-chain yield automation, and serves as high-quality collateral in DeFi and TradFi pipelines.
Future Outlook:	BlackRock plans multi-chain expansion (Arbitrum, Solana, Aptos) and broader institutional adoption. The fund surpassed Franklin Templeton's tokenized money-market fund and continues to grow as a bridge between TradFi and digital markets.

Source: Securitize, 2024

B. Kinexys – Institutional Asset Tokenization

Entities Involved:	Kinexys Digital Assets, Apollo Global Management, Axelar, Oasis Pro, and Provenance Blockchain
Use Case Title:	Industrialising Institutional Asset Tokenization via Kinexys
Target Customers:	Institutional investors, wealth managers seeking efficient portfolio solutions, fee-based service providers.
Use Case Description:	• Kinexys, JPMorgan's tokenization platform, evolved from its Project Guardian pilot with MAS and Apollo. • In November 2023, Onyx (now Kinexys) released a proof-of-concept enabling fund managers to tokenize assets across blockchains. It integrates permissioned layers (Provenance) and bridges (Axelar, Oasis Pro) to settle tokenized funds and collaterals on-chain. • The platform has processed over US$1T in notional value, US$2B daily, with applications including intraday repo, municipal bonds, and treasury transactions before shifting to investment fund tokenization.
Value Proposition:	It streamlines collateral flows and fund distribution, enables 24/7 liquidity management for institutions, and reduces manual operations via blockchain integration.
Future Outlook:	JPMorgan plans to open Onyx (now Kinexys) for third-party applications, including foreign exchange and permissioned public blockchain support. The focus is on "industrialising PoCs" responsibly for real-world deployment.

Source: Ledger Insights, 2024

C. DAMAC & MANTRA – US$1B RWA Tokenization

Entities Involved:	DAMAC Group, MANTRA Chain, U.A.E. regulators
Use Case Title:	Institutional-Scale Real-World Asset Tokenization
Target Customers:	Institutional and high-net-worth investors seeking diversified exposure to Dubai RWAs
Use Case Description:	• In January 2025, DAMAC Group partnered with MANTRA, a Layer-1 blockchain built for RWAs, to tokenize US$1B of assets, including real estate, hospitality, and data centres. • The collaboration builds upon earlier projects, including a DLT pilot with MAG. Anandible token issuance is slated for early 2025.

Value Proposition:	This unlocks previously illiquid assets for global investment, ensures regulatory compliance via MANTRA's on-chain modules, and demonstrates institutional-grade tokenization at scale.
Future Outlook:	The project supports Dubai's ambition to become a global digital finance hub. It may scale to public participation, additional asset classes, and cross-border trading capabilities.

Source: Mantra, 2025

2.6 The Benefits of Asset Tokenization

Tokenization of assets introduces a structural shift in capital markets by enabling the representation of real-world assets on blockchain. As evidenced across various industry case studies, tokenization holds immense promise in reshaping ownership models, improving liquidity, and streamlining financial operations.

Table 2.15:

Benefits of Tokenization

Benefit	Description
Fractional Ownership	By dividing assets into smaller units, tokenization allows investors to purchase fractions of high-value assets, lowering investment barriers and broadening access to a wider investor base.
Increased Liquidity	Tokenization transforms traditionally illiquid assets, such as real estate or fine art, into digital tokens that can be easily traded on blockchain platforms. This process enhances marketability by enabling assets to be bought, sold, or transferred quickly in digital markets, often 24/7.
Enhanced Transparency	Blockchain's immutable ledger ensures that all transactions are recorded transparently, reducing fraud and enhancing trust among stakeholders through verifiable and auditable records.
Improved Efficiency	Smart contracts automate processes such as settlement and compliance checks, reducing the need for intermediaries and accelerating transaction times.
Cost Reduction	By minimising intermediaries and automating processes, tokenization can lead to significant cost savings in asset issuance, trading, and management.
Programmability	Tokens can be programmed with specific rules and conditions, enabling functionalities like automated compliance, dividend distribution, and complex financial instruments.
Broadened Access	Tokenization democratizes investment opportunities by allowing a broader range of investors to access markets that were previously limited to institutional players.
Real-Time Settlement	Transactions involving tokenized assets can be settled in real-time, reducing settlement risk and improving cash flow management.
Enhanced Security	Tokenization enhances security by replacing sensitive data with unique tokens, reducing the risk of data breaches and unauthorised access.
Global Reach	Digital tokens can be accessed and traded globally, enabling issuers to reach a wider audience and investors to diversify their portfolios across borders.

2.7 Adoption Rate of Tokenization

2.7.1 RWA Tokenization Market Size and Segment Breakdown

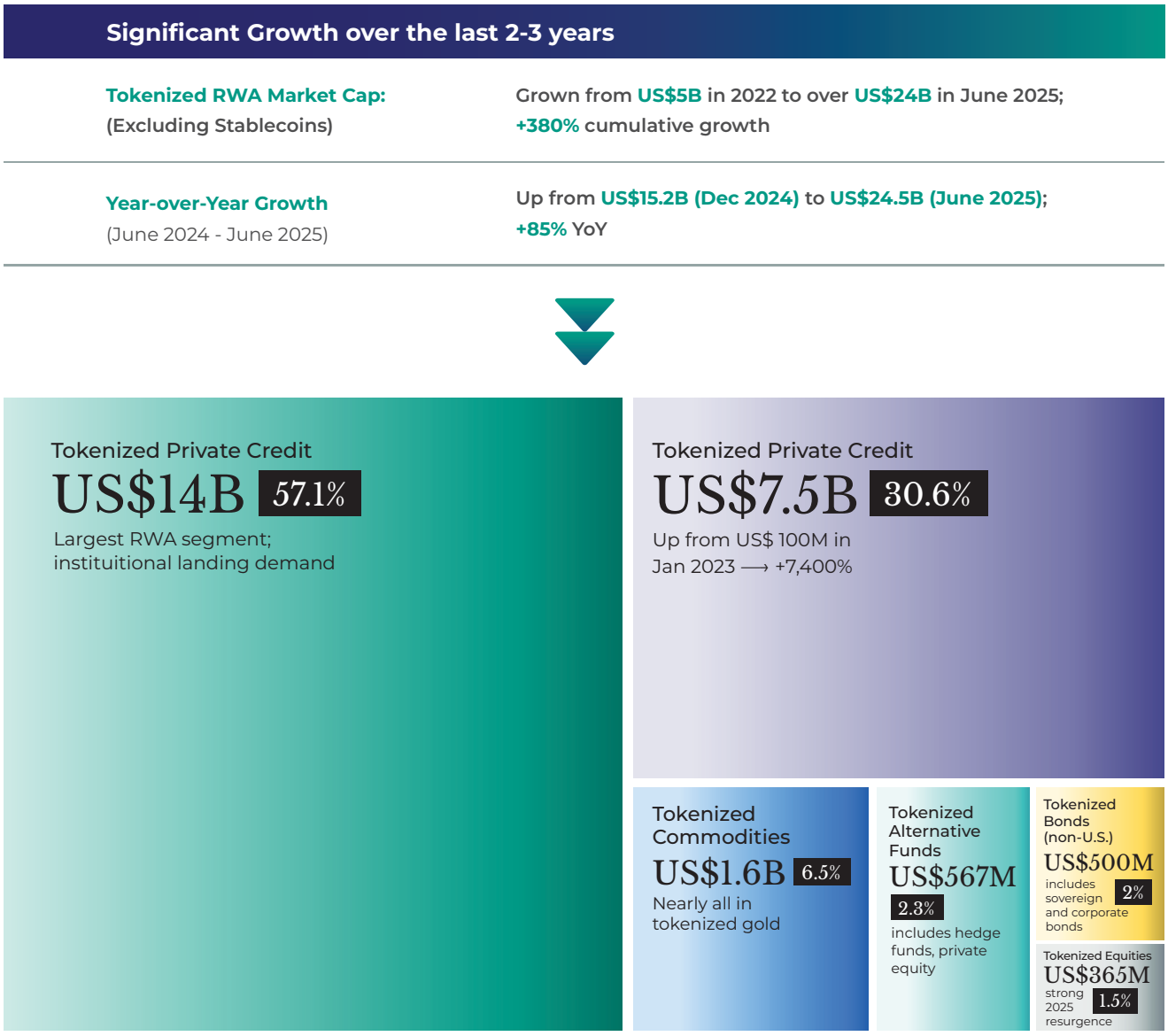
RWA tokenization has entered a phase of exponential growth, expanding from a US$5 billion market in 2022 to over US$24.5 billion[35] by mid-2025, representing 380% cumulative growth. The market grew 85% between June 2024 and June 2025, underscoring increasing institutional interest, maturing infrastructure, and supportive regulatory pilots.

Private credit has emerged as the largest segment, totalling US$14 billion[36] or 57% of the market, driven by strong institutional appetite for tokenized lending instruments. U.S. Treasuries have seen a remarkable surge, from US$100 million in early 2023 to US$7.5 billion[37] in 2025, fuelled by their role as programmable collateral in the digital asset ecosystem.

Other growing categories include tokenized commodities (primarily gold), alternative funds, non-U.S. sovereign and corporate bonds, and tokenized equities. The rising diversity of asset types signals a broader shift toward token-native capital markets that are increasingly interoperable, transparent, and real-time.

Figure 2.3:

Real-World Asset (RWA) Tokenization: Adoption Snapshot - June 2025



Source: RWA.xyz, accessed June 2025

[35] RWA.xyz, accessed June 2025
[36] RWA.xyz, accessed June 2025
[37] RWA.xyz, accessed June 2025

2.7.2 Tokenization Outlook by Asset Class and Industry

In the midpoint scenario, the tokenization of real-world assets is projected to expand from approximately US$0.6 trillion in 2025 to US$18.9 trillion by 2033, representing a compound annual growth rate of 53%[38], as highlighted in a report by BCG and Ripple. The same report projects that stablecoins will dominate the landscape with an estimated US$3.9 trillion in tokenized value by 2033, supported by demand for digital cash equivalents, cross-border payments, and digital dollar accounts in emerging economies. Real estate follows closely at around US$3.1 trillion, fuelled by liquidity gains through fractional ownership and access to global property markets. Funds (approximately US$2.4 trillion) and alternative investments such as private equity and hedge funds (approximately US$2.2 trillion) are also expected to see substantial adoption, reflecting institutional appetite for streamlined private market access. Lending and credit (approximately US$1.8 trillion) along with treasury and liquidity products (approximately US$1.2 trillion) round out the next tier of growth, underscoring tokenization's relevance to capital markets and yield-bearing instruments. Meanwhile, asset classes such as equities, deposits, fixed income, and derivatives, though smaller in scale, are projected to benefit from innovations in settlement efficiency, programmability, and risk management. Collectively, these figures highlight tokenization's transformative role in reshaping financial market infrastructure over the coming decade.

Table 2.16:

Estimated Growth Projections by Asset Classes (Tokenized Volume in US$ trillion)

Asset Class	Estimated Tokenized Values by 2033	Key Drivers
Stablecoins	**~US$3.9T**	Rising demand for digital cash equivalents, cross-border payments, and digital dollar accounts in emerging econimies.
Real Estate	**~US$3.1T**	Improved liquidity via fractional ownership and access to global property markets.
Funds	**~US$2.4T**	Simplified fund management and broader investor access through tokenized units.
Alternative investments (PE, Hedge Funds)	**~US$2.2T**	Instituitional appetite for private market access and streamlined operations.
Leading & credit	**~US$1.8T**	Growth in both DeFi lending platforms and on-chain private credit markets, enabling faster, collateralized, and undercollateralized lending.
Equities	**~US$1.7T**	24/7 trading, programmable dividends, and fractional ownership at lower cost.
Treasury & Liquidity Products	**~US$1.2T**	On-chain money market instruments and short-term instruments for DeFi yield.
Other alternative investments and RWA	**~US$1.1T**	Commodities, carbon credits, and infra-linked assets with traceability.
Deposits	**~US$0.6T**	Tokenized bank liabilities offering instant settlement and programmatic finance.
Fixed Income	**~US$0.4T**	Increased efficiency in issuance, custody, and coupon payments on-chain.
Derivatives	**~US$0.4T**	Automated execution, risk management, and lower-cost access via smart contracts.

Source: BCG & Ripple Report on Tokenization, 2025

Note: Market size estimations for 2033 are approximations. Figures were derived by proportionally allocating the reported total value of US$18.9 trillion.

[38] BCG & Ripple Report on Tokenization, 2025

From an industry perspective, the same report estimates that investment and corporate banks (approximately US$3.7 trillion), along with retail and universal banking (approximately US$3.6 trillion), will anchor the adoption of tokenization through large-scale issuance of tokenized securities, stablecoins, and programmable consumer finance. Alternative investments (approximately US$3.5 trillion) and private banking & wealth (approximately US$3.2 trillion) are expected to benefit from democratised access to private markets and high-value assets, particularly for HNWIs and UHNWIs. Technology and digital infrastructure (approximately US$1.9 trillion), as well as payments and Fintech (approximately US$1.6 trillion), represent the next growth wave, driven by tokenized money for real-time settlement, software rights, and cross-border payments. These projections illustrate how tokenization adoption may reshape entire industries, creating new operating models and revenue pools.

Table 2.17:

Estimated Growth Projections by Industries (Tokenized Volume in US$ trillion)

Industry	Estimated Tokenized Values by 2033	Notable Trends
Investment & Corporate Banks	**~US$3.7T**	Large-scale inssuance of tokenized securities, repo markets and structured products on-chain.
Retail & Universal Banking	**~US$3.6T**	Growth of tokenized deposits and stablecoins; integration of programmable finance for consumers.
Alternative Investments (PE/VC)	**~US$3.5T**	Tokenized access to private equity and venture capital, improving liquidity and access.
Private Banking & Wealth	**~US$3.2T**	Democratization of high-value assets via fractional ownership for HNWIs and UHNWIs.
Technology & Digital	**~US$1.9T**	Tokenization of IP, software rights, and digital infrastructure financing (e.g., data centres).
Payments & Fintech	**~US$1.6T**	Use of tokenized money for real-time settlment, cross-border payments, and DeFi integrations.
Consumer & Healthcare	**~US$0.7T**	Tokenized loyalty programs, health data rights, and alternative financing for healthcare providers.
Industrials & Resources	**~US$0.6T**	Tokenized of equipment leases, carbon credits, and commodities across global supply chains.
Government & Regulators	**~US$0.2T**	Pilot programs for CBDCs, sovereign bonds, and infrastructure tokenization by public instituitions.

Source: BCG & Ripple Report on Tokenization, 2025

Note: Market size estimations for 2033 are approximations. Figures were derived by proportionally allocating the reported total value of US$18.9 trillion.

2.7.3 Tokenization Forecasts Range Widely, but Consensus on Growth

The BCG, Ripple report projects tokenized markets to scale between US$12.5 trillion in a conservative scenario and US$23.4 trillion in an optimistic scenario, with an average case estimate of US$18.9 trillion by 2033. Standard Chartered places the figure as high as US$30.1 trillion[39] by 2034. Outlier Ventures sits in between, projecting around US$20 trillion[40] by 2030.

In contrast, as shown in figure 2.4 McKinsey & Company takes a more cautious view, estimating only US$1–4 trillion[41] by 2030, while Citi projects US$4–5 trillion by the same year. These conservative estimates highlight the uncertainty around adoption speed and scaling, yet even at the lower end, they signal a multi-trillion-dollar opportunity taking shape within the decade. These projections are grounded in growing institutional interest, technological maturity, and the development of regulatory clarity.

[39] Standard Chartered Tokenization, 2024
[40] Outlier Ventures Tokenization, 2023
[41] McKinsey Tokenization Estimates, 2024

Figure 2.4: Growth Projections of Asset Tokenization by Leading Institutions

Asset Tokenization Landscape: Market Size Projections

#	Publication Source	Growth Projections (By Year)	Report Publication Year
1	McKinsey & Company	**US$1-4T** (2030) Average case: **US$2T**	**2024**
2	citi	**US$4-5T** (2030)	**2023**
3	Chainlink Ecosystem	**US$10T** (2030)	**2024**
4	Roland Berger	**US$10.9T** (2030)	**2023**
5	Mordor Intelligence	**US$13.55T** (2030)	**2025**
6	BCG ripple	**US$23.4T-12.5T** (2033) Average case: **US$18.9T**	**2025**
7	Outlier Ventures	**US$20T** (2030)	**2023**
8	standard chartered	**US$30.1T** (2034)	**2024**

Sources: McKinsey, 2024; Citi, 2023, Chainlink, 2024; Roland Berger, 2023; Mordor Intelligence, 2025; Ripple, 2025; Outlier Ventures, 2023; Standard Chartered, 2024

2.7.4 Three Phases of Adoption

The journey toward mass adoption is unfolding across three distinct phases:

Table 2.18:

Tokenization Adoption Phases

Phase	Description	Key Characteristics	Illustrative Examples
Phase 1: Low-Risk Adoption	Financial institutions initiate tokenization with familiar, low-risk assets to test infrastructure and gain operational insights.	• Tokenization of assets like U.S. Treasuries and money market funds. • Focus on operational efficiency and compliance readiness. • Establishment of foundational infrastructure such as digital custody solutions.	• BlackRock's USD Institutional Digital Liquidity Fund on Ethereum. • Franklin Templeton's tokenized money market fund.

Phase 2: Institutional Expansion	Broader adoption across institutions, extending tokenization to more complex and higher-yield assets.	• Tokenization of private credit, real estate, and alternative investments. • Development of secondary markets and enhanced interoperability. • Increased engagement with regulators to address compliance and risk management.	• Centrifuge's tokenization of real-world assets. • Maple Finance's undercollateralized lending pools.
Phase 3: Market Transformation	Comprehensive integration of tokenization across financial markets, leading to systemic changes in asset issuance and trading.	• Widespread tokenization of traditionally illiquid assets. • Standardisation of protocols and regulatory frameworks. • Enhanced collaboration between traditional finance and decentralized platforms.	• Project Guardian's initiatives for cross-border tokenized asset transactions. Development of global tokenization standards by industry consortia.

Sources: S&P Global, 2025; JP Morgan, 2023; Ripple, 2025; FCA, 2024; GFTN, 2024; McKinsey, 2024; BCG, 2025; WEF, 2025

2.7.5 Global Adoption Landscape

Table 2.19:

Tokenization Adoption as per Geography

Region	Adoption Focus	Market Highlights
United States	Tokenized funds, treasuries, collateral	Growth supported by major institutional pilots (e.g. BlackRock, Franklin Templeton, Fidelity) and increasing regulatory clarity around digital assets.
Europe	Tokenized securities, funds	Regulatory momentum through MiCA promotes digital asset harmonisation and introduces a pan-E.U. framework for tokenized securities.
Switzerland	End-to-end tokenized infrastructure	Strong legal foundation and DLT-native infrastructure via SDX enable seamless institutional tokenization of equity and private shares.
Middle East	Real estate, private credit	U.A.E. and K.S.A. lead with state-backed initiatives. Dubai Land Department and ADGM advance tokenization strategies, including frameworks and pilot platforms.
Asia-Pacific	Bonds, structured finance	Singapore, Hong Kong, and Japan pioneer regulatory sandboxes (e.g. MAS's Project Guardian) to test and scale interoperable tokenized finance.
Latin America	Tokenized dollar deposits, SME credit	Brazil and others drive retail use cases through exchanges like Mercado Bitcoin, which partnered with Polygon Labs to tokenize over US$200M worth of assets.

Sources: ESMA, accessed Sep 2025; Reuters, 2025; Government of Dubai, accessed Sep 2025; The Straits Times, 2023; Coindesk, 2025

2.8 Concerns, Challenges, and Barriers to Adoption

While tokenization presents transformative potential across asset classes and financial systems, adoption remains uneven due to a set of persistent frictions. These challenges span legal clarity, market infrastructure, institutional readiness, and technological robustness.

Table 2.20:

Barriers to the Adoption of Tokenization

#	Challenge	Description
1	**Regulatory Uncertainty**	Lack of clear and harmonised regulatory frameworks across jurisdictions. Ambiguities persist around asset classification and legal treatment of tokens.
2	**Technology & Infrastructure Complexity**	Integration with legacy systems is difficult; blockchain models introduce design choices (e.g. permissioned vs. permissionless) that affect control/compliance.
3	**Custody and Security Risks**	Institutional-grade custody, wallet management, and insurance provisions remain underdeveloped for high-value tokenized assets.
4	**Liquidity Fragmentation**	Tokenized markets often operate in silos with shallow order books and limited interoperability between platforms.
5	**Legal Recognition and Enforceability**	Token holders face uncertainty regarding the enforceability of claims in insolvency or dispute, especially across jurisdictions.
6	**Institutional Change Management**	Budget limitations, risk aversion, and siloed operations delay project initiation and scaling across large organisations.

"Issuance alone is not enough. For tokenized securities to be bankable and usable as collateral, they need the right legal wrapper, custodians willing to hold them, and payment rails that support settlement. Without these, tokenization risks being a technical exercise without practical utility."

Fernando Luis Vasquez Cao - Senior Advisor, SBI Digital Asset Holdings

Market activity in asset tokenization has accelerated in 2025, with leading financial institutions and technology firms engaging in a wave of partnerships, product launches, acquisitions, and regulatory filings across multiple regions. Table 2.21 highlights some of the key developments during Q1-Q3, 2025.

Table 2.21:

Asset Tokenization: Market Activities

Quarter	Entities	Geography	Activity	Product	Description
	Circle, Hashnote	U.S.	Acquisition	RWA	Circle acquired Hashnote, a real-world asset issuer.
	ABN AMRO	Netherlands	Partnership	RWA	ABN AMRO conducted an on-chain trade of tokenized assets against stablecoins alongside Germany-regulated 21X.
	Standard Chartered Bank (Hong Kong), China Asset Management (Hong Kong)	China	Partnership	Fund	Standard Chartered Bank (Hong Kong) announced plans to support China Asset Management (Hong Kong) in launching a tokenized retail market fund in Asia Pacific.

Q1 2025 (Jan-Mar)	**Franklin Templeton**	U.S.	Launch	Treasury	Franklin Templeton launched its tokenized U.S. Treasury fund in Luxembourg, expanding access to European institutional investors.
	Mercado Bitcoin, Polygon Labs	Latin America	Partnership	RWA	Mercado Bitcoin partnered with Polygon Labs to expand the tokenization of RWAs in the region.
	Circle	Bermuda	Launch	Fund	USDC stablecoin issuer Circle plans to bring its recently acquired Hashnote Tokenized Money Market Fund under Bermuda's regulatory oversight.
	BlackRock-Securitize, Superstate and Centrifuge	U.S.	Launch	Treasury	BUIDL, issued by BlackRock and Securitize and backed by U.S. Treasury bills and repurchase agreements, is set to receive US$500M allocation.
	DLD	U.A.E.	Launch	Real estate	DLD began a pilot for real estate tokenization, using blockchain technology for property title deeds.
	Fidelity Investments, SEC	U.S.	Registration	Treasury	Fidelity Investments filed paperwork to register a blockchain-based, tokenized version of its U.S. dollar money market fund.
	ADGM, Chainlink	U.A.E.	Partnership	RWA	ADGM signed a memorandum of understanding with Chainlink to collaborate on compliant frameworks for tokenized assets.
	Custodia, Vantage Bank	U.S.	Partnership	USD demand deposits	Custodia Bank and Vantage Bank complete the tokenization of U.S. dollar demand deposits on the Ethereum mainnet.
	DTCC	U.S.	Launch	Collateral management	The DTCC launched a blockchain-based platform for tokenized collateral management to enhance efficiency and real-time operations.
	VARA, DLD	U.A.E.	Warning	Real estate	Dubai's crypto regulator issued an alert, warning of firms falsely claiming to be part of the city's high-profile real estate tokenization pilot.

Q2 2025 (Apr-Jun)	**Blackrock, BNY Mellon**	U.S.	Partnership	Treasury	BlackRock introduced a digital share class for its US$150B Treasury Trust fund, utilising blockchain technology through BNY Mellon.
	Citi, SDX	Switzerland	Partnership	Stocks	Citi and SIX Digital Exchange (SDX) partnered to tokenize non-publicly traded shares.
	Robinhood	U.S.	Registration	RWA	Robinhood submitted a regulatory proposal to the U.S. SEC seeking the creation of a federal framework for the tokenization of real-world assets.
	R3, Solana	Global	Partnership	RWA	R3 and Solana Foundation partnered to bring regulated real-world assets onto a public blockchain.
	Ant International, HSBC	Hong Kong	Partnership	Deposit	Ant International partnered with HSBC Hong Kong to enable the bank to offer tokenized deposits.
	Kraken	U.S.	Launch	Stocks	Kraken announced plans to offer 24/7 global trading of tokenized shares in over 50 U.S. stocks and ETFs, including Nvidia, Tesla, and SPY.
	DLD, Prypco	U.A.E.	Launch	Real estate	The DLD launched its tokenized real estate platform, called Prypco Mint, developed in partnership with real estate Fintech firm Prypco.
	Robinhood	E.U.	Launch	Stocks	Robinhood developed its own blockchain network based on Arbitrum and launched tokenized stock trading for European users.
	Gemini	E.U.	Launch	Stocks	Gemini partnered with Dinari to offer tokenized U.S. stocks to users in the European Union.
	Midas	E.U.	Launch	Credit	Tokenization firm Midas introduced private credit product with Fasanara, Morpho and Steakhouse.
	Republic	U.S.	Launch	Stocks	Republic announced plans to launch tokenized shares in SpaceX (rSpaceX tokens).

BUIDL	U.S.	Launch	Treasury	BlackRock USD Institutional Digital Liquidity Fund (BUIDL) can be used as collateral on Crypto.com and Deribi.
JPMorgan	Global	Pilot	Deposit Token	JPMorgan announced the pilot of JPMD on Base, the layer 2 Ethereum network built by listed exchange Coinbase (COIN).
Coinbase	U.S.	Approval	Stocks	Coinbase seeks approval from the U.S. SEC to launch tokenized stock trading
Moody's Ratings, Alphaledger	U.S.	Trial	RWA	Moody's Ratings and Alphaledger completed a test to embed municipal bond ratings into tokenized securities issued on Solana.
Zodia Custody, GEMx	U.K.	Partnership	RWA	Zodia Custody will handle the safekeeping of tokenized emeralds, through a partnership with GEMx.
BounceBit, Franklin Templeton	U.S.	Partnership	Fund	BounceBit added Franklin Templeton's tokenized money market fund as settlement layer to its structured yield platform, combining U.S. Treasury yields with crypto yield strategies.
CACEIS, Kriptown	France	Acquisition	Stocks	CACEIS, the asset servicing arm of Credit Agricole, acquired a minority stake in French Fintech Kriptown to support the launch of Lise, a blockchain-based exchange aimed at SMEs and mid-cap companies.
Assetera	Global	Launch	Securities	Assetera introduced an API offering instant MiFID II compliance for tokenized securities. The product enables crypto exchanges to list stocks, bonds, ETFs without needing their own regulatory licence.
VERT Capital	Brazil	Plans	Securities	Brazilian securitization firm VERT Capital plans to tokenize up to US$1B in debt and receivables on the XDC Network.
EToro	Global	Plans	Stocks	EToro plans to tokenize U.S.-listed equities on the Ethereum blockchain to enhance trading capabilities.

Q3 2025 (Jul-Sep)	**BNY Mellon, Goldman Sachs**	U.S.	Partnership	Fund	BNY Mellon and Goldman Sachs partnered to roll out tokenized money market funds for clients.
	VERT Capital	Brazil	Launch	Credit	Brazil's VERT launched a tokenized credit platform on XRP Ledger with US$130M issuance.
	GATES	Global	Plans	Real estate	GATES Inc. announced plans to tokenize US$75M worth of Tokyo property using the Oasys blockchain, with ambitions to expand to US$200B.
	Mercado Bitcoin	Brazil	Plans	RWA	Crypto exchange Mercado Bitcoin announced plans to tokenize US$200M in real-world assets on XRP Ledger.
	Ondo Finance	Global	Launch	RWA	Ondo Finance launched a US$250M initiative with Pantera Capital to invest in real-world asset tokenization projects.
	VersaBank	Canada	Pilot	Deposits	VersaBank, a Canadian digital bank, started testing a tokenized deposit, called USDVB, which represents one U.S. dollar held on deposit at VersaBank U.S
	SBI Group, Chainlink	Japan	Partnership	RWA	SBI Group teamed up with Chainlink to develop tokenized assets in Japan.
	State Street, JPMorgan	U.S.	Partnership	Credit	State Street has joined JPMorgan's blockchain platform as the first third-party custodian for tokenized assets.
	DBS Bank	Singapore	Launch	Structured notes	DBS Bank launched tokenized structured notes on the Ethereum blockchain, expanding access to complex financial products.

2.9 The Future Outlook of Tokenization

As tokenization moves from experimentation to mainstream adoption, the next decade is expected to witness a decisive pivot, one that will reshape the architecture of capital markets and create new economic models rooted in programmable value and decentralized trust.

2.9.1 Market Size Projections and Growth Trajectory

Estimates for the asset tokenization market by 2030 vary significantly, reflecting differing assumptions about adoption speed, regulatory clarity, and underlying infrastructure maturity. Leading consulting firms forecast the market to range between US$2 trillion and US$16 trillion, with some anticipating growth driven by the tokenization of financial instruments such as bonds, funds, real estate, and private equity. However, certain institutions within the banking sector have presented more aggressive outlooks, suggesting the market could exceed US$30 trillion, especially when factoring in sectors like trade finance. Standard Chartered estimates[42] that tokenized trade finance alone could account for up to 16% of the total tokenized asset market by 2034, reaching approximately US$4.8 trillion of the US$30.1 trillion projected overall tokenization market.

2.9.2 Demand-Side Momentum

According to the EY-Parthenon HNWI Tokenization Survey[43] (2023), institutional and HNWI investors are rapidly increasing their exposure to tokenized assets, signalling growing confidence in the market:

- Institutional investor allocations to tokenized assets are projected to grow from 2.7% in 2024 to 5.6% in 2026, and reach 7.2% beyond 2027, representing a 2.5x increase. High Net Worth Individuals (HNWIs) have stronger demand, with allocations expected to rise from 5.9% in 2024 to 8.6% in 2026, and 9.3% beyond 2027.
- Interest is concentrated in real estate and private equity: 63% of institutional investors and 59% of HNWIs identified private equity as the most attractive tokenized asset class, followed closely by real estate, cited by 56% and 49%, respectively.
- 72% of institutional investors and 62% of HNWIs stated they would increase their allocations to tokenized assets if the ecosystem matured — specifically citing regulatory clarity, greater issuance by asset managers, and more developed marketplaces as key drivers.

2.9.3 Supply-Side Acceleration

Supply, however, is still catching up. In 2025:

- As of mid-2025, the total value of tokenized RWAs (excluding stablecoins) had reached approximately US$24.5 billion, up from around US$5 billion in 2022. Growth has been concentrated in U.S. Treasuries, private credit, and commodities, which together account for the majority of tokenized asset issuance to date.
- Initiatives such as Project Guardian (Singapore), Project Jura (Switzerland and France), and HKMA's Project Evergreen are accelerating frameworks for public-private asset tokenization platforms.

Mastercard's joint research with Ava Labs[44] reinforces this view, highlighting a shift from "infrastructure buildout" (2021–2024) to "scalable deployment" from 2025 onward, aided by interoperability standards, digital identity frameworks, and tokenized settlement rails.

2.9.4 Strategic Catalysts for Expansion

Several converging forces will determine the pace and scope of tokenization's future:

Table 2.22:

Drivers for Adoption of Tokenization

Strategic Driver	Description
Regulatory Clarification	Jurisdictions like the U.K., U.A.E., Singapore, and Switzerland are leading with sandbox-based or modular licensing regimes that support tokenized securities, funds, and money markets. Going forward, we expect further developments in pass portable licensing (regulatory approvals designed to be recognised across multiple jurisdictions), clearer treatment of tokenized versus traditional financial instruments, and standardised disclosure and custody rules.

[42] Standard Chartered, 2024
[43] EY-Parthenon HNWI Tokenization Survey, 2023
[44] Mastercard, 2025

	Regulatory action is still required in areas such as secondary market infrastructure, cross-border recognition of tokenized instruments, interoperability and clarity on DeFi-related asset classes such as synthetic assets and on-chain derivatives.
Interoperability Standards	Adoption of ISO 20022, token taxonomy frameworks, and cross-chain messaging protocols are helping bridge digital asset ecosystems with traditional systems. Looking ahead, we expect increased alignment around shared messaging formats, identity frameworks (such as decentralized identifiers), and integration of token standards across blockchains (e.g. ERC-3643, ERC-1400). Industry-wide orchestration is still needed to ensure composability and resilience in multi-chain environments, especially for cross-border settlement and synchronised asset servicing.
Programmable Finance	Increasing demand for on-chain compliance, auto-rebalancing funds, and dynamic covenants is enabling programmable asset management structures. In the future, we anticipate more complex financial products embedding real-time triggers, automated tax or ESG screening, and adaptive investor protections. Asset managers may begin deploying programmable fund mandates tailored to investor profiles or regulatory zones. To scale responsibly, action is needed on standardising smart contract auditability, governance structures, and fallback mechanisms for failure or dispute resolution. Alignment between DeFi tooling and institutional-grade compliance will be essential.
Bank Participation	Financial incumbents are emerging as key enablers by offering token custody, issuance platforms, and structured token products. Over time, we expect greater integration of tokenized assets into existing core banking systems, including wealth management portals, corporate treasuries, and lending products. Banks are also likely to move toward multi-asset settlement platforms that accommodate digital bonds, tokenized deposits, and real-world assets. However, significant work remains in harmonising custody and settlement standards, managing counterparty risks in token networks, and gaining regulatory clarity on the balance sheet treatment of tokenized instruments.
Public Sector Involvement	Multilateral agencies, sovereign funds, and central banks are increasingly using tokenized instruments for development financing and green investments. Looking ahead, we anticipate broader adoption of tokenized carbon credits, impact-linked bonds, and programmable disbursements tied to ESG outcomes. Further action is needed to ensure interoperability with private sector platforms, as well as data assurance and traceability in impact reporting. There is growing convergence on the use of public blockchains for transparency, paired with permissioned layers for sensitive policy use cases.

The next phase of tokenization is no longer about if, but how fast and how broad. The convergence of enabling technologies, regulatory momentum, and macroeconomic demand for more efficient and transparent financial markets points to an inevitable transformation. For regulators and institutions alike, the imperative now is to develop inclusive frameworks and interoperable platforms that can accommodate tokenized finance at scale, balancing innovation with systemic integrity.

3 Crypto Exchanges & Retail Access

3.1 Introduction

Cryptocurrency exchanges play an increasingly prominent role in the digital assets ecosystem, acting as the primary gateways enabling individuals and institutions to buy, sell, and trade digital assets. These platforms range from basic digital marketplaces to sophisticated ecosystems offering spot markets, derivatives, custody, tokenized products, and fiat-crypto bridges. Their core functions, facilitating fast transactions, liquidity matching, and fiat integration, are vital to preserving the integrity and efficiency of the broader crypto market.

The size of the crypto exchange market is expanding significantly. As of 2025, the global market size of cryptocurrency exchange platforms, measured as the total revenue generated by these platforms, is estimated at around US$ 63.4 billion[45], with projections placing the market at over US$186.6 billion by 2030. Several key macro factors have been fuelling this growth: rising institutional interest, integration of exchanges with traditional financial systems, and ongoing regulatory clarification that lowers entry barriers while enhancing market trust. Yet this rapid expansion brings systemic considerations: exchanges' control of user funds can pose counterparty risks, and centralized models may introduce vulnerabilities, such as liquidity concentration, custodial inefficiencies, and cybersecurity threats.

As a result, regulators globally have prioritised understanding how exchanges operate, what they offer, and where material risks lie. This underscores the regulatory impetus behind in-depth market monitoring, aligned licensing standards, and supervisory frameworks aimed at ensuring the safety and stability of digital asset markets.

3.1.1 Types of Cryptocurrency Exchanges

Cryptocurrency exchanges can be broadly classified based on their operational models, custody mechanisms, and interaction frameworks. As digital asset markets have evolved, so have exchange architectures, ranging from centralized platforms that offer high liquidity and fiat integrations to decentralized ecosystems promoting transparency and non-custodial trading. More recently, hybrid models have emerged to bridge the best features of both systems. Understanding these categories is fundamental for regulators and market participants alike, as the risk profiles, compliance requirements, and user responsibilities vary significantly across them. The table below provides an overview of the most common types of cryptocurrency exchanges in operation today:

[45] Business Research Company, 2025

Figure 3.1:

Types of Cryptocurrency Exchanges

Exchange Type	Key Characteristics	Examples	Advantages	Disadvantages
Centralized Exchange	Operated by an intermediary, users deposit funds into the platform's custodial wallets	**Binance, Coinbase, Kraken, Bybit**	Higher liquidity, user-friendly, flat on-ramps, fast order execution	Custodial risk, potential for hacks, and regulatory dependency
Decentralized Exchange	Peer-to-peer, non-custodial trading via smart contracts; users retain control of funds	**Uniswap, PancakeSwap, Curve**	Enhance privacy, lower counterparty risk, permissionless participation	Lower liquidity, slower execution, vulnerable to smart contract bugs, and no flat support
Hybrid Exchange	Combines custodial infrastructure with decentralized asset handing or matching engines	**Qurrex, Nash, Eidoo**	Balances liquidity and privacy; may offer custodial choice or layered compliance mechanisms	Regulatory complexity implementation challenges, and still evolving standards

Source: GFTN Analysis

3.1.2 Functional Typology of Modern Crypto Exchanges

Over time, cryptocurrency exchanges have moved beyond simple asset swaps or basic trading functions. Modern platforms are adopting multi-functional service models, offering brokerage-like interfaces and complex financial instruments, to serve a broader user base and institutional clients. This transformation reflects growing market sophistication, competition, and demand for advanced tools and accessibility.

Table 3.1:

Advanced Exchange Service	Key Features	Advantages	Challenges	Examples
Brokerage Platforms	Advice, analytics, and automation tools like robo-advisors and trading bots	Beginner-friendly UX, instant trades, easy onboarding	Higher fees, limited trading options, opaque pricing	Coinmama, Changelly, eToroX
Derivatives & Margin Platforms	Offers futures, options, leveraged tokens, and perpetual contracts	Sophisticated tools for hedging, speculation, and institutional investors	High complexity and risk, regulatory scrutiny, and often lacks spot trading support	Bybit, BitMEX, dYdX

Source: GFTN Analysis

"In most countries, broker-dealers are not yet ready to distribute tokenized securities. Even when retail demand exists, the infrastructure for custody, sub-custody, and compliant distribution is still missing. That is why we step in as enablers, until the ecosystem matures."

Fernando Luis Vasquez Cao - Senior Advisor, SBI Digital Asset Holdings

3.1.3 Functional Architecture of Cryptocurrency Exchanges

Cryptocurrency exchanges are not just trading venues; they are end-to-end digital financial infrastructures that combine multiple roles typically separated in traditional capital markets.

For example, unlike an equity exchange, which functions primarily as a matching engine with custody, clearing, settlement, and client interfaces handled by external brokers and central securities depositories, a centralized digital asset exchange integrates all these functions within a single technology stack. A typical transaction lifecycle spans tightly coupled layers: backend order matching and liquidity management, custody and wallet infrastructure for on-chain settlement, fiat on/off ramps, front-end user experience, and embedded regulatory compliance modules. This vertical integration creates both efficiency and risk concentration: the same platform manages execution, asset safekeeping, and client onboarding.

Regulators interact with this stack at multiple points, i.e. for supervising custody arrangements, enforcing AML/KYC through integrated onboarding modules, and imposing operational resilience standards on trading engines and wallet infrastructures. The core difference from equity exchanges is structural: crypto exchanges combine exchange, broker, and custodian roles into a single platform, while also bridging decentralized blockchain settlement with centralized user interfaces. This convergence makes digital asset exchanges more akin to a hybrid of a trading venue and a custodian bank than a pure equity exchange, demanding a regulatory and operational lens that reflects this unique architecture. The table below illustrates this vertically integrated model, where execution, settlement, custody, fiat gateways, and user onboarding all converge within one platform.

Figure 3.2:

Architecture and Funtional Modules of a Crypto Exchange

Functional Modules	Core Functionality	Supporting Tools
Frontend (UI/UX)	Provides users with access to trading, staking, portfolio views, and reporting.	Web/mobile interfaces, dashboards, APIs
Compliance & Reporting	Tracks suspicious activity, generates tax reports, and handles regulatory submissions and audits.	STR, travel rule transmitters, tax calculator
Support & Resolution	Manages customer service, disputes, and redressal in line with local consumer protection laws.	Ticketing systems, chatbots, dispute handling workflows
Payment & Fiat Gateway	Facilitates fiat on/off-ramps via partnerships with banks and payment providers.	Card processing, SWIFT, SEPA, e-wallet integrations
Wallet & Account Mgmt	Manages user balances, internal transfers, withdrawal rights and security protocols.	Wallet GUIs, 2FA/MFA, address whitelisting
KYC/Onboarding Module	Onboards users while verifying identity, risk scoring, and compliance.	Document verification, biometric authentication, PEP/sanctions screening
Trading & Matching Engine	Core engine for real-time matching of orders, execution pricing, and liquidity routing.	Order books, algorithms, market maker integrations
Custody Engine	Safeguards user funds via cold/hot wallet segregation, MPC, and third-party custodians.	Cold wallets, hot wallets, MPC, key management systems
Blockchain Interface	Enables asset onboarding/offboarding by connecting to public and private blockchains.	Blockchain nodes, APIs for deposits/withdrawals
Infrastructure Layer	Hosts the exchange on secure, scalable cloud or hybrid infrastructure.	Data centres, distributed servers, CDN, encryption frameworks

Source: GFTN Analysis

3.2 Regulatory Landscape for Crypto Exchanges

3.2.1 Overview and Context

As cryptocurrencies transition from niche instruments to integral components of modern capital markets, crypto exchanges stand at the epicentre of this transformation, serving as systemic touchpoints for digital asset liquidity, pricing, and custody. As exchange-based activity has been growing in both volume and sophistication, regulators worldwide are intensifying efforts to establish comprehensive oversight regimes that promote market integrity, protect investors, and mitigate systemic risks.

By 2025, several jurisdictions have advanced their regulatory regimes for crypto exchanges, moving from fragmented or experimental frameworks to more harmonised, enforceable, and principle-based approaches. International assessments in 2025 note that this convergence is still pretty uneven. The FSB's thematic review report[46] observes that while many major markets now impose comprehensive licensing for CASPs, other jurisdictions are still limited to basic AML registration or remain in the process of formulating their regimes. Similarly, IOSCO's 2025[47] review finds regulatory frameworks still developing in the majority of surveyed jurisdictions, underscoring that further reforms are required before global regulatory standards for crypto-asset platforms are fully implemented in practice. In short, progress toward robust and uniform CASP oversight is underway but far from complete across all jurisdictions.

The following sections present a comparative analysis of crypto exchange regulation across key markets, including the E.U., U.S., U.K., U.A.E., Singapore, Japan, Switzerland, Brazil, India, and Hong Kong.

GFTN Survey Insights: Digital Money & Stablecoins

Survey Insight 3.1

Centralized Exchanges: Top Regulatory Concern

33%

Centralized crypto exchanges were selected by 33% of respondents as the digital asset business model most in need of regulatory attention, making it the top-ranked concern overall. This highlights ongoing risks related to custody, user protection, and transparency within centralized trading platforms.

Survey Insight 3.2

Investor Protection Gaps Remain Critical

36%

Consumer and investor protection was cited by 36% of respondents as their organisation's main priority regarding digital asset risk. For crypto exchanges, this underscores the need for stronger safeguards around custody, disclosures, asset listing standards, and user fund protection.

Survey Insight 3.3

Securities Classification Still Unclear

25%

Securities classification was cited by 25% of respondents as a digital asset regulation that was most challenging to navigate. For digital asset exchanges, this reflects ongoing uncertainty over whether and when tokens should be treated as securities, which has major implications for listing practices, disclosures, and compliance obligations.

[46] FSB, 2025
[47] IOSCO, 2025

3.2.2 Comparative Regulatory Architecture Across Jurisdictions

A. Legal Classification and Licensing Frameworks

The legal and regulatory treatment of cryptocurrency exchanges remains highly fragmented across global jurisdictions. In jurisdictions such as the United Arab Emirates, the European Union, Japan, Singapore, Hong Kong, and Switzerland, regulators have introduced dedicated licensing regimes specifically designed to address the unique risks associated with digital asset platforms. These include stringent requirements around the custody of customer funds, compliance with the FATF Travel Rule, and enhanced consumer protection measures.

> " In Singapore, MAS has taken a strong institutional-first approach. Our focus is entirely on institutional clients and accredited investors. We believe regulation is clear: if you want to trade, get licensed, and stay compliant."

Deng Chao - CEO, HashKey Capital

In contrast, jurisdictions like the United States and India rely on traditional financial licensing frameworks, often requiring crypto exchanges to operate under MSB registrations and MTLs. However, these frameworks are not tailored to the specific dynamics of crypto markets, and a unified crypto-specific regulatory regime is still lacking. Brazil represents a middle ground, having passed landmark legislation but still in the process of fully implementing and enforcing its provisions.

The European Union's MiCA Regulation establishes a comprehensive structure for crypto exchanges, designating them as CASPs and mandating national licensing, along with compliance with capital, custody, and governance requirements.

In the United States, exchanges typically register with FinCEN as MSBs. While no federal framework exists yet, legislative proposals such as the Lummis-Gillibrand Responsible Financial Innovation Act aim to clarify regulatory responsibilities across the SEC and CFTC, especially concerning spot and derivatives markets.

MAS regulates exchanges under the Payment Services Act, requiring licensing for "Digital Payment Token" services, accompanied by strict AML/CFT controls and user fund safeguards. In June 2025, MAS tightened rules further, requiring even digital token service providers serving only overseas clients to obtain a licence to operate beyond June 30, 2025. The regulator indicated that approvals for such models would be rare as part of efforts to reduce money laundering risks and rebuild market confidence after a series of high-profile incidents.

In Japan, the FSA mandates full licensing for "Crypto Asset Exchange Service Providers," with requirements including asset segregation, risk controls, and ongoing supervisory oversight.

Switzerland has a distinctive regulatory approach for licensing pathways for cryptocurrency exchanges and other VASPs. Exchanges that offer crypto-fiat conversion, custodial trading, or related payment services can operate under the Anti-Money Laundering Act by joining a SRO. These SROs are themselves supervised by the Swiss FINMA and act as the primary licensing and compliance gatekeepers for crypto exchanges that are not full banks or securities dealers. Membership in an SRO allows a crypto exchange to conduct activities under strict AML obligations while benefiting from a lighter, more flexible regime than a full banking licence. To qualify, exchanges must demonstrate robust AML programs, internal controls, and fit-and-proper management, as well as maintain a real economic presence in Switzerland. All SRO-affiliated exchanges are subject to annual independent audits covering financial soundness and AML compliance, including client onboarding and transaction monitoring.

Meanwhile, India requires crypto platforms to register with the FIU, though a dedicated regulatory regime has yet to be enacted. In Brazil, the recently passed Crypto assets Law (Law No. 14,478/2022) mandates licensing and custodial standards, with enforcement delegated to the Central Bank of Brazil, although implementation is ongoing.

The U.A.E. has taken notable steps toward establishing regulatory clarity in the digital asset space. The VARA in Dubai and the FSRA in Abu Dhabi's ADGM have established robust, internationally aligned licensing frameworks, setting a benchmark for comprehensive oversight in the crypto sector.

Table 3.2:

Global Crypto-Exchange Regulatory Landscape

Jurisdiction	Regulatory Status	Regulatory Regime	Regulatory Body
U.S.	Under development	No unified crypto licence; MSB + state MTL	Regulated via FinCEN (MSB), state MTLs; SEC/CFTC oversight; new bill like CLARITY Act ongoing
E.U.	In force	MiCA - Crypto - Asset Service Provider regime	European Commission - Regime is crypto-exchange-specific
Japan	In force	PSA - Crypto - Asset Exchange Service Provider under FSA	Financial Services Agency - Regime is crypto-exchange-specific
India	Not initiated	Virtual Digital Asset Service Provider (VDASP) via PMLA	Financial Intelligence Unit - India - Exchanges must register with FIU-IND;
U.K.	Under development	U.K. Crypto Asset Business Registration with the FCA	Finanical Conduct Authority - Under consultation stages
Brazil	In force	VASP licensing under Law No. 14,478/22	Central Bank of Brazil / CVM - licensed with AML obligations and consumer safeguards
K.S.A	Not initiated	SAMA/CMA exploring sandbox; no crypto-exchange licence yet	Saudi Central Bank / Captial Market Authority
Switzerland	In force	FINMA VASP licensing / AMLA SRO model	Swiss Financial Market Supervisory Authority - Regime is crypto-exchange-specific
Singapore	In force	Digital Token Service Provider licensing under FSM Act	Monetary Authority of Singapore - Regime is crypto-exchange-specifc
U.A.E.	In force	VARA VASP Licence	Viritual Assets Regulatory Authority - Regime is crypto-exchange-specific
Hong Kong	In force	SFC Virtual Asset Trading Platform Licence	Securities and Futures Comission - Regime is crypto-exchange-specific
Qatar	In force	QFC Digital Assets Framework	QFC Regulatory Authority - Crypto trading banned

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

The following sections provide a comparative assessment of crypto exchange regulatory frameworks across selected jurisdictions that have enacted or enforced specific crypto exchange-related rules. Jurisdictions such as the United Kingdom, United States, India, and Saudi Arabia have been excluded from this comparative analysis, as these markets either lack dedicated crypto exchange regulations or remain in early-stage development or consultation phases.

Additionally, Qatar has been excluded due to the formal prohibition of crypto trading activities within its jurisdiction.

Table 3.3:

Crypto Exchange-Specific Licensing Regimes

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
Regulation/Licence Name	MiCA – Crypto Asset Service Provider	Crypto-Asset Exchange Service Provider Registration	VASP Licensing under Law No. 14,478/22	FINMA VASP Licensing/AMLA-based SRO model	Digital Token Service Provider under FSM Act	VARA VASP Licence	SFC Virtual Asset Trading Platform Licence
Launch Date	June 30, 2023	PSA (2017) – FSA regime ongoing; FIEA amendments planned 2026	December 2022 (Law enacted); implementation began in June 2023	FINMA VASP guidance 2019; AMLA enhanced June 2025	Digital Token Service Provider under FSM Act passed in 2023; secondary legislation expected in 2025	VARA Act passed in early 2022; rulebook effective June 19, 2025	Applications accepted since June 1, 2023
Regulatory Body	European Commission / National Competent Authorities	FSA	Central Bank of Brazil (Banco Central do Brasil)	FINMA	MAS	VARA	SFC

Source: Press announcements and frameworks released by regulatory authorities, accessed April - June 2025.

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
Licensing Mandatory	✓	✓	✓	✓	✓	✓	✓
Tiered/ Differentiated Licences	✓	✓	✓	✓	✓	✓	✓
Local Entity Requirement	✓	✓	✓	✓	✓	✓	✓
Foreign Licence Recognition	✓[1]	✗	✗	✓[3]	✓[2]	✗	✗

[1] MiCA grants passporting; a licence in one Member State is valid across all EEA countries
[2] Limited; MAS indicates cross-border VASP licensing is required even for overseas customers
[3] FINMA accepts foreign VASP licences via equivalence or bilateral recognition

✓ In place ✗ Does not exist

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

B. Operational, Risk & Safeguarding Requirements

As crypto exchanges have evolved from niche trading platforms into more integrated components of the digital financial ecosystem, regulators globally have introduced more stringent operational, risk, and custodial requirements to ensure consumer protection, mitigate systemic risk, and enhance institutional confidence.

i) Capital Requirements and Risk Management

In jurisdictions such as the E.U., Japan, and Singapore, crypto exchanges are expected to meet prudential obligations akin to traditional financial institutions. These include capital adequacy requirements aimed at strengthening institutional resilience against market shocks and liquidity crises. Notably, Brazil is yet to formalise capital thresholds in binding legislation, although draft policies suggest movement in that direction.

Risk management frameworks are universally enforced in major jurisdictions, with mandates for internal controls, incident reporting, and enterprise risk assessments. Singapore and the E.U. have led the way in implementing structured policies that mandate exchanges to establish internal audit mechanisms and segregated risk teams. This has created a risk-aware ecosystem, increasing regulatory trust and supporting institutional participation.

ii) Custody and Insurance Safeguards

Custody and asset segregation requirements are increasingly being codified. Jurisdictions such as Switzerland and Singapore mandate the clear separation of customer assets from proprietary holdings to reduce exposure to commingling risks, a vulnerability highlighted by high-profile exchange failures in the past. While most leading jurisdictions have adopted these policies, India and Brazil lag, with no enforceable requirement as of mid-2025.

Insurance coverage for custodied digital assets remains inconsistent across jurisdictions. While Japan and the E.U. require exchanges to maintain insurance or comparable financial guarantees, countries like Japan and Brazil have not imposed such rules uniformly. The U.A.E. has recently introduced custody insurance guidelines as part of its evolving virtual asset regulatory strategy.

iii) Business Continuity Obligations

To address potential operational disruptions, including cyberattacks or technological outages, most jurisdictions, including Singapore and the E.U., have introduced business continuity and disaster recovery requirements. These policies require exchanges to maintain documented protocols and conduct regular systems testing. Such safeguards play a crucial role in reducing systemic risk during periods of market volatility.

Table 3.5:

Global Exchange Operational, Risk & Safeguarding Requirements

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
Capital Requirements	✓	✓	✓	✓	✓	✓	✓
Custody & Segregation Rules	✓	✓	✓	✓	✓	✓	✓
Risk Management Frameworks	✓	✓	✓	✓	✓	✓	✓
Insurance Requirement	✓	✗	✗	✓	✓	✓	✓
Business Continuity Obligations	✓	✓	✓	✓	✓	✓	✓

✓ In place ✗ Does not exist

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

C. AML/CFT Compliance and the Travel Rule

A cornerstone of regulatory alignment across jurisdictions is the enforcement of AML and CFT norms. All of the regimes align with the FATF's guidance on VASPs, including obligations around CDD, suspicious transaction reporting, and record-keeping.

The Travel Rule, requiring exchanges to transmit originator and beneficiary information for transfers above a certain threshold, is now enforced in all jurisdictions. The E.U. and U.K. impose no threshold, mandating Travel Rule compliance for all crypto transfers. Singapore enforces similar requirements under MAS Notice PSN02. Japan and Hong Kong require compliance as part of their licensing obligations. The U.A.E. sets a threshold at AED 3,500 (Around US$950).

Table 3.6:

Crypto Exchange AML/ CFT Compliance

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
KYC & ID Verification	✓	✓	✓	✓	✓	✓	✓
Suspicious Transaction Reporting	✓	✓	✓	✓	✓	✓	✓
FATF Travel Rule Adopted	✓	✓	✓	✓	✓	✓	✓

✓ In place

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

D. Consumer Protection and Market Integrity

Jurisdictions have introduced investor protection mechanisms tailored to crypto-specific risks. These include asset segregation, conflict of interest disclosures, mandatory audits, and insurance obligations. Notwithstanding these steps, IOSCO's 2025 thematic review[48] cautions that investor safeguards are still falling short in practice. The IOSCO report observes that even though many jurisdictions have adopted stronger rules, risks to investor protection and market integrity remain present in the crypto market. IOSCO emphasises that regulators should strive to fully implement all recommended measures, eighteen key policy recommendations, covering issues from conflict of interest management to disclosure standards, as soon as possible.

In the E.U., MiCA mandates consumer rights to redress and robust disclosure for CASPs. Singapore requires custodial segregation of assets and imposes strict disclosure norms under the PSA. Japan enforces comprehensive user protection protocols, including frequent inspections and on-chain monitoring. Brazil and Switzerland focus on safeguarding client funds through asset segregation.

[48] IOSCO, 2025

Table 3.7:

Crypto Exchange Consumer Protection & Market Conduct

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
Transparency of Fees & Orders	✓	✓	✓	✓	✓	✓	✓
Complaint Redressal Mechanism	✓	✓	✓	✓	✓	✓	✓
Advertising & Promotion Rules	✓	✓	✓	✓	✓	✓	✓
Retail Suitability Testing	✓	✓	✓	✓	✓	✓	✓

✓ In place

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

E. Token Handling & Infrastructure

Regulatory focus on product governance and infrastructure integrity is increasing, and several jurisdictions are introducing formal frameworks for token issuance, listing, and integration within crypto exchanges.

i) Token Listing Frameworks and Restrictions

Regulated exchanges across the E.U., Japan, and Singapore are now required to implement structured token listing frameworks. These entail due diligence processes to assess legal clarity, risk categorisation, project credibility, and compliance with securities laws before a token is approved for trading. Simultaneously, restrictions on privacy tokens (e.g. Monero, Zcash) have been enforced in jurisdictions like Japan and Singapore, citing AML/CFT risks. In these markets, tokens that provide untraceable transactions are either banned outright or subject to enhanced surveillance. The E.U. has also imposed indirect constraints through their broader AML frameworks.

ii) Custodianship, Wallet Security, and Gateway Support

Requirements around cold/hot wallet management and third-party custodianship are universally present across most developed jurisdictions. Switzerland, Singapore, and the U.A.E. maintain rigorous oversight of wallet operations, including mandatory disclosure of wallet architecture, access control policies, and key management systems. Support for stablecoin-fiat gateways is emerging as a key enabler for exchange-integrated payment services.

Table 3.8:

Crypto Exchange Token Handling & Infrastructure

Category	E.U.	Japan	Brazil	Switzerland	Singapore	U.A.E.	Hong Kong
Token Listing Framework	✓	✓	✓	✓	✓	✓	✓
Token Restrictions (Privacy Coins)	✓	✓	✓	✓	✓	✓	✓
Cold/ Hot Wallet Requirements	✓	✓	✓	✓	✓	✓	✓
Third-Party Custodian Allowed	✓	✓	✓	✓	✓	✓	✓
Stablecoin-Flat Gateway Support	✓	✓	✓	✓	✓	✓	✓

✓ In place

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

Table 3.9:

Case Study: E.U. – ESMA's Crackdown on CASP-Misleading Claims

A. Clarity Over Confusion: ESMA's Post-MiCA Crackdown on Crypto Ad Misrepresentation

Regulation:	Following MiCA's implementation, the E.U. mandated that crypto ads must clearly identify regulated status, highlight risks, and separate regulated from non-regulated services.
Trigger:	On July 11, 2025, ESMA publicly warned CASPs against using their regulated status as a marketing ploy, clarifying that promoting non-MiCA services alongside regulated ones creates investor confusion.
Impact on Crypto Exchanges:	Exchanges must overhaul marketing content to segregate product types, include clear disclaimers (e.g. "Not covered by MiCA"), and remove any claims implying full regulatory protection when absent.

