PHAROS
RESEARCH

Convergence & Divergence: Baselines and Fault Lines in Crypto Regulation

Table of Contents

Abstract

In recent years, major jurisdictions have been steadily building out regulatory frameworks for crypto-asset trading platforms and services. At the global level, regulators have already formed a consensus around four key “regulatory baselines” in several core risk-control areas, namely:

(1) Anti–money laundering and customer due diligence (KYC/AML);

(2) Segregated and independent custody of client assets;

(3) Market manipulation prohibitions;

(4) Management and prevention of conflicts of interest on trading platforms.

These areas have become the cornerstone of regulatory convergence across countries. However, there are marked policy divergences across jurisdictions in three “emerging domains”:

(1) Regulatory paths for stablecoins;

(2) Market access for crypto-derivatives and privacy coins;

(3) The regulatory perimeter for real-world asset tokenization (RWA) and decentralized finance (DeFi).

This pattern of convergence and divergence not only reflects differences in legal traditions and risk preferences across national financial systems, but also poses challenges for the compliance strategies of cross-border crypto-asset businesses. It is particularly worth noting that, given the stringent prohibitions on crypto-asset trading in mainland China and the Hong Kong Special Administrative Region’s active pursuit of Web3.0 policy experiments under “one country, two systems,” this article takes Hong Kong’s compliance practice as the primary reference when discussing the “China perspective.” This is intended to highlight the unique experimental role that the Hong Kong market plays in the global regulatory landscape. Drawing on a comparative analysis of regulatory statutes, institutional rules, and representative cases from the United States, the European Union, the United Kingdom, Hong Kong (China), Singapore, Japan, and other key jurisdictions, the article sets out both the emerging global consensus on “regulatory red lines” in crypto trading and the main areas of regulatory divergence.

Keywords: public-chain assets, cross-jurisdictional comparison, institutional evolution, regulatory convergence and divergence

01 / Introduction

The cross-border liquidity of blockchain and crypto assets presents regulators around the world with the challenge of balancing financial innovation against systemic risk. Against this backdrop, jurisdictions are gradually sketching out a set of “regulatory red lines” that cannot be crossed, in order to govern public-chain asset trading activities and protect investor rights. For example, anti–money laundering (AML) and know-your-customer (KYC) requirements have become almost universal. Most major jurisdictions now bring virtual asset service providers (VASPs) within the scope of their AML frameworks.[1] Likewise, mandating segregated and independent custody of client assets—so that client assets are shielded from third-party creditors in the event of bankruptcy—is widely regarded as a baseline requirement. In addition, preventing market manipulation, curbing insider trading, and avoiding conflicts of interest between trading platforms and their affiliates have become shared objectives among regulators seeking to preserve market integrity and investor confidence.[2][3]

Although regulation has converged in these key areas, jurisdictions diverge sharply on several emerging questions. Stablecoin regulation is a prime example: some countries restrict stablecoin issuance to licensed banks or similar institutions and impose stringent reserve requirements, while others remain in the exploratory phase of legislation.[4][5] In the realm of crypto-derivatives, a few jurisdictions (such as the United Kingdom) directly prohibit the sale of such high-risk products to retail customers,[6] whereas others license and supervise derivatives trading with leverage caps and other safeguards. There are also wide disparities in the legal status of privacy coins (anonymity-enhancing cryptocurrencies): some countries explicitly ban exchanges from supporting privacy-coin trading, while others have not imposed outright bans but use stringent compliance requirements to indirectly suppress circulation.[7] Furthermore, regulators differ in their approach to the tokenization of real-world assets (RWA) and DeFi: some actively create sandboxes and bespoke rules to bring such innovations under supervision, while others prefer to subsume them under existing securities or financial regulations.

To systematically analyze this pattern of convergence and divergence, this article conducts a cross-jurisdictional comparison of regulatory frameworks in several representative regions, including the United States, the EU/UK, and East Asia. Chapters 2 through 5 focus on specific topics related to regulatory red-line consensus and institutional divergence. Drawing on actual statutory provisions, official documents issued by regulatory authorities, and representative institutional practices and cases, these chapters outline each jurisdiction’s regulatory approach.[2][8] Chapter 6 then synthesizes the similarities and differences in regulatory experience and discusses the implications of this regulatory landscape for the global crypto-asset market. The concluding section offers reflections on the future of international regulatory coordination and the development of industry compliance.

Through this analysis, the article aims to provide detailed reference material for crypto-asset institutions and compliance researchers, helping them better understand both the shared “red-line” baselines and the divergences across jurisdictions, so that they can more effectively manage compliance risk in cross-border operations. It also seeks to offer policymakers a comparative perspective for exploring possible paths toward regulatory coordination at the global level.

02 / Consensus Red Lines on Funding Compliance and Asset Safety

This chapter examines the first two baselines on which global regulatory consensus is strongest: AML (KYC/AML) and client asset segregation. Although jurisdictions are broadly aligned at the conceptual level, there remain noteworthy differences in implementation details.

2.1 Global benchmarks for customer identification and AML (KYC/AML)

Since 2018, it has become a global regulatory consensus that AML and counter–terrorist financing (CFT) requirements must fully extend to crypto assets. At the international level, the Financial Action Task Force (FATF) revised Recommendation 15 in 2019, bringing VASPs within the scope of AML/CFT obligations on essentially the same footing as traditional financial institutions.[1] FATF also introduced the "Travel Rule," which requires VASPs to collect and transmit identity information of the originator and beneficiary for large crypto transactions.[13] These global standards provide a benchmark for domestic legislation. As of 2025, the vast majority of major jurisdictions have incorporated VASPs into their national AML systems, establishing customer identification (KYC), suspicious transaction reporting, and other regimes. According to FATF's latest report, 99 jurisdictions have enacted or are advancing laws to implement the Travel Rule and improve transparency for cross-border virtual asset transfers.[14]

In the United States, AML obligations are primarily established under the Bank Secrecy Act (BSA, 1970) and its implementing regulations. The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury, has since 2013 explicitly recognized that most crypto-asset trading platforms fall under the category of "money services businesses" (MSBs), and must therefore register with FinCEN and comply with the BSA.[2] Specific obligations include implementing written customer identification program (CIP) procedures to collect and verify basic information such as name, address, and ID number; conducting customer due diligence (CDD) to identify beneficial owners of legal-entity customers and understand the purpose and intended nature of customer relationships;[15] maintaining transaction records; and filing suspicious activity reports (SARs). In addition, the 2021 Infrastructure Investment and Jobs Act introduced tax reporting obligations for crypto transactions, and further legislation is under consideration to strengthen reporting requirements for transactions involving unhosted wallets. On the enforcement side, U.S. authorities have repeatedly brought civil and criminal cases against crypto firms that failed to comply with AML rules. For example, the well-known derivatives exchange BitMEX was effectively found to be a "money laundering platform" due to its failure to implement KYC/AML programs. Its founders pleaded guilty to BSA violations and paid a total of USD 100 million in penalties.[16][17] In another case, a former Coinbase employee was prosecuted for insider trading in connection with crypto listings and accused of profiting by circumventing KYC and other compliance controls, underscoring the intensity of U.S. enforcement efforts against money laundering and fraud in the crypto industry.

The European Union brought virtual currency exchanges and custodial wallet providers within the scope of AML regulation with the Fifth Anti–Money Laundering Directive (5AMLD) adopted in 2018, requiring them to register and fulfil KYC/AML obligations.[18] Member States revised their domestic laws accordingly (for example, Germany's Anti–Money Laundering Act and France's Monetary and Financial Code) to subject crypto service providers to identity verification and suspicious activity reporting requirements. In 2023, the EU formally adopted the Markets in Crypto-Assets Regulation (MiCA, Regulation (EU) 2023/1114), which establishes a unified authorization regime for crypto-

asset service providers (CASPs).[19] While MiCA itself focuses primarily on market conduct and investor protection, it is complemented by a new AML Regulation (AMLR) and amendments to the Sixth Anti–Money Laundering Directive (6AMLD), agreed in 2024, which impose enhanced customer due diligence and beneficial ownership identification requirements on CASPs and other obliged entities.[20] The EU also plans to establish a dedicated Anti–Money Laundering Authority (AMLA) to strengthen cross-border supervision and coordination. As a result, every crypto trading platform operating within the EU must implement robust KYC procedures, conduct ongoing monitoring of customer transactions, and cooperate with law-enforcement authorities to combat money laundering, or risk license revocation and substantial fines.

Asian financial hubs have likewise followed international standards and established AML frameworks for crypto assets. Regulators in Hong Kong, Singapore, Japan, and other Asian jurisdictions emphasize that both centralized exchanges and other types of VASPs must implement comprehensive AML compliance programs and may not become conduits for money laundering or illicit capital flows.

