CERTIK
SKYNET

Skynet Intelligence Report

State of Digital Asset Regulations

Several key developments define the current regulatory environment for digital assets. Regulatory frameworks on digital assets are now enforceable in the US, the EU, Hong Kong, Singapore, the UAE, Japan, Turkey, Brazil, and more.

Executive Summary

Several key developments define the current regulatory environment for digital assets. Regulatory frameworks on digital assets are now enforceable in the US, EU, Hong Kong, Singapore, the UAE, Japan, Turkey, Brazil and more. AML enforcement has overtaken securities classification as the primary regulatory risk, with AML-related financial penalties against crypto and related financial institutions exceeding $900 million in H1 2025. Smart contract security audits have become statutory or quasi-statutory requirements globally.

The Basel Committee's cryptoasset prudential standard carries a January 1, 2026 implementation date at the BCBS level, with jurisdictions transposing it into local law on varying timelines. Prudential standards for exchanges, custodians, and issuers now match those applied to traditional financial market infrastructure. Tokenized assets scale under existing securities law rather than bespoke regimes.

For companies evaluating market entry or expansion, multi-jurisdictional licensing is the cost of operating at scale. AML compliance budgets must match the penalties now being imposed. Security audit costs are recurring and jurisdiction-specific. Capital planning must reflect the Basel framework's differentiated treatment of asset classes, as codified by the applicable local regulatory regime.

Global Regulatory Trends for 2026

Stablecoin Regimes Move from Design to Implementation

Binding requirements including those on reserves, redemption rights, governance, and disclosure are now enforceable in the United States (GENIUS Act), the EU (MiCA), Hong Kong (Stablecoins Ordinance), Singapore (MAS under its licensing framework for Payment Service Providers), the UAE (VARA and ADGM frameworks), and Brazil (BCB Resolutions 520/521, classifying stablecoins as FX transactions). Central banks are testing interoperability between systemic stablecoins and domestic payment systems. In 2026, the primary hurdle for issuers has shifted from achieving legal status to managing regulatory friction, as conflicting requirements on local reserves and more, no license passporting, and costs to comply globally are becoming significant pain points.

AML Enforcement Replaces Securities Classification as Primary Concern

SEC crypto-specific enforcement fell 60% in volume and 97% in penalty value year over year between 2024 and 2025. DOJ and FinCEN filled the gap, imposing over $900 million in AML-related fines and settlements in H1 2025. The OKX settlement ($504 million) and KuCoin settlement ($297.4 million) established the scale of penalties exchanges face for transaction monitoring failures. European AML fines rose 147% in H1 2025. Asia-Pacific regulators favored license revocation and business improvement orders over monetary penalties. Across every major jurisdiction, the enforcement question for digital asset businesses is now more about transaction monitoring and sanctions compliance, not token classification.

Security Assessments Become Licensing and Compliance Requirements

Almost all global jurisdictions now require some form of independent smart contract assessment as a precondition for licensing or token admission. This is either required by explicit mandates over smart contract auditing, or indirectly by requiring “source code reviews” or general security testing over critical assets identified as part of ICT risk management procedures (which should include smart contracts supporting business processes).

Hong Kong's HKMA Stablecoins Ordinance requires an independent smart contract security audit as a precondition for stablecoin issuer licensing, with the SFC's VATP Guidelines imposing parallel independent assessor requirements for token admission by virtual asset trading platforms. VARA's Technology and Information Rulebook requires annual smart contract audits and retains authority to require Threat-Led Penetration Testing. ADGM's FSRA requires DLT stress testing and code validation. The EU's DORA imposes operational resilience obligations

that effectively compel code review. NYDFS imposes the most developed state-level requirements, and Wyoming's Special Purpose Depository Institution framework and Stable Token Act establish cybersecurity and reserve attestation obligations for state-chartered digital asset entities. Japan and South Korea achieve similar outcomes through self-regulatory bodies. Brazil's IN 701 (effective February 2026) requires independent technical certification covering cybersecurity, asset segregation, and key management as a precondition for SPSAV authorization. Turkey's CMB requires TÜBİTAK technical infrastructure audits before licensing. Two years ago, none of these mandates existed in their current form.

Prudential and Custody Standards Tighten

Crypto exchanges, custodians, and stablecoin issuers now operate under prudential and operational resilience regimes comparable to those applied to traditional financial market infrastructure. Requirements cover capital adequacy, asset segregation, liquidity management, and recovery planning. Supervisors are imposing these standards directly rather than waiting for voluntary adoption.

Basel Capital Treatment Creates a Structural Divide

The Basel Committee's finalised cryptoasset prudential standard carries an implementation date of January 2026 for BCBS member jurisdictions. Transposition into binding local law (e.g., EU CRR3, US federal banking rules) is occurring on differing timelines. Group 1 assets (tokenized traditional instruments and qualifying stablecoins) receive standard risk weighting. Group 2 assets (BTC, ETH, and other unbacked tokens) face significantly higher risk weightings, often requiring near-100% capital charges. This distinction will determine which digital assets are economically viable for bank balance sheets and which remain structurally constrained for institutional adoption.

Tokenized Assets Scale Under Existing Securities Law

While specific hubs like Dubai, Luxembourg and Hong Kong have developed specific guidelines or frameworks for RWA, global harmonization is still lacking and most legislations continue to apply “modified traditional securities laws”. The current approach is consistent globally: apply existing investor protection rules to a new settlement layer. Franklin Templeton's FOBXX operates as a registered fund with on-chain settlement. Singapore's Project Guardian is a collaboration between MAS and global banks on tokenization of fixed income, FX, and asset management products. ADGM's FSRA Guidance on the Regulation of Digital Securities Activity sets out how existing securities laws apply to tokenized private credit, REITs, and other digital securities. Brazil's Piloto Drex provides the most advanced sovereign CBDC infrastructure for institutional tokenization in Latin America, with BCB-supervised DLT rails supporting fixed income, trade finance, and real estate settlement.