Source: Reuters, 2025

Case Study: Singapore – MAS Bans Public & Influencer Advertising

B. MAS Draws the Line: Singapore's Ban on Public & Influencer Crypto Advertising

Regulation:	In 2022, MAS issued new guidelines under the Payment Services Act, restricting DPT service providers from promoting their services to the general public.
Trigger:	Public memos and amendments prohibited ads on broad-reaching channels (public transport, websites, broadcast, social media influencers), citing concerns over impulsive retail investor behaviour.
Impact on Crypto Exchanges:	Exchanges now restrict marketing to their own websites, apps, or direct channels and avoid mass-reach campaigns. They are also implementing pre-investment risk assessments for retail users.

Source: Vulcan, 2022

Case Study: U.S. – SEC Enforcement on Influencer Non-Disclosure

C. Disclosure or Penalty: U.S. Regulatory Recoil on Crypto Promotion

Regulation:	Crypto advertising in the U.S. follows the same standards as securities regulation and consumer protection.
Trigger:	Notable SEC actions include: • Paul Pierce: US$1.4 million penalty in 2023 for undisclosed paid endorsements and misleading token statements. • Kim Kardashian: US$1.26 million penalty in 2022 for ETHMax promotion without disclosing payment. • Shaquille O'Neal: NBA legend Shaquille O'Neal agreed to a settlement of US$1.8 million in a class action lawsuit alleging he promoted FTX without disclosing payment.
Impact on Crypto Exchanges:	Platforms now implement strict influencer compensation policies: partners must disclose fees, include risk disclaimers, and adhere to SEC antifraud rules.

Source: Investopedia, accessed September 2025

Case Study: BaFin (Germany) — MiCA Alignment with Prudential Rigour

D. BaFin's MiCA Implementation: Institutional Licensing and Prudential Oversight

Entities Involved:	BaFin
Strategic Focus:	BaFin has taken a methodical, prudentially grounded approach to implementing the MiCA. While MiCA enforcement began across the E.U. in 2025, BaFin has prioritised institutional licensing and operational resilience, positioning Germany as a key jurisdiction for MiCA-compliant activity.
Key Actions:	• Licensed BitGo under MiCA to provide digital asset services within the E.U.. BitGo is a leading U.S.-based crypto custody provider, highlighting BaFin's openness to foreign institutional players. • Issued a MiCA licence to Boerse Stuttgart Digital, a traditional German financial institution expanding into crypto.
Regulatory Stance:	BaFin continues to uphold high supervisory standards, applying MiCA within its existing framework of prudential oversight, licensing due diligence, and operational audits. By licensing entities with robust institutional backbones and emphasising custody and disclosure controls, BaFin reflects a stance of measured openness with systemic safeguards.

Sources: BaFin, 2025; BitGo, 2025; Coindesk, 2025

Case Study: Malta's Crypto Licensing Surge

E. Malta's Crypto Crossroads: Balancing Licensing Ambition with Regulatory Accountability

Entities Involved:	MFSA, ESMA
Licences Involved:	MiCA and MiFID II
2025 Developments and Licensing Trends:	In 2025 alone, Malta's MFSA approved or pre-authorised multiple major crypto players: • Crypto.com received a MiCA licence. • OKX secured both a MiCA pre-authorisation and a MiFID II licence. • Gemini received a MiFID II licence.

Emerging Criticism from E.U. Regulators:

- The ESMA criticised the MFSA for issuing licences to crypto firms without sufficient due diligence and technical scrutiny.
- The E.U. regulator expressed concerns that this rapid licensing model could introduce systemic risks, as poorly vetted firms may use Maltese registration to passport services across the E.U.

Response and Reactions from the MFSA:

- The MFSA defended its procedures, stating that its licensing process adheres to the technical standards of MiCA and MiFID II and that it has enforced strict capital, governance, and risk control requirements.
- However, MFSA has also acknowledged the feedback and committed to undertaking a comprehensive review of its licensing assessment criteria and ongoing supervision practices.

Source: Reuters, 2025

Crypto exchanges continue to face some of the most active regulatory scrutiny, with jurisdictions moving quickly to bring them under licensing and supervisory frameworks. The first half of 2025 has seen a surge of approvals and registrations across Europe, Asia, the Middle East, and the U.S., reflecting both the implementation of MiCA in the E.U. and parallel licensing regimes in other markets. Table 3.10 outlines key regulatory initiatives for crypto exchanges in Q1-Q3 2025.

Table 3.10:

Crypto Exchange: Regulatory Initiatives

Quarter	Entities	Regulatory Authority	Activity	Description
Q1 2025 (Jan - Mar)	Hidden Road	Dutch AFM	Approval	Hidden Road secured a MiCA Licence from the Dutch AFM.
	Crypto.com	MFSA	Approval	Crypto.com announced its Malta entity has received a MiCA licence from the MFSA.
	Boerse Stuttgart	BaFin	Approval	Boerse Stuttgart Digital received an E.U.-wide licence under the Markets in MiCA.
	OKX	MFSA	Pre-authorisation	OKX secured a Markets in MiCA pre-authorisation.
	Bitget	National Revenue Agency	Approval	Bitget obtained a VASP licence from Bulgaria's National Revenue Agency.
	LTP	Hong Kong SFC	Approval	LTP secured Type 1 (Dealing in Securities), 2 (Dealing in Futures Contracts), 4 (Advising on Securities), 5 (Advising on Futures Contracts), and 9 (Asset Management) licences from the Hong Kong SFC.
	Ripple	DFSA	Approval	Ripple received approval from the DFSA to provide regulated crypto payments and services in the DIFC.
	OKX	MFSA	Approval	OKX secured a MiFID II licence in Malta
	MoonPay	Wisconsin Department of Financial Institutions	Approval	MoonPay was granted a Wisconsin Money Transmitter Licence by the Wisconsin Department of Financial Institutions.
	Bitget	CNAD	Approval	Bitget obtained the DASP licence from El Salvador's CNAD.
	Avian Labs	Dutch AFM	Approval	Avian Labs Netherlands was granted a MiCA licence by the Netherlands AFM.
	MetaWealth	Bank of Lithuania	Approval	MetaWealth UAV was granted a VASP licence from the Bank of Lithuania.

Q2 2025 (Apr - Jun)	BitGo	BaFin	Approval	BitGo announced that Germany's BaFin granted BitGo Europe GmbH a MiCA licence to provide digital asset services in the E.U..
	Vivid	Dutch AFM	Approval	Vivid received its MiCA licence from the Dutch AFM.
	Merge	ACPR and AMF	Activation	Merge activated its EMI licence and VASP registration in France.
	Bybit	Austrian FMA	Approval	Bybit received its MiCA licence from the Austrian FMA.
	Openbank	Banco de España	Application	Openbank applied for licences to offer its retail clients access to cryptocurrencies under the E.U.'s MiCA regulation.
	MoonPay	NYDFS	Approval	MoonPay was granted a BitLicence and a Money Transmitter Licence by the NYDFS.
	Coinbase	CSSF	Approval	Coinbase secured a MiCA licence from Luxembourg's financial regulator, CSSF
	Gemini	MFSA	Approval	Gemini secured a MiFID II licence from the MFSA.
	Bitget	TFZ	Approval	Bitget secured a digital asset licence in Georgia to operate as a provider of digital asset exchange and custodial wallet services through the TFZ.
	Kraken	Central Bank of Ireland	Approval	Kraken was granted a licence under the E.U.'s MiCA by the Central Bank of Ireland.
	Crypto.com	Cyprus Securities and Exchange Commission	Approval	Crypto.com secured a MiFID licence after receiving approval of its acquisition of A.N. Allnew Investments Ltd (Allnew) from the CySEC.
	Circle	OCC	Application	Circle Internet Group applied for a national trust philippines charter, aiming to establish a national trust bank called First National Digital Currency Bank, N.A.
	Ripple	OCC	Application	Ripple applied for a national banking licence with the OCC.
Q3 2025 (Jul - Aug)	OKX, ByBit and Bitget	The Philippines SEC	Guidance	The Philippines SEC said it may take action against crypto exchanges including OKX, ByBit and Bitget for operating without appropriate registration and warned the public against using the platforms.
	Not Applicable	Bank of Ghana	Plans	Ghana announced plans to begin licensing cryptocurrency platforms in response to a surge in demand for digital assets.
	Gemini	Malta Financial Services Authority	Approval	Gemini has secured a MiCA licence from the Malta Financial Services Authority.

As regulatory frameworks mature, leading exchanges are adopting tailored licensing strategies to secure market access and build institutional credibility. In 2025, much of this activity has centred on the European Union's MiCA regime, with exchanges seeking licences across multiple jurisdictions. Table 3.11 outlines how major exchanges are positioning themselves through regulatory approvals and licences, and the strategic objectives driving these moves.

Table 3.11:

2025 Regulatory Strategy of Leading Exchanges

Exchange	Jurisdiction	Licence Type	Key Regulator(s)	Strategic Objective
Bybit	Austria	MiCA Licence	FMA (Austria)	Entry into the MiCA-regulated E.U. market.
Coinbase	Luxembourg, U.S.	MiCA Licence	CSSF (Luxembourg), OCC (U.S.)	Dual-licensing for E.U. access and integration with U.S. banking stack.
Crypto.com	Cyprus	MiFID Licence via M&A	CySEC (Cyprus)	Expand crypto-investment products in the E.U.
Kraken	Ireland, E.U.	MiCA Licence	Central Bank of Ireland	Institutional derivatives under a compliant structure.
OKX	Malta	MiCA Licence	MFSA (Malta)	Malta-to-E.U. regulatory gateway.

Table 3.12:

Case Study: Kraken — Licensing Across the E.U. for Risk Product Expansion

A. Kraken: Advancing Compliance Through Strategic Approvals

Jurisdictional Focus:	E.U.
Licence Secured:	MiCA licence
Regulator Involved:	Central Bank of Ireland
Strategy & Direction:	Kraken's approval by the Central Bank of Ireland and its active positioning under MiCA show intent to offer advanced trading products, such as crypto derivatives and structured crypto asset instruments, to E.U. clients.

Source: Kraken, 2025

Case Study: Coinbase – E.U. and U.S. Conformity Through Licensing Expansion

B. Coinbase's Institutional Expansion: Building a Global Compliance Backbone

Jurisdictional Focus:	E.U. and U.S.
Licence Secured:	• MiCA licence (E.U.) • Banking licence in the U.S. (pending)
Regulator Involved:	CSSF (Luxembourg), OCC (U.S.)
Strategy & Direction:	Coinbase continues its multi-jurisdictional compliance build-out. With its receipt of a MiCA licence from Luxembourg, Coinbase is solidifying its access to the E.U. market. Simultaneously, its banking licence application with the U.S. OCC aims to integrate fiat on/off ramps and custodial services under one regulatory umbrella.

Sources: Coinbase, 2025; Reuters, 2025

Case Study: Crypto.com – MiFID Licensing and Regulatory M&A in the Mediterranean

C. Crypto.com: Anchoring Presence Through MiCA Licences	
Jurisdictional Focus:	E.U.
Licence Secured:	MiCA and MiFID licence
Regulator Involved:	CySEC (Cyprus), MFSA (Malta)
Strategy & Direction:	Crypto.com's MiFID licence acquisition via A.N. Allnew Investments Ltd in Cyprus aligns with its strategy to operate within E.U. investment service frameworks, giving it regulatory cover for expanded crypto-financial offerings, including tokenized securities. This move exemplifies a regulatory acquisition strategy, where licensed entities are absorbed to expedite compliance and cross-border operational readiness.

Sources: Crypto.com, 2025; Crypto.com, 2025

3.3 Rapid Adoption of Cryptocurrency Exchanges

The rapid expansion of cryptocurrency exchanges reflects a convergence of rising user adoption, growing market capitalisation, and increasing trading activity. As digital assets move into the mainstream, exchanges are emerging as critical financial infrastructure, driving global participation at unprecedented scale.

3.3.1 Global Crypto Ownership Trends

Cryptocurrency ownership has seen exponential growth across both developed and emerging markets. A Statista survey[49] shows penetration reaching 25% in South Africa, 23% in Brazil, and 20% in India by 2025, underscoring strong adoption in high-inflation and remittance-driven economies. Mature markets like Switzerland and the Netherlands also show steady gains, climbing above 19–22% by 2025. Exchanges have played a central role in onboarding users, particularly retail, by providing accessible entry points into the digital asset ecosystem.

" Our digital exchange integrates with DBS Bank, giving accredited individuals safe and regulated access to digital assets, on/off-ramp facilities, and custody. The goal is to provide exposure to an asset class our customers are demanding, under the same prudential standards as our other businesses."

David Hui - Chief Commercial Officer, DBS Digital Exchange

[49] Statista Survey, 2025

Table 3.13:

Top 15 Countries: Cryptocurrency Ownership and Usage Trends (2019-2025)

#	Country	2019	2020	2021	2022	2023	2024	2025
1	South Africa	16%	17%	18%	23%	22%	22%	25%
2	Brazil	18%	12%	12%	22%	28%	24%	23%
3	Switzerland	10%	9%	13%	18%	21%	19%	22%
4	India	8%	8%	10%	22%	27%	22%	20%
5	Netherlands	10%	9%	10%	19%	19%	16%	19%
6	South Korea	6%	8%	8%	19%	20%	16%	19%
7	Australia	7%	8%	9%	16%	17%	16%	16%
8	Austria	8%	7%	8%	14%	14%	14%	16%
9	United Kingdom	6%	5%	5%	10%	12%	13%	16%
10	Spain	10%	10%	10%	15%	15%	15%	15%
11	Mexico	12%	11%	9%	12%	13%	17%	14%
12	Poland	7%	7%	8%	11%	14%	15%	14%
13	Germany	4%	6%	6%	12%	12%	13%	14%
14	United States	5%	7%	8%	15%	16%	16%	13%
15	Canada	4%	6%	6%	14%	13%	13%	13%

Share of respondents owning or using cryptocurrencies across selected countries.
Source: Statista online survey; April 1 , 2024 – March 27, 2025; 2,000–12,000 respondents per country; ages 18–64; residential online population; 12-month rolling average; respondents selecting cryptocurrency (e.g. Bitcoin).

3.3.2 Expanding Market Scale and Future Forecasts

By 2025, identity-verified crypto asset users are projected to reach 750 million[50] globally, with market forecasts predicting around 1 billion[51] users by 2030. The total cryptocurrency market cap stands at US$4 trillion[52] (July 2025), with projections of US$8 trillion[53] by 2030 at a 30.1% CAGR. The crypto exchange platform market, measured by revenues, is estimated at US$63.4 billion[54] in 2025 and forecasted to triple to US$ 186.6 billion by 2030 under a 24.1% CAGR.

[50] Statista, 2024
[51] Cointelegraph, 2022
[52] Coingecko, accessed September 2025
[53] Mordor Intelligence, accessed September 2025
[54] Research and Markets, 2025

Table 3.14:

Global Cryptocurreny Exchange Market Outlook (2025-2030)

	2025	Forecast (By 2030)
Global Crypto Ownership	750M users (Statista, lowest forecast)	~1000M users by 2030 (BCG)
Global cryptocurrency market cap	US$4.0T (Coingecko, July 28 2025)	US$8.0T by 2030 (Mordor Intelligence, assumption of CAGR of 30.1% during 2025-2030)
Crypto Exchange Market Size#	US$63.4B (Research and Markets)	US$186.6B* by 2030 (Research and Markets, assumption of CAGR of 24.1% during 2025-2029)

Sources: Statista, 2025; BCG, 2022; Coingecko, 2025; Mordor Intelligence, 2025; Research and Markets, 2025

#Market size (US$ billion): The cryptocurrency exchange platform market size value reflects the total revenues generated by exchanges through core activities such as trading and transaction fees, token listing fees, withdrawal and deposit charges, as well as ancillary services including staking, margin and futures trading, and custodial solutions.

3.3.3 Market Adoption and Scale Indicators

By mid-2025, there were over 17,000 cryptocurrencies traded across over 1,328 exchanges[55], highlighting both innovation and the complexity of the ecosystem. Cryptocurrency wallets have emerged as the primary on-ramp for retail participation, with over 820 million[56] unique wallets active globally in 2025, representing 7.4% of all internet users. Asia-Pacific leads with 350 million users (43% of global share), followed by Europe (140 million), North America (134 million), Latin America (92 million), Africa (75 million), and the Middle East (29 million). The total crypto market value exceeds US$4 trillion, with Bitcoin commanding 57% and altcoins accounting for over US$1.6 trillion. Market complexity continues to grow, with over 30 new cryptocurrencies launched every week. These metrics demonstrate the sheer scale exchanges are required to handle and the infrastructure demands created by rapid asset and user expansion.

[55] Coingecko, accessed September 2025

[56] Coinlaw Crypto Wallet Statistics, accessed September 2025

Figure 3.4:

Crypto Exchange Market: 2025 Adoption & Scale Indicators

17,000+ (July 2025)	cryptocurrencies are currently in circulation worldwide	US$4T+ (July 2025)	is the total value of the cryptocurrency market
1,328+ (July 2025)	crypto exchanges facilitate trading across centralized and decentralized platforms globally	57% (July 2025)	of cryptocurrency market cap held by Bitcoin
33 (July 2025)	new cryptocurrencies are created on average every week	750-900M (July 2025)	verified crypto users forecast for 2025
US$1.6T+ (July 2025)	altcoin market cap	US$9.4T+ (Jan - Jun 2025)	trading volume was recorded across crypto exchanges in the first half of 2025

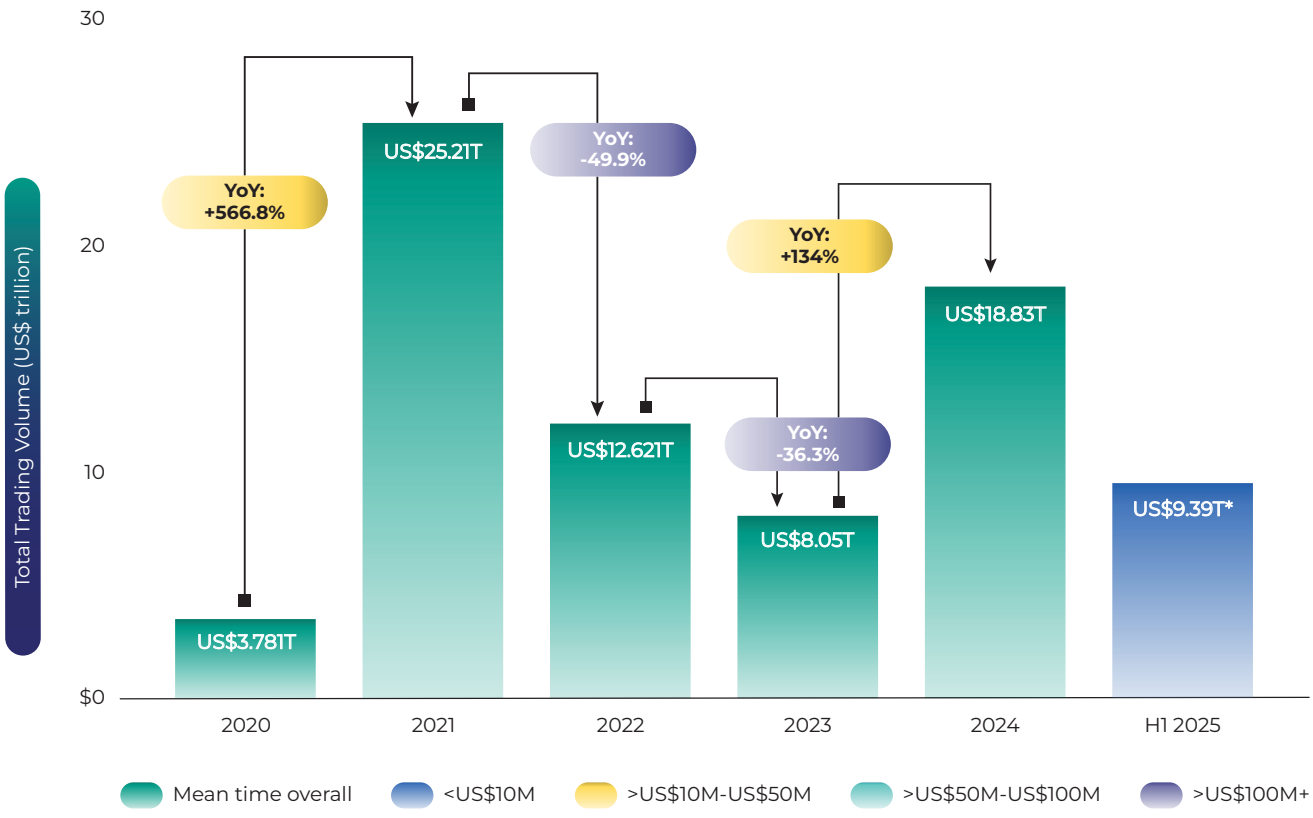
Sources: Coingecko, July 2025; Statista, 2025, The Block, 2025

3.3.4 Trading Volumes as an Adoption Barometer

Exchange trading volumes reflect the market's cyclical yet accelerating adoption curve. After peaking at US$ 25.2 trillion in 2021, crypto exchange trading volumes contracted sharply to US$12.6 trillion in 2022 and further to US$8.05 trillion in 2023, before rebounding to US$18.8 trillion in 2024 (134% YoY). In just the first half of 2025, exchanges have already processed US$9.4 trillion, signalling strong liquidity and sustained demand. The trajectory underscores how crypto exchanges are evolving into critical market infrastructure comparable to traditional capital markets in scale.

Figure 3.5:

Crypto Exchange Annual Cumulative Trading Volume, 2020 - 2024 and H12025



US$9.39T shown for H1 2025 reflects cumulative trading volume for the first half of the year (Jan–June).
Source: The Block, 2025

Table 3.15:

Case Study: Coinbase — Institutional Diversification and Strategic Acquisition

A. Coinbase: Positioning as Crypto's Global Rails & Payment Backbone	
Strategic Focus Overview:	Coinbase is evolving into a crypto financial infrastructure provider, pursuing integrations with payment giants and onboarding global developers and merchants.
Key Moves:	• **Stablecoin Infrastructure**: Crypto-as-a-Service stack, USDC checkout rails, and merchant-focused APIs. • **Big Tech & Bank Partnerships**: Shopify, JPMorgan Chase, PayPal, and American Express for cards and wallets. • **DeFi & Layer-2 Ecosystem**: Launched Base, a Layer-2 network optimised for consumer dApps.
Regulatory Implication:	Coinbase's diversification introduces risks in stablecoin licensing, cross-border fund flows, advertising, and consumer protection. Supervisory alignment is crucial with payment system regulations.

Source: Coinbase, 2024

Case Study: Binance — Global Expansion through Cultural Adaptation

B. Binance: Driving Institutional Products & Regional Solutions	
Strategic Focus Overview:	Binance is shifting focus toward compliant fund management, tokenized fund rails, and regional infrastructure solutions across APAC.
Key Moves:	• **Institutional Launches:** USD Bank Transfer for APAC, institutional token management • **Strategic Solutions**: Fund strategy for managers; Bot Trading integration for pro users. **Travel/Tourism Crypto Payments**: Integration in Southeast Asia and tourism-heavy markets.
Regulatory Implication:	These moves demand oversight of institutional onboarding standards, cross-border money movement controls, and retail trading protections. Stablecoin-related services also require AML attention.

Source: Ecoinimist, accessed September 2025

Case Study: Bybit — Operational Efficiency via Payment and Trading Tools

C. Bybit: Betting on Retail-Friendly Financialisation	
Strategic Focus Overview:	Bybit is expanding rapidly into payment and trading tools targeted at the retail sector, blending traditional Fintech services with digital asset rails.
Key Moves:	• **Launches**: Payment card for international users; Spread Trading Mode; Kazakhstan fiat onramp. • **Retail Strategy**: Simplification of trading interfaces and retail spread optimisation
Regulatory Implication:	Bybit's growing retail footprint necessitates rigorous consumer protection enforcement, including around spread disclosures, retail testing, and custody standards.

Source: Cointelegraph, 2025

Case Study: OKX — Institutional DeFi and Proof-of-Reserves

D. OKX: Bridging Tokenization & TradFi Collateralization

Strategic Focus Overview:	OKX is leaning into tokenized collateral markets and TradFi interoperability, building products that converge traditional and crypto financial systems.
Key Moves:	• **Collateral Mirror Program**: Partnered with Standard Chartered to tokenize money market funds for trading activities. • **Platform Upgrades**: Launched OKX Pay, a next-gen payment wallet tied to token rails.
Regulatory Implication:	This direction invites oversight on tokenized asset custody, segregation requirements, and classification under existing financial instruments law.

Source: Coindesk, 2023

3.4 Factors Affecting the Adoption of Crypto and Cryptocurrency Exchanges

The adoption of cryptocurrencies and the growth of cryptocurrency exchanges are shaped by a combination of technological innovations, macroeconomic dynamics, regulatory clarity, and evolving user preferences. On one hand, factors such as financial inclusion, innovation in blockchain infrastructure, and investor appetite for decentralized assets have acted as strong drivers, accelerating global crypto adoption. On the other hand, inhibitors like regulatory ambiguity, cybersecurity concerns, and limited fiat integration continue to restrain broader adoption, particularly in emerging markets or risk-averse jurisdictions.

The interplay of these forces varies significantly across jurisdictions, investor classes (retail vs. institutional), and product offerings (spot, derivatives, staking), making it essential for regulators to tailor their supervisory frameworks in a way that fosters innovation while mitigating systemic risk.

Table 3.15

Drivers and Inhibitors of Adoption & Usage of Crypto Exchange Platforms

Drivers	Category	Inhibitors
Jurisdictions offering clear legal frameworks (e.g., MiCA in the E.U., VARA in the U.A,E).	**Regulatory Environment**	Lack of unified global standards, fragmented licensing across states (e.g., U.S. MTLs)
Access to digital assets for the unbanked via mobile wallets and exchanges.	**Financial Inclusion**	Low internet/ mobile penetration in some developing economies.
Advancements in blockchain scaling (L2s), DEX infrastructure, custodial innovations.	**Technology & Infrastructure**	Poor backend infrastructure, high transaction fees and L1 chains.
Institutional entry (e.g., ETFs, custodians), diversified crypto products (yield, staking).	**Market Maturity**	Volatility, price manipulation fears, and pump-dump schemes.
Seamless flat-crypto integrations with cards, bank APIs, payment partners	**Fiat On/ Off-Ramps**	Restricted banking access for exchanges, de-risking by traditional financial institutions
Rise in educational content, compliance-focused exchanges, and influencer awareness campaigns	**User Trust & Education**	Persistent scams, rug pulls, and lack of crypto literacy.
Hedging against inflation and devaluation in countries with weak monetary systems	**Economic Uncertainty**	High-risk perception during global downturns or post-FTX contagion events.
Proactive initiatives such as crypto asset taxation guidance and sandbox frameworks for exchanges	**Governmental Support**	Crypto bans or restrictions (e.g., India's evolving stance, China;'s tightened controls).
Emergence of regulated custodians, insurance, and compliance tech.	**Institutional Infrastructure**	Lack of clarity on securities vs. commodities status of tokens
Expansion of tokenized real-world assets and cross-chain bridges	**Innovation & Interoperability**	Cross-chain vulnerabilities and exploit risks.

Source: GFTN Analysis

" Tax policy plays a critical role in shaping how markets develop and where activity occurs. Proportionate approaches help encourage participation in regulated environments while supporting greater transparency and oversight. Disproportionate treatment undermines regulatory intent by driving activity offshore, rendering AML oversight ineffective and reducing potential revenue contribution."

Katie Mitchell - Head of APAC and Middle East Policy, Coinbase

Table 3.17:

Crypto Exchange: Market Activities

Quarter	Entities	Activity	Description
Q1 2025 (Jan - Mar)	Kraken	Launch	Kraken launched Kraken Pay, a service that allows users to send payments using over 300 cryptocurrencies and fiat currencies.
	Coinbase	Partnership	Coinbase partnered with Onboard Global to offer crypto P2P payments to Nigerians.
	Coinbase	Partnership	Coinbase partnered with Morpho to launch Bitcoin BTC -0.36% -backed on-chain loans, a decentralized lending protocol available on Ethereum and Coinbase-incubated Ethereum Layer 2 network Base.
	Bybit	Launch	Bybit launched the Bybit Physical Card for international users.
Q2 2025 (Apr - Jun)	Crypto.com	Partnership	Crypto.com partnered with Green Dot Corporation to offer new banking and money management tools to Crypto.com's U.S. customers.
	Kraken	Launch	Kraken launched Krak, an all-in-one global money app designed to simplify how users manage and move money across borders.
	Kraken	Launch	Kraken launched Kraken Embed, a new CaaS solution for neobanks, Fintechs, and traditional banks to provide clients with direct access to cryptocurrency.
	Kraken	Launch	Kraken launched Kraken Prime, a solution designed to offer institutional investors access to trading, custody, and financing.
	Kraken	Acquisition	Kraken announced the completion of its acquisition of U.S. retail futures trading platform NinjaTrader.
	Kraken	Partnership	Kraken partnered with Alpaca to expand crypto trading to FIs.
	Kraken	Partnership	Kraken collaborated with Backed to launch xStocks.
	Kraken	Partnership	Kraken partnered with Mastercard to launch its debit card, allowing customers in the U.K. and Europe to spend their crypto assets at more than 150 million merchants worldwide.
	Kraken	Partnership	ClearBank partnered with Kraken to provide GBP clearing services and access to secure banking infrastructure for U.K. clients.
	Kraken	Partnership	DFDV partnered with Kraken to list the tokenized stock of its publicly traded equity on the Solana (SOL) blockchain.
	Kraken	Partnership	Kraken launched a new Bitcoin staking product through a protocol integration with Babylon Labs.
	Coinbase	Launch	Coinbase launched Coinbase Business, a platform for startups and SMEs to send and receive payments, manage crypto assets, and automate financial workflows
	Coinbase	Launch	Coinbase launched a stablecoin payments stack to make it easier for online merchants around the world to accept USDC.
	Coinbase	Launch	Coinbase unveiled the x402 protocol to automate online payments with stablecoins, allowing direct transactions from holder to merchant without intermediaries.
	Coinbase	Launch	Coinbase launched its CaaS, allowing banks and Fintechs to integrate crypto features directly into their apps using Coinbase's infrastructure.
	Coinbase	Acquisition	Coinbase acquired crypto derivatives exchange Deribit for US$2.9B.
	Coinbase	Partnership	Coinbase teamed up with American Express to launch the Coinbase card, a credit card that offers up to 4% back in bitcoin on everyday purchases.
	Coinbase	Partnership	Shopify partnered with Coinbase and Stripe to offer frictionless and secure stablecoin payments to merchants around the world.

Quarter	Entities	Activity	Description
Q2 2025 (Apr - Jun)	Coinbase	Partnership	PayPal expanded its partnership with Coinbase to increase the adoption, distribution, and utilisation of the PayPal USD (PYUSD) stablecoin.
	Coinbase	Partnership	JPMorgan Chase partnered with Coinbase to launch a deposit token for institutional clients.
Q3 2025 (Jul - Aug)	Binance	Launch	Binance launched Fund Accounts, a solution that simplifies cryptocurrency asset management for fund managers by mimicking traditional financial infrastructure.
	Binance	Launch	Binance launched Spot Copy Trading for automated, risk-free trading.
	Binance	Partnership	Bhutan partnered with Binance Pay to launch a national crypto payment system for tourism, enabling international visitors to use crypto for a wide range of travel-related expenses.
	Bybit	Launch	Bybit launched Spread Trading, a new functionality aiming to optimise the manual technical crypto trading environment.
	Bybit	Partnership	Bybit Kazakhstan launched a fiat deposit and withdrawal channel in partnership with Bank CenterCredit.
	OKX	Partnership	Standard Chartered partnered with OKX to launch a collateral mirroring programme that allows institutional clients to use cryptocurrencies and tokenized money market funds as collateral for trading activities.
	OKX	Launch	OKX introduced OKX Pay, a platform that will support stablecoin payments using USDT and USDC, with additional assets expected to be added later.
	Bitget	Launch	Bitget launched BGUSD, a yield-bearing stable asset certificate that enhances capital efficiency and provides passive income opportunities for users worldwide.
	Crypto.com	Partnership	Crypto.com partnered with Bread Financial to launch crypto-based rewards credit cards in the U.S.
	Tether, Bit2Me	Investment	Tether has invested 30 million euros in Spanish crypto exchange Bit2Me, acquiring a minority stake.
	Coinbase	Partnership	JP Morgan partnered with Coinbase, enabling its clients to connect their bank accounts to Coinbase, redeem rewards points for USDC, and use credit cards to fund crypto purchases.
	OKX	Launch	OKX introduced regulated crypto derivatives for retail traders in U.A.E.
	Coinbase	Partnership	PNC Bank announced plans to use Coinbase's Crypto-as-a-Service platform to offer crypto trading and custody to its clients.
	Kraken	Launch	Kraken debuted its U.S.-regulated crypto derivatives trading platform.
	Coinbase	Partnership	Coinbase partnered with Perplexity AI to bring real-time crypto market data to traders.
	Crypto.com	Partnership	Emirates Airline announced plans to introduce cryptocurrency payments through a partnership with Crypto.com.
	Bybit	Partnership	Circle penned a revenue sharing agreement with crypto exchange Bybit.
	Gemini	Launch	Gemini expanded its staking services to the U.K., allowing all customers to earn rewards on ether and solana directly through its platform.
	Kraken, Capitalise.ai	Acquisition	Kraken acquired Capitalise.ai, an Israel-based firm that specialises in no-code, natural-language trading automation.
	Gemini	Funding	Gemini's S-1 IPO filing revealed a credit agreement with Ripple, with an existing US$75M credit line, that may extend to US$150M, potentially using Ripple's RLUSD stablecoin.
	Bybit	Launch	Bybit E.U. introduced spot margin trading for European users at up to 10x leverage, compliant with the region's MiCA regime.

Table 3.18:

Case Study: Revolut — Digital Bank Pivots Toward Crypto Ecosystem

A. From Fintech to Crypto-Finance: Revolut's Regulatory-First Expansion	
Strategic Direction:	Revolut, a licensed digital bank in certain jurisdictions, has progressively integrated crypto features to evolve from a neobank into a holistic digital finance platform. Its crypto strategy centres on improving accessibility, enhancing user control, and offering regulated staking and trading services globally.
Key Product Launches:	• **Crypto Staking**: Expanded in early 2025 to allow users to earn rewards on assets like Ethereum, Cardano, and Polkadot. • **On-Ramp Expansion**: Rolled out fiat-to-crypto conversion in 45 U.S. states with robust regulatory adherence. • **Spend-from-Crypto Cards**: Enabled automatic conversion of crypto holdings for real-time purchases via its Revolut debit card.
Regulatory Insight:	Revolut operates under digital banking regulations in Europe and the U.K. and has obtained necessary BitLicence-related approvals for U.S. operations, complying fully with KYC/AML, custody segregation, and consumer protection standards.

Source: Revolut, 2024

Case Study: eToro — Social Trading Meets Crypto Assets

B. Bridging TradFi and DeFi: eToro's Evolution into a Hybrid Crypto Investment Hub	
Strategic Direction:	Originally built around stocks and social trading, eToro has integrated crypto as a long-term growth pillar. Its crypto roadmap balances user demand with product innovation through staking, educational offerings, and seamless conversion between traditional and digital assets.
Key Product Launches:	• **Crypto Staking Expansion**: Users can stake assets like Ethereum and Cardano with institutional-grade custodianship. • **Integrated Wallet App**: Updated to support multiple chains, with built-in swap and lending features. • **Crypto Card (2025)**: New Visa debit card tied to eToro accounts with automatic asset conversion and reward benefits.
Regulatory Insight:	Authorised by the U.K.'s FCA and registered with Cyprus's CySEC, eToro has updated its Visa co-branded debit card program and crypto wallet, ensuring compliance with AML/CFT, investor suitability testing, and custody safeguards.

Source: eToro, 2025

Case Study: Robinhood — Brokerage-Evolved Crypto Integration

C. Retail Trading Rewired: Robinhood's Crypto Pivot and Regulatory Realignment	
Strategic Direction:	Robinhood, primarily a stock app, has enhanced its crypto features throughout 2025: enabling 24/7 trading for crypto, launching crypto-equity deposit tokens, and expanding functionalities for institutional clients. It also upgraded its secure wallet with multi-sig and custodial insurance.
Key Product Launches:	• **24/7 Crypto Trading Platform**: With market and limit orders, real-time quotes, and zero-commission execution. • **Robinhood Wallet**: Launched with multi-chain support, hardware integration, and self-custody features. • **Institutional Deposits**: Rolled out crypto deposit accounts and launched exploratory stablecoin issuance.
Regulatory Insight:	Registered with FinCEN as an Money Services Business (MSB) and holding state-level Money Transmitter Licences (MTLs), Robinhood has also submitted applications for OCC-Fintech charters, adopting enhanced KYC/AML, cryptographic wallet protections, and clearer user protections.

Source: Robinhood, 2025

3.5 Emerging Challenges, and Future Outlook

As regulatory regimes for crypto exchanges mature across major jurisdictions, a clear pattern of convergence is emerging around key themes such as anti-money laundering compliance, investor protection, custody segregation and market integrity. While this harmonisation provides greater systemic stability and fosters institutional confidence, it also creates a fundamentally different operating environment for exchanges. The shift is forcing platforms to transition from lightly regulated technology businesses into entities that resemble fully supervised capital markets institutions.

For exchanges, one of the most immediate challenges is the rising cost of compliance. Frameworks such as the E.U.'s MiCA, Singapore's Payment Services Act and Japan's FSA licensing regime impose prudential standards that require higher capital buffers, independent audits, asset segregation and, in some cases, insurance coverage. Large players with global footprints are building enterprise-grade infrastructure across multiple jurisdictions simultaneously, while mid-tier platforms may be struggling under the weight of duplicated licensing and governance requirements, which is already accelerating consolidation in the sector. For example, Binance expanded into Brazil by acquiring the brokerage firm Sim;paul, with approval from the Central Bank of Brazil, while Coinbase acquired Deribit to strengthen its derivatives offering and Kraken completed two major acquisitions, NinjaTrader and Breakout, to enhance its infrastructure and proprietary trading capabilities.

This is compounded by operational fragmentation: despite FATF alignment on principles, the technical implementation of rules such as the Travel Rule, local custody mandates and licensing standards varies widely. Exchanges are often forced to operate jurisdiction-specific entities with separate order books and compliance stacks, creating inefficiencies and undermining the global liquidity pools that underpin their business models.

Another strategic tension lies in balancing cross-border access with increasingly strict localisation mandates. On one side, centralized crypto exchanges depend on deep, unified liquidity pools. The ability for users in different countries to trade against each other on the same order book is what gives these platforms competitive pricing and high volumes. A "global" exchange model lowers operational cost and concentrates liquidity, similar to how FX market volume concentrates in a few large hubs. On the other side, more jurisdictions are imposing localisation mandates. These can include:

- **Local licensing with entity incorporation** (e.g. E.U. under MiCA, Hong Kong SFC, Singapore MAS) – requiring exchanges to create separate legal entities in each market.
- **Data residency rules** – forcing exchanges to store transaction and customer data domestically (e.g. India's data protection framework, U.A.E., and E.U. requirements).
- **Asset ring-fencing** – requiring client funds to be held in local banks or trust accounts and not commingled

with global liquidity pools (e.g. Japan, Singapore, and Hong Kong).

- **Customer base restrictions** – prohibiting serving local residents from offshore entities without a licence (e.g. U.S. SEC/CFTC enforcement, Hong Kong post-2023 VASP rules, Singapore's MAS clarification on the scope of its Digital Token Service Providers in June 2025).

Simultaneously, the industry's traditional revenue model is under pressure. As competition intensifies and fee compression continues, exchanges are seeing their high-margin products, i.e. derivatives, staking, and lending, curtailed in several markets due to investor protection rules. This is pushing them to diversify into adjacent businesses such as asset tokenization, stablecoins, payment rails and institutional custody, each of which comes with its own regulatory scrutiny and capital demands.

Exchanges often navigate differing institutional and retail regulatory expectations, which can diverge in implementation due to varying risk profiles and user needs. Institutions require rigorous segregation of assets, robust reporting and bank-grade risk controls, while retail regimes are increasingly focused on marketing restrictions, suitability testing and limits on leverage and yield products. Building infrastructure that simultaneously satisfies both segments within a single platform has become a complex task. As a result, many exchanges are developing parallel service lines or separate entities to cater to these distinct user bases while maintaining compliance. Looking ahead, the global outlook points towards a smaller number of highly regulated "tier one" exchanges emerging alongside regional champions and niche players, mirroring patterns seen in traditional capital markets. Compliance technology will be a critical differentiator: automated Travel Rule integration, on-chain proof-of-reserves, AI-driven market surveillance and institutional-grade custody will evolve from competitive advantages into baseline requirements. For exchanges, the message is clear: regulatory convergence is not just a policy trend, but a strategic inflection point that will define which platforms survive and which fail to make the leap into becoming truly institutional-grade components of the digital asset financial system.

4 Staking

4.1 Introduction

Staking is the process by which holders of PoS cryptocurrencies commit or "lock up" their tokens to help validate transactions and secure a blockchain network. In exchange for this service, participants (often called validators or stakers) earn rewards in the form of additional crypto assets, similar to earning interest. This mechanism is integral to PoS networks as an energy-efficient alternative to proof-of-work mining, relying on economic incentives rather than costly computation to maintain network integrity.

Staking allows crypto asset holders to "put their crypto assets to work" by holding and pledging assets to the network. By doing so, users both strengthen blockchain security and earn passive rewards for their contribution.

How Staking Works

In a PoS system, the right to validate new blocks (and earn rewards) is proportional to the amount of crypto staked. Validators are selected to create or verify blocks of transactions based on their stake. To incentivise honest behaviour, if a validator acts maliciously or fails to follow protocol, a portion of their staked assets can be slashed (confiscated as a penalty). This risk-reward balance ensures honest validators gain rewards, whereas dishonest or negligent actors can lose part of their stake. Through staking, network security is crowdsourced to asset holders, aligning the health of the blockchain with the economic interests of its community.

Since Ethereum's transition of its consensus mechanism from PoW to PoS with the implementation of "The Merge" in September 2022[57], staking has continued to move to the forefront of crypto markets. As of July 2025, PoS networks collectively represent a market exceeding US$800 billion[58] in market capitalisation, which is about 20% of the total crypto market capitalisation. An estimated 42% of crypto holders participate in staking in some form, drawn by average annual rewards of around 6.8% across major platforms, with some altcoins offering yields exceeding 12%.[59]

" Staking is a core element needed to secure blockchain technology, rather than a financial product in the traditional sense. Well-calibrated, risk-based frameworks can enable responsible participation and preserve consumer protection within a supervised perimeter. Increasingly markets across the world are taking pragmatic approaches to staking which occurs within protocols, on centralized exchanges, and can be performed by and for institutions. We're beyond the era of banning staking as consensus is clearly emerging on how best to regulate the activity."

Katie Mitchell - Head of APAC and Middle East Policy, Coinbase

4.1.1 Taxonomy of Staking Models in PoS Blockchain Networks

PoS networks have developed a range of staking models designed to balance decentralization, accessibility, and capital efficiency. Each model involves trade-offs:

- **Ease of access vs. control**: Users with limited crypto or technical know-how gravitate toward pooled, delegated, or liquid staking options that lower barriers (no node setup, no minimum investments). However, these often require trusting a third-party or smart contract, unlike solo staking, where users retain full control and responsibility of their funds.
- **Risk vs. reward**: Generally, the more layers introduced (custodians, smart contracts, multiple protocols), the higher the risk to stakers. Solo staking is risky in terms of technical performance, but compound models like restaking add new dimensions of risk (slashing across services) in pursuit of stacked rewards. Liquid staking introduces liquidity and DeFi utility at the cost of additional smart contract risk.

[57] Fidelity, 2025
[58] Coingecko, accessed September 2025
[59] Coinlaw, accessed September 2025

- **Reward distribution**: Solo stakers and some delegators receive network-issued rewards directly, whereas staking via intermediaries/pools involves revenue-sharing. Reputable providers disclose their fee structures (e.g. exchanges often pay out 45-90% of the yield to users, keeping the rest[60]). Liquid staking protocols typically take a protocol fee and pass remaining rewards into the Liquid Staking Token (LST) value.

In practice, these models are complementary. For instance, an average retail user might stake via an exchange or staking-as-a-service for convenience, while an institution might run dedicated nodes or use enterprise staking providers that offer white-glove custody and slashing insurance.

Figure 4.1:

Types of Staking Models in PoS Blockchain Networks

Staking Models	Key Characteristics	Examples	Advantages	Disadvantages
Direct Staking (Solo/Native staking)	User runs their own validator node directly on the blockchain; requires technical expertise and minimum stake.	***Ethereum solo validator, Solana validator***	Full control of funds, supports network decentralization, maximizes rewards.	Requires technical setup, high minimum stake (e.g., 32 ETH for Ethereum), risk of slashing.
Staking-as-a-Service (Delegated)	Third-party platforms manage validator infrastructure while users delegate tokens.	***Coinbase, Binance, Kraken***	Simplifies staking, no need for technical setup, professional validator management.	Custodial risk, fees reduce yield, dependency on provider reliability.
Pooled Staking	Users combine smaller amounts of tokens to meet minimum staking requirements and share rewards.	***Lido, Rocket Pool***	Lowers entry barrier, easy participation for retail, shared validator costs.	Rewards split among participants, potential custody risks depending on provider.
Liquid Staking	Stakers receive a tokenized derivative (e.g., stETH) representing staked assets.		Access to DeFi while earning staking rewards, composability with other protocols.	Smart contract risk, de-peg risk for derivative token.
Restaking	Staked assets or liquid staking derivatives are "re-staked" to secure additional protocols or services.	***EigenLayer (Ethereum), Solayer***	Maximizes capital efficiency, earns layered rewards.	Added slashing risk, complexity of tracking rewards.

Source: Journal of Business & Technology Law, 2023; Hogan Lovells, 2025; GFTN Analysis

For the purpose of this chapter, the analysis will concentrate on the first three staking models, i.e. Direct Staking, Staking-as-a-Service, and Pooled Staking, using Ethereum as a reference network. These models are the foundation of validator participation and represent the bulk of staking activity in native Proof-of-Stake environments. The other two categories, Liquid Staking and Restaking, are important to the ecosystem but are primarily executed through DeFi protocols, which are beyond the scope of this chapter.

Staking, a staker operates their own validator node, locking up 32 ETH to earn the full share of rewards, reinforcing decentralization and direct participation. Staking-as-a-Service retains the same one-to-one relationship between staker and validator but outsources the technical operation to a provider in exchange for a fee, making it accessible to less technical participants. Pooled Staking aggregates smaller ETH contributions from multiple users to collectively meet the 32 ETH validator threshold, lowering entry barriers for retail holders and distributing rewards proportionally across the pool.

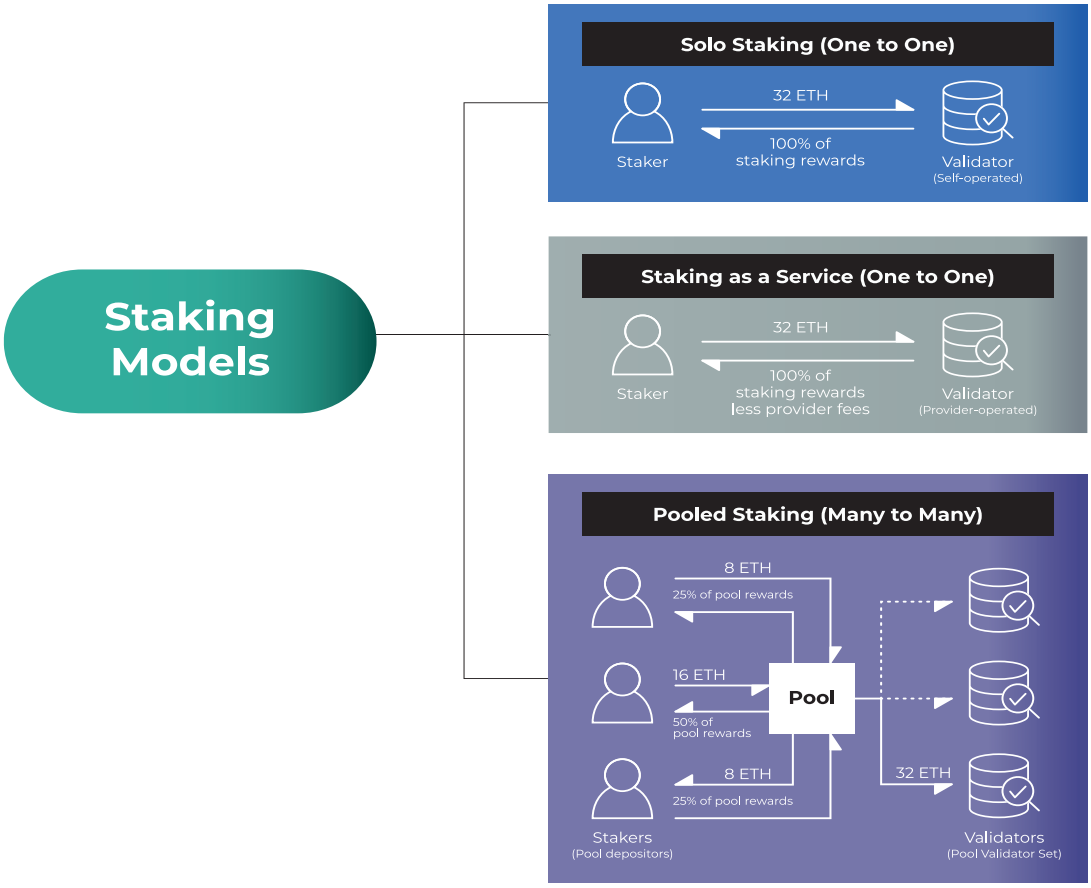
4.1.2 Implementation of Core Staking Models in Ethereum

Figure 4.2 illustrates how the three primary staking models function within Ethereum's Proof-of-Stake network. In Solo

[60] eToro, April 2025

Figure 4.2:

Staking Models in Action: Ethereum's Validator and Reward Flows



Sources: Consensys, 2022; GFTN analysis

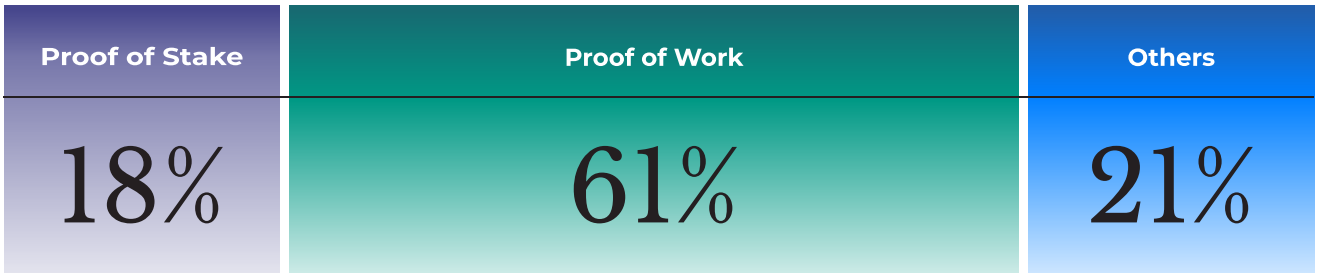
These models collectively underpin Ethereum's security while catering to different user profiles, balancing decentralization, usability, and reward distribution.

4.2 Market Share Shift Toward Proof-of-Stake

The distribution of crypto market capitalisation by consensus mechanism highlights a structural shift in the industry. While Proof-of-Work still represents the largest single share at 61%[61], the rapid rise of Proof-of-Stake networks has redefined the landscape, capturing a growing portion of overall market value. The remainder falls into alternative consensus mechanisms, including hybrids and enterprise-grade solutions, signalling ongoing experimentation in blockchain design.

Figure 4.3:

Crypto Market Capitalisation by Consensus Mechanism of the Underlying Blockchain



Sources: CoinGecko, 2025; The Digital Economy Initiative, 2025

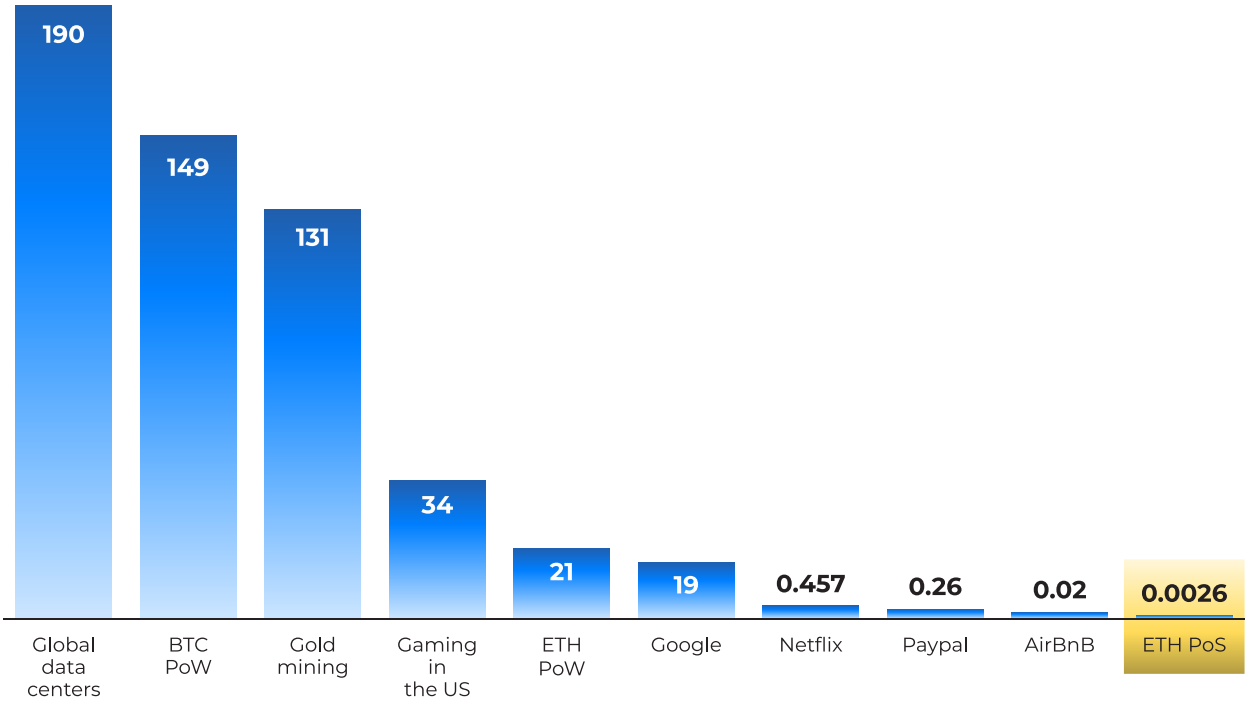
[61] The Digital Economy Initiative, 2025

4.2.1 Energy Efficiency as a Catalyst for Staking Adoption

One of the strongest drivers behind the global shift to PoS and the resulting surge in staking activity is energy efficiency. Figure 4.4 below highlights the dramatic contrast in annual energy consumption between traditional PoW systems and PoS networks. Bitcoin's PoW network consumes around 149 TWh/year, comparable to global-scale industries like gold mining, while Ethereum's former PoW model consumed approximately 21 TWh/year. In contrast, Ethereum's transition to PoS reduced its energy usage to just 0.0026 TWh/year, a reduction of over 99.9%.[62]

Figure 4.4:

Annual Energy Consumption:PoW vs. PoS and Other Industries in terawatt-hours per year (TWh/year)



Source: Ethereum's energy expenditure article, 2025

This environmental and operational efficiency has become a key regulatory and market narrative, aligning blockchain networks with global sustainability goals. The shift has not only reduced the environmental footprint but also opened staking as a mechanism for millions of token holders to actively secure networks while earning returns, fuelling staking's rise as a core economic activity in the digital asset ecosystem.

4.2.2 Staking Market Concentration and Network Implications

Figure 4.5 illustrates the market capitalisation of the top PoS networks, showing Ethereum's overwhelming dominance with nearly half a trillion dollars in market cap, followed by BNB and Solana. This concentration underscores how staking power and liquidity are consolidating around a few major networks, shaping the dynamics of validator economics and influencing digital asset propositions built on top of these chains.

[62] Ethereum, 2025

Figure 4.5:

Staking Powerhouse: Top 10 Proof of Stake (PoS) Networks by Market Cap

Source: Coingecko, accessed July 2025

For policymakers and industry players, the implication is clear: staking is becoming a key pillar of network security and token economics. As capital pools concentrate in major PoS ecosystems, the interplay between staking rewards, network governance, and liquidity provisioning will play a central role in shaping the next phase of on-chain finance.

" Staking isn't a side product, it's part of the same ecosystem as stablecoins and tokenized assets. The goal is composability, sustainability, and decentralization. As stablecoin use cases explode, staking becomes even more essential to network health and security."

Lu Yin - APAC Lead, Solana Foundation

4.3 Regulatory Landscape for Staking

4.3.1 Overview and Context

As staking matures into a core component of the digital asset ecosystem, regulators globally are converging on a critical question: How should staking be classified within existing financial frameworks? The answer defines the licensing perimeter, risk controls, and consumer protections for the sector.

At the heart of this debate lies the categorisation and classification challenge. Staking shares surface similarities with custody, investment schemes, and lending, but diverges in critical dimensions:

- From a **custody** perspective, users lock up assets, but the staking protocol itself may never confer control of private keys to a service provider, making the function operationally distinct from traditional custodial activity.
- Pooled staking models resemble collective investment schemes, yet often lack "management" of pooled assets in the fund sense, creating regulatory ambiguity around whether they should be treated as **securities products** or infrastructure/administrative services.
- Lock-up periods and redemption can mimic **lending** arrangements, but staking does not involve a transfer of title or creation of a borrower–lender relationship, making direct application of lending rules insufficient.

Regulators are increasingly using functional and risk-based frameworks to draw these boundaries. Rather than forcing staking into legacy categories, leading jurisdictions (E.U. MiCA, U.K. FCA proposals, U.A.E. VARA, FINMA, H.K. VATPs Circular) are defining staking as a discrete activity with bespoke licensing or guidance layered on top of custody and market conduct rules. The SEC has already clarified[63] that solo staking, delegated staking (non-custodial) and custodial staking, when tied directly to a network's consensus process, do not qualify as securities offerings.

GFTN Survey Insights: Staking

Survey Insight 3.1

Challenges in Securities Classification

25%

Securities classification was cited by 25% of respondents as a digital asset regulation that was most challenging to navigate. This is particularly relevant to staking protocols, which have come under scrutiny from regulators, who have questioned whether certain staking-as-a-service models constitute investment contracts under securities laws. The survey highlights persistent ambiguity around staking rewards, validator roles, or pooled token arrangements, calling for clearer regulatory guidance.

Survey Insight 3.2

Consumer Protection as a Priority in Digital Assets

30%

Consumer and investor protection was identified by 30% of respondents as the top area requiring regulatory attention in digital assets. This is particularly relevant for custodial staking services, where users delegate tokens to intermediaries (like exchanges or platforms) without full transparency into how rewards are calculated, where assets are held, or what risks are assumed. This underscores the need for clear guardrails to protect retail and institutional stakers.

