BLOCKSEC

2026.01

Crypto Payment Compliance

Handbook

The industry's first comprehensive compliance guide for crypto payments

WWW.BLOCKSEC.COM

Acknowledgments

We are committed to building a secure and compliant blockchain ecosystem, which is our shared responsibility.

This manual is our latest approach to blockchain security, strictly adhering to regulatory frameworks and aligning with the latest regulatory policies and requirements. As a leading blockchain service provider, BlockSec is committed to serving clients who operate in compliance with regulations and are deeply engaged in legitimate businesses. We firmly support regulatory guidance.

We have established a partnership framework through the Interface and KYB/KYC, working with clients to proactively identify and respond to emerging security threats in the ecosystem. This is to ensure business stability and provide clients with cutting-edge security solutions.

We adhere to domain, protocol, and Web3 infrastructure-level risk management, conducting comprehensive risk assessments across all business operations, jointly building a secure ecosystem and ensuring the healthy development of the financial digital system.

BlockSec Team & Grandway Law Offices Web3 Team

Version History

Version 3.0 - October 2025:
New chapter added: "Crypto Payment Licenses," authored by Grandway Law Offices, comprehensively covering crypto payment license requirements and application processes across major jurisdictions in Europe, Asia, the Americas, Africa, and other regions; further improving the global compliance guidance framework.

Version 2.0 - August 2025:
Added KUN virtual asset industry compliance practice cases; included in-depth regulatory policy analysis articles from BlockSec official account; improved industry practice guidance content.

Version 1.0 - July 2025:
Initial release, covering global regulatory background, on-chain risk analysis, response strategies, and industry practice cases.

Update Notes:
This manual will be continuously updated according to regulatory policy changes. For suggestions, please contact: contact@blocksec.com

Contents

Chapter 1 Regulatory Landscape

Global regulatory efforts concerning crypto payments have evolved from general principles to more refined, region-specific enforcement. From FATF's global blueprint to jurisdiction-specific frameworks in the United States, European Union, Hong Kong, and the United Arab Emirates, a multilayered and tightly coordinated supervisory system has emerged. For crypto payment firms, this makes the one-size-fits-all compliance strategies ineffective. Given the unique transaction thresholds, reporting obligations, and risk indicators in each region, companies must adopt sophisticated and customizable compliance tools to navigate this increasingly complex regulatory environment.

This chapter provides an overview of key regulatory developments across major economies, outlining their legal frameworks and implications for stablecoin-based payment service providers.

1.1. FATF: The Global Requirement for AML/CFT

The Financial Action Task Force (FATF) serves as the primary global standard-setting body and watchdog for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT), widely regarded as the authoritative reference in designing national virtual asset regulatory regimes. Since its inception in 1989 by the G7, the FATF has continuously tracked emerging financial crime typologies, published evaluation reports on the AML/CFT performance, and regularly updated its flagship policy framework—the FATF Recommendations. While the Recommendations are formally non-binding, the FATF has effectively established a regime of compliance through its mutual evaluation mechanism and grey-listing process. The resulting reputational and financial risks associated with non-compliance—such as impaired access to international financial systems and increased due diligence from foreign financial institutions—create a powerful incentive for jurisdictions to align with the Recommendations, thereby rendering them de facto obligatory in international practice.

FATF's latest Global Regulatory Assessment Report released in 2025 reveals significant differences in compliance status across countries. We have provided a detailed analysis of this in our in-depth article published on BlockSec's official account, with specific details available in Appendix 7.2.

Key Provisions for Payment Services

As of October 2018, FATF expanded Recommendation 15 to explicitly include Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). In June 2019, it released an Interpretive Note clarifying that VASPs must comply with AML/CFT obligations, including:

- **Customer Due Diligence (CDD)**: Identity verification (KYC), monitoring of transactions, and reporting of suspicious transactions (STRs).
- **Travel Rule**: VASPs must collect and share originator and beneficiary information for transactions above a certain threshold (commonly USD/EUR 1,000), ensuring transaction traceability.
- **Risk-Based Approach**: Enhanced due diligence (EDD) is required for high-risk scenarios, such as transactions involving PEPs, high-risk jurisdictions, or anonymity-enhancing technologies.
- **Recordkeeping & Reporting:** VASPs must retain transaction and due diligence records for at least five years and be capable of reconstructing transaction trails. Suspicious activity must be reported to the competent Financial Intelligence Unit (FIU).

In June 2020, FATF clarified that its AML/CFT standards also apply to stablecoins:

"So-called stablecoins and their service providers fall under the definition of VASPs when they engage in or facilitate virtual asset activities. They are not exempted from the FATF Standards and must comply with all relevant AML/CFT obligations."

(Report to the G20 Finance Ministers and Central Bank Governors on So-called 'Stablecoins')

Summary

Due to its technological neutrality and global legitimacy, the FATF framework has become the foundational template for national regulatory schemes. Licensing requirements, registration systems, and the extension of traditional financial rules to VASPs are all built upon FATF's Recommendations.

1.2. Hong Kong: Fiat-Backed Stablecoin Licensing Regime

On May 21, 2025, the Legislative Council of the Hong Kong Special Administrative Region passed the **Stablecoin Bill** in its third reading. The law is scheduled to take effect on August 1, 2025, and establishes a licensing regime for fiat-backed stablecoins. Under the new framework, any entity issuing fiat-referenced stablecoins in Hong Kong or pegged to the value of the Hong Kong Dollar outside of Hong Kong must obtain a license from the **Hong Kong Monetary Authority (HKMA)**. Only licensed issuers may offer such stablecoins to retail investors.

Issuers are required to meet stringent entry requirements similar to those imposed on banks, including the establishment of a local entity, a minimum paid-up capital requirement (e.g., HKD 25 million), full backing with highly liquid reserve assets, independent custody and regular audits of reserves, robust local governance, and comprehensive AML/CFT compliance systems. Algorithmic and under-collateralized stablecoins are excluded from the regulatory scope.

Key Requirements for Payment Services

- **Licensing and Counterparty Requirements:** The Stablecoin issuers must operate under a license. Payment companies, as part of the broader stablecoin ecosystem, are expected to select licensed issuers as their partners. The HKMA imposes strict AML/CFT capability standards on licensed entities.

- **Reporting Obligations:** Under the Organized and Serious Crimes Ordinance and the Drug Trafficking (Recovery of Proceeds) Ordinance, VASPs are required to file Suspicious Transaction Reports (STRs) with the Joint Financial Intelligence Unit (JFIU) upon detecting suspicious activities. These reports must include clearly selected "suspicious indicators" (e.g., turnaround transactions, involvement of offshore entities) and the suspected offense (e.g., fraud, terrorist financing).

- **Transaction Thresholds:** According to the SFC's Guideline on Anti-Money Laundering and Counter-Terrorist Financing, for non-wire transfers involving virtual assets, if the amount is equal to or exceeds HKD 8,000, financial institutions must conduct customer due diligence (CDD) before executing the transaction.

Summary

Hong Kong's regulatory regime is marked by a clear licensing structure and granular enforcement. By setting concrete transaction reporting thresholds and detailed STR obligations, Hong Kong translates FATF's principle-based guidance into highly actionable local law. This imposes a higher degree of operational and compliance scrutiny on VASPs operating within the jurisdiction.

1.3. United States: Federal Regulation of Stablecoins

The U.S. regulatory landscape is renowned for its aggressive enforcement and severe penalties. Enforcement authority is not only exercised through legislation but also operationalized via existing legal instruments such as the **Bank Secrecy Act (BSA)** and powerful enforcement agencies like the **Office of Foreign Assets Control (OFAC)** under the Department of the Treasury, and the **Department of Justice (DOJ**).

In June 2025, the U.S. Senate passed the GENIUS Act (The Guiding and Establishing National Innovation for U.S. Stablecoins Act)—the first federal legislation aimed at establishing a compliance framework for U.S. dollar-pegged stablecoins. The bill, currently under review by the House of Representatives, intends to subject major issuers such as USDT and USDC to formal oversight, potentially extending U.S. regulatory influence globally.

The GENIUS Act clarifies that payment stablecoins are neither securities, commodities, nor instruments insured by the Federal Deposit Insurance Corporation (FDIC), thereby avoiding overlap with the **Securities and Exchange Commission (SEC)** and the **Commodity Futures Trading Commission (CFTC)**. It authorizes only federally or state-licensed banks, credit unions, or nonbank financial institutions to issue payment stablecoins. Technology firms (e.g., Meta, Amazon) must meet additional financial risk control and data privacy requirements. Foreign issuers (e.g., Tether) must register with U.S. authorities and comply with equivalent regulations or face restrictions from servicing U.S. platforms.

The act further mandates 100% reserve backing, monthly disclosures and audits, and obligates issuers to adopt AML controls equivalent to those required under the BSA, including customer due diligence and suspicious activity reporting.

Key Requirements for Payment Services

- **Mandatory Adherence to OFAC Sanctions**: Transactions involving individuals, entities, or addresses listed by OFAC are strictly prohibited. Stablecoin issuers (e.g., Tether, Circle) are required to immediately freeze related assets upon detection of such transactions.

- **Legislative Clarity**: The GENIUS Act and similar proposals aim to bring stablecoin issuers fully under the scope of the BSA, mandating the development of comprehensive AML programs. Innovation is encouraged in AML processes, including the use of advanced technologies to detect and prevent illicit activities. Measures include public comment solicitation, studies by the Treasury and **Financial Crimes Enforcement Network (FinCEN)**, and periodic reporting to Congress.

- **Detailed Risk Identification Guidelines**:
  FinCEN has issued detailed red flag indicators, including:
  - switching from SSN to ITIN usage,
  - multiple businesses using the same address,
  - account openings at institutions distant from a customer's residence.

These indicators help in identifying suspicious financial behavior.

Summary

The U.S. regulatory framework is characterized by a dual-track approach of stringent enforcement and progressive legislation. Authorities leverage existing laws such as the BSA while simultaneously developing a federal legislative regime for stablecoins, particularly those pegged to the U.S. dollar. These efforts exert de facto extraterritorial influence over VASPs worldwide.

The mandatory nature of OFAC sanctions, the deterrent effect of billion-dollar fines, and the legislative advancement of the GENIUS Act collectively form a high-pressure regulatory environment with global reach.

1.4. European Union: A Unified Framework via Token Classification

The **Markets in Crypto-Assets Regulation (MiCA)**, adopted by the European Union, entered into full force on December 30, 2024. It applies across all 27 EU Member States and three European Economic Area (EEA) countries. MiCA aims to resolve longstanding regulatory fragmentation and arbitrage issues within the EU by introducing a comprehensive and harmonized framework.

MiCA adopts **a token classification approach**, categorizing crypto-assets into three primary types:

- **Electronic Money Tokens (EMTs)**: Pegged to official currencies, used as a means of payment.
- **Asset-Referenced Tokens (ARTs)**: Pegged to a basket of assets, including currencies, commodities, or other values.
- **Utility Tokens (UTs)**: Provide digital access to goods or services.

Based on these classifications, MiCA imposes specific authorization and compliance obligations on crypto-asset issuers and service providers, covering areas such as capital requirements, corporate governance, consumer protection, disclosure, reserve management, redemption rights, and AML/CFT compliance. Notably, fully decentralized assets (e.g., most NFTs) fall outside MiCA's scope.

Key Requirements for Payment Services

- **Counterparty Authorization Requirements**: MiCA mandates that stablecoin issuers must be authorized within the EU. Payment service providers wishing to integrate stablecoins into their systems must work exclusively with MiCA-compliant entities. Noncompliance constitutes unauthorized business activity, subjecting firms to enforcement actions within the EU.

- **Stringent Operational Standards**: MiCA imposes strict requirements on reserve management, corporate governance, disclosures, and consumer protections—on par with traditional financial regulation.

- **Market Abuse Prevention**: MiCA explicitly prohibits insider trading and market manipulation. VASPs must have effective systems in place to detect and prevent such

misconduct.

- **Unified AML/CFT Oversight**: The EU is establishing a centralized **Anti-Money Laundering Authority (AMLA)** and adopting a comprehensive AML/CFT legislative package. This initiative will produce a unified rulebook applicable to all **Crypto-Asset Service Providers (CASPs)**, including those offering stablecoin payment services. The result will be a coordinated and harmonized regulatory structure for monitoring financial flows.

Summary

MiCA represents the world's first fully harmonized and comprehensive regulatory framework for crypto-assets. Alongside the forthcoming **Anti-Money Laundering Regulation (AMLR)** and the AMLA, it constitutes a dual-pillar system:

- **MiCA** governs markets, operations, and consumer protection.
- **AMLR/AMLA** establishes a unified AML/CFT enforcement architecture.

Together, they aim to eliminate regulatory arbitrage and bring clarity and consistency to crypto-asset supervision across the EU.

1.5. United Arab Emirates: An Emerging Web3 Hub Balancing Innovation and Regulation

As countries like Singapore tighten their regulatory grip on Web3 projects, the **United Arab Emirates (UAE)**—driven by the dual engines of **Dubai and Abu Dhabi**—has become an increasingly attractive destination for project teams, developers, and investors. The UAE's pro-business environment and forward-looking policies have attracted global enterprises; however, its openness is firmly grounded in robust compliance principles.

While adhering to the core tenets of the **FATF**, the UAE's regulatory framework also features more concrete and localized compliance requirements.

Key Regulatory Characteristics of the UAE

Minimum Capital Requirements: Both the **Dubai Virtual Assets Regulatory Authority (VARA)** and the **Abu Dhabi Global Market (ADGM)** require licensed entities to meet specific minimum capital thresholds. These thresholds serve as market entry filters to ensure only financially sound institutions are authorized.

Rigorous Technological and Governance Vetting: Regulators in both jurisdictions emphasize technical resilience and corporate governance. Applicants must submit detailed technical

architecture documentation, cybersecurity measures, business continuity plans, and undergo background checks for key personnel. These requirements are more detailed and stringent than FATF's general risk management guidelines.

Granular Licensing Regime (as pioneered by VARA): VARA has introduced a modular licensing framework, issuing distinct licenses for different business activities such as trading, brokerage, custody, payments, lending, and advisory services. This granularity requires businesses to clearly define their operational scope and meet the compliance obligations specific to each activity.

Explicit AML/CFT Supervision

- **VARA** has published a **Compliance & Risk Management Rulebook**, outlining licensed entities' AML/CFT obligations, including customer due diligence, transaction monitoring, and suspicious activity reporting.
- **ADGM's Financial Services Regulatory Authority (FSRA)** enforces its **AML Rulebook**, mandating comprehensive CDD, transaction monitoring, and the maintenance of high capital adequacy and technical governance standards.

Summary

The UAE's regulatory architecture—represented by Dubai and Abu Dhabi—strikes a deliberate balance between fostering innovation and enforcing stringent compliance.

- **Dubai's VARA** features a modular, activity-based regime.
- **Abu Dhabi's ADGM,** grounded in common law principles, offers a mature framework.

In both jurisdictions, licensing eligibility is closely tied to an entity's AML/CFT capabilities, reinforcing the message that embracing technological advancement must go hand-in-hand with adherence to international compliance norms.

Table 1: Overview of Regulatory Authorities by Country (Region)

HONGKONG SAR	The Securities and Futures Commission (SFC) of Hong Kong Hong Kong Monetary Authority
USA	U.S. Securities and Exchange Commission (SEC) U.S. Commodity Futures Trading Commission (CFTC) Financial Crimes Enforcement Network (FinCEN) State financial regulators (e.g., New York Department of Financial Services, NYDFS)
European Union	European Securities and Markets Authority (ESMA) National financial regulators of member states, such as the Federal Financial Supervisory Authority of Germany (BaFin)
Singapore	Monetary Authority of Singapore (MAS)
United Arab Emirates (Dubai)	Dubai Virtual Assets Regulatory Authority (VARA) Dubai Financial Services Authority (DFSA)

After understanding the overall background and development trends of global crypto asset regulation, we can see that regulatory authorities worldwide are transitioning from an initial wait-and-see attitude toward establishing more comprehensive and systematic regulatory frameworks. With the gradual establishment of international regulatory standards such as FATF guidance, the EU's MiCAR regulations, and US FinCEN requirements, along with the cautionary effect of major compliance cases such as Binance's $4.3 billion fine, crypto payment service providers are facing unprecedented compliance pressure. In this regulatory environment, obtaining appropriate licenses and authorizations has become a fundamental requirement for the compliant operation of crypto payment institutions.

From the macro perspective of the regulatory background, we will now delve into the specific requirements and implementation details of crypto payment licenses. Chapter 2 will provide a detailed analysis of license types, application conditions, regulatory requirements, and compliance standards across major jurisdictions, offering practical guidance for crypto payment service providers on license acquisition and maintenance.

Chapter 2 Crypto Payment Licenses (Grandway Law Offices)

With crypto-asset regulation rapidly maturing worldwide, securing compliant crypto payment licenses has become a fundamental requirement for the lawful operation of enterprises. This chapter, authored by the Web3 team of Grandway Law Offices, provides a comprehensive analysis of the crypto payment licensing systems in major jurisdictions worldwide, offering practical guidance for enterprises to develop global compliance strategies.

This chapter covers:
- Europe: Unified regulation under the MiCA framework and practices in Member States
- Asia: Divergent regulatory approaches in Japan, South Korea, Hong Kong, Singapore, and Dubai
- Americas: The complex dual-layer regulatory system in the United States and emerging markets in South America
- Africa: Regulatory developments in key markets such as Nigeria, South Africa, and Ghana

About Grandway Law Offices:
Established in 1994, Grandway Law Offices has grown into a leading large-scale law firm in China with a high degree of specialization after over three decades of steady development. The firm is distinguished by its prominent expertise, particularly in the capital markets sector, and ranks among the top tiers in specialized fields such as Web3, dispute resolution, real estate and construction engineering, cross-border investment and M&A, and banking and finance. The Web3 team at Grandway Law Offices has accumulated extensive experience in areas including the establishment of overseas structures for Web3 projects, investment and financing, the setup and management of crypto funds, and domestic and international compliance. As one of the earliest teams in China to engage in Web3 legal services, we provide legal solutions to leading participants across various sectors.

2.1. Crypto Payments in Europe

2.1.1 The Unified EU Framework: MiCA and AMLA

The *Markets in Crypto-Assets Regulation (MiCA)*, promulgated by the European Union, represents the world's first comprehensive and unified regulatory framework for crypto-assets, signifying a transition from fragmented to systematic crypto-asset supervision in Europe. This Regulation will become fully applicable on 30 December 2024 across the 27 EU Member States and 3 European Economic Area states. Its core objectives are to provide legal certainty for the entire single market, support technological innovation, and ensure a high level of consumer protection, market integrity,

and financial stability. Complementing MiCA is the forthcoming establishment of the Anti-Money Laundering Authority (AMLA), which will introduce a layer of centralized anti-money laundering supervision for high-risk entities, collectively constituting a dual-pillar supervisory architecture.