The State of Global Stablecoin Regulation

Stablecoin regulation has converged with unusual speed. Across every major jurisdiction, regulators have arrived at a structurally similar framework: full fiat reserve backing, prohibition of algorithmic stabilization mechanisms, independent attestation of reserves, and licensing of issuers. The variation is in the details of implementation, not in the underlying architecture.

Jurisdiction	Reserve Composition	Reserves & Technical Assessment	Issuer Licensing	Important Notes	Status
United States	100% liquid assets (Treasuries, cash). Segregated.	Monthly. Public accounting firm.	OCC charter or state equivalent.	GENIUS Act signed July 2025. Rulemaking expected through 2026.	Signed; rulemaking ongoing
European Union	HQLA. 30% held in credit institutions.	Regular independent audits.	Only (authorized) credit institutions or EMI can issue EMT.	ARTs subject to daily transaction volume limits.	MiCA operational
Hong Kong	100% liquid fiat or equivalents.	Monthly public disclosure.	HKMA licensing. Non-mandatory sandbox (pre-Ordinance HKMA program; not a licensing precondition).	Cap. 656 effective 2025.	Enacted
Singapore	100% liquid fiat or equivalents.	Monthly checks.	MAS MPI/SPI licence. S$250,000 minimum base capital (MPI).	Single-currency peg only under the proposed MAS-regulated SCS label; non-SCS issuance remains subject to the existing DPT regulatory regime.	SCS framework finalized 2023; full legislative effect expected 2026
UAE	Under CBUAE: Full fiat backing. AED for domestic stablecoins. Segregated.	Third-party Proof of Reserves.	Central Bank of the UAE (CBUAE),VARA, ADGM.	Under CBUAE foreign currency stablecoins prohibited for merchant payments.	Enacted
Japan	100% fiat held in Japanese trust accounts.	Annual statutory audits.	FSA. Restricted to banks, trust companies, and FTOs.	Governed by the Payment Services Act	Enacted
Brazil	BCB Res. 520/521. Stablecoins treated as FX. Segregated.	IN 701: independent technical certification.	BCB SPSAV authorization. R$10.8M-R$37.2M capital.	Stablecoin flows classified as FX transactions.	Enacted (Feb 2026)

Figure 1: Comparison of Global Stablecoin Regimes Table

The GENIUS Act established the first federal stablecoin framework in the United States, placing the OCC in a supervisory role over stablecoin issuers. Implementation rulemaking by the federal banking agencies is expected throughout 2026, with an effective date no later than January 2027. New York's Department of Financial Services operates the most developed state-level regime, with requirements for 1:1 reserves, daily redemption, and monthly attestations. Wyoming has been the leading US state on digital asset legislation, having authorized Special Purpose Depository Institutions and launched its own state-issued stable token.

Hong Kong's Stablecoins Ordinance (Cap. 656) requires a HKMA licensing regime. MiCA classifies stablecoins into Asset-Referenced Tokens and E-Money Tokens, each with separate reserve requirements and authorization tracks. The CBUAE requires AED-denominated backing for domestic payment stablecoins, prohibiting foreign currency and algorithmic stablecoins for merchant transactions. Japan restricts issuance to licensed banks, trust companies, and fund transfer operators, with reserves held exclusively in Japanese trust accounts. Brazil's BCB treats stablecoin flows as foreign exchange transactions under Resolutions 520 and 521, requiring independent technical certification under IN 701 and imposing capital requirements of R$10.8 million to R$37.2 million on all service providers. South Korea's stablecoin legislation is pending as part of Phase 2 regulatory development.

Enforcement Trends

Global regulatory penalties for AML/KYC/sanctions penalties across all financial institutions peaked at approximately $4.6 billion in 2024 before declining 18% to roughly $3.8 billion in 2025. The decline is misleading. Enforcement has moved from securities classification disputes to anti-money laundering, sanctions, and transaction monitoring failures.

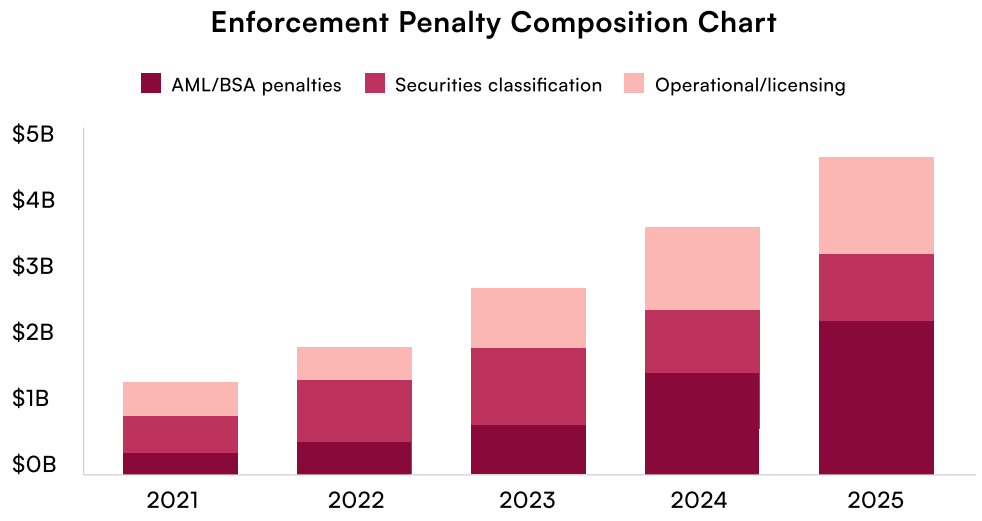


Figure 2: Enforcement Penalty Composition Chart (2021–2025)