Hong Kong amended its Anti–Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) in 2022, introducing a mandatory licensing regime for VASPs effective June 2023.[21] Under the AMLO and related guidelines issued by the Securities and Futures Commission (SFC), trading platforms must implement strict measures for customer identification, risk assessment, transaction monitoring, and periodic review. They must also comply with the Travel Rule by rapidly transmitting customer and transaction information to counterparty institutions for qualifying transfers.[21]

Singapore's Payment Services Act (PSA), enacted in 2019, brings digital payment token service providers under the supervision of the Monetary Authority of Singapore (MAS). MAS Notice PSN02 sets forth detailed AML/CFT requirements, including the application of the Travel Rule to virtual asset transfers above SGD 1,500 and enhanced due diligence for transactions involving unhosted wallets.[22]

Japan amended its Payment Services Act and Act on Prevention of Transfer of Criminal Proceeds as early as 2017, requiring crypto-asset exchange service providers to register with the Financial Services Agency (FSA) and comply with KYC and anti–money laundering obligations.[23] Exchanges must verify customer names and addresses when opening accounts, monitor transactions, and conduct enhanced scrutiny for transactions above certain thresholds (for example, JPY 100,000).[23] Japan is also one of the most active promoters of the Travel Rule, incorporating it into domestic law so that virtual asset transfers above JPY 100,000 must be accompanied by information about senders and recipients.[24]

Figure 1: Anti money laundering and Travel Rule (cross platform transfer information accompanying)

legal jurisdiction	Execution Status	Key points notes
European Union (EU)	Effective	The Regulations on the Transfer of Funds (TFR) apply to encrypted transfers; Fully implemented from December 30, 2024, regulatory technical guidelines will be issued by the EBA.
United Kingdom (UK)	Effective	Starting from September 1, 2023, encryption companies within the UK industry must collect, verify, and transmit information of the beneficiary/beneficiary when making cross platform transfers.
Singapore (SG)	Effective	MAS Notice PSN02 requires DPT service providers to collect and transmit necessary information along with transactions above a threshold, and retain records.
United States (US)	Effective	FinCEN explicitly states that "Convertible Virtual Currency" (CVC) is subject to the "Travel Rule" for funds, and MSB is required to transmit the information of the beneficiary/beneficiary along with eligible transfers.
Hong Kong (HK)	Principle alignment with FATF	According to the anti money laundering framework and VASP/VATP guidelines, carry out risk-based customer due diligence and transfer information obligations (specific implementation details depend on licensing arrangements).

Source: Pharos Research

In sum, KYC/AML regulation has become a “baseline” consensus in the crypto-asset trading space: while legislative techniques and enforcement intensity vary, all major jurisdictions recognize that strengthening customer identification and transaction transparency is a first-order priority for safeguarding the financial system from criminal abuse.[1] This emerging consensus has created, to some extent, a unified compliance threshold for cross-border crypto business: global institutions must meet local KYC standards and cooperate with suspicious transaction monitoring in all relevant jurisdictions, or they will struggle to obtain operating licenses. At the same time, enforcement intensity and specific rules differ by jurisdiction (for example, U.S. criminal prosecutions of violators, the EU’s emphasis on harmonized rules, and Asian regulators’ focus on licensing and supervisory conditions), requiring firms to tailor global compliance strategies to local regulatory details.

2.2 Segregated and independent custody of client assets

Client asset segregation is a core regulatory tool for protecting investors and preventing the transmission of insolvency risk in financial intermediaries. In traditional securities and derivatives markets, many jurisdictions already have mature rules (such as the U.S. SEC’s customer protection rules and the UK FCA’s Client Asset Sourcebook) requiring brokers to hold client funds separately from their own assets. For crypto-asset trading platforms, a series of scandals in recent years—including the sudden collapse of a major global exchange in late 2022 due to the misappropriation of client funds—have further highlighted the importance of segregating client assets. Regulators around the world increasingly agree that platforms must not commingle user-custodied digital assets with their own assets, and must not unilaterally use client assets for lending, investment, or other purposes. Otherwise, a platform’s financial distress can severely harm investors. Asset segregation has thus become one of the key regulatory red lines across major jurisdictions.

The EU’s MiCA sets out clear requirements regarding the custody and segregation of clients’ crypto assets. Authorized CASPs holding crypto assets on behalf of clients must segregate those client assets from the provider’s own assets in both legal and operational terms.[3] In practice, CASPs are required to clearly label client assets on distributed ledgers and maintain ledger records that distinguish client-held tokens from the provider’s proprietary tokens.[3] MiCA further emphasizes that client assets are legally separate from the CASP’s estate, such that platform creditors have no claim on client-custodied crypto assets in the event of insolvency.[25] In other words, clients retain ownership or beneficial rights in their custodied assets and do not become general unsecured

creditors of the platform upon bankruptcy. These provisions are consistent with long-standing principles of client asset segregation in EU securities regulation. Articles 67 and 68 of Regulation (EU) 2023/1114 detail CASPs' custodial duties and asset segregation measures, including separate accounting for client and proprietary assets in both technical and operational systems as well as internal control and audit mechanisms to ensure effective segregation.[26][27] The EU's intent is to learn from past exchange failures, eliminate legal uncertainty about the status of client assets, and provide investors with a level of bankruptcy protection analogous to that in traditional finance.

At the U.S. federal level, there is no single statute specifically dedicated to crypto-asset custody and segregation, but some state regulators and federal agencies have begun to act. Notably, the New York State Department of Financial Services (NYDFS)—known for its strict stance—issued guidance in January 2023 for virtual currency custodians (those holding a BitLicense or trust charter). NYDFS requires custodians to "separately account for and segregate" client virtual currency from the custodian's own crypto holdings. This may be achieved by maintaining individual wallets or sub-ledger accounts for each client, or by holding client assets in an omnibus account that is strictly segregated from proprietary holdings. Regardless of the method, custodians must ensure that client assets are not recorded as their own balance-sheet assets, nor used for any purpose other than safekeeping. NYDFS also reiterates that custodians may not rehypothecate, lend, or otherwise deploy client assets without the client's explicit instruction. This guidance responds directly to high-profile industry failures (such as Celsius and FTX), where courts disputed whether client-held crypto constituted customer property or part of the bankruptcy estate, leaving users with substantial losses. By clarifying that client assets enjoy priority over other creditors, NYDFS sets a regulatory benchmark for client asset segregation in the United States.[10] Other states, such as Wyoming, have enacted digital asset laws that recognize custodied digital assets as client property rather than custodian property, thereby providing similar bankruptcy-remote protection.

In Hong Kong, the SFC's 2023 "Guidelines for Virtual Asset Trading Platform Operators" identify "proper custody of client assets" as one of the core principles for licensed platforms.[5] The guidelines require platforms to adopt measures to ensure the secure safekeeping of client virtual assets, including storing the vast majority of client assets in high-security cold wallets and imposing strict withdrawal limits and multi-signature controls on hot wallets. The guidelines also require a clear separation of client assets from platform assets. In practice, licensed platforms in Hong Kong typically hold clients' fiat funds in segregated trust accounts and maintain client crypto assets in dedicated addresses or custody accounts to achieve legal and operational segregation. For example, some platforms state that 98% of client assets are stored in cold wallets under the control of an independent custodian, with only 2% reserved for daily withdrawals, and they periodically report reserve levels to regulators. These measures are designed to prevent platforms from misusing client assets for proprietary purposes and to mitigate losses in extreme events such as platform insolvency or hacking incidents. In late 2023, the SFC issued additional circulars emphasizing that client asset custody must be subject to strong governance and audit controls: senior management should regularly review custody arrangements and private-key management processes, and external auditors should be engaged to verify client asset balances, thereby enhancing transparency.[11][12] These requirements show how seriously Hong Kong's regulators take client asset safety, aiming to avoid a repeat of overseas exchange failures and to safeguard Hong Kong's reputation as a compliant crypto hub.

The MAS in Singapore also scrutinizes custody arrangements and internal controls when licensing digital payment token service providers, ensuring that client assets are not misused. Although Singapore has not yet enacted a dedicated statute on client asset segregation, MAS guidance encourages licensees to hold client tokens in separate on-chain addresses from operating funds and to implement daily reconciliation and proof-of-reserves mechanisms. In Japan, the FSA has, since 2018, required exchanges to "trustify" client assets, meaning that clients' fiat deposits must be

entrusted to third-party trust banks, and at least 95% of client crypto assets must be held offline. Amendments to the Financial Instruments and Exchange Act in 2019 brought crypto assets within the definition of financial instruments and formalized requirements for daily reconciliation of client assets: if client holdings fall below the required level, exchanges must immediately report to the FSA. This effectively establishes a reserve-like requirement and is another form of asset segregation.

Figure 2: Customer Asset Isolation and Custody (Platform/Custody Institution)

legal jurisdiction	Clear requirement for separation of customer assets from self owned assets	Other key points
European Union (EU)	Article 75 of MiCA: Customers' encrypted assets must be legally and operationally isolated from their own assets; Customer rights should be protected	Regular reconciliation, custody policy, liability for loss compensation, and secondary custody only for authorized CASPs.
United Kingdom (UK)	The payment system and custody requirements supported by stablecoins will be refined in accordance with BoE/FCA rules	At present, the applicability of pure encrypted custody that is not included in the regulated scope is limited, and it needs to be evaluated based on specific licenses and business boundaries.
Singapore (SG)	DPT service providers must isolate customer assets in trust, separate on chain addresses, maintain ⩾ 90% cold storage, perform daily reconciliation and information disclosure (guidelines)	Restricting lending/pledging to retail customers; Establish independent custody functions and risk control processes.
United States (US)	The issuer and custodian requirements are parallel to state/federal requirements: New York has clear separation/audit requirements for stablecoins and custodians; Securities assets are subject to the SEC/CFTC framework	There is no unified federal "encrypted version CASS" at the platform level, and applicable state laws, federal disclosure, and prudence obligations must be followed.
Hong Kong (HK)	Under the guidance of VATP, customers are required to strictly manage their assets, maintain a ratio of hot and cold wallets, arrange third-party custody, and perform daily reconciliation	The detailed requirements shall be subject to the licensing conditions, business scope, and audit arrangements.