[63] U.S. SEC Statement, 2025

4.3.2 Staking Regulatory Frameworks Across Jurisdictions

The regulatory treatment of staking is entering a phase of convergence, with major jurisdictions moving to formalise frameworks that balance innovation with investor protection. Regulators are focusing on defining staking as a distinct financial activity, introducing licensing requirements, and embedding consumer safeguards such as asset segregation and disclosure rules. While approaches vary, a clear trend is emerging: staking-as-a-service is increasingly regulated under custody and market conduct regimes, while solo and non-custodial staking largely is allowed and not treated under securities laws.

Table 4.1:

Global Staking Regulatory Landscape (July 2025)

Jurisdiction	Regulatory Status	Staking-Specific Rules	Regulatory Body
U.S.	Under development	May 2025: The SEC clarified that solo staking, delegated staking (non-custodial) and custodial staking, when tied directly to a network's consensus process, do not qualify as securities offerings.	SEC
E.U.	In force	MiCA includes staking service as ancillary to custody services which are fully covered under MiCA (Article 75). Platforms must be authorized CASPs.	European Commission/ ESMA
Japan	Under development	FSA's 2024 tax reforms classify staking income. April 2025 consultation includes staking under revised PSA.	FSA
India	Not initiated	No staking-specific rules. Staking rewards taxed as "Income from Other Sources" or "Capital Gains." No licensing framework.	FIU-IND
U.K.	Under development	2025 HMT guidance excluded staking from fund compliance; FCA DP25/1 (2025) consults on consumer protections & validator transparency.	FCA / HM Treasury
Brazil	Not initiated	2023 tax reforms impose up to 15% on staking rewards, treated as income. No operational regulation for staking services.	Central Bank of Brazil / CVM
K.S.A	Not initiated	No staking-specific rules on staking rewards taxation; No licensing framework for staking services.	SAMA / CMA
Switzerland	In force	In December 2023, FINMA issued supervisory guidance clarifying the regulatory treatment of custodial staking by supervised institutions.	FINMA
Singapore	In force (Institutional only)	MAS banned retail staking (Oct 2023); staking allowed for licensed institutions with risk controls. No retail framework announced till July 2025.	MAS
U.A.E.	In force	VARA introduced "Staking-from-Custody" rules (2023); updated 2025 rulebooks enforce segregation, node ops, disclosures.	VARA
Hong Kong	In force	In April 2025, the SFC issued its first regulatory circular, permitting licensed VATPs to offer staking. This was a major policy shift, as staking was previously prohibited under the Guidelines for VATPs in 2023.	SFC
Qatar	Not initiated	Cryptocurrency trading restricted; no staking allowed.	QFCA

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

" We are closely studying how to launch non-custodial staking under a bank's custody model. This would be the first of its kind, bringing staking into a fully regulated environment. It's a natural evolution of services customers ask for, making balances work for them, while ensuring principal risk is understood and managed."

David Hui - Chief Commercial Officer, DBS Digital Exchange

" DeFi isn't systemically significant today. That said, the FCA is examining issues like staking, whether it's a form of credit or requires investment firm regulation. From our side, the concern is whether such innovations could, in aggregate, create systemic risk over time."

Tom Mutton - Director of Fintech, Bank of England

The U.S. regulatory stance on staking continues to evolve with clearer delineation between protocol-level and service-mediated models. In May 2025, the SEC confirmed that solo and delegated non-custodial staking directly tied to a network's consensus process does not constitute a securities offering. For custodial staking, recent SEC commentary has provided important nuance. In a custodial arrangement, the custodian, whether a node operator or not, acts as an agent rather than providing entrepreneurial or managerial efforts to the crypto asset owner. The custodian merely stakes the deposited assets on behalf of the owner and, in some cases, selects a node operator, but does not determine whether, when, or how much to stake. These administrative or ministerial functions are not sufficient to meet the Howey Test on "efforts of others". Rewards are generated by the protocol, and while custodians may deduct fees, they do not guarantee or set the amount of returns. This interpretation provides a clearer path for regulated custodial staking-as-a-service being classified as not a security.

The E.U.'s Markets in Crypto Assets Regulation (MiCA) does not explicitly legislate staking but captures it indirectly under custody and administration of crypto assets. Platforms offering staking-as-a-service must be licensed as CASPs and comply with segregation and AML requirements. ESMA and the EBA have recently flagged risks tied to liquid staking and restaking in their joint report, emphasising liquidity and consumer protection as priority areas for future guidance.[64] Japan's FSA has not yet formalised staking-specific rules but has begun addressing it via tax reforms, classifying staking rewards as income. April 2025 consultations under the revised PSA signal an upcoming framework, with discussions on how to regulate exchange-operated staking services and protect retail investors while accommodating institutional use. [65]

The U.K. has taken a proactive route with a staged approach. A statutory instrument effective 31 January 2025 confirmed that qualifying crypto asset staking arrangements are not classified as collective investment scheme[66]. Draft legislation under consultation now proposes bringing staking fully into the FCA's financial services perimeter[67]. The FCA's discussion paper on Regulating Crypto Asset Activities (May 2025) further explores consumer understanding, operational risks, and validator safeguards[68]. AML rules and the financial promotions regime also apply to staking services involving custody of client assets. In Switzerland, FINMA's December 2023 guidance provided a comprehensive framework for custodial staking, emphasising segregation of client assets and legal clarity in insolvency scenarios[69]. Building on this, Swiss banks have launched institutional and retail staking products, including PostFinance's ETH staking service in January 2025, underlining Switzerland's role as a regulated hub for PoS participation.

In Singapore, under MAS rules, retail staking through service providers has been banned since October 2023 as part of expanded DPT consumer protection measures. Licensed DPT providers can offer staking to accredited and institutional clients with strict segregation and risk controls, making Singapore's framework a two-tiered model[70]. Solo on-chain staking by individuals remains outside the regulatory perimeter. In the U.A.E, Dubai's VARA has integrated staking into its 2023 "Staking-from-Custody" rules, allowing licensed custodians to provide staking without an additional fund licence, subject to segregation and disclosure obligations.[71] Updated 2025 rulebooks by VARA further embed operational standards for node operations and slashing risk management, positioning the U.A.E. as a leading jurisdiction for regulated staking infrastructure.[72] On 7 April 2025, the H.K. SFC issued its first

[64] EBA, ESMA, 2025
[65] Digital Watch Observatory, 2025
[66] HM Treasury, 2025
[67] HM Treasury, 2025
[68] FCA, 2025
[69] FINMA, 2023
[70] MAS, 2023

circular on staking services, allowing licensed VATPs to offer staking under strict custody and disclosure requirements.[73] This marked a major policy shift from the 2023 VATP Operators Guidelines, which prohibited staking entirely. The SFC continues to evaluate staking-linked ETFs, signalling a cautious but open approach to institutional adoption.

India and Brazil are yet to introduce dedicated staking regulations but have imposed taxation on staking returns. India taxes staking rewards as income or capital gains under existing tax law, while Brazil's 2023 reforms raised taxes on staking-related earnings to 15%, treated as income. Neither jurisdiction has a licensing or consumer protection framework in place for staking. Saudi Arabia and Qatar remain conservative. Saudi Arabia has not initiated a staking framework, while Qatar continues to prohibit most virtual asset trading services, making staking effectively off-limits under its regulatory regime.

Table 4.2:

Staking: Regulatory Initiatives

Quarter	Entities	Regulatory Authority	Country	Activity	Description
Q1 2025 (Jan - Mar)	HashKey	SFC	Hong Kong	Consultation	Hong Kong regulators are in active talks to allow ETF staking, with HashKey expected to be a key pilot participant.
	Ethereum Foundation	Multiple Regulators	Worldwide	Evaluation	The Ethereum Foundation is considering staking a portion of its ETH reserves, citing the significantly improved regulatory environment.
	U.S. National Banks	OCC	United States	Guidance	OCC clarified that U.S. national banks can engage in staking, act as validators, and provide crypto custody without prior supervisory approval.
	Ethereum ETFs	SEC	United States	Review	The SEC is reviewing the inclusion of staking for proposed Ethereum ETFs, a move that could integrate yield-bearing ETH products into traditional finance.
	Hong Kong SFC	SFC	Hong Kong	Roadmap	The SFC unveiled a roadmap that includes enabling regulated staking services which are supported by technical and custodial safeguards.
	U.K. Government	U.K. Treasury	United Kingdom	Guidance	The U.K. government confirmed that staking services are not classified as collective investment schemes, easing regulatory pressure on exchanges.
	Coinbase	Vermont Department of Financial Regulation	United States	Resolution	Vermont dropped its case against Coinbase over staking services after the SEC dismissed enforcement action; South Carolina followed suit.
	Kraken	SEC	United States	Relaunch	Kraken reinstated its U.S. staking services under updated compliance frameworks as regulatory pressure eased.
	Uphold	FCA	United Kingdom	Relaunch	Uphold resumed crypto staking services in the U.K. after FCA regulatory adjustments allowed compliant offerings.
Q2 2025 (Apr - Jun)	U.S. SEC	SEC	United States	Guidance	SEC clarified its view that certain PoS blockchain protocol "staking" activities are not securities transactions within the scope of the federal securities laws.
	Hong Kong SFC	SFC	Hong Kong	Guidelines	The SFC released updated guidelines outlining licensing and compliance standards for staking services within regulated virtual asset platforms.
	Proof of Stake Alliance	SEC	United States	Engagement	CCI's Proof of Stake Alliance (POSA), alongside nearly 30 major crypto organisations, submitted a detailed letter to the SEC's Crypto Task Force urging clear guidance on the regulatory treatment of staking.
	Everstake	SEC	United States	Engagement	Everstake engaged with the SEC on the regulatory future of non-custodial staking.

[73] SFC Circular, 2025

Quarter	Entities	Regulatory Authority	Country	Activity	Description
Q2 2025 (Apr - Jun)	HM Treasury (HMT)	U.K. Government	United Kingdom	Draft Bill`	HM Treasury published draft legislation for crypto assets that includes a regulatory framework for staking services under U.K. law.
	Coinbase	California Department of Financial Protection & Innovation	United States	Scrutiny	Coinbase is facing regulatory pressure in California over its staking services, reflecting state-level enforcement trends.
	Japan FSA	JFSA	Japan	Proposal	Japan's FSA proposed a new framework to regulate crypto staking activities, focusing on investor protection and exchange oversight.
Q3 2025 (Jul - Aug)	U.S. SEC	SEC	United States	Evaluation	The SEC's Division of Corporation Finance declared that properly structured liquid-staking protocols and their receipt tokens generally do not constitute securities under U.S. law.

Table 4.3:

Case Study: U.K. Regulators — Building a Framework for Staking

A. HM Treasury & FCA: Defining Staking Under U.K. Law

Strategic Focus Overview:

The U.K. has taken a phased approach to integrating staking into its crypto regulatory framework, balancing innovation with investor protection. Between January 2025 and March 2025, HM Treasury (HMT) and the Financial Conduct Authority (FCA) issued key guidance and legislative drafts clarifying how staking will be treated under U.K. law, setting a foundation for compliant institutional and retail staking services.

Key Moves:

- **January 2025**: HM Treasury confirmed that crypto asset staking would be excluded from the U.K.'s fund compliance regime, ensuring staking is not automatically classified as a collective investment scheme. This provided much-needed clarity for exchanges and custodians offering staking products.
- **February 2025**: HMT published draft legislation establishing a bespoke regulatory framework for crypto assets, including staking services, outlining licensing and operational standards.
- **March 2025**: The FCA issued Discussion Paper DP25/1, seeking industry feedback on consumer protection, validator transparency, and custody rules for staking platforms under the U.K.'s evolving digital asset regime.

Regulatory Implication:

This series of initiatives positions the U.K. as one of the first G7 jurisdictions to define staking outside of traditional fund management laws while creating a pathway for regulated staking providers. The timeline demonstrates an intent to foster a competitive yet compliant staking market, setting a precedent for other financial hubs.

Sources: Skadden, 2025; Regulation Tomorrow, 2025; FCA, 2025

Case Study: MiCA — Standardising Staking Across the E.U.

B. E.U. Markets in Crypto Assets Regulation: Staking Under a Unified Framework

Strategic Focus Overview:	The E.U.'s MiCA, effective from June 2024 with expanded provisions in 2025, is creating a harmonised regime for staking across 27 member states. While MiCA does not impose a separate licensing regime for staking, it classifies StaaS as an ancillary custody activity under Article 75, requiring providers to hold authorisation to offer crypto asset custody and administration services. This has shifted both institutional and retail behaviours across the European staking market.
Key Moves:	• Staking participation on MiCA-compliant platforms increased by 39% in 2025 as investors sought regulatory clarity and security. • Ethereum staking deposits in the E.U. surged by 28%, reaching US$90 billion in total staked ETH, driven largely by institutional adoption under MiCA's legal protections. • Institutional staking participation rose to 44%, up from 31% in 2024, as MiCA ensured reward stability and provided a clear framework for custodial staking providers. • Validator nodes in the E.U. grew by 19%, reflecting MiCA's mandate for staking platforms to maintain security reserves and decentralized infrastructure. • Regulatory-compliant providers now control 80% of E.U. staking pools, significantly reducing the market share of offshore and unregulated entities. • Staking yields stabilised at 5.2% on average, down from 7.4% in 2024, as new rules reduced volatility in rewards and imposed a mandatory 10% staking reserve to ensure liquidity for withdrawals. • Retail staking deposits declined by 7.8%, as some retail users migrated to offshore platforms offering higher, riskier yields outside MiCA's compliance perimeter.
Regulatory Implication:	MiCA has not prohibited staking; rather, it has anchored staking services to custody licensing, ensuring legal protections and liquidity safeguards while shifting market share to regulated players. The 2025 data underscores MiCA's impact in institutionalising PoS participation, enhancing validator security, and stabilising staking yields, positioning the E.U. as one of the first major blocs with a clear, standardised staking regime.

Sources: LawyersWeek, 2024; ESMA, 2024; Coinlaw, accessed September 2025

Case Study: U.S. SEC — Defining Staking and Navigating ETF Integration

C. SEC: Clarifying Protocol Staking and Evaluating ETF Proposals

Strategic Focus Overview:

In May and June 2025, the U.S. SEC took major steps to clarify the regulatory treatment of staking while reviewing Ethereum ETF proposals incorporating staking features. These actions marked a critical point for both protocol-level validators and institutional financial products tied to Proof-of-Stake networks.

Key Moves:

- **May 29, 2025**: The SEC issued an official statement on "Certain Protocol Staking Activities," confirming that native protocol staking—including solo, non-custodial, and custodial validator operations—does not constitute an offer or sale of securities when rewards are generated by protocol consensus rather than managerial efforts (SEC Statement).
- The statement drew a clear line between protocol-driven rewards and staking-as-a-service models that may qualify as investment contracts depending on marketing and pooling structures.
- **April–July 2025**: The SEC acknowledged and then extended decision deadlines for multiple Ethereum ETF proposals incorporating staking, including filings from Bitwise (NYSE Arca) and BlackRock (iShares Ethereum Trust- ETHA). BlackRock's proposal formally submitted in April 2025 triggered a 240-day countdown for a final SEC decision and included provisions for staking a portion of ETH held by the trust to generate additional yield (Federal Register – Genfinity -Bitwise ETH ETF Staking | CryptoSlate – BlackRock ETH ETF Staking).

Regulatory Implication:

The May 2025 protocol staking statement delivered long-awaited clarity for PoS networks and validators, allowing compliant participation without automatic securities designation. However, the ongoing delays on Ethereum ETF staking approvals underscore unresolved concerns around investor risk, potential market manipulation, and the treatment of yield-bearing ETFs under securities law. The SEC's bifurcated approach distinguishes native network staking as protocol activity from ETF and custodial staking services that require case-by-case investment contract analysis

Sources: SEC Statement, 2025; CoinGape, 2025; CryptoSlate, 2025

Case Study: Hong Kong SFC — Integrating Staking into a Regulated VA Framework

D. Securities and Futures Commission (SFC): Establishing Rules for Staking

Strategic Focus Overview:

In 2025, Hong Kong's SFC advanced its goal of making the city a leading regulated hub for virtual assets by formally incorporating staking into its VA framework. The SFC's initiatives targeted both exchange-based staking and the inclusion of staking in ETPs.

Key Moves:

- **February 2025**: The SFC unveiled a new roadmap for the development of its VA regulatory framework, which included the creation of a licensing regime for institutional staking providers and risk-based capital requirements for custodians offering staking services (Regulation Tomorrow).
- **March 2025**: Hong Kong regulators entered active consultations on enabling Ethereum ETF staking, with HashKey identified as a likely pilot participant. The move aimed to integrate yield-bearing ETH products into the city's ETP regime while aligning with investor protection mandates (The Block).
- **April 2025**: The SFC issued updated guidelines for licensed VA trading platforms, explicitly allowing staking services for approved PoS tokens under strict custody and segregation rules. The guidance required on-chain transparency and enhanced disclosure for reward distribution (SFC Circular).

Regulatory Implication:

Hong Kong's 2025 initiatives positioned it as one of the first major financial hubs in Asia to integrate staking into both exchange-level services and ETF structures under a comprehensive regulatory regime. The inclusion of staking in VA platform licensing and institutional custody standards signals a strong alignment with global institutional demand for yield-bearing PoS assets, while providing a blueprint for other Asian markets.

Sources: Regulation Tomorrow, 2025; The Block, 2025; SFC Circular, 2025

4.4 Global Staking Adoption Rates and Market Dynamics

Staking is rapidly becoming a core pillar of blockchain network security and crypto asset management. As of July 2025, an estimated 42%[74] of crypto holders actively participate in staking, with Ethereum, Solana, and Cardano leading network engagement. Retail participation continues to rise, with 38%[75] of stakers leveraging pooled and delegated staking models to lower entry barriers and access rewards without running their own validators.

The economics of staking remain attractive, with average annual rewards across major platforms at approximately 6.8%, while some altcoins deliver yields exceeding 12%.[76] The ecosystem is also maturing with US$28 billion[77] worth of staked assets now protected by insurance and anti-slashing mechanisms, signalling growing institutional confidence.

Figure 4.6:

State of the Staking Ecosystem: Adoption, Returns, and Market Size (July 2025)

Global Staking Participation

42% of crypto holders actively participate in staking across major networks, with Ethereum, Solana, and Cardano leading the pack.

38% of retail stakers use staking pools and DPoS systems for easier access and lower fees.

Global Staking Participation

6.8% is the average annual staking reward across top platforms, with some altcoins offering 12%+ yields.

US$28B in staked assets are now covered by insurance and advanced anti-slashing protection.

Global Staking Landscape: Market Size & Ecosystem

US$800B+ (July 2025) is the combined market cap of all PoS networks.

US$159B (July 2025) Value of native tokens staked across the top 10 Proof of Stake projects.

US$20B+ (July 2025) Value locked in restaking platforms such as EigenLayer, where staked assets are reused to secure additional protocols and generate extra yield.

US$101B (July 2025) Market cap of liquid staking protocols like Lido and Rocket Pool.

US$18B+ (July 2025) Market cap of DeFi yield farming strategies, where users supply or lock assets in liquidity pools to earn rewards and trading fees, often leveraging liquid staked tokens.

Sources: Coinlaw Staking Statistics, Token Terminal Staking market cap, Coingecko Crypto Categories Market Cap, all accessed in July 2025

[74] Coinlaw, July 2025
[75] Coinlaw, July 2025
[76] Coinlaw, July 2025
[77] Coinlaw, July 2025

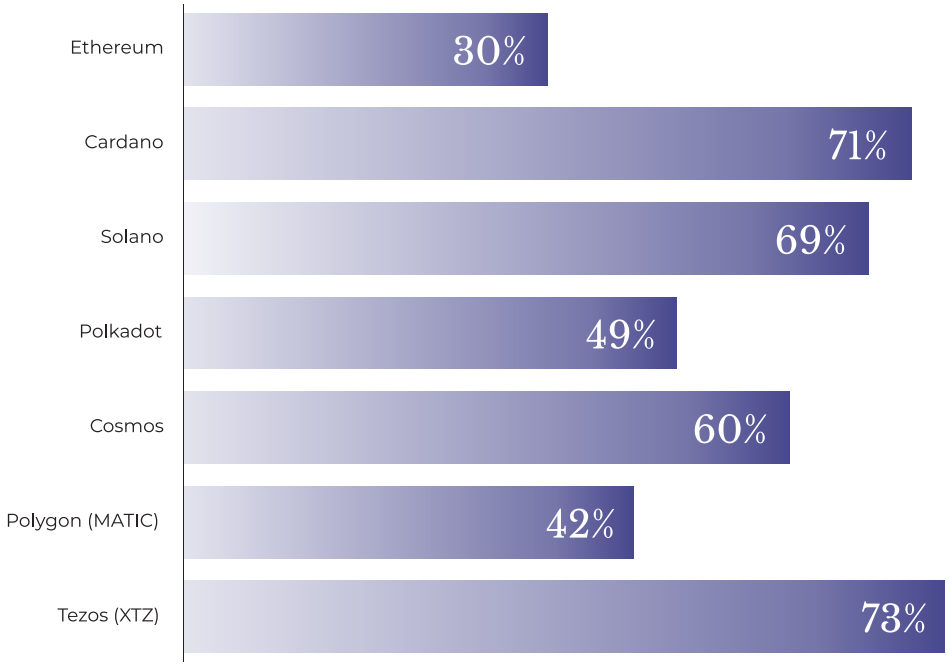
In terms of market structure, PoS networks collectively represent over US$800 billion in market capitalisation. Within this, native tokens staked across the top 10 PoS projects account for roughly US$159 billion, while liquid staking protocols like Lido and Rocket Pool now comprise over US$101 billion in market cap. Emerging restaking platforms such as EigenLayer are locking more than US$20 billion in reused staked assets, and DeFi yield strategies leveraging staked tokens contribute another US$18 billion to the market. Together, these dynamics illustrate how staking is fast evolving from a network security function into a multi-layered financial ecosystem underpinning PoS networks, decentralized apps and DeFi.

4.4.1 Staking Participation on Major PoS Networks

The scale of staking activity is growing. Across leading PoS blockchains, participation rates (the share of circulating supply staked) are substantial. For example, around 30% of Ethereum's ETH supply is staked by July 2025, alongside 69-73% of tokens in high-engagement networks like Solana, Cardano and Tezos.

Figure 4.7:

Global Staking Participation Rates Across Major Blockchain Networks (July, 2025)



Source: CoinLaw, 2025

These high participation levels indicate that staking is now becoming a mainstream behaviour among crypto holders.

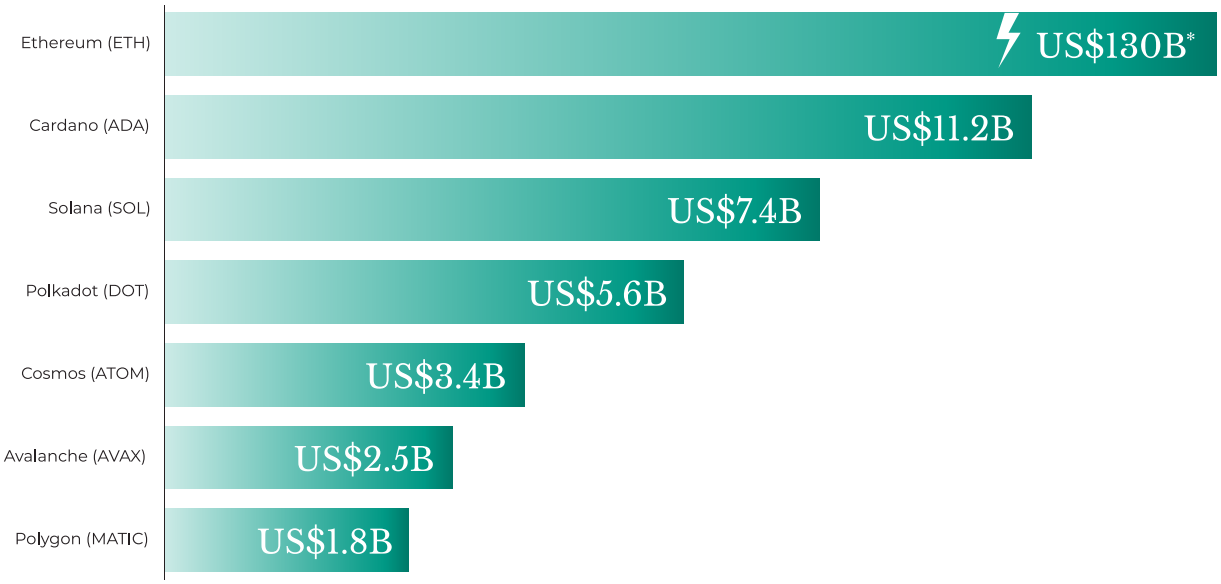
4.4.2 Leading PoS Networks by Staked Value

In dollar terms, the total value of crypto assets being staked has been growing. Staked asset concentration in PoS networks continues to be heavily dominated by Ethereum, which accounts for approximately US$130 billion in staked value as of July 2025. Cardano, Solana, and Polkadot follow at a distant second tier, highlighting the strong network effects of early PoS adopters. Cosmos, Avalanche, and Polygon demonstrate the growing diversity of PoS ecosystems, with their combined staked value underscoring the role of interoperability and application-specific chains in expanding the staking landscape. This distribution reflects both network maturity and the pace of adoption of staking mechanisms across the broader crypto market.

Ethereum stands out in absolute staking value, which is driven by several reinforcing factors. First, Ethereum anchors the largest smart contract ecosystem, hosting DeFi, tokenization, and stablecoin activity at scale. This breadth of use cases makes ETH a productive asset widely held across retail, institutional, and treasury portfolios. Second, institutional adoption has accelerated following the launch of spot ETH ETFs in the U.S. which, while not yet staking directly, have increased ETH's long-term investor base. Third, Ethereum benefits from the most mature liquid staking infrastructure, such as Lido, Rocket Pool, and exchange-based solutions like Coinbase cbETH, which allows capital to participate in staking while remaining liquid for DeFi and collateralized uses. And finally, ETH's total market capitalisation (Around US$ 450 billion in July 2025) dwarfs most other tokens. Even with a lower staking ratio (about 30% of supply), the absolute dollar value staked is far higher.

Figure 4.8:

Top PoS Blockchain Networksby Total Staked Assets (July 2025)



*Ethereum's staking ecosystem remains robust with 35.7M ETH staked (around 30% of its total supply), representing approximately US$130B in staked assets as of July 2025.

Source: CoinLaw.io, 2025

Staking yields vary by network and over time but generally fall in the mid-single digits annually for large cap PoS networks such as Ethereum, Cardano, and Solana. In 2025, the average annual staking reward across top platforms is about 6-7%.[78] Some smaller or newer networks offer higher promotional yields (10-15%)[79] to attract validators, whereas mature chains like Ethereum have more modest rates (about 3–4% APR[80] for validators in mid-2025).

Table 4.4:

Case Study: PostFinance — National Bank Integrating Crypto Staking

A. PostFinance: Launching ETH Staking for Mass Adoption

Strategic Focus Overview:	PostFinance, Switzerland's government-owned bank, has introduced Ethereum staking services to its 2.7 million customers, representing nearly a quarter of the country's population. This marks one of the largest-scale institutional staking rollouts in Europe.
Key Moves:	• Launch of ETH staking service integrated into PostFinance's existing digital banking platform. • Targeted at retail users, enabling seamless access to staking without technical setup. • Built in partnership with regulated crypto infrastructure providers to ensure compliance and security.
Regulatory Implication:	As a state-owned bank, PostFinance's move reinforces Switzerland's position as a leader in regulated crypto adoption. The launch highlights how clear frameworks under FINMA can enable traditional banks to integrate staking into mainstream financial products, creating a template for other state-backed or regulated banks in Europe.

Source: Cointelegraph, 2025

[78] Coinlaw, July 2025
[79] Coinlaw, July 2025
[80] Coinlaw, July 2025

Case Study: Revolut — Expanding Retail Access to Staking in Europe

B. Revolut: Integrating Crypto Staking into its Super-App

Strategic Focus Overview:	Revolut, the London-based digital bank, has steadily expanded crypto staking to retail users as part of its mission to build a comprehensive financial super-app. In February 2023, Revolut launched staking services in the U.K. and EEA, making Ethereum (ETH), Polkadot (DOT), Cardano (ADA), and Tezos (XTZ) available to over 25 million customers. Building on this, in July 2025, Revolut extended staking to Hungary, offering ETH and DOT to further penetrate Central and Eastern Europe's growing crypto market.
Key Moves:	• **February 2023**: Initial launch of staking in the U.K. and EEA covering ETH, DOT, ADA, and XTZ for over 25 million users. • **July 2025**: Expanded staking to Hungary with ETH and DOT, prioritising jurisdictions with favourable regulatory clarity. • Integrated staking into its custodial super-app interface, lowering the entry barrier for retail investors.
Regulatory Implication:	Revolut's phased rollout highlights how regulatory clarity drives staking adoption in retail Fintech platforms. Early launches in the U.K. and EEA leveraged emerging crypto frameworks, while the Hungary expansion signals a strategy of aligning staking products with compliant E.U. jurisdictions ahead of full MiCA implementation.

Sources: Fintech Magazine, 2023; CoinDesk, 2025

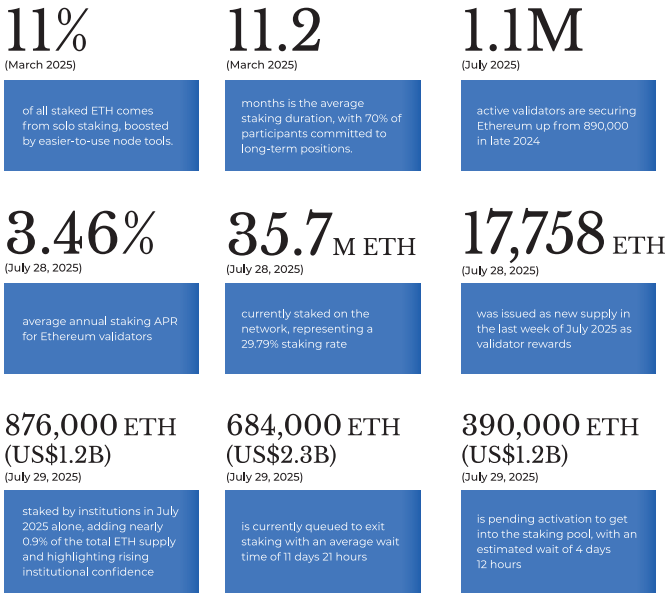
Table 4.5:

Case Study: Ethereum Staking Adoption Rise and Market Outlook

Ethereum continues to anchor the global staking landscape, with 35.7 million ETH staked as of July 2025, representing nearly 30% of total supply. Validator participation has surged, surpassing 1.1 million active validators, up from 890,000 in late 2024, reflecting the network's growing decentralization. Solo staking now accounts for 11% of all staked ETH, supported by improved node tools that are making self-validation more accessible to individual users.

Institutional participation has emerged as a key growth driver, with 876,000 ETH staked by institutions in July 2025 alone, signalling increasing confidence in staking as a yield-bearing and network-supporting activity. The staking queue reflects continued demand, with 684,000 ETH waiting to exit and 390,000 ETH pending activation, highlighting the dynamic flow of capital within the ecosystem.

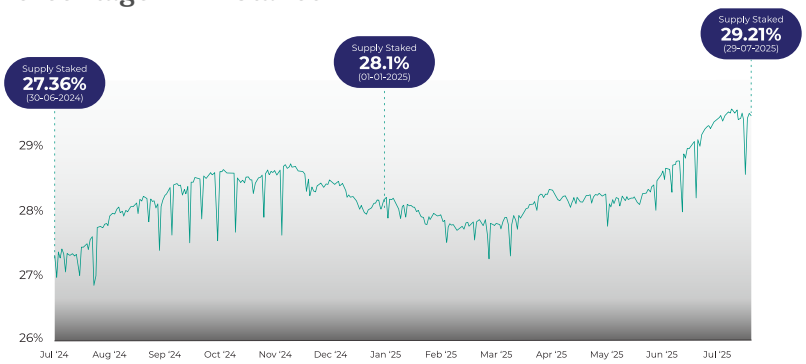
Ethereum Staking 2025: Key Milestones and Market Outlook



Sources: Coinlaw, 2025; EBunker, 2025; Ethereum News, accessed July 2025

The percentage ETH Staked chart underscores the steady rise in the proportion of ETH supply being staked, climbing from 27.36% in mid-2024 to over 29.2% by July 2025. This sustained growth demonstrates Ethereum's strong staking demand and signals increasing market confidence in ETH as a yield-bearing asset, particularly amid a rising price environment. As more ETH is locked into staking contracts, circulating supply tightens, potentially exerting upward pressure on prices and reinforcing Ethereum's store-of-value narrative alongside its utility as a network token.

Percentage ETH Staked



Source: Ethereum Validator Queue, accessed July 28, 2025

Market Outlook

For network security, higher staking participation translates into a broader validator set and enhanced decentralization with reduced attack vectors. The Ethereum Foundation has announced that it is considering staking a portion of its ETH reserves amidst increasing regulatory clarity. This signals a potential strategic shift in managing its assets, which was around 268,774 ETHs in January 2025.

This trend highlights a feedback loop where price appreciation drives more staking, which in turn affects ETH's supply dynamics, network resilience, and its acceptance as a key collateral asset across the digital asset ecosystem.

4.4.3 Factors Affecting the Adoption of Staking Solutions

The evolution of staking services in the first half of 2025 reflects a convergence of regulatory clarity, institutional adoption, and technological innovation, while also being shaped by emerging trends such as participation of banks in Staking, and the use of ETH as a treasury asset. Below are some of the key trends affecting the adoption of staking services:

- **Regulatory Clarity and Institutional Participation**
  Regulatory clarity is emerging as a major catalyst, with frameworks like the E.U.'s MiCA, Hong Kong's SFC guidance, U.S. SEC's clarifications on Protocol Staking, and the U.K.'s classification of protocol staking outside securities law encouraging compliant growth. This has fuelled a surge in institutional staking demand, highlighted by Ethereum's activation queue consistently reaching 300,000–350,000 ETH, as well as a shift towards regulated, custodial staking platforms. At the same time, regulatory uncertainty persists in the U.S. around newer product structures, as seen in the SEC's ongoing delays[81] in approving Ethereum staking ETFs for BlackRock and Bitwise[82], underscoring that important policy gaps remain.

- **Licensed Banks offering Staking Services**
  Licensed banks are beginning to integrate staking into their offerings. Licensed banks such as Sygnum Bank, SEBA bank, and PostFinance in Switzerland, Anchorage Digital in the U.S., provide institutional-grade staking services. These offerings allow clients to earn yield on digital assets while benefiting from regulatory safeguards, segregation of assets, and professional custody standards. The inclusion of staking-as-a-service by licensed banks who provide custody of digital assets shows how institutional demand is reshaping staking markets, bridging digital asset innovation with regulated infrastructure.

- **ETH Treasuries and Non-Dilutive Yield**
  Another emerging driver is the rise of Ethereum as a digital asset treasury reserve. DAOs, protocols, and corporates are increasingly holding ETH on balance sheets and staking it to generate non-dilutive yield. As of September 2025, Strategic ETH Reserve data[83] shows 4.99 million ETH held in strategic reserves, worth about US$22.9 billion. This represents 69 participants and roughly 4.1% of the total ETH supply. Unlike equity issuance or debt financing, staking rewards provide sustainable income without diluting ownership or creating liabilities.

[81] Cryptoslate, 2025
[82] Mitrade, 202
[83] Strategic ETH Reserve, accessed September 2025

- **Technological Innovation and Capital Efficiency**
  Technological innovation continues to enhance capital efficiency through liquid staking and restaking platforms such as Lido and EigenLayer, while macro market dynamics are driving demand for predictable yield as traditional interest rates remain subdued. However, persistent challenges remain. Technical risks, including smart contract vulnerabilities, de-pegging of staking derivatives, and interoperability issues, pose threats to platform resilience.

- **Market Volatility and Adoption Barriers**
  Market volatility adds another layer of complexity. The rapid growth of Ethereum's validator exit queue to 684,000 ETH (worth US$2.3 billion) during July 2025 illustrates how price surges can accelerate staking outflows and affect yield dynamics. At the same time, limited institutional-grade infrastructure in emerging markets and retail staker education gaps are slowing broader adoption. Against this backdrop, the ability to balance innovation with risk management and regulatory alignment will define the trajectory of staking services globally.

Table 4.8:

Staking Market Activities

Quarter	Entities	Activity	Description
Q1 2025 (Jan - Mar)	Trezor & Everstake	Partnership	Trezor integrated Solana staking via a partnership with Everstake, allowing users to stake SOL directly from Trezor hardware wallets.
	Bedrock, Binance	Launch	Bedrock's BR token launch achieved a 9653% oversubscription on Binance Wallet IDO, reinforcing community-driven Bitcoin staking initiatives.
	Bedrock	Launch	Introduced PoSL protocol and BR airdrop checker, aiming to boost liquidity in Bitcoin staking.
	PostFinance	Launch	Swiss government-owned PostFinance launched Ether staking for its 2.7 million customers, extending staking access to roughly a quarter of Switzerland's population.
	Rakurai	Funding	Secured US$3M for building Solana staking infrastructure, focusing on validator optimisation and institutional tools.
	Northstake & Lido	Partnership	Northstake to adopt Lido's stVaults, providing stETH access to ETF issuers.
	Acre	Funding	Bitcoin staking platform Acre raised funds at a US$60M token valuation to scale decentralized BTC staking infrastructure.
	Bitwise	Acquisition	Acquired Attestant, a leading Ethereum validator and staking service provider, to expand institutional ETH staking.
	Everstake	Certification	Achieved vital SOC 2 Type 1 certification as Ethereum staking grew by 74%, bolstering institutional trust in validator security
	Credix Finance	Funding	Raised US$8M to launch a staking-integrated credit marketplace, leveraging tokenized yields to back real-world asset lending.
Q2 2025 (Apr - Jun)	EigenLayer	Funding	Raised US$70M from a16z to launch an off-chain verifiability platform, strengthening restaking infrastructure for Ethereum.
	Lido & Maple Finance	Partnership	Partnered to offer stablecoin loans backed by liquid staking tokens (stETH), merging staking yield with credit markets.
	Mega Matrix	Treasury Strategy	Approved allocation of Bitcoin and Ethereum as treasury reserve assets, with a focus on staking ETH holdings for yield generation.
	Turtle Club	Funding	Secured US$6.2M to develop an on-chain liquidity distribution protocol integrated with staking yield strategies.
	Solv Protocol	Launch	Announced the first Shariah-compliant Bitcoin yield offering in the Middle East, targeting institutional BTC adoption.
	Sol Strategies	Funding	Raised US$500M to expand SOL holdings and boost Solana staking infrastructure, targeting validator and yield optimisation.
	Coca & Everstake	Partnership	Launched an Ethereum staking product offering up to 10% APR, targeting retail and institutional clients.
	BingX	Launch	Introduced StakeStone Launchpool to unlock staking and cross-chain liquidity solutions.
Q3 2025 (Jul - Aug)	Decibel	Launch	Decibel, an on-chain trading protocol, started operations on the Aptos devnet, combining spot trading, perpetual futures and yield strategies into a single interface.
	CoinShares	Launch	CoinShares launched a new ETP with staking yield across Europe.
	Revolut	Launch	Revolut restarted crypto staking services for its customers in Hungary after pausing for a couple of weeks.

4.5 Future Outlook: The Next Phase of Staking Evolution

Staking is entering a phase where market dynamics and regulatory clarity are reinforcing each other to create a more mature, sustainable ecosystem. Several themes are shaping the trajectory:

- **Regulatory Convergence and Standardisation**
  Jurisdictions are moving from ambiguity to clarity, laying down consistent rules that integrate staking into existing financial services and/or crypto assets perimeters. The E.U.'s MiCA framework anchoring staking-as-a-service under custody licensing has enabled institutional inflows, with Ethereum staking deposits in the E.U. surging by 28% in 2025 to US$90 billion as platforms aligned with Article 75 compliance. Similarly, the U.K.'s phased approach, starting with its January 2025 statutory instrument and culminating in FCA DP25/1, demonstrates a template for balancing innovation with investor protection.

- **Expansion of PoS Networks and DeFi Ecosystems**
  The rapid growth of Proof-of-Stake protocols and their energy efficiency is fuelling a new wave of decentralized applications and DeFi products built on these networks. This development is expected to impact token economics: as network usage and application demand increase, underlying coin prices are likely to appreciate, intensifying the trade-off between staking for yield and maintaining liquidity for participation in DeFi or trading. With the rise of liquid staking tokens, this trade-off is increasingly managed by allowing staked assets to remain usable within DeFi, though it also links validator security more closely to broader market cycles. This dynamic could create cyclical pressures as investors move between staking for yield and unstaking for liquidity, which in turn influences validator incentives and the overall security of the PoS networks.

- **Infrastructure Scaling and Capital Efficiency**
  Market activity in 2025 highlights a strong focus on scaling infrastructure for advanced staking models. EigenLayer's US$70 million raise to enhance Ethereum restaking verification and Acre's US$4 million fundraise at US$90 million valuation to build decentralized BTC staking infrastructure reflect a pivot to enterprise-grade solutions. The rise of liquid staking and restaking, exemplified by Lido and Maple's Q2 2025 partnership on stETH-backed stablecoin lending, is unlocking capital efficiency while prompting regulators to examine derivative risks.

- **Staking as a Yield-Bearing Asset Class**
  Ethereum's activation and exit queues consistently reaching 300,000–350,000 ETH, underscore rising demand for predictable yield in a low-rate macro environment. The SEC's May 2025 clarification that protocol-level staking is not a securities offering, alongside pending Ethereum ETF staking proposals from BlackRock and Bitwise, signals a path for staking to become a core yield-bearing asset class integrated into mainstream financial products.

- **Uneven Global Adoption**
  While hubs such as the E.U., U.K., U.S., U.A.E., Switzerland, Hong Kong, and Singapore are setting structured regimes, lagging jurisdictions underline the fragmentation risk. India and Brazil have only imposed tax treatment on staking returns without operational frameworks, while Saudi Arabia and Qatar have not initiated regulatory or tax regimes, highlighting the uneven pace of global adoption.

The evolution of staking over the next phase will be shaped by the interaction between regulatory clarity, network growth, and capital allocation dynamics. For regulators, the priority will be to extend emerging frameworks beyond custodial staking to address derivative models like liquid staking and restaking. As Proof-of-Stake networks expand and host more DeFi applications, supervisors will need to ensure that increasing token value and yield competition do not create systemic risks or undermine network security. Building standards around asset segregation, liquidity management, and disclosure for both traditional and derivative staking products will become central to policy design.

For market participants, the growth of PoS ecosystems and rising coin valuations will create a natural tension between locking assets for staking yield and keeping liquidity for trading and DeFi activity. Staking service providers, custodians, and infrastructure providers will need to innovate around flexible staking models while meeting stricter regulatory expectations. Networks themselves may have to adjust staking economics to balance validator incentives with user demand for liquidity, especially as price surges drive cycles of staking and unstaking.

5 Decentralized Finance & On-Chain Lending

5.1 Introduction

Decentralized finance has been fast evolving from a niche experiment to a fast-growing global system, with adoption expanding across geographies, user groups, and digital infrastructures. The ecosystem is no longer confined to early adopters or niche communities, it is rapidly becoming a mainstream channel for financial activity. As per Coinlaw's 2025 statistics[84] on DeFi adoption, DeFi has grown into a truly global phenomenon with 312 million active users worldwide in Q2 2025, spanning 88 countries. 47 million monthly active users now interact with Ethereum-based DeFi applications, while 25 million new users have been onboarded via Layer-2 networks such as Arbitrum and Base. These scaling solutions have lowered transaction costs and broadened access, enabling more seamless participation for users across markets. The demographic profile points to a generational shift in financial services. 61% of DeFi users are under the age of 35, highlighting how younger, digitally native populations are driving adoption. 39% YoY growth in first-time DeFi users entering via mobile wallets, demonstrates that DeFi is embedding itself into the daily digital habits of consumers.

> " Institutions are leaning toward TradFi which is tokenized, regulated finance. Retail users are powering DeFi which is open, global, permissionless. These two paths will converge. We're building infrastructure for that convergence, where you can have regulatory-grade oversight and DeFi-level flexibility on the same stack."
>
> **Richard Teng** - CEO, Binance

Figure 5.1:

DeFi vs Traditional Banking: Key Metrics Snapshot (2025)

Metric	DeFi	Traditional Banking
Average transaction fee	**US$1.07** on L2	**US$9.40** per bank wire (est.)
Time to finalize/settle	**3.6 seconds**	**~28 hours** for international wire
Average yield (savings/ staking & lending)	**8.2%** average across DeFi staking/lending	**2.1%** average global savings rate
High-range stablecoin lending yield	**14%** (select protocols)	**1.9%** avg 1-yr fixed deposits (U.S.)
Security losses/ fraud (H1 2025)	**US$1.1B** exploits & protocol hacks	**US$2.8B** fraud losses (U.S. banks)
Leading exploit/ fraud type	**52%** of DeFi-related breaches occurred due to smart contract vulnerabilities.	**97%** of banking fraud involved account takeovers or unauthorized transactions.

Source: Coinlaw, 2025

While DeFi remains smaller in scale compared to the US$370 trillion in global banking assets, its operating metrics highlight its growing importance. Average transaction fees on Layer-2 networks are barely US$1.07, compared to nearly US$9.40 per international bank wire, and settlement times are measured in seconds rather than days. Yields are also markedly higher, an average of 8.2% across DeFi staking and lending, compared with 2.1% for global savings deposits and 1.9% for U.S. fixed deposits.

[84] Coinlaw, 2025

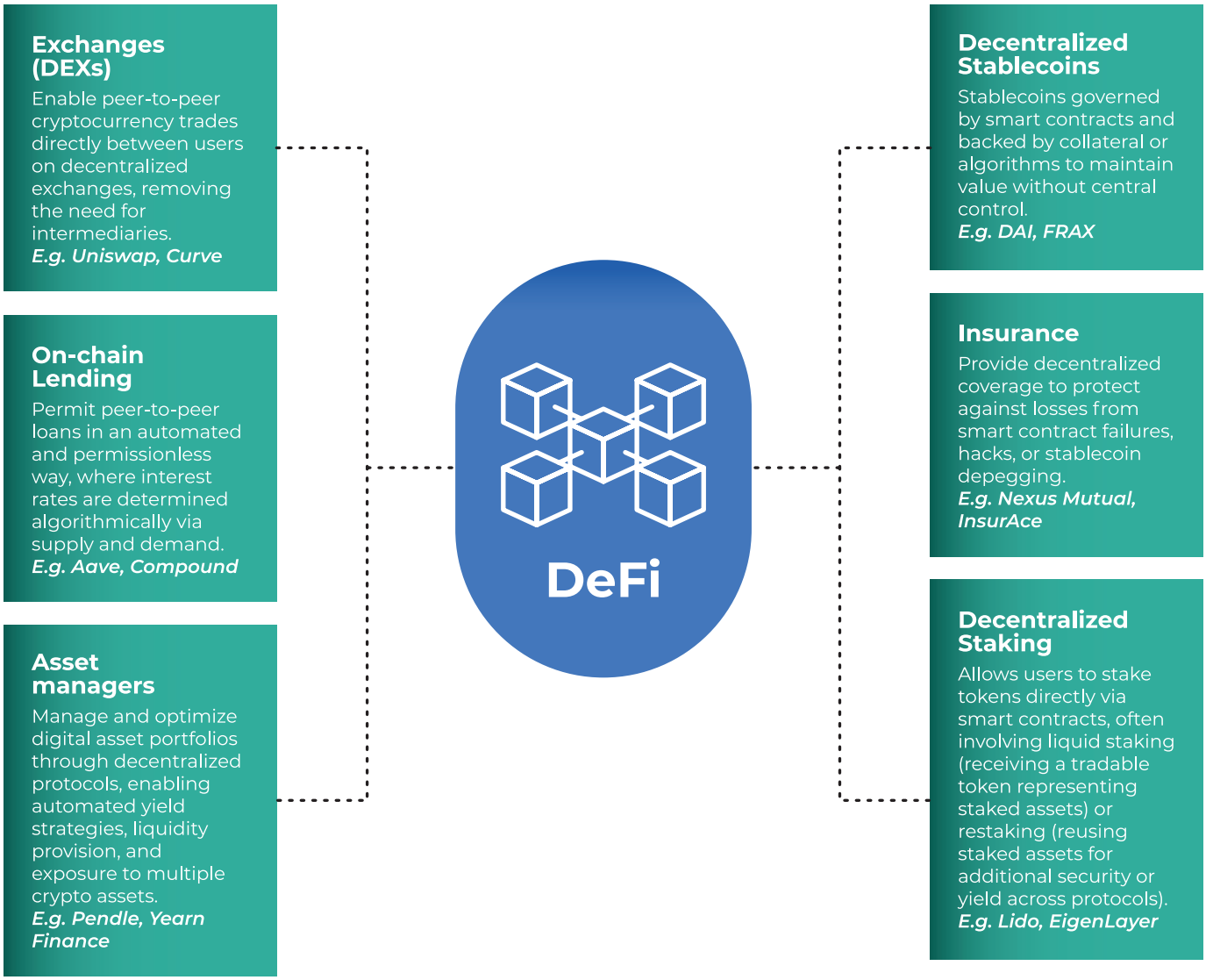
At the same time, the risks are real and distinct. DeFi lost US$1.1 billion in protocol hacks and exploits in the first half of 2025, with over half of breaches tied to smart contract vulnerabilities. In comparison, U.S. banks reported $2.8 billion in fraud losses over the same period, primarily from account takeovers. This contrast underscores that while both systems face vulnerabilities, DeFi's risks are concentrated in technical code and protocol governance, rather than in identity or account management.

5.1.1 Overview of the DeFi Ecosystem

DeFi refers to a broad ecosystem of financial services built on blockchain networks, using self-executing smart contracts instead of traditional intermediaries. These on-chain financial platforms, commonly referred to as DeFi protocols, mirror many functions of traditional finance, but in an open, permissionless, and automated environment. Unlike CeFi platforms, which custody user funds and rely on institutional trust, DeFi protocols allow users to retain control of their assets and transact peer-to-peer with transparency provided by the public ledger.

Figure 5.2:

DeFi Ecosystem: Key Sectors and Use Cases (illustrative, not exhaustive)



Sources: CCAF DeFi Navigator, 2025; GFTN Analysis

The DeFi ecosystem comprises several interlinked sectors, each replicating and extending core financial services through smart contracts:

- **Decentralized Stablecoins**: Stablecoins such as DAI and FRAX are governed by smart contracts and backed by collateral or algorithmic mechanisms to maintain a stable value. They serve as the settlement layer of DeFi, facilitating lending, trading, and payments while reducing exposure to crypto volatility.
- **On-Chain Lending**: Platforms such as Aave and Compound enable users to lend and borrow digital assets in a permissionless, automated manner. Borrowers post collateral to secure loans, while lenders earn yield on their deposits. Interest rates are dynamically set through algorithms balancing supply and demand. On-chain lending provides a transparent, peer-to-peer credit market, allowing users to unlock liquidity without selling their holdings, and has become a cornerstone of the DeFi sector.
- **DEXs**: Protocols like Uniswap and Curve allow users to trade cryptocurrencies directly, without centralized intermediaries. Using AMM mechanisms, DEXs provide continuous liquidity and transparent pricing, making them a vital infrastructure layer for token swaps and price discovery.
- **Asset Management Protocols**: Platforms such as Yearn Finance and Pendle automate yield strategies, liquidity provision, and portfolio management. By pooling assets and executing algorithmic investment strategies, they lower the barriers for individuals to access sophisticated, diversified DeFi strategies.
- **Decentralized Insurance**: Protocols like Nexus Mutual and InsurAce provide coverage against risks unique to DeFi, such as smart contract exploits, stablecoin depegging, or exchange hacks. This emerging sector is critical in building trust and mitigating risk for participants engaging in decentralized markets.
- **Decentralized Staking**: Protocols like EigenLayer allow users to allow users to reuse staked assets as collateral across multiple networks, generating extra yield. Liquid staking platforms like Lido give participants flexibility by issuing tradable tokens that represent their staked positions, integrating staking more deeply into the broader DeFi ecosystem.

Together, these sectors form a self-reinforcing system: stablecoins enable trading and lending, lending underpins liquidity, DEXs provide marketplaces, staking secure networks, asset managers optimise yields, and insurance mitigates risks. On-chain lending sits at the heart of this DeFi ecosystem, linking capital supply and demand while ensuring liquidity circulates throughout DeFi.

5.1.2 State of the DeFi Ecosystem

A commonly used measure of the scale and activity within DeFi is TVL, which captures the total dollar value of digital assets committed to DeFi protocols—whether for lending, staking, trading, or liquidity provision. TVL provides a proxy for both user adoption and the depth of capital supporting decentralized applications.

As shown in the figure 5.3, DeFi experienced a sharp expansion between 2020 and late 2021, peaking at over US$177 billion in November 2021. This rapid rise was driven by strong inflows into lending markets, the popularity of yield farming strategies, and the broader bull market in crypto assets. The subsequent decline through 2022–2023 reflected the impact of market downturns, and the collapse of several centralized players operating under the guise of DeFi platforms that eroded confidence in the sector. By early 2025, however, TVL had rebounded strongly, reaching over US$140 billion in July 2025, supported by the growth of liquid staking, the recovery of major assets such as ETH, and renewed institutional interest in on-chain credit markets.

This trajectory underscores both the volatility and resilience of DeFi. While sensitive to broader market cycles, the ecosystem has continued to rebuild and innovate, with lending and staking protocols now accounting for the largest share of locked value.

Figure 5.3:

DeFi Total Value Locked (TVL)Across Blockchains (Apr 2018–Jul 2025)

Source: DefiLlama, accessed July 2025

Figure 5.4:

State of the DeFi Ecosystem: Total Value Locked Across Chains, Use-cases, Protocol (August 7th 2025)

US$138.10B Total Value Locked in DeFi (All Chains)

US$82.68B Total Value Locked in DeFi (Ethereum)

DeFi Categories by TVL: Capital Allocation Across Major DeFi Use Cases

US$70.93B	US$69.81B	US$22.43B	US$11.60B
Liquid Staking	On-chain Lending	Decentralized Exchanges	Direct Yield Platforms
US$4.77B	**US$238.98M**	**US$197.23M**	**US$8.49M**
Yield Aggregators	On-Chain Insurance	Synthetic Asset Platforms	Uncollateralized Lending

Top DeFi Protocols by TVL: Leading Platforms in Lending, Staking, Restaking, and More

US$34.89B	US$32.52B	US$17.47B	US$7.49B	US$5.58B
AAVE Lending	**LIDO** Liquid Staking	**EIGEN LAYER** Restaking	**PENDLE** Yield	**UNISWAP** DEX

Source: DefiLlama, accessed Aug 2025

Note: The overall DeFi TVL (US$138.1B across all chains) is measured at the blockchain level. In contrast, the category breakdown shows how assets are allocated across different DeFi use-case categories. Because assets can be used in multiple ways on the same chain, for example, tokens staked in one protocol may also be re-used as collateral in another. Due to this, the same value may be counted more than once, in different DeFi protocols. This "multiple counting" explains why the sum of individual use-case TVL is larger than the total DeFi TVL across all chains.

Major DeFi protocols like Aave (lending) and Lido (liquid staking) lead in TVL, each exceeding US$30 billion in locked assets. As these figures indicate, DeFi has grown into a substantial sector within the digital asset landscape. This growth has been fuelled by the proliferation of innovative financial primitives on blockchain (such as automated market makers, algorithmic stablecoins, and collateralized lending platforms) and by users seeking yield opportunities outside traditional banking.

5.1.3 DeFi Adoption Patterns Across Markets

The 2025 Global Crypto Adoption Index[85] highlights a clear divide between advanced and emerging economies in how DeFi is being adopted. In the overall index, large economies such as India, the United States, Brazil, and Nigeria dominate the top ten. Importantly, the DeFi value received rankings within this index show that many emerging markets are among the most intensive users of DeFi. India and the United States hold the top two spots, but countries such as Nigeria (3rd), Indonesia (4th), Brazil(5th) and Vietnam (6th) are close behind, reflecting strong grassroots adoption driven by demand for alternative savings, lending, and cross-border payment channels.

Table 5.1:

The 2025 Global Crypto Adoption Index Top 20

Country	Overall index ranking	DeFi value received ranking
India	1	1
United States	2	2
Pakistan	3	10
Vietnam	4	6
Brazil	5	5
Nigeria	6	3
Indonesia	7	4
Ukraine	8	8
Philippines	9	13
Russian Federation	10	9
United Kingdom	11	12
Ethiopia	12	7
Bangladesh	13	14
Turkiye	14	22
Korea, Rep.	15	24
Yemen, Rep.	16	21
Thailand	17	15
Venezuela, RB	18	37
Japan	19	16
Argentina	20	29

The 2025 Global Crypto Adoption Index Top 20, adjusted by population

Country	Overall index ranking	DeFi value received ranking
Ukraine	1	4
Moldova	2	14
Georgia	3	5
Jordan	4	1
Hong Kong SAR, China	5	6
Vietnam	6	10
Latvia	7	7
Montenegro	8	3
Venezuela, RB	9	52
Slovenia	10	16
Estonia	11	11
Yemen, Rep.	12	29
Cambodia	13	46
Armenia	14	56
Singapore	15	13
Finland	16	8
Belarus	17	39
Korea, Rep.	18	48
Kyrgyz Republic	19	47
Portugal	20	9

Source: Chainalysis, 2025

[85] Chainalysis, 2025

When the index is adjusted for population, the leadership shifts further toward smaller economies. Countries such as Jordan, Montenegro, Ukraine, and Georgia rank in the top five on DeFi value received relative to their population size. This demonstrates that, on a per-capita basis, some smaller economies are experiencing far deeper DeFi penetration than larger markets. In these jurisdictions, DeFi often fills structural gaps in local financial infrastructure, offering access to dollar-denominated assets, remittance channels, and lending opportunities that may be limited in the domestic banking system.

By contrast, advanced economies like the United States, Japan, and the United Kingdom rank highly in absolute terms but lower when adjusted for population. This suggests that while these markets contribute large institutional pools of capital to DeFi, the intensity of adoption across their retail populations is lower compared to smaller or emerging economies.

For policymakers, this divergence underscores two important points. First, emerging markets are at the forefront of DeFi usage, which means risks such as stablecoin dependence, exposure to liquidation cascades, and consumer protection gaps are concentrated in countries with less supervisory capacity. Second, capital-heavy advanced markets remain critical nodes of institutional liquidity provisioning, linking DeFi adoption in smaller economies to global credit and investment flows.