Notable AML-Related Penalties in 2025

Rank	Entity	Penalty	Agency	Basis
1	**OKX (Aux Cayes FinTech Co. Ltd.)**	$504 million	DOJ	Unlicensed MSB; BSA/ AML failures
2	**KuCoin (Peken Global)**	$297.4 million	DOJ	Unlicensed MSB; AML failures
3	**UAE Exchange House**	$54.5 million	UAE regulators	AML deficiencies
4	**Block Inc.**	$40 million	DOJ	BSA/AML compliance failures

Figure 3: Notable Global AML Enforcement Actions of 2025 Table

United States: From Securities to AML

The SEC brought 33 crypto-related enforcement actions in 2024, generating over $4.9 billion in crypto-specific financial remedies (driven largely by the $4.5 billion Terraform Labs settlement). In 2025, that figure dropped to 13 actions and $142 million in penalties, representing a 60% reduction in volume and a 97% reduction in financial remedies. The reduction reflects both a change in administration policy and a broader reassessment of the SEC's jurisdictional approach to digital assets.

DOJ and FinCEN filled the enforcement gap. In H1 2025, AML-related fines and settlements exceeded $900 million. The OKX settlement ($504 million) addressed severe AML failures and Bank Secrecy Act violations. KuCoin settled for $297.4 million. Block Inc. paid $40 million. FinCEN fined Brink's Global Services $37 million. These actions established that transaction monitoring deficiencies carry penalties on a scale previously associated with securities fraud.

Europe: Escalating AML Fines

H1 2025 EMEA fines reached $168.2 million, a 767% increase year over year. The FCA led enforcement activity, imposing penalties of £44 million against Nationwide Building Society, £39.3 million against Barclays, and £21.1 million against Monzo, all for AML deficiencies. The Central Bank of Ireland fined Coinbase Europe €21 million for AML/CFT breaches. The activation of MiCA and the establishment of AMLA will extend this enforcement trajectory across the EU.

Asia-Pacific: License Revocation Over Fines

APAC H1 2025 penalty value was $3.4M, down from $10.7M in H1 2024. The disparity reflects a structural difference in approach. MAS and the SFC prefer license revocation and business improvement orders over fines. Japan's FSA issues administrative orders. Singapore imposed

composition penalties on multiple digital payment token service providers in 2025 for Travel Rule and AML screening failures. The financial consequence for non-compliant firms in this region is loss of operating authorization, not a monetary penalty.

Middle East: Enforcement to Maintain FATF Compliance

In May 2025, the Central Bank of the UAE imposed an AED 200 million (approximately 54.4 million USD) penalty on an unnamed exchange house for AML/CFT framework deficiencies. VARA issued Cease-and-Desist orders against multiple entities. ADGM/FSRA published alerts against unlicensed operators in early 2026. The UAE's removal from the FATF grey list in 2024 was a credibility milestone, and regulators are enforcing visibly to maintain that status.

Sanctions Evasion Driving AML Intensification

According to blockchain intelligence estimates, sanctions-related crypto volume grew over 400% year over year in 2025, driven primarily by Russia-linked networks and state-aligned stablecoin infrastructure. State-driven sanctions evasion volume increased an estimated 694% over the same period. These figures explain the intensification of AML enforcement across every region covered above.

Regulatory Developments by Jurisdiction

United States

Regulatory Framework

The United States operates a multi-agency regulatory regime for digital assets. The SEC oversees instruments classified as securities. The CFTC handles commodities and derivatives, with expanded authority anticipated under the CLARITY Act, which passed the House and awaits Senate action. FinCEN enforces anti-money laundering and Bank Secrecy Act requirements. The OCC now supervises stablecoin issuers under the GENIUS Act.

At the state level, New York's proposed CRYPTO Act (Senate Bill S.8901, introduced January 2026) would criminalize unlicensed virtual currency business activity, with graduated penalties from Class A misdemeanor to Class C felony. The bill remains in committee as of this report's publication. New York's BitLicense remains the most demanding state-level licensing framework, with active holders subject to capitalization, cybersecurity, and transaction monitoring requirements. NYDFS mandates code reviews, penetration testing, and capitalization assessments before a licensee can approve new token listings.

Wyoming has approved several Special Purpose Depository Institution bank charters (100% reserve, no lending). Texas mandates annual Proof of Reserves audits under HB 1666.
Implementation and Outlook

The Treasury Department and federal banking agencies (Fed, OCC, FDIC) will issue rulemakings and guidance on GENIUS Act implementation during 2026. The CLARITY Act, if passed, would establish CFTC jurisdiction over digital commodity spot markets. The OCC has begun granting de novo charter approvals to digital asset-focused institutions. The Federal Reserve ended its Novel Activities Supervision Program in August 2025, returning oversight of banks' DLT and crypto activities to the standard supervisory process.

European Union

MiCA and DORA Implementation

MiCA became operational for CASP in December 2024 and represents the EU's single-market framework for crypto-assets. Over 180 entities hold CASP (Crypto-Asset Service Provider) authorization, with Germany and The Netherlands leading in license volume. A single CASP authorization is passportable across all 27 member states, and unauthorized offshore providers are barred from soliciting EU clients. Transitional provisions apply through July 1, 2026.