Source: Pharos Research

Overall, client asset segregation has become a common regulatory baseline across jurisdictions. In Europe, North America, and the Asia-Pacific region alike, regulators use statutes and administrative guidance to require crypto-asset trading platforms to provide independent custody and separate accounting for client assets, which may not be treated as company property or used for proprietary purposes.[25] Proper implementation of these requirements helps shield investors from misappropriation by insiders or dilution by other creditors, thereby strengthening market confidence. However, firms operating across multiple jurisdictions must pay attention to local nuances: some require third-party custodians, while others allow self-custody subject to minimum capital or insurance requirements, and so on. These differences are discussed further in subsequent chapters. In any case, “do not use client assets” has become a red line among red lines, and violations may trigger severe regulatory sanctions or even criminal liability.

03 / Consensus Red Lines on Market Manipulation and Conflicts of Interest

This chapter discusses two baselines relating to market fairness: prohibitions on market manipulation and requirements for managing conflicts of interest.

3.1 Market manipulation: market integrity and manipulation prevention

The high volatility of crypto-asset markets and the relative absence of traditional market infrastructure make them vulnerable to manipulation, including wash trading, pump-and-dump schemes, insider trading, and other forms of market abuse. If manipulation is allowed to proliferate, it not only harms investors but also undermines price discovery and public confidence in crypto markets. Accordingly, regulators in major jurisdictions treat the fight against market manipulation and insider trading as a red line, requiring trading platforms and intermediaries to monitor and prevent suspicious activity, and to report suspected manipulation to regulators where appropriate, in order to maintain fair and orderly markets.[4] In many jurisdictions, serious market-manipulation offenses are criminalized and subject to penalties similar to those in traditional markets.

In the United States, the legal framework for combating manipulation in securities and derivatives markets is relatively well developed. For digital tokens classified as securities, Section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5 prohibit market manipulation and securities fraud, and insider trading is prohibited and punishable under federal securities laws and case law. For digital assets treated as commodities (such as Bitcoin and Ether, as recognized by U.S. regulators), the Commodity Exchange Act (CEA) grants the Commodity Futures Trading Commission (CFTC) authority over manipulation in derivatives markets and enforcement power against fraud and manipulation in spot commodity markets. In recent years, U.S. authorities have increasingly invoked these laws to target misconduct in crypto markets. For example, in 2021, the U.S. Department of Justice brought what is widely regarded as the first crypto-related insider trading case against an employee of a major exchange, alleging that he purchased tokens in advance of listing announcements and profited from the subsequent price increases. The SEC brought parallel civil charges, taking the position that the tokens in question were securities. This was the first “insider trading” enforcement action in the crypto space and demonstrates that the U.S. will not relax enforcement merely because an asset takes a novel form. In another case, the CFTC sued executives of a crypto trading platform, alleging that they knowingly allowed wash trading to inflate reported volumes and mislead the market, and invoked anti-manipulation provisions of the CEA. Although the United States has not enacted crypto-specific spot-market manipulation legislation, regulators are making active use of existing securities, commodities, and anti-fraud laws. State attorneys general have also relied on broad antifraud authorities, such as New York’s Martin Act, to investigate exchanges suspected of inflating trading volumes (for example, the NYAG’s 2018 report on virtual market integrity). Overall, the U.S. emphasizes a “technology-neutral” approach: manipulative conduct that would be illegal in traditional securities or commodities markets is likewise illegal when carried out with digital assets.

In the European Union, the Market Abuse Regulation (MAR) provides a comprehensive framework against insider dealing and market manipulation in traditional securities markets, but it primarily applies to financial instruments traded on regulated markets and thus does not directly cover most crypto assets. MiCA seeks to fill this gap by introducing market integrity obligations specific to crypto assets. Article 80 of MiCA and related provisions prohibit any person professionally involved in

crypto trading from using inside information or engaging in manipulation, and they require CASPs operating trading platforms to establish systems capable of detecting and addressing market-abuse behavior.[4] Specific measures include transaction-surveillance algorithms to detect abnormal large orders, frequent order submissions and cancellations, and other suspicious patterns; mechanisms to maintain orderly trading during extreme price swings; and thresholds for price movements or volumes that trigger automatic order rejections. CASPs must also report suspected manipulation or insider trading to competent authorities. In addition, MiCA requires continuous public disclosure of order book data and trading information to enhance market transparency and reduce scope for opaque practices. These provisions effectively transplant EU experience from securities markets to crypto-asset trading under the principle of "same business, same risks, same rules." As MiCA takes effect, national regulators (such as the AMF in France and BaFin in Germany) will gain clear mandates to address manipulation in crypto markets. For example, if an individual orchestrates a pump-and-dump scheme through a Telegram group, that behavior may be deemed market manipulation and sanctioned under MiCA. In parallel, the EU's new AMLR, expected to be implemented by 2027, will prohibit privacy coins and anonymous crypto accounts (see below), which also contributes to market integrity by limiting opaque trading channels.[12]

In Hong Kong, the SFC requires licensed virtual asset trading platforms to establish market surveillance teams or systems capable of real-time monitoring for abnormal trading. The SFC's guidelines call on platforms to identify and prevent manipulative trading, including wash trades between related accounts and abusive order placement and cancellation, and to maintain logs for regulatory review. If a platform detects serious suspected manipulation, it must report to the SFC and law-enforcement agencies. Although most crypto assets are not classified as "securities" under Hong Kong's Securities and Futures Ordinance (SFO)—and thus are not directly subject to statutory market-manipulation offenses—licensed platforms are nonetheless obligated by their licensing conditions to ensure fair markets. This is an example of using licensing to achieve regulatory objectives. In Singapore, MAS applies the Securities and Futures Act (SFA) market-abuse regime to digital tokens that are classified as securities or derivatives and traded on regulated markets. However, for pure crypto assets that fall outside the SFA, Singapore currently relies primarily on industry guidance and self-discipline, while MAS repeatedly issues investor alerts warning of manipulation risks in crypto markets. As of 2025, Singapore is considering amendments to extend certain market-conduct rules to crypto assets of significant public interest, such as prohibitions on disseminating false or misleading information to influence token prices.

To support regulators and platforms in fulfilling their surveillance obligations, specialized blockchain analytics and market-surveillance solutions are increasingly being deployed. Some exchanges use on-chain analytics to monitor patterns of fund movements among related addresses and detect potential collusive schemes; others deploy AI models that identify abnormal price patterns or order-book behavior. Regulators are also relying more heavily on these tools. The SEC has established a dedicated crypto-asset enforcement unit that uses big-data analytics to examine exchange trading records and identify abnormal volatility. ESMA and national authorities in the EU have considered setting up consolidated trade repositories for crypto transactions to detect cross-market manipulation.

In summary, combating market manipulation and insider trading is a shared regulatory red line across jurisdictions, albeit with variations in enforcement tools and legal bases. As crypto markets become increasingly intertwined with traditional finance, regulators are likely to extend existing market-conduct frameworks to crypto activity. For example, the FSB's 2023 recommendations urge countries to ensure "effective regulation and oversight of crypto-asset markets to maintain market integrity," including adequate enforcement powers against manipulation and fraud.[14] This global guidance is expected to be translated into more explicit requirements within national legal systems, so that manipulation of crypto markets will carry legal consequences whether it occurs in New York,

London, or Singapore. For market participants, this trend means that more transparent and fair trading environments are on the way, which is a necessary condition for the long-term health of the industry.

3.2 Conflict-of-interest controls: business separation and internal governance

Managing conflicts of interest is a fundamental requirement for ensuring that financial institutions fulfil their fiduciary duties and protect client interests. In the crypto-asset trading sector, potential conflicts of interest include: platforms that both operate trading venues and engage in proprietary trading or control affiliated market makers, thus being able to profit from client order-flow information; platforms issuing their own tokens and listing them for trading, raising concerns about price support and information asymmetry; and executives or employees conducting personal trades with access to sensitive market information (insider trading), among others. If left unchecked, such conflicts can harm clients and market fairness, and in extreme cases trigger systemic risks—as seen in instances where exchanges collapsed due to related companies taking high-risk positions with client assets. Regulators therefore treat the prevention and management of conflicts of interest as a red line, requiring crypto-asset service providers to establish internal controls and governance arrangements to identify, mitigate, and disclose potential conflicts.

MiCA sets out explicit, mandatory conflict-of-interest rules for CASPs. Under Article 72,[28] CASPs must establish and maintain effective policies and procedures to identify, prevent, manage, and disclose conflicts of interest that may arise between (a) the CASP and its shareholders, directors, and employees; (b) different clients; or (c) different business functions carried out by the CASP or its affiliates. CASPs must review and update their conflict-of-interest policies at least annually and take all appropriate measures to address identified conflicts. They must also publicly disclose, typically on their websites, the nature and sources of conflicts and the steps taken to mitigate them, so that clients are adequately informed. CASPs operating trading platforms are subject to heightened expectations: they must adopt special procedures to avoid conflicts of interest between the platform and its clients in trading, such as limiting or prohibiting proprietary trading against clients, controlling interactions with affiliated market makers, and preventing staff from trading on non-public information. Regulatory technical standards will further specify disclosure formats and detailed requirements, illustrating the EU's view that conflicts of interest warrant strong regulatory intervention. One core motivation behind these rules is to avoid repeating the failures of exchanges that combined multiple roles and exploited clients, thereby ensuring that platforms cannot both "run the casino" and take bets against their own customers.