5.1.4 Systemic Relevance of On-Chain Lending

While DeFi encompasses a wide spectrum of use cases (ranging from decentralized exchanges, derivatives, liquid staking, stablecoins, and structured products to novel primitives like prediction markets), this chapter focuses primarily on on-chain lending for below reasons:

- **Market Concentration and Scale**: On-chain lending is one of the most established and systemically significant use cases within DeFi, with top 5 protocols, Aave, Morpho, SparkLend, JustLend, and Kamino Lend, together accounting for 70-75% of total TVL in lending protocols. This concentration highlights both the maturity of the sector and the systemic importance of a few dominant protocols.
- **Regulatory Relevance**: Lending models concentrate key prudential risks, such as collateral valuation, leverage, liquidity mismatches, and liquidation cascades, that echo challenges in traditional banking. These risks have already manifested in failures of centralized lenders (e.g. Celsius, BlockFi, Voyager) and have drawn regulatory scrutiny.
- **Linkages to Global Systemic Finance**: On-chain lending is no longer an isolated crypto market phenomenon; it increasingly interacts with broader financial plumbing in three ways:

1) Balance Sheet Transmission: Institutional actors are now experimenting with on-chain collateral such as tokenized MMFs (e.g. BlackRock with Securitize[86]; Franklin Templeton with DBS[87], etc.). When tokenized RWAs (e.g, tokenized T-bill, tokenized MMFs, etc.) are used as collateral in on-chain lending, price declines can automatically trigger liquidations, forcing rapid sales of the tokens and redemptions of the underlying securities. These redemptions can lead to cash sales in traditional markets, pushing prices lower even further, which in turn triggers forward on-chain liquidations. The result is a self-reinforcing loop that transmits and amplifies volatility from DeFi into the broader financial system.

2) FX and Cross-Border Transmission: The two largest dollar stablecoins, USDT and USDC, together account for around 85–90%[88] of the stablecoin market. This dominance means that most DeFi loans are effectively dollar-denominated. On Aave[89], for instance, users deposit assets like ETH or BTC as collateral (e.g. 10 ETH worth $4,000 allows borrowing up to $3,200 at an 80% loan-to-value ratio). The borrowed assets are typically stablecoins such as USDC, USDT, or DAI, making DeFi credit dollarised in practice, even though the underlying collateral is crypto. This embeds U.S. monetary policy spillovers into emerging markets, where borrowers take on stablecoin-denominated debt. Aave accepts major USD stablecoins, USDC and PYUSD[90], for supply/borrow and, where enabled, as collateral, reinforcing the dollar-denominated nature of DeFi credit and linking on-chain lending to off-chain cash/T-bill markets. DeFi lending rates for USDC/USDT are set by protocol mechanics (utilisation/supply-demand). When the Fed raises rates, investors find off-chain T-bill/MMF yields more attractive, so they pull stablecoins out of DeFi or demand higher on-chain rates. Central-bank research[91] shows DeFi rates are volatile and can be partly disconnected from policy rates, but there are channels of transmission through opportunity cost and arbitrage.[92]

[86] Nasdaq, 2024
[87] DBS, 2025
[88] Stablecoin Insider, 2025
[89] Coinmarketcap, 2022
[90] The Block, 2025
[91] Banque de France, 2024
[92] SSRN Paper, 2025

3) Interbank Settlement and Tokenized Deposits: Hybrid CeDeFi models (e.g. Coinbase and Morpho collaborations[93], Aave and Ant Digital collaboration[94], JPM Coin[95], Partior's partnership with SBI Shinsei[96]) demonstrate how tokenized deposits and wholesale lending are getting into regulated banks' balance sheets. When these settlement layers connect with on-chain rails, they touch systemic infrastructures such as RTGS systems, payment rails, and collateral management frameworks. As banks and Fintechs start routing tokenized deposits and collateral through permissioned on-chain environments, the boundary between DeFi and CeDeFi blurs, making interbank settlement exposed to smart-contract and market risks.

By focusing on on-chain lending trends, we examine the most important DeFi category for policymakers, given its combination of micro-level risks, such as collateral volatility and liquidation cascades and macro-financial linkages, including dollar spillovers, institutional balance sheet exposures, and connections to systemic infrastructure components.

5.2 On-Chain Lending Taxonomy

On-chain lending has evolved into multiple models and platforms, each with distinct mechanics and use cases. Broadly, DeFi lending protocols can be categorised by how loans are originated and collateralized:

- **Over-Collateralized Money Markets**: These are by far the most common form of On-chain lending. Protocols like Aave and Compound operate pool-based lending markets where users deposit assets into liquidity pools and others borrow from those pools by posting collateral. Interest rates are determined algorithmically based on supply and demand for each asset in real-time. Borrowers must typically over-collateralize their loans (e.g. depositing US$150 of collateral to borrow US$100) to account for the volatility of crypto assets. If the value of a borrower's collateral falls below a required ratio, the protocol automatically liquidates the collateral to repay the loan, ensuring lenders remain whole.
- **Decentralized Stablecoin Lending**: A special subset of over-collateralized lending is the creation of decentralized stablecoins through collateralized debt positions. The prime example is MakerDAO, where users lock volatile crypto (e.g. ETH) in a smart contract and borrow a stablecoin (DAI) against it. This is essentially on-chain lending where the borrower mints new DAI (a loan) while their collateral is held until repayment.
- **Undercollateralized and Peer-to-Peer Lending**: In contrast to the pooled, over-collateralized approach, some platforms attempt to offer loans with lower collateralization or none at all, usually by incorporating identity or trust off-chain. Protocols like Maple Finance, TrueFi, and Goldfinch facilitate under-collateralized loans primarily for institutional borrowers, where creditworthiness is assessed through means such as borrower whitelists, legal agreements, or staking by third parties who vouch for the loans.
- **Flash Loans**: A uniquely blockchain-native lending model is the flash loan, which are unsecured loans with no collateral, but they exist only within the duration of a single blockchain transaction. Borrowers can take millions of dollars in a flash loan instantaneously, provided they repay it (plus interest) within the same transaction block. If they fail to do so, the entire transaction (and loan) is reverted as if it never happened. A smart contract issues the loan, authorises the borrower to execute one or more operations (e.g. arbitrage, collateral swaps, liquidations), and automatically enforces repayment of the principal and fee before the transaction is finalised. If repayment isn't met at any step, the entire sequence is atomically reverted, i.e. no funds leave the lender, and the transaction is discarded (the borrower only loses gas fees). Flash loans enable complex arbitrage, refinancing, and liquidation strategies, allowing borrowers to leverage large sums of capital for short intervals of time.

[93] Morpho, 2025
[94] Crypto News, 2025
[95] The Block, 2025
[96] Ledger Insights, 2025

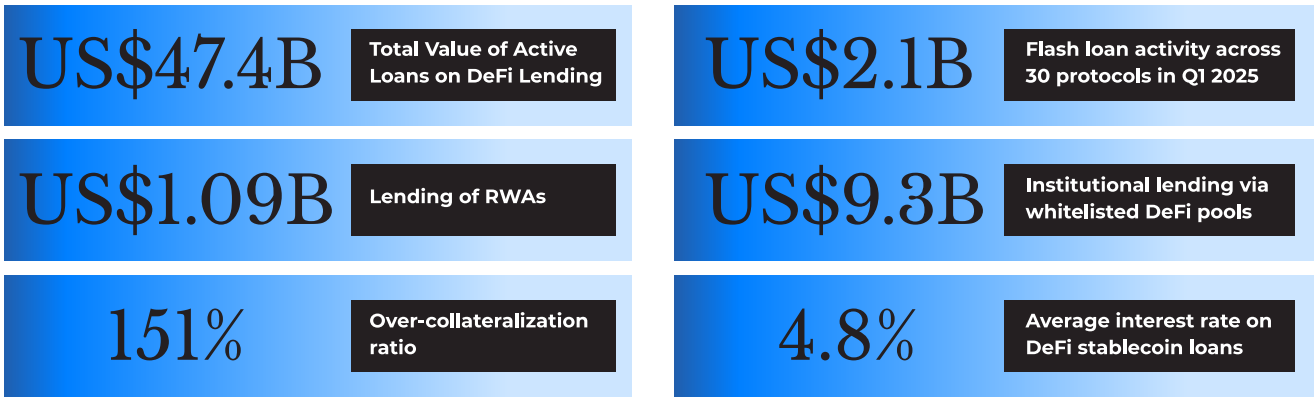
- **Liquid Staking and Re-Staking**: Although not lending in the traditional sense, liquid staking protocols (e.g. Lido) and emerging re-staking services (e.g. EigenLayer) have introduced new dimensions to on-chain yield generation that intersect with lending. In liquid staking, users stake cryptocurrency (like ETH) to secure a network and receive a tokenized representation of that stake (staked ETH) which can then be used in DeFi. Re-staking goes further by allowing staked assets to be pledged to secure other protocols (leveraging the same collateral multiple times). These mechanisms expand the collateral base available in DeFi and blur the lines between pure lending, staking, and other yield strategies. They have grown rapidly (liquid staking alone accounts for over US$70 billion TVL, the single largest DeFi category), indicating how interwoven on-chain lending and staking yield strategies have become.

5.2.1 The Evolution of On-Chain Lending

By September 2025, the DeFi lending market had grown into a sizable segment of DeFi, with active loans reaching US$47.4 billion[97]. Institutional adoption has accelerated, with lending via whitelisted pools surpassing US$9.3 billion[98], a 60% increase from last year. At the same time, lending against real-world assets has expanded to US$1.9 billion[99], led by tokenized treasuries and receivables. Risk practices are also evolving. Over-collateralization ratios have declined from 163% in 2024 to 151% in 2025, reflecting that more sophisticated risk engines are enabling improved capital efficiency while still maintaining conservative buffers.

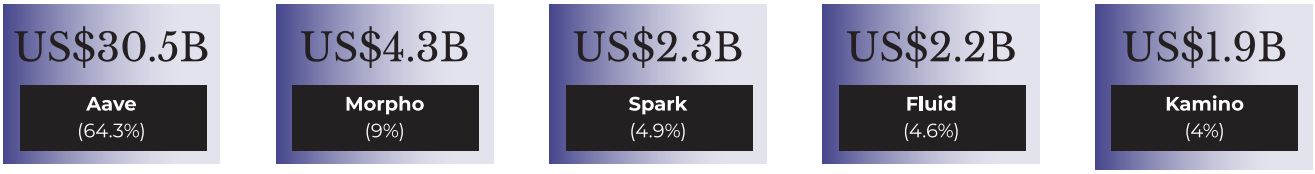
Figure 5.5:

On-Chain Lending Landscape: Market Size, Usage, and Leading Protocols (September 2025)



DeFi Lending Protocols Usage Trends: Across Top 10 Projects

Top DeFi Lending Protocols by Active Loans: Value and Market Share In Lending



Sources: Coinlaw, 2025; Token Terminal, accessed September 2025

[97] Token terminal, accessed September 2025
[98] Coinlaw, 2025
[99] Coinlaw, 2025

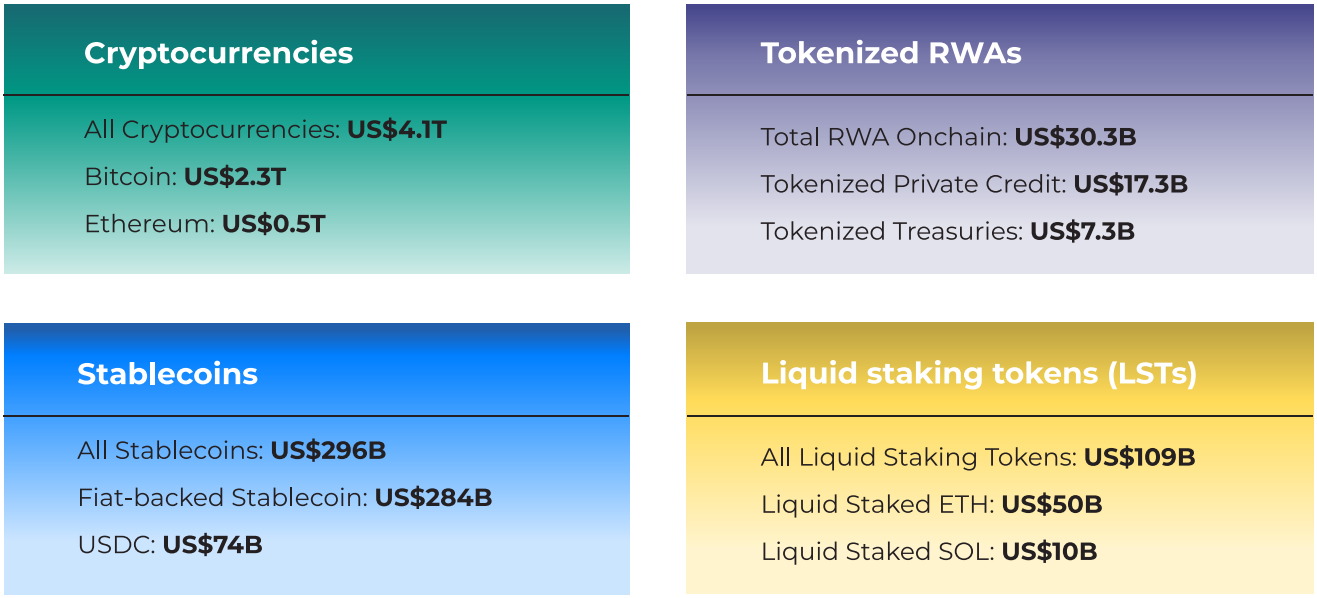
User engagement is steady, with almost 346,000 monthly users, generating close to 490 million transactions in the past year. Yet the market remains highly concentrated, with Aave alone accounting for 64% of outstanding loans, far outpacing the next ranked players like Morpho, Spark, Fluid, and Kamino. These trends signal that DeFi lending is becoming both more efficient and more intertwined with traditional finance. The balance between efficiency gains and stability safeguards will define how far on-chain credit can scale in the years ahead.

5.2.2 Collateral Evolution in DeFi Lending

DeFi lending collateral has been expanding beyond crypto-native assets such as cryptocurrencies and stablecoins, liquid staking tokens (LSTs), to tokenized RWAs.

Figure 5.6:

Collateral Types for DeFi Lending



Sources: Coingecko, accessed September 2025; RWA.xyz, accessed September 2025

Recent market developments include - Aave's Horizon pilot for tokenized treasuries[100], Flux Finance's use of tokenized U.S. government securities[101], Centrifuge's real-world assets infrastructure for off-chain assets[102], and Maple's integration of liquid-staked ETH[103] and MakerDAO's $1 billion[104] Tokenized Treasury Investment. This broadens funding sources and attracts institutional participants. It also imports familiar traditional-finance risks, such as price volatility, interest-rate and duration risk, liquidity and redemption constraints, and questions around legal ownership and custody.

[100] Blockonomi, 2025
[101] Hexn, 2025
[102] The defiant, 2025
[103] Maple, 2025
[104] Binance, 2024

Table 5.2:

Collateral types in DeFi and associated risks

Collateral type	Value proposition	Key Risks
Cryptocurrencies (BTC, ETH, etc.)	Deep on-chain liquidity; composable with many protocols; easy to price and liquidate.	High price volatility and correlation; liquidation cascades.
Stablecoins (USDC, USDT, etc.)	Price-stable collateral; tight spreads; widely used funding leg for loans.	Peg breaks/run risk; issuer transparency and blacklist /sanctions controls; reserve concentration at a few banks.
Liquid staking tokens (stETH, weETH, etc.)	Better capital efficiency; highly liquid on major DEXs; large user base.	Depeg vs. underlying ETH; validator/ slashing risk; redemption/withdrawal queues can slow exits; basis/oracle risk
Tokenized RWAs (T-bills, MMFs, private credit, etc.)	Lower correlation with crypto price swings; predictable cash flows; institutional on-ramp.	Interest-rate/duration risk (for T-bills/ MMFs); redemption gates & cut-off times; legal/title & servicer risk (private credit/ Real Estate); slower/less continuous pricing (NAV or appraisal lag).

Source: GFTN Analysis

As the share of RWA collateral increases, the channels of risk transmission expand: stress can jump from crypto prices to sovereign debt markets, credit markets, and fund liquidity dynamics. Below are some examples of how the DeFi risks may spill over into traditional markets:

- **Tokenized Treasuries under rate stress**: A sharp rise in U.S. Treasury yields would lower the value of tokenized T-bills. In leveraged DeFi pools, automated liquidations could force large-scale sales of these securities. This feedback loop could spill over into the broader Treasury market, especially if exposures scale into the tens of billions.
- **Redemption gates and timing mismatches**: Tokenized money-market funds may impose redemption gates or cut-off times. If DeFi protocols liquidate collateral overnight but redemptions are only processed at day-end, mismatched settlement could generate losses, weaken confidence, and trigger broader runs.
- **Credit pools and servicer defaults**: In tokenized private-credit pools, unexpected defaults or servicer failures could delay recoveries. These delays would undermine confidence in the tokens as collateral, potentially spreading losses across interconnected DeFi protocols.

For regulators, the above examples highlight how DeFi exposures are no longer contained within the crypto ecosystem. As collateral increasingly shifts toward off-chain assets, stress events could transmit into sovereign bond markets, short-term funding markets, and credit portfolios.

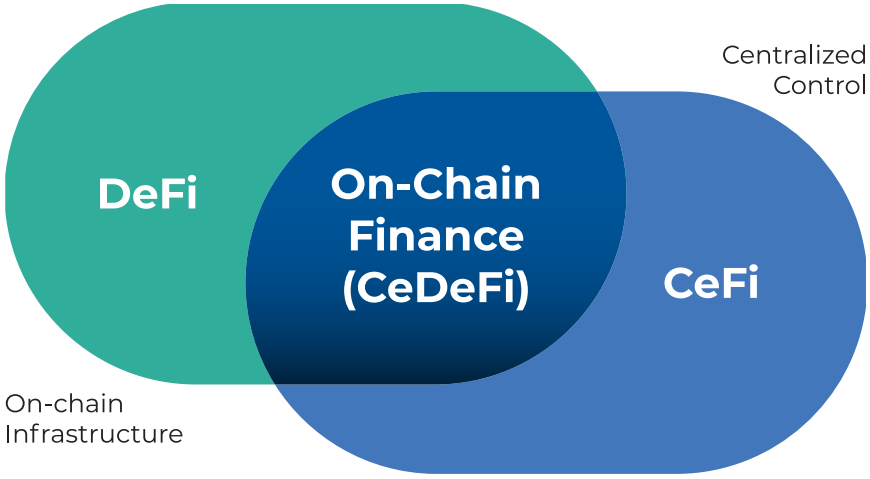
Regulators may need to consider clarifying supervisory boundaries, for example, whether securities regulators oversee the underlying tokenized asset while prudential authorities monitor lending risk. There is also a need to establish disclosure and reporting standards to track concentration, redemption terms, and default performance. This will ensure that DeFi's growing role as a parallel credit market does not become a source of systemic risk.

5.3 Evolution from CeFi to DeFi: Failures and Lessons

The rise of DeFi in the late 2010s and early 2020s coincided with a parallel boom in CeFi platforms offering similar yield and lending services. Companies like Celsius Network, BlockFi, Voyager Digital, and hedge fund Three Arrows Capital (3AC) attracted users by providing high-yield deposit accounts or arbitraged lending opportunities, but they operated as traditional intermediaries (taking custody of user funds and reinvesting them in the background). For a time, CeFi platforms were the main gateway for retail users to earn yield on crypto, since they abstracted the complexity of DeFi into a familiar account interface. However, the crypto market downturn of 2022 exposed fundamental weaknesses in many CeFi business models, resulting in a number of insolvencies, withdrawal suspensions, and wind-downs.

Figure 5.7:

The Financial Continuum Between DeFi and CeFi



Source: Journal of Financial Regulation, 2024

By mid-2022, a cascade of CeFi collapses shook the industry:

- **Terraform Labs**' UST stablecoin collapse triggered the failure of 3AC (a highly leveraged crypto fund), which in turn left lenders like Celsius and Voyager with huge holes in their balance sheets.
- **Celsius** froze customer withdrawals and ultimately filed for bankruptcy after it was unable to meet obligations, exacerbated by illiquid positions (e.g. staked ETH) and risky strategies.
- **BlockFi**, another major lender, incurred significant losses from its exposure to Three Arrows Capital (3AC) and, following the collapse of FTX, filed for bankruptcy.[105]

These failures were driven by poor risk management, opaque operations, and the contagion of a few centralized players all lending to each other. Crucially, they were not failures of truly DeFi platforms, but of centralized entities operating without adequate safeguards. Almost all of the crypto firms that went insolvent in the 2022–2023 crypto winter were CeFi services.[106]

In contrast, major DeFi lending protocols like Aave, Compound, and MakerDAO, which generally avoided off-chain leverage and operated through transparent, code-based rules, proved relatively more resilient overall. While CeFi failures stemmed from opaque risk-taking, maturity mismatches, and poor governance, DeFi protocols continued operating as designed, automatically liquidating under-collateralized positions and maintaining solvency throughout the downturn. For example, when crypto prices plummeted, DeFi protocols automatically liquidated under-collateralized positions as designed. The transparency of on-chain reserves and the programmatic enforcement of collateral ratios meant that systemic risk was better contained. Indeed, reports found that the major over-collateralized lending protocols had minimal bad debt during the worst of the downturn, whereas CeFi lenders were stuck with massive unpaid loans.[107]

> " Centralized lenders like FTX and BlockFi collapsed, but protocols like Compound, Aave, and MakerDAO have run continuously for five years without a hitch. If there was ever proof that self-driving financial protocols are resilient, that's it."

Haseeb Qureshi - Managing Partner, Dragonfly

[105] CNBC, 2022
[106] S&P Global, 2023
[107] S&P Global, 2023

5.4 Emergence of CeDeFi: Hybrid Approaches

As the industry internalised the lessons from CeFi's failures, a middle ground began to emerge: CeDeFi. CeDeFi refers to hybrid models that combine elements of decentralized infrastructure with some degree of centralized oversight or compliance. The goal of CeDeFi is to offer the best of both worlds, i.e. the efficiency, transparency, and innovation of DeFi alongside the risk management, customer protection, and regulatory compliance associated with CeFi.

In a CeDeFi model, a central entity (such as a regulated financial institution or a well-known crypto company) might provide an interface to DeFi services or even run its own DeFi-like platform, but with added controls. For example, a CeDeFi lending platform may use smart contracts to automate loans and yield generation, yet require users to pass KYC/AML checks, and have provisions for halting or modifying the protocol in emergencies. Coinbase's lending program is one illustration: Coinbase (a centralized exchange) has offered crypto-backed loans to clients while leveraging DeFi protocols like Morpho on the back end to source yield. Here, Coinbase acts as a gatekeeper and risk manager, but the liquidity and loan matching occur on decentralized platforms.

This raises debates on how decentralized such systems truly are. Indeed, projects that market themselves as DeFi but have centralized aspects are sometimes dubbed "**DINO**" – Decentralized In Name Only. Regulators are increasingly alert to DINO protocols that present themselves as decentralized to avoid regulation, while in reality a core team or entity holds significant power (e.g. control over upgrades or a privileged role in operations).[108]

Table 5.3

Comparative Overview of CeFi, CeDeFi, and DeFi

Parameter	CeFi (Centralized Finance)	CeDeFi (Centralized–Decentralized Finance)	DeFi (Decentralized Finance)
Definition	Refers to crypto-based financial services run by centralized entities.	Hybrid model where a central entity offers DeFi-like products but with some centralized control, compliance, and custody.	Financial services run entirely on decentralized protocols and smart contracts, with no central authority.
Examples	Anchorage Digital, Coinbase, Circle.	Coinbase(CeFi) offering of crypto-backed loans powered by Morpho(DeFi).	Uniswap, MakerDAO, Compound
Custody of Funds	Held by central entity (custodial).	Often hybrid, i.e. non-custodial for some assets, custodial for others.	Non-custodial (user controls private keys).
Regulatory Oversight	Mostly regulated in various jurisdictions.	Partially regulated. central operator can implement KYC/AML.	Minimal regulatory intervention; relies on protocol-level rules, pseudonymous participation.
Governance & Control	Fully centralized. Corporate governance structures (board, executives).	Centralized operational oversight (e.g., KYC/AML, whitelist management) with automated execution on-chain.	No central authority. Governed by smart contracts and DAO voting.
Transparency	Limited — internal audits and disclosures.	Higher than CeFi (on-chain activity visible), but some parts opaque on centralized platforms.	Full on-chain transparency (all transactions & code public).
KYC / AML	Mandatory.	Often mandatory for onboarding.	Rarely mandatory (unless front-end imposes it).
Smart Contract Risk	Low. Services not primarily run on-chain.	Medium. Uses smart contracts but with central oversight.	High. Entirely reliant on smart contracts' logic.
Counterparty Risk	High. User must trust the institution.	Medium. Central party exists but risks are mitigated by blockchain settlement.	Low. Trust in code rather than a single entity.
Scalability	High. Internal ledgers and databases scale easily.	Medium to high (depends on chain used).	Medium — limited by blockchain throughput and gas fees.
User Experience	Easiest for mainstream users.	Medium to high. DeFi features in the backend with centralized UX frontend.	Requires technical literacy and non-custodial wallet management.

Source: GFTN Analysis

[108] DeFining the American Spirit, 2025

Key characteristics that distinguish CeDeFi from pure DeFi and pure CeFi include:

- **Hybrid Custody**: CeDeFi platforms might allow users to retain control of funds via smart contracts (non-custodial), but a central party could still have certain controls (e.g. an emergency admin key or a permissioned access layer).
- **Regulatory Compliance**: CeDeFi by definition leans into compliance. Participants may be verified, transactions monitored, and certain activities restricted. A central operator can implement KYC/AML procedures and blacklists even as transactions are settled on-chain. This makes CeDeFi more palatable to regulators and institutions.
- **Governance and Control**: Instead of full decentralized governance by token holders, CeDeFi systems often have a traditional corporate governance overseeing the protocol's parameters and upgrades. Users benefit from professional risk management, but at the cost of some decentralization and censorship-resistance.
- **User Experience**: CeDeFi hides most of DeFi's complexity. Users interact with a familiar, account-based centralized app for sign in, view balances, and get customer support, while the DeFi provider executes the underlying transactions with smart contracts in the backend. This familiar UX (managed keys, fiat on/off-ramps, helpdesk) lowers the learning curve and reduces user error, making DeFi accessible to mainstream users without requiring them to manage wallets or gas settings.

Table 5.4:

Case Study: Coinbase Morpho Partnership for On-Chain Lending at Scale

A. Coinbase–Morpho: Bridging CeFi Institutions with DeFi Lending Infrastructure	
Strategic Focus	Coinbase has launched crypto-backed loans powered by Morpho in Jan 2025, bringing on-chain lending seamlessly into its main app. Users can potentially borrow USDC against their BTC holdings on Coinbase, with plans to expand collateral options. This partnership effectively bridges institutional-grade DeFi with a mainstream retail platform, making on-chain lending more accessible than ever.
Adoption & Scale	By the end of July 2025 (since its launch in Jan 2025), Coinbase's Morpho-powered lending has achieved remarkable growth: • **Over US$500M in Active Loans** through Coinbase's Morpho-powered lending, making it one of the largest institutional DeFi integrations to date. • **Over US$600M in Total Loan Originations**, reflecting rapid growth since the product launch. • **Over US$1B in Collateral Supplied** by Coinbase clients, underscoring strong institutional and retail demand for crypto-backed borrowing.
Regulatory Implication	Coinbase's use of Morpho highlights the **CeDeFi model**: blending regulated custody and client onboarding (KYC/AML under Coinbase) with decentralized liquidity and settlement (Morpho). This structure raises questions on supervisory oversight of hybrid platforms, particularly around securities classification, lending licences, and prudential safeguards.

Source: Morpho, August 2025

5.5 Regulatory Landscape and Challenges

Unlike traditional finance, where identifiable institutions can be licensed and supervised, DeFi's disintermediated, borderless architecture challenges regulatory frameworks built around intermediaries and national jurisdictions. As of 2025, approaches to DeFi regulation vary widely across jurisdictions, and significant gaps remain in the legal framework. Key challenges include determining who (if anyone) is accountable in a decentralized protocol, how to oversee software-driven financial services running 24/7 worldwide, and how existing laws apply to novel constructs like governance tokens and smart contracts.

5.5.1 Global Regulatory Approaches Across Jurisdictions

Table 5.5:

Global DeFi Regulatory Landscape (July 2025)

Jurisdiction	Regulatory Status	DeFi / On-Chain Lending – Rules, Proposals, and Regulatory Developments	Regulatory Body	Regulatory Approach
U.S.	Initial discussions	Series of multiple SEC Crypto Task Force roundtables (Mar–Jun 2025), culminating in a roundtable on DeFi in June 2025. In the DeFi roundtable, SEC Commissioner Hester M. Peirce stressed that publishing open-source code alone should not trigger regulation; SEC Crypto Task Force is further planning to host a series of Roundtables (around 10) across the U.S. Launch of "Project Crypto" (Aug 2025): reforming securities rules to support on-chain markets (token classification, exemptions, custody, "innovation exemption" for novel business models).	SEC, CFTC	Regulation-by-enforcement in practice until 2024; self-regulation proposals on record under new administration (2025).
U.K.	Under development	FCA (DP 25/1) proposes that truly decentralized DeFi activities should remain outside the regulatory perimeter, but where cryptoactives involve regulated activity and a clear controlling person is identifiable, the same obligations applied to trading platforms, intermediaries, staking, lending, etc., would equally apply to DeFi.	HM Treasury / FCA	Proportionate oversight focused on identifiable responsible persons.
E.U.	Initial discussions	MiCA does not explicitly regulate DeFi protocols, but applies where there is an identifiable service provider or issuer. ESMA/EBA Joint Report (Art. 142 MiCA) formally analyses DeFi and crypto lending/borrowing/staking and flags policy options for the Commission's review, i.e., monitoring now, potential future perimeter changes.	European Commission / ESMA / EBA	MiCA applies to intermediaries and identifiable persons; fully decentralized activities remain out of scope (for now).
Switzerland	In force	FINMA applies "same business, same risks, same rules": DeFi lending/credit activities fall under existing licensing if substance matches regulated intermediation. Projects are assessed economically, not technologically, for licensing (e.g. banks or securities dealers). FINMA enforces substance-over-form, including for lending/credit DeFi. Swiss DLT-Act enables tokenization infrastructure under FMIA. Additionally, a regulatory sandbox allows DeFi pilot experimentation under limited supervision.	FINMA	Activity-based licensing; regulated sandboxing for innovation.
Japan	In force	Introduction of CAISP licence for non-custodial platforms, including DeFi interfaces. Japan has established a formal DeFi Study Group, meeting every two to three months with representatives from the FSA, industry and academia to explore regulatory approaches for decentralized platforms and DeFi.	FSA	Formal licensing for non-custodial platforms.
Hong Kong	In force	SFC has signalled that DeFi trading platforms fall under SFO licensing (Type 7, CIS rules), and its 2025 "ASPIRe" roadmap includes regulatory controls over DeFi activity.	SFC (and HKMA for intermediaries)	Activity & conduct-based, licensing-centric.
Singapore	Partially in force	MAS has explicitly signalled that DeFi lending-of-token arrangements for retail customers are prohibited under the licensing framework. However, Project Guardian enables institutional DeFi pilots (tokenized bond issuance and tokenized asset lending) under regulated custody and risk controls. MAS has issued consultations on the future perimeter of DeFi licensing and supervision.	MAS	Activity & risk-based; strong retail safeguards; innovation via sandboxes/pilots.
U.A.E.	In force	VARA's Lending & Borrowing Services Rulebook (2025) prescribes licensing, liquidity, disclosure, client documentation and reporting obligations for VASPs engaging in lending/borrowing.	VARA	Prescriptive, activity-based licensing.

Jurisdiction	Regulatory Status	DeFi / On-Chain Lending – Rules, Proposals, and Regulatory Developments	Regulatory Body	Regulatory Approach
India	No formal regime	DeFi remains unregulated; No integration allowed between regulated traditional finance and unregulated DeFi. VDA service providers are covered under the Prevention of Money Laundering Act (PMLA) since March 2023.	RBI, SEBI	Unregulated.
Saudi Arabia	No formal regime	No legal recognition of DeFi; CMA developing framework, SAMA monitoring closely, exploring digital innovation; banks barred from crypto services.	SAMA, CMA, MOF	Unregulated.
Qatar	No formal regime	No direct DeFi regulation; framework focuses on tokenization of real-world assets.	QCB, QFCRA	Unregulated.
Brazil	No formal regime	While no dedicated DeFi regulation exists, the CVM engages with decentralized projects via regulatory sandboxes. Financial institutions, including banks, are piloting tokenized lending and decentralized liquidity models. Broader Virtual Assets Law (BVAL) applies to intermediaries for AML/KYC compliance.	Central Bank of Brazil, CVM	Unregulated.

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

Below, we outline the regulatory stances in major jurisdictions for DeFi.

- **United States**: U.S. regulators, until the end of 2024, mostly applied "regulation-by-enforcement" to crypto activities, pursuing cases against firms or founders (e.g. centralized exchanges, token issuers) rather than issuing DeFi-specific rules. However, 2025 has seen initial steps toward formal guidance. The SEC convened a series of Crypto Task Force roundtables on DeFi in the first half of 2025, where officials like Commissioner Hester Peirce cautioned that merely publishing open-source code should not automatically trigger securities regulation. There are discussions about clarifying the status of DeFi protocols under securities and commodities laws. Notably, the SEC launched "Project Crypto" in August 2025, aimed at reforming securities rules to better accommodate on-chain markets to address issues like token classification, custody of digital assets, and even exploring an "innovation exemption" for novel decentralized business models. Despite these moves, the U.S. has yet to enact comprehensive DeFi legislation.
- **United Kingdom**: The U.K. is actively exploring how to bring DeFi into its regulatory perimeter in a proportionate way. In early 2025, the FCA released Discussion Paper DP25/1, which suggests a threshold test for decentralization. The proposal is that truly decentralized DeFi arrangements, where no identifiable entity exerts control, should remain outside traditional regulation, similar to how open-source software might be treated. However, if a DeFi activity involves a "clear controlling person" or performs a regulated activity (like lending or deposit-taking) in substance, the same laws and obligations that apply to conventional financial intermediaries would apply to those responsible. In other words, if a protocol is decentralized in name only, U.K. regulators intend to treat it as centralized. This approach directly targets DINO protocols by focusing on the presence of an identifiable operator. The U.K. is still in the proposal stage, but the direction seems to be toward a **"same risk, same regulatory outcome**" principle, with careful consideration of how to enforce rules when governance is dispersed. The Bank of England and FCA's Digital Securities Sandbox[109] provides a controlled environment to adapt FMI law and rules for DLT-based market infrastructure, with the FCA stating it will draw lessons for the crypto asset market. In parallel, HM Treasury's crypto assets regime[110] (such as RAO and FSMA amendments[111]) will bring a wide set of crypto activities into the regulatory perimeter, to be implemented by the FCA. Together, these initiatives demonstrate U.K. authorities coordinating on potential legal and regulatory updates relevant to DeFi-adjacent activity.

[109] Bank of England, 2024
[110] Gov.UK, 2025
[111] FCA, 2025

- **European Union**: The E.U.'s MiCA which came into effect 2024–2025, largely sidesteps fully decentralized DeFi. DeFi protocols without an identifiable operator are not explicitly covered. However, MiCA did mandate European regulators (ESMA and EBA) to study DeFi and report on potential adaptations. In January 2025, a joint ESMA/EBA report under Article 142 of MiCA analysed DeFi lending, borrowing, and staking, outlining policy options for the European Commission's review.[112] The current stance is to monitor the DeFi market and possibly extend the regulatory perimeter later. If a DeFi application has a legal entity or individuals providing a service (for example, a front-end operator or a development company earning fees), E.U. authorities can apply existing financial or AML laws to those actors.

- **Switzerland**: Switzerland has been proactive in incorporating crypto into its regulatory framework, and this extends to DeFi. Swiss regulators (FINMA) apply the doctrine of "same risks, same rules".[113] In practice, if a DeFi lending service essentially performs the function of a bank or securities dealer (taking deposits and making loans, or facilitating trades), FINMA will assess it under existing licensing categories. The emphasis is on the economic substance over technological form.

- **Japan**: Japan has recently instituted a new category to address DeFi and other non-custodial services. In 2023–2024, Japan introduced the CAISP licence, which explicitly covers entities like DeFi platform interfaces that are not holding customer assets but facilitate peer-to-peer transactions. This was accompanied by the establishment of a formal DeFi Study Group under the Financial Services Agency (FSA)[114]. The study group, including regulators, industry, and academics, meets regularly to explore how Japan's regulatory regime should adapt to truly decentralized platforms. The FSA's current stance requires even non-custodial DeFi facilitators (like a web portal or an operator of a front-end for a lending protocol) to register and comply with certain standards, especially around consumer protection and AML.

- **Hong Kong**: Hong Kong's approach is to require DeFi platforms that facilitate trading of security-like tokens or investment products to get licensed under the SFO (Securities and Futures Ordinance). The SFC's 2025 "ASPIRe" roadmap (a policy agenda for virtual assets) explicitly includes developing regulatory controls for DeFi activity.[115] As of July 2025, enforcement and licensing are in the early stages, but the legal framework to supervise even decentralized platforms (through their creators or facilitators) is being put in place..

- **Singapore**: Singapore has taken a cautious but innovative stance on DeFi. The MAS distinguishes between retail and wholesale DeFi usage. On the retail side, MAS has prohibited licensed crypto firms from offering DeFi lending services to retail customers, viewing practices like yield farming or token lending as too risky for the general public under current rules. However, for institutional and wholesale market experimentation, MAS launched Project Guardian, which allows banks and investors to test DeFi protocols in a controlled setting (for example, tokenizing bonds and trading them on a DEX with regulatory guardrails). The result is a bifurcated approach: strict protection for retail, coupled with an open invitation for companies to explore DeFi's potential under the regulator's eye for the wholesale market.

- **United Arab Emirates**: The U.A.E., through the VARA, has established a detailed framework governing lending and borrowing services in the virtual asset sector.[116] VARA's Lending & Borrowing Services Rulebook (2025) prescribes strict requirements for licensing, liquidity management, client documentation, and reporting obligations for VASPs engaged in such activities. In parallel, ADGM's DLT Foundations Regulations (2023) provide a legal wrapper for DAOs/DeFi foundations in Abu Dhabi; however, DeFi businesses conducted from ADGM still require authorisation under the FSRA's Virtual Asset framework where regulated activities are performed. This reflects a prescriptive, activity-based licensing approach, ensuring that centralized and semi-centralized platforms operating in the U.A.E. adhere to robust compliance standards.

Overall, the regulatory landscape for DeFi remains uneven and is evolving. In the U.S. and E.U., supervisors are assessing the application of existing financial laws to DeFi and drafting targeted guidance. In more proactive jurisdictions (Switzerland, Japan, Hong Kong, Singapore, U.A.E.), authorities have begun tailoring or extending regulations to capture on-chain lending and similar activities, each with different focal points. This inconsistency creates challenges for DeFi developers and users: a protocol might be considered legal and unregulated in one country but deemed an unlicensed financial service in another. Such disparity also opens the door to regulatory arbitrage, where projects might jurisdiction-shop for a friendly home base.

International bodies like the **FATF** and **IOSCO** have called for closer monitoring of DeFi, particularly around money laundering risks, but implementation remains uneven across jurisdictions.

---

[112] EBA, ESMA Joint Report, 2025
[113] FINMA, 2021
[114] Cointelegraph, 2025
[115] SFC HK, 2025
[116] VARA Rulebook, 2025

According to the FSB report[117], stakeholders highlighted DeFi as a rapidly expanding segment that warrants close and continuous monitoring of market developments. Respondents in the report highlighted that as DeFi scales, vulnerabilities such as smart contract risks, market manipulation, and operational failures could become increasingly systemic. The report also emphasised the need for regulatory approaches that mitigate these risks without stifling innovation, ensuring that oversight frameworks evolve in step with technological and market advances.

FATF 2025 Targeted Update[118]: Status of DeFi-related regulatory implementation across jurisdictions

- Roughly half of surveyed jurisdictions that are more advanced on virtual-asset rules (48%; 47 out of 99) now require certain DeFi arrangements to register or licence as VASPs where a creator/owner/operator (or another party) exercises control or sufficient influence.
- Among the remaining 52 out of 99 jurisdictions that do not yet apply their VASP AML/CFT framework to DeFi entities, only 31% (16 out of 52) report taking preparatory steps (e.g. risk studies, industry engagement), while 42% (22 out of 52) report no specific action.
- Even where requirements exist, practical uptake is limited: of those 47 jurisdictions, only about 9% (4 out of 47) report registered/licensed DeFi entities, about 15% (7 out of 47) have taken supervisory/enforcement actions, about 2% (1 out of 47) have identified unregistered entities without action, and about 75% (35 out of 47) have not identified any such entities—underscoring how slowly implementation is progressing.
- FATF notes continuing challenges in applying the Standards to DeFi and plans a short DeFi-focused report in 2025/2026 (ecosystem updates, typologies, and best practices).

IOSCO DeFi recommendations (2023–2024): Scope and implementation status

- **Policy scope**: IOSCO's final DeFi policy recommendations are organised into six areas[119]. (1) Understanding DeFi arrangements; (2) Achieving common regulatory outcomes; (3) Identifying and managing key risks; (4) Clear, accurate, and comprehensive disclosures; (5) Enforcement of applicable laws; (6) Cross-border cooperation.
- **Implementation mechanism**: IOSCO established the Fintech Task Force – Implementation Working Group to coordinate adoption of the DeFi recommendations across member jurisdictions.
- **Progress tracking**: The FTF IWG conducted a 2024 survey of all IOSCO members to assess implementation progress and practical challenges.
- **Ongoing work**: IOSCO is analysing shared regulatory pain points and developing follow-up actions to encourage and support implementation of the DeFi recommendations.

5.5.2 Decentralization versus Regulation: Key Challenges

Regulating DeFi raises several fundamental challenges, stemming from the very features that make DeFi innovative. Authorities and lawmakers are confronting novel questions around accountability, technological enforcement, and the limits of existing legal concepts. Some of the most pressing challenges include:

Lack of Legal Personhood:

Traditional regulation assumes a regulated entity, i.e. a company or individual, who can be licensed, monitored or held legally liable. DeFi upends this by presenting platforms that are just code. If something goes wrong (e.g. a collapse of a lending protocol or a hack draining user funds), there is often no legal entity accountable. Some jurisdictions have floated the idea of recognising DAOs as legal persons (as Wyoming[120] in the U.S. has done), so that a protocol community could voluntarily register and assume a legal status. However, many DeFi communities are reluctant to register as legal entities, as legal structuring may dilute decentralization and introduce participant liability. The lack of a personhood or a domicile means users have little recourse if they suffer losses. This challenge is fundamental: it may require new legal constructs (perhaps treating developer teams or governance token holders as a collective "person") or creative approaches like targeting the interfaces (e.g. websites) that give access to protocols.

Global, 24/7 Operations Across Borders:

DeFi protocols are inherently global. A liquidity pool or lending market is accessible to anyone in any country by design. This breaks with the traditional model of financial regulation, which is jurisdictionally bounded. A user in France could borrow from a pool composed of lenders from Asia and South America, all mediated by a smart contract on a blockchain run by nodes worldwide. No single regulator

[117] FSB, 2025
[118] FATF, 2025
[119] IOSCO, 2024
[120] Global Fintech & Digital Assets, 2024

has a clear authority over that transaction. This global diffusion makes coordination essential: if country A tries to ban or block a DeFi protocol, it still may be accessible via country B or via direct blockchain interactions.

Additionally, DeFi operates **24/7/365** with no downtime or concept of closing hours, which strains regulators' monitoring capabilities and traditional market safeguards (like circuit breakers for crashes, which do not exist in DeFi markets). International regulatory bodies are starting to discuss cooperative frameworks for DeFi oversight, but achieving consensus is slow. In the meantime, some regulators focus on the touchpoints between DeFi and the local economy – for example, requiring crypto-to-fiat gateways (exchanges and banks) to blacklist transactions associated with unregulated lending platforms.

Immutable Code and Autonomous Operations:

One of the celebrated features of DeFi is that once a smart contract is deployed, especially if its admin controls are renounced, it can operate autonomously with immutable, censorship-resistant execution. But this poses a nightmare scenario for regulators: what if a contract is doing something illegal (for e.g. offering unregistered loans or facilitating money laundering) and there is no off-switch? With CeFi, a regulator can order a business to stop an activity or freeze assets; with DeFi, even the creators might be unable to halt the contract if it is truly immutable. This has led to debates about whether there should be mandated backdoors or "circuit breakers" in DeFi code for emergency use, a suggestion that DeFi purists vehemently oppose, as it undermines the trustless nature of DeFi. Immutability also means if a regulation changes (for instance, a new requirement to limit borrowing amounts or to exclude certain users), existing deployed contracts might not be upgradable to comply.

Regulators and industry face a structural gap. On-chain activities are governed by code, but they continue to fall within the scope of law. Going forward, we may see more projects adopt upgradable contract patterns (with multi-sig control by DAO governance) to allow tweaks for compliance, but this reintroduces some centralization.

In light of these challenges, regulators are in a delicate position: clamp down too hard and risk stifling innovation or driving it underground; take too soft a touch and risk market abuses or consumer harm. A likely scenario is the development of a more nuanced regulatory toolkit for DeFi. One that might include certification or safe harbour regimes for compliant DeFi protocols, international cooperation for oversight, and perhaps new legal definitions (like recognising algorithmic governance or giving legal status to on-chain actions).

Regulators and industry stakeholders' views on governing DeFi responsibly

" MiCA is not designed for decentralized protocols without intermediaries. Regulation today is tied to entities — issuers, service providers, custodians. If DeFi grows and causes harm, a new regulatory paradigm will be needed. Until then, we watch. If a crisis forces action, we may be stuck with suboptimal rules, better to prepare in advance, but only with a usable model."

Peter Kerstens - Advisor for Financial Sector Digitalisation and Cybersecurity, European Commission

" DeFi regulation is incredibly hard because the protocols are open-source and don't sit within any single jurisdiction, and that's at the heart of their extensibility and power. But we're starting to see serious thinking around how to efficiently regulate at the endpoints. You should not regulate the code, but you can gate who accesses it — through KYC, risk scoring, or whitelisted pools, and these regulations can be encoded at the connectivity layer."

Jason Rozovsky - Head of Legal & Policy, InterOps Labs

" Decentralization is not opposed to investor protection, but it is opposed to the regulatory philosophy of finding a single accountable entity. Regulators want one party to carry the responsibility, yet that creates a single point of failure. The challenge is to reconcile distributed accountability with effective regulatory oversight."

Joe Kohler - Chief Legal and Chief Operating Officer, Nethermind

" More and more, regulators are coming to us with questions like: what can we regulate in DeFi? What's technically enforceable? We help them understand the perimeter, not to ban it, but to govern it responsibly."

Lex Fisun - CEO & Co-Founder, Global Ledger

GFTN Survey Insights: DeFi & On-chain Lending

Survey Insight 5.1:

Regulatory Clarity on DeFi Risk Management

23%

Prudential standards for DeFi lending and liquidity pools were flagged by 23% of respondents as requiring immediate regulatory clarity, making it the second-highest ranked priority. This highlights rising concern around the risk management practices of DeFi protocols, especially those offering yield through liquidity provisioning or collateralized loans without traditional oversight.

Survey Insight 5.2:

Opportunities in Emerging DeFi Models

27%

New models for decentralized finance were cited by 27% of respondents as one of the most promising opportunities for digital assets over the next three years. This reflects a growing recognition of DeFi's potential to unlock open, permissionless financial services.

5.6 Future Outlook

The future of DeFi and on-chain lending sits at a crossroads of technological innovation, market maturation, and regulatory response. Despite the hurdles, there is a broad expectation that DeFi is here to stay as a fundamental component of the crypto economy, and its influence on mainstream finance is likely to grow. The coming years might bring entirely new paradigms in on-chain lending. One possible direction is creditworthiness on-chain, i.e. systems that let borrowers build reputation or link real-world credit data to their blockchain identity, enabling under-collateralized loans at scale. Another direction is the integration of RWA into DeFi lending. Already, there are experiments with tokenized real estate, invoices, or even trade finance assets being used as collateral in DeFi.

In the near future, we anticipate more clarity from regulators which, counterintuitively, could be bullish for DeFi's growth. Clear rules would give more mainstream investors the confidence to engage with on-chain lending, knowing the legal boundaries. Jurisdictions might introduce tailored licences for DeFi platforms or recognise DAO governance in legal terms. Regulatory frameworks are likely to coalesce around concepts discussed earlier: requiring identifiable CeDeFi gateways to enforce compliance, while perhaps carving out safe harbours for truly decentralized protocols (with transparency and self-governance standards). Some countries may compete to be DeFi-friendly hubs by offering sandboxes and clearer legal status for DeFi communities.

Artificial Intelligence is poised to become a major driver of innovation in DeFi, shifting parts of decision-making, risk control, and user experience from purely protocol-driven mechanisms to hybrid systems combining on-chain rules with adaptive intelligence. In practice, AI has already started to shape DeFi at three layers:

(i) Market Intelligence & Execution, where autonomous agents extend today's trading bots into lending agents that can optimise collateral management, liquidations, or stablecoin rebalancing without human intervention

(ii) Risk & Compliance Automation, where AI-enhanced monitoring can flag anomalous on-chain lending behaviour in real-time, such as early detection of wash trading or money-laundering patterns

(iii) Credit Scoring & Reputation Systems, where AI models applied to on-chain transaction history, wallet clustering, or off-chain credit data could generate decentralized credit scores, making under-collateralized lending more sustainable.

At the same time, AI introduces new forms of risks. The same AI tools that make DeFi more efficient and secure can also be misused. For example, autonomous agents could make it easier to extract profits from users by exploiting how transactions are ordered on blockchains (known as maximal extractable value). In extreme cases, malicious actors could create fully automated 'exploit bots' that identify and attack vulnerabilities in protocols without human involvement. Supervisors may increasingly need to treat AI-powered DeFi agents as systemic actors in their own right, warranting oversight comparable to large intermediaries in traditional finance.

Industry perspectives on the next phase of DeFi Innovation

" DeFi is evolving. The next phase includes agentic AI interacting with identity-secured wallets on permissionless ledgers. We're already building that — embedding Legal Entity Identifiers and verifiable credentials so AI agents can transact, audit, and govern themselves responsibly. This is the infrastructure for tomorrow's capital markets."

Frederik Gregaard - CEO, Cardano Foundation

" 'Send and Earn More' redefines the purpose of remittances by turning every transfer into an opportunity for financial growth. When beneficiaries don't need immediate access to their funds, those remittances can seamlessly transition into digital savings, earning value over time instead of sitting idle. This early-stage innovation bridges the worlds of payments and decentralized finance, showcasing how the next generation of remittances can evolve from simple money transfers to intelligent, value-enhancing financial experiences."

Joseph Cleetus - Vice President Business Transformation, Lulu Financial Holdings

" Chainlink has already enabled tens of trillions in onchain transaction value. What matters now is not just powering leading protocols like Aave and Lido, but enabling the secure, compliant, and seamless interoperability needed for institutional adoption. Chainlink's industry-standard oracle platform enables DeFi to directly connect with traditional finance, unifying both into a single global internet of contracts."

Niki Ariyasinghe - Head of Business Development, Asia-Pacific and Middle East, Chainlink Labs

Looking ahead, the future outlook for DeFi and on-chain lending is one of cautious optimism. The sector has evolved from a niche experiment to a multi-billion dollar market in just a few years. It has demonstrated the potential to make financial markets more accessible, efficient, and transparent. However, it has also highlighted new risks and forced a rethinking of regulatory paradigms. The coming chapter of this story will be about integration: integrating DeFi with traditional systems and centralized entities, integrating more complex real-world assets into on-chain form, and integrating safeguards so that the wild innovations of recent years can settle into reliable infrastructure. If the pioneers of DeFi and the stewards of regulation can find common ground, the result could be a financial system that is more inclusive, innovative, and robust – a true synthesis of the decentralized ethos with the lessons of centuries of finance.

6 Anti-Money Laundering & Know Your Customer Risks

6.1 Introduction

The proliferation of digital assets has been transforming the financial industry by offering unprecedented speed, transparency, and global access. However, this very efficiency and openness have also introduced new vectors for illicit finance, including money laundering, terrorism financing, and sanctions evasion. As early as 2018, the FATF formally recognised this risk, calling for urgent regulatory convergence around VASPs. In 2024, global penalties imposed on crypto firms for AML and KYC lapses exceeded US$5 billion, a 39% increase compared to 2023, with several landmark cases underscoring the growing seriousness of enforcement.[121]

While traditional financial institutions are long accustomed to complying with stringent AML/KYC mandates, digital asset players have, until recently, operated in regulatory grey zones, taking advantage of jurisdictional arbitrage, decentralized infrastructures, and anonymity-enhancing technologies. Regulatory responses have varied widely: some countries like Singapore and the European Union have created comprehensive, forward-looking frameworks that integrate crypto assets within mainstream AML legislation; others, such as the U.S. and the U.K., have extended legacy AML provisions to the crypto sector without introducing bespoke digital asset-specific rules.

From the perspective of regulators, the imperative is clear: to mitigate the misuse of crypto for financial crime while not stifling legitimate innovation. This requires a nuanced balance between enforcement, incentivising Regtech adoption, and cross-border cooperation. A well-structured AML/KYC regime for digital assets must ensure three critical outcomes:

1. That VASPs implement risk-based CDD and EDD where applicable.
2. That suspicious transactions are actively monitored, detected, and reported to national FIUs.
3. That privacy and decentralization concerns are addressed without compromising law enforcement capabilities.

6.2 Global AML/CFT Initiatives and Adoption Metrics

The FATF, the global AML standard-setter, has been instrumental in shaping how jurisdictions govern digital assets. Its 2019 update to Recommendation 15 defined AML/CFT obligations for VASPs, bringing them in line with regulated financial institutions.

In parallel, Recommendation 16 (Travel Rule) requires VASPs to collect and transmit originator and beneficiary information during virtual asset transfers, mirroring the SWIFT-based information exchange in traditional banking.

By mid-2025 in its sixth targeted review of implementation, FATF reported that among the 138 jurisdictions that had been assessed, compliance levels varied: 40 were found to be “largely compliant” and 68 “partially compliant” with Recommendation 15. (Figure 6.1)

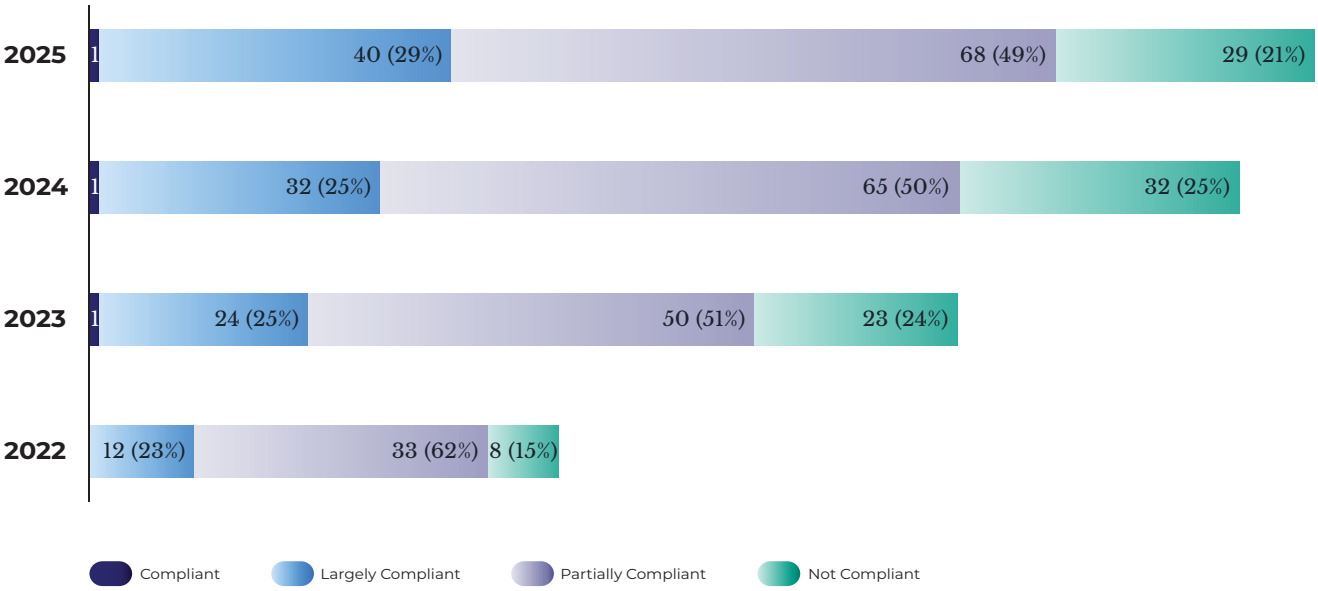
FATF’s compliance evaluations emphasise five core pillars for AML regulation in crypto:

1. **Licensing and Registration:** All VASPs must be registered or licensed and subject to AML supervision.
2. **CDD:** Standard KYC practices to verify identity and assess customer risk.
3. **EDD:** Triggered by high-risk scenarios, such as cross-border transfers or PEPs.
4. **Suspicious Activity Reporting (SAR):** Mandatory obligation to file suspicious transaction reports to domestic FIUs.
5. **Travel Rule Compliance:** Mandatory collection and secure transmission of transactor data for transfers above specified thresholds.

[121] CoinLaw, accessed September 2025

Status of Compliance with FATF Recommendation 15 (as of April 2025)

Figure 6.1:



Source: 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers' report by FATF, 2025

The global reporting still focuses heavily on compliance scores and headline legislation, but it is equally important to assess how AML obligations are being implemented at the protocol and wallet level. Recent industry surveys provide a clearer picture of this operational layer. Notabene's State of Crypto Travel Rule 2025 Report found that 100% of surveyed VASPs expect to be Travel Rule compliant by the end of 2025.[122] The report also highlighted a 431% YoY increase in VASPs blocking withdrawals until beneficiary information is confirmed, jumping from 2.9% in 2024 to 15.4% in 2025. Additionally, 19.8% of VASPs return deposits if the originator fails to provide the required Travel Rule data. Taken together, these data show that the success of AML/CFT oversight in digital assets does not rest only on national compliance scores or enforcement actions. It increasingly depends on the operational adoption of compliance tools across VASPs, protocols, and wallets.

Industry Perspectives on Embedding AML/KYC into Digital Asset Business Models

"We filter every transaction through risk checks — wallet screening, address reputation, transaction history. Banks rely on us for pre-transaction AML/KYC and rely on that to decide whether to process settlements. This is core to our OTC and payment partner operations."

Deng Chao - CEO, HashKey Capital

"Our AI systems handle AML and sanction screening, using LLMs to reduce false positives. Most of our effort isn't always in tech development — it's in structuring data governance, ensuring confidential data isn't improperly shared. The regulatory environment makes it harder to build shared models, even for clear public good like suspicious transaction detection."

Bjørn Krog Andersen - Chief Compliance Officer, Banking Circle

"We engineer all our products to ensure AML, sanctions screening, and payment controls apply as required by existing regulations. The only new risk was operational — 24/7 infrastructure and programmability. For regulators, it's about understanding risks and mitigations. If you are clear on both, regulatory dialogue is constructive."