2.1.1.1 Core Principles of MiCA: A Pan-European Crypto-Asset Rulebook

The cornerstone of MiCA lies in its classification-based regulatory approach for crypto-assets, designed to impose proportionate regulatory requirements based on the risks and functions of different tokens. The Regulation primarily categorizes crypto-assets into three classes, with the first two being directly relevant to crypto payment businesses:

1. **E-Money Tokens (E-Money Tokens, EMTs):** These are crypto-assets that maintain a stable value by referencing the value of a single fiat currency and are designed to function as a means of payment, analogous to electronic money. Stablecoins such as USDC or EURC, if issued within the EU, would fall under this category.
2. **Asset-Referenced Tokens (Asset-Referenced Tokens, ARTs):**These are crypto-assets that maintain a stable value by referencing any other value or right or a combination thereof, including one or more official currencies. For instance, stablecoins pegged to a basket of currencies or commodities belong to this category and may also be used as a means of payment or store of value.
3. **Other Crypto-Assets:** This constitutes a residual category encompassing all crypto-assets not classified as EMTs or ARTs, such as utility tokens.

Based on this classification, MiCA establishes explicit authorisation and operational requirements for crypto-asset issuers and Crypto-Asset Service Providers (CASPs). The definition of a CASP is broad, covering a range of activities critical to the crypto payments ecosystem, including the exchange of crypto-assets for fiat currency, the transfer of crypto-assets, the custody and administration of crypto-assets, and the operation of trading platforms. Any entity wishing to provide such services within the EU must first obtain CASP authorisation from the National Competent Authority (NCA) of its home Member State.

2.1.1.2 Special Focus: Division of Powers – ESMA as Standard-Setter and NCAs as Gatekeepers

The successful implementation of MiCA relies on a sophisticated division of powers and collaboration between EU-level bodies and national authorities of Member States. This directly addresses a key concern for enterprises planning compliance strategies: who sets the rules, and who enforces them?

The Role of the European Securities and Markets Authority (ESMA): Unified Standard-Setter and Coordinator

ESMA plays a central role as the "standard-setter" within the MiCA framework. Its primary responsibility is not the direct authorisation or supervision of the vast majority of CASPs, but rather ensuring the consistent application of MiCA's high-level principles across the entire EU through the development of detailed "Level 2" and "Level 3" measures. These measures include Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS), which provide specific, operational guidance on matters such as CASP applications, corporate governance, conflict of interest management, and IT system requirements.

ESMA's core objective is to promote "supervisory convergence." This means that regardless of whether an crypto payment company applies for a CASP licence in Lithuania, Ireland, or Germany, its application will be assessed against the same detailed standards developed by ESMA. This fundamentally prevents "regulatory arbitrage" – wherein firms seek registration in jurisdictions with the least stringent requirements – thereby safeguarding a level playing field within the EU single market and ensuring uniform investor protection standards.

The Role of National Competent Authorities (NCAs): "Gatekeepers" for Market Access

The NCAs of individual Member States, such as the German Federal Financial Supervisory Authority (BaFin), the Luxembourg Commission de Surveillance du Secteur Financier (CSSF), or the Central Bank of Ireland, serve as the primary implementers and "gatekeepers" under the MiCA framework. Their key responsibilities include:

- **Authorisation:** The NCA is the sole body responsible for receiving, assessing, and ultimately approving or rejecting applications for CASP authorisation. Applicant firms must submit their application to the NCA of the Member State where they are established.
- **Ongoing Supervision:** Once authorised, the NCA conducts continuous, day-to-day supervision of CASPs within its jurisdiction to ensure compliance with all operational, prudential, and conduct obligations under MiCA.
- **Enforcement:** The NCA is responsible for handling consumer complaints, investigating infringements, and is empowered to take administrative measures and impose penalties.

Collaboration Mechanism Between ESMA and NCAs

This division of powers creates an efficient collaborative system: ESMA develops a unified, detailed rulebook at the EU level, while NCAs are responsible for implementing this blueprint at the national level. A CASP seeking authorisation must submit comprehensive application documentation to its home NCA, including its business plan, governance arrangements, ICT systems compliant with the Digital Operational Resilience Act (DORA), and AML/CFT controls. The NCA will rigorously review this application against the technical standards developed by ESMA before making the final authorisation decision.

This institutional design introduces a significant strategic consideration. While MiCA aims to unify rules, it decentralises the power of authorisation and supervision to 27 different national authorities. Consequently, although the rulebook is uniform, subtle differences may persist in the style, efficiency, expertise, and risk focus of different NCAs during the review process. Therefore, when selecting an EU "home state," enterprises must not only consider the application procedure itself but also conduct in-depth due diligence on the long-term supervisory stability and expertise of the relevant NCA.

2.1.1.3 The EU Passport: Single Licence for the Unified Market

One of the most transformative advantages introduced by the MiCA framework for the crypto industry is the "EU passport" mechanism. Once a CASP (e.g., a crypto payment provider) successfully obtains authorisation from the NCA of its "home" Member State, it acquires the right to provide its authorised services to clients across the entire EU single market, without needing to seek additional licences from the other 26 Member States.

This mechanism operates based on notification rather than re-approval. When an authorised CASP plans to provide services in another "host" Member State, it simply notifies its home NCA. The home NCA subsequently transmits the relevant information to the host NCA. This significantly reduces the regulatory costs and time for pan-European expansion, con

trasting sharply with the fragmented US system requiring state-by-state licensing. It constitutes a decisive advantage for enterprises aiming to establish pan-European payment networks.

However, the powerful functionality of the EU passport carries an inherent risk: "home state dependency risk." A firm's entire EU operations are contingent upon the licence granted by a single home state. This implies that if the relationship with the home NCA deteriorates, or if the home NCA's supervisory stance becomes more stringent, or ultimately revokes the licence, the firm would immediately lose its operational eligibility across the entire EU market. This potential single point of failure renders the selection of the home state jurisdiction a critical long-term strategic decision.

2.1.1.4 The Superimposed Effect of AMLA: Centralised AML/CFT Supervision for High-Risk Entities

While MiCA unifies market access rules, the EU is concurrently strengthening its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) enforcement capabilities through the establishment of the new Anti-Money Laundering Authority (AMLA). AMLA was legally established in June 2024, is headquartered in Frankfurt, and is expected to commence direct supervisory activities in 2028.

The establishment of AMLA marks a significant shift in EU AML/CFT supervision from a fully

decentralised to a partially centralised model. One of its core responsibilities is the direct AML/CFT supervision of a selected group of the highest-risk cross-border financial institutions, with CASPs explicitly included within this scope. Starting in 2027, AMLA will select up to 40 financial groups or entities as its "directly supervised entities," based on criteria such as risk assessment and cross-border activity.

For these selected high-risk CASPs (which may include large cross-border crypto payment platforms), AMLA will lead "Joint Supervisory Teams" comprising its own staff and staff from relevant NCAs, responsible for conducting on-site and off-site inspections, and empowered to impose significant financial penalties directly. For all other CASPs not selected, AMLA will play an indirect supervisory role by coordinating Member State NCAs and issuing guidelines and technical standards to ensure consistent and effective implementation of AML/CFT rules across the EU.

This structure effectively creates a potential two-tier supervisory system for CASPs in the EU. All CASPs will be subject to comprehensive MiCA-based supervision by their home NCA (covering corporate governance, consumer protection, prudential requirements, etc.). However, for those leading CASPs that are large, operate in multiple countries, and are deemed high-risk, an additional, direct layer of supervision focused specifically on AML/CFT risk from AMLA will apply. This implies that as a business scales, its compliance costs and complexity will increase non-linearly. Crossing the threshold for AMLA selection will demand a qualitative leap in the firm's compliance resources, systems, and governance to simultaneously meet regulatory requirements at both the national and supranational levels.

2.1.2. State Practice

Prior to the full implementation of MiCA, Baltic States such as Estonia and Lithuania, by virtue of their relatively lenient VASP registration regimes, attracted a significant number of crypto-asset enterprises. Presently, with the advent of the MiCA era, these jurisdictions are undergoing a profound "regulatory rebranding," transitioning from their former status as "registration hubs" to high-quality "financial centres" fully compliant with MiCA standards.

2.1.1.1 Estonia

Estonia was among the first European Union Member States to establish a licensing regime for Virtual Asset Service Providers (VASPs), and its permissive policy once attracted thousands of companies to register. However, commencing in 2019, driven by anti-money laundering concerns, its policy began to tighten significantly. In 2020, its Financial Intelligence Unit (FIU) revoked over 1,000 VASP licenses in a single action, marking the commencement of this shift.

With the advent of MiCA, regulatory competence in Estonia has been formally transferred from the

FIU to the more traditional financial regulator – the Estonian Financial Supervision and Resolution Authority (EFSRA). Pursuant to its new *Crypto-Asset Markets Act*, all new Crypto-Asset Service Providers (CASPs) must obtain authorization from EFSRA, while holders of previously issued VASP licenses from the FIU must complete the transition to the new regime by 1 July 2026. The new authorization requirements are substantially more stringent than in the past, including the mandatory requirement for companies to have at least two members of the management board, establish a physical office in Estonia, and meet higher capital requirements, fully aligning with MiCA standards.

2.1.1.2 Lithuania

Lithuania, another popular jurisdiction for VASP registration, has also proactively embraced MiCA. Its newly enacted *Republic of Lithuania Law on Crypto-asset Markets* explicitly designates the Bank of Lithuania as the sole competent authority for the authorization and supervision of CASPs.

Lithuania's approach to the MiCA transitional period is particularly noteworthy. Although MiCA permits Member States to provide incumbent VASPs with a grandfathering transition period of up to 18 months (until 1 July 2026), Lithuania opted for a more accelerated timeline. Following parliamentary debate, the final deadline for domestic VASPs to adapt to the new regulations was set at 1 January 2026. Subsequent to this date, any incumbent VASP failing to obtain a MiCA license must cease operations. The Bank of Lithuania has also issued multiple guidance documents to the market, emphasizing its high expectations regarding corporate governance, prudential requirements, and investor protection, clearly signalling its intent to attract high-quality, compliance-conscious enterprises.

These initiatives by the Baltic States are not coincidental. They collectively reflect a clear strategic pivot: moving away from registration convenience and volume as competitive advantages, and instead positioning themselves as reliable, high-quality crypto-financial centres within the EU through the rigorous and efficient implementation of the MiCA framework. The target clientele for this strategy is no longer small startups seeking regulatory arbitrage, but rather more mature, institutional-grade crypto-asset enterprises seeking long-term development within a unified and stable EU market.

2.1.3. Switzerland

As a non-EU Member State, Switzerland has charted a distinct path in crypto-asset regulation,

markedly different from that of the European Union. Eschewing the creation of an entirely new, comprehensive code specifically for crypto-assets, it adheres to the principle of "technology neutrality," flexibly applying its existing, mature financial market legal framework to emerging Distributed Ledger Technology (DLT) and crypto-assets. The advantage of this approach lies in its stability and predictability, affording enterprises a high degree of legal certainty.

2.1.3.1 The FINMA Framework: Technology Neutrality and the DLT Act

The Swiss Financial Market Supervisory Authority (FINMA) is the sole federal regulator for the Swiss financial market. The core of its regulatory philosophy is to focus on the economic function and inherent risks of an activity, rather than the specific technology employed. In its 2018 ICO Guidelines, FINMA pioneered the classification of tokens into three categories: payment tokens, utility tokens, and asset tokens, regulating them according to their function under the existing financial regulatory framework. For crypto payment services, the classification of "payment tokens" is particularly relevant, as it directly engages the application of anti-money laundering law.

To further consolidate its position as a DLT hub, Switzerland fully implemented the *DLT Act* in 2021. This Act is not a standalone law, but rather a systematic revision of over ten existing laws. Its core achievement is the legal recognition of "DLT securities" as a new asset class, providing a solid legal foundation for their issuance, trading, and custody. Furthermore, the Act introduced a new licensing category – DLT trading facilities – paving the way for regulated secondary markets in DLT securities.

2.1.3.2 The FinTech Licence: A Flexible Option Tailored for Innovation

One of the most attractive innovations within the Swiss regulatory system is the "FinTech Licence," introduced in 2018. This constitutes a "light-weight banking licence," specifically designed for innovative fintech companies that accept public deposits but do not engage in traditional credit and interest margin businesses.

Under the *Swiss Banking Act*, any commercial acceptance of public deposits from more than 20 parties requires a banking licence. The FinTech Licence provides a significant exception to this rule. It permits licensed institutions to accept public deposits up to 100 million Swiss Francs, provided these deposits are not used for investment and do not bear interest. This provision perfectly aligns with the business models of cryptocurrency exchanges, payment providers, and custodians, as their core activity involves holding client funds for trading or payment purposes, not lending.

2.1.3.3 Deconstructing Switzerland's Composite Advantages

Switzerland's status as a globally recognized "Crypto Valley" stems not merely from any single policy, but from a unique ecosystem comprising regulation, taxation, and business environment, which is difficult to replicate.

1. **Regulatory Stability and Clarity:** FINMA's consistent, principles-based regulatory approach provides the industry with valuable legal certainty. In an industry characterized by rapidly changing global regulatory policies, this predictability is itself a core asset. Furthermore, FINMA is renowned for its open and pragmatic attitude, encouraging applicants to engage in informal communication and project presentation prior to formal application submission, significantly reducing uncertainty and sunk costs during the application process. For innovative enterprises, this enables constructive dialogue with the regulator.

2. **Tailored Licensing Regime:** The FinTech Licence is the epitome of Switzerland's "regulation for innovation" ethos. It precisely addresses the core need of the crypto payment industry – the lawful holding of client funds – while avoiding the imposition of onerous traditional banking regulatory requirements that are ill-suited to their business models. This flexibility is key to attracting innovative enterprises.

3. **Highly Competitive Corporate Tax System:** This is one of Switzerland's most notable economic advantages. Switzerland's tax system is highly decentralized, comprising federal, cantonal, and communal levels. Cantons engage in fierce tax competition to attract businesses and talent. This enables cantons like Zug to offer very low corporate income tax rates, with a combined effective tax rate of approximately 11.8%, significantly lower than most major European economies. For highly profitable crypto enterprises, this translates to substantial cost savings.

4. **Investor-Friendly Personal Tax Policy:** Swiss tax law is also favourable for individual investors. For individuals classified as private investors, capital gains derived from movable private assets (including cryptocurrencies) are generally tax-exempt. While Switzerland levies an annual wealth tax, the rate is very low, typically not exceeding 1%. This policy strongly incentivizes individual participation in crypto-asset investment and attracts global crypto founders and top talent to relocate to Switzerland. Notably, the canton of Zug has accepted Bitcoin and Ethereum for tax payments since 2021, further demonstrating its embrace of the crypto economy.

2.2. Crypto Payments in Asia

2.2.1. Japan

Japan was one of the first countries globally to regulate cryptocurrency exchanges. Its regulatory framework, led by the Financial Services Agency (FSA), is renowned for its detailed, stringent, and highly localized requirements. Any entity engaging in activities such as buying/selling, exchanging, brokering, or custodying crypto-assets in Japan must register as a Crypto Asset Exchange Service Provider (CAESP). These services form the foundation of crypto payment operations (e.g., fiat-to-

crypto exchange, payment gateway services).

2.2.1.1 FSA Authorization: Crypto Asset Exchange Service Provider (CAESP)

Obtaining a CAESP licence in Japan is a protracted and arduous process. The application cycle typically ranges from 6 to 12 months, and this does not include the months or even longer period of "pre-consultation" with the FSA prior to formal application submission. The FSA conducts an extremely thorough review of the applicant's business model, governance structure, technical systems, and compliance framework.

2.2.1.2 Core Licence Requirements: Local Entity, Capital & Governance

FSA requirements are exceptionally strict, particularly regarding "Local Substance", which constitutes the most significant barrier to entry for foreign enterprises into the Japanese market.

- **Mandatory Local Presence:** The applicant must be a legal entity incorporated in Japan (typically a "Kabushiki Kaisha") and maintain a physical office in Japan. Virtual offices are unacceptable. More critically, the company must have a management team resident in Japan. The FSA explicitly requires that the company have at least one full-time director residing in Japan, who must possess a deep understanding of Japanese financial regulations and relevant professional experience. This means foreign companies cannot simply manage their Japanese operations remotely but must make deep localization investments.
- **Capital and Financial Requirements:** The FSA requires companies to maintain positive net assets at all times and possess sufficient financial resources to support their operations. Furthermore, companies must strictly segregate client assets from proprietary assets and establish independent custody and management systems for client fiat and crypto-assets, all subject to verification through annual independent audits.
- **Comprehensive Application Documentation:** The licence application requires submission of an extremely detailed set of documents, all of which must be translated into Japanese and notarized. These documents include, but are not limited to: a detailed business plan including financial projections for the coming years; the company's organizational chart and internal governance rules; a complete set of AML/KYC policies and procedures; detailed descriptions of information technology systems, cybersecurity measures, and data protection; and background check documents and criminal record certificates for all directors, major shareholders, and key management personnel.
- **Stringent Ongoing Supervision:** Upon licence grant, CAESPs are subject to strict ongoing supervision by the FSA, including regular submission of detailed business reports and annual on-site or off-site inspections.

Japan's regulatory framework is, in effect, designed to form a non-tariff trade barrier. Its rigid requirements for local entities and resident managers significantly increase the operational costs and management complexity for foreign companies. This design is not accidental; it reflects the FSA's policy orientation of prioritizing investor protection and financial system stability. By setting high entry barriers, the FSA intentionally filters out enterprises with insufficient capital, weak compliance capabilities, or an unwillingness to make long-term localization investments. Consequently, Japan's crypto market is dominated by a small number of large, well-capitalized domestic companies that have passed the rigorous tests, and a few international giants that have made significant localization investments. While this somewhat limits market competition dynamism, it ensures that market participants possess high compliance standards and risk resilience.

2.2.2. South Korea

South Korea's crypto-asset regulatory system is jointly overseen by the Financial Services Commission (FSC) and its subordinate Korea Financial Intelligence Unit (KoFIU). All Virtual Asset Service Providers (VASPs) operating in South Korea or providing services to South Korean users must report to and complete registration with KoFIU. South Korea's regulatory framework is renowned for its unique "Three Pillars," which collectively constitute one of the strictest compliance regimes globally.

2.2.2.1 VASP Registration Process: Dual Supervision by FSC and KoFIU

The primary basis for regulation is the *Act on Reporting and Use of Specified Financial Transaction Information*, amended in 2021 to formally bring VASPs within the ambit of AML/CFT regulation. Additionally, to enhance investor protection, South Korea formally implemented the *Virtual Asset User Protection Act* in July 2024, imposing stricter requirements on VASPs regarding customer asset protection and the prohibition of unfair trading practices.