In traditional financial markets, the United States has long relied on structural rules and conduct standards to address conflicts of interest, such as separating exchange and broker-dealer functions and imposing firewalls for banks. In the crypto context, there is currently no statute that categorically prohibits exchanges from engaging in proprietary trading or vertically integrating multiple functions, but regulators have repeatedly expressed concerns. In a 2024 public statement, a CFTC commissioner pointed to FTX as an example of how vertically integrated structures—combining exchange, broker, market maker, and custodian roles without robust external oversight—can give rise to severe conflicts of interest and systemic risk. The commissioner called for rules limiting such vertical integration.[15] Although FTX was not fully regulated in the United States, its collapse prompted U.S. lawmakers and regulators to consider whether crypto exchanges should face rules similar to those in securities markets that require separation of trading, brokerage, and advisory functions. Draft bills such as the Digital Commodities Consumer Protection Act (DCCPA) contemplated restrictions on exchange activities that conflict with client interests—such as lending out customer assets and certain related-party transactions—but have not been enacted.

Meanwhile, regulators have used enforcement and supervisory tools to address conflicts of interest. The SEC, for instance, has raised concerns in enforcement actions and public statements about platforms whose executives sell tokens ahead of negative events, or whose in-house investment arms trade in tokens listed on the platform without proper disclosure. The SEC has suggested that such behavior can constitute conflicts of interest that harm investors. The Department of Justice has prosecuted staff of exchanges for trading on non-public listing information, while NYDFS requires BitLicensees to submit conflict-of-interest policies addressing restrictions on personal trading by directors and senior management and mitigation measures for multi-function business models. These actions indicate that, even absent a single omnibus rule like MiCA, conflicts of interest have become a focus of U.S. supervisory and enforcement practice in the crypto sector.

Hong Kong's SFC explicitly requires licensed platforms to avoid conflicts of interest. For example, platforms are prohibited from engaging in proprietary trading for their own accounts (i.e., they may not act as "dealers" against clients). Where affiliates of a platform group conduct market-making activities, the platform must notify the SFC and implement strict information barriers (Chinese walls) to prevent leakage of sensitive information. Executives and employees are subject to constraints on personal crypto trading, including pre-approval and periodic reporting. If a platform proposes to list tokens in which it has an interest (such as projects it has invested in or its own native token), the SFC may require enhanced disclosure or even refuse to approve the listing, in order to prevent platforms from "listing with one hand and dumping with the other." This approach mirrors conflict-of-interest controls in Hong Kong's securities markets, such as separating proprietary trading from agency brokerage. Since the first cohort of licenses was granted in 2023, licensed platforms have highlighted in their disclosures that they do not engage in proprietary trading or compete with clients for profits, as a signal of integrity.

International standard setters are also paying close attention. The FSB's July 2023 high-level recommendations emphasize that jurisdictions should ensure that merged multi-function crypto-asset service providers are subject to appropriate oversight, including requirements to manage conflicts of interest and, where necessary, separate certain functions.[26] IOSCO's 2022 consultation report makes similar recommendations, urging regulators to require disclosure of proprietary trading by exchanges, restrict inappropriate staff trading, and consider structural separation of functions such as trading and custody. Over time, these principles are likely to coalesce into more unified international standards under the "same risks, same functions, same rules" doctrine.

In short, conflict-of-interest management has become a basic regulatory expectation for the crypto industry. From MiCA's binding rules in the EU to licensing conditions in Hong Kong and Singapore, and to the U.S. regulators' statements and enforcement actions, the message is clear: intermediaries must build effective internal controls so that they do not exploit client information or positions for unfair gain, and must promptly disclose and address conflicts when they arise. Strengthening these controls is essential to restoring trust in the wake of high-profile scandals and steering the industry toward greater transparency and integrity. For firms, this implies greater investment in governance—appointing independent chief compliance officers, conducting regular conflict-of-interest risk assessments, and training staff on ethics and conduct standards—so as to meet regulatory expectations and safeguard their own reputations.

04 / Regulatory Divergence I: Different Paths for Stablecoin Regulation

Stablecoins—crypto tokens pegged to fiat currencies or other assets—have grown rapidly worldwide and attracted intense attention from regulators. On the one hand, stablecoins promise more efficient payments and greater financial inclusion; on the other, their widespread use may threaten financial stability and monetary sovereignty, especially when issuance is not fully backed or transparent, as illustrated by the collapse of the algorithmic stablecoin UST in 2022. Consequently, many jurisdictions are exploring regulatory frameworks for stablecoins. However, differences in legislative philosophy and financial systems have made stablecoin regulation one of the most contentious topics in cross-jurisdictional regulation. Key divergences concern who may issue stablecoins, reserve and capital requirements, investor-protection measures, and restrictions on use in payments and trading.

4.1 Licensing and caps for fiat-backed stablecoins

MiCA distinguishes between two types of stablecoins: “e-money tokens” (EMTs), which are pegged to a single fiat currency, and “asset-referenced tokens” (ARTs), which are backed by baskets of assets or non-fiat values. Both categories are subject to stringent licensing and supervision. EMT issuers must be authorized as credit institutions (banks) or electronic money institutions and may issue tokens only with regulatory approval. They must maintain reserves of high-quality liquid assets equal to the face value of tokens in circulation (primarily deposits in the referenced currency or high-grade government bonds) to ensure 1:1 redemption. MiCA also prohibits paying interest on EMT holdings to prevent competition with bank deposits.

Uniquely, to mitigate potential risks to monetary policy from foreign-currency stablecoins, MiCA introduces usage caps: for EMTs pegged to non-euro currencies (for example, U.S. dollar–denominated tokens such as USDT), daily transactions within the EU may not exceed EUR 200 million or 1 million transactions. If these thresholds are breached, the issuer must take measures to limit use, including, if necessary, suspending new issuance or redemptions. This “hard cap” (the EUR 200 million and 1 million transaction thresholds) is designed to prevent any single stablecoin from gaining excessive traction as a means of payment and displacing the euro. The regime has attracted significant industry attention.[16][27] In addition, issuers of “significant” EMTs and ARTs face stricter supervisory requirements, including more frequent reporting, tighter liquidity management, and enhanced reserve custody rules. MiCA’s stablecoin rules take effect ahead of other provisions—beginning in 2024, with a transition period—after which issuers must be fully compliant to operate within the EU.

By contrast, the United States still lacks a comprehensive federal statute dedicated to stablecoins, leaving a substantial regulatory gap. Congress has debated the issue for years. The President’s Working Group on Financial Markets recommended in 2021 that stablecoin issuance be restricted to insured depository institutions and called for legislation. Several bills—the Stablecoin Transparency and Protection Act, the Digital Commodity Exchange and Stablecoin Act, and others—have been introduced but remain stalled amid political disagreement. In the meantime, stablecoin issuers operate under a patchwork of existing rules: some, such as Paxos and Circle, issue tokens through state trust company charters and are overseen by state banking regulators; others, notably Tether, are headquartered offshore and largely outside direct U.S. oversight, though their banking relationships (and thus their reserves) are subject to some regulation. Federal agencies have intervened indirectly: the OCC has provided guidance on national banks’ ability to issue stablecoins

subject to prudential conditions, while the Federal Reserve and FDIC have warned banks about the risks of stablecoin-related reserve or settlement services.

At the state level, NYDFS has taken a leading role, approving and supervising several dollar stablecoins. Its 2022 guidance requires NYDFS-regulated issuers to maintain 100% reserves in cash and short-term U.S. Treasuries, support daily redemption at par, and undergo regular attestations. Wyoming has also explored innovative charters for digital-asset banks and stablecoin issuers, but no major projects have yet launched.[5] The absence of a uniform federal regime has produced a fragmented market: large issuers like Tether and Circle maintain voluntary high-reserve policies and publish attestations, while algorithmic stablecoins such as TerraUSD proliferated in regulatory grey areas until their collapse. This has prompted renewed legislative efforts, including a 2023 draft federal stablecoin bill that would create a federal licensing framework and grant the Federal Reserve certain oversight powers over non-bank stablecoin issuers. But the legislative outlook remains uncertain. In this transitional environment, U.S. regulators have relied on existing authorities: the SEC has challenged certain interest-bearing or investment-like stablecoin arrangements as securities, while the CFTC has asserted that major stablecoins are commodities and retains enforcement powers over fraud and manipulation.

Japan has adopted a comparatively conservative approach. In June 2022, the Diet passed amendments to the Payment Services Act and related laws, defining stablecoins as “electronic payment instruments” and sharply limiting who may issue them.[4][19] Under the new framework, only licensed banks, registered money transmission businesses with high capital requirements, or trust companies may issue stablecoins. This rules out most private companies (such as Tether) from legally issuing stablecoins in Japan. The law requires 100% backing in fiat deposits held at regulated institutions, and prohibits algorithmic stablecoins and other non-collateralized designs. The FSA has been cautious about allowing foreign stablecoins into the domestic market, and Japanese exchanges have so far refrained from listing major foreign stablecoins like USDT. Instead, trust banks and financial groups are piloting yen-pegged tokens such as “Progmat Coin.” Subsequent discussions have focused on further constraints—for example, requiring that only trust banks (and not ordinary banks) may issue stablecoins on public chains, and applying full KYC and Travel Rule obligations to stablecoin transfers. In practice, Japanese stablecoins are treated as close substitutes for bank deposits and are subject to similarly strict regulation.