Naveen Mallela - Global Co-Head, Kinexys by J.P. Morgan

[122] Notabene's 2025 Travel Rule Report, 2025

6.3 Jurisdictional Implementations

While FATF provides the blueprint, domestic regulators translate these guidelines into enforceable laws. The global implementation of AML/KYC frameworks for digital assets reflects a spectrum of regulatory maturity.

Jurisdictions such as the E.U., Singapore, Japan, Hong Kong, Switzerland, U.A.E., and Brazil have established full-spectrum, crypto-specific AML regimes. These frameworks require VASPs to be licensed, comply with CDD and EDD protocols, monitor transactions, and submit STRs. The E.U., under MiCA, and Singapore, via PSN02 (Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service), offer some of the most mature and detailed compliance expectations.

In contrast, countries such as the U.S., U.K., India, Saudi Arabia, and Qatar maintain AML controls via traditional financial crime statutes, such as the Bank Secrecy Act (U.S.) or India's PMLA, without a crypto-specific legislative framework. While STR and CDD mandates exist across all reviewed jurisdictions, gaps remain in licensing mandates, particularly for countries like the U.K., U.S., and India, where crypto asset service providers operate under broader financial entity designations.

Table 6.1:

AML/KYC Frameworks for Digital Asset Service Providers

Jurisdiction	Regulatory Body	Details
U.S.	FinCEN (MSB) & state regulators	Covered under BSA; not standalone crypto law
E.U.	European Commission & national authorities under MiCA	Crypto-specific regulations under MiCA
Japan	Financial Services Agency	Crypto-specific AML/KYC laws embedded in Payment Services Act And the Act on Prevention of Transfer of Criminal Proceeds
India	Financial Intelligence Unit – India	Covered under PMLA; no dedicated crypto AML law
U.K.	Financial Conduct Authority	Regulated under amended AML Regs; not crypto-specific law
Brazil	Central Bank of Brazil & Comissão de Valores Mobiliários	Crypto-specific AML regulation as per Law 14.478/2022
K.S.A	Saudi Central Bank & Capital Market Authority	Covered under traditional AML regulations
Switzerland	Swiss Financial Market Supervisory Authority	Crypto-specific AML compliance mandated via FINMA under AMLA
Singapore	Monetary Authority of Singapore	Crypto-specific regulations under PSN02 and AML Notice
U.A.E	Securities and Commodities Authority, Dubai Virtual Assets Regulatory Authority , Dubai Financial Services Authority	Crypto-specific AML framework under bespoke VASP laws
Hong Kong	Securities and Futures Commission	Crypto-specific VASP licensing rules introduced
Qatar	Qatar Financial Centre	AML applies only to QFC-licensed token activities; crypto banned otherwise

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

"Innovating cross-border payments is sensitive. Even if the technology has obviously potential in this field, an adequate mitigation of the enhanced risks to avoid money laundering, terrorist financing and sanctions circumvention is key and often challenging for market players"

Matthias Obrecht - Head, Market Analysis, FINMA

"Financial licensing is more complicated than, say, getting a driver's licence. It comes with responsibility, staffing, and compliance infrastructure. AML and KYC requirements may create duplication across providers, adding costs and frustrating customers. Singapore has shown how acceptance of streamlined digital identity, such as MyInfo, for KYC purposes can reduce this burden to some extent"

Tang Wei - Head of Public Policy, Southeast Asia and Greater China, Stripe

Table 6.2:

AML/KYC Compliance Obligations for Digital Asset Service Providers

Jurisdiction	Licensing VASPs	KYC/CDD required by law	EDD & transaction monitoring	STR reporting
U.S.	✗	✓	✓	✓
E.U.	✓	✓	✓	✓
Japan	✓	✓	✓	✓
India	✗	✓	✓	✓
U.K.	✗	✓	✓	✓
Brazil	✓	✓	✓	✓
K.S.A	✗	✓	✓	✓
Switzerland	✓	✓	✓	✓
Singapore	✓	✓	✓	✓
U.A.E.	✓	✓	✓	✓
Hong Kong	✓	✓	✓	✓
Qatar	✗	✓	✓	✓

CDD - Customer due diligence, EDD - Enhanced Due Diligence, STR - Suspected transaction reporting

✓ In place ✗ Does not exist

Sources: MiCA, 2025; PMLA guidelines for VASPs, 2023; Hacken, 2025; Sumsub, 2025; Gofaizen & Sherle, 2025; Lawrange, 2025; Legalbison, 2025; FSA, 2025; FCA, 2025; VARA, 2025; MAS, 2022; General Secretariat Deputy Directorate for Legal Affairs, Brazil, 2025; QFC, 2024; FINMA, 2025

Jurisdictional Case Studies: Country and Regional Approaches

Case Study: Singapore – Risk-Based Crypto AML Framework via MAS

Table 6.3:

A. Singapore: Supervisory Precision through Licensing and Risk-Based Enforcement	
Regulation:	AML/CFT regulations issued under the PSA, 2019, including Notices PSN01 and PSN02, and subsequently enhanced through MAS advisories and circulars (2021–2023).
Trigger:	The PSA was formulated based on FATF's 2015–2018 guidance on virtual assets and Singapore's domestic risk assessments. Following FATF's 2021 updates, MAS issued updated supervisory expectations to strengthen crypto AML enforcement.
Implementation & Scope:	DPT service providers must be licensed and comply with full AML/CFT requirements, including CDD, EDD, ongoing transaction monitoring, STR, and Travel Rule implementation. MAS supervises crypto AML on a risk-sensitive and activity-based model, enforcing differentiated expectations for exchanges, custodians, and intermediaries.

Sources: MAS - PSN01 & PSN02, accessed September 2025

Case Study: Singapore – Project Guardian Embeds AML in Digital Asset Innovation

B. Singapore: Supervisory Innovation through Embedded AML in Tokenized Finance	
Overview:	Project Guardian is a financial infrastructure initiative launched by the MAS in 2022. It explores the tokenization of financial assets and DeFi use cases within a controlled environment, with embedded AML/CFT modules as a core design pillar.
Trigger:	Rapid expansion of tokenized finance and DeFi posed challenges for traditional AML enforcement. MAS proactively addressed the risk of anonymity and illicit flows through architecture-level safeguards and programmable compliance.
Implementation & Scope:	Under Project Guardian, participating financial institutions and Fintechs must implement AML protocols at the protocol and smart contract level. Use cases are tested for KYC automation, real-time suspicious activity alerts, and data-sharing mechanisms that comply with the Travel Rule. MAS collaborates with global regulators and standard-setters to harmonise risk controls across jurisdictions. The initiative is a global benchmark in combining compliance-by-design with innovation enablement.

Source: MAS Project Guardian, 2023

Case Study: European Union – Integrated Oversight via MiCA & AMLR

C. European Union: Twin Frameworks of MiCA and AMLR for Unified Compliance	
Regulation:	The MiCA Regulation (adopted 2023) and the AMLR (finalised 2024), both applicable across the E.U.'s 27 Member States.
Trigger:	Fragmented treatment of crypto assets across Member States and shortcomings under AMLD5 highlighted by FATF and ECB assessments drove the need for a harmonised regime.
Implementation & Scope:	Under MiCA, CASPs must be authorised and meet governance, disclosure, and conduct obligations. AMLR subjects CASPs to full AML/CFT rules, including CDD, EDD, transaction monitoring, STR filing, and Travel Rule compliance. The newly created AMLA will supervise high-risk CASPs from 2026.

Sources: ESMA MiCA & AMLA, accessed September 2025

Case Study: Japan – Early and Comprehensive Crypto AML Enforcement

D. Japan: Global First Mover in Crypto AML Legislation and Supervised Self-Regulation

Regulation:	AML/CFT obligations for crypto entities are codified under two key laws: the PSA and the APTCP. Supervision is conducted by the FSA, supported by the JVCEA as a licensed self-regulatory body.
Trigger:	The collapse of Mt. Gox in 2014, one of the largest exchange failures, prompted Japan to adopt formal licensing and AML rules for crypto platforms as early as 2017.
Implementation & Scope:	All crypto exchanges must be registered with the FSA and adhere to AML controls including CDD, EDD, STR reporting, and the Travel Rule, implemented through the JVCEA, a licensed self-regulatory body.

Sources: PSA & APTCP, accessed September 2025

Case Study: United Arab Emirates – Multi-Zone Crypto Oversight

E. U.A.E.: Federated Oversight with Zone-Specific AML Regimes

Overview:	AML rules for crypto are enforced by VARA (Dubai), FSRA (Abu Dhabi Global Market), and SCA, each with distinct regulatory mandates.
Trigger:	The U.A.E.'s ambition to be a global crypto hub and FATF's 2022 greylisting pushed authorities to formalise AML/CFT controls specific to VASPs.
Implementation & Scope:	VARA's Rulebooks and FSRA's AML framework mandate full AML/CFT compliance: licensing, CDD, EDD, STRs, Travel Rule, and periodic audits. FSRA also supervises DeFi and NFTs under sandbox conditions.

Sources: AML Regulations by FSRA, SCA, and VARA, accessed September 2025

Case Study: Switzerland – AML Extension via FINMA with Limited Licensing

F. Switzerland: Functional Regulation of Crypto Intermediaries under AMLA

Regulation:	AML obligations for crypto intermediaries applied under the AMLA, supervised by the Swiss FINMA. In August 2019, FINMA issued guidance explicitly stating that crypto intermediaries are subject to AMLA, including CDD, EDD, STR, and Travel Rule compliance. The Swiss DLT Act (passed in 2020, implemented in phases through August 2021) clarified the legal status of DLT securities and infrastructures, placing them under AMLA where applicable. In June 2022, FINMA amended its AMLO-FINMA to reinforce transaction monitoring and due diligence for crypto actors.
Trigger:	Switzerland's early emergence as a "Crypto Valley" in Zug and the growing use of crypto in financial intermediaries led FINMA to clarify that AMLA applies to crypto brokers and custodians.
Implementation & Scope:	Crypto entities acting as financial intermediaries must either obtain FINMA authorisation or affiliate with a SRO. Obligations include CDD, STR filing, EDD, and documentation retention. Licensing is not crypto-specific but based on function (e.g. exchange, custody).

Source: AMLA by the FINMA, accessed September 2025

Industry Case Studies: Commercial Entities and Enforcement Actions

Case Study: Binance – Global Crackdown and Multinational Fines

A. Binance: Multinational AML Breaches and the Largest Global Crypto Settlement

Incident:	Binance facilitated billions in transactions with minimal or no KYC/AML controls, failed to report over 100,000 suspicious transactions, and allowed access to sanctioned regions.
Regulatory Body:	• United States: FinCEN, OFAC, CFTC, DOJ • India: FIU-IND • Netherlands: De Nederlandsche Bank • France: AMF • Australia: AUSTRAC • Canada: OSC & CSA
Violation Type:	Operating without proper licenses, wilful neglect of AML obligations, failure to report SARs, inadequate CDD/KYC, facilitation of transactions to sanctioned individuals and darknet markets, misleading regulators, recordkeeping failures.
Outcome:	• US$4.3B U.S. global settlement (Nov 2023): US$3.4B (FinCEN), US$968M (OFAC), US$50M (CFTC) • €3.3M (Netherlands – DNB, July 2022) • ₹18.82 Cr (Approximately US$2.26M, India – FIU, Dec 2023) • US$4.4M (Canada, May 2024) • Pending actions in France, Nigeria • Numerous licence applications were withdrawn or denied in different jurisdictions • Operations suspended in Netherlands, U.K., and Nigeria
Post-Enforcement Compliance Measures:	• As part of a November 2023 settlement with the U.S. Department of Justice, Binance's founder and former CEO Changpeng Zhao pleaded guilty to violations of anti–money laundering laws and stepped down from his role. Richard Teng, a veteran with more than three decades of experience in financial services and regulation, was appointed CEO, succeeding Zhao. • In April 2024, Binance's founder Changpeng Zhao was sentenced to four months in federal prison following his guilty plea to charges of failing to maintain an effective anti–money laundering program at the exchange. • Binance reinforced its compliance and enforcement capabilities through new senior appointments — notably Todd McElduff, Enterprise Compliance Director and former PayPal and Morgan Stanley executive, and Céline Inial and Caner Akyürek, law-enforcement veterans to oversee special investigations in France and Turkey. • Binance announced plans to expand its compliance team to 645 full-time employees by the end of 2024, marking a 34% increase from November 2023 • Enhanced transaction monitoring tools, Travel Rule compliance, and sanctions screening capabilities.

Source: WSJ, 2022; Binance, 2023; Binance, 2023; Binance, 2024; Reuters, 2024; Binance, 2024; CNBC, 2024

Case Study: Coinbase – AML Shortcomings and Monitoring Deficiencies

B. Coinbase: Gaps in AML Oversight and Monitoring

Incident:	Coinbase failed to maintain a robust AML compliance program. New York regulators identified systemic failures in transaction monitoring and delays in filing thousands of SARs.
Regulatory Body:	• NYDFS • U.K. FC
Violation Type:	Failure to maintain effective AML systems, delays in filing SARs, weak risk-based controls for customer onboarding, non-compliance with U.K. AML obligations under the MLR 2017.

Outcome:	• US$50M fine by NYDFS (January 2023), plus US$50M mandated compliance investment. • £3.5M (Approximately US$4.5M) fine by FCA (Feb 2024) on Coinbase under U.K. Money Laundering Regulations (MLR) 2017.
Post-Enforcement Compliance Measures:	• Invested US$50M (as required by NYDFS) into AML system improvements. • Enhanced suspicious activity report (SAR) filing infrastructure, automated detection systems, and risk-based onboarding procedures. • Released transparency reports detailing law enforcement data requests.

Sources: NYDFS, accessed September 2025; FCA, 2024; Coinbase, 2023; Coinbase, 2023; Coinbase, 2024

Case Study: OKX – U.S. AML Enforcement and US$505M Settlement

C. OKX: DOJ Criminal Settlement for Operating an Unlicensed Crypto Platform

Incident:	OKX allowed U.S. customers (retail and institutional) to trade on its global platform without registration as a money transmitter and with inadequate AML/KYC controls. Between 2018 and early 2024, OKX is estimated to have facilitated over US$1T in transactions involving U.S. retail and institutional customers; and processed more than US$5B in suspicious or illicit flow.
Regulatory Body:	U.S. Department of Justice, with investigative support from FinCEN and the FBI
Violation Type:	Operating an unlicensed money transmitting business; failure to implement AML/KYC programs; allowing U.S. persons to bypass KYC; failure to monitor and detect suspicious transactions; advising users to falsify identity information; violation of FATF/CFT standards.
Outcome:	• Total penalties exceeded US$505M, comprising an US$84.4M criminal fine and US$420.3M in forfeiture. • DOJ granted a 25% reduction on the baseline fine due to cooperation.
Post-Enforcement Compliance Measures:	• Introduced updated onboarding procedures, verified user geolocation, and banned U.S. IP access. • Committed to independent third-party audits of its compliance functions.

Source: Department of Justice, 2025; GlobalLegalInsights, 2025; Crypto news, 2025

Case Study: Crypto.com – Registration Failures and AML Lapses

D. Crypto.com: Registration Lapses and AML Failures in the Netherlands

Incident:	Operated without mandatory AML registration in the Netherlands; failed to meet baseline CDD/KYC thresholds and did not sufficiently report or escalate flagged transactions.
Regulatory Body:	De Nederlandsche Bank
Violation Type:	Operating without registration, violation of Dutch AML laws (Wwft), insufficient CDD/EDD protocols, reporting failures, lack of consumer protection disclosures.
Outcome:	• €2.85M fine in March 2024, for offering services without AML registration from May 2020 to Nov 2022; retroactive penalty issued under Dutch AML laws.
Post-Enforcement Compliance Measures:	• Completed retroactive AML registration in the Netherlands. • Updated internal compliance protocols to meet E.U. CDD/EDD requirements. • Expanded disclosures on consumer protection risks and added new reporting tools.

Source: DNB, 2024; The block, 2023; Crypto.com, 2025

Case Study: Kraken – Registration Failures and Margin Product Breaches

E. Kraken: Multi-Agency Scrutiny Over AML, Sanctions, and Securities Violations

Incident:	Kraken has been penalised in the Netherlands and the U.S. for violations spanning AML registration, sanctions compliance, and securities law. In the Netherlands, Kraken operated without required registration. In the U.S., it facilitated transactions for users in Iran and offered services in violation of federal securities regulations.
Regulatory Body:	• De Nederlandsche Bank • OFAC, SEC
Violation Type:	• Netherlands: Operating without required AML registration under Dutch Anti-Money Laundering Act • U.S.: Operating as an unregistered securities exchange, broker, dealer, and clearing agency; violations of the Iranian transactions and sanctions regulations.
Outcome:	• Netherlands: €4M fine imposed April 2024. • US$0.3M settlement with OFAC (November 2022) for sanctions violations.
Post-Enforcement Compliance Measures:	• Added geolocation blocking to prevent clients in prohibited locations from accessing their accounts on Kraken's website. • Began implementing multiple blockchain analysis tools to assist with sanctions monitoring and invested in additional compliance-related training for its staff, including in blockchain analytics. • Hired a dedicated head of sanctions to direct Kraken's sanctions compliance program, in addition to hiring new sanctions compliance staff. • Contracted with a vendor that assists with identification and nationality verification by using artificial intelligence tools to detect potential issues with supporting credentials provided by users.

Sources: VIXIO, 2024; AXIOS, 2022; Department of Treasury, 2022

Case Study: BitMEX – Wilful AML Neglect and Criminal Charges

F. BitMEX: Criminal AML Negligence and Founders' Guilty Pleas in the U.S.

Incident:	BitMEX allowed anonymous trading without KYC, evaded AML laws, and facilitated US$209M in suspicious transactions tied to darknet markets, hacks, and mixers.
Regulatory Body:	U.S. CFTC, FinCEN, DOJ (U.S.)
Violation Type:	Operating as an unregistered FCM, no AML/KYC program, failure to implement STR processes, enabling illicit finance, ignoring direct regulator warnings.
Outcome:	• US$100M settlement in August 2021 (shared between CFTC and FinCEN). • Each founder fined US$10M individually as part of plea agreements (May 2022). • Ongoing scrutiny of derivatives trading in DeFi and offshore entities.
Post-Enforcement Compliance Measures:	• Overhauled its leadership, including the resignation of Arthur Hayes and other founders. • Engaged in development of an AML program and user verification program, and appointed a new Chief Compliance Officer. • Emphasized its progress in strengthening compliance through the integration of best-in-class KYC and AML systems.

Source: Fincen, 2021; DOJ, 2022; Fintelegram, 2020; Fincen 2021; BItmex, 2024, Crypto news, 2025

6.4 Key Trends in AML/KYC Enforcement for Digital Assets

Enforcement activities related to AML and KYC obligations in the digital asset space have escalated sharply in the past two years. This acceleration is being driven by global regulators aligning around FATF standards, particularly the Travel Rule and the definition of VASPs. The result is not only larger penalties but a more consistent, global pattern of enforcement across jurisdictions, firm sizes, and risk categories.

Industry Perspectives on AML/KYC Compliance Initiatives in the Digital Assets Ecosystem

"We've mapped over 500 million wallets. In 8 out of 10 transactions, we can identify the source and destination, and link it to real-world entities. Crypto isn't anonymous. It's hyper-transparent. With blockchain data and off-chain signals, we know who's involved, what they're doing, and why."

Lex Fisun - CEO & Co-Founder, Global Ledger

"Because Axelar is a blockchain, it publicly logs every detail of cross-chain transfers. Chain, wallet, transaction ID, it's all there. That means anyone, whether a client, a compliance officer or a forensic analyst, can trace activity and validate that a transaction happened. Axelar is the gold standard for cross-chain traceability."

Jason Rozovsky - Head of Legal & Policy, InterOps Labs

"Project Mandala showed us the potential of digital assets to automate compliance. By embedding FX rules, KYC, and AML checks directly into smart contracts, we could create a much more efficient and scalable process. This would reduce operational burdens for banks while giving regulators stronger assurance. It is a common pain point many central banks as well as commercial banks can all work on together."

Park Kwan Hoon - Executive Director, Group Strategic Planning Office, OCBC

Figure 6.2:

AML/KYC Enforcement Actions Against Crypto Exchanges

Source: Press announcements and media releases, accessed April - June 2025.

The following trends highlight how enforcement has evolved in both scope and scale, and how different regions are responding:

- **A Steep Rise in Global AML Enforcement Activity**

According to Coinlaw, global penalties for AML/KYC non-compliance surpassed US$5.1 billion in 2024, a 39% YoY increase. The vast majority of these penalties were linked to poor or absent compliance frameworks. Notably, 83% of crypto-related compliance fines in 2024 stemmed directly from AML/KYC violations. In Europe, fines surged to €1.2 billion, with MiCA alone driving €850 million in penalties. The Middle East saw a 45% increase, led by enforcement in the U.A.E. and Saudi Arabia. By Q1 2025, penalties already reached US$1.3 billion, indicating an even more aggressive trajectory ahead.[123]

- **Enforcement Becoming More Frequent, Not Just Bigger**

As per data from Coinlaw, the number of enforcement cases globally rose to over 400 in 2024, reflecting not just larger penalties but greater consistency in prosecuting even mid-sized VASPs.[124] Regulators are clearly signalling that AML/KYC compliance is not optional, regardless of firm size, jurisdictional complexity, or client volume. The U.S. CFTC alone filed 35 crypto enforcement cases in 2024, up from 22 in 2023, with 20% of the CFTC's enforcement actions targeting overseas crypto platforms offering services to U.S. customers without proper registration.[125]

- **United States Leads in Volume and Severity**

As per Coinlaw, the United States remained the most aggressive enforcement jurisdiction, contributing nearly US$2.4B in fines in 2024, accounting for 47% of global crypto compliance fines.[126] Regulatory agencies such as the DOJ, FinCEN, OFAC, and the SEC escalated coordinated actions, with a particular focus on large-scale centralized exchanges in 2024. Recent policy shifts under the new administration suggest a more nuanced landscape. Enforcement is being recalibrated: the DOJ has disbanded the National Cryptocurrency Enforcement Team and issued a memo in April 2025 instructing prosecutors to move away from "regulation by prosecution," particularly in cases involving exchanges, mixing services, and offline wallets for unintentional violations.[127] Other congressional measures are also advancing, such as the Blockchain Regulatory Clarity Act, which proposes exempting software developers from direct AML/KYC obligations. Alongside, executive orders and working groups have been established to align various agencies around digital asset oversight while reducing duplicative litigation risk.

- **Europe Responds Through MiCA-Driven Enforcement**

With the rollout of the MiCA and the AMLR and directive (AMLD6) set to apply from July 1, 2027, the European Union has sharply increased its regulatory interventions. As cited by Coinlaw, fines across E.U. member states rose by 28% in 2024 with strong action taken in the Netherlands, France, and the U.K. (pre-Brexit framework).[128] MiCA enforcement triggered widespread delistings, licence revocations, and forced restructuring, resulting in total E.U. crypto compliance penalties reaching €1.2 billion in 2024.

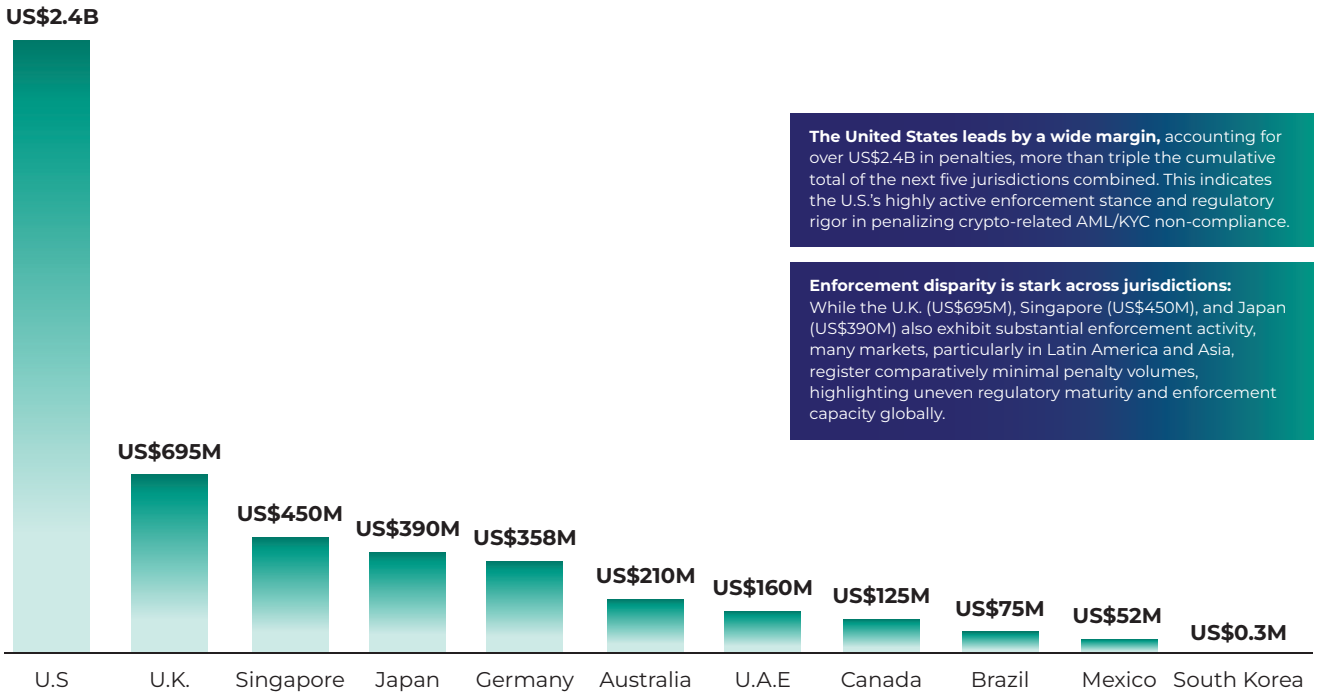
- **Asia-Pacific Rising as an Enforcement Powerhouse**

Although historically conservative in enforcement, Asia-Pacific regulators, particularly in Singapore, Japan, and Australia, have adopted a more interventionist stance. As per Coinlaw, in 2024, enforcement actions in the region increased by 55%, largely driven by AML deficiencies, lack of risk-based customer due diligence, and delayed implementation of the Travel Rule. Singapore's MAS alone levied US$450 million in fines across multiple crypto platforms.[129]

[123] CoinLaw, accessed September 2025
[124] ibid
[125] CoinLaw, accessed September 2025
[126] CoinLaw, accessed September 2025
[127] AP News, 2025
[128] CoinLaw, accessed September 2025
[129] ibid

Figure 6.3:

Regional Breakdown of Non-Compliance Penalties in Crypto Transcations (US$ million) in 2024



Source: CoinLaw, accessed September 2025

GFTN Survey Insights: AML & KYC

Survey Insight 6.1

Strengthening AML/CFT Compliance in Crypto

92%

Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) was marked as a critical regulatory priority by 92% of respondents, highlighting widespread consensus on the need for stronger compliance frameworks in the digital asset space. This underscores concerns about the pseudonymous nature of crypto transactions, use of privacy-enhancing tools, and the need for robust transaction monitoring standards to prevent illicit finance activities.

Survey Insight 6.2

FATF Travel Rule Implementation Challenges

25%

25% of respondents identified the technical implementation of the FATF Travel Rule as a significant operational burden in managing digital assets. This underscores ongoing compliance challenges in aligning blockchain transactions with anti-money laundering (AML) standards, particularly around secure and interoperable data sharing across jurisdictions

Survey Insight 6.3

AML Compliance as a Key Industry Challenge

20%

20% of respondents highlighted AML obligations as one of the most challenging aspects of digital asset regulation to navigate. This underscores industry concerns that current AML frameworks are not fully suited to the unique features of digital assets, such as peer-to-peer transfers, mixers, privacy tokens, and non-custodial wallets.

"The travel rule has created operational challenges. Some countries have implemented it, while others are yet to do so, and the vendor landscape is fragmented. We've had to onboard a number of vendors because no one single vendor covers all jurisdictions and tokens"

Robert MacDonald - Chief Legal & Compliance Officer, Bybit

6.5 Gaps and Barriers in Implementation of the FATF's Travel Rule

The FATF's 2025 review identifies several persistent gaps in the global implementation of the FATF's Travel Rule. Between 2024 and 2025, the number of jurisdictions implementing the FATF Travel Rule increased from 65 to 85, reflecting a tangible expansion in adoption. In parallel, jurisdictions reporting that they are in the process of implementation increased from 15 (out of 80 surveyed in 2024) to 14 (out of 117 surveyed in 2025), suggesting a steady momentum. Overall, 73% of surveyed jurisdictions in 2025, i.e. 85 out of 117, confirmed that legislation is now in place. Yet, despite this progress, global uptake remains incomplete. Of the FATF's broader universe of 205 jurisdictions, at least 42 did not provide survey responses in 2025, and it is likely that many of these have not implemented the requirements. Even among jurisdictions that have passed legislation, enforcement remains limited, with 59% yet to issue supervisory actions or directives against VASPs, reflecting both the recency of adoption and difficulties in operationalising oversight frameworks.[130]

The result is a patchwork of enforcement that continues to leave VASPs, and virtual assets exposed to regulatory blind spots. The lack of participation from many jurisdictions that did not respond to the FATF's survey further suggests under-implementation, widening regulatory fragmentation. These persistent gaps, ranging from legislative delays and weak supervisory capacity to uneven international alignment, pose serious concerns, as they undermine the goal of achieving a consistent, effective, and globally harmonised framework to mitigate risks of financial crime in the virtual asset ecosystem.

6.6 FATF Priority Actions and Recommendations (2025–2026)

In response to the identified deficiencies, the FATF's 2025–2026 roadmap calls for a focused push to address the weakest links in global AML/KYC enforcement.[131] Key priorities include (1) requiring all member jurisdictions to demonstrate concrete enforcement of Recommendation 16 (Travel Rule) by mid-2026, especially around cross-border transfers; (2) clarifying KYC expectations in DeFi, P2P, and unhosted wallet environments, areas now seen as systemic vulnerabilities; and (3) enhancing technical assistance to support low-capacity jurisdictions, particularly in the MENA and Sub-Saharan African regions. On a structural level, the FATF has proposed the creation of an IMG with a mandate to track national progress across supervisory actions, KYC audit trails, and suspicious transaction reporting. It also encourages regulatory sandboxes to test KYC solutions for emerging Web3 models. Importantly, the FATF now explicitly calls for binding timelines and interim milestones, marking a shift from past reliance on voluntary compliance. 2026 will serve as a formal checkpoint, by which point all jurisdictions are expected to have active and risk-based KYC enforcement frameworks applicable to all licensed and operating VASPs.

6.7 Future Outlook

As discussed in Chapter 2, tokenization is projected to scale to become US$30 trillion by 2034, when AML/KYC implications will become even more critical. At that scale, AML enforcement will no longer be limited to crypto-native exchanges or isolated VASPs; it will extend deeply into tokenized RWA pools spanning treasuries, private credit, and real estate. Without robust controls, these risk pools become systemic vectors for illicit finance, given their cross-border liquidity and institutional integration. This risk is compounded by developments described in the DeFi and On-Chain Lending chapter (Chapter 5), where tokenized treasuries and money-market funds are already being used as collateral in lending protocols. Automated liquidations and cross-chain transactions, while efficient, create opacity in ownership trails and complicate the detection of suspicious flows. The combination of programmable assets and permissionless lending magnifies exposure, making it harder to reconcile AML obligations with real-time activity across chains.

Against this backdrop, harmonisation cannot remain a distant aspiration. AML frameworks will need to evolve to address the tokenization's growth trajectory and associated risks. Supervisors and standard-setters will need to ensure that tokenized securities, RWA pools, and DeFi platforms are interoperable across jurisdictions while also embedding systemic AML safeguards.

[130] FATF, 2025
[131] ibid

The FATF's 2025 targeted update highlights a critical inflection point. The gap between global standard-setting and effective implementation has itself become a vulnerability. More than 40% of jurisdictions remain non-compliant or only partially aligned with FATF rules, while even "compliant" regimes often lack enforcement strength and technological interoperability. With the 2026 evaluation horizon approaching, the next 12–24 months are pivotal. Priorities include fully operationalising customer due diligence, activating the Travel Rule for cross-border transfers, and deploying monitoring tools that can function across varied technical architectures and business models. Supervisors must also develop the capacity to assess compliance maturity across the entire digital asset value chain, from custodians and exchanges to wallets and decentralized protocols.

For jurisdictions where frameworks already exist, the focus must shift decisively to enforcement. Where rules are still emerging, speed, clarity, and internal coherence are critical to avoid regulatory arbitrage. Capacity-building, supervisory cooperation across borders, and sustained industry engagement will be essential to ensure that gaps do not harden into structural blind spots.

Ultimately, the future of AML and KYC in the digital asset ecosystem is about embedding resilience. As compliance expectations rise in complexity, so too will the reputational and operational stakes for all market participants.

7 Privacy & Cybersecurity Risks

7.1 Introduction

The rapid growth of digital assets has introduced new paradigms of value exchange, capital formation, and financial autonomy. Yet, alongside these innovations lies a complex web of challenges related to privacy and data security, issues that bear systemic implications for market integrity and consumer protection. In contrast to traditional finance, where data governance, cybersecurity, and regulatory compliance frameworks are deeply entrenched, the digital asset ecosystem generally operates with minimal intermediaries and often outside the perimeter of conventional oversight.

The intersection of privacy and data security extends beyond a mere technological issue; it constitutes a foundational pillar for ensuring financial stability, institutional trust, and systemic resilience in the digital asset ecosystem. The growing prevalence of cyber intrusions, smart contract exploits, cross-chain laundering schemes, ransomware financing, combined with the absence of global standards for key management and the persistent vulnerabilities of hot wallet configurations, underscores the urgent need for robust policy interventions. According to Chainalysis, in 2024 alone, illicit actors stole more than US$2.17 billion from crypto platforms, with an unprecedented share of these attacks, 43.8%, attributed to private key compromises.[132] Simultaneously, actors such as the North Korean Lazarus Group exploited increasingly sophisticated cross-chain laundering methods, accounting for over US$1.34 billion in stolen funds. These developments, while alarming, also provide an opportunity to recalibrate supervisory strategies and ensure that privacy does not come at the expense of accountability, and that innovation does not undermine the core tenets of trust and transparency.

> "People assume crypto is private but post your wallet publicly, and suddenly your entire financial life is visible. Donations, dark net purchases, exchange activity, DeFi interactions, all of it is on-chain. Combine that with off-chain patterns, and privacy becomes a myth."
>
> **Lex Fisun** - CEO & Co-Founder, Global Ledger

> "Scaling and privacy are the two biggest unsolved challenges. Everything on-chain is transparent, which is both a virtue and a limitation. Until privacy-preserving technologies mature, many use cases will remain constrained despite the potential."
>
> **Haseeb Qureshi** - Managing Partner, Dragonfly

7.2 Privacy and Security in the Context of Digital Assets

Privacy in the digital asset ecosystem manifests in multifaceted ways, each with significant implications for both end users and regulators. At its most fundamental level, privacy refers to the ability of individuals to engage in transactions without exposing their identity or sensitive data. This is typically facilitated through pseudonymous wallet addresses, zero-knowledge protocols, and privacy-enhancing technologies such as mixers and anonymising networks. While these tools serve legitimate purposes, such as shielding users in high-risk jurisdictions or preserving financial confidentiality, they also create blind spots that malicious actors exploit to launder proceeds of crime, evade sanctions, and orchestrate fraud. If fallback authority resides in a single privileged actor, such as a protocol developer or exchange operator, then concentration risk remains acute, regardless of how decentralized the front-facing platform appears. By contrast, multi-signature arrangements or MPC distribute control across several independent actors, ensuring that no one party can unilaterally move funds or override safety locks. Some protocols have further automated the process by embedding on-chain circuit breakers that trigger fund freezes or rate-limit withdrawals when anomalous activity is detected. These variations have different supervisory implications: centralized control can aid rapid intervention but undermines resilience, while distributed or automated controls enhance security but may slow down recovery in emergencies.

[132] Chainalysis, 2024

"There's a policy trilemma between security, privacy, and efficiency. Push one too far and the others suffer. Regulatory frameworks must live in the middle. Financial stability isn't about standing still; it's like riding a bicycle, you must move forward to stay upright. The challenge is to balance responsible innovation with oversight, without sacrificing essential safeguards."

Peter Kerstens - Advisor for Financial Sector Digitalisation and Cybersecurity, European Commission

While blockchains by their nature make every transaction visible, regulators must look beyond transaction data to assess whether the underlying smart contract logic is auditable and trustworthy. Open-source protocols allow public review of their code base, theoretically enabling independent security verification. However, transparency cuts both ways: attackers can also identify vulnerabilities more quickly. This makes independent third-party audits and continuous monitoring a regulatory necessity rather than a best practice. Supervisory technology (Suptech) can augment these processes by applying blockchain analytics to flag vulnerabilities and monitor protocol behaviour across chains in real-time.

Security, by contrast, pertains to the integrity and resilience of the technical and operational layers that underpin DeFi protocols and centralized crypto platforms. The decentralized and automated nature of these systems, where smart contracts execute immutable transactions, bridges transfer value across chains, and custodial wallets store billions in crypto assets, means that vulnerabilities in a single line of code, API misconfiguration, or compromised validator node can have cascading effects. The immutability of blockchain transactions, while a hallmark of trustless systems, also precludes reversibility, amplifying the impact of exploits. Regulators must therefore evaluate not only whether a platform maintains adequate perimeter defence, but also whether it has been designed to anticipate and prevent failures, fallback mechanisms, multi-party governance, and continuous security audits as foundational components of risk management.

The interplay between privacy and security is further complicated by the rise of composability in the digital asset ecosystem. Protocols often integrate with or rely upon other dApps, oracles, and third-party infrastructure. This web of interdependencies magnifies the attack surface, introducing risks that extend beyond any single protocol's boundaries. A vulnerability in one digital asset protocol or primitive (basic building blocks or core functions, such as lending, borrowing, or swaps, that other protocols stack together to create more complex financial products) can be exploited to trigger exploits in another, a phenomenon exemplified by the increasing prevalence of cross-protocol flash loan attacks (attackers borrow large sums without collateral, move them across several DeFi platforms in one transaction, manipulate markets, then repay the loan, leaving the exploited protocols with losses) and recursive lending loops (attackers repeatedly use borrowed funds as new collateral, cycling them through protocols to inflate their borrowing capacity and extract more than they should). For regulators, this underscores the need for systemic supervision that accounts not just for individual protocol robustness, but also for network-wide interconnectivity and cascading failure scenarios.

Table 7.1:

Privacy and Security Dimensions in the Digital Asset Ecosystem

Category	Component	Description	Examples
Privacy	User Anonymity	Enables pseudonymous interaction by removing identity verification and using anonymising tools.	Wallets without KYC, Monero, Tornado Cash
	Protocol Confidentiality	Use of smart contracts that lack transparency through the absence of audits or intentionally hidden logic.	Obfuscated or unaudited smart contracts
	Cross-Chain Obfuscation	Movement of assets across multiple chains to disrupt traceability.	Chain-hopping via DEXs, bridges, atomic swaps
Security	Smart Contract Codebases	Vulnerabilities in code logic are exploitable for the manipulation or draining of funds.	Flash loan attacks, oracle manipulation
	Bridging Infrastructure	Weaknesses in interoperability mechanisms between chains have been exploited for large-scale hacks.	Validator collusion, signature replay
	Custodial Systems	Threats to stored user assets and data due to poor key management or database security.	Private key theft, backend database leaks
	Exchange APIs	Poorly secured APIs enabling unauthorised access or rate-based manipulation.	Rate limit bypass, API credential misuse

Sources: BIS, 2023; BIS, 2021 and BIS, 2022; Elliptic, 2022; ARXIV, 2022

7.2.1 Privacy versus Regulatory Oversight: The Wallet Dimension

While anonymity and pseudonymity are often framed as purely technical issues, there is a deeper tension between preserving financial privacy and fulfilling regulatory obligations, especially around wallets, which lie at the intersection of privacy tools and regulatory oversight. Many users hold digital assets in non-custodial wallets. These provide strong control and privacy, but also reduce visibility for regulators. Absence of global standards for key management and insecure wallet configurations exacerbate risks such as private key loss, phishing, and use of wallets in illicit finance.

Recent initiatives show how regulation is trying to catch up. For example, **Project Aurum 2.0**[133], launched by the BIS Innovation Hub and Hong Kong Monetary Authority, places "privacy by design" at its core, exploring how retail e-wallets can balance wallet privacy with compliance requirements using technologies such as pseudonymisation and ZKPs. Also, privacy coins and privacy-focused wallets like Samourai have prompted legal scrutiny for their mixing or anonymisation features, raising questions about whether wallet design itself can be regulated (e.g. through licensing, traceability, or optional disclosure) while retaining privacy guarantees.[134]

[133] Fintech Hong Kong, 2024
[134] Techopedia, accessed Sep 2025

7.3 The Risk Hierarchy of Cryptocurrency Exchanges

As the principal gateways to the digital asset ecosystem, centralized digital exchanges occupy a unique position of trust and systemic importance. These platforms, which facilitate trading, custody, fiat on-and-off ramps, and increasingly offer staking, lending, and yield products, represent the confluence of user activity, liquidity concentration, and critical infrastructure. Yet their vertically integrated architectures, combining exchange, custodian, wallet provider, and sometimes market maker roles within a single platform, create layered and tightly coupled risk exposures.

- **Operational and technological risks** remain pervasive and under-addressed. Centralized exchanges, despite being built on decentralized asset classes, often rely on traditional web infrastructure, cloud services, and internal permissioning systems. Misconfigured APIs, insufficient rate-limiting, and outdated access controls can lead to data exfiltration, wallet compromise, or service outages. In several documented cases, attackers have exploited backdoors in trading interfaces, manipulated gas estimators, or targeted internal key management systems, resulting in multi-million-dollar losses and the exposure of sensitive user data.
- **Cybersecurity risk**, though overlapping with operational and technological risks, is distinct in its adversarial nature. It involves deliberate attempts to breach the exchange's digital perimeter, steal funds, or gain unauthorised access. This includes malware attacks on hot wallets, phishing campaigns targeting employees and users, and sophisticated nation-state or organised criminal group campaigns. These risks are compounded when platforms fail to segment critical infrastructure, use inadequate multi-factor authentication, or allow engineers excessive write permissions in live production environments.
- **Market risk** arises from the volatility of underlying crypto assets, liquidity fragmentation, token delistings, and the impact of leverage products. When prices drop sharply, collateral values fall and trigger margin calls or stop-loss orders, forcing large waves of liquidations. These forced sales add further downward pressure, deepening the price decline and setting off a cascading cycle of additional liquidations, a feedback loop most severe on retail-heavy platforms with thin order books.
- **Conduct risk** encompasses a wide range of malpractices, from wash trading, insider token listings, and undisclosed affiliated market making, to user data harvesting and misleading claims about reserves. These practices not only distort market integrity but also erode investor confidence.
- **Bad actor risk** refers to the internal dimension, rogue employees, founders with questionable track records, or insider collusion. History has shown that some of the most catastrophic failures in the digital asset space, FTX, QuadrigaCX, and others, were not purely technical breaches, but failures of governance, ethics, and fiduciary responsibility. The opacity of exchange operations, absence of board oversight, and lack of jurisdictional clarity only heighten these risks. For regulators, this necessitates a dual approach: not only mandating technical standards and audit trails, but also enforcing fit-and-proper tests for key persons, independent custody, and transparent conflict-of-interest disclosures.

"Hedera's consensus mechanism avoids forking and orphan blocks. It's not just proof-of-stake — it's a hashgraph with deterministic finality. That means we don't waste energy on discarded blocks, and we don't face MEV vulnerabilities. These protocol-level features matter deeply to institutions evaluating long-term security and compliance."

Isadora Arredondo - Global Policy Director, Hedera

7.4 Typologies of Exploits: The Anatomy of Common Attack Vectors

A review of the most prolific attack vectors in the digital asset space reveals a convergence of technical sophistication and financial incentive.

- **Flash loan attacks** have emerged as a particularly pernicious threat. These exploits take advantage of protocols that allow users to borrow large amounts of capital without collateral, provided the funds are returned within the same transaction. While flash loans have legitimate arbitrage and liquidity use cases, malicious actors have used them to manipulate on-chain prices, drain liquidity pools, and bypass governance thresholds. In one of the earliest incidents involving the bZx protocol, attackers executed a multi-step arbitrage strategy that resulted in the theft of millions of dollars in assets, highlighting the speed at which such exploits can occur and the inadequacy of existing mitigation tools at the time. Mitigations include price-guarded oracles, capped slippage, and one-block reentrancy guards for composable calls, which could be deployed to reduce these risks.

- **Rug pulls** represent another endemic vulnerability in the digital asset ecosystem, particularly in the context of unvetted token listings and decentralized liquidity provision. In these schemes, developers create seemingly legitimate tokens, seed them with initial liquidity, market them aggressively through social media and influencers, and then withdraw all funds, often using obfuscation techniques such as token minting, honeypot functions, or disabling selling functionalities. The scale of rug pulls and ponzi schemes are growing, with over US$4.6 billion lost in 2024 alone according to Coinlaw, often within hours of token deployment.[135] These schemes disproportionately affect retail investors, many of whom operate under the false assumption that the presence of liquidity or token audits equates to legitimacy.

- **Private key compromises** have also surged in recent years and now represent the single largest vector for fund theft across digital asset platforms. Whether through phishing campaigns, clipboard hijackers, malware-infected wallets, or insecure custody infrastructure, attackers continue to find ways to access critical signing keys. According to Chainalysis, in 2024, private key compromises accounted for almost 43.8% of all stolen funds, a staggering figure that illustrates the inadequacy of current key management practices.[136] This underscores persistent weaknesses in wallet management, particularly in hot wallet infrastructures and inadequate multi-signature or hardware key protections. While many platforms continue to rely on hot wallets with single-signature setups, leaving billions in user deposits exposed to single points of failure, most large custodians today employ advanced safeguards such as Multi-Party Computation (MPC) and Hardware Security Modules (HSMs) to mitigate these risks.

- **Social engineering and insider manipulation** have likewise escalated in sophistication. North Korean-affiliated actors, for example, have been documented by the FBI, infiltrating companies by posing as engineers or consultants during recruitment processes.[137] Once inside, they exfiltrate credentials or insert malicious code into production environments. Other forms of social engineering include spear phishing campaigns, deepfake-enabled video interviews, and SIM-swap attacks. These techniques bypass technical perimeters entirely, exploiting the human layer of security, a layer that is frequently neglected in the design of DeFi protocols or user-facing exchanges.

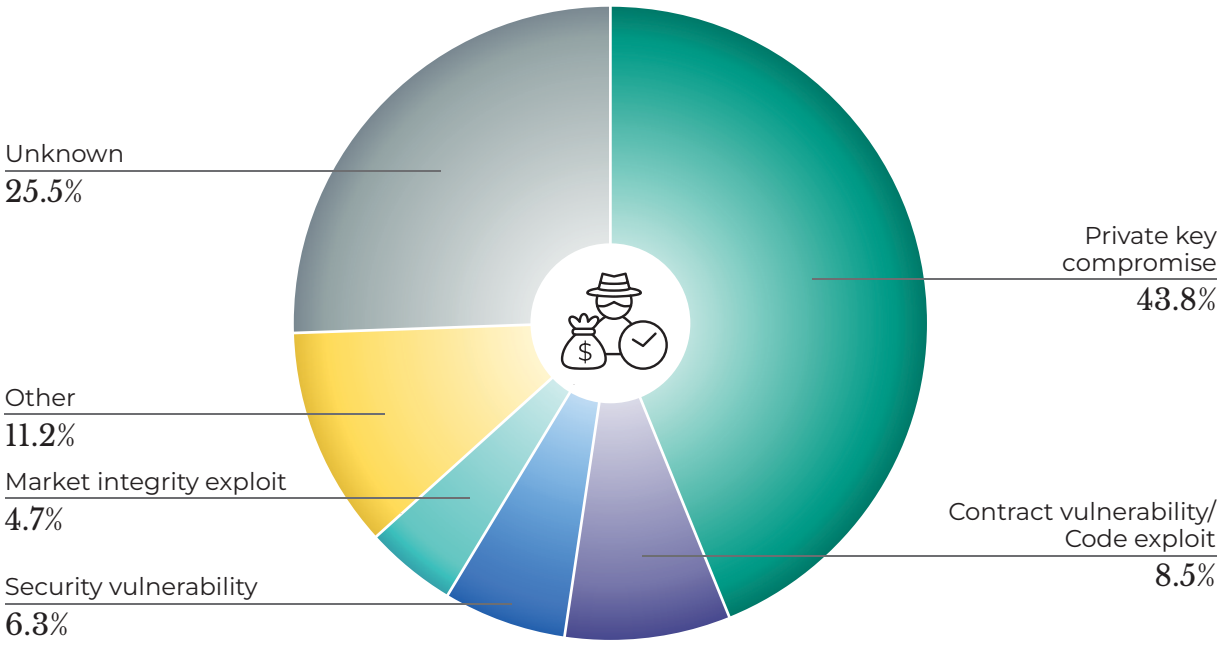
> "Our hack response was a turning point. Within hours, we informed users and the wider community, launched investigations, and coordinated with global law enforcement. Our proof-of-reserves were re-audited, and we published the Lazarus Bounty site to help the industry trace stolen funds. This wasn't just crisis management — it was a show of transparency, resilience, and industry coordination."
>
> **Robert MacDonald** - Chief Legal & Compliance Officer, Bybit

As described in figure 7.1, unknown causes comprise 25.5% of the total, indicating significant gaps in post-incident forensics and attribution. This suggests that many entities either lack the technical capability to conduct comprehensive breach investigations or are unwilling to disclose detailed information due to reputational risk. As per Chainalysis' Crypto Crime Report, other notable compromise types (11.2%) likely include phishing, insider leaks, and social engineering attacks; contract vulnerability/code exploits (8.5%), a common weakness in DeFi protocols where improperly audited smart contracts are manipulated; and market integrity exploits (4.7%), which often involve price manipulation tactics such as oracle manipulation and flash loan abuse. Lastly, security vulnerabilities, which account for 6.3%, highlight issues like misconfigured servers, weak access controls, and unpatched systems.[138]

[135] CoinLaw, accessed September 2025
[136] Chainalysis, 2025
[137] Federal Bureau of Investigation, 2024
[138] Chainalysis, 2025

Figure 7.1:

Funds stolen by type of companies (Jan 2024 - Nov 2024)



Source: The Chainalysis Crypto Crime Report, 2025

7.5 How Stolen Crypto Is Laundered into Untraceability

The laundering lifecycle of stolen crypto assets in 2025 is marked by a multi-layered obfuscation strategy that increasingly defies traditional forensic tools. Following an initial exploit, illicit actors typically disperse funds across multiple wallets and chains, leveraging automated bots to fragment the holdings and trigger chain-hopping via decentralized bridges. DeFi security losses in 2024 fell to approximately US$474 million, a 40% drop from 2023, with bridge exploits decreasing markedly from US$338 million in 2023 to US$114 million in 2024.[139] Although centralized exchanges are regulated entities in many jurisdictions, they remain a significant laundering channel when oversight is weak, or compliance is inconsistent. Launderers typically move stolen or illicitly obtained crypto into CEXs, where they convert it into other crypto assets or fiat currencies. When an exchange operates in a jurisdiction with poor KYC/AML enforcement, criminals can open accounts under false identities or use "layering" techniques, rapidly trading across multiple pairs to blur the audit trail. Some exploit exchanges with high liquidity to execute large trades without drawing attention, while others deliberately target smaller or offshore platforms with limited monitoring capacity. Even when exchanges have basic controls, the sheer transaction volume often allows suspicious transfers to blend in with legitimate activity, making detection difficult. Mixers, used to break traceability links, reflect their continued exploitation despite enforcement actions like OFAC sanctions against Tornado Cash. Other destinations include DeFi protocols, OTC brokers, and gambling platforms, each contributing smaller but strategically important roles in the overall laundering pipeline. Together, the data validates that modern laundering is not linear but deeply fragmented, exploiting the interoperability, pseudonymity, and regulatory gaps of the crypto ecosystem to defeat conventional tracking systems.

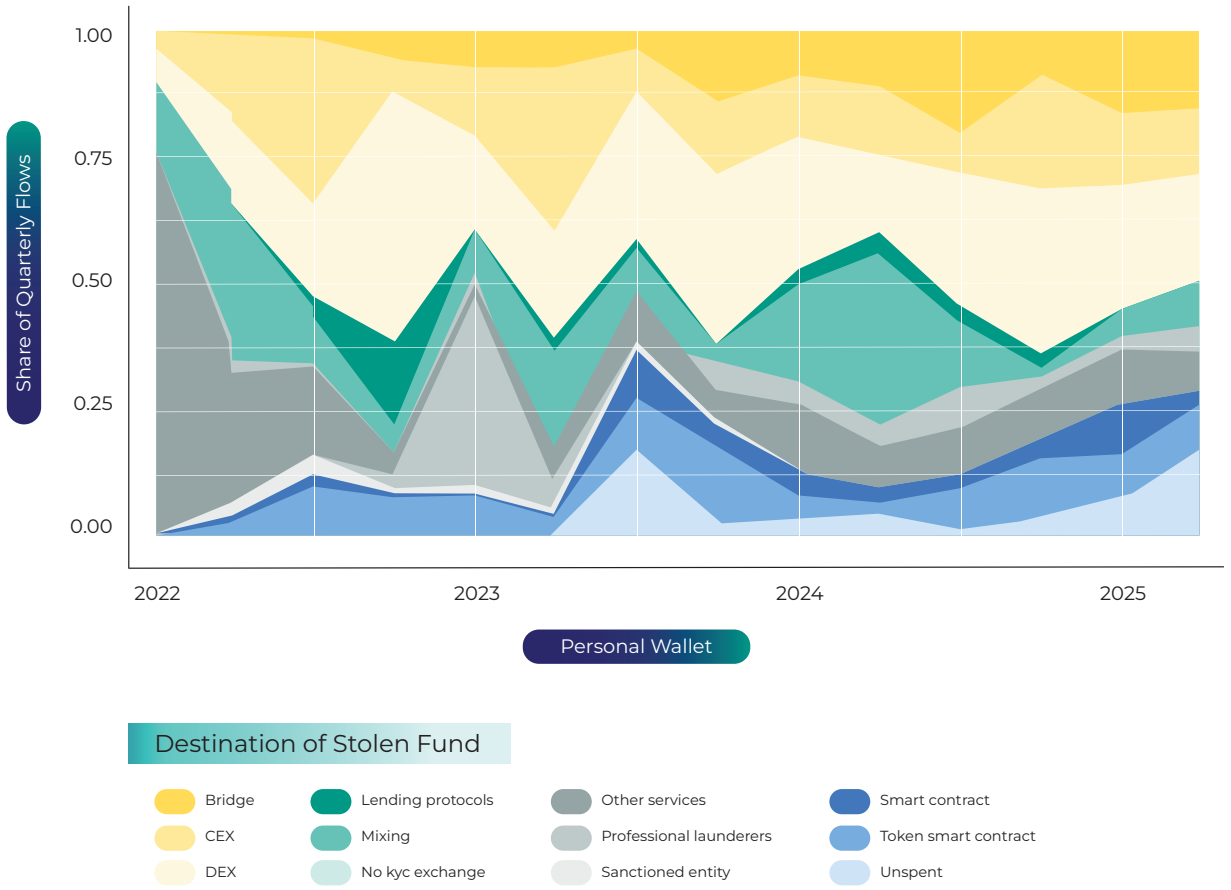
"The main obstacle is off-chain data. On-chain records are public, but law enforcement needs KYC and transaction details from exchanges. Many exchanges move jurisdictions or split into subsidiaries, making it difficult to identify the right entity. This lack of transparency, combined with slow mutual legal assistance treaties, creates a major hurdle to timely investigations."

Sungyong Kang - Criminal Intelligence Officer, Interpol Financial Crime and Anti-corruption Centre

[139] Cointelegraph, 2025

Figure 7.2:

Stolen fund laundering behaviour by victim type and fund destination



Source: The Chainalysis 2025 Crypto Crime Mid-year Update, 2025

7.6 A Statistical Overview of Crypto Theft and Cross-Chain Crime

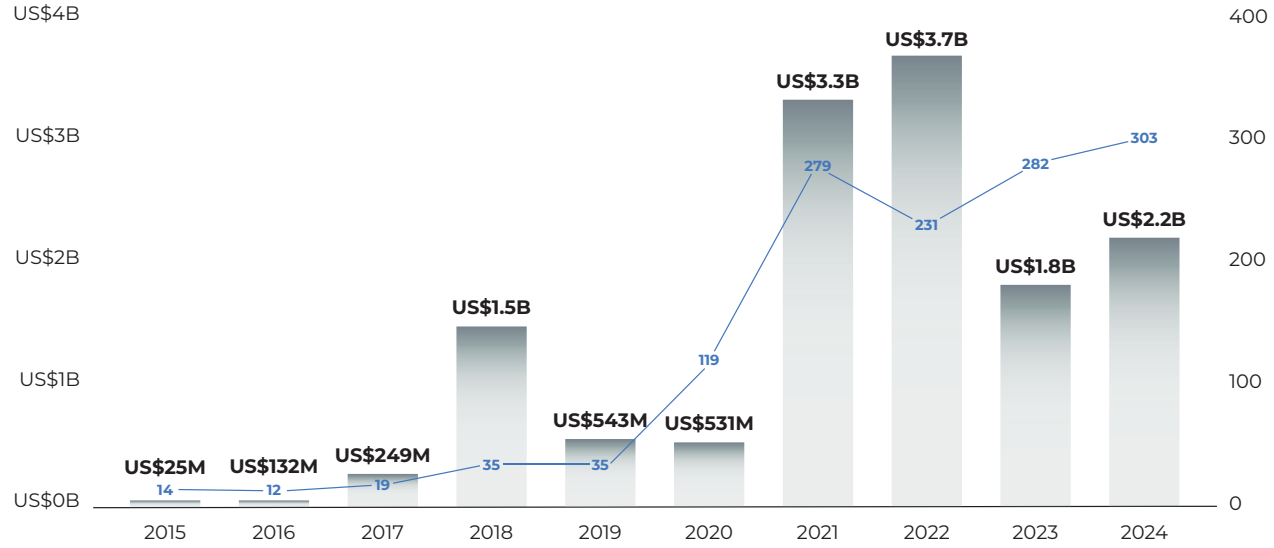
In the first half of 2025, TRM Labs notes that US$2.1 billion was stolen across approximately 75 exploits and hacks, nearly matching the entire-year loss totals for 2024.[140] The single largest incident this year remains the US$1.5 billion Bybit hack in February 2025, allegedly linked to North Korean state-sponsored actors. According to Chainalysis, this single event alone constituted nearly 69% of the total stolen crypto value in 2025 so far.[141] Ransomware payments surged back to record levels, reaching US$1.1 billion, after a decline in 2022–2023, with LockBit, BlackCat, and Cl0p ranking among the most prolific ransomware families. These groups often receive payments in Bitcoin or Monero and utilise chain-hopping mixers to evade forensic tracking.