2.2.2.2 South Korea's Three Compliance Pillars: Real-Name Accounts, ISMS Certification & Travel Rule

Any VASP wishing to operate legally in South Korea must simultaneously satisfy the following three core requirements:

1. **Real-Name Verified Bank Accounts:** This is the cornerstone of the South Korean regulatory system and the element with the greatest impact on crypto payment services. If a VASP wishes to offer Korean Won (KRW) fiat deposit/withdrawal services – the foundation of all local payment operations – it must establish a partnership with a domestic South Korean commercial bank to provide all users with real-name verified deposit/withdrawal accounts. This means every user's fiat transaction is processed through a bank account

strictly linked to their verified identity, significantly enhancing transaction transparency and traceability. However, South Korean commercial banks are extremely cautious in selecting VASP partners, subjecting them to rigorous due diligence on their compliance systems, security capabilities, and internal controls. Very few VASPs successfully secure banking partnerships, making real-name account cooperation the primary bottleneck for market entry.

2. **Information Security Management System (ISMS) Certification:** All VASPs must obtain ISMS certification from the Korea Internet & Security Agency (KISA). This involves a comprehensive and stringent audit of the company's information security management processes and technical controls, designed to ensure the VASP's capability to protect user data and assets from cyber-attacks and internal threats.
3. **Strict Travel Rule Implementation:** South Korea was one of the first countries to mandatorily enforce the FATF's "Travel Rule." Under the regulations, when a VASP processes a virtual asset transfer exceeding 1 million KRW in value, it must collect, retain, and transmit the originator and beneficiary information to the recipient VASP. This is crucial for the compliant operation of cross-border payment services.

Beyond these three pillars, South Korean VASPs must adhere to other stringent operational standards, such as: storing at least 80% of customer crypto-assets in offline cold wallets; fully segregating customer deposits from company funds; and obtaining liability insurance or establishing a reserve fund to cover potential user losses from security incidents like hacking.

South Korea's regulatory model effectively "outsources" a portion of key "gatekeeper" responsibilities to the traditional banking sector. The mandatory real-name account cooperation requirement grants commercial banks significant power to determine which VASPs can effectively enter and serve the South Korean market. The risk appetite and due diligence standards of banks largely shape the market landscape and pace of innovation in the crypto industry. A VASP must not only meet KoFIU's registration requirements but also convince a highly risk-averse commercial bank, which may impose even more demanding criteria than the regulator. This "dual gatekeeper" mechanism makes the South Korean market one of the most challenging to enter globally and creates a unique ecosystem where the crypto industry is highly intertwined with and dependent on the traditional financial system.

2.2.3. Hong Kong

The Hong Kong MSO licence governs the regulatory responsibilities for fiat currency exchange, remittance businesses, and cross-border transfer activities, emphasizing the security of the entire transaction chain through a meticulous Anti-Money Laundering (AML) framework. The VA OTC licence, conversely, is the core licence for handling conversion transactions between stablecoins and fiat currency, or between other virtual assets.

2.2.3.1 Money Service Operator Licence (MSO)

Since early 2024, Hong Kong's virtual asset regulatory framework has undergone significant evolution and deepening. According to a consultation paper released in February of that year, the initial conception was to bring all entities providing virtual asset spot trading services under the regulatory purview of the Hong Kong Customs and Excise Department. This design stemmed from Customs' longstanding and mature regulatory practice over traditional Money Service Operators (MSOs), reflecting considerations of institutional continuity. However, following months of industry consultation and in-depth deliberation among regulators, the final regulatory scheme announced in June 2025 saw a major shift – regulatory authority over Virtual Asset Over-the-Counter (VA OTC) trading or Virtual Asset Dealing services was explicitly assigned to the Securities and Futures Commission (SFC). This adjustment profoundly embodies the core principle of "same business, same risks, same regulation" that permeates Hong Kong's approach to financial innovation regulation.

Under the MSO regulatory regime, Hong Kong has established a comprehensive and detailed regulatory system:

1. Its legal foundation is the *Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO)*, providing clear legal authority for regulation;
2. Hong Kong Customs acts as the regulatory body, leveraging extensive enforcement and supervisory experience;
3. The scope of regulated activities explicitly covers core areas such as fiat currency exchange, remittance services, and cross-border fund transfers;
4. Regarding capital and financial requirements, while no rigid minimum capital threshold is set, emphasis is placed on the institution's obligation to continuously maintain adequate financial resources and positive net assets, and to strictly implement segregation and custody of client funds;
5. The compliance system requires the establishment of comprehensive AML/CFT mechanisms, including in-depth customer due diligence, ongoing risk assessment, and suspicious transaction monitoring;
6. Technical requirements mandate the deployment of secure and reliable information technology systems to ensure transaction security and data integrity;
7. Local presence requirements include establishing a Hong Kong registered legal entity, maintaining a physical management office, and ensuring senior management personnel pass stringent "fit and proper" assessments, effectively preventing shell company abuse of the system;
8. Ongoing supervision mechanisms include regular compliance reporting, combined with various regulatory tools such as on-site inspections and off-site monitoring.

This institutional arrangement makes the MSO licence a foundational access credential in Hong Kong's crypto payment sector. Any crypto payment enterprise intending to serve the Hong Kong

market and involving fiat currency flows must clear this mandatory regulatory hurdle, fully demonstrating Hong Kong's firm commitment to preventing and controlling money laundering and terrorist financing risks.

2.2.3.2 Virtual Asset Over-the-Counter Trading Licence (VA OTC)

The regulatory framework for Virtual Asset Over-the-Counter trading exhibits characteristics more adapted to financial innovation:

1. Its legal basis shifts to the *Securities and Futures Ordinance (SFO)*, signifying a profound change in regulatory logic;

2. The regulatory authority is designated as the SFC, primarily based on considerations of unified regulatory efficacy: consolidating virtual asset regulatory functions under the SFC avoids regulatory arbitrage opportunities arising from fragmented oversight and fully leverages the professional expertise and extensive experience the SFC has accumulated in virtual asset regulation;

3. The regulatory scope achieves comprehensive coverage. Any business involving "making or offering to make an agreement with another person, or inducing or attempting to induce another person to make or offer to make an agreement, for or with a view to acquiring, disposing of, subscribing for or underwriting virtual assets; or the purpose or purported purpose of which is to secure a profit or avoid a loss to any party by reference to fluctuations in the value of virtual assets" falls within the definition of VA Dealing services requiring licensing. This specifically includes:

- Traditional OTC Business Forms: Encompassing exchanges between different virtual assets and sale/purchase transactions between virtual assets and fiat currency, whether conducted through physical storefronts or online platforms;
- Innovative Business Models: Such as acting as a broker to match virtual asset trades, or providing customized, large-scale, non-public block trading services for institutional investors or high-net-worth individuals.

4. Specific regulatory standards heavily draw upon the mature regulations for Virtual Asset Trading Platforms (VATPs), establishing consistent high standards in areas such as fit and proper requirements, adequacy of financial resources, strength of AML measures, client asset protection mechanisms, and prohibition of market abuse, ensuring investors receive an equivalent level of protection whether through centralized exchanges or OTC brokerage channels.

The SFC has demonstrated an open and inclusive regulatory posture in this process, actively encouraging potential applicants with innovative business models, unique technical architectures, or optimized compliance solutions to engage in pre-application communication with the regulator.

This forward-looking dialogue mechanism helps enhance subsequent approval efficiency and reflects regulatory support for market innovation.

However, Hong Kong's current virtual asset licensing regime still faces several practical challenges. Firstly, the stringent requirement for a localized senior management team, while aiding in enforcing regulatory accountability, objectively constrains the international operational efficiency of enterprises, particularly affecting the flexibility of cross-border business deployment for global crypto payment platforms. Secondly, a single VA Dealing licence may be insufficient to fully support a robust and competitive business ecosystem. Industry practice suggests that a complete closed loop for cross-border payments or digital asset trading services often requires the coordination of multiple licences – for instance, an MSO licence handling fiat currency flows, coupled with other functional licences covering derivative services. Furthermore, for traditional brokerages or integrated financial platforms planning to expand into virtual asset services, regulatory guidance is increasingly clear: it is advisable to obtain a Type 1 (dealing in securities) regulated activity licence concurrently with the VA Dealing licence application. The regulatory logic behind this suggestion is highly prospective: the legal characterisation of a virtual asset may change dynamically based on its evolving functionality or regulatory re-classification; a token considered a non-security today might be re-classified as a security product in the future. Holding multiple licences simultaneously not only ensures business activities remain within the regulatory perimeter but also provides enterprises with ample space to adapt to future regulatory changes. Finally, against the macro-background of a globally tightening regulatory environment for crypto-assets, a key challenge for both regulators and industry participants is how Hong Kong can maintain its attractiveness and competitiveness for emerging projects and innovative enterprises while safeguarding financial stability and market integrity. This requires ongoing dialogue and balance between regulatory wisdom and market innovation.

2.2.4. Singapore

The unified digital asset regulatory framework constructed by the Monetary Authority of Singapore (MAS) through the *Payment Services Act (PS Act)* is one of the most mature and flexible regulatory models in Asia. The Digital Payment Token Service (DPT) licence targets services within Singapore, while the Digital Token Service Provider (DTSP) licence specifically governs overseas business, forming a segregated "domestic-external" regulatory structure. The new DTSP policy clears out shell companies without substantive business, emphasizing that "local registration, global service" requires licensing. This reflects the regulator's precise grasp of market segmentation and differentiated management approach based on varying risk profiles.

2.2.4.1 Digital Payment Token Service Licence (DPT)

During the 2020-2022 period, the *Payment Services Act (PS Act)* initially established the DPT regulatory framework, creating the DPT licensing system.

Key regulatory aspects of the DPT licence are as follows:

1. Regulatory Basis: Payment Services Act.
2. Applicant: Singapore-registered legal entity.
3. Capital Requirements: 1. Standard Payment Institution (SPI): Minimum paid-up capital requirement of SGD 100,000. 2. Major Payment Institution (MPI): Minimum paid-up capital requirement of SGD 250,000.
4. AML/KYC System: Comprehensive customer identity verification and transaction monitoring.
5. Technical Security: Compliance with MAS requirements for technology risk management and cybersecurity.
6. Personnel: Stringent fit and proper and qualification requirements for senior management.
7. Scope of Business: Payment and exchange services involving digital payment tokens, excluding security token trading.

The DPT licence embodies MAS's commitment to the security of digital payments and legal compliance, demonstrating a high degree of balance in reconciling innovation with risk management. By advocating regulatory dialogue and dynamic adjustments, MAS provides enterprises with growth space and flexible choices for compliance pathways.

2.2.4.2 Digital Token Service Provider Licence (DTSP)

1. Policy Background

2022: *The Financial Services and Markets Act (FSM Act)* came into effect, providing the framework for regulating digital token services, defining digital tokens, specifying the scope of regulated activities, and laying the groundwork for subsequent detailed regulatory measures.

October 2024: A consultation paper focused on "shell company" risks was released. On 4 October 2024, MAS issued a consultation paper on Digital Token Service Providers (DTSPs), proposing a series of regulatory requirements for digital token enterprises serving overseas clients, including the need to obtain a DTSP licence and fulfil obligations related to anti-money laundering and cybersecurity, with preliminary explanations on eligibility criteria for licence applications.

30 May 2025: Final Guidelines were released. On 30 May 2025, MAS published its response to the aforementioned consultation paper, confirming that the DTSP provisions would take effect formally

on 30 June 2025, further clarifying regulatory details and requirements, such as the compliance obligations of licensed entities and the specific application process, while emphasizing penalties for non-compliance.

6 June 2025: MAS Clarification. The announcement of Singapore's new DTSP regulations generated widespread attention and discussion throughout the crypto industry. On 6 June 2025, MAS issued a further clarification: 1) From 30 June 2025, DTSPs providing services solely to users located outside Singapore related to digital payment tokens and capital markets products tokens will require licensing. 2) Providers serving users within Singapore with digital payment token or capital markets product token services are already regulated under the *PS Act*, *Securities and Futures Act (SFA)*, and *Financial Advisers Act (FAA)*, and there are no changes to the business scope permitted for these licensed providers. Such providers serving Singapore users may also provide services to users outside Singapore.

Historically, Singapore was regarded by many crypto practitioners as an ideal jurisdiction for company incorporation, with its status as an international financial centre and innovation-friendly policies being highly attractive to crypto businesses registered in Singapore but operating globally. However, recent international regulatory standards (e.g., from the FATF) require Singapore to implement stricter regulatory standards for the crypto industry to prevent "regulatory arbitrage." Furthermore, several high-profile crypto company failures raised concerns that if companies registered in Singapore engage in high-risk global operations and subsequently collapse/abscond, Singapore, as the jurisdiction of incorporation, might face reputational pressure. Consequently, the MAS guidelines explicitly state that the large number of companies registered in Singapore providing digital token services to overseas users has seriously impacted Singapore's international financial reputation. The new DTSP regulations specifically target these "based in Singapore, serving the globe" crypto industry participants. The FSM Act clearly states that without a DTSP licence, an enterprise must not provide any "digital token service" to persons outside Singapore through its "place of business" in Singapore.

2. DTSP Regulatory Key Points

Regulatory Requirement: Pursuant to the FSM Act, any individual or company conducting a business of providing any digital token service in Singapore must hold a licence, unless exempted. "Digital token service" encompasses various types, including dealing in digital tokens, facilitating the exchange of digital tokens, and transferring digital tokens between digital token accounts.

No Transition Period: MAS will not provide transitional arrangements for DTSPs. Operating without a licence constitutes an offence, potentially leading to fines, deregistration, or even criminal liability. MAS provided only an initial four-week preparation period for DTSPs, refusing to grant any transition period or temporary exemption. Unlicensed entities must cease all relevant services by 30 June 2025.

Stringent Compliance Obligations: Entities holding a DTSP licence must meet a series of strict regulatory standards, including but not limited to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), cybersecurity requirements, technology risk management, client fund segregation, and audit and reporting obligations. For instance, regarding AML/CFT, measures such as KYC, customer risk assessment, transaction monitoring, and suspicious transaction reporting must be implemented. Concerning cybersecurity, enhanced system protection, data encryption, disaster recovery systems, and security audit reports are required.

Restrictions on Licensees: MAS has imposed restrictions on the operational activities of licensed digital token service providers, including prohibiting the provision of de facto payment or transmission of digital payment tokens to Singapore users without reasonable justification; and prohibiting the provision of digital token services while knowing or having reason to suspect that a customer, or a person acting on behalf of a customer, is engaged in certain specified activities.

Given that DTSP-related services are internet-based and cross-border in nature, they pose money laundering and terrorist financing risks and may increase the risk of such services being used or misused for illicit purposes, harming Singapore's reputation. In light of these risks, MAS advocates a prudent and cautious approach and will consider granting a DTSP licence under the FSM Act to applicants only in very exceptional circumstances. Notably, DTSP licence applicants must also demonstrate to MAS that they have no intention to serve Singapore users: As the purpose of the DTSP new policy is precisely to combat the "regulatory arbitrage" model of "Singapore registration, global service," the DTSP new policy explicitly stipulates that DTSP licence applicants must demonstrate to MAS that they "do not intend to carry on a business of providing digital token services in Singapore despite operating in or being formed or incorporated in Singapore."

3. Policy Impact

Tightening Regulatory Environment: Singapore, once attracting a large number of Web3 entrepreneurs and enterprises with its open and innovative regulatory environment, now signals a shift towards a more cautious and stringent regulatory stance with the implementation of the new rules. This undoubtedly imposes business adjustment pressures on Web3 industry participants and steers the entire industry towards a more compliance-oriented path.

Reshaping Industry Ecosystem: As smaller enterprises or non-compliant businesses unable to meet regulatory requirements are forced to exit the market, the Web3 industry's landscape will be reshaped. Larger enterprises with stronger financial capabilities and technical prowess to meet stringent regulatory requirements will hold a comparative advantage, potentially leading to further industry consolidation. Some small innovative enterprises may face survival difficulties.

Impact on Web3 Industry Innovation: Strict regulatory provisions may pose challenges to the innovation momentum within the Web3 industry. Some small innovative enterprises, lacking

sufficient resources and capacity to meet regulatory demands, may find their innovation constrained. Larger enterprises, under compliance pressure, might also approach innovative business expansion with increased caution. Regarding the direction of innovation, enterprises and developers may focus more on innovation within the compliance framework, exploring how to develop safer, more reliable, and efficient digital asset-related products and services while meeting regulatory requirements – for instance, enhancing blockchain technology applications in compliant areas, developing better risk management and monitoring tools – to adapt to the new regulatory environment.

2.2.5. Dubai (UAE)

Leveraging its innovative technology ecosystem and forward-looking policy framework, Dubai has rapidly emerged as a significant global hub for cryptocurrency and blockchain technology in the Middle East in recent years. Throughout this development, Dubai has progressively established a multi-layered regulatory system with clearly delineated responsibilities. Within this framework, the Dubai International Financial Centre (DIFC) operates as an independent financial free zone, with its financial activities regulated by its dedicated regulator, the Dubai Financial Services Authority (DFSA). Virtual asset activities conducted anywhere in Dubai outside the DIFC fall under the unified jurisdiction of the Virtual Assets Regulatory Authority (VARA), established in 2022. VARA's creation stems from the Dubai government's objective to foster innovation and implementation of virtual assets and blockchain technology in a safe and orderly manner by establishing a clear regulatory framework. The establishment and authority of this entity are directly based on *Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai*. This foundational law not only provides a clear legal basis and operational guidance for the issuance, trading, custody, and other related services concerning virtual assets but also, at the legislative level, demonstrates Dubai's intent to attract leading global virtual asset enterprises and projects through proactive policy support, thereby consolidating its globally forward-looking position in the emerging digital finance sector.

2.2.5.1 Dubai VARA Licence

In Dubai, any individual or company wishing to engage in virtual asset-related activities, such as cryptocurrency trading, custody, or lending, must first obtain a licence from VARA. The innovative aspect of the VARA system lies in its detailed categorization of Virtual Asset Service Provider (VASP) activities and the design of specialized licences for each category. For crypto payment enterprises, the most relevant licences are:

1. VA Transfer & Settlement Services: Encompasses the transmission and settlement of virtual assets, including the transfer of virtual assets from one entity to another or from one address to another, involving the exchange of fiat currency for virtual assets, transfers between virtual assets, and settlement.

2. VA Broker-Dealer Services: Encompasses various activities related to the buying and selling of virtual assets. This includes: arranging buy/sell orders for virtual assets between entities; accepting client orders for virtual asset transactions and facilitating the matching of transacting parties; acting as an agent for clients or providing virtual asset issuance services; and trading for the broker-dealer's own account.