Hong Kong’s Monetary Authority (HKMA) issued a discussion paper in 2022, making clear that algorithmic stablecoins would not be permitted and that regulation would initially focus on fiat-referenced payment stablecoins. A dedicated Stablecoin Ordinance (working title) was drafted and is scheduled to take effect in August 2025.[7] Under the Ordinance, any issuer of fiat-pegged stablecoins in Hong Kong must obtain a license from the HKMA. Applicants must establish a local presence, meet minimum capital requirements, and implement robust risk-management and technical controls. Issuers must maintain 100% reserve assets (limited to high-quality liquid assets) and redeem stablecoins at par on demand. The HKMA is empowered to inspect and supervise issuers, including reviewing reserve composition and governance. Unlike Japan’s bank-only model, Hong Kong does not restrict issuance exclusively to banks, but it subjects non-bank issuers to bank-like prudential oversight. The first batch of licenses is expected to be granted between 2024 and 2025, with a “start small and scale gradually” approach. Importantly, Hong Kong’s framework brings stablecoin issuers and distributors within the AML/CFT regime, requiring KYC and Travel Rule compliance. This positions Hong Kong as a regional benchmark for stablecoin regulation and offers a clear licensing pathway for fintech firms that wish to issue or distribute stablecoins on a fully regulated basis.

4.2 Capital and reserve requirements for non-fiat-backed stablecoins (asset-referenced tokens)

Beyond single-fiat stablecoins, some projects back their tokens with baskets of fiat currencies, commodities, or crypto assets, or rely on algorithmic and over-collateralized mechanisms to stabilize value. These are often categorized as ARTs. Such designs are more complex and carry greater risks. After the controversial Libra (later Diem) project, which proposed a basket-backed global stablecoin, regulators expressed concerns that such tokens could threaten monetary sovereignty and financial stability.

MiCA brings ARTs into its regulatory perimeter, subjecting them to licensing and disclosure requirements similar to those for EMTs, but with stricter conditions. ART issuers must hold higher minimum capital (at least EUR 350,000 or 2% of reserves, whichever is greater), reflecting the additional risks, and must maintain fully segregated reserve assets that are legally and operationally distinct from the issuer's own assets. Reserves may be held by qualified custodians (such as authorized CASP custodians or banks) and must be diversified to reduce concentration risk. Issuers must implement periodic audits and disclose reserve composition at least quarterly. For "significant" ARTs, regulators may impose further obligations, such as constraints on size or detailed stress-testing. MiCA also prohibits paying interest or other financial incentives to ART holders, to prevent ARTs from becoming investment products in disguise. Overall, MiCA's regime for ARTs covers governance, risk management, and user protection in a comprehensive manner.

The United States, by contrast, has no dedicated legal framework for basket-backed or algorithmic stablecoins. In the wake of the Libra controversy, multiple agencies signalled that a project of that scale would likely be treated as systemically important and subject to stringent regulation. If an ART is backed by securities, the SEC might treat it as an exchange-traded fund (ETF) share and require registration; if it is used for large-value payments, the Financial Stability Oversight Council (FSOC) might designate its issuer as a systemically important institution subject to Federal Reserve oversight. Nonetheless, because no major ART has fully launched in the U.S. market, these theories remain largely hypothetical. Meanwhile, enforcement actions against algorithmic stablecoins illustrate regulators' willingness to apply existing laws. For example, the SEC has scrutinized certain algorithmic stablecoin projects as unregistered securities offerings, and the CFTC has examined whether they are commodity-based derivatives. The overarching principle remains that novel structures do not escape existing securities and commodities laws.

Singapore consulted on stablecoin regulation in 2022, proposing rules for single-currency stablecoins backed by G10 currencies and setting minimum reserve quality requirements, but signalled limited appetite for multi-asset ARTs. MAS's view has been to first establish a robust regime for fiat-pegged single-currency stablecoins and then reassess more complex designs in light of international consensus. Hong Kong's draft Ordinance likewise focuses on fiat-referenced stablecoins and excludes algorithmic and commodity-backed tokens from the licensing scope. South Korea's Financial Services Commission has indicated a sceptical stance toward algorithmic stablecoins and instruments promising high yields, discouraging such products on domestic exchanges. Japan's bank/trust-only model leaves effectively no room for ARTs. As a result, while MiCA provides a comprehensive framework for ARTs, most other jurisdictions are more restrictive or cautious.

For stablecoin businesses seeking global expansion, this divergence translates into very different compliance obligations. Within the EU, issuers must obtain licenses and comply with usage caps and reserve rules; in the United States, they face uncertainty from fragmented state and federal oversight as well as potential enforcement; in Japan and Hong Kong, they must contend with stringent licensing conditions or outright restrictions on certain designs. Bridging these differences is

likely to be one of the central challenges in future international regulatory coordination on stablecoins.

05 / Regulatory Divergence II: Market Access and Innovation Boundaries

This chapter examines three additional areas of significant cross-jurisdictional divergence: regulation of crypto-derivatives, the legal status of privacy coins, and emerging approaches to RWA tokenization and DeFi. These domains implicate investor protection, criminal law enforcement, technological anonymity, and the boundaries of financial innovation. As such, they have prompted divergent regulatory strategies and no widely accepted international standards have yet emerged.

5.1 Market access and investor protection for crypto-derivatives

Crypto-derivatives are contracts referencing the price of crypto assets, such as futures, options, and contracts for difference (CFDs). They can be used for hedging and speculation and can magnify both gains and losses. High leverage and volatility make them especially dangerous for retail investors. Traditional derivatives markets are subject to strict licensing and infrastructure requirements, yet many crypto-derivatives platforms have historically operated from offshore jurisdictions without licenses, targeting users worldwide. Regulators have responded differently: some jurisdictions permit such trading under supervision, others limit retail access, and some prohibit it altogether.

As noted above, the United States treats Bitcoin, Ether, and certain other assets as commodities and regulates their derivatives under the CEA, with the CFTC as the primary regulator. Any platform offering crypto-derivatives to U.S. persons must register as a designated contract market (DCM) or swap execution facility (SEF), and intermediaries must register as futures commission merchants (FCMs) and comply with client asset protection and reporting rules. Only a small number of regulated venues, such as the CME, have listed crypto futures, primarily targeting institutional and professional investors. Most U.S. retail traders have instead turned to unregistered offshore platforms such as BitMEX and Binance, which is unlawful under U.S. law. The CFTC and other agencies have taken aggressive enforcement actions against such platforms, including the BitMEX and Binance cases mentioned above, alleging unregistered derivatives offerings and AML violations. The United States also restricts retail access to certain complex derivatives: the SEC and CFTC have both expressed concern about retail participation in leveraged swaps and have not permitted retail marketing of crypto-linked CFDs.

The UK's FCA, after assessing the risks of crypto-derivatives for consumers, announced in October 2020 a ban on the sale, marketing, and distribution of derivatives and ETNs referencing unregulated crypto assets to retail clients, effective January 2021.[6][8] This ban covers CFDs, futures, options, and ETNs referencing crypto assets. At the time, it was a global first. The FCA concluded that due to extreme volatility, lack of reliable valuation, prevalence of market abuse, and retail investors' limited understanding, such products were "ill-suited" to retail consumers. The ban was projected to save UK retail investors around GBP 53 million annually in losses.[6] In October 2025, however, with a view to enhancing the UK's competitiveness as a digital-asset hub, the FCA lifted the retail ban on certain crypto ETNs while maintaining the ban on CFDs and other high-leverage derivatives.[18] Thus, retail investors in the UK can now access some regulated exchange-traded products referencing crypto, but not leveraged OTC derivatives. This policy evolution illustrates an attempt to balance investor protection with market development. For now, UK retail investors cannot trade crypto futures and options on locally regulated platforms but can invest in carefully structured ETNs.

In the EU, MiCA does not directly cover derivatives, as it focuses on spot markets and primary issuance. However, many Member States treat crypto-derivatives as financial instruments subject to

MiFID II, requiring firms providing such services to hold investment firm licenses and comply with conduct-of-business rules. ESMA has included crypto-CFDs in its product intervention measures, imposing maximum leverage limits (e.g., 2:1 for crypto CFDs, lower than for FX) to protect investors. Some Member States briefly considered or implemented retail bans on crypto-derivatives, but the EU has not adopted a union-wide prohibition akin to the UK's. Instead, regulated brokers in countries such as Cyprus can offer crypto-CFDs under leverage and risk disclosure constraints. As EU financial regulations evolve, dedicated rules for crypto-derivatives may emerge, but for now the general framework for financial derivatives applies.

Asian jurisdictions have taken diverse approaches. Japan's 2019 amendments to the Financial Instruments and Exchange Act brought crypto-derivatives within the definition of financial instruments, requiring registration for providers and imposing leverage limits that were gradually reduced to 2:1. Thus, Japanese investors can trade low-leverage crypto margin products, but the market remains relatively small. South Korea prohibits domestic exchanges from offering any crypto-derivatives to residents and has pressured banks to restrict remittances to foreign derivatives platforms. Hong Kong's licensing regime for virtual asset trading platforms currently does not permit retail access to crypto-derivatives; only spot trading is allowed for retail, and derivatives may be offered to professional clients under tight conditions and primarily via traditional licensed intermediaries. Hong Kong and Singapore have allowed certain crypto-linked ETFs or structured products on regulated exchanges for public investors, but generally restrict retail participation in leveraged derivatives. MAS has also tightened marketing rules, banning promotion of high-risk digital payment token services to the general public and restricting access to derivatives-based products to institutional and accredited investors.