DORA took effect on January 17, 2025, mandating ICT risk management, structured incident management and reporting, security and operational resilience testing, ICT third party risk

management and threat intelligence sharing for all regulated financial entities, including CASPs. While MiCA does not isolate smart contract audits as a standalone requirement, DORA's operational resilience obligations effectively compel code reviews for any CASP that deploys or relies on smart contract infrastructure. Hundreds of millions in penalties have been signaled for cyber and operational non-compliance.

The new Anti-Money Laundering Regulation (AMLR), complemented by the Anti-Money Laundering Authority (AMLA) Regulation, overhauls the EU's AML framework with specific provisions for the crypto-asset sector. AMLA will centralize supervision and begin direct oversight of a group of financial institutions particularly exposed to cross-border money laundering risks including CASPs by 2028.

MiCA's substance-over-form approach to DeFi applies full CASP licensing requirements to any DAO or development team that exercises material control over a protocol, regardless of how the governance structure is characterized.

Hong Kong

Licensing Framework

Twelve Virtual Asset Trading Platforms hold SFC licenses as of March 2026 under a dual Securities and Futures Ordinance (SFO) and Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) framework. Minimum paid-up share capital is HK$5 million. A 98% cold storage requirement applies. The SFC has indicated that new licensing categories for standalone custody, OTC dealing, and advisory and management services are expected in 2026.

Hong Kong operates a dual-regulator model. The SFC supervises virtual asset trading platforms, custodians, and intermediaries dealing in tokens classified as securities or futures contracts. The HKMA supervises stablecoin issuers under the Stablecoins Ordinance (Cap. 656), which took effect in 2025. On 10 April 2026, the first two licensees were added under HKMA's official register. The Ordinance requires HKMA licensing for any entity issuing a fiat-referenced stablecoin in or from Hong Kong, with full reserve backing, monthly disclosures, redemption-at-par requirements, and an independent smart contract security audit as a precondition for licensing. The HKMA-SFC split mirrors the broader regional pattern of separating issuer prudential supervision from market intermediary conduct supervision.

Smart Contract Audit Mandate

Hong Kong has the most explicit smart contract audit requirements of any major jurisdiction, split across both regulators. The HKMA Stablecoins Ordinance requires an independent smart contract security audit as a precondition for stablecoin issuer licensing, covering reserve management contracts, minting and burning logic, and any on-chain components of the stabilization mechanism. The SFC VATP Guidelines impose a parallel requirement at the token admission stage: an independent assessor must evaluate the security, functionality, and operational integrity of the contract code for any smart contract-based virtual asset before it can be admitted for trading by a licensed platform.

The SFC's Virtual Asset Accelerator program targets institutional-grade token admission processes, with evaluation across security, regulatory compliance, market integrity, and issuer governance dimensions.

Singapore

Thirty-seven licensed Digital Payment Token service providers operate under MAS as of March 2026. The pre-licensing process includes a mandatory independent assessment of technology and cybersecurity risks, covering digital wallets and smart contracts. MAS reserves the right to reject the assessor and demand re-performance. Minimum base capital is S$250,000 (with additional security deposit requirements depending on transaction volume).

Enforcement favors composition penalties: S$960,000 across five firms in June 2025 for Travel Rule and AML screening failures. Project Guardian, the MAS-led collaboration with global banks on tokenization of fixed income, FX, and asset management products, is the most prominent institutional tokenization initiative in Asia-Pacific.

United Arab Emirates

VARA (Dubai)

VARA has licensed dozens of VASPs across several activity categories: exchange services, broker-dealer operations, lending and borrowing, custody, advisory, management and investment, and transfer and settlement. Privacy coins are explicitly prohibited. The Technology and Information Rulebook mandates annual smart contract audits by independent third parties and grants VARA authority to require Threat-Led Penetration Testing on live production environments, a power drawn from the banking sector's TIBER framework.

ADGM (Abu Dhabi)

ADGM oversees dozens of regulated firms conducting virtual asset or fiat-referenced token activities, with a portfolio skewing toward institutional finance, fund structures, and real-world asset tokenization platforms. FSRA requires testing of underlying DLT and smart contract code validation for token admission.

DFSA (Dubai)

The Dubai Financial Services Authority regulates digital asset activities within the Dubai International Financial Centre (DIFC) under an updated Crypto Token regime effective in 2026. The framework transfers token suitability assessment from the regulator to authorised firms, which must document their own assessments against five DFSA criteria covering governance, technology, regulatory treatment, market characteristics, and AML/CFT compatibility. The framework includes additional criteria to assess the suitability of fiat crypto tokens, requiring

them to be backed by high-quality liquid reserves, and it excludes algorithmic designs. DFSA jurisdiction is limited to the DIFC; virtual asset activity elsewhere in Dubai falls under VARA's regulatory framework.

CBUAE

The Payment Token Services Regulation requires AED-denominated backing for domestic payment stablecoins. Foreign currency and algorithmic stablecoins are prohibited for merchant transactions. The UAE was removed from the FATF grey list in 2024.

 Japan

In April 2026, Japan's Cabinet approved a draft amendment to the Financial Instruments and Exchange Act (FIEA) that would classify crypto assets as financial instruments. The amendment prohibits insider trading in crypto assets, requires annual disclosures from issuers, and raises maximum penalties for unregistered operation to ten years' imprisonment and ¥10 million in fines. A separate tax proposal under discussion would apply a 20% flat rate to crypto gains in place of the current progressive rate of up to 55%. If enacted, the FIEA changes would take effect as early as fiscal year 2027. Stablecoin issuance remains under the Payment Services Act and restricted to licensed banks, trust companies, and fund transfer operators. A 95% cold wallet requirement applies. The JVCEA's pre-approval process for token listings functions as a de facto security assessment through self-regulation.