VARA Licence Regulatory Key Points:

1. Licence Categories: Eight categories in total, including VA Transfer & Settlement Services, VA Broker-Dealer Services, Advisory Services, Category 1 VA Issuance, Custody Services, Exchange Services, Lending and Borrowing Services, and VA Management and Investment Services.
2. Capital Requirements: Flexibly adjusted based on risk levels.
3. Legal Entity: Requires registration in Dubai and maintenance of a local office.
4. Management Review: Detailed background and compliance qualification checks for senior management.
5. Technology and Fund Security: Segregation of client assets, robust risk controls, and comprehensive incident response mechanisms.
6. Ongoing Supervision: Regular submission of compliance reports and acceptance of on-site inspections.
7. By balancing innovation incentives with risk prevention, VARA has attracted numerous Web3 projects; however, the regulatory mechanism requires continuous refinement, particularly in cross-border regulatory cooperation and international compliance.

2.3. Crypto Payments in the Americas

2.3.1. United States

The US regulatory environment for crypto payments is characterized by its complexity and fragmentation, forming a unique dual-layer structure. Enterprises must not only comply with federal anti-money laundering regulations but also navigate a patchwork of licenses with varying requirements independently enacted by individual states. This dual regulatory system presents significant compliance challenges and costs for companies seeking to operate nationwide.

2.3.1.1 Federal Level Oversight: Bank Secrecy Act & FinCEN

At the federal level, the core regulation for crypto payment companies is the *Bank Secrecy Act (BSA)*, enforced by the Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of

the Treasury.

1. Money Services Business (MSB) Registration Requirement:

Pursuant to FinCEN guidance, companies providing payment-related services such as cryptocurrency exchange or transfer are typically considered "Money Transmitters," and thus fall within the category of "Money Services Business" (MSB). As MSBs, these companies must register with FinCEN. The registration process itself is relatively straightforward, completed by online submission of FinCEN Form 107, must be filed within 180 days of company formation, and must be renewed every two years. However, it is crucial to clarify that FinCEN MSB registration is essentially an anti-money laundering registration, confirming the company is subject to BSA regulation and corresponding compliance obligations.

2. Federal AML Program & OFAC Sanctions Compliance:

The core implication of MSB registration is that the company must establish and implement a comprehensive, effective, risk-based AML compliance program. Under the BSA, this program must include at least four core pillars (often referred to as the "Five Pillars" when including Customer Due Diligence):

- **Written Policies, Procedures, and Internal Controls:** Develop detailed Anti-Money Laundering policy documentation designed to identify, assess, and mitigate money laundering and terrorist financing risks.
- **Designated Compliance Officer:** Appoint a Compliance Officer vested with the responsibility of overseeing the day-to-day operation of the Anti-Money Laundering program.
- **Ongoing Employee Training:** Conduct regular training sessions for relevant personnel regarding their Anti-Money Laundering obligations and responsibilities.
- **Independent Review/Audit:** Perform periodic independent testing of the effectiveness of the Anti-Money Laundering program.

Additionally, MSBs must fulfil stringent reporting and recordkeeping obligations, including filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs).

Equally critical is compliance with economic sanctions programs administered by the Office of Foreign Assets Control (OFAC), requiring screening of customers and transactions.

2.3.1.2 State-Level Regulatory Patchwork: Money Transmitter Licenses (MTLs)

The operational authority is granted primarily at the state level. With limited exceptions, any company wishing to do business in the US must individually apply for and obtain a Money

Transmitter License (MTL) in each state where it plans to offer services. This is an extremely time-consuming and costly process, constituting the core legal requirement for providing crypto payment services in the US.

1. Common MTL Requirements:

While requirements vary by state, MTL applications typically involve a common set of prudential and governance standards.

Common requirements include:

- **Minimum Net Worth / Capital:** Licensees are required to maintain a prescribed minimum net worth, with amounts varying by jurisdiction from tens of thousands to millions of United States Dollars, contingent upon the scale and scope of business operations.
- **Surety Bond:** Applicants must procure a surety bond, which serves as financial security for consumer protection and safeguards user funds in the event of corporate insolvency or operational failure. The bond amount is typically correlated with the applicant's transaction volume and is subject to disparate requirements across state jurisdictions.
- **Permissible Investments:** Licensees are obligated to hold approved low-risk liquid assets, such as cash or government securities, equivalent in value to their outstanding payment obligations, thereby ensuring the safeguarding of user funds.
- **Comprehensive Background Investigations:** All control persons, directors, and executive officers of the applicant entity must submit fingerprints and undergo thorough criminal history and financial background checks conducted by both state and federal authorities, including the Federal Bureau of Investigation (FBI).
- **Exhaustive Documentation Submission:** The application materials shall generally include, without limitation, detailed business plans, audited financial statements, Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) compliance programs, information security policies, and corporate governance documents.

2. Case Study: New York's BitLicense and its Enhanced Requirements

Among the regulatory frameworks of all states, New York stands apart due to its unique dual-track system and exceptionally high regulatory standards. Entities engaging in virtual currency business activity in New York may elect to apply for either a standard Money Transmitter License (MTL) or a "BitLicense" specifically tailored for the cryptocurrency industry, issued by the New York State Department of Financial Services (DFS). Some entities, seeking operational comprehensiveness, apply for and hold both licenses concurrently.

The requirements for a BitLicense substantially exceed those of a typical MTL, establishing more stringent and specific standards for crypto payment and trading businesses across multiple dimensions:

- **Capital Requirements:** The DFS determines the requisite capital levels that a licensee must maintain on a case-by-case basis, considering the entity's business model, operational scope, and specific risk profile, rather than applying a fixed minimum standard.
- **Cybersecurity:** A BitLicense holder shall be required to comply with the pioneering cybersecurity regulations of New York State (*23 NYCRR Part 500*), which mandates the establishment and maintenance of a comprehensive cybersecurity program. Such program shall include, without limitation, the implementation of periodic risk assessments, penetration testing conducted at least annually, and vulnerability assessments performed on a quarterly basis.
- **Consumer Protection:** The regulations stipulate explicit consumer protection provisions. These include the custody of assets (requiring holders to maintain virtual currency of the same type and amount as their customer obligations), transaction receipts, procedures for handling consumer complaints, and clear disclosures regarding the risks associated with virtual currencies. These provisions are critical for end-users of payment services.
- **AML Compliance:** In addition to federal requirements, the DFS imposes more specific demands on Anti-Money Laundering (AML) programs. These include, for instance, enhanced due diligence (EDD) for high-risk customers and the implementation of effective transaction monitoring systems.

The substantial investment of costs, time, and compliance resources required to obtain a BitLicense has led many cryptocurrency companies to forgo the New York market entirely. However, this exceptionally high barrier has produced an unintended effect. The U.S. regulatory system, particularly the state-level MTL regime, has created a significant "compliance moat" within the market. To operate nationwide, an entity must commit millions of dollars in initial costs (for application fees, legal counsel, state-specific surety bonds, etc.) and expend several years navigating the license application processes across nearly 50 states. This considerable upfront investment is manageable for well-capitalized, established firms but presents a nearly insurmountable barrier for innovative startups. Consequently, this regulatory structure inherently protects large incumbent players in the market, dampening competition from new entrants and leading to a more concentrated and less dynamic market landscape. Concurrently, although New York's BitLicense applies only within a single state, it effectively functions as a federal standard-setter. Owing to the rigorous nature of its application process, particularly the in-depth scrutiny of cybersecurity and consumer protection frameworks, the successful acquisition of a BitLicense is regarded industry-wide as a premier mark of compliance certification.

2.3.2. Argentina

2.3.2.1 Cryptocurrency: Non-Legal Tender Parallel Currency

Argentina currently permits Bitcoin and certain other digital currencies to circulate as non-legal

tender parallel currencies alongside traditional fiat money. Following the election win of the Milei government, it announced the formal permission for the use of Bitcoin and other cryptocurrencies for contract settlement and payments. Individuals and businesses are allowed to freely choose their preferred payment methods. Cryptocurrencies like Bitcoin are treated as non-legal tender parallel currencies, capable of circulating concurrently with traditional currency.

2.3.2.2 Regulation of VASPs

Commencing June 2024, the Argentine National Securities Commission / Comisión Nacional de Valores (CNV) initiated a registry for Virtual Asset Service Providers (VASPs), mandating registration for all individuals and entities engaged in virtual asset-related activities. This requirement extends to entities utilizing ".ar" domain names to conduct activities in collaboration with third parties or affiliated entities in Argentina, as well as those directing advertising towards Argentine residents. Entities whose total transactional volume does not exceed 35,000 units of purchasing power (UVAs) within any one-month period are exempt from this registration obligation.

Since 2024, Argentina's Financial Intelligence Unit (UIF) has explicitly classified VASPs as "Obligated Subjects," requiring them to adhere to the UIF's regulatory framework. VASPs must comply with stringent Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) requirements equivalent to those applicable to financial institutions such as banks, trust companies, and exchanges. These obligations encompass risk assessment standards, Know-Your-Customer (KYC) protocols, and reporting requirements, among others.

To provide crypto payment-related services in Argentina, it is necessary to establish a local legal entity in Argentina in accordance with VASP registration requirements. This process includes the appointment of a designated compliance officer and the development of a formal, comprehensive AML/CFT program. This program must delineate the specific nature of the services offered, projected transaction volumes, target markets, and detailed operational procedures.

2.3.2.3 PSP License: Limitations of Traditional Payment Licenses

The Central Bank of the Argentine Republic / Banco Central de la República Argentina (BCRA) bears primary regulatory responsibility for traditional Payment Service Providers (PSPs) that offer payment accounts, including conventional fintech companies providing electronic wallet and fund transfer services. Upon obtaining authorization, PSPs are permitted to engage in the following services:

- The establishment and administration of payment accounts;
- The execution of payment operations, including transmitting, receiving, and remitting funds;
- The issuance of payment instruments;
- Activities related to payment card issuance, acquisition, and processing;

- The provision of electronic funds transfer services;
- The operation of payment gateway services.

Historically, BCRA-imposed restrictions limited licensed PSPs from assisting clients with transactions involving non-regulated digital assets like crypto-assets. Post-April 2025, following the removal of forex controls on the US dollar, indications suggest these restrictions are being relaxed. The PSP license, as a traditional fiat payment license, may now potentially permit licensees to conduct services like transfer, exchange, and trading of cryptocurrencies under newly implemented norms.

2.3.3. Brazil

2.3.3.1 PSP License under BCB Regulation

The Brazilian payment system comprises two core components: Financial Market Infrastructures (FMIs) and Payment Schemes. The Payment Schemes component encompasses the comprehensive set of rules and procedures governing the provision of specific payment services to the public, such as Pix and credit card operations. Beyond the schemes themselves, this component includes scheme owners and participants, which may be financial institutions or payment institutions.

The Central Bank of Brazil / Banco Central do Brasil (BCB) is the competent authority for issuing Payment Service Provider (PSP) licenses within Brazil. Activities permitted under a PSP license include:

- Withdrawal of funds from payment accounts;
- Execution of payment instructions related to specific payment services;
- Management of payment accounts;
- Issuance and provision of payment instruments; and
- Funds transfer and exchange.

Pursuant to BCB regulatory requirements, PSP licenses are granted exclusively to legal entities constituted under Brazilian law. Applicants must develop an overall business plan and organizational structure compliant with BCB requirements, establish defined roles, responsibilities, and operational procedures in accordance with PSP regulations, and provide detailed descriptions of existing technology and security measures, as well as AML/KYC policies and procedures during the application process. The BCB does not mandate a physical registered office address; consequently, PSP applicants may successfully obtain a license utilizing a virtual office address.

The BCB imposes differentiated financial requirements for PSP license applications based on annual transaction volume. The minimum capital requirement for applicants is generally BRL 2-3 million. Should the annual transaction volume exceed BRL 100 million, financial metrics are determined based on a floating scale. The BCB retains the authority to assess and adjust capital requirements based on the specific risk profile of individual cases.

2.3.3.2 VASP Licensing under BCB Regulation

Under Brazil's relevant legislative framework for virtual assets, the Central Bank of Brazil / Banco Central do Brasil (BCB) is responsible for regulating virtual assets and Virtual Asset Service Providers (VASPs). The BCB collaborates with other regulatory bodies, such as the Brazilian Securities and Exchange Commission / Comissão de Valores Mobiliários (CVM), in formulating virtual asset regulatory policies and plans to develop internal regulatory plans addressing payments and foreign exchange involving stablecoins. Payment services involving virtual assets are included within the scope of services provided by VASPs. It has been disclosed that the final standards for VASP authorization by the BCB are anticipated by the end of 2025, with the BCB potentially commencing authorization of VASP licenses in 2026.

2.3.3.3 Crypto Payments and the Pix System in Brazil

In 2020, the BCB launched the Pix instant payment system, whose speed, ease of use, and low cost have reshaped the country's digital financial ecosystem. Unlike credit and debit cards, Pix is free for individuals and incurs minimal fees for businesses, with transactions settling within seconds compared to hours or days for traditional bank transfers. In 2024 alone, Pix processed approximately 64 billion transactions, with a total value of approximately US$4.6 trillion.

Currently, Brazil has not authorized direct payment services using cryptocurrencies. Most crypto payment companies integrate into the Pix instant payment system through partnerships with local acquirers. This enables users to make payments directly using self-custody cryptocurrencies by scanning any Pix QR code. The transaction process automatically converts the selected crypto-asset into Brazilian Reais at the moment of payment, without requiring pre-conversion or third-party services.

2.4. Crypto Payments in Africa

Driven by significant growth in the crypto-asset market, transaction volumes by individuals and enterprises across Africa have surged in recent years. From peer-to-peer trading hubs in Nigeria and Kenya to blockchain-based land registry systems in Ghana, the continent is actively embracing crypto-assets. With approximately 350 million unbanked adults in Sub-Saharan Africa, coupled with high transaction costs and limited access to foreign currency, the region presents fertile ground for crypto-asset adoption. While some African nations have introduced forward-looking frameworks to encourage innovation, others maintain a cautious stance, issuing warnings or outright prohibitions on cryptocurrency use.

2.4.1. Nigeria

Among emerging market economies, Nigeria was an early adopter of cryptocurrency. Between 2016 and 2020, Nigerians increasingly turned to Bitcoin and other digital assets to circumvent foreign exchange restrictions and inflation. According to the 2023 Global Crypto Adoption Index of Chainalysis, Nigeria ranked among the top three countries globally for crypto-asset adoption. Nigeria currently maintains the Naira as its official currency; no crypto-asset possesses official currency or legal tender status. Banks and other licensed financial institutions are prohibited from holding assets or liabilities denominated in or related to crypto-assets. Furthermore, crypto-assets cannot be utilized as loan collateral.

2.4.1.1 VASP Licensing Framework

Pursuant to "A Framework on Accelerated Regulatory Incubation Program (ARIP) for the Onboarding of Virtual Assets Service Providers (VASPs) and other Digital Investments Service Providers (DISPs)" issued by the Securities and Exchange Commission (SEC) of Nigeria, the SEC of Nigeria launched the ARIP in June 2024. This program aims to facilitate the registration of cryptocurrency startups and operators within a sandbox-like environment. It allows VASPs to obtain a provisional permit, enabling the Commission to assess digital asset business models to ensure VASPs possess appropriate governance structures and implement adequate risk mitigation measures concerning investor protection and anti-money laundering requirements before full-market deployment.

- ARIP approval constitutes an approval-in-principle, valid only for a specified period not exceeding 12 months.
- Approved VASPs must, upon expiry of the approval-in-principle, transition to full registration by complying with all applicable registration requirements or other stipulations the Commission may prescribe.

Under the revised rules, VASPs may apply to the Nigerian SEC for registration under one of the following functions: Digital Asset Offering Platform (DAOP), Digital Asset Exchange (DAX), Digital Asset Custodian (DAC), or Digital Asset Intermediary (DAI). A VASP may apply for only one of the listed functions; combining two or more functions is prohibited. Financial requirements for payment-related functions are as follows:

1. Digital Asset Exchange (DAX)

- OTC Model: Minimum Capital - ₦1 billion; Registration Fee - ₦100 million; Processing Fee - ₦10 million.
- Digital Brokerage Model: Minimum Capital - ₦1 billion; Registration Fee - ₦1 billion; Processing Fee - ₦1 billion.

2. Digital Asset Intermediary (DAI) - Broker/Dealer:** Minimum Capital - ₦500 million; Registration Fee - ₦50 million; Processing Fee - ₦5 million.

Where an applicant is regulated by another primary regulator, it must submit a "No Objection" or approval letter from the relevant primary regulator with its application.

2.4.1.2 CBN Bank Account Compliance Requirements for VASPs

Nigerian banks were previously prohibited from providing deposit accounts and other financial services to cryptocurrency exchanges or related companies. However, according to a circular issued by the Central Bank of Nigeria (CBN) in December 2023, VASPs licensed by the SEC of Nigeria are permitted to maintain local bank accounts.

Per the CBN circular, where a Nigerian bank opens an account for a VASP, such action requires approval from senior management at the level of Assistant General Manager (AGM) or above. The VASP must submit its own AML/CFT/CPF policies to the bank. Most notably, the use of the designated bank account is restricted as follows: the account may only be used for virtual/digital asset transactions and for no other purpose; cash withdrawals from the account are prohibited; third-party cheques may not be cleared through the account unless for the settlement of virtual/digital asset transactions, with settlement to be effected via transfer to another designated account, and withdrawals permitted only via manager's cheque or transfer to an account; the account shall not be used for concessionary arrangements with financial institutions. Permissible activities for financial institutions in dealing with VASPs are limited to the following: opening designated accounts; providing designated settlement accounts and settlement services; serving as a channel for foreign exchange flows and transactions; and other activities the Central Bank may permit from time to time.

2.4.2. South Africa

2.4.2.1 South African Crypto Asset Regulation

Under the *Financial Advisory and Intermediary Services (FAIS) Act*, crypto assets are classified as financial products in South Africa, although the South African Reserve Bank has clarified that they are not legal tender. As one of the few African nations implementing suitability-based regulation for the crypto asset industry, the Financial Sector Conduct Authority (FSCA) primarily approves relevant companies to conduct designated services through the issuance of Crypto Asset Service Provider (CASP) licenses.

2.4.2.2 CASP License Application Requirements

Applicants for a Crypto Asset Service Provider (CASP) license from the South African Financial Sector Conduct Authority (FSCA) must constitute a legal entity registered in South Africa (such as a private limited company), or an institution registered offshore but maintaining a fixed place of operations

within South Africa. Where the applicant is a foreign company conducting business in South Africa (including providing services as a CASP), it must register as an "external company" under the provisions of *the Companies Act* within twenty business days of commencing operations for the first time in South Africa, and must maintain at least one office within the Republic. All entities providing "advice" or "intermediary services" in relation to crypto assets are required to obtain authorization from the FSCA. This regulatory requirement implies that exchanges, wallet providers, crypto payment gateways, and similar service providers are obligated to apply for the requisite license.

The application fees for a South African CASP license are comparatively modest and are categorized according to license type, including Financial Services Provider (FSP), Discretionary FSP, Hedge Fund FSP, Administrative FSP, and Assistant FSP, among others. With the exception of the Administrative FSP, which carries an application fee of approximately US$3,000, the application fees for other FSP categories are relatively low. The standard application processing period is approximately six months or longer.