Figure 3: Retail Accessibility and Derivatives Red Line

legal jurisdiction	Retail spot trading	Retail derivatives (leverage/contracts/ETN)
European Union (EU)	The CASP licensing framework specification under MiCA	Constrained by MiFID/EMIR; Member states generally impose strict requirements on retail leveraged products, requiring investment service licenses and investor protection measures.
United Kingdom (UK)	Constrained by AML, gold promotion and other rules	FCA PS20/10 prohibits the sale of encrypted derivatives to retail; The rules regarding encrypted ETN will be evaluated and adjusted in subsequent policies.
Singapore (SG)	Constrained by PSA and DPT guidelines	The provision of leverage/credit, pledge and other activities for retail is significantly restricted; Strictly manage based on the principle of investor protection.
United States (US)	Subject to state/federal law enforcement and disclosure constraints	Only through compliant markets regulated by CFTC (such as regulated futures exchanges); Strict enforcement of retail derivatives provided by unregistered platforms.
Hong Kong, China (HK)	SFC VATP conditionally opens to retail	At present, VATP is not allowed to provide derivatives, margin or lending services to retail.

Source: Pharos Research

These divergent approaches have contributed to regulatory arbitrage and concentration of global derivatives liquidity in loosely regulated jurisdictions. In countries with strict bans or tight controls (such as the U.S., UK, Hong Kong, and South Korea), many users continue to access high-leverage offshore platforms via VPNs and foreign accounts, hampering enforcement. This in turn leads to risk concentration and vulnerability to platform failures. International bodies such as the FSB and IOSCO have called for stronger cross-border cooperation, including information sharing on unlicensed platforms and joint enforcement actions. Over time, a broad consensus appears to be emerging:

high-leverage derivatives are generally unsuitable for retail investors and should be tightly restricted, while limited derivatives activity may be permitted for institutional or professional investors under robust regulatory safeguards. The UK's partial reversal of its ETN ban exemplifies a nuanced approach that may influence other jurisdictions.

5.2 The legal status and regulatory challenges of privacy coins

Privacy coins are cryptocurrencies that use advanced cryptographic techniques (such as ring signatures or zero-knowledge proofs) to obfuscate transaction details and addresses, examples being Monero (XMR), Zcash (ZEC), and Dash (DASH). Proponents argue that privacy coins protect financial privacy, while regulators worry that they facilitate money laundering, sanctions evasion, and other illicit activities because conventional blockchain analytics tools cannot easily trace them.[7] Regulatory responses vary widely: some jurisdictions ban privacy coins outright, others severely restrict their circulation through AML rules, and a few have taken no formal action but have nonetheless seen privacy coins marginalized in regulated markets.

Japan was among the first countries to effectively prohibit privacy coin trading. Following incidents such as the Coincheck hack, in which hackers allegedly used anonymous coins to launder stolen assets, the FSA directed domestic exchanges to delist high-anonymity coins including Monero and Dash. The self-regulatory body JVCEA implemented these directives, and new licenses are not granted to exchanges seeking to list such coins. FSA officials emphasized that privacy coins are inconsistent with Japan's AML requirement of transaction traceability and thus have no place in compliant markets. Similarly, after amendments to the Act on Reporting and Use of Certain Financial Transaction Information (the "Special Act") in 2021, South Korea's FSC barred VASPs from dealing with digital assets for which transaction records cannot be identified, leading local exchanges to delist privacy coins.[10] South Korea also prohibits mixing services that are designed to obscure transaction origins. Dubai's 2023 virtual asset regulations likewise ban the issuance and trading of anonymity-enhanced cryptocurrencies. These jurisdictions have effectively opted for outright prohibition, viewing the risks as outweighing any privacy benefits.

The EU has not yet enforced an immediate ban, but it is moving in that direction. The politically agreed AMLR package includes provisions to ban crypto services involving anonymous accounts and privacy coins by 2027.[8][20] According to information published in May 2025, VASPs operating in the EU will not be allowed to offer services involving privacy coins from July 2027 onward, and they will face strict identification requirements for transactions with self-hosted wallets above EUR 1,000. Some Member States are already tightening supervision ahead of the EU-wide ban: Belgian and French regulators, for instance, have discouraged exchanges from listing privacy coins and flagged such assets as high-risk for AML purposes. Europol has repeatedly highlighted the challenge privacy coins pose to tracing illicit funds. While some in the crypto industry criticize these moves as encroachments on privacy rights, EU policymakers have prioritized the integrity of AML/CFT frameworks.

The United States has not banned holding or trading privacy coins per se, but most major compliant exchanges (such as Coinbase) do not list them, largely because of perceived AML/CFT risks and the difficulty of satisfying compliance expectations. U.S. authorities have instead focused on anonymity-enhancing services. In 2022, OFAC sanctioned the Tornado Cash mixing protocol, sending a strong signal that fully anonymous channels are unacceptable when used at scale for illicit purposes. This enforcement action, although distinct from privacy coins, has led many to speculate that the U.S. could take similar actions against specific privacy coin ecosystems or addresses linked to illicit activity. Meanwhile, the DOJ and IRS have invested in tools to analyze privacy coin transactions, though technical limitations remain. Exchanges such as Kraken and ShapeShift have delisted privacy coins from their U.S. platforms, citing regulatory and banking-relations concerns.

Singapore likewise has no explicit statutory ban, but MAS's AML guidelines require VASPs to treat anonymity-enhanced transactions as high-risk and subject them to enhanced scrutiny, effectively making it difficult for licensed entities to support privacy coins. Australia and other jurisdictions are considering EU-style rules that severely limit or prohibit fiat on- and off-ramps for privacy coins.[21]

The regulatory debate around privacy coins crystallizes the tension between financial privacy and AML/CFT requirements. On one side, strong financial privacy is an important civil liberty, and pervasive surveillance may be seen as overreach; on the other, completely untraceable assets pose serious risks to law enforcement and financial integrity. Some have proposed technological compromises—such as "view keys" that allow authorized parties to inspect transaction histories—but mature, widely accepted solutions have yet to emerge. For now, most regulators appear willing to sacrifice the mainstream viability of privacy coins to preserve the effectiveness of AML/CFT systems. FATF has identified anonymity-enhancing features as a key risk factor in its evaluations, and compliant institutions are increasingly reluctant to touch privacy coins. As more major economies move toward bans or quasi-bans, the regulatory divergence in this area is actually narrowing, but largely in the direction of greater restriction. Privacy coins are likely to remain confined to niche communities and unregulated venues, and users and businesses will face significant jurisdictional compliance risks if they engage with them.

5.3 Regulatory exploration of real-world asset tokenization (RWA) and DeFi

RWA tokenization refers to representing real-world assets—such as bonds, equities, real estate, or commodities—on distributed ledgers in token form. DeFi encompasses decentralized applications that use smart contracts to provide financial services such as trading, lending, and derivatives. Both are seen as frontiers of blockchain-based financial innovation, with potential benefits in terms of efficiency and financial inclusion, but they also challenge existing regulatory frameworks. How to bring these decentralized or cross-boundary models under supervision is one of the most complex and rapidly evolving issues in crypto regulation.

The United States has adopted a primarily enforcement-driven, "existing law first" approach to RWA and DeFi. For RWA, the SEC treats tokenized securities as securities in all respects, requiring registration or exemptions for issuance and compliance with securities laws in secondary trading. In several cases between 2018 and 2020, tokenized stock or bond offerings were halted or sanctioned as unregistered securities. Even when tokens represent interests in physical assets such as real estate or gold, SEC applies the Howey test; if investors contribute capital with an expectation of profit from the efforts of others, the tokens are likely to be deemed securities. Similarly, the CFTC has taken action against DeFi protocols that facilitate commodity swaps or leveraged trading without registration. The 2022 Ooki DAO case marked the first enforcement action against a DAO, with the CFTC alleging that the protocol operated an unregistered leveraged trading platform; the court entered a default judgment and penalties against the DAO. The U.S. Treasury's 2023 assessment of illicit finance risks in DeFi highlighted numerous instances in which DeFi services failed to implement BSA obligations and signalled that authorities would seek to bring such services into the AML framework.[23]

At the same time, there are calls within the U.S. for regulatory innovation and safe harbours. Some states, such as Wyoming, have passed laws recognizing DAOs as legal entities, potentially providing a path for compliant DeFi projects to assume legal responsibility and interact with regulators. However, absent federal reforms, DeFi projects remain exposed to considerable legal uncertainty, and some have chosen to relocate or limit access by U.S. users. U.S. authorities have exercised long-arm jurisdiction over offshore DeFi projects in certain cases, particularly where U.S. investors or

financial institutions are involved, underscoring that decentralization does not guarantee regulatory immunity.

The EU deliberately left fully decentralized activities outside MiCA's immediate scope, recognizing that it would be difficult to regulate protocols with no identifiable central operator. Instead, the European Commission commissioned research and public consultations on DeFi, exploring concepts such as "embedded supervision," where regulatory nodes would directly read on-chain data for compliance and monitoring purposes.[22] This approach, advocated by the BIS and some national regulators, aims to make smart contracts themselves a source of regulatory data rather than relying solely on centralized intermediaries. In parallel, the EU introduced a pilot regime for market infrastructures based on distributed ledger technology (Regulation (EU) 2022/858), allowing regulated institutions to operate tokenized securities trading and settlement systems within a sandbox framework.[25] Several exchanges and central banks have joined this pilot, experimenting with tokenized bonds, fund shares, and other RWAs. The goal is to assess legal and operational challenges and inform future permanent legislation. The EU is therefore relatively open to RWA innovation under controlled conditions, while remaining cautious about permissionless DeFi.