 Brazil

Regulatory Framework

Brazil is the largest crypto market in Latin America, receiving an estimated $318.8 billion in crypto value between July 2024 to June 2025, with 109.9% period-over-period growth and ranking fifth on the 2025 Global Crypto Adoption Index. Approximately 90% of that volume is stablecoin-denominated, used primarily for payments, settlement, and cross-border transfers. Monthly reported transaction volumes reach $6 to $8 billion.

BCB Resolutions and the SPSAV Framework

Banco Central do Brasil (BCB) Resolutions 519, 520, and 521 (November 2025) took full effect on February 2, 2026, with a 270-day grace period through October 2026. Together, they create the SPSAV (Sociedades Prestadoras de Serviços de Ativos Virtuais) authorization framework. All entities operating as custodians, exchanges, or intermediaries must apply for SPSAV authorization and will be supervised by the BCB. Foreign platforms must either establish a local subsidiary or partner with a licensed local entity, and must migrate Brazilian clients to the authorised structure. Capital requirements vary depending on the scope of services.

Resolution 520 addresses cybersecurity directly. Firms must document and implement comprehensive security measures covering identity management controls, continuity and incident response plans, and protections for sensitive information. Resolution 521 also establishes specific requirements for stablecoins and other fiat-referenced virtual assets, treating stablecoin flows as FX transactions subject to BCB reporting.

BCB Instruction No. 701/2026

Instruction No. 701, effective February 2, 2026, complements Resolution 520 by establishing the requirements for independent technical certification that must accompany SPSAV authorization applications. The technical opinion must cover asset segregation and proof of reserves, assessment of relevant services (cloud, processing, data security, foreign providers), risk management and governance (with focus on AML/CFT, cybersecurity, internal audit, and continuous monitoring), listing and delisting procedures for assets (with specific requirements for stablecoins under Article 65 of Resolution 520), internal controls and key redundancy for custodians handling mint/burn mechanisms and reserve management, and user transparency including disclosure of staking risks, asset exposure, and infrastructure operations.

Each item must be analyzed individually; the BCB will not accept generic opinions. The BCB reserves the right to request additional detail at any time, reinforcing ongoing supervisory engagement. For firms seeking to operate with stablecoins, tokenization, or market infrastructure in Brazil, IN 701 brings the compliance bar to a level comparable with Hong Kong and Singapore's pre-licensing requirements.

Tax Reporting: DeCripto and CARF Alignment

Since 2019, the Receita Federal (RFB) has required reporting of crypto transactions through Normative Instruction No. 1,888/2019. Domestic exchanges must report all transactions including counterparties, dates, values, wallet addresses, and fees. Individuals and companies must report crypto sales exceeding BRL 30,000 per month. Non-compliance triggers fines from BRL 1,500 to 3% of the undeclared amount.

Normative Instruction No. 2,291/2025 replaces the existing reporting system with DeCripto, effective July 1, 2026. DeCripto aligns with the OECD's Crypto-Asset Reporting Framework (CARF) and requires exchanges to classify transactions into specific categories: crypto-to-fiat trades, crypto-to-crypto swaps, retail payments over $50,000, wallet transfers, and movements to unhosted wallets. Brazil has committed to implementing CARF by April 2027, joining 67 jurisdictions in the automatic exchange of crypto tax information.

Capital gains from crypto are taxed at 15% to 22.5% on monthly gains above BRL 35,000.

Institutional Infrastructure: Piloto Drex

The Piloto Drex CBDC provides BCB-supervised DLT infrastructure for institutional tokenization, including fixed income, trade finance, and real estate. It is the most advanced sovereign CBDC tokenization platform in Latin America and positions Brazil as a jurisdiction where traditional and digital asset infrastructure can converge under a single regulatory authority.

South Korea

The Virtual Asset User Protection Act (VAUPA) has been fully operational since July 2024. Twenty-six VASPs are registered, but only five exchanges are permitted to offer fiat-to-crypto trading through mandatory real-name verified bank partnerships. The first criminal prosecution referrals for market manipulation under VAUPA occurred in 2025.

DAXA requires security assessments and code reviews before domestic listings. Financial Service Commission's Phase 2 legislation covering token issuance rules, stablecoin frameworks, and institutional investment access is pending.

India

India operates without a comprehensive crypto regulatory framework, but has built a substantial enforcement and tax infrastructure around digital assets. Crypto is legal to own, buy, sell, and trade, but is not recognized as legal tender. The Reserve Bank of India (RBI) has consistently resisted legislation that would confer legitimacy on the sector, and a proposed discussion paper on comprehensive regulation has been shelved repeatedly, most recently in April 2026. Differences in regulatory approach between the Finance Ministry and the RBI remain unresolved.

Despite the legislative vacuum, operational compliance requirements are extensive. Since March 2023, VASPs have been classified as reporting entities under the Prevention of Money Laundering Act (PMLA). The Financial Intelligence Unit (FIU-IND) has registered 49 platforms as of early 2026. In January 2026, FIU-IND issued updated AML/CFT guidelines introducing mandatory CERT-In cybersecurity audits, tighter Travel Rule norms with no minimum threshold, enhanced KYC rules including live selfie verification with liveness detection, and geolocation capture (latitude/longitude, IP addresses, device identifiers) at onboarding. Privacy coins, tumblers, and mixers are flagged as carrying serious money laundering risks.