2.4.3. Ghana

Ghana has emerged as one of Africa's most active nations in terms of cryptocurrency interest and ownership. According to the 2024 State of Crypto: Africa, over 900,000 Ghanaians – representing approximately 3.01% of the country's population – hold at least one type of cryptocurrency. Amidst rapid depreciation of Ghana's official currency and the high costs associated with maintaining foreign accounts, cryptocurrencies have gained widespread popularity among Ghanaians for savings, payments and other purposes. For many Ghanaians, stablecoins offer a means of storing value in an inflationary environment. Compared to the official currency, which carries significant depreciation risks, stablecoins effectively preserve the purchasing power of local currency.

2.4.3.1 Ghana's Cryptocurrency Regulatory Framework

Currently, Ghana has not formally enacted any specialized legislation governing cryptocurrencies. The Bank of Ghana (BOG) has issued several circulars clarifying that cryptocurrencies are not recognized as legal tender within the country, no existing laws regulate the cryptocurrency market, and participants engaging in transactions assume all associated risks. In August 2024, the Bank of Ghana (BOG) published draft digital asset guidelines requiring risk disclosures, strict implementation of anti-money laundering and counter-terrorist financing controls, and the establishment of a regulatory sandbox to foster innovation while protecting consumers. Under these draft guidelines, all Virtual Asset Service Providers (VASPs) must obtain licenses corresponding to their specific products and services. Entities failing to complete registration within the stipulated timeframe will be deemed to be operating illegally.

2.4.3.2 Ghana Payment License PFTSP

The Bank of Ghana (BOG) has established a separate licensing regime for Payment and Financial Technology Service Providers (PFTSPs). The Bank of Ghana (BOG) notes that PFTSPs typically play a critical role across the financial service delivery value chain through partnerships with licensed PSPs, banks, etc., acting as operational extensions of regulated entities. Services provided by PFTSPs include, but are not limited to:

- Digital product development, delivery, and support services for activities including payments, savings, insurance, investment, and loyalty programs;
- Credit score predictive analytics;
- Centralized AML/CFT platforms;
- Fraud control services;
- KYC and CDD verification services.

Pursuant to Bank of Ghana (BOG)'s requirements, entities providing services falling under the PFTSP category must submit a license application to the Bank of Ghana (BOG). PFTSPs are mandated to obtain ISO 27001 certification, develop IT security policies and risk management frameworks, and comply with relevant data protection and consumer protection laws and regulations.

After gaining an in-depth understanding of the application requirements, regulatory frameworks, and compliance standards for crypto payment licenses across different countries, it becomes clear that both licensed and unlicensed institutions face a common challenge: how to effectively identify and prevent the risk of platforms being infiltrated by illicit funds. As demonstrated by cases such as BitPay's $507,000 fine for failing to block sanctioned addresses and Coinbase's $50 million penalty for failing to report suspicious transactions in a timely manner, merely obtaining a license is far from sufficient. The core of compliant operations lies in establishing a comprehensive risk identification and monitoring system.

A key question repeatedly emphasized by regulatory authorities during license approval and routine supervision is: how can we ensure that crypto payment platforms are not exploited for criminal activities such as money laundering, terrorist financing, and sanctions evasion? This directly involves the identification and prevention of on-chain "dirty money." To meet FATF guidance and regulatory requirements across jurisdictions, crypto payment service providers must develop a deep understanding of the characteristics, sources, and flow patterns of illicit funds on-chain.

Therefore, building upon the legal framework of license compliance, Chapter 3 will lead readers into an in-depth exploration of the world of on-chain dirty money, systematically analyzing the characteristics of various types of illicit funds, including high-risk entities such as hacks, scams, ransomware, and darknet markets, as well as their behavioral patterns on the blockchain, providing a technical foundation for establishing an effective risk identification and prevention system.

Chapter 3 Typologies of On-Chain Illicit Funds

While blockchain enables trustless transactions, it also leaves indelible digital trails that reveal its use in serious criminal activity. These trails—known as on-chain illicit funds—are not abstract risk indicators but real-world manifestations of harm, often linked to terrorism financing, child exploitation, hacking, phishing, darknet markets, and ransomware.

An effective AML/CFT framework must begin with a fundamental understanding of these illicit financial flows. Only then can risk be promptly identified and effectively intercepted. This chapter provides a detailed breakdown of the primary categories of on-chain illicit funds to support the development of precise and efficient detection strategies.

3.1. Terrorist Financing

Definition

Terrorist financing refers to any person or organization that directly or indirectly, unlawfully and willfully, provides or collects funds with the intent or knowledge that they will be used, in whole or in part, to carry out terrorist acts.

Sanctioned entities refer to individuals, groups, corporations, or governments listed by international organizations (e.g., the UN) or national authorities (e.g., OFAC, U.S.) as subjects of financial and trade restrictions in response to threats to national security, foreign policy, or economic stability.

In the blockchain, both categories of actors exploit cryptocurrencies for the following purposes:

- **Fundraising**: Soliciting donations via social media or dark web platforms, leveraging cryptocurrency's pseudonymity to attract supporters.
- **Funds transfer and storage**: Converting illicit proceeds from diverse sources—including the traditional financial system—into cryptocurrencies to evade surveillance and enable cross-border movement and preservation of value.
- **Procurement and operations**: Using cryptocurrencies to purchase weapons, equipment, or propaganda materials from black markets or vendors accepting crypto payments to support daily operations or planned attacks.

Although blockchain transactions are public, their pseudonymous nature—where addresses are not directly tied to identities—poses significant challenges for law enforcement attempting to attribute addresses to real-world actors.

FATF has classified terrorist financing as a Critical-level risk indicator, with countries such as North Korea, Iran, and Myanmar being placed on the blacklist. We have provided a detailed analysis of relevant international sanctions lists on the BlockSec official account, which can be found in Appendix 7.2.

Emerging Trend

Unlike high-profile attacks such as hacking or ransomware, terrorist financing tends to involve small, fragmented transactions, making detection via on-chain data alone extremely difficult. Without off-chain intelligence, such transactions are often indistinguishable from legitimate ones. According to public blockchain monitoring data, sanctioned entities collectively received approximately **USD 16.2 billion** in crypto assets in 2024.

Take **Hamas** as an example. The group—especially its military wing, the Izz ad-Din al-Qassam Brigades—was among the first to experiment with cryptocurrency-based fundraising. (This discussion is strictly technical in nature and does not imply any political position by BlockSec.)

The group's on-chain fundraising patterns evolved across three stages:

- **2019 and earlier (Static Address Stage)**:
  Hamas published a single Bitcoin address on its website to receive global donations. This fixed address was quickly linked by law enforcement to a U.S. exchange and seized due to lack of obfuscation.
- **2019–2021 (Single-Use Address Strategy)**:
  Hamas began generating a unique Bitcoin address for each donor (i.e., an "address diversification" tactic), storing funds in non-custodial wallets, significantly increasing traceability complexity.
- **Post-2021 (Semi-Public Evasion Phase)**:
  In April 2023, facing tightening global oversight, Hamas publicly declared it would stop accepting crypto donations due to "concerns for donor safety." However, blockchain intelligence platforms revealed that operations continued via dynamic addresses shared in Telegram groups and pro-Hamas media like "Gaza Now," with more than 17 donation addresses in use.

Money Laundering Techniques

To obfuscate fund origins, break transactional linkages, and eventually convert cryptocurrency into fiat, terrorist organizations and sanctioned entities employ a multi-layered laundering strategy:

- **Layering via wallet hops**: Funds pass through dozens or hundreds of intermediary wallets in small increments, complicating tracing.

- **Mixers**: Services that pool users' funds and redistribute them, severing the link between source and destination. Some mixers (e.g., Tornado Cash) have been designated "primary money laundering concerns" by the U.S. Treasury.
- **Privacy coins**: Cryptocurrencies like Monero or Zcash, which conceal sender, recipient, and transaction amount by design.
- **Chain-hopping**: Moving funds across blockchains (e.g., Ethereum to Bitcoin) to fragment the audit trail across incompatible ledgers.
- **Exchanges**: Launderers often use exchanges with weak or nonexistent KYC/AML protocols (e.g., instant-swap platforms like ChangeNOW) in lax jurisdictions to convert funds.

A typical laundering path might look like:

Donor → Initial receiving address → Multiple intermediary wallets / chain-hopping → Mixer / privacy coins → Exchange → OTC broker / shell company → Fiat conversion into traditional financial system.

Case Study: Israel–Iran Conflict Fundraising

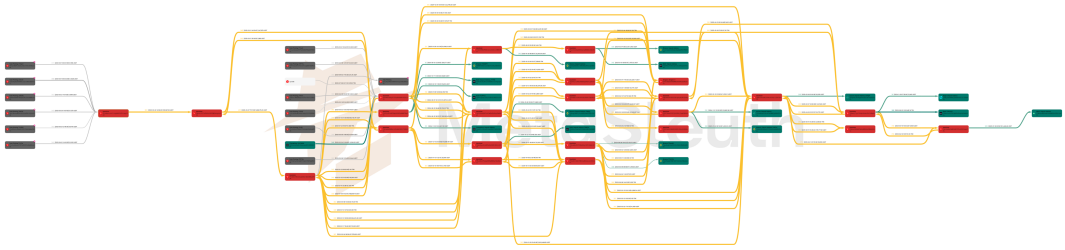
Between **June 13–30, 2025**, amid heightened hostilities between Israel and Iran, **Tether froze 151 addresses**. We analyzed administrative seizure orders issued by Israel's **National Bureau for Counter Terror Financing (NBCTF)**, using them as a representative sample to assess terrorist-linked USDT transactions.

- **Timing**: Only one new seizure order was issued after the June 13 escalation, dated **June 26**. The prior order was from **June 8**, indicating a delay in enforcement during geopolitical tensions.

- **Targeted Organizations**: Since October 7, 2024, NBCTF issued eight orders—four of which explicitly mention **Hamas**; the latest names **Iran** for the first time.

- **Assets Seized**:

  - 76 USDT (TRON) addresses
  - 16 Bitcoin addresses
  - 2 Ethereum addresses
  - 641 Binance accounts
  - 8 OKX accounts

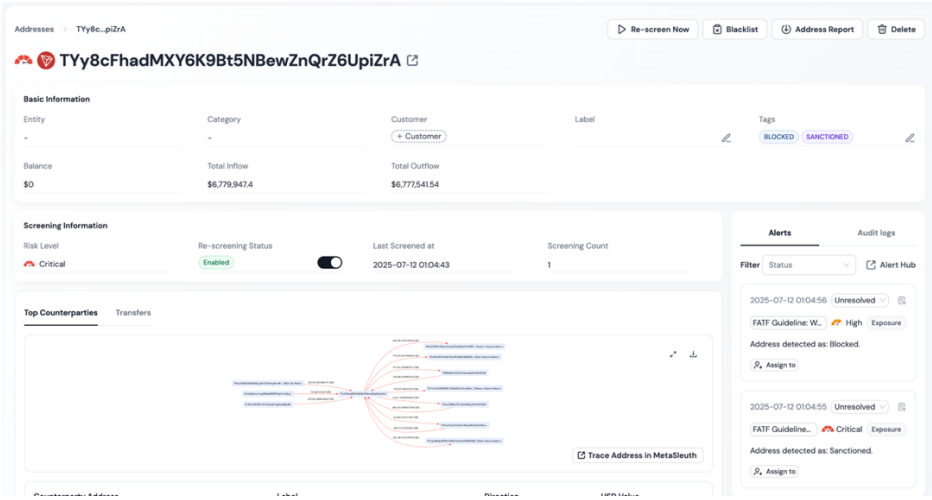


[Figure 2.1.4 - NBCTF Seized Address Map]

Using **MetaSleuth**, BlockSec's on-chain investigation platform, we traced fund sources and destinations. We found that some exchanges appeared at both ends of the transaction graph—as sources (via hot wallets) and destinations (via deposit addresses)—highlighting their central role in the laundering process.

Compliance Alert

Weak execution of AML/CFT protocols and delays in asset freezes may allow illicit transfers to occur before enforcement actions take effect. We recommend stronger mechanisms for monitoring, detection, and interdiction to proactively mitigate these risks. All addresses in this case have already been flagged by **Phalcon Compliance**, our compliance monitoring product.



[Figure 2.1.5 – Phalcon Compliance Alert Triggered by Israel–Iran Related Addresses]

3.2. Child Sexual Abuse Material (CSAM)

Definition and Connection to Cryptocurrency

Child Sexual Abuse Material (CSAM) refers to content that depicts the sexual abuse or exploitation of minors. In the context of cryptocurrencies, this term specifically refers to the use of digital assets by offenders to purchase, distribute, or monetize such illegal materials. Cryptocurrencies' pseudonymity and decentralized nature have been leveraged to support CSAM-related activities in the following ways:

- **Obscured transaction medium**: CSAM transactions often occur in the dark web or private forums, escaping routine monitoring.
- **Complex on-chain patterns**: Funds are transferred through intricate paths, complicating real-time identification and intervention.

Alarming Trends

In February 2024, the **Financial Crimes Enforcement Network (FinCEN)** released a **Financial Trend Analysis** highlighting the significant rise in cryptocurrency-related **Online Child Sexual Exploitation (OCSE)** and **human trafficking** activities:

- **Exponential report growth**: BSA filings related to such activities increased from **336 in 2020** to **1,975 in 2021**, nearly a fivefold surge.
- **Larger transaction volumes**: CVC (Convertible Virtual Currency) transactions related to CSAM rose from **USD 133 million in 2020** to **USD 278 million in 2021**.
- **Strong CSAM linkage**: 95% of the CVC-related reports were tied to CSAM or human trafficking-related CSAM, underscoring the central role CSAM plays in these illegal markets.

Case Study: Taiwan's "Creative Private Room" Forum

The **"Creative Private Room"** was once the largest illegal adult content marketplace in Taiwan, notorious for its sale of CSAM. The forum's operational and payment methods offer textbook examples of blockchain-enabled CSAM financing:

- **Forum persistence & crypto adoption**:

After being shut down in 2021, the forum re-emerged under a new domain and began accepting **USDT (Tether)** to enhance transaction anonymity and facilitate cross-border payments.
In 2024, it returned to public attention after a Taiwanese celebrity was exposed as a VIP member.

- **On-chain payment addresses & volumes**:

Intelligence reports revealed that between November 2021 and May 2024, the forum used **four TRON addresses**, collecting a total of approximately **USD 896,000 in USDT**.

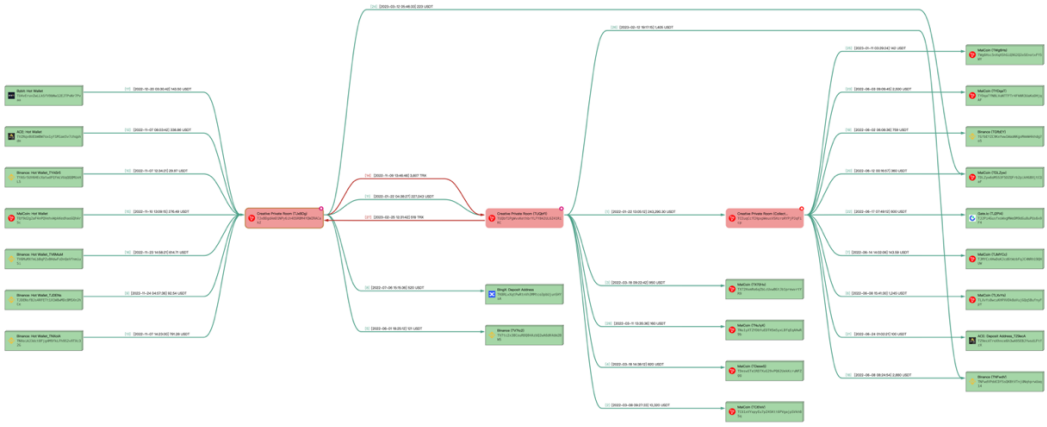
- **Money flow typology**:

The forum's flow pattern followed a classic structure:
"Small-value deposits → layered laundering → aggregation → redistribution to exchanges."
For example, examining address **TJxBDgdAmD1NPy6ih4E6RBM4YQWZRACakZ**, we observe:

  - **Inbound flow**:

Users transferred funds from exchanges, often directly or via a single intermediary, in small increments consistent with membership payments.

  - **Outbound flow**:
    - Funds moved first to a primary aggregation address for consolidation and partial disbursement to content providers.
    - They were then sent to a second aggregation layer for further obfuscation.
    - Finally, funds were split and deposited into multiple exchange accounts (e.g., Binance, MaiCoin) for conversion and cash-out.



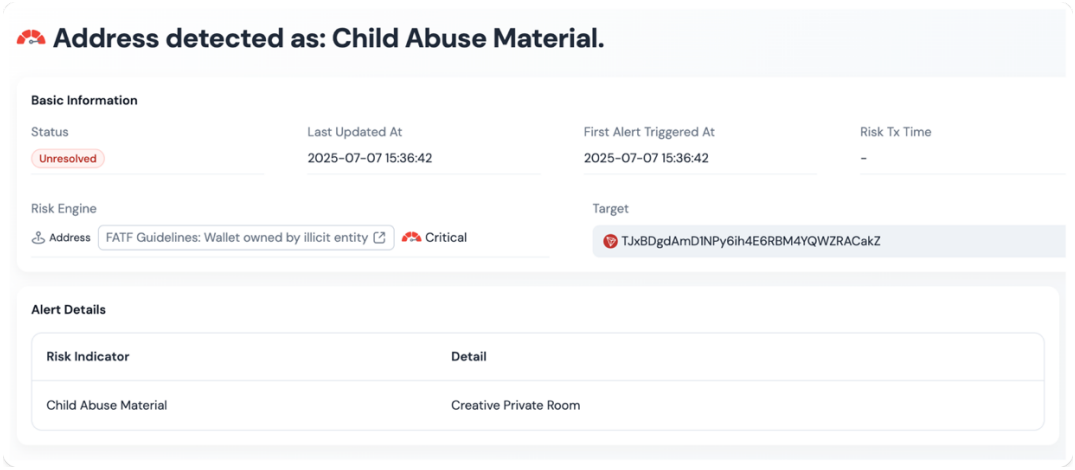
[See Figure 2.2.3 – "Creative Private Room" Flow Map (Address TJxBD...)]

Compliance Alert

Transactions linked to CSAM—especially those involving USDT addresses used for payment or dissemination—represent **the highest level of AML/CFT risk**. Service providers must:

- Deploy **Know Your Address (KYA)** systems to apply high-risk labels to relevant addresses.
- Utilize **Know Your Transaction (KYT)** tools to identify laundering patterns, such as "high-frequency micro-deposits → layered transfers → cross-chain withdrawals."

Upon detection of addresses or behavioral traits indicative of CSAM activity, platforms must immediately activate freezing and blocking protocols to prevent misuse of services for dissemination or monetization.