Singapore has adopted a forward-looking but controlled approach. MAS's Project Guardian, launched in 2022, brings together major financial institutions to pilot the use of DeFi protocols for wholesale financial markets, including tokenized bonds and interbank lending. In 2023, DBS and other banks successfully completed tokenized government bond transactions using DeFi-based automated market-making mechanisms, under MAS supervision. Singapore also operates a regulatory sandbox that allows DeFi startups to test products with limited waivers under close oversight. Nevertheless, MAS maintains that if a DeFi protocol provides regulated services, such as operating a market or facilitating securities lending, the responsible parties must hold appropriate licenses under the SFA, regardless of the technology used. Hong Kong has shown growing interest in DeFi as well: the HKMA's e-HKD pilots include DeFi payment experiments, and SFC officials have signalled openness to exploring DeFi governance models, particularly for institutional applications, while keeping a cautious stance on retail access. Mainland China, by contrast, maintains stringent bans on public crypto trading and DeFi, but has experimented with consortium chains and enterprise-grade "open permissioned blockchains" in initiatives such as the BSN, exploring digitalization of assets within permissioned networks.

Given the cross-border nature of DeFi and RWA tokenization, international bodies have begun to formulate principles. The FSB's 2023 report on DeFi warns that many DeFi activities are highly interconnected with traditional finance and often exhibit de facto centralization, arguing that they should be brought within the scope of existing regulatory frameworks.[22] IOSCO's 2023 policy recommendations for crypto-asset markets extend certain principles to DeFi, emphasizing functional equivalence: activities that are economically similar to regulated securities or derivatives services should be subject to comparable rules, irrespective of whether they are delivered through centralized or decentralized means. Future regulatory innovations may include legal recognition of DAOs, requirements for "compliance agents" who interface with DeFi protocols, and technical standards for embedding compliance checks and supervisory access into smart contracts.

At present, however, regulatory experimentation in RWA and DeFi remains diverse. The United States relies heavily on enforcement, the EU combines sandbox regimes with conceptual work on embedded supervision, and Asian hubs such as Singapore and Hong Kong pursue controlled pilots. These differences reflect varying attitudes toward innovation and risk, as well as differences in legal systems and market structures. Over time, feedback from pilot programs and enforcement cases is likely to inform a more convergent international framework—for example, broad agreement that RWA tokenization is welcome provided it meets existing investor-protection and custody standards, and that DeFi protocols with identifiable controlling parties must comply with AML and market-

conduct rules. Truly decentralized, ownerless protocols pose more difficult questions, and regulators may respond by focusing on access points such as front-end interfaces and fiat on- and off-ramps.

For market participants, jurisdiction selection and licensing strategy are crucial. In RWA, firms must choose regulatory environments that accommodate tokenized instruments, such as the EU's DLT pilot regime or MAS's sandbox, and secure appropriate licenses. In DeFi, projects seeking to operate compliantly may need to establish legal entities, appoint responsible persons, and build compliance interfaces into their code. Continuous monitoring of global regulatory developments is essential, as changes can materially affect the viability of different business models.

06 / The Meaning of Regulatory Convergence and the Institutional Implications of Divergence

The foregoing comparative analysis reveals a regulatory landscape in which “converging foundational principles” coexist with “divergent regime choices.”

On the one hand, major jurisdictions are increasingly aligned on core risk-control principles and are building a de facto set of baseline “red lines”: KYC/AML, client asset segregation, market-manipulation prohibitions, and conflict-of-interest management have become standard features of crypto regulation. This convergence is driven by the work of international standard setters such as FATF, the FSB, and IOSCO, and by collective lessons from a series of market failures and scandals. For instance, FATF standards have spurred widespread upgrades of national AML laws, making “anonymous, no-KYC” crypto trading models increasingly untenable.[1] High-profile exchange collapses have led regulators to strengthen client asset-protection rules across jurisdictions (as reflected in MiCA, NYDFS guidance, and SFC requirements).[10][11][25] Repeated enforcement actions against manipulation and insider trading have reinforced awareness of the importance of market integrity.[4] The catastrophic impact of conflicts of interest—epitomized by the FTX case—has prompted regulators to plug institutional gaps and tighten structural and governance requirements.[5][13][15]

These trends reflect the gradual incorporation of crypto-asset activities into mainstream financial regulation: regulators are adapting the mature toolkits of securities, derivatives, and banking supervision to the crypto domain under the principle of “same business, same risks, same regulation.” For cross-border crypto firms, this convergence is, on balance, positive: more consistent regulatory expectations reduce compliance uncertainty and lower friction costs in multi-jurisdictional operations. As KYC, AML, and anti-fraud requirements become universal, compliant firms can design global processes to meet high standards rather than juggling conflicting obligations. At the same time, rising baseline requirements raise entry thresholds: business models premised on anonymity or lax asset protection (such as unlicensed anonymous exchanges or platforms that commingle client assets) will find it increasingly difficult to survive, leading to a cleaner market environment and better investor protection.

On the other hand, substantial divergence remains in regulatory choices on specific instruments and emerging topics. Stablecoins, derivatives, privacy coins, RWA tokenization, and DeFi illustrate how legal traditions, risk tolerance, and policy priorities differ. The EU has opted for a comprehensive, precautionary legislative approach (MiCA’s full coverage of stablecoins and CASPs and proactive constraints on stablecoin scale), while the United States has relied more on incremental enforcement and administrative guidance in the absence of comprehensive legislation. The UK has taken an interventionist approach to retail derivatives, while continental Europe has leaned toward risk-based regulation under MiFID II. In Asia, some jurisdictions are very conservative (Japan and Korea banning privacy coins and restricting retail access to derivatives), while others are more open to experimentation (Singapore’s and Switzerland’s tokenization and DeFi pilots). These differences reflect deeper variations in financial structure, legal philosophy, and the weight assigned to innovation versus stability. In areas such as DeFi, where uncertainty is particularly high, a period of experimentation and divergence is likely to continue.

For crypto businesses, regulatory divergence presents both opportunities for regulatory arbitrage and significant risk. Historically, some firms have exploited differences by establishing operations in permissive jurisdictions while targeting users in stricter ones. However, as baseline red lines are

reinforced and cross-border cooperation intensifies, the room for such strategies is shrinking. As illustrated by the BitMEX and Binance cases, unlicensed platforms targeting users in major jurisdictions can face enforcement actions regardless of their nominal place of incorporation. Similarly, even if privacy coins remain legal in some countries, bans and restrictions in major markets severely impair their global liquidity and value. “Regulatory weakest-link” effects are also emerging: risky activities tend to migrate to regulatory havens, which can attract heightened scrutiny and pressure from abroad. The FSB has warned that jurisdictions that become havens for noncompliant activity may ultimately suffer reputational damage and face greater domestic and international risks.[14][22]

From an institutional perspective, the areas of convergence demonstrate the enduring relevance of traditional regulatory logic. KYC/AML mechanisms developed in banking continue to be effective in curbing illicit crypto flows;[1] market-surveillance techniques from securities and derivatives markets can be adapted to detect abusive trading in crypto markets.[4] This confirms that the underlying economic risks of financial activities are often technology-neutral, and that regulatory experience can be transplanted across sectors. At the same time, areas of divergence highlight the limits of existing frameworks. When innovations transcend core assumptions of traditional regulation—such as the presence of identifiable intermediaries or clear jurisdictional boundaries—existing tools become less adequate. Global stablecoins and fully decentralized DeFi protocols pose precisely such challenges. Addressing them may require new forms of international cooperation and regulatory technology, including frameworks for global stablecoins, recognition regimes for DAOs, cross-border sandboxes, and technical standards for embedded supervision.

From the vantage point of international coordination, the emerging consensus on baseline red lines lays a foundation for mutual recognition and cooperation. FATF standards enable mutual evaluations and risk-based information exchange on VASPs; convergent client asset-protection principles could support cross-border arrangements for returning client assets in insolvency; and common approaches to market manipulation facilitate cross-border data sharing and joint investigations. The FSB has floated the idea of a global monitoring framework for crypto-asset risks, which would depend on such convergence.[14][22][24] For cross-border firms, a plausible future operating model is to obtain licenses in multiple major jurisdictions, adhere to similar high standards, and benefit from regulatory equivalence or mutual recognition to reduce duplicative compliance costs. As regulatory convergence deepens, such models may become more feasible, creating a fairer competitive environment for compliant players versus noncompliant ones.

In short, today’s crypto-asset regulatory landscape is one of converging foundational rules combined with divergent approaches to frontier issues. This reflects both the proactive extension of traditional regulatory systems to new financial phenomena and the experimentation inherent in institutional innovation. Industry participants and regulators alike must navigate this environment with care: upholding baseline red lines to maintain market order and confidence, while allowing prudent experimentation to generate evidence for future reforms. In this sense, regulatory convergence and divergence are not simply a snapshot of the present; they form the starting point for the next stage of institutional evolution.

07 / Conclusion

As a frontier of 21st-century financial innovation, public-chain asset trading has experienced a decade of both explosive growth and tightening regulation. Globally, regulators have moved from initial uncertainty to gradually outlining shared red lines and norms, in a process of ongoing experimentation, error correction, and learning. Convergence in regulation has brought greater order and confidence to markets, while divergence reminds us that the interplay between law and innovation is continuous and that institutional evolution is never complete.

For crypto-asset institutions engaged in speculative or high-risk business models, understanding and respecting each jurisdiction's red lines is the basic prerequisite for compliant operation. For those pursuing sustainable cross-border strategies, carefully assessing the opportunities and risks created by regulatory divergence is a core strategic task. By presenting a cross-jurisdictional comparison, this article has sought to map the current regulatory landscape and provide material and inspiration for future policy and academic discussions.