The FIU has demonstrated willingness to use sharp enforcement tools. Under Section 79(3)(b) of the Information Technology Act, FIU can trigger takedowns of apps and URLs of offshore platforms serving Indian users without registration. In late 2023 and October 2025, the FIU blocked access to 25 offshore exchanges. Show-cause notices have been issued to Binance, KuCoin, Huobi, Kraken, Gate.io, Bittrex, Bitstamp, MEXC Global, and Bitfinex for non-compliance. The Income Tax Department has identified undisclosed crypto assets worth INR 888.82 crore and sent over 44,000 communications to flagged taxpayers.

The tax regime imposes stringent rates: 30% flat tax on all crypto gains with no loss offset against other income, 1% TDS on all transactions, and mandatory reporting under the Income Tax Act. The CBDT's March 2026 notification reclassified crypto-assets as financial assets under India's FATCA/CRS reporting framework, retroactive to January 1, 2026. India has committed to implementing the OECD's CARF by April 2027.

For companies considering India as a market: there is no VASP licensing pathway, but the AML/KYC and tax reporting obligations are banking-grade. The enforcement posture is strict toward non-compliant offshore platforms, and the tax burden is among the highest globally.

Turkey

Regulatory Framework

Turkey has moved from a fragmented watch-and-wait posture to a comprehensive VASP licensing regime. The July 2024 amendments to the Capital Markets Law require all Crypto Asset Service Providers (CASPs) to obtain an operating license from the Capital Markets Board (CMB). Turkey was removed from the FATF grey list in 2024, and the regulatory push is partly driven by the need to maintain that status.

The CMB issued its operational regulations in March 2025 (Communiqués No. III-35/B.1 and III-35/B.2), detailing minimum capital requirements, managerial qualifications, information system infrastructure standards, and internal control mechanisms. Minimum charter capital is TRY 150 million (approximately $4.1 million) for CASPs providing platform services and TRY 500 million (approximately $13.7 million) for depository institutions. Companies on the existing "List of Actively Operating Organizations " were required to apply for an operating license by June 30, 2025, with full authorization expected by June 30, 2026.

AML/CFT and MASAK

The Financial Crimes Investigation Board (MASAK) enforces AML/CFT compliance. CASPs are classified as obligated entities under Law No. 5549. MASAK Circular No. 29 (June 2025) and the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism impose withdrawal restrictions (including limits on amounts and number of transactions) and transaction disclosure requirements. The Travel Rule applies, with Turkey aligning its implementation to FATF Recommendation 16. A proposed bill would grant MASAK authority to freeze and shut down accounts suspected of engaging in illegal activities on crypto platforms, banks, electronic money institutions, and payment firms.

Technical Standards and Security

TÜBİTAK (the Scientific and Technological Research Council of Türkiye) sets technical infrastructure and cybersecurity standards for CASPs. It evaluates and audits platform infrastructure before licensing. The CMB requires CASPs to segregate customer assets from proprietary holdings and maintain documented risk management, governance, and internal audit programs. Customer assets must be stored separately, and the CMB retains authority to appoint custody institutions. It also imposes an explicit smart contract audit requirement for staking services.

The combination of CMB licensing conditions, TÜBİTAK technical audits, and MASAK AML requirements creates a multi-layered compliance regime. For companies evaluating Turkey as a market: the licensing process is operationally heavy, the capital requirements are significant, and the regulatory infrastructure now mirrors the dual-authority model (market regulator plus AML enforcer) seen in more established jurisdictions.

Taxation

There is no specific crypto tax law as of early 2026. Profits from trading or mining are taxable under general income tax rules. A transaction tax (proposed at 0.03%) has been discussed but not implemented. The government's approach remains cautious: the 2021 ban on crypto for payments still applies, and the CBRT is piloting a Digital Turkish Lira alongside the regulatory buildout for private crypto.

Other Jurisdictions

United Kingdom

FCA authorization under the Senior Managers and Certification Regime (SM&CR). A dual FCA and Bank of England stablecoin framework is under development with holding limits. No decentralization exemption exists for DeFi. AML enforcement is escalating significantly. Smart contract audit requirements are implied through operational resilience obligations but are not yet explicitly mandated. The FCA's FSMA-based authorization period opens in September 2026.

Saudi Arabia

CMA draft rules for tokenised securities are expected by early 2026. The approach is wholesale-focused and deliberately avoids retail speculation.

Australia

AFSL framework administered by ASIC. AUSTRAC AML compliance required by July 2026.

Nigeria

Mandatory VASP licensing under the Investment and Securities Act 2025. Banks are now permitted to serve SEC-licensed entities.

Smart Contract Security: Regulatory Mandates

Smart contract security regulation has moved from voluntary best practice to statutory requirement within the past 2 years.

Jurisdiction	Requirement	Mechanism	Mandate Type
Hong Kong	SC audit as precondition for Stablecoin licensing. Independent assessor for SC-based virtual assets before token admission.	HKMA Stablecoins Ordinance (for stablecoin issuers); SFC VATP Guidelines (for token admission by VATPs)	Statutory
VARA (Dubai)	Annual SC audits by independent third parties.	Technology and Information Rulebook	Statutory
ADGM (Abu dhabi)	DLT stress testing. SC code validation.	FSRA token admission requirements	Statutory
Singapore	Independent technology and cybersecurity assessment incl. smart contracts.	MAS Guidelines On Licensing For Payment Service Providers	Statutory
EU	Digital operational resilience testing (incl. source code reviews)	DORA	Statutory
US (NYDFS)	Code reviews and penetration testing for new token listings.	BitLicense requirements	State mandate
Japan	Security review for token listing pre-approval.	JVCEA self-regulatory process	Self-regulatory
South Korea	Security assessments and code reviews before domestic listings.	DAXA self-regulatory process	Self-regulatory
Brazil	Independent technical certification covering cybersecurity, asset segregation, and key management under BCB IN 701/2026, supplemented by the direct smart contract testing requirement in BCB Resolution No. 520 (Art. 48.VIII)	BCB Resolution No. 520 (Art48.VIII)	Statutory
Turkey	Technical infrastructure and cybersecurity audit by TÜBİTAK.	CMB CASP licensing process	Statutory