[Figure 2.2.4 – Phalcon Compliance Alert for CSAM-Linked Addresses]

3.3. DeFi Attacks

Definition

The rise of decentralized finance (DeFi) has attracted not only capital and innovation but also a wave of opportunistic attackers. **Attacking incidents** refer to the unauthorized acquisition of crypto assets through exploitation of vulnerabilities in on-chain or off-chain infrastructure, such as smart contracts, blockchain nodes, exchange applications, or wallet software.

Common attack vectors include:

- **Smart contract exploits**: Leveraging logic flaws or coding bugs to drain funds.
- **Price manipulation**: Tampering with price oracles to create artificial arbitrage opportunities.
- **Malicious governance proposals**: Submitting or influencing governance votes to extract funds directly or indirectly.
- **Private key theft**: Gaining access to critical accounts or contract admin keys via 0-day exploits, network intrusions, or social engineering.

Funds obtained through such attacks are deemed **illicit on-chain proceeds**, and hackers typically attempt to conceal their origins and evade tracing through obfuscation techniques.

Evolving Threats

Despite the use of professional auditing firms prior to deployment, DeFi protocols remain susceptible to novel attack techniques and an expanding attack surface. Even top-tier protocols with high **Total Value Locked (TVL)** and multiple audit rounds have not been immune. Notable incidents include:

- In **2023**, the stablecoin DEX **Curve** and **Balancer** were both exploited, with Curve losing approximately **USD 60 million**.
- In **February 2025**, centralized exchange **Bybit** suffered one of the largest Web3 heists to date, with nearly **USD 1.5 billion** stolen from a Safe multisig wallet.

According to industry data:

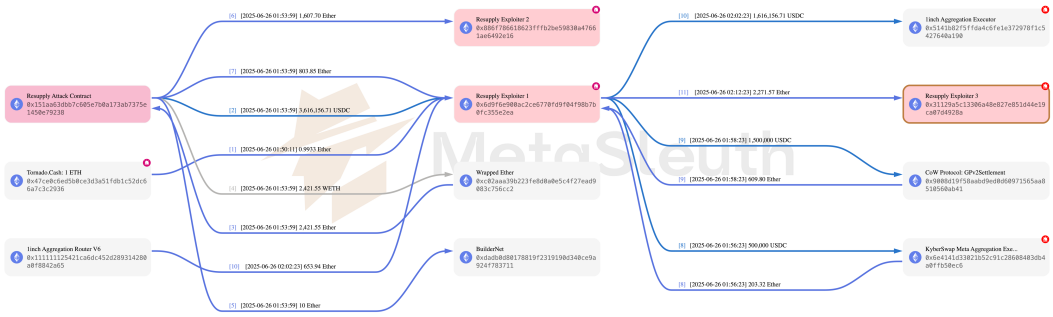
- **2023** saw over 70 on-chain attacks resulting in losses exceeding **USD 100,000** each, totaling over **USD 540 million**.
- **2024** witnessed 84 such incidents, with total losses of approximately **USD 490 million**.

Case Study: Resupply Attack

On **June 26, 2025**, **Resupply**, a stablecoin protocol within the Curve ecosystem, was exploited on Ethereum mainnet, resulting in the loss of approximately **USD 10 million**.

- **Root cause**: A flaw in Resupply's price oracle mechanism enabled a **donation attack** targeting a low-liquidity market.
- **Exploit mechanics**: The attacker manipulated the price of Resupply's stablecoin **reUSD** to near-zero, bypassing health checks on borrowed positions and draining assets via over-borrowing.

Using **MetaSleuth**, we reconstructed the attacker's fund flow:



[See Figure 2.3.3 – Resupply Attacker Fund Flow Analysis]

- **Step 1: Attack Preparation**

The attacker funneled **1 ETH** via **Tornado Cash** into a clean account (Account 1), concealing the origin of funds.

- **Step 2: Execution**

During the attack, the attacker paid a **10 ETH** miner tip to the block builder (**BuilderNet**) to prioritize the malicious transaction.

- **Step 3: Distribution**

Proceeds in **USDC** and **ETH** were split into three parts and sent to related accounts to reduce traceability.

- **Step 4: Laundering**

USDC was swapped to ETH across **1inch**, **Cow Protocol**, and **KyberSwap**, thereby masking the exit route.

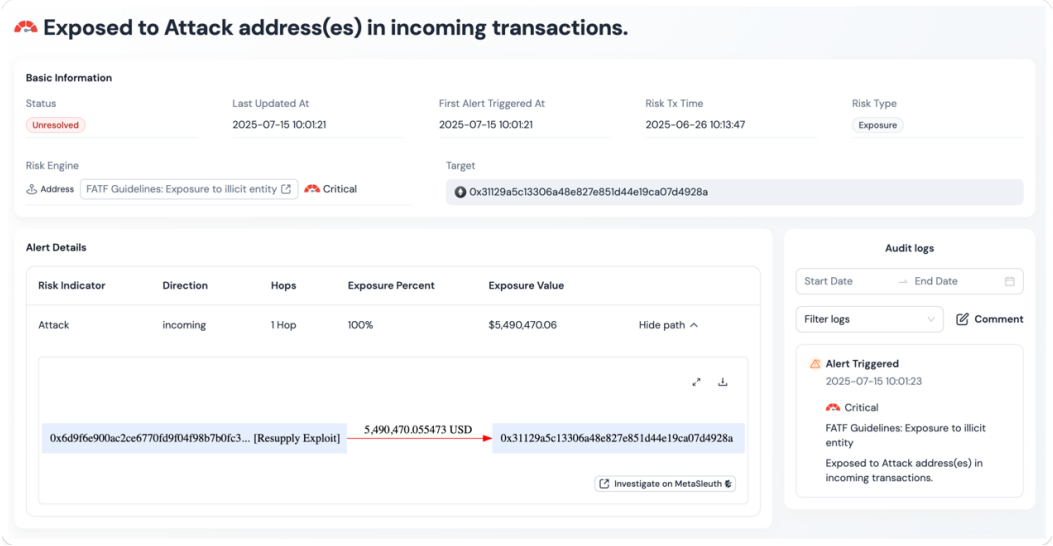
Compliance Alert

As attack involves unauthorized and illegal asset acquisition, the associated fund flows constitute **high-priority risk categories** under AML/CFT frameworks.

Service providers should:

- Monitor high-risk addresses and smart contracts in real time using **KYA/KYT** systems.
- Flag and isolate transactions linked to known exploit activity.
- Prevent illicit funds from entering legitimate financial pipelines.

Incorporating threat intelligence (e.g., public disclosures of attack vectors and associated addresses) into dynamic risk models is critical for ensuring regulatory compliance and ecosystem stability.



[Figure 2.3.4 – Phalcon Compliance Alert for Hacking-Linked Addresses]

3.4. Phishing Attacks

Common Types of On-Chain Phishing

With the rapid expansion of blockchain and DeFi ecosystems, **phishing transactions** have surged, resulting in substantial user losses. Based on our observations, on-chain phishing typically falls into the following four categories:

1. **Direct Token Transfer Phishing**

Attackers trick users into signing transactions that directly transfer native tokens (e.g., ETH) or ERC-20/ERC-721 tokens to wallets under their control.

Common tactics include impersonating legitimate airdrops, reward campaigns, or urgent security notices, with messages like “Claim Rewards” or “Security Update” prompting unsuspecting users to approve malicious transfers.

2. **Approval Phishing**

The ERC-20 approval mechanism allows users to grant smart contracts permission to transfer their tokens.
Phishing contracts disguise themselves as legitimate DeFi operations (e.g., swaps or liquidity provision), luring users to unknowingly authorize attackers. Once granted, approvals can be exploited without further user interaction to drain tokens.

3. **Address Poisoning**

Attackers send zero-amount or small-value transfers from an address that closely resembles the user's own address, thereby inserting a fake address into the transaction history.
When users later copy-paste from prior transactions, they may inadvertently send funds to the attacker's lookalike address.

4. **NFT Zero-Price Listings**

In NFT markets, sellers usually sign off-chain sell orders specifying price and sale intent.
Phishers manipulate this by tricking users into signing orders with an extremely low or zero sale price. These orders are then submitted to platforms like OpenSea, allowing attackers to acquire valuable NFTs for free.

Due to the complexity of NFT signatures, users often struggle to detect such exploits.

Case Studies: X Account, Discord Server, and Website Compromises

Phishing campaigns often hijack the visibility and trust of well-known projects or influencers by compromising their official communication channels. Here are notable examples:

- **Case 1**: On **May 26, 2023**, the X (Twitter) account of **Steve Aoki** was hacked and used to post a phishing link. Analysis revealed a **SIM swap** attack: the attacker used social engineering and personal data to trick the telecom provider into porting the victim's number to a new SIM under attacker control, enabling account takeover.

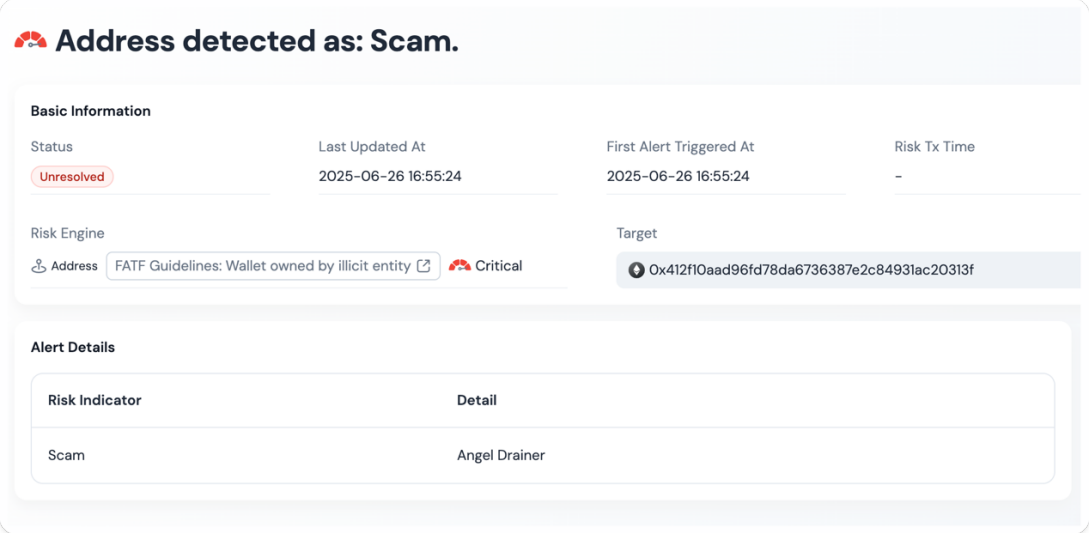
- **Case 2**: On **May 31, 2023**, the **Pika Protocol** Discord server was breached.
  The attacker posted phishing links in official channels. Investigation showed that an admin visited a spoofed website containing malicious JavaScript, which was triggered by simple UI interactions (e.g., clicking a button or saving a bookmark), resulting in Discord token theft and unauthorized server control.

- **Case 3**: On **October 6, 2023**, **Galxe's** official website was redirected to a phishing site.
  An impersonator posing as a Galxe representative submitted forged documents to the domain registrar, bypassing security checks and gaining unauthorized access to DNS settings. The phishing site was then deployed on the official domain, deceiving users into signing malicious transactions.

Compliance Alert

On-chain phishing exhibits clear behavioral patterns. Platforms should:

- Leverage **KYA (Know Your Address)** systems to preemptively tag known phishing deployer addresses.
- Immediately block deposit, bridge, and withdrawal permissions for flagged addresses.
- Implement transaction-level screening to prevent platform infrastructure from being abused to launder phishing proceeds or facilitate scam monetization.



[Figure 2.4.3 – Phalcon Compliance Alert for Phishing-Linked Addresses]

3.5. Darknet Transactions

Definition and Context

Beyond the familiar **Surface Web** and the less-visible **Deep Web**, the **Dark Web** is an even more concealed part of the Internet, accessible only through specialized tools such as **Tor**, **I2P**, or **Freenet**. These technologies rely on anonymous communication protocols designed to obscure users' geolocation, identities, and server origins. While the dark web was originally intended to safeguard the privacy of journalists and dissidents under authoritarian regimes, its anonymity has since attracted widespread criminal activity.

Over time, the dark web has evolved into a mature, well-organized black market ecosystem offering virtually every category of illicit goods and services. For example, **Silk Road**, launched in 2011, was the first large-scale darknet drug marketplace. Despite being shut down by the FBI in 2013, many successors—such as **Agora**, **AlphaBay**, **Hydra**, and **Archetyp**—have emerged with even greater functionality and scale.

Today's darknet platforms typically emulate full-featured e-commerce websites with search engines, item directories, user reviews, support teams, automated escrow, anonymous messaging, and integrated crypto payment gateways.

Popular illicit trade categories include:

- Narcotics (e.g., fentanyl, cocaine, ecstasy)
- Firearms and ammunition
- Forged IDs and passports
- Stolen financial credentials (credit cards, bank accounts)
- Hacking tools and remote access malware
- Ransomware-as-a-Service (RaaS)
- Large-scale money laundering networks

Nearly all payments on the dark web are settled in cryptocurrencies. **Bitcoin** and **stablecoins** like **USDT** have become integral to the underground economy.

Cryptocurrencies are foundational to darknet commerce because they:

- Eliminate dependence on traditional finance
- Allow pseudonymous, global transfers
- Do not require identity verification

While **Bitcoin** was initially dominant, its traceability and volatility prompted a shift toward stablecoins like **USDT**, valued for:

- **Price stability**
- **High liquidity and transaction speed**
- **Laxer regulatory scrutiny**

Some darknet vendors adopt **escrow payment models**, where buyers deposit USDT into platform-controlled wallets. Only after successful delivery is the payment released—creating a false “trust” mechanism that also enables fraud. In laundering schemes, USDT’s stability and wide acceptance make it the preferred vehicle for transforming illicit gains into usable funds.

Case Study: Telegram-Based “Haowang Guarantee” Laundering Network

In **June 2025**, police in **Uttar Pradesh, India**, dismantled a transnational laundering network operated via **Telegram**, using **USDT-TRC20** as the primary payment rail.

- **Structure**: A Chinese controller remotely managed local Indian "money mules" who provided bank accounts to receive cash converted from USDT.

- **Process**:
  - Victims sent USDT to designated Telegram wallets.
  - Funds were converted and withdrawn in cash.
  - Couriers delivered cash to "crypto brokers" who redistributed it offshore through P2P trades and non-custodial wallets.

No KYC, invoices, or official records existed. Funds were broken into small amounts to avoid detection. Authorities arrested **9 individuals**, seized **16 phones**, **laptops**, and **185,000 INR in cash**, demonstrating how USDT enables discreet, mid-scale money laundering.

A separate category of darknet laundering platforms offers **"escrow laundering"** services to scam syndicates. The largest known example is **Haowang Guarantee**, also known as **Huione Guarantee**, which operated in **Chinese** on **Telegram** from 2021 to 2025.

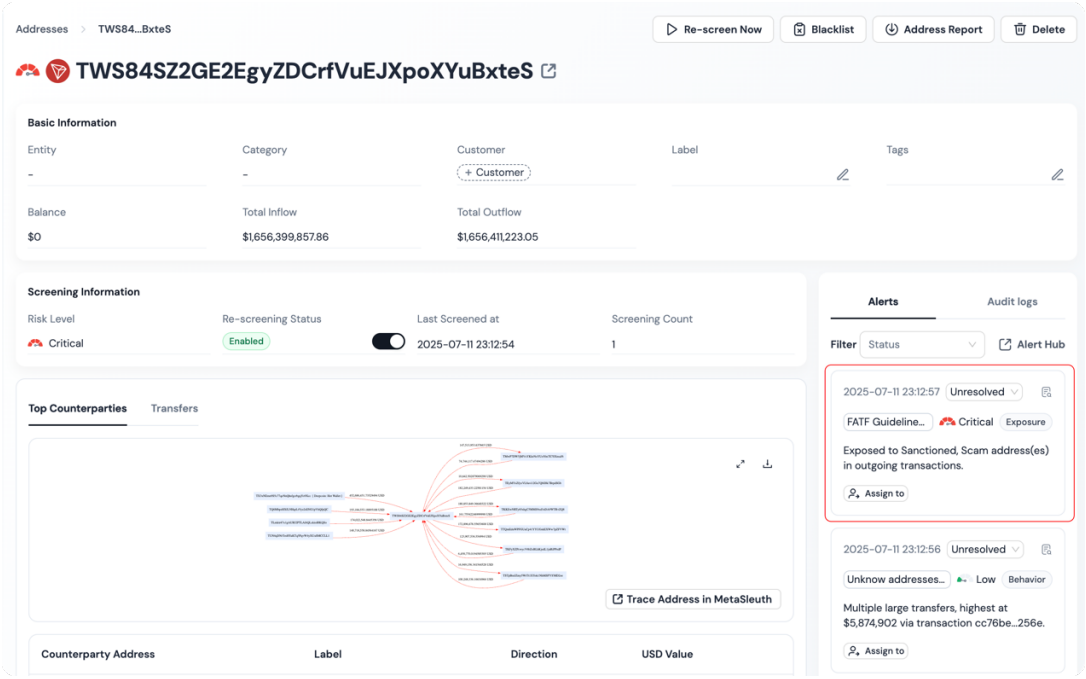
- **Function**: Not a seller of goods or services, but a **financial infrastructure** for fraud networks. Services included:
  - Escrow holding of scam proceeds
  - Address rotation and microtransaction layering
  - Cross-chain and cross-border fund conversion
  - Fake documents, IP spoofing, fraud scripts
  - Payment handling for human trafficking rings
- **Scale**: Over **USD 27 billion** laundered, making it the largest known black-money hub.
- **Takedown**: In **May 2025**, following a **WIRED** exposé on its role in Asian and African romance and telecom fraud, **Telegram** shut down hundreds of channels. Servers were reportedly seized, and admin accounts disappeared. However, operators began migrating to **Line** and **WeChat** under new aliases.

Compliance Alert

Cryptocurrencies—especially **USDT**—are widely used in darknet settlements for drugs, weapons, forged IDs, and more. Escrow contracts and intermediary ("stepping-stone") addresses are common laundering tactics.

Service providers should:

- Use **KYA/KYT** systems to detect high-risk address patterns
- Restrict services to flagged accounts
- Prevent platform abuse in laundering or escrow processes



[Figure 2.5.3 – Phalcon Compliance Alert for Haowang Guarantee-Linked Addresses]

3.6. Pig Butchering Scams

Definition

"Pig Butchering" scams refer to elaborate fraud schemes in which scammers cultivate long-term online relationships—via social media, dating platforms, or impersonation—before inducing victims to invest in cryptocurrency. Scammers typically build trust over weeks or months, then lure victims into depositing funds into fake crypto platforms, which often include:

- Professionally designed fake investment dashboards
- Deepfake video chats or AI chat agents
- Demonstration payouts to simulate legitimacy

Once confidence is secured, victims are persuaded to invest increasingly large amounts, eventually resulting in total financial loss—hence the term "butchering."