Total Value Stolen in Crypto Hacks and Number of Hacks (2015–2024): According to TRM Labs, illicit volume in 2024 declined to around US$45 billion, amounting to about 0.4% of total crypto transaction volume, with fraud and scams still among the top categories.[142] This suggests that while compromise vectors remain serious, the share of top-end losses is easing somewhat. This indicates that while hacks are becoming more frequent, they are increasingly directed at platforms with stronger defences or smaller pools of assets, resulting in lower average losses per incident. The data also indicates that 2021 and 2022 marked an inflection point for high-value heists, coinciding with crypto market booms and rapid DeFi adoption. Despite the decline in stolen value, the persistent rise in hack volume points to escalating systemic vulnerabilities and a broader base of opportunistic attackers.

[140] TRM Labs, 2025
[141] Chainalysis, 2025
[142] TRM Labs, 2025

Figure 7.3:

Yearly total value stolen in crypto hacks and number of hacks (2015 - 2024)

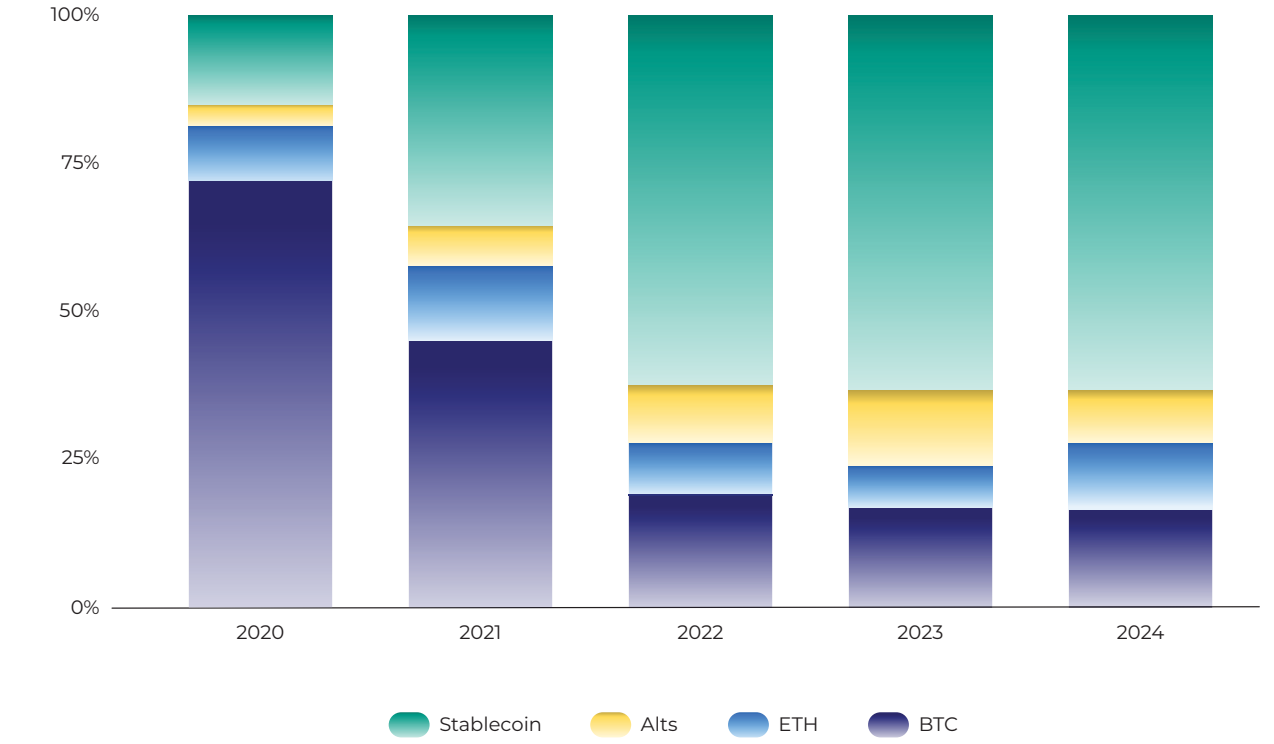


Source: The Chainalysis Crypto Crime Report, 2025

On-chain Crime by Asset (2020–2024): In 2020, Bitcoin (BTC) dominated illicit transaction volumes, constituting nearly three-quarters of all assets involved in crypto crime. However, by 2024, stablecoins have overtaken BTC to become the predominant vehicle for on-chain illicit finance. This transformation reflects both the growth of stablecoin adoption in legitimate commerce and the increasing attractiveness of their low volatility and speed for bad actors. Ethereum (ETH) and alternative tokens (Alts) have maintained a steady but modest presence, suggesting targeted but consistent usage by fraudsters. The trend indicates a maturing criminal ecosystem that mirrors mainstream crypto usage.

Figure 7.4:

On-chain crime by asset (2020 - 2024)

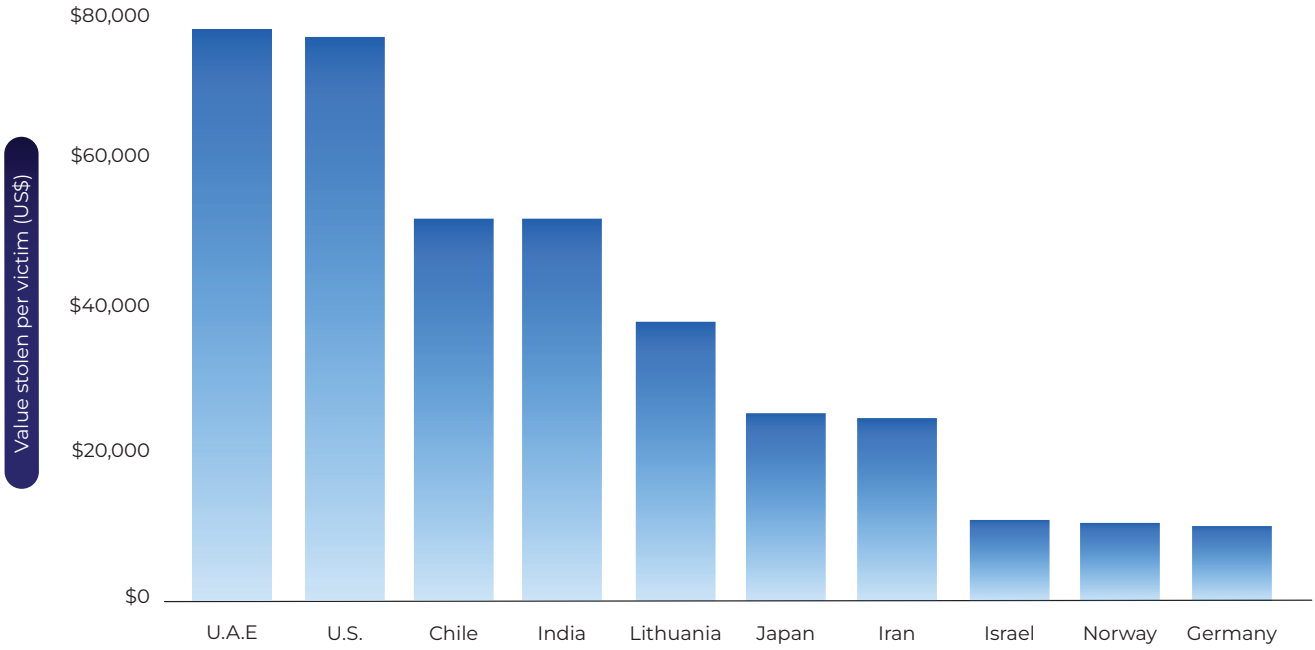


Source: The Chainalysis Crypto Crime Report, 2025

Top 10 Countries by Value Stolen Per Victim (Jan–Jun 2025): According to Chainalysis, the U.A.E. and the U.S. top the list, each exceeding US$75,000 per victim, indicating that attackers may be deliberately prioritising high-net-worth individuals or targeting platforms with large wallet holdings in these nations.[143] Countries like Chile, India, and Lithuania also show unexpectedly high average losses, hinting at gaps in local compliance infrastructure or a concentration of successful high-value scams. Japan, Iran, Israel, Norway, and Germany round out the list with decreasing loss values, reflecting both a broadening attack footprint and variability in platform security, user awareness, and law enforcement response.

Figure 7.5:

Top 10 countries by value stolen per victim (Jan 2025 - June 2025)



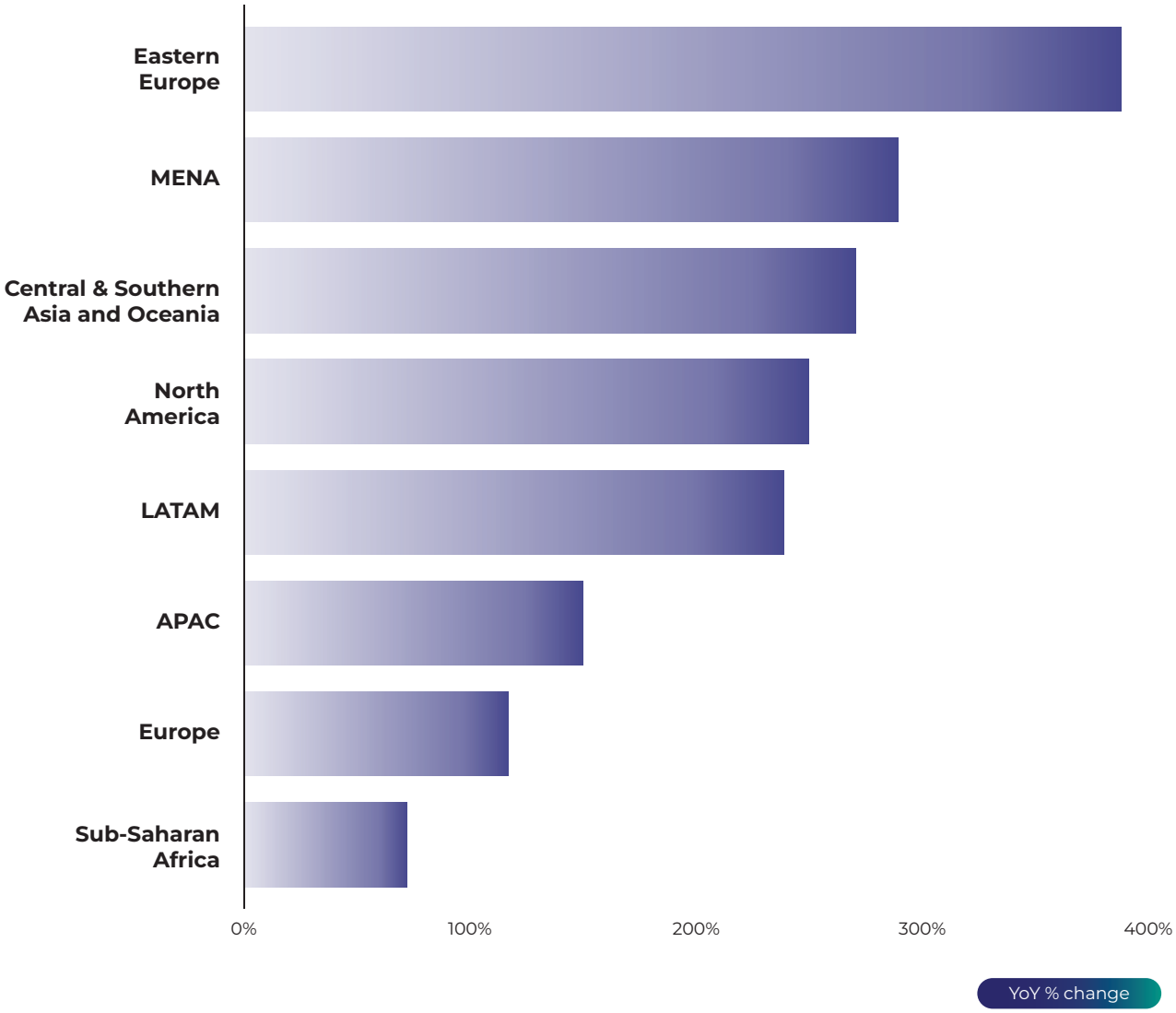
Source: The Chainalysis 2025 Crypto Crime Mid-year Update, 2025.

Average Number of Distinct Individuals (or wallets) Affected: "Average victim totals" or average number of distinct individuals (or wallets) targeted has seen a YoY percentage growth across global regions. Eastern Europe experienced the steepest surge, followed by the MENA and Central & Southern Asia and Oceania regions, indicating the expansion of targeting campaigns in geopolitically unstable or technologically maturing markets. North America and LATAM also show substantial growth, while Europe and Sub-Saharan Africa reflect comparatively lower increases. These trends suggest that cybercriminals are increasingly exploiting emerging markets with weaker KYC norms, lax enforcement, or under-resourced investigative frameworks.

[143] Chainalysis, 2025

Figure 7.6:

H1 2024 to H1 2025 change in average victim totals region



Sources: The Chainalysis Crypto Crime Report, 2025; The Chainalysis 2025 Crypto Crime Mid-year Update, 2025

Table 7.2:

Chronology of Major Thefts, Data Breaches, and Privacy Incidents

Year	Entity	Incident Type	Impact	Incident Details	Aftermath & Improvements
2025	Nobitex	Hot wallet compromise (Iran conflict)	US$90M	Source code leaked; hot wallets exploited amid political tensions; attackers claimed to destroy funds, not launder.	**Company:** Nobitex moved more reserves to cold storage, introduced multi-sig wallets, and launched a compliance review program. **Regulatory:** Iranian regulators urged exchanges to adopt custody minimum standards, and discussions opened on licensing reforms.
2025	Bybit	Cold-to-warm wallet exploit via API breach	US$1.5B	Largest single heist to date as of September 2025; API vulnerabilities enabled attackers to bypass internal wallet segregation controls.	**Company**: Bybit fully reimbursed customers via reserves, expanded its bug bounty, and rebuilt its wallet segregation model. **Regulatory:** MAS and other APAC regulators cited the case as a driver for stricter wallet isolation and segregation standards across exchanges.
2025	Coinbase	Insider-enabled leak	Over 69,000 users data exposed; ransom demand of around $20M	Rogue support agents leaked sensitive data and attempted ransomware extortion; no private key/funds lost.	**Company:** Coinbase fired implicated staff, enhanced insider threat monitoring, and mandated hardware access tokens. **Regulatory:** U.S. supervisory commentary highlighted insider risk, prompting new expectations on access controls and staff credential management.
2025	Binance, Coinbase, Kraken, Gemini, Crypto.com	Dark Web Data Dump	Around 18 million U.S. users' records listed for sale	Reports surfaced of a purported dataset; primary validation limited.	**Company:** Exchanges jointly launched user advisories, offered credential refreshes, and coordinated on fraud monitoring. **Regulatory:** E.U. MiCA and U.S. FTC both referenced the breach in calls for stronger user data protection and coordinated cybersecurity audits for VASPs.

Source: Reuters, 2025; Elliptic, 2025; Techcrunch, 2025; Mitrade, 2025

Table 7.3:

Resilience Indicators

Metric	Definition	Latest Datapoint	Benchmark	Implication
Breach Disclosure Latency	Average time from incident discovery to public notice.	Median 87 days to notify in 2024; broader studies show around 3.7 months on average.	72 hours to authority under GDPR Art. 33; 4 business days for public issuers under new SEC rule.	Average disclosure still lags mandated norms by months, limiting victim protection and regulatory response.
Attribution Rate	Share of major hacks with identified compromise vector.	≈75% identified in 2024: private-key compromise (43.8%), bridge/smart-contract defects, etc.; ≈ 25% still "unknown cause".	No formal global norm.	Attribution is improving, but a quarter of stolen value remains without clear cause, constraining prescriptive controls.
Forensic Recovery	Portion of stolen funds ultimately traced, frozen, or returned.	≈$675M (about 25%) of hacked funds recovered in 2023; 2025 seizures include >$200M in single U.S. enforcement actions.	No global threshold.	Recovery is increasingly feasible, but still uneven and ad-hoc; mandatory tracing and stablecoin blacklists accelerate freezes.

Sources: Databreaches, 2025; Comparitech, 2025; GDPR, accessed Sep 2025; Reuters, 2024; Chainanalysis, 2025; Cointelegraph, 2024; DoJ, 2025

7.7 A Chronological Evolution of Crypto Heists (2021–2025)

From 2021 to 2025, the crypto ecosystem experienced a series of increasingly sophisticated monetary thefts and data breaches, revealing an alarming evolution in both the scale and complexity of cyber threats. In 2021, the trend began with BitMart losing US$196 million[144] through a private key exploit, alongside Gemini's third-party data leak affecting 5.7 million users[145]. The following year marked a pivotal shift, with multiple high-impact bridge exploits including Ronin (US$625 million)[146] and Wormhole (US$320 million)[147], indicating that cross-chain infrastructure had become a primary attack vector. Concurrently, Crypto.com lost US$15 million[148] in ETH due to a transfer vulnerability, although no user funds were reportedly lost.

In 2022, the scope of threats expanded. Nomad Bridge (US$190 million)[149] and Beanstalk Farms (US$182 million)[150] were both targeted through smart contract vulnerabilities, and Binance Smart Chain faced a US$570 million[151] exploit via a cold-to-warm wallet vector. The year also witnessed FTX's dramatic collapse involving US$477 million[152] in internal fraud and misappropriation, highlighting that threats were not limited to external actors. Simultaneously, Binance was accused (though it denied the claim) of leaking 12.8 million user records[153].

By 2023, data and asset vulnerabilities had become deeply entwined. Mixin lost US$200 million[154] in a third-party cloud exploit, while Euler Finance suffered a US$197 million[155] loss through a flash loan attack, both cases signalling how infrastructure providers had become indirect points of failure. In 2024, Poloniex (US$132 million)[156] and DMM Bitcoin (US$ 308 million)[157] were breached via hot wallet vulnerabilities

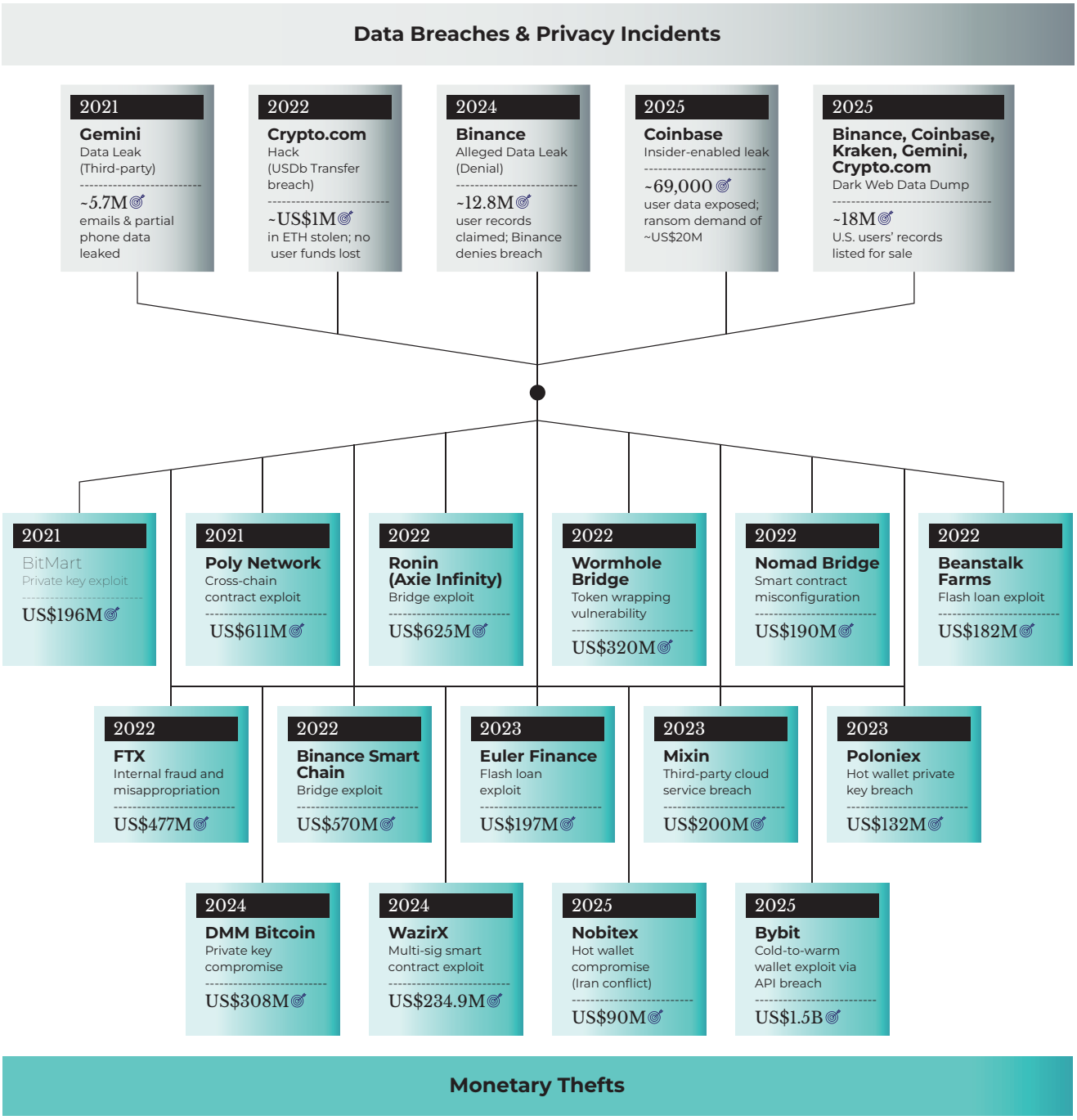
[144] Coindesk, 2021
[145] Cointelegraph, 2022
[146] Forbes, 2022
[147] Bloomberg, 2022
[148] Investopedia, 2022
[149] Yahoo Finance, 2022
[150] Coindesk, 2022
[151] Reuters, 2022
[152] Investopedia, 2022
[153] Binance, 2024
[154] Reuters, 2023
[155] Binance, 2023
[156] CertiK, 2023
[157] FBI, 2024

and private key compromises, while WazirX saw a US$235 million[158] multi-sig smart contract exploit, further underlining weaknesses in custody and governance.

2025 underscored the culmination of these trends: insider threats, API breaches, and massive-scale thefts defined the year. Coinbase reported a leak of 69,000 user records[159] linked to internal malfeasance, while 18 million[160] U.S. user records from major exchanges like Binance, Kraken, and Gemini surfaced for sale on the dark web. Meanwhile, Nobitex experienced a US$90 million[161] theft caused by internal conflict, and Bybit suffered the largest attack of the timeline, a staggering US$1.5 billion[162] breach through API exploitation and wallet compromise.

Figure 7.7:

Chronology of Major Crypto Asset and Data theft



Source: Press announcements and media releases, accessed April - June 2025.

Impact

[158] WazirX, 2024
[159] Techcrunch, 2025
[160] Binance, 2025
[161] TRM Labs, 2025
[162] Reuters, 2025

"Real-time information sharing and interdiction are essential in the fight against crypto-enabled crime. Blockchain technology gives us the unprecedented ability to trace funds across borders in seconds — but that advantage only matters if we act together. Through TRM's Beacon Network, members across the private sector and global law enforcement agencies are connecting the dots, sharing signals, and coordinating responses in real-time. That collaboration is what turns transparency into action — and disruption."

Ari Redbord - Global Head of Policy and Government Affairs, TRM Labs

Table 7.4:

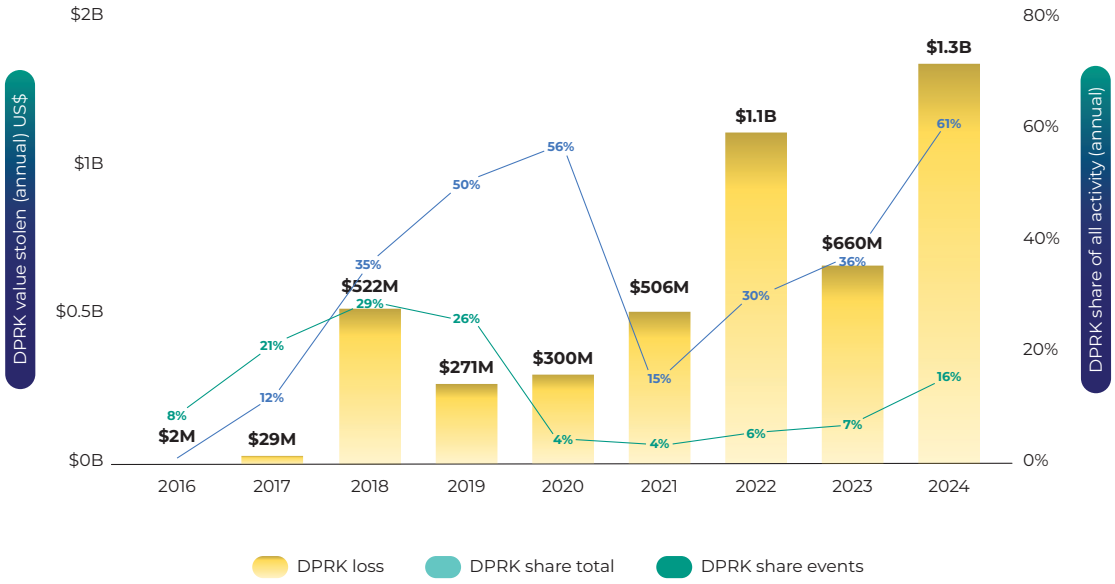
Case Study: State-Sponsored Cybercrime by Lazarus Group (North Korea)

A. The Lazarus Playbook: North Korea's State-Sponsored Crypto Heists	
Actor	Lazarus Group (North Korea)
Strategic Objectives	Lazarus' crypto operations serve as a critical foreign exchange pipeline for the North Korean regime, helping to bypass international sanctions and finance weapons proliferation, espionage, and internal economic stability.
Scope of Activity	Responsible for 6 of the top 10 largest crypto hacks in 2024–2025, including Bybit (US$1.5B), Ronin (US$625M), and Stake.com (US$41M). Total thefts attributed to Lazarus exceeded US$1.34B in 2024.
Tactics and Tools	Lazarus employs spear-phishing, fake job résumés embedded with malware, CI/CD pipeline injections, and trojanised DeFi applications. They exploit wallet access points, validator systems, and bridge vulnerabilities.
Laundering Workflow	Funds are obfuscated via Sinbad and Tornado Cash mixers, privacy coins (e.g. Monero), and chain-hopping through DeFi bridges. Cash-outs are routed via Chinese OTC desks and low-KYC exchanges. North Korea has been linked to over US$2.7B in cross-chain laundering volumes.
Operational Alliances	Increasing collaborations have been observed with cybercrime groups in Russia and Iran, suggesting a state-aligned cybercrime ecosystem with shared infrastructure.
Trend Shift	Time-to-cash-out reduced to under 72 hours in 2025, indicating streamlined laundering operations. Targets have expanded beyond CEXs to include DeFi bridges, custodians, and CI pipelines.

Source: BBC, 2025

Figure 7.8:

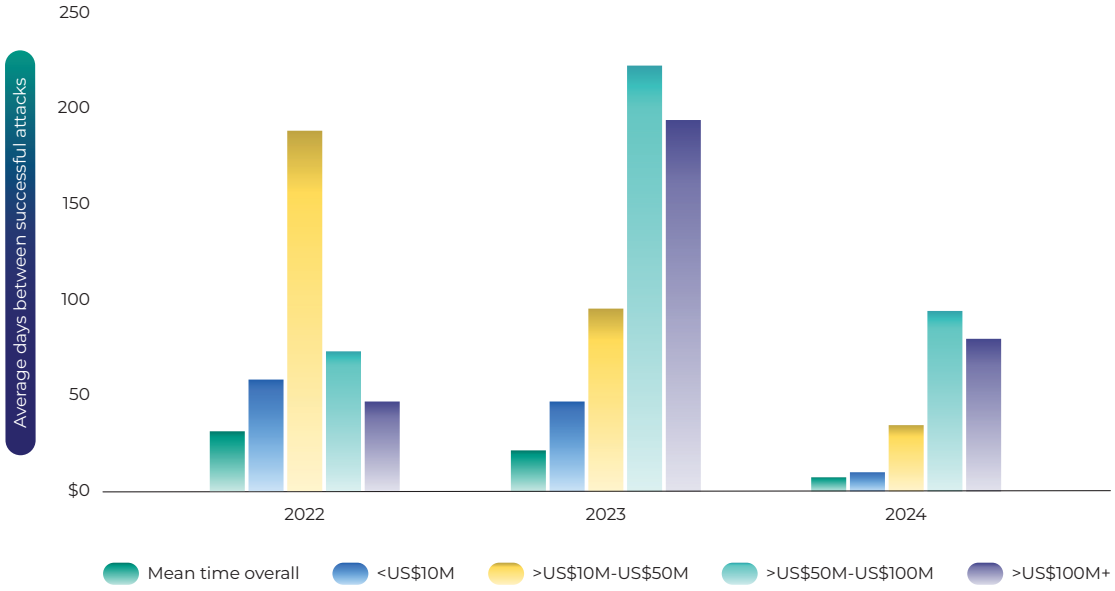
DPRK hacking activity (2016 - Nov 30, 2024)



Source: The Chainalysis Crypto Crime Report, 2025

Figure 7.9:

Time between successful DPRK attacks (2022 - 2024)



Source: The Chainalysis Crypto Crime Report, 2025

Table 7.5:

Case Study: Crypto-Enabled Sanctions Evasion and Ransomware Laundering by Iran

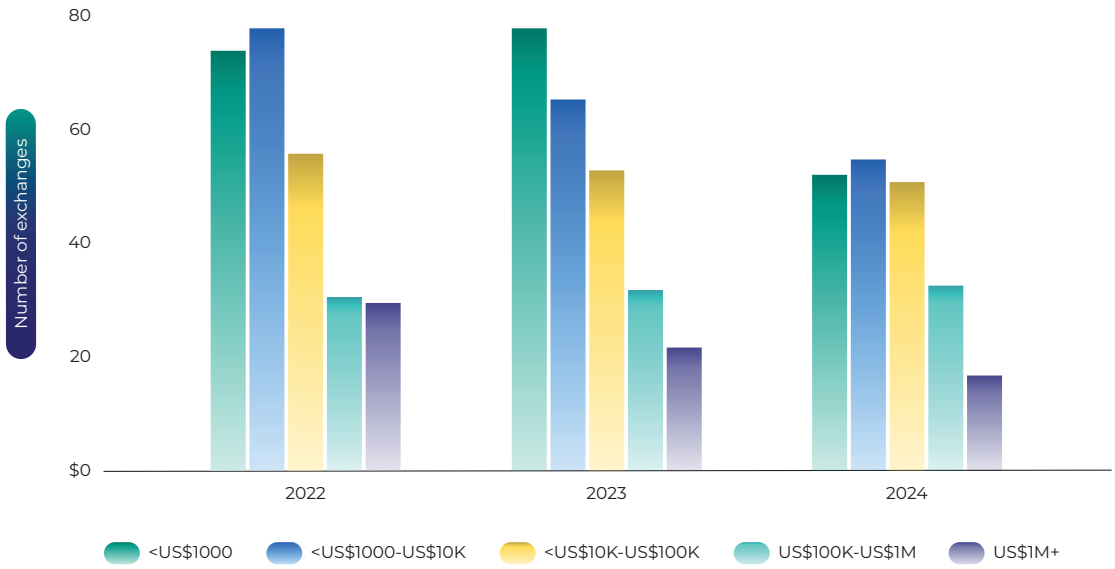
A. Shadow Finance: Iran's Role in Laundering and Sanctions Evasion via Crypto	
Actor	Iranian-Affiliated Threat Groups
Strategic Objectives	The primary goal is to evade economic sanctions and finance state-aligned proxy operations across the region. Crypto plays a key role in enabling opaque cross-border financial transfers.
Scope of Activity	In 2024 and early 2025, over US$300M in crypto transactions were linked to Iran. Funds were primarily derived from ransomware, extortion, and sanctioned financial entities.

Tactics and Tools	Use of ransomware groups like Phobos and Midas to demand Bitcoin/Monero payments. Integration with low-KYC exchanges, privacy-preserving chains, and stablecoin bridges (notably USDT on Tron and Ethereum).
Laundering Workflow	Leveraged regional OTC brokers, illicit front companies, and DeFi infrastructure to obscure fund origins. Combined illicit flows with legitimate trade activity to blur audit trails.

Source: TRM Labs, 2025

Figure 7.10:

Number of exchanges interacting with Iranian services (both inflow and outflow) **by total transfer size** (2022-2024)



Source: The Chainalysis Crypto Crime Report, 2025

7.8 Recovery and Negotiation Tactics

In the wake of high-value exploits, crypto exchanges and decentralized protocols have increasingly turned to a diverse set of strategies to recover stolen funds or engage with malicious actors. These tactics are not merely technical but also deeply behavioural, legal, and social. On-chain messaging platforms, social media, and DAO governance forums have emerged as unconventional but effective negotiation spaces. Common strategies include: appealing to attackers' ethics through open letters, incentivising returns via white-hat bounties or legal amnesty, engaging communities in governance-led recovery votes, and publicly tracking hacker wallets to restrict laundering pathways. While not all efforts lead to full restitution, these approaches have collectively shaped a new layer of post-incident response mechanisms, redefining accountability and resilience in the digital asset ecosystem.

The following real-world examples illustrate the strategies adopted by exchanges and protocols to reclaim stolen funds or negotiate with attackers post-incident:

Table 7.6:

Case Study: Poly Network – Hacker Dialogue via Social Media

A. The Hacker Who Spoke Back: Poly Network's Ethical Grey Zone	
Platform	Poly Network
Summary	After a US$611M hack, the attacker began communicating with the team via on-chain messages and social media, asserting their white-hat intentions.

Negotiation Strategy	Poly Network publicly acknowledged the hacker's cooperation and requested the return of funds, reinforcing trust-building over threats.
Outcome	Funds were gradually returned; the hacker was offered a security advisor role and bounty, though they declined. This case reshaped perspectives on ethical hackers and exploit communication.
Post Incident Improvement	Poly Network implemented multi-signature authorisation and real-time monitoring for cross-chain contract calls after the hack, reducing single points of failure.

Source: Reuters, 2021

Case Study: Euler Finance – On-Chain Open Letter

B. Negotiating with Anonymity: Euler Finance's On-Chain Open Letter

Platform	Euler Finance
Summary	In March 2023, US$197M was stolen via a flash loan exploit. The team posted an on-chain open letter appealing to the hacker's conscience.
Negotiation Strategy	Euler initiated negotiations with empathy, offered a bounty, and publicly tracked fund movements, avoiding legal threats initially.
Outcome	The hacker returned most funds after weeks of back-and-forth. Euler issued a public thank-you and increased engagement in white-hat incentives.
Post Incident Improvement	Euler conducted comprehensive audits and added circuit breakers to prevent similar flash loan exploits.

Source: Coinbase, 2023

Case Study: Mango Markets – DAO-Governed Negotiation

C. Governance on Trial: Mango Markets' Hacker-Led Proposal and DAO Vote

Platform	Mango Markets (Solana-based)
Summary	A user manipulated oracle prices in October 2022 to drain US$114M. He later proposed to return funds in exchange for a legal immunity vote via DAO.
Negotiation Strategy	The DAO community held a vote on the hacker's proposal and partially accepted the terms for fund return, effectively legalising the arrangement on-chain.
Outcome	Roughly US$67M was returned. The case highlighted the legal grey areas of DAO-driven "reparative" negotiation.
Post Incident Improvement	Mango updated its governance model, introducing higher quorum thresholds and emergency vetoes for DAO votes.

Source: Yahoo Finance, 2022

Case Study: Nomad Bridge – Public Refund Campaign

D. The Nomad White-Hat Campaign: A Community Call for Reversing Chaos

Platform	Nomad Bridge
Summary	US$190M was exploited in August 2022 after a smart contract bug was discovered. Multiple unrelated actors joined in draining the bridge.
Negotiation Strategy	Nomad launched a public amnesty campaign for white-hat returners, pledging no legal retaliation if funds were returned voluntarily.
Outcome	Over US$36M was recovered. While not fully restored, the campaign was seen as a partial success and set a precedent for coordinated recovery under chaotic attack vectors.
Post Incident Improvement	Nomad upgraded its smart contract upgradeability controls and partnered with external auditors.

Source: TRM Labs, 2025

Case Study: Transit Swap – Hacker Helped Fix Vulnerability

E. Transit Swap's Compromise Recovery: Collaboration Over Confrontation

Platform	Transit Swap (BSC-based DEX aggregator)
Summary	In October 2022, an exploit drained US$21M. The hacker responded to communications within 24 hours.
Negotiation Strategy	Transit offered the hacker a reduced bounty and legal immunity in exchange for return and vulnerability details.
Outcome	Approximately US$18.9M was returned. The hacker's cooperation was used to patch the protocol's routing logic and inform similar DEX designs.
Post Incident Improvement	Transit deployed enhanced routing logic testing frameworks and mandatory third-party audits before upgrades.

Source: Cointelegraph, 2022

7.9 Global Regulatory Reactions to High-Profile Crypto Incidents

In response to the increasing frequency and magnitude of crypto exploits and data breaches, governments around the world have begun to operationalise more aggressive regulatory frameworks, investigative collaborations, and punitive actions.

Authorities in the United States, the European Union, and the Asia-Pacific have not only issued sanctions and seizure warrants but have also deepened interagency coordination and public-private intelligence sharing. A growing number of jurisdictions have established specialised crypto-financial investigation units, empowered FIUs with blockchain analytics tools, and begun enforcing real-time disclosure obligations for crypto service providers.

"Global crime is borderless, but law enforcement remains bordered. Even within Europe, tools like the European Investigation Order help, but globally cooperation is still fragmented. Without stronger international enforcement mechanisms, regulations alone are insufficient — criminals will continue to exploit jurisdictional gaps."

Sungyong Kang - Criminal Intelligence Officer, Interpol Financial Crime and Anti-corruption Centre

"Fraud and scams are our biggest concern. At one point, 90% of scam proceeds exited through crypto channels. We have imposed KYC requirements, quotas, and delays on crypto transfers to disrupt these flows. Balancing innovation with consumer protection is our central challenge."

Dr Daranee Saeju - Assistant Governor, Bank of Thailand

Table 7.7:

Case Study: U.S. Department of Justice – Bitfinex Asset Recovery (2022)

A. Bitfinex Asset Recovery: Blockchain Analytics in Enforcement	
Jurisdiction	United States
Platform	Bitfinex
Regulators Involved	DOJ, FBI, and IRS-C
Target	Two individuals involved in laundering funds stolen from Bitfinex (2016 hack)
Incident Summary	The DOJ traced and seized 94,000 BTC (worth US$3.6B) that were part of the original Bitfinex hack.
Regulatory Response	DOJ, FBI, and IRS-CI used blockchain analytics, warrants, and chain attribution to seize assets and arrest suspects in New York.

Source: DoJ, 2023

Case Study: Netherlands – Tornado Cash Developer Arrest (2022)

B. Developer Accountability: Criminal Liability in Open-Source Decentralized Protocol	
Jurisdiction	Netherlands
Platform	Tornado Cash
Regulators Involved	Netherlands – Tornado Cash Developer Arrest (FIOD), Public Prosecution Service of the Netherlands (Openbaar Ministerie), U.S. Treasury Department's OFAC
Target	One of Tornado Cash's core developers
Incident Summary	After OFAC sanctioned Tornado Cash for facilitating money laundering, Dutch authorities arrested a core developer linked to the platform.
Regulatory Response	The FIOD arrested the developer, signalling that developers of laundering-enabling protocols may face legal liability.

Source: Rechtspraak, 2024

7.10 Gaps and Barriers

Despite growing sophistication in detection, attribution, and response, meaningful gaps persist across the digital asset privacy and security landscape. First, the absence of global standards for key management, especially among cross-border custodial service providers, creates a fragmented security baseline. Many platforms continue to rely on insecure hot wallet configurations or opaque access controls, heightening susceptibility to private key compromises. Second, smart contract vulnerabilities remain prolific due to poor auditing standards and the proliferation of copy-pasted code. Incident disclosure also remains inconsistent; protocols are under no binding obligation in many jurisdictions to notify users or regulators swiftly after a breach. Moreover, the legal ambiguity around governance exploits, white-hat negotiations, and bounty-driven restitution limits enforceability and may incentivise rogue behaviour under the guise of ethical hacking. Lastly, data protection frameworks like GDPR or PDPA are often ill-equipped to handle pseudonymous blockchain data, further complicating recourse pathways for affected users.

GFTN Survey Insights: Privacy & Security

Survey Insight 7.1

Fraud and Scam Risks in Digital Assets

79%

79% of respondents flagged fraud and scams as a highly critical risk, making it the most cited threat in the digital asset ecosystem from a regulatory priorities standpoint. This highlight growing concerns over deceptive schemes, phishing attacks, and misuse of private keys, especially affecting retail users in under-regulated environments.

Survey Insight 7.2

Addressing Cybersecurity Threats in Crypto

75%

75% of respondents rated cybersecurity threats as a critical concern from a regulatory priorities standpoint. This underscores the urgent need for enhanced security infrastructure, including smart contract audits, multi-signature custody protocols, and layered defence mechanisms to protect against hacks, protocol exploits, and infrastructure attacks.

Survey Insight 7.3

Digital Asset Platforms and Operational Risks

23%

Cybersecurity and operational risks were cited by 23% of respondents as one of their main priorities, reinforcing the ecosystem's ongoing struggle with platform vulnerabilities, protocol exploits, and infrastructure mismanagement.

7.11 Risk Implications and Technology Solutions

The risk landscape outlined in this chapter underscores that privacy, security, and operational vulnerabilities in the digital asset ecosystem may become systemic threats with implications for financial stability and consumer trust. Private key compromises expose billions in user funds to single points of failure; bridge exploits and cross-chain laundering schemes demonstrate how vulnerabilities in one protocol can cascade across entire markets; and insider threats, rug pulls, and social engineering illustrate the persistent conduct and governance risks that weaken resilience.

Advances in cryptography, identity frameworks, and supervisory technology offer regulators and market actors new tools to embed resilience into the system itself. Multi-Party Computation strengthens custody by reducing single points of failure, ZKPs enable compliance without exposing sensitive data, and blockchain analytics enhance the detection of illicit flows across chains. In the next chapter, we will explore how such technologies are beginning to move from pilot stage to practical deployment, and how they have the potential to mitigate the risks highlighted here.

7.12 Future Outlook

Looking forward, the supervision of privacy and cybersecurity in digital assets cannot rely on static rules alone. The rapid pace of innovation, combined with the growing involvement of nation-state actors and sophisticated criminal groups, underscores the importance for regulators to consider a scenario-based approach to supervision and policy design. This allows supervisory frameworks to anticipate multiple possible futures, translate risks into measurable regulatory priorities, and embed guardrails that both industry and regulators can monitor.

Scenario 1: Programmable Compliance at Scale (Optimistic Case)

- **Scenario Description:** Stablecoins and tokenized real-world assets (RWAs) embed compliance features at issuance, such as allow-lists, FATF Travel-Rule payloads, and zero-knowledge proofs for selective disclosure. Compliance becomes "programmable," reducing reliance on ex-post monitoring.

- **GFTN Proposed Guardrails:**
  - Introduce a certification scheme for "compliance-capable contracts" that verifies embedded AML/KYC modules.
  - Establish measurable targets, such as tracking the percentage of stablecoin supply under policy controls, reported quarterly.
  - Establish a supervisory data pipeline that requires digital asset issuers to send standard, machine-readable quarterly reports to supervisors, feed them into risk dashboards to track market risks and automate stress tests with alerts (liquidity/redemption shocks; triggers for LCR, reserve diversification, concentration caps).
  - Establish supervisory colleges for major issuers and exchanges, bringing together payments, securities, prudential and other relevant authorities, to coordinate across the full lifecycle: licensing, ongoing supervision, and incident response.

- **Supervisory Priority:** Develop frameworks for auditing ZK-proof systems and ensuring interoperability between compliance-embedded tokens across jurisdictions. Build infrastructure to ingest data feeds such as the quarterly reports, agree upon a common data format and API specifications, enable onward sharing with foreign supervisors, and run periodic joint stress tests.

Scenario 2: Sovereign-Grade Exploits on Tokenized Bonds (Stressed Case)

- **Scenario Description:** A state-sponsored actor targets an RWA oracle or cross-chain bridge during a spike in government bond redemptions, leading to manipulation of redemption prices and liquidity freezes.

- **GFTN Proposed Guardrails:**
  - Mandatory circuit-breakers for tokenized securities, halting transactions under abnormal price or volume swings.
  - Liquidity backstops (capital buffers or pre-arranged lines with custodians) for regulated RWA issuers.
  - Crisis disclosure runbooks requiring immediate regulatory notification and coordinated industry response.
  - Mandate active-active redundancy and rapid failover for critical components (oracles, bridges, custody) and conduct coordinated crisis exercises with regulators and trading venues to align trading halts, liquidity support, and public communications

- **Supervisory Priority:** Establish RWA stress-testing protocols that simulate oracle or bridge compromise scenarios, with reporting obligations to regulators.

Scenario 3: Retail Harm via Rug-Pulls and Key-Theft (Base Case)

- **Scenario Description:** Despite industry progress, a long tail of smaller-scale losses persists through rug-pulls, phishing, and private key compromises. Retail investors remain the most affected victims, eroding confidence in DeFi.

- **GFTN Proposed Guardrails:**
  - Establish minimum licensing and disclosure standards for DeFi platforms serving retail, with requirements such as proof of audit, wallet-segmentation practices, and key management standards. In parallel, consider baseline consumer protection measures at the exchange level, including wallet allowlisting by default and default insurance coverage up to a specified cap.
  - Mandate retail harm dashboards that track rug-pull and key-theft incidents by jurisdiction, linked to consumer education campaigns.
  - Mandate a short, standardized "Key Facts" disclosure for all retail crypto/DeFi platforms that covers risks, fees, lock-up periods, conflicts, and incident/insurance coverage.
  - Apply activity-based retail safeguards to all providers, centralized or decentralized, including suitability disclosures (whether the product's risk, complexity, and volatility are appropriate for the customer), fair-marketing rules, and a complaints/redress process.

- **Supervisory Priority:** Harmonise consumer-protection standards across crypto asset services with activity-based coverage similar to MiCA, extending obligations even to decentralized applications once they exceed thresholds of user adoption.

Scenario-based guardrails provide regulators with a dynamic supervisory toolkit. Optimistic cases can be supported through certification and innovation sandboxes; Stressed cases can be contained through structural safeguards and disclosure rules; and Base-case risks can be managed through targeted retail protections. This forward-looking, scenario-driven approach ensures that supervisory regimes remain adaptive, measurable, and globally harmonised.

8 Emerging Technologies & Future Trends

8.1 Introduction

The next phase of the digital asset ecosystem is being shaped by a concentrated set of privacy-enhancing, security-strengthening, and interoperability-enabling technologies. Rather than emerging in isolation, these tools are converging to address regulators' most persistent challenges, ensuring market integrity, enabling proportionate oversight, and maintaining user trust in decentralized environments. From advanced cryptography for selective disclosure to AI-enabled risk monitoring and cross-chain infrastructure that preserves auditability, the focus is shifting toward embedding compliance and resilience directly into the technology stack.

While regulatory adoption of emerging digital asset technologies is still uneven, several trends indicate accelerating uptake. For example, the European Commission has set a goal for 80%[163] of E.U. citizens to actively use the EUDI Wallet by 2030, signalling a strong policy commitment to decentralized and verifiable identity. In blockchain analytics, Chainalysis reports serving over 1,300 customers globally, including nearly 300 public sector agencies, underscoring the increasing reliance of law enforcement and regulators on on-chain intelligence tools.[164] In the cross-chain interoperability space, LayerZero claims that its messaging and OFT standard now covers roughly 70%[165] of the total stablecoin market cap and cross-chain messaging volume. MPC plays a central role in institutional custody strategies; Fireblocks and EY jointly acknowledge it as a leading standard for secure wallet infrastructure, reinforcing operational resilience.[166]

GFTN Survey Insights: Emerging Technologies & Future Trends

Survey Insight 8.1

Infrastructure Challenges in Digital Assets

40%

Insufficient infrastructure was identified by 40% of respondents as a significant barrier to the mainstream adoption of digital assets. Challenges related to access, security, liquidity, scalability, and regulatory compliance can undermine trust, usability, and confidence, factors that are essential for widespread adoption.

Survey Insight 8.2

Technological Limitations in Digital Assets

19%

Technological limitations were identified by 19% of respondents as a significant barrier to the mainstream adoption of digital assets. Issues such as network scalability, security vulnerabilities, and complex user interfaces can reduce usability, trust, and seamless integration, thereby hindering broader adoption.

Survey Insight 8.3

Regulatory Flexibility for Digital Asset Innovation

11%

11% of respondents believe that technology-neutral regulation can support innovation and growth in digital assets. By establishing a flexible, future-proof framework that encourages experimentation without favouring any specific technology, such regulation can balance safety with adaptability, fostering innovation, competition, and sustainable growth in the digital asset ecosystem.

[163] European Commission, 2024
[164] Chainalysis, 2024
[165] Layerzero, 2025
[166] Fireblocks, 202

Table 8.1 maps the main categories of emerging technologies against their core focus and expected relevance to the financial system over the next 5–10 years. It highlights how privacy tools, identity frameworks, custody innovations, and interoperability solutions are converging to address regulatory and market priorities.

Table 8.1:

Emerging Technologies and associated use-cases

Use Case	Technologies	Core Focus	Relevance to the Financial System (Next 5–10 Years)
Privacy & Confidentiality	1. Zero-Knowledge Proofs 2. Fully Homomorphic Encryption	Advanced cryptographic methods to preserve data confidentiality while enabling verifiable computation and compliance-friendly transparency.	ZKPs and FHE will allow financial institutions to verify compliance (e.g. AML/KYC status) without revealing sensitive customer information. In 5–10 years, these technologies can enable privacy-preserving regulatory reporting, secure interbank data exchange, and encrypted compliance audits.
Identity & Compliance	1. Verifiable Credentials 2. Self-Sovereign Identity	Decentralized identity systems that streamline KYC/AML processes while maintaining user privacy and regulatory compliance.	These tools can reduce onboarding friction, eliminate identity fraud, and enable portable KYC across borders and platforms. Banks, wallets and exchanges may rely on global interoperable identity standards, cutting cost and complexity of customer verification.
Security & Custody	1. Multi-Party Computation 2. Quantum-Resistant Cryptography	Strengthening private key security, detecting illicit activity, and enabling real-time regulatory oversight of on-chain transactions.	MPC will redefine custody models for custodians, enabling collaborative control over assets without key exposure. As quantum threats emerge, quantum-resistant cryptography will become mandatory for secure digital asset infrastructure.
Automation & Intelligence	1. Generative AI 2. Blockchain Analytics	Leveraging AI for autonomous decision-making, predictive analysis, fraud detection, and automated compliance in decentralized environments.	AI-enabled analytics will automate suspicious activity detection, conduct real-time risk scoring, and drive regulatory reporting intelligence. In 5–10 years, regulators may deploy AI-driven supervision models, especially for complex DeFi environments.
Interoperability & Scalability	1. Cross-Chain Messaging Protocols 2. Oracles	Enabling seamless data and value transfer across heterogeneous blockchain networks, supporting scalable DeFi and multi-chain applications.	Cross-chain infrastructure will underpin tokenized finance and programmable money by ensuring secure interoperability. Oracles will evolve to become regulated data feeds critical to executing smart contracts in financial-grade applications.

8.2 Key Emerging Technologies and Applications

This section reviews the technologies most likely to define the next phase of digital asset adoption. These innovations go beyond pilots; they are already being tested by banks, custodians, and regulators, with clear implications for compliance, market resilience, and systemic oversight. The following table sets out the adoption status, risks, benefits, and cost–revenue opportunities of these technologies, providing a forward-looking view of where supervisory attention might be required.

Table 8.2:

Adoption Trends, Risks and Benefits of Emerging Technologies in Digital Assets

Technology	Adoption Status (2025)	Risk Considerations	Potential Benefits	Potential Revenue & Cost Optimisation Opportunities
Zero-Knowledge Proofs	Actively used in privacy-preservin g blockchain projects (Zcash, Mina, Starknet), with growing enterprise testing in compliance.	• **Medium:** Implementation complexity • Interoperability challenges • Still lacks widespread regulatory clarity	• **High:** Enables selective disclosure of compliance information challenges • Bridges privacy and transparency requirements; ideal for AML/KYC proof without PII leaks	• **Revenue:** Launch private DeFi products, offer privacy-as-a-service • **Cost:** Reduces KYC friction and verification redundancies across entities
Fully Homomorphic Encryption	Still in early prototype stage; IBM, Microsoft, and DARPA-led pilots underway. Limited production deployments due to performance costs.	• **High:** Computationally expensive, hardware-intensive • Regulatory uncertainty around encrypted compliance systems	• **High:** (long-term): Enables real-time AML/analytics on encrypted data • Vital for privacy-preserving Regtech and cross-border PII control	• **Revenue:** High-value data analytics services for institutions • **Cost:** Reduces data breach exposure, avoids data replication overhead
Verifiable Credentials & Self-Sovereign Identity	Pilots launched under EBSI (E.U.), MAS sandbox trials, and W3C-aligned identity networks.	• **Medium:** Interoperability across issuers still limited • Fragmentation in trust registries • User revocation flows are underdeveloped	• **High:** Transforms onboarding, KYC updates, and cross-jurisdiction portability • Reduces repeated verification costs	• **Revenue:** White-labeled KYC identity vaults, cross-border identity monetisation • **Cost:** Cuts onboarding and re-verification costs by around 50–80%
Generative AI (for compliance)	Actively used in SAR drafting, fraud pattern detection, and model-driven AML scoring across crypto compliance teams and Tier 1 banks.	• **Medium:** Risk of false positives/negatives, hallucinations • Lacks legal auditability unless explainability standards are enforced	• **Very High:** Cuts compliance overhead by 50–70% • Enables proactive AML investigation triggers, improves STR quality	• **Revenue:** Sell AI compliance tooling, proactive risk advisory services • **Cost:** May reduce human compliance overhead by 60–70% in large institutions
Multi-Party Computation	Used in Coinbase Custody, Fireblocks, Copper, and Zodia; widely deployed in institutional crypto custody.	• **Low:** Battle-tested in many settings • Regulatory concerns mainly around operational governance (not tech)	• **High:** Eliminates single-point-of-fail ure, improves institutional confidence, essential for tokenized asset custody	• **Revenue:** Launch institutional custody products (B2B, tokenized assets) • **Cost:** Avoids fraud and key-loss liabilities; reduces insurance premiums

Blockchain Analytics	Ubiquitously used by regulators, VASPs, and financial surveillance units.	• **Low-Medium:** Black-box models, may mislabel addresses • Privacy tradeoffs remain a concern	• **Very High:** Drives risk scoring, wallet monitoring, sanctions screening, and real-time analytics at scale	• **Revenue:** Provide analytics APIs, wallet risk scores, regulator dashboards • **Cost:** Cuts manual review burden, automates Travel Rule and sanctions screening
Cross-chain messaging & Oracles	Widely adopted (Chainlink CCIP, LayerZero); used in bridges, DEXs, and liquid staking protocols.	• **High:** Frequent target of exploits, oracle price manipulation still a concern	• **High:** Enables cross-chain value flow, supports interoperability for compliance data, DeFi-TradFi integration	• **Revenue:** Launch compliance-enabled bridges; support cross-chain financial flows • **Cost:** Reduces integration costs with DeFi partners, avoids bridge downtime losses
Quantum-resistant cryptography	Still experimental; NIST shortlisted algorithms (e.g. Kyber, Dilithium) under test.	• **Low-Immediate, High-Future:** Threat window opens around 2030 • Current crypto infra not ready	• **High:** Critical for future-proofing CBDCs, secure key management, and identity protection in the post-quantum era	• **Revenue:** Offer quantum-compliant vaults or custody • **Cost:** Future-proofs infrastructure; avoids costly overhauls later

8.2.1 Privacy & Confidentiality

Cryptographic advances are enabling compliance checks and regulatory reporting without exposing sensitive user data. These approaches balance user confidentiality with verifiable oversight, creating new pathways for privacy-preserving supervision.

Trend 1: Zero-Knowledge Proofs

Definition: ZKPs are cryptographic protocols that allow one party to prove the truth of a statement without revealing any underlying data. In blockchain contexts, these mechanisms enable verification, such as balance, transaction legitimacy, and eligibility, without disclosing identity or transaction specifics.

Trends:

- **Scalable cryptography frameworks:** zk-SNARKs and zk-STARKs have become scalable and cost-efficient enough to power production-grade solutions (e.g. Ethereum Layer-2s like zkSync, StarkNet).
- **Regulatory experimentation:** Regulators are exploring selective disclosure frameworks (e.g. AML compliance proofs) that allow institutions to submit zero-knowledge attestations instead of raw data. The BIS Innovation Hub has included ZKPs in its PET taxonomies as a key enabler for privacy-preserving supervision.
- **Early pilots and compliance use cases:** At present, ZKPs are primarily being tested in pilots and proofs-of-concept (e.g. Polygon ID, zkSync) rather than as mainstream regulatory tools. However, early pilots for privacy-preserving identity and AML/KYC compliance suggest potential pathways for broader adoption as standards mature.

Applications:

- **AML/KYC "proofs without data":** exchanges or custodians can prove compliance (e.g. sanctions-checked) to regulators using a ZKP, while preserving user privacy
- **CBDC design:** central banks, like those involved in Project Aurum 2.0 (HKMA & BIS), are prototyping retail CBDCs that allow transaction blinding, while regulators can audit selectively via ZKP triggers.
- **DeFi compliance:** protocols can require proofs of solvency or LTV thresholds via ZKP before unlocking risk functions or governance.

Case Study:

Project Aurum 2.0 (Hong Kong): The BIS Innovation Hub, together with the Hong Kong Monetary Authority, prototyped retail CBDC issuance using ZKPs to enable privacy-preserving transactions with selective regulatory auditability. The pilot informed CBDC privacy architecture discussions across central banks.

Trend 2: Fully Homomorphic Encryption

Definition: FHE allows computation to be performed on encrypted data, producing encrypted results that, when decrypted, match the outputs of the same operations run on plain text. In practice, this means analytics can be conducted without exposing raw input data.

Trends:

- **Institutional experimentation:** IBM and other vendors now offer FHE frameworks and prototyping toolkits, bringing FHE from academic theory into institutional experimentation.
- **DeFi compliance initiatives:** In the DeFi space, FHE is gaining attention for enabling encrypted watermarking, private risk scoring, and AML testing while preserving data confidentiality.

Applications:

- **Encrypted AML analytics:** VASPs or regulators can run sanction screening or behavioural models on encrypted wallet data without ever decrypting personally identifiable transactions.
- **Privacy-preserving Regtech:** Central banks and supervisory agencies can use FHE to evaluate aggregated risk metrics from encrypted bank submissions without access to customer-level data.
- **Confidential smart contract inputs:** DeFi protocols could accept encrypted state inputs for governance, triggering events only if criteria are met, without exposing sensitive data.