Figure 4: Statutory Smart Contract Security Mandates Table

The Empirical Case for Mandatory Audits

CertiK's internal Web3 Security analysis of the top 100 exploited protocols found that 80% had never undergone a formal security audit before the breach. Those unaudited protocols accounted for 89.2% of total value lost. The 20% that had been audited accounted for 10.8% of losses. Regulators across jurisdictions now cite this type of empirical evidence when justifying mandatory audit requirements.

Exploit Trends: Infrastructure Over Code

On-chain exploit losses rebounded in 2025 after declining from the 2022 peak. By mid-year, over $2.17 billion had been stolen, already exceeding the full-year 2024 total. The mix of attacks changed: infrastructure compromises (private key theft, access control failures, wallet orchestration exploits) drove 76% of 2025 losses by value. Smart contract code exploits accounted for a declining share.

The Bybit breach in February 2025 ($1.46 billion, attributed to North Korean operatives by the FBI) illustrated this shift. The smart contracts were not exploited; the signing infrastructure was compromised. This evolution has implications for regulatory mandates: security requirements that focus exclusively on code audits address a diminishing proportion of actual losses. Comprehensive security assessments that include infrastructure review, access control evaluation, and operational security testing are increasingly necessary to match the threat environment.

Cross-Jurisdictional Comparison

Convergence is strongest on AML/KYC requirements and stablecoin reserve standards across eleven jurisdictions. DeFi treatment and smart contract audit mandates show the widest divergence.

Jurisdiction	Authority	Licensing Framework	Stablecoin Regime	DeFi Treatment	AML/KYC Statute	Smart Contract Audit
US	SEC, CFTC, OCC, FinCEN, NYDFS	State MTL + federal multi-agency. CLARITY Act passed House; Senate pending.	GENIUS Act (signed 2025; rulemaking ongoing). 1:1 reserves required.	IRS digital asset broker rule applies to front-ends.	BSA. FATF Travel Rule via FinCEN.	NYDFS guidance only. No federal mandate.
EU	ESAs (ESMA, EBA, EIOPA), ECB, NCAs	MiCA CASP authorization. Passportable across EU-27.	ART/EMT under MiCA. EBA oversight of significant issuers.	Substance-over-form. DAOs with material control = CASP licensing.	6AMLD + AMLR, TFR for Travel Rule	Source code reviews mandated under DORA
UK	FCA, BoE	FCA cryptoasset firm registration. Broader regime in development.	Joint FCA / BoE stablecoin regime in consultation.	No specific exemption.	MLRs 2017. JMLSG Travel Rule guidance.	Implied via operational resilience expectations.
HK	SFC, HKMA	SFC VATP under SFO + AMLO. HK$5M paid-up capital. 98% cold storage.	HKMA Stablecoins Ordinance (Cap. 656, effective 2025).	Not yet addressed.	AMLO. Strict traceability. Travel Rule mandatory.	HKMA mandatory for stablecoin issuers; SFC mandatory for token admission.
SG	MAS	PSA Digital Payment Token licence under MPI or SPI category. S$250,000 base capital minimum for MPI.	MAS-regulated SCS framework (proposed). Non-SCS under DPT regime.	Not yet addressed.	AMLA + PSN02. Composition penalties used for enforcement.	Pre-licensing independent technology assessment mandatory.
UAE	CBUAE, VARA and DFSA (Dubai), ADGM FSRA	VARA (Dubai); ADGM FSRA (Abu Dhabi); CBUAE for retail PSP. 20+ active ADGM firms.	CBUAE Payment Token Services Regulation. AED-backed only domestically.	Not yet addressed.	Federal Decree-Law 20/2018. FATF grey list cleared 2024.	VARA annual security testing (incl. Smart contracts). ADGM FSRA DLT stress testing.
JP	FSA	PSA Crypto Asset Exchange Service Provider (CAESP). 28 registered.	Governed by Payment Services Act. Banks and trust companies only.	Not yet addressed.	APTCP. FSA administrative orders for breaches.	Self-regulatory via JVCEA.
KR	FSC, FIU	VASP registration under Specified Financial Information Act. Bank partnership required.	Phase 2 legislation pending under Digital Asset Basic Act.	Not yet addressed.	SFIA. Criminal penalties for unregistered VASPs.	Self-regulatory via DAXA.
BR	BCB, CVM	BCB SPSAV under Resolutions 519 / 520 / 521. Effective October 2026.	BCB Resolution 520 / 521 FX and payment-token treatment.	Not yet addressed.	Law 9.613/98. DeCripto reporting Jul 2026. CARF 2027.	IN 701 independent technical certification (eff. Feb 2026). BCB Res. 520 Art. 48.VIII smart contract testing.
IN	FIU-IND, SEBI (limited)	No formal VASP license. FIU-IND registration required.	No framework.	Not yet addressed.	PMLA. FIU enforcement. CARF 2027.	None
TR	CMB (SPK), MASAK	CMB CASP license. TRY 150M minimum capital.	No specific framework.	Not yet addressed.	MASAK regulation. FATF Travel Rule.	TÜBİTAK infrastructure and cybersec audit.