Looking ahead, deeper international cooperation and advances in regulatory technology may gradually narrow some regulatory gaps and give rise to new institutional arrangements. Only through sustained dialogue and mutual adjustment between regulators and industry participants can a more mature balance be struck between financial stability and innovation. The convergence and divergence of regulatory red lines are a defining feature of the present moment, but they are also the point of departure for the future. With collective effort, it is possible to envision a global crypto-asset market that is both orderly and dynamic, where public-chain assets are integrated into a sustainable and robust financial system.

References

[1] Crypto KYC Requirements – Regulatory Standards for VASPs. https://blog.amlbot.com/crypto-kyc-requirements-in-2025-regulatory-standards-for-vasps/

[2] Regulation (EU) 2023/1114 (MiCA) on Markets in Crypto-assets. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

[3] Virtual Asset Trading Platforms Operators in Hong Kong. https://cpl.thalesgroup.com/compliance/apac/virtual-asset-trading-platforms-operators

[4] Japan Passes Legal Framework for Stablecoins. https://blockworks.co/news/japan-passes-legal-framework-for-stablecoins

[5] Global Crypto Laws in 2025: A Snapshot. https://boldergroup.com/news/global-crypto-laws-in-2025-a-snapshot/

[6] FCA bans the sale of crypto-derivatives to retail consumers. https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers

[7] What Are Privacy Coins And How To Investigate Them?. https://blockchaingroup.io/guides/what-are-privacy-coins-and-how-to-investigate-them/

[8] New EU regulation to track crypto transfers and ban privacy coins. https://dig.watch/updates/new-eu-regulation-to-track-crypto-transfers-and-ban-privacy-coins

[9] BitMEX fined $100 million by US judge for anti-money laundering violations. https://www.reuters.com/technology/us-says-bitmex-fined-100-million-violating-bank-secrecy-act-2025-01-15/

[10] NYDFS to Virtual Currency Asset Custodians: Segregate, Don’t Integrate. https://www.ballardspahr.com/insights/alerts-and-articles/2023/01/nydfs-to-virtual-currency-asset-custodians

[11] Circular to licensed virtual asset trading platform operators on ensuring the robust custody of client virtual assets. https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=25EC44

[12] SFC issues further guidance on custody of virtual assets for exchanges. https://www.kwm.com/hk/en/insights/latest-thinking/sfc-issues-further-guidance.html

[13] Despite polarizing FTX hearing, bipartisan support exists for crypto-regulation. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ftx-hearing-crypto-regulation/

[14] High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final report. https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/

[15] Statement of Commissioner Johnson: Dissenting Statement on Incomplete Conflicts of Interest Rules, Need for Vertical Integration Rules, and Equity Transfer Rules. https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement022024c

[16] MiCA Takes Effect: New EU Regulations Transforming Stablecoin Market. https://www.shiftmarkets.com/blog/mica-stablecoin-effect-june-2024

[17] Japan is wary of allowing banks to issue stablecoins, other than trust banks. https://www.ledgerinsights.com/japan-is-wary-of-allowing-banks-to-issue-stablecoins-other-than-trust-banks/

[18] UK digital asset market poised for 20% growth as FCA lifts four-year retail ban on crypto ETNs. https://www.theblock.co/post/373828/uk-digital-asset-market-poised-20-growth-fca-lifts-four-year-bancrypto-etns

[19] State of the Japanese Crypto Market. https://assets.ctfassets.net/m1hizt3hapq0/6D1gCPoxzTsHz0HPdKQKhD/899ac783aaf93e69ee85667282adbb60/State_of_the_Japanese_Crypto_Market.pdf

[20] EU to Enforce Crypto Ban on Anonymous Accounts and Privacy Coins by 2027. https://www.reddit.com/r/CryptoCurrency/comments/1keg11e/eu_to_enforce_crypto_ban_on_anonymous_accounts/

[21] Are Privacy Coins Still Viable Under Stricter Regulations In 2025?. https://flashift.app/blog/are-privacy-coins-still-viable-under-stricter-regulations-in-2025/

[22] FSB report on the financial stability risks of decentralised finance. https://www.regulationtomorrow.com/global/fsb-report-on-the-financial-stability-risks-of-decentralised-finance/

[23] U.S. Treasury Dept. Publishes Risk Assessment Addressing Illicit Finance Risks of DeFi. https://www.bakerlaw.com/insights/u-s-treasury-dept-publishes-risk-assessment-addressing-illicit-finance-risks-of-defi/

[24] Report on the proposal for a regulation of the European Parliament and of the Council (AMLA package). https://www.europarl.europa.eu/doceo/document/A-9-2023-0151_EN.html

[25] Tokenized securities and blockchain: Opportunities of the DLT Pilot Regime. https://www.dlapiper.com/insights/publications/2022/12/tokenized-securities-and-blockchain-opportunities-of-the-dlt-pilot-regime

[26] FSB reports on financial stability risks of DeFi and future work. https://content.next.westlaw.com/practical-law/document/I6104e651ada611ed8636e1a02dc72ff6/

[27] Tether's EU Future: Can USDT Weather the MiCA Storm, and What Should Crypto Businesses Do?. https://aurum.law/newsroom/Tethers-EU-Future

[28] Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-assets (MiCA). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

Contributors

Authors: Huiping Yang (Northwest University of Political Science and Law)

Reviewers: Colin Su, Grace Gui, NingNing, Owen Chen

Design: Alita Li

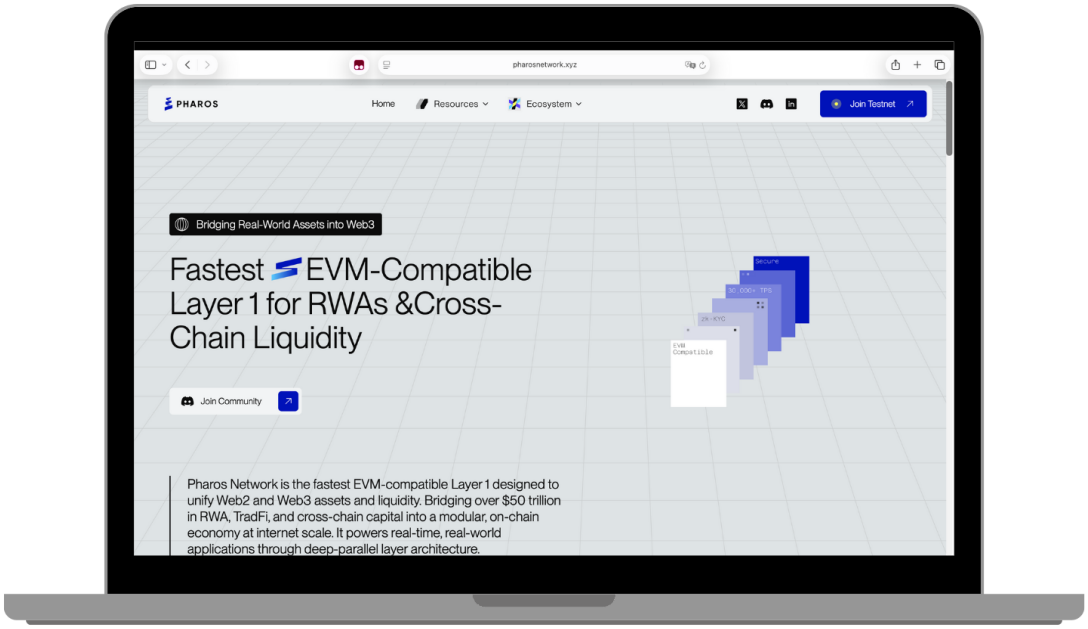
Disclaimer

This material is prepared by Pharos Research for the purpose of providing general information. It does not constitute and should not be deemed as investment, legal, accounting, or tax advice, nor does it form an offer, solicitation, or recommendation with respect to any securities, cryptographic assets, or strategies. The information and opinions contained herein may be derived from internal or third-party sources. While efforts are made to ensure their reliability, their accuracy, completeness, or timeliness is not guaranteed. Any decisions made and risks arising therefrom shall be borne solely by the reader. Past performance is not indicative of future results. This material may contain forward-looking statements (including forecasts and scenarios), which are subject to uncertainties and not guaranteed to be achieved. Cryptographic assets are highly volatile, and total loss may occur. They are also exposed to risks such as liquidity, technology, smart contract, counterparty, and compliance risks. To the extent permitted by law, the Research Institute and/or its affiliates or researchers may hold positions in the relevant assets, have business relationships with relevant entities, or otherwise have interests that may affect the objectivity of opinions. This material is not intended for persons in restricted jurisdictions. Reading, following, or subscribing to this material does not constitute a client relationship. Without prior written permission, no institution or individual may reproduce, copy, modify, or distribute this material. Any quotation shall be objective and complete, with the source clearly credited as "Pharos Research".

Contact

Pharos Network is a next-generation public blockchain for Real-World Assets (RWA) and stablecoins, focused on asset tokenization and on-chain circulation. We connect traditional institutions with the Web3 ecosystem, enrich the types of on-chain assets, expand revenue sources, and meet the allocation needs of a broader range of investors. Meanwhile, we help traditional enterprises unlock sustainable value on-chain through customized solutions. Boasting profound professional expertise and top-tier technical capabilities, our team builds a secure, efficient, and scalable infrastructure, providing institutions with a comprehensive decentralized ecosystem for onboarding assets onto the blockchain. We welcome strategic partners with a long-term perspective to co-build an open, compliant, and sustainable RWA ecosystem. For industry exchanges with us, please contact: chris@pharoslabs.xyz

Pharos' Official Website: https://www.pharosnetwork.xyz/



WeChat Official Account: Pharos Research

微信搜一搜

Pharos Research

PHAROS
RESEARCH

From RWA to On-Chain Finance.
Mapping Real-World Value.