Case Study:

CryptoLab & UClone Partnership: In April 2025, CryptoLab partnered with UClone to launch FHE-powered AI agents for consumers. This initiative demonstrates how FHE can move beyond research and institutional pilots into everyday applications, enabling secure AI-driven services while ensuring that sensitive personal data remains encrypted throughout processing.

"There is a structural gap between permissionless blockchains and the way banks manage AML and KYC. Today, banks cannot control who holds tokens once they move on a public chain. Zero-knowledge proofs and new identity models may eventually bridge this, but risk policies need to evolve too."

David Hui - Chief Commercial Officer, DBS Digital Exchange

"Zero-knowledge proofs are critical to the future of compliance and privacy. They allow a user to demonstrate exactly what an authority needs to know—identity or eligibility—without exposing irrelevant personal data. This not only reduces privacy risks but also relieves financial institutions from maintaining massive compliance databases, freeing up resources for better AML monitoring."

Joe Kohler - Chief Legal and Chief Operating Officer, Nethermind

8.2.2 Identity & Compliance

Decentralized identity frameworks offer the potential to streamline onboarding, reduce fraud, and support cross-border KYC portability. By embedding compliance into reusable digital credentials, these tools could lower costs while enhancing regulatory assurance.

Trend 3: Verifiable Credentials

Definition: VCs are tamper-evident, cryptographically signed digital attestations (such as identity, licence, or compliance status) that holders can present selectively. They enable trust in decentralized ecosystems without requiring personal data to be broadly exposed.

Trends:

- **Rapid adoption via eIDAS 2.0:** The European Commission is actively rolling out the EUDI Wallet, with pilots across finance, mobile ID, and education, targeting 80% citizen adoption by 2030. This standardisation pushes VCs toward mainstream use.
- **Cross-border interoperability pilots:** Standards bodies such as the OpenID Foundation, EDSSI, and Hyperledger Aries are accelerating interoperable VC deployment, paving the way for global portability of KYC credentials and licensing.

Applications:

- **Onboarding reuse:** A user who has been verified by a trusted issuer (e.g. a bank or KYC provider) can present a VC to multiple VASPs or crypto platforms without repeating identity checks, reducing redundancies and data exposure.
- **Regulator-issued attestations:** Supervisory authorities could provide regulated entities with VCs for licences or compliance status, allowing firms to present them to counterparties or auditors in verifiable format.
- **Encrypted Travel Rule compliance:** VCs help exchanges send encrypted identity attestations across transfers, avoiding manual data entry while fulfilling FATF Travel Rule requirements.

Case Study:

Polygon ID by Polygon Labs: Polygon has developed Polygon ID, a solution allowing users to carry VCs such as “jurisdictions verified” or “accredited investor,” which can then be selectively and privately proved to DeFi protocols or NFT platforms. This approach enables compliance gates (e.g. restricting access by geography or KYC status) without disclosing personally identifiable information. Early integrations include decentralized exchanges and art marketplaces on Polygon.

Trend 4: Self-Sovereign Identity

Definition: SSI is a decentralized identity framework where individuals or organisations control their own digital identity without reliance on a central issuing authority. It uses blockchain or distributed ledger technology to verify credentials, while giving users granular control over what information is shared, with whom, and for how long.

Trends:

- **Rising integration into national ID ecosystems:** Countries like Estonia, Canada, and South Korea are integrating SSI principles into digital ID rollouts to give citizens greater privacy and interoperability.
- **Financial services adoption:** SSI is increasingly tested in DeFi onboarding, where privacy-preserving verification enables regulatory compliance without creating honeypots of personal data.
- **Standards development:** The DIF and W3C are advancing interoperability standards that combine SSI with Verifiable Credentials, reducing silos across industries.

Applications:

- **Privacy-preserving compliance:** Users can satisfy AML/KYC checks by proving required attributes (e.g. age, residency) without exposing unrelated personal details.
- **Cross-border regulatory alignment:** Regulators could recognise SSI-based credentials for licensing or onboarding, streamlining compliance for multi-jurisdictional entities.
- **Fraud prevention in DeFi:** SSI frameworks reduce identity theft by ensuring the holder must cryptographically prove ownership of credentials during onboarding

Case Study:

LACChain SSI Initiative – Inter-American Development Bank: The IDB's LACChain network has implemented SSI-based identity for financial inclusion in Latin America, enabling citizens without formal banking history to prove credentials and access DeFi and microcredit platforms. The SSI framework is interoperable across participating countries and is being explored for compliance use in crypto remittances.

8.2.3 Security & Custody

Custody remains the cornerstone of trust in the digital asset ecosystem. Emerging solutions like MPC distribute control of private keys, while post-quantum algorithms future-proof critical infrastructure against the next wave of cryptographic threats.

Trend 5: Multi-Party Computation

Definition: MPC is a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In the context of digital assets, MPC enables secure private key management by splitting the key into multiple encrypted shares, which are distributed across different entities or systems. No single party ever has access to the complete key, reducing single points of failure.

Trends:

- **Institutional adoption:** Custodians like Fireblocks and Coinbase Custody have integrated MPC to replace traditional HSMs for key storage.
- **Integration in DeFi wallets:** MPC is increasingly embedded in retail and institutional wallet solutions to enable recoverability without compromising security.
- **Regulatory interest:** MPC is being evaluated as part of secure custody compliance frameworks in jurisdictions like Hong Kong and Singapore.

Applications:

- **Secure cross-jurisdictional custody:** Regulators can require MPC-based custody for licensed entities to ensure resilience against insider threats.
- **Disaster recovery assurance:** MPC-based recovery workflows allow institutions to rotate keys without downtime, enhancing operational continuity.

Case Study:

Zodia Custody (Standard Chartered) uses MPC to provide bank-grade digital asset custody for institutions. By leveraging MPC key sharding across independent environments, Zodia meets the FCA's custody compliance requirements while enabling instant transaction approvals.

Trend 6: Quantum-Resistant Cryptography

Definition: Quantum-Resistant Cryptography (also known as post-quantum cryptography) comprises cryptographic algorithms designed to remain secure against the computational power of quantum computers. They protect against future threats that could break widely used signature and encryption systems.

Trends:

- **Venture-backed innovation:** The QANplatform, a Layer-1 blockchain, raised US$15M in VC funding (Dec 2023) explicitly to build quantum-resistant infrastructure suitable for enterprise and DeFi use cases.
- **Lattice-based cryptography adoption:** The platform leverages lattice-based cryptography and hash and is featured as a use case in discussions of future-proof blockchain architecture.
- **Hybrid cryptographic models:** The field is moving toward hybrid models combining classical and quantum-resistant algorithms as part of multi-layered security approaches for DeFi custody, message signing, and consensus.
- **Quantum threat preparedness:** Quantum computing poses a long-term systemic risk to current cryptographic standards. While no present-day systems are at risk, preparations for migration to post-quantum cryptography are already underway.

Applications:

- **Data integrity and audit trails:** Financial institutions and custodians handling high-value tokenized assets could implement quantum-resistant digital signatures in audit logs, transaction attestations, and smart-contract state histories to ensure future verifiability even after quantum-era attacks become feasible.
- **Third-party risk:** Oracles and cross-chain routers must prove they operate on quantum-secure stacks to win listings or compliance clearance.

Case Study:

Quranium Mainnet Launch: In February 2025, Quranium launched its mainnet alongside the QSafe Wallet, introducing a quantum-resistant blockchain platform built to counter the risks posed by quantum computing. The project integrates post-quantum cryptography at the protocol and wallet level, positioning itself as a secure infrastructure layer for the next era of blockchain systems.

"Decentralized infrastructure is the next frontier. We are watching how AI and blockchain combine, with blockchain providing decentralized records and AI optimizing processes. Quantum technologies are also on our radar, with several promising French startups we already support. These will reshape finance alongside digital assets."

Arnaud Caudoux - Deputy Chief Executive Officer, BPI France

8.2.4 Automation & Intelligence

Artificial intelligence and advanced analytics are moving from pilot use cases into supervisory practice. These technologies can automate fraud detection, enhance suspicious activity reporting, and give regulators real-time visibility into complex DeFi markets.

Trend 7: Generative AI

Definition: GenAI refers to models that create or transform content, text, code, images, or synthetic data, often fine-tuned for domain tasks. In supervision, it is used to triage signals, summarise large evidence sets, and augment human analysis, not to replace formal decision-making.

Trends:

- **Supervisory adoption is moving from pilots to tools.** The BIS Innovation Hub's Project AISE develops AI assistants to help supervisors triage risks, accelerate on-site work, and synthesise large document sets.
- **Regulators are building governance rails.** The U.K. FCA has set up an AI Lab and published updates on how it will oversee AI use in finance (model risk, accountability, data governance). ESMA's Data Strategy 2023–2028 likewise embeds AI/ML into analytics and supervisory workflows.

Applications:

- **Market-abuse surveillance augmentation** (pattern mining, narrative stitching across tickets, comms, and on-chain data).
- **Case file synthesis** (SAR triage, cross-entity link analysis, entity-resolution summaries).
- **Policy & consultation analysis** summarising responses, extracting risk themes for rulemaking).

Case Study:

Kraken's Use of Generative AI in M&A Due Diligence: When Kraken, the crypto exchange, evaluated the acquisition of NinjaTrader (a derivatives platform), its team used Termina, an AI-powered due diligence engine, to accelerate the process. Generative AI analysed vast datasets—financial records, customer behaviour, and operations—and generated a detailed report in mere hours, dramatically reducing the time required for review.

Trend 8: Blockchain Analytics

Definition: Blockchain analytics refers to the process of examining, interpreting, and deriving meaningful insights from blockchain data. It involves analysing transactions, addresses, and patterns on public blockchains to understand the flow of funds, identify suspicious activities, and trace the origin and destination of cryptocurrencies.

Trends:

- **Mainstream adoption by regulators:** Authorities like FinCEN, FCA, and MAS now integrate blockchain analytics into supervisory frameworks.
- **AI-enhanced detection:** Leading tools like Chainalysis Reactor, Elliptic Navigator, and TRM Labs use machine learning to detect cross-chain laundering and sanction evasion.
- **Cross-border cooperation:** Data-sharing between national FIUs through analytics platforms is rising, enabling coordinated enforcement.

Applications:

- **Real-time risk flagging:** Regulators can proactively block transactions linked to sanctioned addresses.
- **Market abuse detection:** Enables identification of pump-and-dump schemes, insider trading, and wash trading in token markets.

Case Study:

Coinbase & TRM Labs: Blockchain Analytics in Action

When U.S. law enforcement investigated a high-stakes crypto fraud case involving tens of millions of dollars, Coinbase's compliance team partnered with TRM Labs to trace illicit flows across multiple blockchains. TRM's analytics platform mapped complex transaction patterns, identified links between pseudonymous wallets, and uncovered off-ramping channels into fiat. This intelligence enabled investigators to freeze assets and build a prosecutable case against the perpetrators. The collaboration showcased how blockchain analytics can serve as a critical tool in combating financial crime, providing transparency and accountability in otherwise opaque crypto markets.

"We are beginning to explore the intersection of blockchain and AI, especially in programmability. There's also active interest in quantum resilience and efficiency gains in financial market infrastructure. We see tokenization helping to streamline intermediaries, reduce reconciliation workloads, and create shared infrastructure for complex transaction chains."

Audrey Metzger - Director, Innovation and Financial Markets Infrastructures, Banque de France

"The next big development will be the intersection of blockchain and artificial intelligence. Blockchains can provide decentralized records of what AI agents are doing, protecting against manipulation or fabricated activity. As AI agents become active in trading, they will need crypto or stablecoins to transact, since they cannot hold bank accounts."

Joe Kohler - Chief Legal and Chief Operating Officer, Nethermind

"The intersection of AI and blockchain is particularly interesting. AI agents will increasingly participate in markets, but they cannot hold bank accounts. Stablecoins and blockchain payments make micro-transactions feasible. Blockchains can also provide auditable records of AI activity, addressing concerns around manipulation or opacity."

Pradyumna Agrawal - Managing Director, Investment, Temasek

"I would like to see blockchain and AI come together. Blockchain provides transparency and immutability, while AI offers diagnostics and predictive analysis. Used in combination, they could streamline compliance, enhance monitoring, and create new efficiencies. These technologies should not be seen as separate silos but as complementary tools for solving industry-wide challenges."

Park Kwan Hoon - Executive Director, Group Strategic Planning Office, OCBC

"Blockchain analytics tools are essential. Data is available on-chain, but interpreting it requires sophisticated analysis. That is why we invest in commercial tools and provide training to resource-constrained countries. With projects like Rescue, we are equipping Southeast and South Asian law enforcement with tools and expertise to investigate blockchain-based crime."

Sungyong Kang - Criminal Intelligence Officer, Interpol Financial Crime and Anti-corruption Centre

8.2.5 Interoperability & Scalability

As tokenized finance expands across multiple blockchains, interoperability becomes a systemic requirement. Cross-chain protocols and trusted oracles are critical to ensuring secure settlement, accurate data feeds, and continuity across heterogeneous networks.

Trend 9: Cross-Chain Messaging Protocols

Definition: Cross-chain messaging protocols pass verifiable messages (and optionally tokens) between heterogeneous blockchains, enabling actions like asset transfers, state updates, and risk controls across chains without centralized custodial bridges.

Trends:

- **Programmable messaging is standardising:** Protocols such as LayerZero v2 expose "message libraries," packet formats, and configurable DVNs, shifting control and security configuration to the application layer.
- **Defence-in-depth models are maturing:** Chainlink CCIP adds an independent Risk Management Network to continuously monitor cross-chain operations, reflecting lessons from prior bridge exploits.

Applications:

- **Token mobility with provenance:** Supervisors can observe end-to-end flows (origin → message → execution) across chains, improving sanctions screening and AML analytics.
- **Cross-chain controls:** Protocol-level guardrails (threshold verifiers, RMNs) and signed messages enable fail-safes and halts when anomalies arise.
- **Liquidity and settlement risk management:** Native burn-and-mint designs reduce wrapped-asset risk and fragmented liquidity across venues.

Case Study:

Circle's Cross-Chain Transfer Protocol:

CCTP moves USDC natively across multiple chains using a burn-and-mint process with generalised message passing and off-chain attestations, eliminating custodial lock-and-mint wrappers and unifying liquidity. Circle provides public documentation, quickstarts, and architecture notes that detail the message flow and supported networks.

Trend 10: Oracles

Definition: Oracles are systems that securely bring real-world data (such as price feeds, event outcomes, or weather data) onto blockchain networks to enable smart contracts to interact with external information. Trusted or decentralized oracle services ensure that on-chain logic can rely on accurate, timely, and verifiable inputs.

Trends:

- **Decentralized data infrastructure:** Decentralized oracle networks (e.g. Chainlink) have become the de facto standard for reliable, tamper-resistant data feeds for DeFi, NFTs, and interchain protocols..
- **Resilience and reliability mechanisms:** There is a growing emphasis on resilient oracles featuring multi-party consensus, SLA guarantees, fallback mechanisms, and real-time monitoring.
- **Critical DeFi infrastructure**: Oracles are increasingly viewed as critical infrastructure in DeFi and regulated token markets, subject to governance, audit, and operational risk protocols.

Applications:

- **Resilience requirements:** DeFi protocols and licensed entities should require oracle setups with fallback sources, multi-signer threshold models, and monitoring dashboards.
- **Auditability:** Exchanges and stablecoin issuers can use signed oracle proofs as evidence of compliance, price accuracy, or collateral valuation.
- **Surveillance:** Regulators can tap Oracle timelogs to detect or investigate suspicious market patterns or manipulation.

Case Study:

Hedge Oracle Integration via Chainlink:

Hedge, a DeFi lending platform on Solana offering interest-free loans in exchange for collateral, integrated Chainlink Price Feeds to ensure secure, tamper-resistant valuations of collateral assets. This was critical for executing timely liquidations and supporting their redemption mechanics, which allow users to redeem USH (Hedge's stablecoin) for the underlying collateral at accurate prices.

"Looking ahead to 2026, Chainlink's success will be defined by its establishment as the global standard for on-chain finance. This includes the widespread use of Chainlink services, like CCIP, Data Feeds, and the Chainlink Runtime Environment among top financial institutions and the digital asset ecosystem, across jurisdictions and asset classes."

Niki Ariyasinghe - Head of Business Development, Asia-Pacific and Middle East, Chainlink Labs

8.3 Evolution Trajectories for Emerging Technologies & Trends

This section builds upon the preceding analysis by introducing three trajectories to track the evolution of emerging technologies and trends in the digital asset ecosystem. The first considers the time horizons over which emerging technologies are likely to mature and scale. The second examines the convergence of technologies, highlighting how their combined use may unlock both transformative opportunities and new categories of risk. The third considers regional dynamics and strategic watchpoints for policymakers, emphasising how policy choices and market structures differ across jurisdictions.

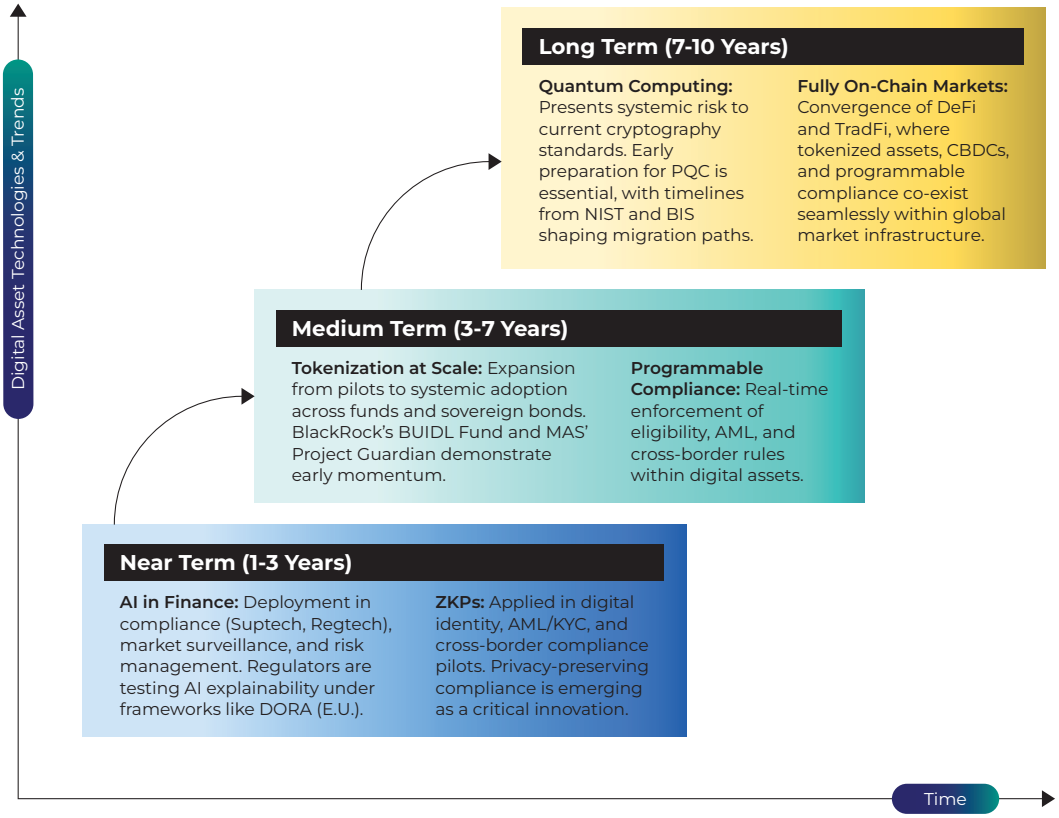
Together, these perspectives provide a structured framework for anticipating how these emerging technologies, business trends, and regulation will interact in shaping digital assets by 2030 and beyond.

8.3.1 Evolution Trajectory Across Time Horizons

Figure 8.1 presents a time-phased framework for the evolution of emerging technologies & trends in the digital asset ecosystem.

Figure 8.1:

Time Horizons for Emerging Technologies & Trends



Source: GFTN Analysis

In the near term, innovation is already observable, with AI systems being piloted in compliance[167], supervisory technology[168], and market surveillance[169] contexts. ZKPs are simultaneously emerging in identity and privacy-preserving compliance pilots.[170]

> "AI is supercharging criminal activity. Deepfakes and advanced automation could enable hackers to steal billions, and this risk is likely to worsen over the next few years. At the same time, detection frameworks will also grow more seamless, leading to an ongoing cat-and-mouse game between illicit actors and regulators."
>
> **Ari Redbord** - Global Head of Policy and Government Affairs, TRM Labs

Over the medium term, the infrastructure for tokenization across funds, sovereign bonds, and other real-world assets, is expected to become viable, alongside the embedding of programmable compliance that enables real-time enforcement of eligibility and anti-money laundering requirements. In the long term, quantum computing may introduce systemic risks to existing cryptographic standards and anticipating this cryptographic standardisation bodies, such as NIST[171] and BIS[172], are already publishing roadmaps for post-quantum cryptography, signalling the importance of long-term risk planning with regards to emerging technologies.

> "The next phase shift may come from ultra high-performance layer twos that stream blocks in real-time. This could unlock entirely new categories of on-chain activity. AI will matter eventually, but it is still too early. Quantum risks are real but at least 15 years out."
>
> **Haseeb Qureshi** - Managing Partner, Dragonfly

---

[167] Bradsol, 2025
[168] BIS, 2025
[169] FCA, 2025
[170] Inatba, 2025
[171] NIST, 2024
[172] BIS, 2025

Over the next decade, the vision of fully on-chain markets is expected to materialise, characterised by the convergence of DeFi and TradFi[173] within an integrated environment where tokenized assets, CBDCs, and programmable compliance function seamlessly as part of global financial infrastructure.

8.3.2 Evolution Trajectory Through Convergence

Figure 8.2 emphasises that the deep value in emerging technologies and trends often lies not in isolated development but in their convergence.

AI-enhanced DeFi[174] can embed predictive compliance and fraud detection directly into decentralized protocols, but raises governance and explainability risks.[175] In parallel, the convergence of quantum computing and post-quantum cryptography highlights the dual trajectory of risk and resilience. While quantum breakthroughs could undermine existing cryptographic systems, coordinated migration[176] to PQC standards led by bodies such as NIST is emerging as a global safeguard. Another important synergy lies in the use of ZKPs as a privacy-preserving technology that enables identity verification while meeting regulatory AML requirements. Moreover, tokenization coupled with the power of data oracles, allow real-world events (rates, delivery status, ESG metrics) to trigger contractual logic embedded in smart contracts. But this also heightens oracle manipulation, data integrity risk, and governance challenges that policymakers need to watch out for.

Figure 8.2:

Convergence of Technologies & Trends

Source: GFTN Analysis

[173] Lighthouse partners, 2025
[174] Truststrategy, 2024
[175] Mitosis University, 2025
[176] NIST, 2025

8.3.3 Evolution Trajectory Across Regions

Table 8.3 presents the emerging trends landscape as of 2025, the projected trajectories for 2026, and the principal indicators that could be monitored for various regions. In the E.U., MiCA is live and DORA standards are enforced, paving the way for institutional tokenization pilots. In Asia (Singapore, Japan, Hong Kong), regulators are actively incubating infrastructure (Project Guardian, digital-yen sandbox, Hong Kong tokenized securities). Meanwhile, the U.S. continues in a state of regulatory fragmentation, even as AI and quantum leadership remain national priorities. In MENA (U.A.E, Saudi Arabia), sovereign tokenization and cross-border corridor experiments (mBridge) are expected to accelerate further next year.

Table 8.3:

Regional Dynamics in Digital Asset Technologies and Trends

Region	2025 Baseline	2026 Trend	Key Indicators to Track
E.U.	MiCA framework operational; DORA resilience standards in force; PQC standardisation underway.	↑ Institutional tokenization pilots launched, with emphasis on harmonisation of cross-border settlement.	MiCA licensing approvals; PQC adoption roadmap; ESMA guidance updates.
Asia (Singapore, Japan, Hong Kong)	Project Guardian (SG), digital yen sandbox (JP), and tokenized securities framework (H.K.) active.	↑ Expansion of tokenized funds and sovereign bond pilots; increased central bank experimentation with wholesale CBDCs.	Supervisory technology (Suptech) adoption; rollout of tokenized securities regimes.
U.S.	Fragmented regulation; jurisdictional overlap between the SEC and CFTC; private-sector leadership in AI and quantum applications.	↔ Continuation of regulatory disputes; strong momentum in private-sector AI and quantum innovation.	Congressional bills; AI explainability mandates; federal funding for quantum research.
MENA (U.A.E., K.S.A.)	U.A.E.'s VARA rulebooks implemented; Dubai real estate tokenization pilots; regional participation in mBridge.	↑ Acceleration of sovereign tokenization programmes, particularly in real estate and sovereign wealth sectors.	State-backed pilot launches; tokenized RWA frameworks; regional CBDC linkages.

Source: GFTN Analysis

8.3.4 Strategic Watchpoints for Policymakers

As adoption of emerging technologies accelerates and new trends emerge in the digital asset ecosystem, policymakers should remain vigilant to a set of critical watchpoints that cut across supervisory priorities and market maturity. Table 8.4 provides a structured overview of these watchpoints, alongside their current status, the key metrics that should be monitored annually, and the principal risks that may warrant early regulatory attention.

These watchpoints are already visible in market activity and regulatory experimentation. AI is being piloted in compliance and supervisory technology, yet a lack of explainability standards could expose firms and regulators to algorithmic blind spots. ZKPs are moving from proof-of-concept into compliance pilots, but absent interoperability standards risk creating fragmented silos. Tokenization of real-world assets has surpassed US$31 billion[177] in market value, but unresolved questions on legal enforceability raise the possibility of liquidity fragmentation. Meanwhile, quantum computing remains at the development stage, with NIST and BIS leading roadmaps for post-quantum cryptography. The absence of institutional migration plans leaves the financial system exposed to sudden cryptographic vulnerabilities.

For policymakers, these watchpoints highlight the importance of proactive monitoring. Establishing harmonised standards, mandating transparency, and coordinating across jurisdictions will be central to ensuring that innovation strengthens rather than destabilises financial markets as the digital asset industry matures.

[177] RWA, accessed 29th September 2025

Table 8.4:

Regional Dynamics in Digital Asset Technologies and Trends

Strategic Watchpoint	2025 Status	Metrics to Monitor Annually	Principal Risks and Red Flags
AI	Pilots underway in Suptech and Regtech.	Number of regulatory AI pilots; adoption of AI governance and explainability frameworks.	Algorithmic failures; lack of explainability standards; risk of biased or opaque decision-making.
ZKPs	Early pilots in digital identity and compliance processes.	Number of regulatory-recognised ZKP pilots; publication of interoperability standards.	Fragmentation across ecosystems; lack of cross-border recognition of proofs.
Tokenization	Approximately US$31B RWA market; early institutional pilots active.	Growth in tokenized market capitalisation; number of regulated tokenization licences issued.	Liquidity fragmentation; unresolved questions around legal enforceability of tokenized claims.
Quantum Computing	Research and development stage; PQC roadmap developed by NIST and BIS.	Progress of PQC adoption; implementation of industry migration checklists by financial institutions.	Lack of migration planning within institutions; systemic vulnerabilities if legacy cryptography is broken.

Source: GFTN Analysis

8.4 Future Outlook

The next phase of digital assets will not be defined by any single technology, but by a sequential maturity of technologies and trends and convergence. In the near term (2026-27), AI and ZKP pilots are expected to determine how far regulators can embed compliance into technology and protocols itself. By the early 2030s, tokenization and programmable compliance are likely to underpin systemic capital markets infrastructure. Looking further ahead, quantum computing poses an existential risk, requiring coordinated PQC migration. Meanwhile, the convergence of AI, tokenization, and oracles will redefine supervision and risk management. For policymakers, the imperative is to move from reactive oversight to anticipatory governance, which includes the monitoring of technology maturity, the pace and scale of adoption, and the systematic tracking of critical watchpoints and areas of convergence. For industry, competitive advantage will go to firms who can operationalise these tools while navigating fragmented regulatory landscapes.

9 Recommendations for Digital Asset Ecosystem Stakeholders

9.1 Recommendations for Regulators

Regulatory approaches to digital assets should reflect the differing stages of market evolution across jurisdictions. **Developed economies** are now in a position to integrate digital assets into mainstream finance, with advanced regulatory and supervisory capacity allowing them to focus on interoperability, prudential safeguards, and systemic oversight. By contrast, **emerging economies** face a dual imperative: harnessing digital assets as tools for financial inclusion and economic development, while also protecting monetary sovereignty and containing risks such as capital flight. In this sense, emerging markets can use digital assets to leapfrog development, enabling broader access to payments, credit, and investment opportunities where traditional financial infrastructure is less mature.

One critical distinction lies in consumer awareness and market sophistication. In advanced economies, retail investors generally have higher financial literacy, and regulators are able to focus on calibrating disclosure and risk frameworks. In emerging markets, however, first-time investors often encounter digital assets without sufficient awareness of volatility, fraud, or cyber risks. This makes consumer education and basic safeguards a critical regulatory priority.

Despite these differences, there are also common regulatory priorities across both developed and emerging markets. Safeguarding financial stability is paramount: stablecoins, tokenized assets, or DeFi arrangements should not undermine banking systems or trigger systemic shocks. Likewise, ensuring consumer and investor protection remains a universal objective, whether through disclosure standards, segregation of client assets, or prudential oversight of key intermediaries. Both groups of jurisdictions also grapple with AML/CFT compliance, data privacy, and cybersecurity risks, which transcend borders and require international coordination.

Drawing on interview insights, the GFTN survey, and our extensive research on market trends and regulatory initiatives, the recommendations are organised around key themes — **Stablecoins, Tokenization, Crypto Exchanges and Retail Access, Staking, DeFi, and AML, Privacy, and Security Risks.** Within each theme, we provide differentiated guidance for developed and emerging economies, recognising their distinct regulatory priorities, while also identifying shared objectives that support a more resilient, transparent, and inclusive global digital asset ecosystem.

9.1.1 Recommendations for Regulators: Oversight of Stablecoins

Developed Economies: Regulate stablecoins as systemic payment instruments with bank-grade safeguards.

- Regulators in advanced markets may consider integrating stablecoins into the regulated financial system under robust safeguards. This means imposing bank-like prudential requirements on major stablecoin issuers (e.g. capital and liquidity standards to ensure 1:1 redemption) and strict oversight of reserves to prevent runs. Several developed economies, including the E.U. under MiCA and Japan under the PSA, have already taken steps in this direction. Other jurisdictions may take inspiration from these first movers and design comparable frameworks tailored to their own market maturity and financial stability priorities.

- Stablecoins that reach systemic scale could be overseen in coordination with banks, given their potential to impact payment systems and financial stability. Regulators could introduce a tiered prudential framework that differentiates between systemically important and smaller stablecoin issuers, applying proportionate capital, liquidity and redemption requirements. Similar to the higher minimum capital and countercyclical buffer requirements applied to global systemically important banks (G-SIBs), large stablecoin issuers could be required to maintain a liquidity coverage ratio of 110–120%, ensuring sufficient high-quality liquid assets to withstand severe but plausible stress scenarios, such as a 30-day redemption shock, a sharp de-pegging event, or a sudden loss of market confidence triggering mass withdrawals. Larger issuers may also be mandated by the regulators to publish real-time reserve attestations, stress test outcomes, and redemption queue visibility. Supervisory authorities across jurisdictions may also conduct joint liquidity stress tests for systemically important stablecoin issuers to assess potential spillovers into payment systems and short-term credit markets.

- Authorities could also prioritise enforcing transparency (regular reserve audits and disclosures) and consumer protection rules for stablecoins, in line with emerging international standards, so that these instruments truly function at par with fiat money without undermining the "singleness" of the currency. Supervisors could integrate market-integrity and operational-resilience testing, ensuring that issuers maintain 1:1 redemption capability and robust governance controls to prevent illicit or manipulative activity.

- Regulators could ensure full AML/CFT compliance, including embedding the FATF Travel Rule into stablecoin transactions where intermediaries are involved. Licensed issuers and wallet providers should conduct customer due diligence, maintain transaction records, and be subject to suspicious transaction reporting.

- Cross-border cooperation is essential, as many stablecoin arrangements operate globally. Developed market regulators could lead in establishing information-sharing and joint supervision frameworks for stablecoins. However, this remains quite challenging to implement in practice, as supervisory coordination across jurisdictions is often slow, resource-intensive, and constrained by differing regulatory priorities. These limitations should be acknowledged when assessing timelines for adoption.

Emerging Economies: Leverage stablecoins for inclusion, but contain currency substitution and capital flight.

- Regulators in emerging markets should remain vigilant about stablecoins' impact on monetary sovereignty and financial stability.

- In economies with high inflation or weak currencies, foreign currency-pegged stablecoins often become attractive as a store of value, which can accelerate currency substitution and potentially weaken the local currency. To manage risks of currency substitution, authorities may consider interim measures that limit the use of stablecoins in sensitive areas such as large-value payments, tax settlements, or government transfers. At the same time, a pathway could be established for regulated corridors, such as remittances or salary disbursements, subject to appropriate caps and guardrails. As stablecoins gain traction for remittances and micro-payments, authorities could embed real-time transaction monitoring and regional cooperation for suspicious-activity alerts. Over the longer term, a more sustainable approach lies in reinforcing macroeconomic fundamentals and strengthening domestic digital payment infrastructure.

- Regulators should acknowledge the benefits stablecoins offer (such as cheaper remittances and access to savings in more stable currency) and thus may consider crafting frameworks to supervise and integrate them in national frameworks. This may include treating stablecoins as financial assets or e-money under existing laws, requiring local licensing for issuers or wallet providers, and coordinating with other countries (and issuers) to manage cross-border flows.

- Crucially, capital flow management measures could be updated for the digital assets age. Authorities may need to monitor and limit large stablecoin-related outflows to guard against excessive capital flight in volatile times.

- Supervisory frameworks of emerging economies could integrate stablecoin activity within capital flow management and monetary oversight systems, ensuring that issuers and intermediaries report detailed data on cross-border transactions, counterparties, and redemption patterns. Strengthening such reporting obligations would help authorities monitor circumvention of foreign exchange regulations and guard against destabilising outflows during episodes of volatility.

- To mitigate illicit finance risks, emerging market regulators could implement Travel Rule compliance and standard AML/KYC requirements for stablecoin issuers, wallet providers, and exchanges operating in their jurisdiction. Where regulatory capacity is limited, regional cooperation (e.g. shared utilities for KYC and transaction monitoring) could help reduce costs and strengthen enforcement.

9.1.2 Recommendations for Regulators: Oversight of Tokenization

Tokenization Scope & Sequencing

Tokenization can be applied across a broad spectrum of assets. The sequencing of regulatory frameworks, however, should be guided by each jurisdiction's economic priorities, market maturity, and consumer and institutional demand. While regulators set the pace and scope of oversight, the sequencing of specific asset classes or commercial innovations may in practice be shaped primarily through industry activity and public-private experimentation. Regulators may also wish to support pilots for selected asset classes within regulatory sandboxes that can help them create an evidence base for proportionate rulemaking.

- **Financial assets:** Regulators could recognise that tokenization has the greatest near-term applicability for financial instruments with established valuation and liquidity frameworks. This includes cash-equivalents such as MMFs, government securities, and commercial paper, as well as sovereign and corporate bonds, fund units/ETFs, repos and securities lending transactions, and trade finance receivables. Over time, tokenization can extend to more complex products such as equities and derivatives, once legal certainty and market infrastructure are sufficiently mature.
- **Non-financial assets:** Beyond traditional financial markets, tokenization can unlock value across a wide spectrum of real-world assets. Priority categories include real estate and land titles, commodities and warehouse receipts, carbon credits, royalties and intellectual property, supply-chain receivables and invoices, as well as tickets and loyalty points. For these assets, tokenization can improve collateralization, expand investor access, and enhance transparency in historically opaque markets.

Developed Economies: Modernise legal frameworks to enable tokenized markets, focus on integrating tokenization into existing capital markets starting with cash-equivalents and high-grade collateral, then scale to other asset classes.

Priority tokenization use cases for industry pilots and sandboxes:

- **Financial use cases:** Initial pilots could focus on relatively low-risk asset classes such as MMFs, short-dated government securities, and repo collateral as pilot assets. These instruments offer clear pricing, daily NAVs, established disclosure regimes, and strong liquidity, making them ideal for early adoption. Over time, expand to corporate bonds, fund units/ETFs, securitizations, and eventually equities and derivatives, once market infrastructure and regulatory clarity are in place.
- **Non-financial use cases:** Focus on real estate and land titles, commodities and warehouse receipts, and intellectual property/royalties to test interoperability with existing registries and settlement systems. These assets can unlock operational efficiencies and improve collateral mobilisation in wholesale markets.

Regulatory guardrails (Make tokens investable, not just digital)

- Regulators in developed markets should proactively update legal and regulatory frameworks to accommodate asset tokenization. This includes clarifying the legal status of tokenized assets; for example, recognising digital tokens as representations of ownership or securities under existing laws, to give investors clear rights and protections.
- Regulators could mandate disclosure and reporting frameworks that mirror traditional securities standards. Issuers of tokenized assets could be required to publish prospectus- or whitepaper-style documents, adhere to consistent NAV and valuation methodologies, and provide ongoing reporting (e.g. portfolio composition for tokenized MMFs). These measures ensure investors can make informed decisions and that tokens are priced transparently.
- Regulators could require segregation of client assets and mandate the use of qualified custodians or regulated banks for the safekeeping of underlying instruments. At the token layer, market standards for key management, wallet security, and recovery mechanisms should be enforced to reduce risks of mismanagement or theft.
- Authorities could permit issuance and regulated secondary trading of tokenized assets on platforms that provide the same level of oversight and investor protection as traditional exchanges. Tokenized high-quality assets could also be deemed eligible collateral for repo and central bank facilities, reinforcing market confidence and utility.
- Supervisors may also establish baseline expectations for cybersecurity and operational resilience in tokenized markets. This includes mandatory smart contract audits, change-management protocols, and

safeguards against oracle or data-feed manipulation. Incident reporting obligations could mirror those in traditional finance to ensure timely detection and resolution of risks.

- It is important to enforce the same standards on tokenized markets as traditional ones ("same activity, same risk, same regulation"): venues dealing in tokenized securities should follow securities laws and KYC/AML rules, and issuers of tokenized assets should provide proper disclosures and adhere to custody and audit requirements.
- Regulators could reinforce governance integrity by requiring functional independence between asset issuers, listing portals, and custodians, preventing conflicts of interest in token approval processes. Mandating independent review panels and conflict-of-interest disclosures would strengthen investor confidence and market fairness in this emerging asset class.
- Given tokenization's cross-border nature, developed economies' regulators ought to coordinate on interoperability standards and mutual recognition. This ensures a token issued in one jurisdiction can be legally traded in another under compatible rules, reducing regulatory arbitrage.

Emerging Economies: Leverage tokenization to democratise access, mobilise SME financing, and digitise real-world assets under simplified but robust guardrails.

Priority tokenization use cases:

- **Financial use cases:** Begin with government bonds, municipal/green bonds, and SME receivables to crowd-in retail and institutional participation.
- **Non-financial use cases:** Focus on land/real-estate registries, commodities and warehouse receipts, and carbon credits, which improve collateralization and financial inclusion.

Regulatory guardrails (Make tokens investable, not just digital)

- Emerging market regulators could view tokenization as an opportunity to leapfrog traditional financial market development, while still prioritising investor protection. By allowing fractional ownership through tokenization, regulators can broaden investment access to populations historically excluded from capital markets. For example, enabling tokenized micro-investments in infrastructure or SME loans could democratise financial access to underserved sectors.
- Regulators may consider crafting simple, clear rules for tokenized offerings, possibly adapting crowdfunding or sandbox regulations, to let startups experiment with tokenization use cases under oversight. At the same time, basic safeguards (such as requiring white papers/prospectuses for token offerings, fit-and-proper checks for platform operators, and limits on how much retail investors can invest in risky tokens) are crucial to prevent fraud.
- Regulators may partner with industry to educate the public on the risks and rights associated with tokenized assets. Additionally, emerging economies should keep pace with global regulatory thinking on tokenization.
- Notably, some smaller but agile financial centres (for example, Singapore, the U.A.E. and others) have moved faster in developing tokenization frameworks than larger economies. These jurisdictions, even though developed economies, have lessons for emerging markets. They demonstrate how innovation can be trialled at a manageable scale, through pilots, sandboxes, or phased rollouts, before extending to the wider economy. In practice, this could mean establishing dedicated 'tokenization hubs' in cities or zones designed for controlled experimentation, before a safer nationwide rollout. By studying these approaches, emerging market regulators can adapt proven methods for phased implementation, ensuring their frameworks remain internationally compatible while containing systemic risks.
- Finally, regulators need to tackle infrastructure challenges: improving internet connectivity and digital identity systems will help tokenization initiatives reach scale in developing markets.

9.1.3 Recommendations for Regulators: Oversight of Crypto Exchanges

Developed Economies: Licence and supervise exchanges as critical market infrastructure with Investor protection at the core.

- In advanced markets, regulators should impose comprehensive oversight on crypto exchanges and brokers to ensure market integrity and consumer protection on par with traditional investment platforms. Many of these safeguards, such as licensing, reserve audits, and client asset segregation, are already in place in certain jurisdictions (e.g., E.U. under MiCA, Japan's FIEA regime, or Singapore's PSA). However, approaches differ, and there is scope for greater harmonisation and cross-border alignment to avoid regulatory arbitrage.
- Licensing or registration should be mandatory for all significant crypto-asset service providers, with requirements for financial soundness and operational resilience.
- Specifically, exchanges must segregate client assets from their own funds (to prevent another FTX-style misuse of deposits) and should undergo regular audits.
- Regulators may also enforce transparency through requiring proof-of-reserves disclosures or audits to give users confidence that exchanges hold sufficient assets to meet liabilities.
- To protect retail investors, developed markets can set standards akin to securities markets: clear disclosure of risks, prohibition of misleading marketing, suitability or appropriateness tests for complex products, and limits on leverage offered to inexperienced traders.
- As exchanges face new-age cybersecurity risks, regulators may also consider implementing structured cybersecurity frameworks for exchanges, including independent penetration testing and clear incident-reporting timelines for breaches (e.g., T+24/T+72 disclosure standards). Authorities could also study the outcomes of formal bug bounty programmes run by exchanges, and consider integrating such practices into supervisory expectations. Additionally, oversight could be extended to cover insider threats, with rules on employee trading, conflict-of-interest disclosures, and whistleblowing protections.
- Regulators in developed economies should also actively monitor crypto advertising and social media promotions, clamping down on false claims. Finally, given that many large exchanges operate globally, developed regulators could coordinate cross-border supervision, sharing information on platform outages, hacks, or misconduct, to prevent bad actors from exploiting jurisdictional gaps.
- For exchanges operating across multiple jurisdictions, regulators could form supervisory colleges to share information on liquidity positions, operational resilience, and cyber-risk incidents. Establishing common definitions for leverage, collateralization, and client-asset segregation would promote greater regulatory convergence and reduce the scope for arbitrage between jurisdictions.
- Exchange frameworks could adopt functional separation between trading, custody, staking, and yield generation services, supported by mandatory governance firewalls. Supervisors may require enhanced group-level disclosures and independent audits of affiliated entities to reduce systemic conflicts of interest.

Emerging Economies: Provide regulatory clarity for exchanges while curbing fraud and unsafe retail access.

- Regulators in emerging markets face the challenge of nurturing a safe crypto trading environment despite often limited regulatory capacity. A top priority is to provide regulatory clarity to reduce uncertainty for both investors and legitimate businesses.
- By establishing a licensing regime aligned with international standards (including KYC/AML requirements and basic security protocols), authorities can encourage reputable global exchanges or competent local startups to operate under supervision, improving consumer choice and tax compliance. Oversight should address the security weaknesses by asking exchanges to maintain robust cybersecurity standards (e.g. requiring multi-factor authentication, cold storage for most funds, and incident reporting) to reduce hacks and fraud.
- Authorities may develop tiered licensing regimes requiring exchanges to demonstrate functional segregation before expanding into custodial or staking services. Such a phased approach supports safer market development and greater transparency, particularly as crypto exchanges in emerging markets

diversify into adjacent services, where overlapping operations could otherwise create conflicts of interest.

- Regulators could mandate that exchanges obtain insurance or contribute to a compensation fund to protect users in case of theft. Another focus is on integrating crypto platforms with the formal banking system. Where banks have been hesitant to serve crypto businesses due to compliance fears, regulators can consider issuing guidance or signal support for bank to explore partnerships with duly licensed exchanges. This ensures users have safe fiat on/off ramps instead of resorting to peer-to-peer trades that are harder to monitor. In addition, emerging market authorities should be mindful of capital flight via exchanges. They could require exchanges to report large foreign-currency crypto transactions and, if needed, impose limits or tighter scrutiny on conversions that might circumvent currency controls.

- Finally, strong consumer education initiatives are recommended: many first-time investors in emerging markets may be lured by crypto's promise without understanding volatility and scams. Regulators, possibly in collaboration with industry and international partners, should run awareness campaigns about the risks of crypto trading and the importance of using regulated platforms.

9.1.4 Recommendations for Regulators: Oversight of Staking Services

Developed Economies: Define staking as a regulated financial product when intermediated; protect users from hidden risks.

- In advanced economies, regulators may consider providing clear guidance on staking services, distinguishing between decentralized protocol participation and staking offered as a financial product. Many proof-of-stake networks allow users to "lock up" assets to secure the network in return for rewards, which, by itself (when done independently), has been deemed not an offer of securities by some regulators. However, when intermediaries pool investors' crypto and promise yield (so-called staking-as-a-service programs), this begins to resemble an investment product that may fall under securities or investment law.

- Rules for staking services could require explicit disclosure of lock-up periods, validation risks, and potential slashing losses. Custodial staking providers should also maintain segregated accounts and adequate risk buffers to protect users' funds in the event of validator downtime, underperformance, or slashing penalties.

- Regulators in developed markets could thus require that any company offering staking to retail (especially if it involves taking custody of users' assets and paying out returns) comply with applicable laws, for example, registering the offering or obtaining a licence, and providing proper disclosure of risks. Supervisors could require platforms to maintain capital buffers or reserve requirements against operational and liquidity risks, while ensuring that retail participation is limited to appropriately qualified investors or products offering transparent risk–return profiles.

- To avoid patchwork enforcement, clear rules or guidance could be issued. This might include criteria for when a staking service is not a security (e.g. if users retain control of keys and rewards are determined solely by protocol rules) versus when it is (e.g. a platform pools assets, adds managerial efforts or guarantees extra rewards).

- Additionally, regulators could impose investor protection measures on staking service providers. The service providers should disclose lock-up periods and potential loss risks (like slashing penalties where funds can be cut if a node misbehaves), and perhaps limit these services to appropriate investors. There is also a custody aspect; if a platform holds staked assets, regulators could ensure they follow custody safeguards similar to those for securities (segregation of assets, bankruptcy protections, etc.).

- By clarifying the regulatory status of staking and enforcing standards, developed markets can allow genuine network staking to flourish (supporting blockchain innovation) while curbing opaque high-yield schemes that could harm consumers.

Emerging Economies: Warn and limit risky yield schemes while building capacity for safe staking models.

- For emerging market regulators, staking is a newer area that may not yet be widespread in their jurisdiction, but it is important to get ahead of potential issues. The primary recommendation is investor education and warnings about risks associated with staking products.

- Emerging economies have seen their share of crypto

yield scams masquerading as “staking” or “investment programs,” where unsophisticated users are promised abnormally high returns.

- Regulators could clearly warn the public that any scheme guaranteeing fixed high yields (far above market rates) is likely too good to be true, and they should encourage use of regulated channels only. Because formal regulations on staking might not exist yet in many emerging markets, authorities could initially issue guidance or circulars stating that companies offering crypto staking services must register and comply with collective investment or banking laws, as applicable.

- In the interim, if the regulatory capacity is limited, simply prohibiting domestic platforms from offering staking to retail without approval might be prudent, as this prevents local startups from launching risky schemes until rules are set. Investors would then only access staking through foreign platforms, which underscores the need for cross-border regulatory cooperation. Where possible, emerging regulators may consider collaborating with international bodies to understand best practices for staking oversight (learning from the precedents in the U.S., E.U., etc.) and potentially leverage technical assistance to develop their own framework. Emerging market jurisdictions may also pilot limited-scale staking frameworks with capped exposure, while requiring domestic intermediaries to disclose performance history and network-level risks to retail participants.

- They might also consider a sandbox approach for staking: allow a pilot where a registered firm can offer staking with limited assets and close reporting, to study the risks before wider rollout. Finally, given that staking often involves locking assets in protocols that operate globally, emerging market authorities should maintain open communication with local banking and tech sectors, for example, ensuring that if banks or Fintechs get involved in staking, they adhere to risk management standards and limit exposures.

9.1.5 Recommendations for Regulators: Oversight of Decentralized Finance

Developed Economies: Extend oversight to DeFi through gateways and governance touchpoints without stifling innovation

- Regulators in developed markets could explore ways to address DeFi activities with a lighter-touch and more flexible approach, recognising both the opportunities and risks that come with open, decentralized systems. DeFi protocols for lending, trading, or asset management share similarities with traditional financial services, but their governance and operational structures often differ significantly. Rather than applying existing frameworks wholesale, authorities might focus first on encouraging greater transparency, robust disclosures, and strong operational safeguards from projects themselves.

- A growing risk is the competitive pressure DeFi platforms exert on bank deposits. With on-chain lending protocols often promoting materially higher interest rates than traditional savings accounts, there is a potential for deposit outflows from regulated banks. Over time, this could affect funding stability and liquidity in the traditional banking sector if left unmonitored. Regulators may wish to monitor interest rate differentials and develop stress-testing scenarios that incorporate the possibility of significant deposit flight toward DeFi markets.

- A second systemic concern arises from tokenization. As tokenized assets such as government securities, real estate, or funds are increasingly used as collateral within DeFi lending markets, the potential for contagion grows. Distress in DeFi markets could reverberate back into traditional finance if the underlying tokenized instruments sit on the balance sheets or under the custody of regulated financial institutions. Regulators should establish reporting requirements for institutions holding tokenized assets and assess cross-market exposures to ensure early identification of contagion channels.

- In many cases, effective oversight may emerge through industry-led standards and self-regulation, especially in areas like code audits, smart contract security, or voluntary reporting of key metrics. Regulatory involvement could concentrate on the most accessible or centralized touchpoints, such as web interfaces, custodial services, or governance groups, where traditional obligations like KYC or investor disclosures may be easier to implement. Additional governance touchpoints may include controls over protocol decision-making, such as multisignature arrangements for treasury management, on-chain voting safeguards, and transparency in protocol upgrade processes. This calibrated approach would allow regulators to monitor risks and protect users without stifling innovation, while also creating space for DeFi participants to demonstrate responsible practices through voluntary codes of conduct and self-regulatory frameworks.

- Collaborating through international standard setters could be crucial. IOSCO has developed policy recommendations to address DeFi risks, such as calling for better understanding of DeFi arrangements, transparency requirements, and accountability for those who can influence DeFi protocols.

- Developed economy regulators could implement such guidance, pushing DeFi towards more compliant and robust models. They can also encourage responsible innovation by setting up regulatory sandboxes or innovation hubs for DeFi, allowing developers to engage with regulators early. This can help strike a balance where beneficial aspects of DeFi (like efficiency and financial inclusion) are not stifled, while guarding against the serious risks (like hacks, opaque governance, and money laundering).

- Additionally, regulators could employ regulatory tech solutions such as on-chain analytics, to monitor DeFi activities (tracking large exposures or illicit finance patterns) in real-time, given the transparent nature of public blockchains. Supervisory frameworks could also embed mandatory technology governance and third-party audits for platforms facilitating DeFi access. DeFi protocols offering retail exposure may be asked to maintain transparency dashboards on liquidity, validator concentration, and risk metrics.

- The FSB has recommended that regulators may explore hosting blockchain nodes[178] to extract trade and transaction data directly from distributed ledgers, to reduce reliance on outdated reporting systems and private on-chain analytics vendors. Regulators could deploy permissioned node clusters connected to major public and private blockchains, integrated with Regtech data pipelines that automatically feed verified transaction, liquidity, and collateral data into prudential monitoring systems. This architecture would allow real-time visibility into large on-chain positions, cross-protocol exposures, and wallet interlinkages, enabling the early detection of leverage build-ups or liquidity mismatches. To maximise its value, coordination bodies such as the FSB and BIS Innovation Hub could standardise data schemas, validation protocols, and access governance frameworks, ensuring regulators across jurisdictions can interpret and act on blockchain data consistently. These data streams could be further embedded into stress-testing and systemic risk dashboards, providing early warnings of cross-border contagion channels between DeFi and TradFi.

Emerging Economies: Build knowledge and safeguards early, align with global DeFi standards to avoid regulatory gaps.

- For emerging markets, DeFi presents both a potential boon (access to financial services beyond local banks) and a route to bypassing local regulations (capital controls, investor protections).

- Regulators may consider investing in capacity building first to understand how DeFi works and its penetration in their markets. This may involve training staff on blockchain analysis and participating in international workshops on DeFi oversight. With this knowledge, emerging regulators can issue guidance to clarify that existing laws (e.g. securities, banking, or derivatives laws) apply to DeFi activities if there are identifiable persons or entities in their jurisdiction.

- For instance, if local developers create a DeFi lending app, they should be encouraged or required to follow licensing that would apply to a comparable Fintech lender. However, if the DeFi apps used are entirely foreign, emerging market authorities face limits in enforcement; thus, a focus on investor awareness and protection is key. They should warn users that DeFi carries significant risks: smart contract vulnerabilities, lack of recourse if things go wrong, and high volatility.

- Public advisories could be issued about major incidents (like hacks or collapses of popular DeFi platforms) to educate the local community on what can go awry. In terms of financial stability, regulators in countries with strict forex controls or banking rules need to monitor if residents are moving funds into DeFi as an escape route. If data analytics (possibly sourced from global partners) show large-scale outflows via decentralized exchanges or stablecoin bridges, authorities should consider proportionate responses, for example, enforcing FX regulations on the on/off-ramp points (banks and exchanges) to limit unchecked leakage.

- Emerging market regulators could engage with bodies like the FSB, IOSCO, and the IMF to contribute to and benefit from global DeFi policy development. Given that many emerging markets may lack the resources to build bespoke DeFi regulations from scratch, adopting international standards (once finalised) will provide a ready-made toolkit. Authorities could focus on regional collaboration for DeFi analytics, pooling technical expertise and supervisory data to identify manipulation patterns and cross-border contagion.

- Emerging-market regulators may establish regional DeFi observatories to coordinate data sharing and supervisory training, focusing on transaction analytics, governance risk, and protocol resilience. Participation in multilateral technical platforms would help ensure consistent standards for DeFi supervision across similar economies.

[178] FSB, 2025

9.1.6 Recommendations for Regulators: Mitigating AML, Privacy & Security Risks

Developed Economies: Embed FATF standards, ban or heavily scrutinise obscured transactions, and treat platforms as critical infrastructure.

- Regulators in developed countries may consider enforcing rigorous AML and CTF standards across the digital asset industry, while also addressing privacy and cybersecurity concerns.
- Concretely, this means requiring all crypto businesses (exchanges, wallet providers, payment processors, etc.) to comply with the FATF recommendations for virtual assets, including the "travel rule," which mandates that identifying information accompany crypto transactions between regulated entities.
- Developed market regulators may consider measures such as regulating or even prohibiting privacy coins and mixers/tumblers that thwart traceability to reduce AML blind spots.
- Where outright prohibitions are not considered appropriate, regulators may wish to require enhanced due diligence for transactions involving such tools. Simultaneously, data protection regulations (like GDPR in Europe) apply to crypto firms, and regulators need to ensure that exchanges and other services protect customer personal data and transaction information from breaches or misuse. Regular audits of data security practices could be instituted, given past hacks that leaked user info.
- AML/CFT, data-protection, and cybersecurity frameworks could be integrated into the broader prudential oversight of crypto-asset firms, to ensure that cyber incidents trigger supervisory escalation similar to prudential breaches. Periodic joint testing of operational resilience and information-security practices between financial and technology regulators could improve systemic defences against cyber contagion.
- On the security front, regulators could treat major crypto platforms as part of critical financial infrastructure, holding them to high cybersecurity standards. For example, exchanges could be required to have independent security audits, maintain insurance or capital reserves against hacking losses. In addition, regulators could establish crypto-specific incident disclosure requirements (e.g. reporting at T+24/T+72/D+30), and mandate minimum security baselines such as multi-party computation or hardware security modules for custodians, hot-wallet exposure limits (e.g. ≤2% of holdings), formal verification of critical smart contracts, and validator transparency for cross-chain bridges.
- Internationally, developed market regulators may consider sharing information on illicit crypto activities, for example, through FinCEN or Europol partnerships, so that enforcement can be coordinated when bad actors operate across borders.

Emerging Economies: Close AML gaps quickly, enforce basic cybersecurity, and partner internationally to build capacity.

- Emerging market regulators often have to play catch-up on AML and security, but doing so is crucial not just to protect their economies but also to maintain international financial links.
- The priority is to implement the FATF's AML/CFT standards in the crypto sector, if not already done. Many emerging economies have been slower to enforce the Travel Rule and VASP (Virtual Asset Service Provider) licensing, which has led to FATF concerns about regulatory arbitrage.
- Regulators could expedite issuing regulations or guidance that exchanges and other crypto businesses should register and comply with AML programs (customer due diligence, transaction monitoring, record-keeping). Not only will this help prevent terrorism financing or sanctions evasion through crypto, but it will also keep the country off FATF's grey list and preserve correspondent banking relationships.
- Given resource constraints, emerging regulators can leverage technology and international cooperation. Regulators may use blockchain analytics tools to trace illicit flows, or join international forums to receive training on crypto investigations.
- Rather than pursuing outright bans on privacy-enhancing coins, regulators may consider measures to ensure that regulated entities do not inadvertently provide easy conduits for opaque transactions. For example, an exchange in an emerging market could be prohibited from listing privacy coins that cannot be traced, and banks might be instructed to scrutinise large crypto movements that could be hiding under anonymising layers.
- Public communication is also key: authorities should inform citizens that even though crypto provides some privacy, it is not absolute, and misuse for crime

will be prosecuted (this can deter the perception that crypto is a lawless haven).

- Every emerging regulator should set basic cybersecurity requirements as part of licensing crypto firms. Even a small checklist, e.g. mandating the use of cold wallets for the bulk of customer assets, two-factor authentication for users, background checks for exchange employees (to prevent insider theft), and a robust operational security policy, can dramatically improve security outcomes.

- Furthermore, regional cooperation among emerging countries can be beneficial: threat intelligence about hacks or fraud schemes targeting one country's citizens can be shared quickly with others. Strengthening participation in cross-border AML information-sharing frameworks, including FATF and regional intelligence exchanges, would enhance collective capacity to trace illicit flows. Developing common minimum security standards and shared threat-intelligence networks across emerging markets could further reduce systemic vulnerabilities.

- Regulators in emerging economies could prioritise forensic capacity building and shared investigation utilities, integrating on-chain analytics with regional AML intelligence networks.