In these scams, **USDT (Tether)** plays a central role:

- **Stable value**: USDT's 1:1 peg to the U.S. dollar reduces perceived investment risk compared to volatile assets like BTC.
- **Ease of transfer**: Quick and anonymous transactions allow for fast movement and obfuscation.

- **Poor KYC enforcement**: Exploited by scammers to avoid identity linkage.
- **Cross-platform communication**: Tools like Telegram and WhatsApp help organize and propagate these fraud rings.

Case Studies

Case 1 : $225M Civil Forfeiture by U.S. Department of Justice (DOJ)

In **June 2025**, the **U.S. DOJ** launched a **civil forfeiture action** against wallets holding approximately **USD 225 million in USDT** linked to pig butchering scams.

- **Scope**:

  - Involved **seven** organized crime groups
  - More than **400 global victims**
  - Funds were deposited into fake investment platforms, then laundered via on-chain layering and transfer to controlled wallets.

- **Intervention**:

  - **Tether** and major exchanges cooperated in freezing the wallets.
  - The USDT was **burned and reissued** into wallets under U.S. government control, enabling potential restitution to victims.

Case 2: U.S. Criminal Indictment Against Daren Li

In **May 2024**, the **U.S. District Court for the Central District of California** indicted **Daren Li** and **Yicheng Zhang** for operating a **laundering network** that washed more than **USD 73 million in USDT** derived from pig butchering scams.

- **Method**:

  - Laundered proceeds through **74 shell companies** and bank accounts
  - Used financial institutions such as **Deltec Bank** to fund crypto exchange accounts
  - Purchased USDT and distributed funds to domestic and foreign wallets

- **Outcome**:

  - In **November 2024**, Daren Li pleaded guilty
  - Faces a maximum sentence of **20 years' imprisonment**

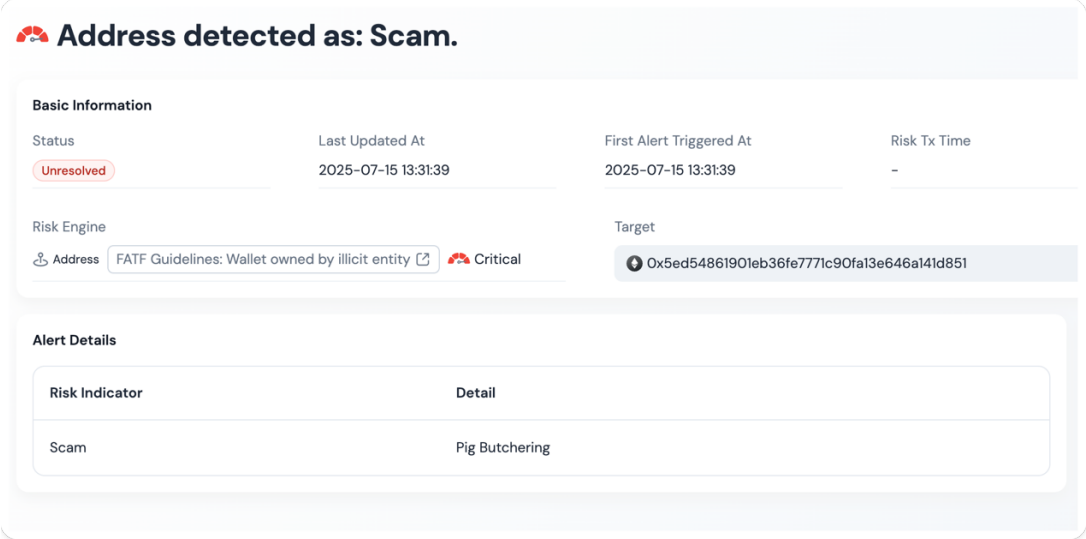
These cases illustrate the evolving laundering path of pig butchering funds:

Victim deposit → Platform wallet → USDT conversion → Fund fragmentation → Offshore laundering → Cash-out.Law enforcement leveraged on-chain forensics and off-chain banking data to expose the shell company infrastructure behind the scheme.

Compliance Alert

Pig butchering scams represent a severe **fraud subtype** with distinct laundering characteristics. Service providers must:

- **Immediately suspend** transaction permissions upon identifying suspected inflows
- **Request source of funds documentation** from flagged users
- **Coordinate with law enforcement** on graylisting addresses and sharing intelligence
- **Integrate real-time screening tools** to prevent scam proceeds from entering the platform



[Figure 2.6.3 – Phalcon Compliance Alert for Pig Butchering-Linked Addresses]

3.7. Ransomware

Definition

Ransomware is a form of malicious software that encrypts a victim's files, systems, or data to extort payment in exchange for decryption keys. In recent years, the widespread adoption of cryptocurrency has fueled the evolution and commercialization of ransomware attacks.

Victims are typically instructed to pay **ransom in cryptocurrency**—commonly **Bitcoin** or **USDT**—to evade traditional financial surveillance and asset freezes. Cryptocurrencies' pseudonymity,

global portability, and decentralization make them the preferred payment method for ransomware operators.

- **Early-stage ransomware** predominantly used Bitcoin.
- As blockchain analytics matured, attackers transitioned to mixers and stablecoins like USDT to reduce volatility and avoid traceability.
- Some ransomware gangs (e.g., **Conti**, **LockBit**, **REvil**) have built **"Ransomware-as-a-Service" (RaaS)** ecosystems, offering malware tools, wallet infrastructure, and laundering services to affiliates—accelerating the industrialization of cyber extortion.

This convergence of ransomware and crypto has driven cybercrime toward greater **organization**, **financial sophistication**, and **international complexity**, presenting major challenges for enforcement and policy response.

Case Study: Colonial Pipeline Attack

In **May 2021**, **Colonial Pipeline**, the largest refined oil pipeline operator in the U.S., suffered a ransomware attack that shut down four major pipelines for one week—triggering an energy crisis across parts of the country.

- **Ransom Payment**: On **May 8**, Colonial paid approximately **USD 4.4 million** in Bitcoin to restore operations.
- **Perpetrator**: The attack was attributed to **DarkSide**, a ransomware group operating under an RaaS model. DarkSide collected revenue from:
    - "License fees" paid by affiliates for using the ransomware
    - A fixed cut of each successful ransom collected by affiliates
- **Seizure**: On **June 7**, 2021, the **U.S. Department of Justice** announced the recovery of **63.7 BTC** from the ransom and released a **seizure warrant**.

Key observations:

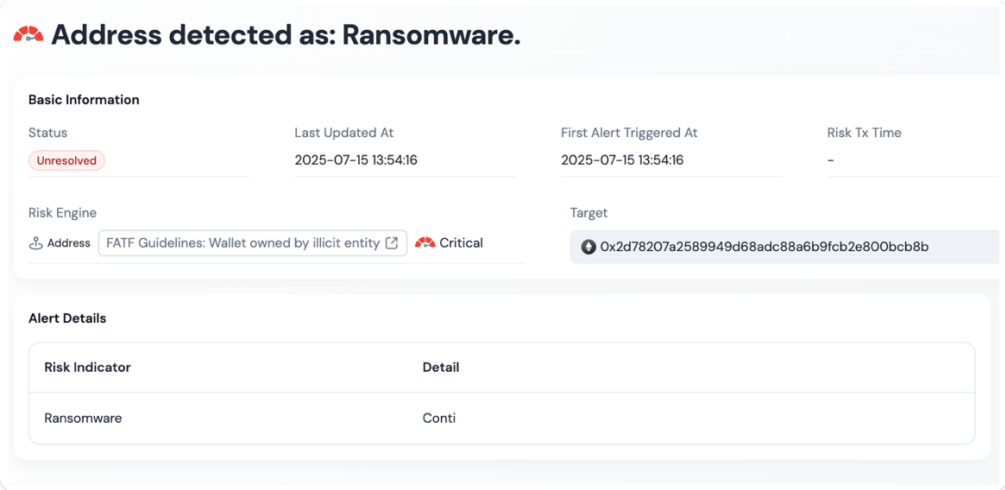
- **May 8 and May 11**: Two large transactions occurred—**~75 BTC** and **78.29 BTC**—matching known ransom amounts paid by Colonial and another DarkSide victim, **Brenntag**, respectively.
- **Transaction Splitting**: Ransom funds were divided after receipt, reflecting DarkSide's revenue-sharing model with affiliates.
- **May 13**: The target wallet's balance was almost entirely transferred to a DOJ-controlled address.

Compliance Alert

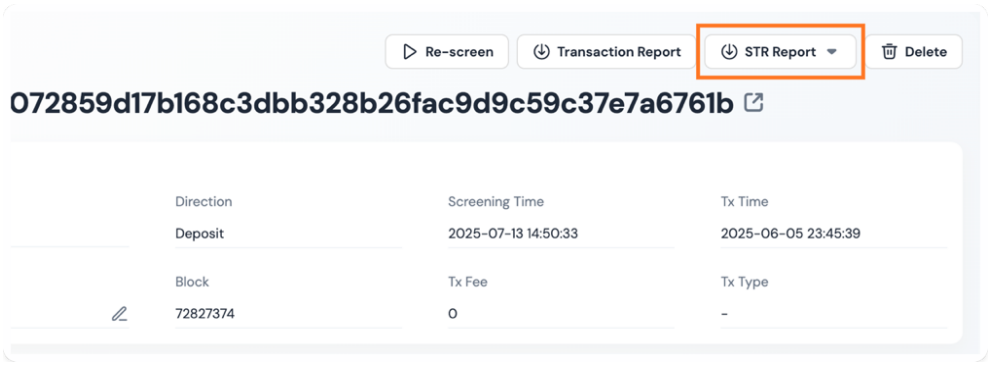
The ransomware–cryptocurrency nexus has spawned a **high-efficiency, decentralized cybercrime ecosystem**. As the initial contact point for ransom flows, crypto platforms bear unique **compliance responsibilities and technical obligations**.

Platforms should:

- **Flag unusual patterns**, such as newly registered accounts receiving large transfers
- **Trigger STR filing** when transactions involve ransomware-linked addresses
- **Retain audit trails** and conduct blockchain-based forensic analysis to support investigations



[See Figure 2.7.3-1 – Phalcon Compliance Alert Triggered by Ransomware-Linked Address]



[See Figure 2.7.3-2 – Phalcon Compliance: One-Click STR Report Export Interface]

Chapter 4 Consequences of Receiving Illicit Funds

Crypto payment institutions that fail to implement effective **AML/CFT** measures—particularly in promptly identifying and responding to on-chain illicit funds—may face serious consequences, including **asset freezes**, **fines**, and even **criminal prosecution**.

4.1. Legal Frameworks

United States

Asset Freezing

The primary objective of asset freezes is to **deprive criminals of the proceeds of crime**. Once law enforcement has reasonable grounds to believe that an asset—whether cryptocurrency, bank deposit, or real estate—is criminally derived or used to facilitate unlawful activity, it may initiate **civil or criminal forfeiture proceedings**. Notably, civil forfeiture in the U.S. does **not** require a conviction; authorities only need to establish a sufficient link between the asset and illicit conduct.

Fines
Fines are designed to penalize non-compliance and illicit profit-making. They fall into two primary categories:

- **Administrative fines**: Under the **Bank Secrecy Act (BSA)**, **U.S. Code Title 31 §5321**, and **Code of Federal Regulations (CFR)**, regulators such as **FinCEN** may impose penalties for failure to implement effective AML programs, customer due diligence (CDD), or suspicious activity reporting (SAR).
  In major cases, fines may reach hundreds of millions or even billions of dollars, calculated based on repeated violations, total transaction volume involved, or settled as part of a negotiated agreement.

- **Criminal fines**: Under **18 U.S. Code §1956**, courts may impose fines following criminal conviction. The maximum fine is **USD 500,000** or **twice the value of the illicit funds involved**, whichever is greater.

- **Imprisonment**
  Criminal prosecution targets individuals and entities with **knowing and willful intent**. Charges may include **money laundering conspiracy** or **unlicensed money transmission business**. Upon conviction, defendants face substantial prison terms. Under **18 U.S. Code**

§1956, the maximum statutory sentence is **20 years**. Actual sentencing is guided by the **Federal Sentencing Guidelines**, which consider the amount involved, complexity of the crime, and other aggravating factors.

Russia

Asset Freezes

The primary goal is to disrupt illicit fund channels and revoke financial licenses. The **Central Bank of Russia (CBR)** may freeze assets suspected of being connected to money laundering. In cases of systematic violations, the CBR may **revoke the entity's banking or payment license**, effectively forcing it into liquidation.

Administrative Fines

Used to penalize compliance failures and serve as pre-escalation warnings.
Under **Russian Code of Administrative Offenses Article 15.27**, financial institutions failing to conduct customer due diligence or report suspicious transactions may be fined:

- **Legal entities**: RUB 500,000–1,000,000
- **Responsible officers**: RUB 30,000–50,000

These fines are often issued prior to extreme enforcement actions such as license revocation.

Imprisonment
Criminal prosecution targets individuals knowingly involved in laundering illicit proceeds.
Under **Russian Criminal Code Articles 174 and 174.1**, penalties are tiered:

- **Basic offense** (under RUB 1.5 million): Fine only
- **Large-scale laundering** (over RUB 1.5 million): Up to **2 years** in prison and fines
- **Extra-large-scale laundering** (over RUB 6 million) or involving criminal organizations: Up to **7 years** imprisonment and fines

4.2. Freezable Crypto: Stablecoin Issuer Capabilities

Traditional Legal Framework for Asset Freezing

Asset freezing is a key mechanism used by judicial or regulatory bodies to prevent the transfer or use of property tied to illegal activity, including fraud, money laundering, and sanctions evasion.

In traditional finance:

- **Courts** may issue seizure or freeze orders based on probable cause.
- **Financial institutions**, such as banks, may independently freeze suspect accounts based on internal policies or regulatory directives.

For example, in the United States, the **Office of Foreign Assets Control (OFAC)** under the Department of the Treasury has authority to issue sanctions that mandate U.S. persons and entities to block any property or interests in property of sanctioned parties, prohibiting any form of transfer or transaction unless specifically authorized.

Under Hong Kong's stablecoin regulatory framework, issuers can establish effective on-chain risk control mechanisms as an alternative to universal KYC requirements. We have provided an in-depth analysis of this regulatory innovation on BlockSec's official account, with detailed analysis available in Appendix 7.1.2.

Freezing Mechanisms in Stablecoin Systems: From Enforcement to On-Chain Execution

In the crypto ecosystem, **stablecoin issuers** are often regarded as **"controllable nodes"**, similar to traditional financial intermediaries, with the ability to block the movement of assets associated with illicit activity. Unlike decentralized assets such as Bitcoin, most stablecoins are **centrally issued**, allowing the issuer to freeze or destroy tokens when necessary.

This capability is enabled by **blacklisting functions** coded into smart contracts.
Examples include:

- **USDT (Tether)**
- **USDC (Circle)**

Both Tether and Circle's smart contracts include privileged functions that allow the issuer to freeze an address, rendering it incapable of sending or receiving tokens. The effect is functionally equivalent to freezing a bank account.

In practice, stablecoin freezes are often triggered by **regulatory or law enforcement requests**.

- In **June 2025**, Tether froze **USD 225 million** worth of USDT tied to a pig butchering scam at the request of the U.S. Department of Justice.
- In **May 2025**, Circle froze **USD 570 million** in USDC linked to the Libra Project under a federal court order.

From Defensive Design to Compliance Cooperation: Strategic Evolution of Freezing Functions

It is worth noting that stablecoin freeze capabilities were **not initially designed for regulatory compliance**. Tether's first freeze occurred in **November 2017**, when it blocked **USD 30 million** of USDT stolen in a hack targeting its hot wallet. This freeze was executed proactively for **internal risk control**—not under any law enforcement directive. Thus, stablecoin blacklisting was originally a **security and risk management** tool. Over time, it evolved into a powerful **compliance enforcement mechanism**.

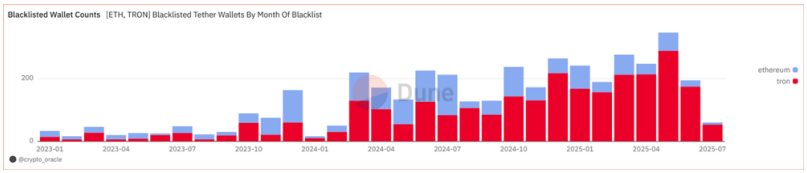
Both Tether and Circle currently retain freezing rights in their contracts, but their exercise of this power differs:

- **Tether** has both **responded to enforcement requests** and **proactively frozen addresses** deemed high-risk, even without public enforcement context.
- **Circle**, in contrast, emphasizes that **freezes are typically based on court orders or official agency requests**, with a **more transparent and procedural approach**.

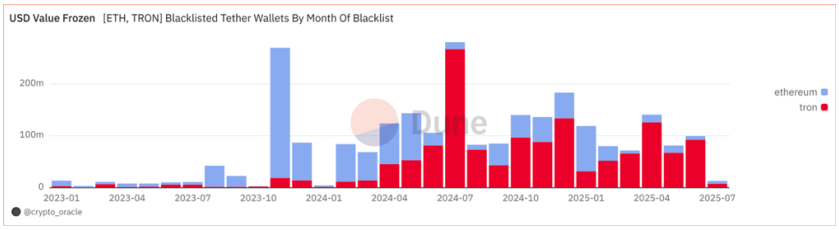
Freeze Activity by Tether and Circle

As of **July 3, 2025**:

- **Tether** has frozen **5,260 addresses** across Ethereum and TRON since 2017.
- In **H1 2025**, it froze **209 Ethereum addresses** holding USDT-ERC20.
- **Circle** froze **44 Ethereum addresses** with USDC-ERC20 in the same period.



[Figure 3.2.4-1 – Number of Wallet Freezes by Tether (ETH + TRON), Jan 2023–Jul 2025]



[Figure 3.2.4-2 – USD Value of Assets Frozen by Tether (ETH + TRON), Jan 2023–Jul 2025]

On **July 8, 2025**, Tether announced that it had cooperated with **over 255 law enforcement agencies** across **55 jurisdictions**, freezing more than **USD 2.7 billion** worth of USDT related to illicit activity.

Given that **USDT** commands approximately **66%** of the U.S. dollar stablecoin market and **USDC** holds about **28%**, Tether's freezing activity significantly exceeds that of Circle in both volume and value.

4.3. Real Cases Against Crypto Payment Companies

Case 1: Wise – AML Failures at a Global Remittance Platform

Wise (formerly TransferWise) is a leading global fintech and remittance provider. Between **July 1, 2022, and September 30, 2023**, a **multi-state regulatory task force** in the United States—comprising agencies from **New York, California, Texas, Massachusetts, Minnesota**, and **Nebraska**—conducted a comprehensive AML compliance review of Wise's U.S. operations. Despite being a licensed money transmitter, regulators found **systemic and fundamental deficiencies** in Wise's AML program.