Figure 5: Regional Regulatory Requirements Summary Table

Implications for Institutional Participants

Regulatory requirements across jurisdictions point in the same direction: higher compliance thresholds, more prescriptive security mandates, and less tolerance for ambiguity. Five implications stand out.

Multi-Jurisdictional Licensing Is the Cost of Entry

MiCA passporting simplifies European access, but every other major jurisdiction requires an independent application with jurisdiction-specific capital, custody, and reporting requirements. Brazil's new SPSAV framework requires foreign platforms to establish a local subsidiary or partner with a licensed entity, with capital requirements up to R$37.2 million and mandatory independent technical certification under IN 701. Operating from a single offshore license is no longer viable for institutions that need regulatory credibility with counterparties and supervisors.

AML Compliance Has Overtaken Securities Classification as the Primary Enforcement Risk

Recent AML settlements exceeding $500 million in a single action established that transaction monitoring deficiencies carry penalties previously associated with securities fraud. Institutions handling digital asset flows should evaluate their AML screening, sanctions checking, and suspicious activity reporting capabilities against the standard that DOJ and FinCEN are now enforcing.

Smart Contract Audits Are a Non-Negotiable Operating Cost

Seven jurisdictions mandate them. Institutions deploying or interacting with smart contracts should budget for independent audits as a recurring requirement in any market with a developed regulatory framework. The empirical basis for these mandates (89.2% of exploit losses concentrated in unaudited protocols) provides the business case as well as the regulatory rationale.

Stablecoin Infrastructure Must Meet Banking-Grade Standards

Full reserve backing, segregated custody, independent attestation, and licensed issuance are required across every major jurisdiction. Algorithmic stabilization models are prohibited everywhere. Reserve management for stablecoin operations requires the same governance and controls applied to a regulated payments institution.

Basel Capital Treatment Will Shape Institutional Portfolio Construction

The Group 1 and Group 2 distinction determines which digital assets banks can hold economically. Tokenized traditional instruments and qualifying stablecoins have a path to institutional adoption. Unbacked tokens face capital charges that make large-scale holdings uneconomical for bank balance sheets.

About CertiK

CertiK provides advisory, security, and compliance services for companies and institutions operating across the digital asset licensing chain. From pre-licensing strategy and regulatory gap analysis through smart contract auditing, penetration testing, and AML infrastructure deployment, CertiK supports clients at every stage of their compliance lifecycle.

Services include DLT strategy and architecture advisory, code security audits and formal verification, penetration testing for exchanges, wallets, and custody platforms, compliance and licensing application support, Skynet Enterprise for continuous risk monitoring and vendor oversight, SkyInsights for transaction monitoring and AML/KYT, Proof of Reserves attestation, and 24/7 incident response.

CertiK operates as a strategic partner to regulators and financial institutions globally, contributing to policy development through security advisory and consultation responses across multiple jurisdictions.

CERTIK
SKYNET

COMPANY INTRO

CertiK is the largest Web3 security services provider, founded in December 2017 in New York by two professors from Yale and Columbia University.

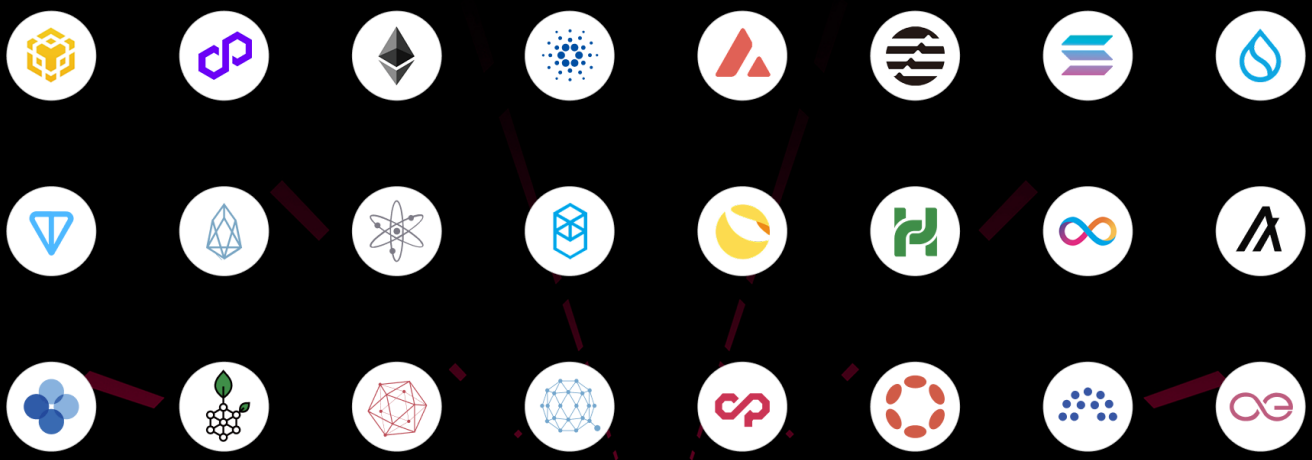
Powered by the industry's largest proprietary Web3 security database, CertiK provides actionable insights, including incident analyses, security reports and guidelines. It has also become a trusted security partner for global regulators, institutions, and Web3 enterprises, supporting both their security needs and their pursuit of innovation.

5,000+
CLIENTS SERVED

180,000+
VULNERABILITIES DETECTED

>$600B
MARKET CAP ASSESSED

>70% OF TOP 500 CMC PROJECTS AUDITED



DIVERSITY IN ECOSYSTEMS