9.2 Recommendations for International Coordination Bodies

International coordination bodies such as the IMF, FSB, BIS, IOSCO, and FATF play a pivotal role in reducing fragmentation in the regulation of digital assets. Given the borderless nature of the digital assets ecosystem, isolated national efforts may have limited impact unless complemented by international coordination. Without harmonisation and standardisation, risks of regulatory arbitrage, uneven enforcement, and cross-border illicit finance will persist and may even scale as the industry grows. These coordination bodies are uniquely positioned to create a global baseline that national regulators can build upon, ensuring interoperability of rules and fostering customer confidence.

9.2.1 Strengthening International Coordination and Standard-Setting

Global standard-setters and coordinating organisations have a critical role in harmonising digital assets regulations and supporting national authorities, especially given the borderless nature of this industry. Key recommendations for these bodies include:

- **Develop and promote unified standards:** International bodies (IMF, FSB, BIS, IOSCO, FATF, and others) should continue to formulate clear, consensus-based standards for crypto-asset regulation. This includes common definitions (taxonomy of crypto assets), supervisory playbooks, cross-border sandboxes, and global disclosure templates. Practical actions could include: publishing baseline model laws for tokenization and stablecoins, maintaining a global directory of licensed VASPs to reduce regulatory arbitrage, and issuing compliance handbooks tailored to developed and emerging markets. These measures would complement the FSB's "same activity, same risk, same regulation" approach and ensure standards are purpose-built and actionable, not just aspirational.

- **Enhance cross-border cooperation and information sharing:** International coordination bodies could facilitate arrangements for regulators to cooperate on supervision and enforcement. Crypto markets operate across borders 24/7, and no single regulator can police all activities. Bodies like the FSB and IMF have urged countries to establish formal **information-sharing mechanisms** and supervisory colleges for globally active crypto firms. In practice, this could mean setting up supervisory colleges for VASPs and DeFi protocols, creating an international crypto incident-reporting platform (similar to IOSCO's fraud alert systems[179]), and developing templates for bilateral MoUs between regulators. The FATF can bolster this by accelerating its roadmap for global AML/CFT implementation in crypto, ensuring countries not only adopt rules but also share intel on illicit flows. Similarly, the BIS and other central bank groups can help coordinate monitoring of stablecoin usage across countries (important for understanding currency substitution and global liquidity impacts). An international registry of major crypto exchanges or issuers and their compliance status could be maintained to assist national regulators. In essence, these bodies could act as conveners for joint surveillance of the crypto ecosystem, so that a threat identified in one region (say, a large exchange showing signs of insolvency) can be quickly communicated and addressed collectively.

[179] IOSCO, 2025

- **Strengthen Cross-Border Supervisory Cooperation through a Global Crypto Oversight Network:** Building on IOSCO's recommendation 11[180], which calls for enhanced supervisory cooperation across the regulatory lifecycle, coordination bodies such as the FSB or BIS Innovation Hub could operationalise a crypto-specific supervisory cooperation network that facilitates continuous information exchange and joint oversight from authorisation and risk monitoring to enforcement. To make this effective, a Global Crypto Supervisory Forum can be conceptualised under the aegis of existing international coordination mechanisms. The forum could maintain a shared registry of licensed global crypto-asset service providers, support real-time supervisory data sharing through interoperable digital channels and coordinate joint risk assessments. To support consistent supervision, coordination bodies could further develop common supervisory templates and escalation protocols to harmonise how jurisdictions evaluate critical issues like stablecoin reserve management, custody risks, and cross-chain exposures. A shared data exchange layer could enable early detection of cross-border contagion risks and liquidity stress. By institutionalising such a networked model of oversight, coordination bodies can transform IOSCO's recommendation 11 into a practical supervisory infrastructure, ensuring regulators remain connected, informed, and coordinated in managing risks that transcend national boundaries.

- **Build regulatory capacity and support emerging economies:** A significant disparity exists between advanced and developing economies in regulatory resources for digital assets. International organisations could launch initiatives to **train and support** regulators in emerging markets. International organisations such as the IMF and World Bank are already providing technical assistance on digital assets. Building on this, they could expand the scope to include structured crypto-regulatory toolkits (e.g. model licensing frameworks for VASPs, template disclosure requirements for tokenized assets, and risk-based supervisory checklists), advanced supervisory training, and shared blockchain analytics platforms accessible to regulators in emerging economies. The G20's recent focus on crypto assets explicitly calls for including non-G20 countries in capacity-building efforts. This ensures that standards implementation is truly global and not limited to wealthy nations. Coordination bodies could set up knowledge-sharing platforms, where regulators can exchange best practices, case studies of enforcement, and even secondment programs (placing regulators from jurisdictions that are in earlier stages of digital assets regulation within more advanced supervisory agencies to learn best practices). By **uplifting the regulatory capacity** worldwide, international bodies reduce the chances of weak-link jurisdictions that could be exploited by criminals or become hotspots of unregulated activity.

- **Foster global consistency while allowing innovation:** The final recommendation recognises the balance needed in a rapidly evolving domain. Coordination bodies should aim for consistent baseline standards, such as capital requirements for stablecoin issuers or licensing criteria for exchanges, to be adopted everywhere, to prevent a race to the bottom. At the same time, they should not stifle beneficial innovation that could arise from healthy competition in regulatory approaches. One way to achieve this is through controlled experimentation: for example, the BIS Innovation Hub and other international groups can run cross-country pilots (for instance multi-CBDC platforms or regulated DeFi Innovation Hubs) which inform policy without risking instability. By sharing the lessons from such experiments widely, all jurisdictions can benefit and calibrate their rules. International bodies may also serve as neutral evaluators of different regulatory models and highlight what works best under what circumstances. Additionally, bodies may convene joint workshops for regulators to compare approaches to DeFi, stablecoin oversight, and digital identity, ensuring innovation is encouraged within clear supervisory guardrails.

9.3 Recommendations for Industry Players

While regulatory frameworks are essential, the resilience and credibility of the digital asset ecosystem also depend heavily on the conduct of industry participants themselves. Firms are often at the front line of consumer interaction, operational risk, and technological innovation. This places a responsibility on them to adopt forward-looking practices that go beyond minimum compliance, in order to foster trust and long-term market stability. Industry players that embed robust governance, transparency, and security standards will be better positioned to withstand regulatory scrutiny, attract institutional adoption, and safeguard consumers.

[180] IOSCO, 2025

9.3.1 Strengthening Industry Practices for Trust and Resilience

The digital asset industry must also take responsibility for mitigating risks and building trust in the ecosystem. Key recommendations for industry participants are:

- **Adopt a proactive compliance culture:** Industry players should not wait for regulations to hit before acting; instead, they ought to **embed compliance and risk management** into their business models from the start. This means implementing robust KYC/AML procedures, even in jurisdictions where they're not yet mandated, and continuously monitoring and reporting transactions for suspicious activity. Practical steps could include hiring experienced compliance officers, integrating blockchain forensics, deploying transaction-monitoring tools powered by AI, and scheduling regular independent audits. Firms that take compliance seriously will be better positioned as trusted partners for regulators and customers. Embracing a culture of compliance and transparency will not only pre-empt a heavy-handed regulation but also attract users and institutional investors who seek safe platforms.

- **Engage constructively with regulators and standard-setters**: Companies in the digital assets space should actively participate in the regulatory dialogue. Rather than viewing regulators as adversaries, industry should treat them as stakeholders in creating sustainable markets. This can involve providing feedback during public consultations (e.g. on proposed laws), joining industry associations that liaise with governments, and even helping with education by sharing expertise on the technology. Beyond consultations, firms could also contribute technical input to rulemaking (e.g. defining DeFi liquidity pool disclosures), co-develop testing frameworks in regulatory sandboxes, and share anonymised and aggregated data on fraud typologies to improve early warning systems. By **participating in regulatory discussions**, businesses can help shape pragmatic rules and stay ahead of compliance obligations. Successful examples include crypto firms contributing to the development of standards (like the messaging formats for the Travel Rule) and collaborating in sandbox programs. Open communication can also mean alerting authorities to emerging issues. For example, if an exchange detects a new type of fraud or cyber threat, promptly sharing this with regulators can help issue sector-wide alerts, strengthening protections for the entire market and supporting responsible participants.

- **Ensure financial and operational transparency:** Industry players could voluntarily uphold high standards of transparency to build confidence. For stablecoin issuers, this means, publishing monthly disclosure of reserve breakdowns and real-time dashboards showing collateral backing. For exchanges, this could include disclosing how they handle custody (e.g. proof-of-reserves with accompanying proof-of-liabilities) and being upfront about listing criteria for tokens. DeFi protocols can open-source their code and security audits to allow public scrutiny. When problems do occur, being honest and prompt in communication with users and regulators is critical.

- **Implement strong security measures and best practices:** Given the prevalence of hacks, thefts, and technical failures in crypto, industry players must make security a non-negotiable priority. This includes cybersecurity and platform integrity. Concrete measures include setting hot wallet exposure caps, mandating multi-signature custody, requiring penetration testing at least quarterly, and publishing incident reports within fixed disclosure timelines (e.g. T+72 hours). Firms should stay updated on evolving threats and regularly upgrade their defences, for example, by engaging external security auditors and participating in threat information sharing groups. It may be advantageous to offer bug bounties to encourage ethical disclosure of vulnerabilities before criminals exploit them. Additionally, companies should have clear incident response plans to minimise damage if a breach occurs. By demonstrating a track record of security consciousness, industry players not only protect their users but also strengthen their case that crypto markets can be as safe as traditional financial markets. Regulators will be less inclined to restrict an industry that proves it can self-police effectively on security matters.

- **Champion consumer protection and education:** Industry participants interact with millions of retail users, so they are on the front lines of consumer protection. Businesses should take it upon themselves to **educate users** about risks. This may include providing clear warnings about volatility, reminding users never to share private keys, and explaining that crypto transactions are largely irreversible. Platforms can build in safeguards like default limit orders to prevent huge losses from fat-finger errors, cooling-off periods for first-time investors, or standardised risk labels on various products. When offering new services (like margin trading or yield products), firms should ensure these are suitable for the target clientele and avoid aggressive promotion to populations who may not understand the downsides.

Platforms could also publish “consumer dashboards” to track incidents such as loss of funds or fraud complaints. Self-regulatory initiatives can make a big difference. Industry associations could take the lead in setting voluntary “safe product” certifications, modelled on existing best practices in payments and securities markets.

- **Embrace interoperability and collaboration:** Industry players should collaborate to solve common challenges rather than operate in silos. For example, they can work together on interoperability standards so that different systems can communicate (benefiting consumers with smoother experiences and reducing systemic risk of fragmentation). Collaboration can also extend to compliance solutions, shared KYC utilities, or blockchain analytics services, which can raise the bar across the board. By joining forces on certain non-competitive fronts (like security, compliance, and infrastructure), companies can achieve economies of scale in meeting regulatory expectations. Importantly, such collaboration can involve traditional financial institutions as well.

- **Innovate responsibly and focus on long-term value:** Finally, industry players should remember that the goal is not short-term hype but long-term sustainable innovation in financial services. Responsible innovation means stress-testing new products for risks, rolling them out gradually, and having contingency plans if things go wrong. For example, a DeFi protocol launching a novel algorithmic stablecoin should incorporate circuit-breakers or pauses if the peg starts to wobble, rather than pursuing growth at all costs (the Terra collapse learnings). Companies should also avoid offering products that are clearly beyond the understanding of their average user or that encourage reckless speculation (unless they build appropriate safeguards). By focusing on delivering real value, such as financial inclusion, faster and cheaper payments, or new investment opportunities, the industry can build a positive narrative. Each firm should consider its broader impact on market stability and societal goals; for example, large exchanges could implement internal risk limits to avoid liquidations cascading market wide.

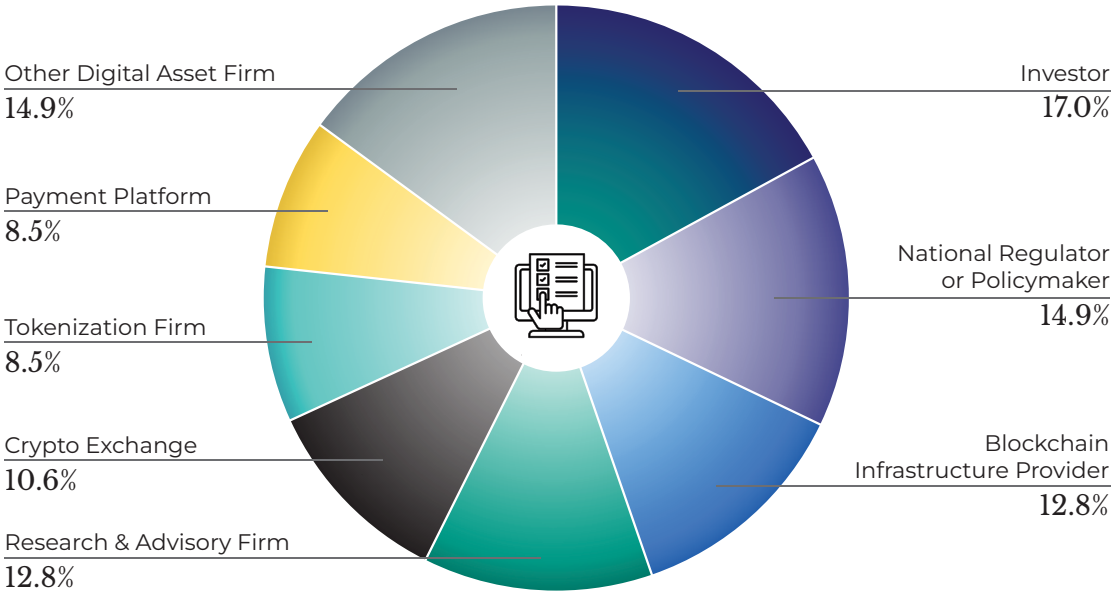
Appendix

1. Profile of GFTN Survey Participants:

Overview of survey respondent demographics by organisation type and geographic region; N=48

Survey Respondents by Organisation Type

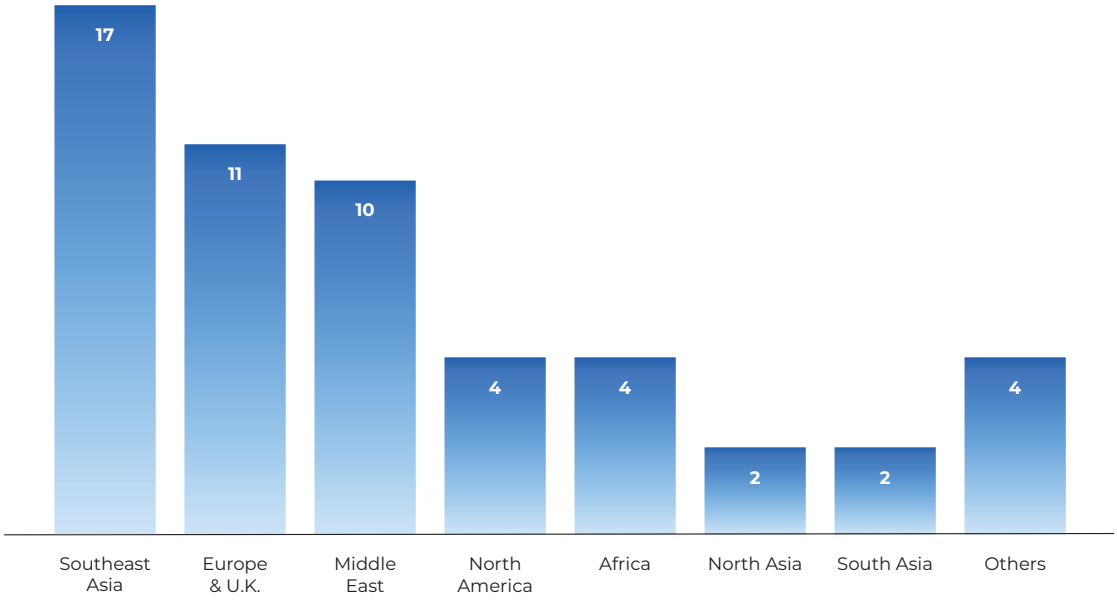
1.1 Please select the type of organisation you represent. (Single choice)



Breakdown of respondents across various segments of the digital asset industry.
N=48; Respondents include various industry participants and regulators.

Survey Respondents by Geographic Region

1.2 What region is your organisation's primary jurisdiction? (Multiple choice)



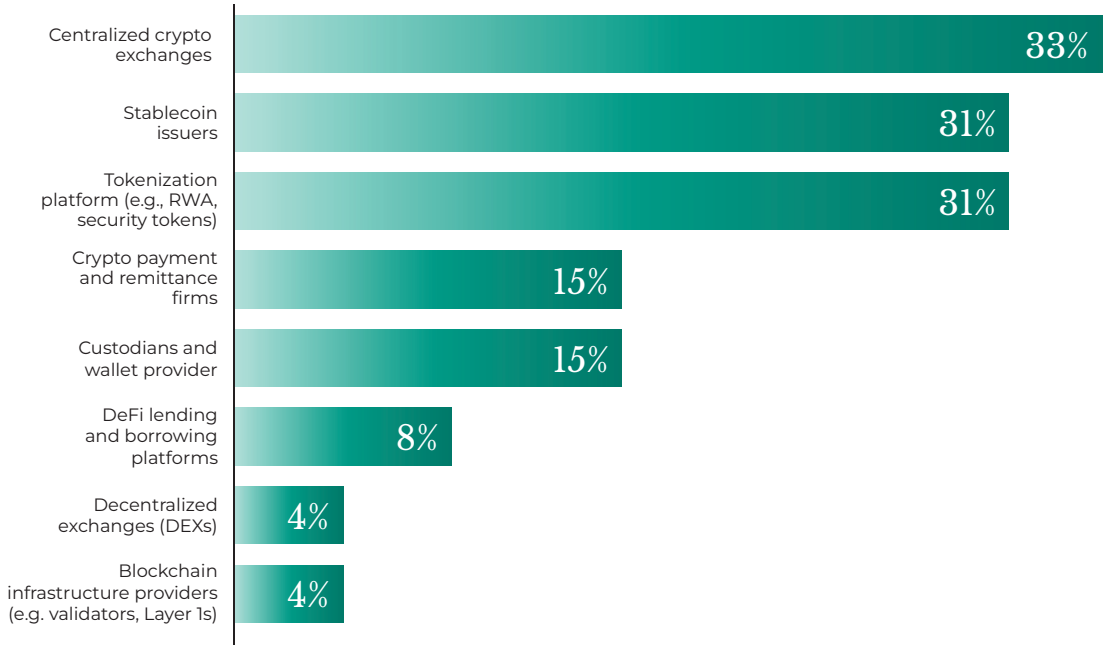
Geographic distribution of respondents, N=48; Respondents include various industry participants and regulators.

2. Regulatory Priorities

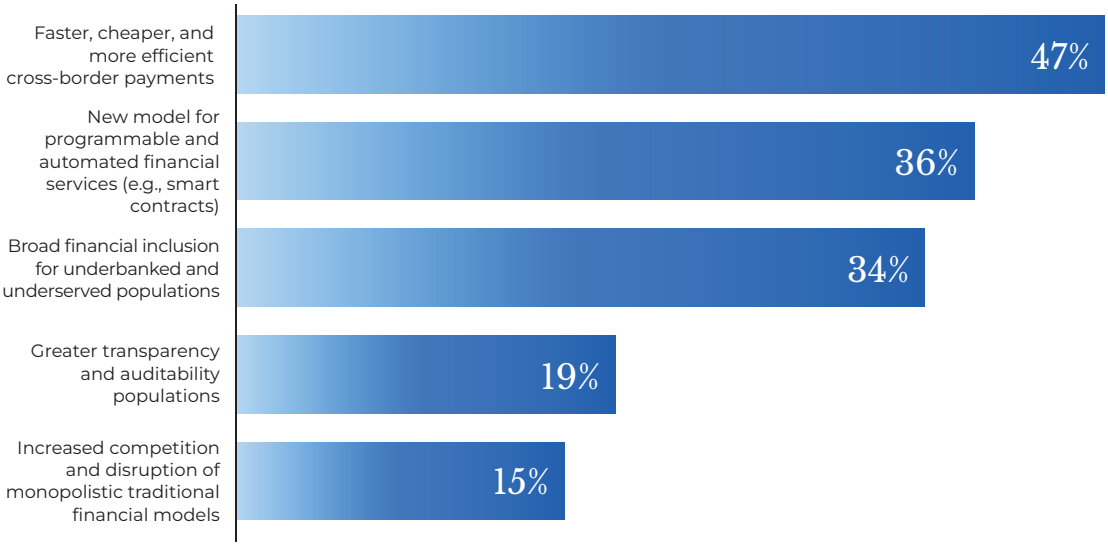
Insights based on responses from various industry participants and regulators; N=48

Regulatory Priorities: Key Digital Asset Segments and Perceived Benefits

2.1 Which digital asset business models require the most regulatory attention in your jurisdiction? (Multiple choice)



2.2 What primary benefit(s) do you believe digital assets bring to the financial system? (Multiple choice)



N=48; Respondents include various industry participants and regulators.

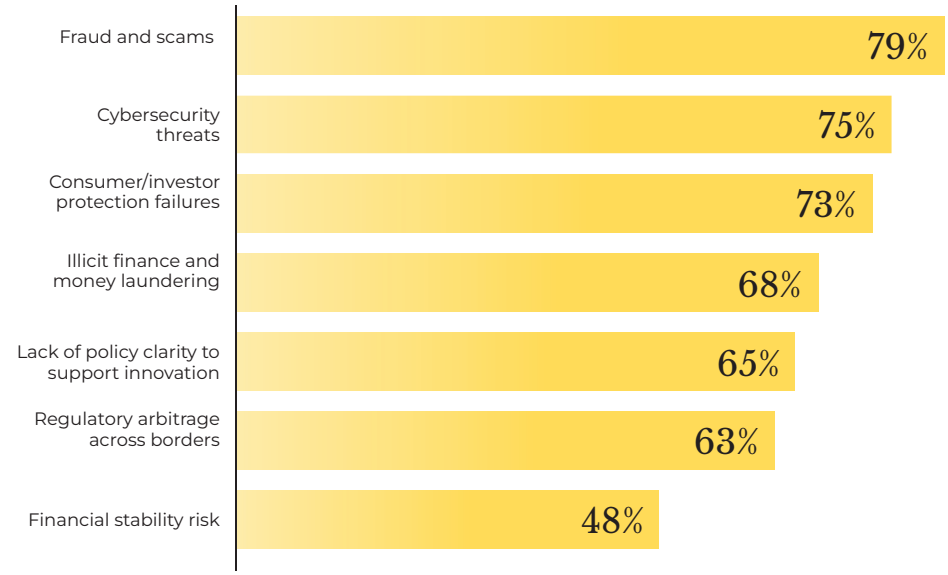
Regulatory Priorities: Perceived Importance of Digital Asset Regulation

2.3 How important do you think regulation of digital assets is for the following areas?

N=48; Respondents include various industry participants and regulators. Importance rated as 4 or 5 on a scale of 1-5.

Regulatory Priorities: Critical Risk Areas in the Digital Asset Ecosystem

2.4 What is the biggest risk associated with digital assets today?

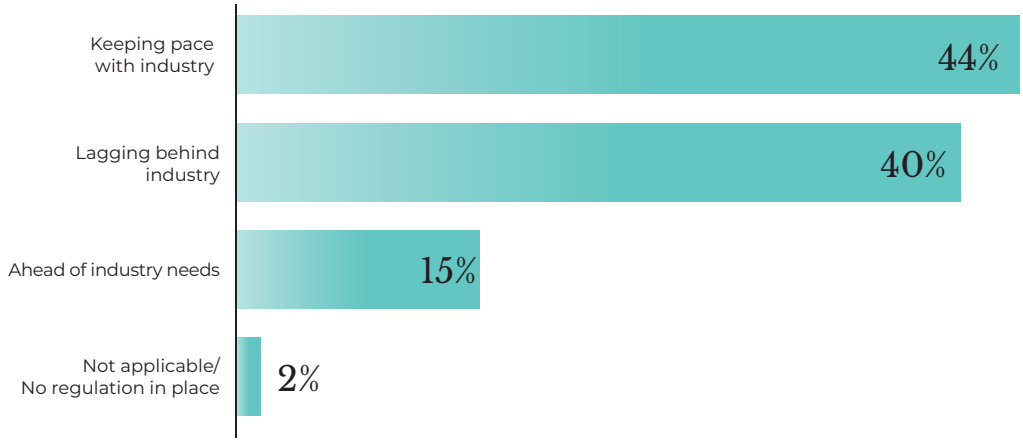


N=48; Respondents include various industry participants and regulators. Critical rated as 4 or 5 on a scale of 1-5.

Regulatory Priorities: Regulatory Clarity and Pace of Regulatory

2.5 How would you rate the current clarity of digital asset regulation in your primary jurisdiction? (Single choice)

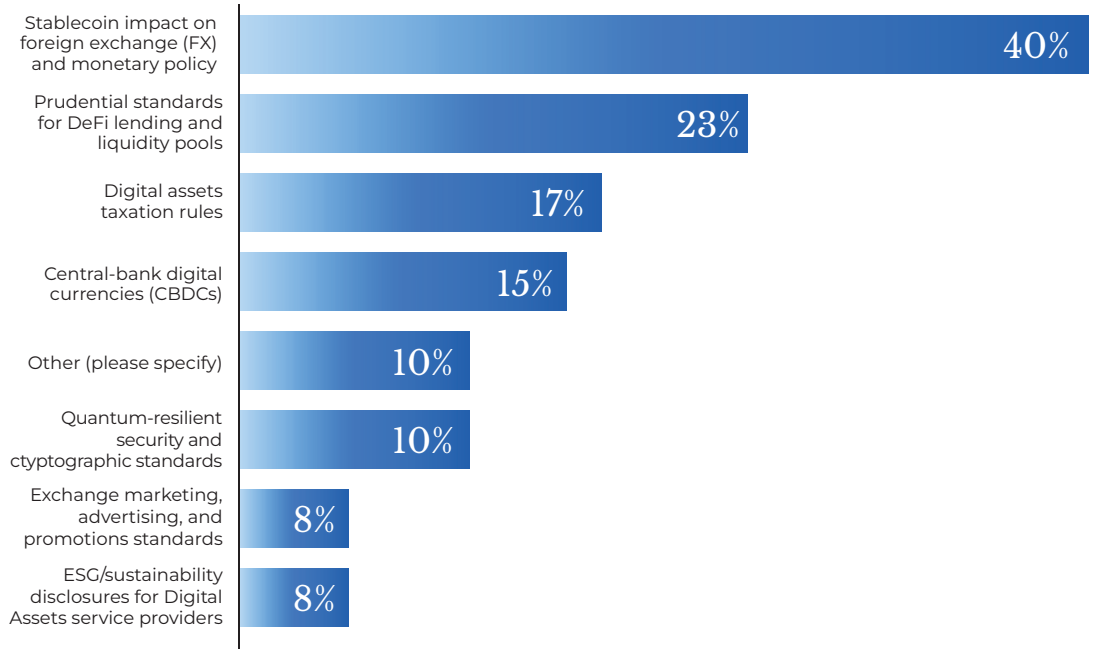
2.6 How do you perceive the pace of regulatory developments in your jurisdiction regarding digital assets? (Single choice)



N=48; Respondents include various industry participants and regulators.

Regulatory Priorities: Emerging Business Models Demanding Immediate Regulatory Focus

2.7 Which new policy frontier requires the most urgent regulatory guidance? (Multiple choice)



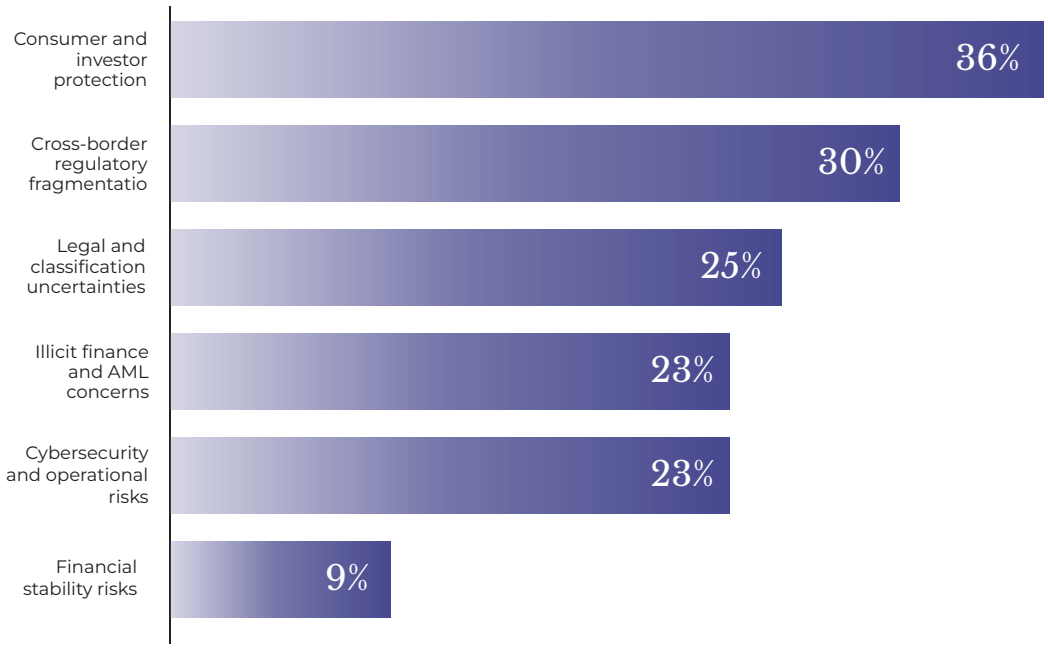
N=48; Respondents include various industry participants and regulators.

3. Industry Outlook

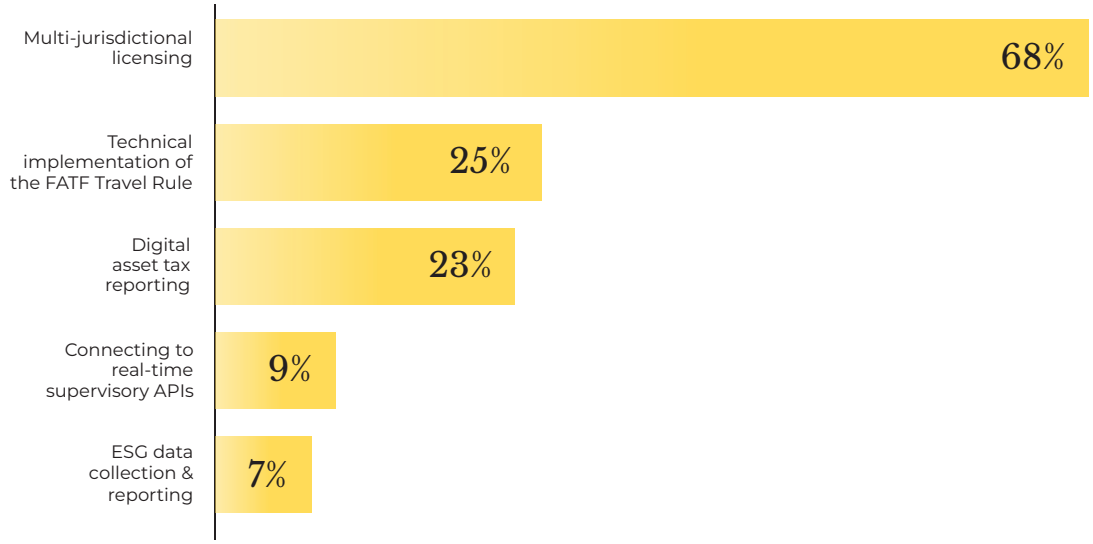
Insights based on feedback from industry stakeholders (excluding regulators); N=44

Industry Outlook: Key Risk Areas and Operational Challenges in the Digital Asset Ecosystem

3.1 What are your organisation's main priorities or concerns regarding digital asset risks? (Multiple choice)



3.2 Which operational burden is currently the most significant? (Multiple choice)

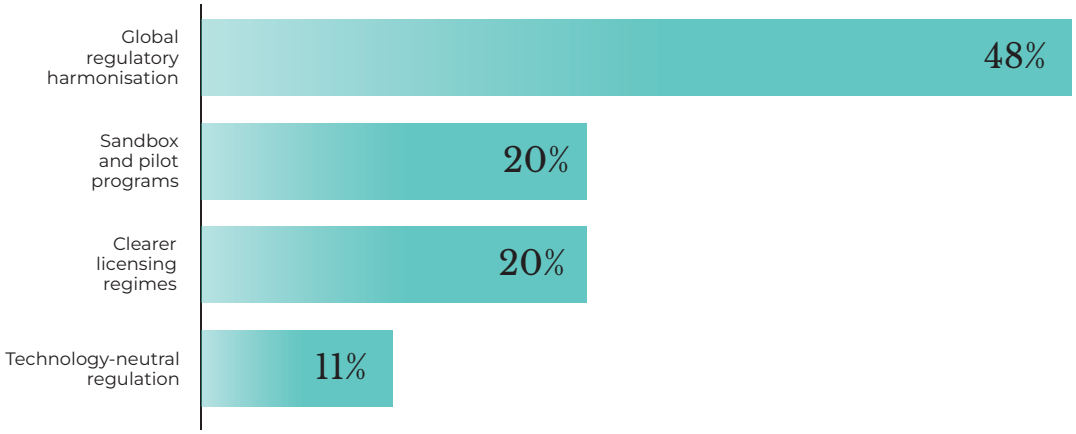


N=44; Respondents include various industry participants.

Industry Outlook: Policy Approaches and Regulatory Measures to Drive Innovation in the Digital Asset Ecosystem

3.3 What policy stance do you think regulators should adopt for digital assets? (Multiple choice)

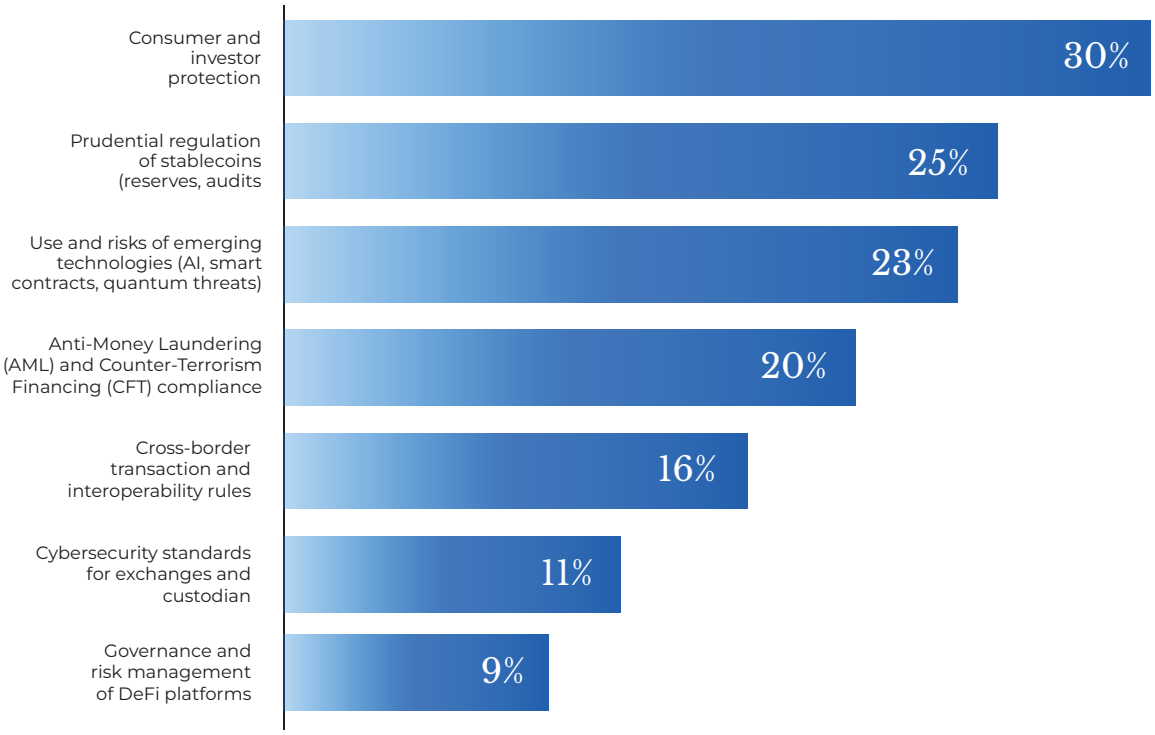
3.4 Which regulatory action would most support your innovation and growth in digital assets? (Multiple choice)



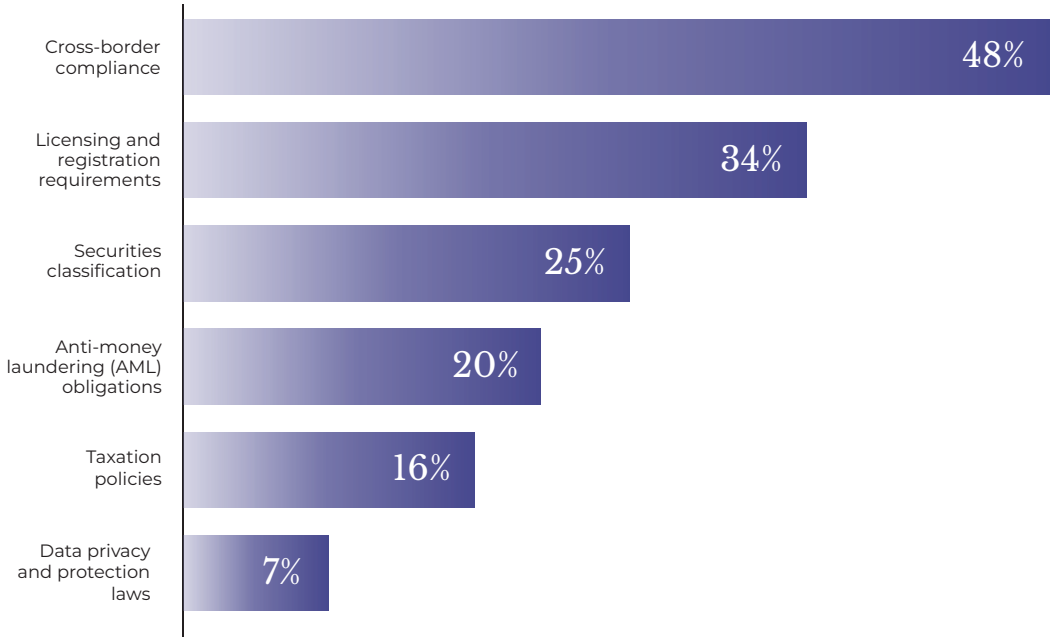
N=44; Respondents include various industry participants.

Industry Outlook: Regulatory Priorities and Compliance Challenges in the Digital Asset Ecosystem

3.5 Which specific areas of digital assets do you think require the most regulatory attention? (Multiple choice)



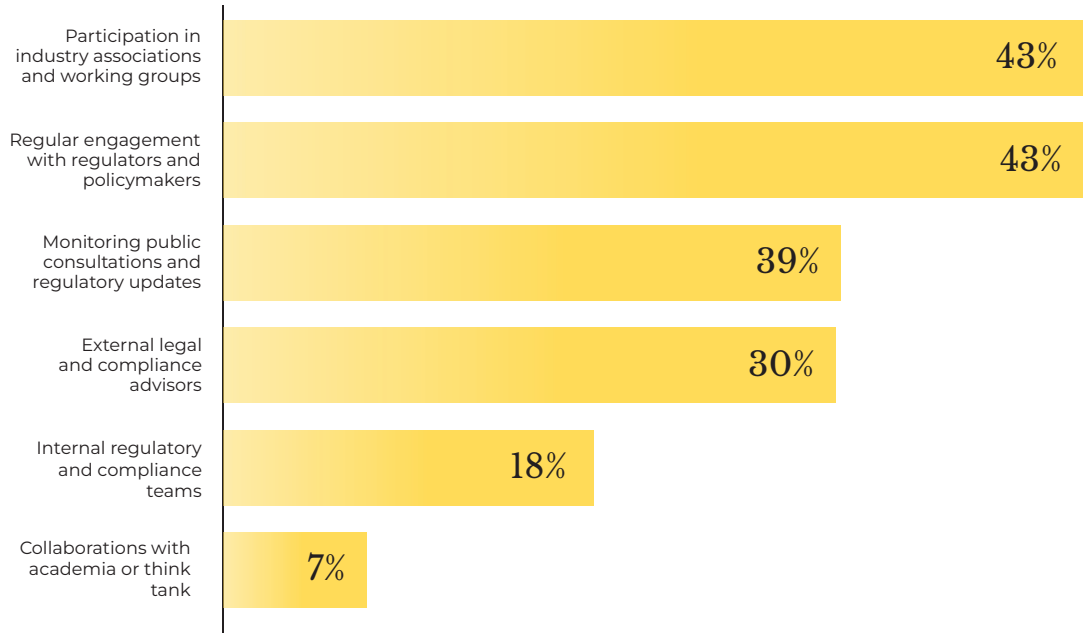
3.6 Which areas of digital asset regulation do you find most challenging to navigate: (Multiple choice)



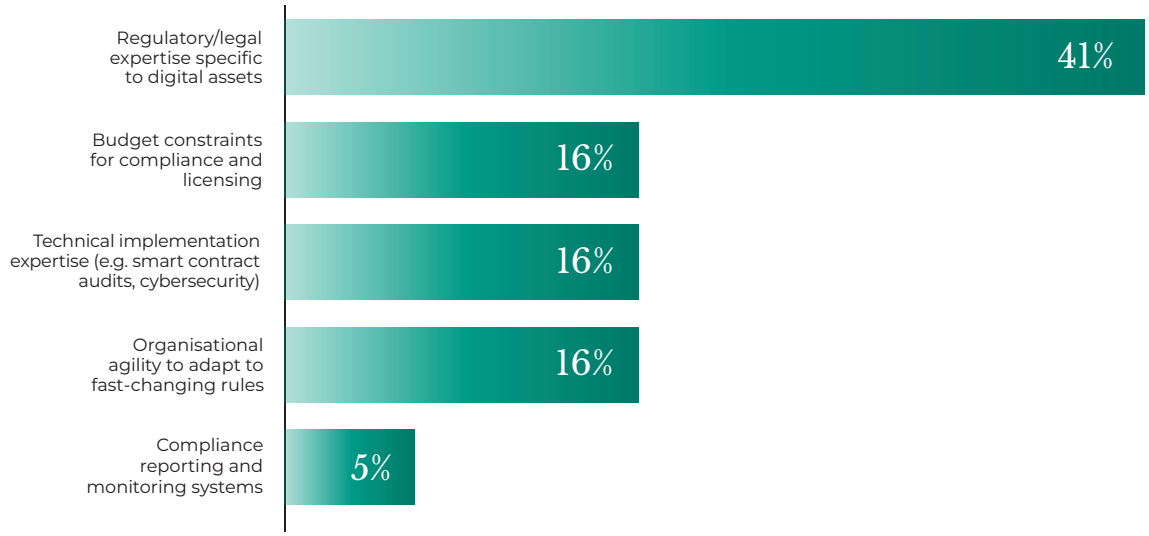
N=44; Respondents include various industry participants.

Industry Outlook: Information Channels and Internal Capability Gaps in the Digital Asset Ecosystem

3.7 How does your organisation stay informed about regulatory developments in digital assets? (Multiple choice)



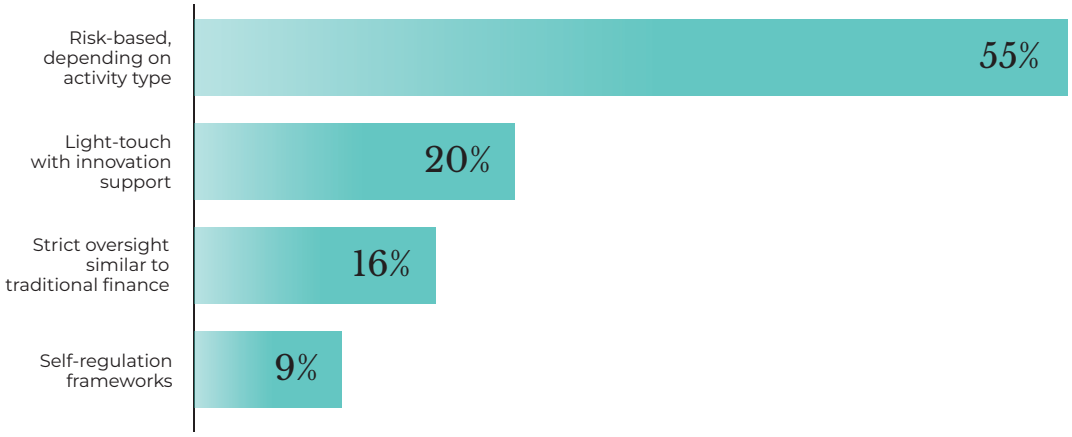
3.8 Which areas of digital asset regulation do you find most challenging to navigate: (Multiple choice)



N=44; Respondents include various industry participants.

Industry outiook: Preferred Supervision Models to Balance Risk Management and Innovation in the Digital Asset Ecosystem

3.9 What kind of supervision model would you prefer for your segment? (Single choice)



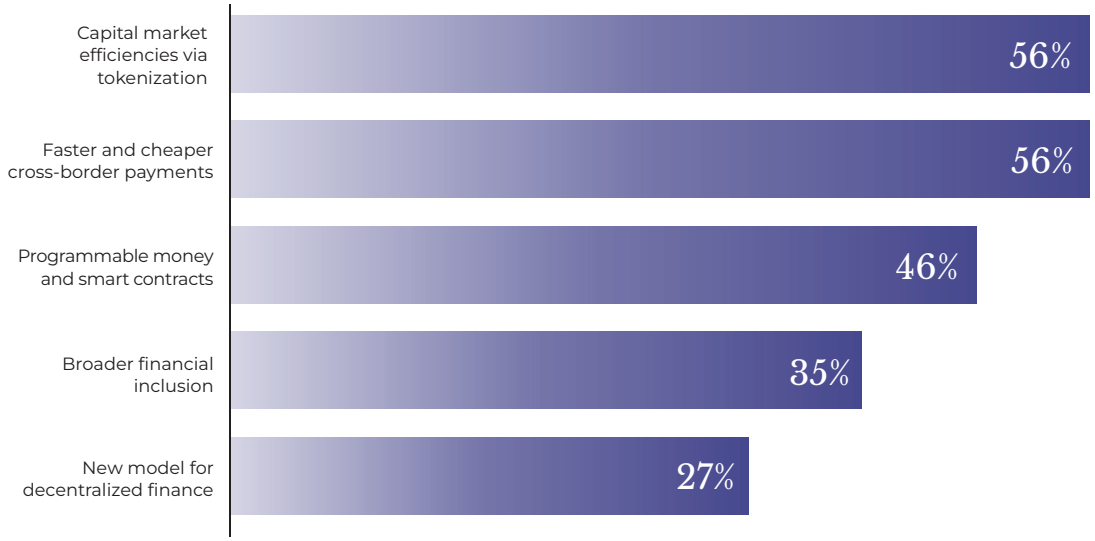
N=44; Respondents include various industry participants.

4. Future Outlook

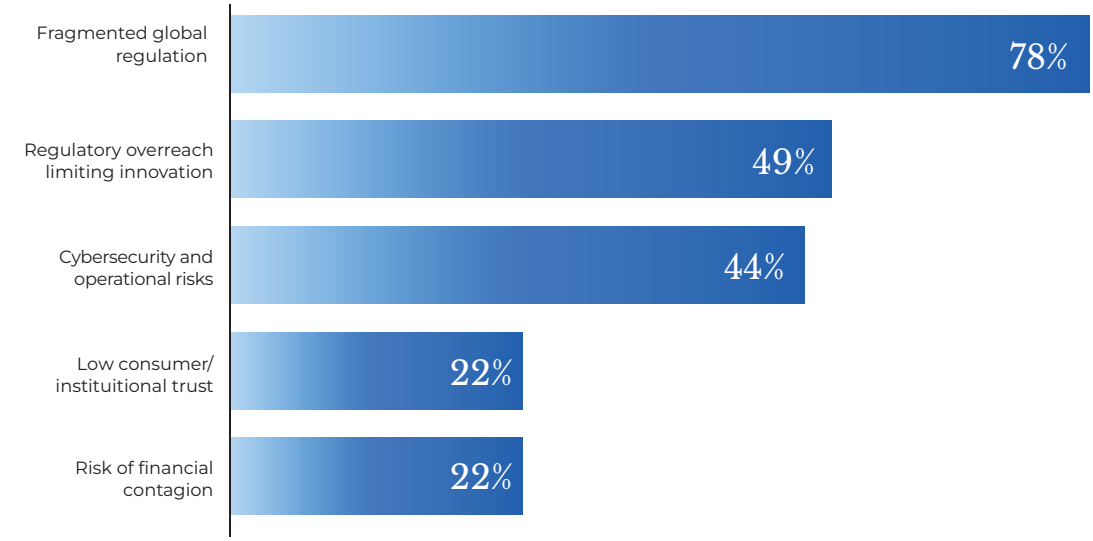
Based on responses from various industry participants and regulators; N=48

Future Outlook: Key Opportunities and Challenges for Digital Assets in the Next Three Years

4.1 What is the biggest opportunity digital assets present over the next 3 years? (Multiple choice)



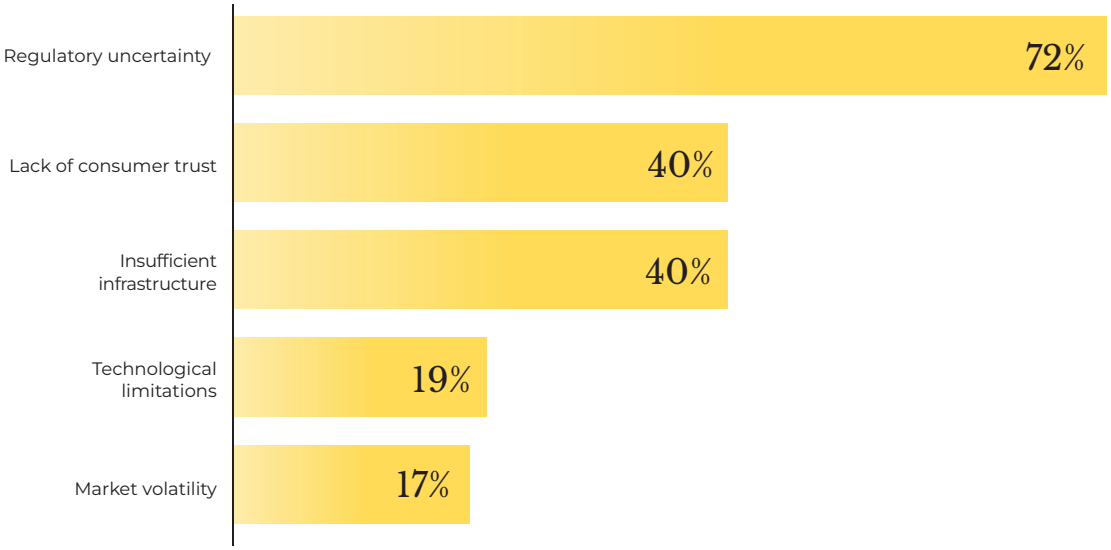
4.2 What is the biggest challenge digital assets will face over the next 3 years? (Multiple choice)



N=48; Respondents include various industry participants and regulators.

Future Outlook: Key Barriers to Mainstream Adoption of Digital Assets

4.3 In your opinion, what is the most significant barrier to the mainstream adoption of digital assets? (Multiple choice)



N=48; Respondents include various industry participants and regulators.

Glossary

Terms	Definition
1. **Capped slippage**	A limit placed on the difference between the expected price of a trade and the price actually executed, to prevent attackers from draining liquidity with manipulated trades. **Example:** A decentralized exchange sets a maximum of 1% slippage on swaps, so even if an attacker tries to push a large trade through, it cannot distort prices beyond this threshold.
2. **Central Bank Digital Currency**	A digital version of national currency issued directly by a central bank. Offers sovereign backing and legal tender status. **Example:** China's e-CNY and the Bahamas' Sand Dollar.
3. **Chain-Hopping**	Moving assets rapidly across multiple blockchains to disrupt traceability. **Example**: North Korea's Lazarus Group uses chain-hopping to launder stolen crypto.
4. **Circuit Breaker** (On-Chain)	A smart contract safety mechanism that can freeze funds or pause withdrawals when anomalies are detected. **Example:** Some DeFi lending protocols embed circuit breakers to prevent mass liquidations.
5. **Decentralized Autonomous Organisation**	A governance structure where rules and decisions are encoded in smart contracts and executed by token holders rather than a central company. **Example:** MakerDAO is governed by holders of its MKR governance token.
6. **Fractional Ownership**	Allows investors to own part of a high-value asset through tokens. Makes traditionally expensive assets accessible to more investors. **Example**: MUFG tokenized an Osaka skyscraper, enabling fractional investment.
7. **Hardware Security Module**	A dedicated physical device designed to securely generate, store, and manage cryptographic keys. HSMs are tamper-resistant and widely used in banking and enterprise environments for high-security operations. **Example**: A crypto exchange stores private keys in HSMs to ensure that sensitive signing operations cannot be extracted or altered, even if its software systems are compromised.
8. **Hot Wallet**	A digital asset wallet that is connected to the internet, allowing fast transactions but exposing the keys to higher hacking risk. **Example:** An exchange's customer-facing wallet that allows instant withdrawals is a hot wallet, often targeted in cyberattacks.
9. **Interoperability**	The ability for digital tokens to be transferred and used across different blockchains or between traditional and digital systems. **Example:** Singapore's Project Guardian tests cross-border settlement of tokenized bonds.
10. **Jurisdictional Arbitrage**	When crypto firms relocate operations to jurisdictions with weaker AML/KYC rules. **Example:** Some exchanges moved operations offshore to avoid strict U.S. oversight.
11. **Legal Finality in Tokenization**	When a token is legally recognised as proof of ownership, ensuring enforceability in courts. **Example:** Switzerland's DLT Act grants legal standing to blockchain-based asset tokens.
12. **Mixer / Tumbler**	A service that obfuscates transaction trails by pooling and redistributing crypto, making tracing difficult. **Example:** Mixers such as Tornado Cash or Blender allow users to pool and redistribute crypto to increase transaction privacy. These services have been used both by legitimate users seeking anonymity and by illicit actors, leading to regulatory scrutiny in several jurisdictions.

Terms	Definition
13. Multi-Party Computation	A cryptographic technique that splits a private key into multiple parts, which are distributed across different servers or devices. No single party ever holds the full key, and transactions are only signed when the key fragments interact securely. **Example:** A digital asset custodian uses MPC so that even if one server is hacked, the attacker cannot access the full private key.
14. Multi-Signature Wallet	A wallet requiring multiple private keys to authorise a transaction, reducing single-point failure risk. **Example:** Exchanges use multi-sig for cold storage of reserves.
15. On-Ramps / Off-Ramps	Services that let users move between fiat money and crypto. On-ramps convert cash/bank deposits into crypto; off-ramps convert crypto back into fiat. **Example:** MoonPay and Coinbase provide fiat–crypto on/off-ramp services.
16. One-block reentrancy guards (for composable calls)	A smart contract security measure that prevents multiple actions (such as borrow, swap, and repay) from being executed within the same block to exploit temporary conditions. **Example:** A DeFi lending protocol installs a guard that stops users from borrowing against collateral and immediately withdrawing it in the same block — a common tactic in flash loan exploits.
17. Oracle Manipulation	Exploiting weaknesses in price feeds to trigger incorrect liquidations or arbitrage. **Example:** Mango Markets lost US$114M from oracle price manipulation..
18. Over-Collateralization	A risk control where borrowers must pledge assets worth more than the loan, to cover volatility. **Example:** To borrow US$100 in DAI on MakerDAO, a user might need to lock US$150 in ETH.
19. Price-guarded oracles	Oracles that include built-in safeguards to prevent extreme price swings from being exploited in a single block or transaction. **Example:** A DeFi lending protocol using Chainlink oracles may reject sudden 50% price changes within one block, preventing attackers from manipulating token prices to borrow more than they should.
20. Programmable Money / Assets	Tokens with built-in logic for automatic actions, such as conditional payments or real-time coupon distribution. **Example:** Tokenized green bonds in Hong Kong with automated interest payments.
21. Proof of Reserves	An audit practice where exchanges demonstrate on-chain that they hold sufficient assets to cover customer balances. Builds trust and regulatory confidence after exchange failures. **Example:** OKX publishes regular PoR audits for user funds.
22. Proof of Stake	A consensus mechanism where participants "stake" their tokens to validate transactions and secure the network. Replaces energy-intensive mining with economic incentives. **Example:** Ethereum shifted to PoS in 2022, reducing energy use by 99%.
23. Rug Pull	A fraudulent scheme where token developers withdraw all liquidity, leaving investors with worthless assets. **Example:** Over US$150M lost in rug pulls in 2024.
24. Sanctions Screening	The process of checking wallets or transactions against international sanction lists (e.g. OFAC). **Example:** Blacklisting North Korean-linked wallets involved in hacks.

Terms	Definition
25. Single-Signature Wallet	A type of wallet that requires only one private key to authorise transactions. While simple, it creates a single point of failure if the key is compromised. **Example:** A user storing their Bitcoin in a single-signature wallet risks losing all funds if their private key is stolen through malware.
26. Slashing	A penalty applied to validators who act dishonestly or fail to perform their duties in PoS networks. A portion of their staked tokens is confiscated to maintain network integrity. **Example:** Ethereum slashes validators if they try to approve fraudulent blocks.
27. Social Engineering (Crypto Context)	Techniques like phishing, fake job offers, or deepfakes used to trick insiders into giving access. **Example:** North Korean hackers infiltrated firms via fake LinkedIn job postings.
28. Stablecoin	A digital token pegged to a stable asset such as the U.S. dollar or euro. Designed to reduce volatility and enable fast payments. **Example:** USDC by Circle, widely used in cross-border payments.
29. STR / SAR (Suspicious Transaction/Activity Report)	A global requirement (from FATF) that forces digital asset transactions above a threshold to include information on sender and recipient, to prevent money laundering. **Example:** Implemented in the E.U., the U.K., and Hong Kong stablecoin frameworks.
30. Tokenized Deposit	Mandatory reports submitted to regulators when unusual or potentially illicit activity is detected. **Example:** U.S. FinCEN requires SAR filings for suspicious wallet activity.
31. Travel Rule (for Digital Assets)	A global requirement (from FATF) that forces digital asset transactions above a threshold to include information on sender and recipient, to prevent money laundering. **Example:** Implemented in the E.U., the U.K., and Hong Kong stablecoin frameworks.
32. Wallet Allowlisting	A security measure that restricts withdrawals or transfers from a user's account to a pre-approved list of wallet addresses. By only permitting transactions to designated addresses, allowlisting reduces the risk of theft from hacks, phishing attacks, or unauthorised access. **Example:** An exchange may require customers to register external wallets in advance, and transfers are permitted only to those approved addresses.

**Global Finance &
Technology Network (GFTN)**

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com