Violations Identified:

- Inadequate customer due diligence (CDD)
- Ineffective monitoring of suspicious transactions
- Delayed filing of **Suspicious Activity Reports (SARs)**
- Data integrity issues in monitoring and risk systems
- Failure to remediate previously identified compliance weaknesses

Consequences:

In **July 2025**, Wise reached a **settlement** with the six state regulators, agreeing to:

- Pay **USD 4.2 million** in civil penalties
- Undertake corrective actions, including:
    - Historical "look-back" reviews of past accounts to identify missed suspicious activity
    - Strengthened AML/CFT risk assessment and due diligence procedures
    - Appointment of an **independent third-party auditor** to verify remediation effectiveness
    - Quarterly reporting to regulators over a two-year period

Key Lesson:

This case illustrates that **merely having an AML framework on paper is not sufficient**. Regulators focus on **program effectiveness**—whether the controls are properly tailored to the company's business model, risk exposure, and operational complexity.

Case 2: QIWI Bank – License Revocation in Russia

QIWI Bank was a major Russian payment service provider. The **Central Bank of Russia (CBR)** found that QIWI had **knowingly facilitated settlements** for illegal online casinos, betting operations, and unregistered crypto exchanges.

Consequences:

- **License Revocation**:
  After repeated warnings and restrictions proved ineffective, the CBR **revoked QIWI Bank's license in February 2024**.
  This action forced the bank to cease operations immediately, freeze all accounts, and initiate liquidation.
- **Prior Sanctions**:
  Before revocation, QIWI had been subject to fines and operational limitations but failed to implement corrective actions.
- **Criminal Risk**:
  The CBR's findings of **intentional facilitation of illicit finance** laid the groundwork for potential **criminal investigations** against company executives.

Case 3: Liberty Reserve – The First "Crypto Bank" Shut Down

Liberty Reserve was a digital currency payment processor offering **anonymous transactions** without identity verification. It became a haven for cybercriminals, used to launder proceeds from credit card fraud, Ponzi schemes, and hacking—reportedly facilitating **over USD 6 billion** in illicit transfers.

Consequences:

- **Global Asset Seizures**: In **2013**, U.S. and international agencies from **17 countries** coordinated a takedown. Liberty Reserve was designated a **"primary money laundering concern"**; its servers, domains, and bank accounts were seized.
- **Asset Forfeiture**: As the entire operation was deemed criminal infrastructure, all company assets were **forfeited** as proceeds of crime—beyond standard regulatory fines.
- **Criminal Prosecution**:
  Founder **Arthur Budovsky** and key personnel were indicted by the **U.S. Department of Justice**. Budovsky was convicted of **money laundering conspiracy** and sentenced to **20 years in federal prison**.

How Payment Companies Should Respond

In the context of crypto payments, illicit funds and sophisticated laundering techniques pose serious compliance challenges. Payment service providers (PSPs) must detect suspicious inflows and outflows in real-time, establish robust mitigation procedures, and build comprehensive risk control systems to remain compliant with global AML/CFT obligations.

4.4. Risk Identification

Accurately Identifying On-Chain Risk Types

In real-world crypto operations, the risks associated with on-chain transactions generally fall into the following categories:

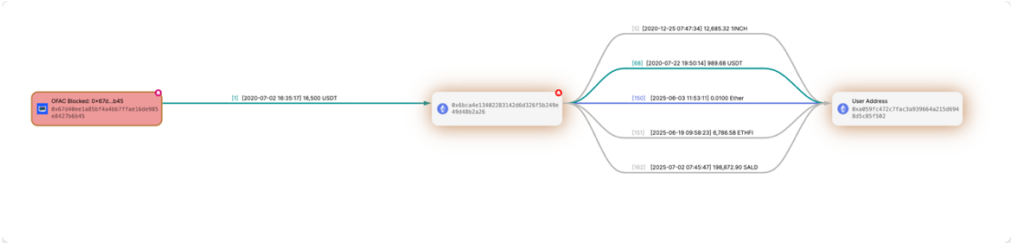
1. **Direct Risk**
   The clearest form of risk: the transaction involves an address that is already flagged as high-risk (e.g., on a sanctions list, or associated with known attacks).
   Such risks can be swiftly identified using blacklist address databases and classified as immediate threats.

2. **Indirect Risk Through Association**
   Even if a wallet address has no direct risk label, it may still be associated with high-risk entities via its transaction history.
   Due to blockchain transparency and traceability, these links can be detected and analyzed:

   - **Direct linkage**: If a client address has received funds directly from a sanctioned wallet, that address and the transaction may be flagged for risk.

[Figure 4.1.1-1 – Direct Association Risk Example: Fund Flow Diagram]

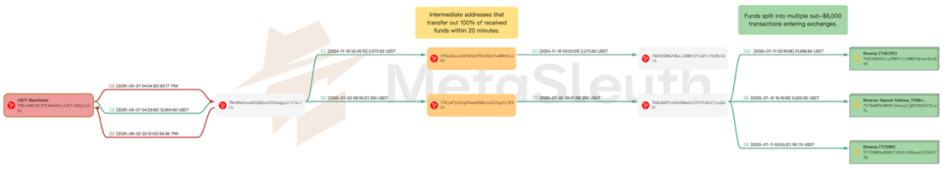
   - **Indirect linkage**: Risk may also arise through multiple "hops" (intermediate wallets) that attempt to obscure the source of funds.
     With DeFi and multi-chain ecosystems becoming more complex, tracing cross-chain and multi-hop flows becomes essential.



[Figure 4.1.1-2 – Indirect Association Risk Example: Fund Flow Diagram]

3. **Unlabeled Address Risk**

With thousands of new wallet addresses created daily, many lack historical tagging. Criminal actors often exploit this by frequently rotating wallets to obfuscate illicit flows. Therefore, reliance solely on blacklist databases is insufficient. PSPs must complement them with **behavioral pattern analysis**, including: rapid inflow and outflow cycles ("fast in, fast out") and micro-transaction structuring (smurfing).



[Figure 4.1.1-3 – Fast In/Out and Micro-Split Laundering Pattern: Fund Flow Diagram]

4. **Cross-Border Risk**

Transactions involving jurisdictions with differing AML/CFT regimes present inherent risk. For example, countries listed by **FATF** as **high-risk or non-cooperative jurisdictions** may introduce elevated compliance exposure.

How to Detect the Risk

To manage the above risk categories, PSPs must combine **on-chain intelligence**, **transaction path analysis**, and **behavioral heuristics** for continuous, traceable surveillance. The industry standard involves deploying specialized tools such as:

- **KYA (Know Your Address)**
- **KYT (Know Your Transaction)**

These tools should offer:

- **Rich intelligence labeling**: Including global sanctions lists, law enforcement disclosures, and high-risk entity identifiers (e.g., hacker groups, phishing actors).

- **Path tracing capabilities**: Automated tracking of fund origins and destinations, including support for **cross-chain**, **DeFi**, and **mixing services**.
- **Behavioral analysis**: Assessing transaction frequency, value distribution, timing patterns to spot anomalies (e.g., high-frequency low-value transfers, suspicious bridging activity).
- **Dynamic risk scoring**: Real-time risk assessment of wallets or transactions, continuously updated as new intelligence becomes available.

Example: Phalcon Compliance APP by BlockSec：

[Figure 4.1.2 – Screenshot of Phalcon Compliance APP]

Phalcon Compliance APP is a smart compliance and risk control platform developed by **BlockSec**, offering full-spectrum support for the above capabilities:

- Integrates **400+ million labeled addresses** and a FATF-aligned rules engine
- Detects hidden laundering patterns using **AI-powered behavior models**
- Supports unlimited-depth cross-chain fund tracing
- Built-in **MetaSleuth** integration for investigative drill-down
- Real-time alerts delivered via email, Telegram, Slack, Lark, Discord, and others
- Features **custom rule sets**, **team collaboration**, and **one-click STR report generation**
- Currently adopted by licensed institutions to lower compliance costs and regulatory exposure

4.5. Risk Mitigation

After identifying suspicious funds or high-risk activities, payment service providers (PSPs) must implement structured mitigation measures in accordance with internal policies and local regulations. The objective is to balance risk control, customer relationship management, and legal compliance.

Risk Mitigation Measures

1. **Transaction Restriction or Freezing**
   Upon risk detection, immediately restrict account operations by:

   - Lowering transaction limits
   - Temporarily disabling key functions
   - Freezing specific accounts or funds
     This helps prevent further risk propagation.

2. **Fund Segregation**
   Once high-risk funds are detected, systems must isolate them from normal funds—e.g., by transferring to a segregated wallet—to avoid collateral impact on compliant funds and operations.

3. **Return of Funds**
   If the customer fails to provide sufficient documentation proving legitimate fund sources within a reasonable time, the suspicious funds may be **returned to the original sender**. PSPs should:

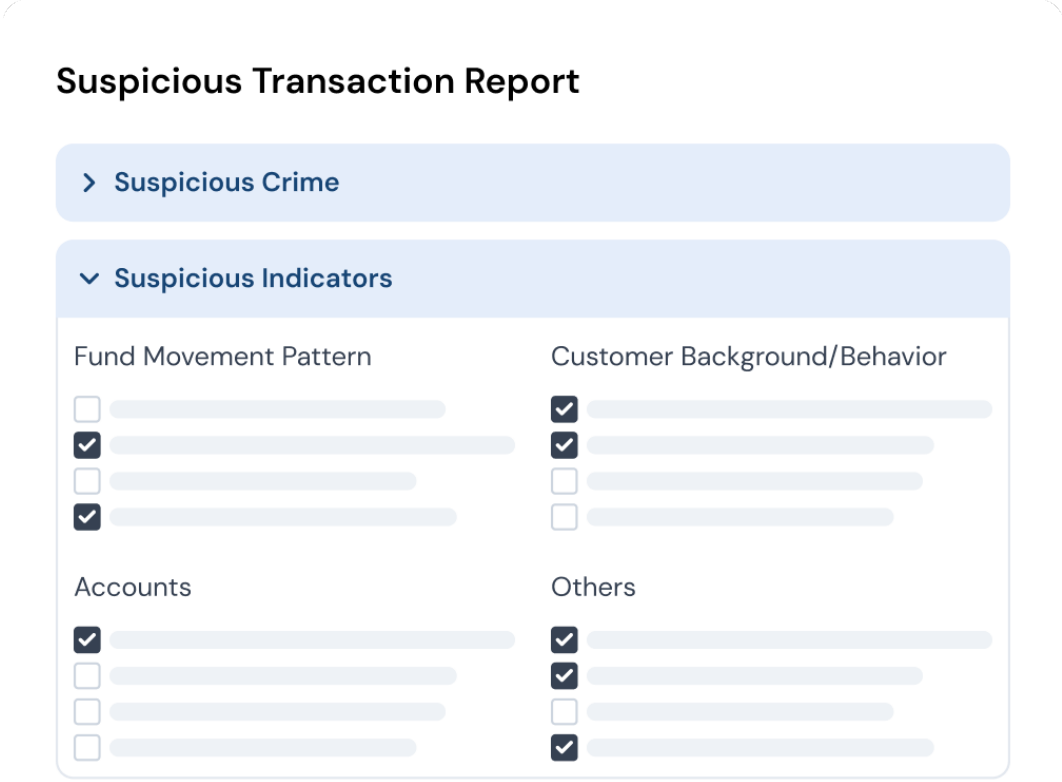
   - Retain complete on-chain records
   - Provide customers with detailed reasoning and return transaction data

4. **Supplemental Documentation Review**
   In cases with plausible explanations (e.g., legitimate investments or business payments), the PSP may require the customer to submit:

   - Proof of identity
   - Fund origin evidence
   - Business contracts
   - On-chain transaction screenshots
     Failure to respond or submit adequate documentation may trigger risk escalation based on internal policy.

5. **Suspicious Transaction Reporting & Recordkeeping**

   - **STR/SAR Filing**: If a transaction is suspected to involve illicit activity, the provider must file a **Suspicious Transaction Report (STR)** with the relevant **Financial Intelligence Unit (FIU)**.
     [Figure 4.2 – STR Auto-Export Feature in Phalcon Compliance]
   - **Data Retention**: All related transaction and compliance records should be securely stored for a minimum of **five years** to facilitate audits or investigations.



Risk-Based Mitigation Principles

Mitigation efforts should be **tiered** based on the level of assessed risk:

Risk Level	Response
High	Freeze assets or restrict transactions
Medium	Segregate funds, request documentation
Low	Monitor passively, flag for review

By following a full-spectrum workflow—encompassing risk identification, monitoring, and mitigation—payment companies can effectively manage AML/CFT compliance in the crypto domain. Here, **KYA/KYT tools** are essential for increasing accuracy and operational efficiency in risk control.

4.6. Industry Practice: Interlace's Risk Management Framework

Interlace, founded in 2019, is a fintech platform specializing in global card issuance and digital asset management. It provides cross-border, multi-currency, and multi-system financial solutions to Web3 companies, cross-border e-commerce platforms, B2B traders, and developers.

As a licensed institution across multiple jurisdictions (e.g., United States, Hong Kong, Lithuania, Luxembourg) and a PCI DSS Level-1 certified provider, Interlace prioritizes **strict compliance** with global AML (Anti-Money Laundering) and CFT (Counter-Terrorist Financing) regulations.

Its comprehensive risk management framework ensures the safety of customer funds, integrity of on-chain interactions, and overall platform compliance.

Fund Custody Risk Management

Objective: Prevent systemic risk and single points of failure associated with centralized custody.

1. **MPC Wallet Technology**

- Employs **Multi-Party Computation (MPC)** to distribute private key control
- Eliminates single-point risks inherent in traditional custody
- Enhances both security and reliability of private key management

2. **Distributed Custody**

- Client assets are dispersed across multiple decentralized wallets
- Implements "distributed custody" strategy to reduce systemic exposure

3. **Cold & Hot Wallet Segregation**

- **Cold Wallets**: Used for long-term asset storage; remain completely offline to mitigate network attacks
- **Hot Wallets**: Serve operational needs; protected via real-time monitoring and withdrawal limits

4. **Periodic Audits & Monitoring**

- Third-party audits verify the safety and transparency of custodial assets
- Continuous wallet activity monitoring to flag anomalies

Transaction Risk Management

Objective: Identify and block high-risk transactions using on-chain and off-chain analytics to prevent money laundering and terrorist financing.

1. **Inbound (Deposit) Risk Controls**
    - **KYA & KYT Screening**
        - Real-time scanning of counterparties and source of funds
        - Multi-dimensional analysis of address history and path tracing
    - **Risk-Based Response**
        - **High / Very High Risk**: Restrict deposit, request additional documents (e.g., proof of origin); may return or freeze funds for 7–30 business days based on regulatory requirement
        - **Medium Risk**: Subject to periodic backtesting and dynamic evaluation
2. **Outbound (Withdrawal) Risk Controls**
    - **High-Risk Address Blocking**
        - Prohibit withdrawals to addresses flagged as high/very high risk
    - **Dynamic Screening**
        - Retrospective scans ensure newly flagged risks are applied to past addresses
        - Trace downstream transaction paths for hidden exposures
    - **Real-Time Interception**
        - Automated systems block suspicious transactions before execution
        - Manual review for flagged outflows

Address Security

Objective: Prevent address contamination and mitigate risk from on-chain interactions.

1. **Contaminated Address Alerts**
    - Identify wallets that have interacted with high-risk addresses using KYA
    - Notify clients to avoid using such addresses in future operations
2. **Rotating MPC Wallets**
    - Regularly rotate primary MPC addresses for asset storage and withdrawals
    - Reduces risk from prolonged address exposure
3. **Whitelist Enforcement**
    - Implement address whitelisting to restrict client activity to verified addresses

- Regular updates to remove addresses compromised over time

4. **Multi-Sig & Dynamic Verification**
    - Use multi-signature mechanisms for critical address usage
    - Adjust signature policies based on transaction value and risk level

Supplementary Measures

1. **Customer Education**
    - Conduct AML/safety education campaigns
    - Provide real-time support for risk-related inquiries to build client trust

2. **Regulatory Engagement**
    - Proactively engage with global regulators
    - Submit reports and participate in investigations as needed

4.7. Industry Practice: KUN's Virtual Asset Compliance Framework

KUN, as a fintech institution specializing in virtual assets, has developed unique practical experience in on-chain risk identification and Travel Rule compliance by combining Hong Kong regulatory requirements with its proprietary risk control system.

Multi-dimensional On-chain Risk Identification

- **Dual KYA/KYT Mechanism**: Integrates blockchain analytics tools, automatically synchronizes global sanctions lists, covering typical risk types including hacking, fraud, and ransomware
- **Penetrative Fund Path Analysis**: Deep tracing of multi-hop associated high-risk addresses, with focus on identifying covert money laundering behaviors through DeFi, mixers, and cross-chain bridges
- **Behavioral Modeling**: Captures suspicious characteristics such as "quick in, quick out" and "micro-splitting," dynamically adjusting customer risk profiles

Travel Rule Compliance Implementation

- **Core Information Collection**: Strictly collects complete identity information of payers and payees for transfers of HKD 8,000 and above
- **Travel Rule Platform Integration**: Enables encrypted transmission of compliance data

between institutions through external platforms
- **Counterparty Capability Due Diligence**: Evaluates VASPs' Travel Rule compliance capabilities, refusing cooperation with institutions lacking such capabilities

Tiered Wallet Management

- **Micro-payment Verification**: Requires customers to complete micro-payment tests or message signature authentication to confirm wallet ownership
- **Dynamic Whitelist**: Periodically reviews wallet risk status, removing from whitelist upon risk signals
- **Unhosted Wallet Special Controls**: Implements stricter identity verification mechanisms for personally controlled wallets

Tiered Risk Management

- **High Risk**: Immediate freezing and reporting to JFIU
  JFIU (Joint Financial Intelligence Unit) is a financial intelligence unit jointly established by the Commercial Crime Bureau of the Hong Kong Police Force and the Narcotics Investigation Bureau of Customs, responsible for receiving and analyzing suspicious transaction reports, and coordinating anti-money laundering and counter-terrorist financing enforcement actions.
- **Medium Risk**: Limit amounts and require supplementary documentation
- **Low Risk**: Normal processing with continuous monitoring

Compliance failures often stem from technical oversights—such as the lack of effective sanctions list screening systems, inadequate risk identification engines, or inability to detect suspicious transaction patterns in a timely manner. This indicates that payment companies need not only compliance strategies but also professional technical tools and service support.

Chapter 6 will introduce how BlockSec, as a one-stop blockchain security service provider, helps payment companies transform compliance theory into practical technical protection capabilities through innovative solutions such as its Phalcon Compliance APP.

Chapter 5 BlockSec: Full-Stack Security Service Provider

5.1. Company Overview

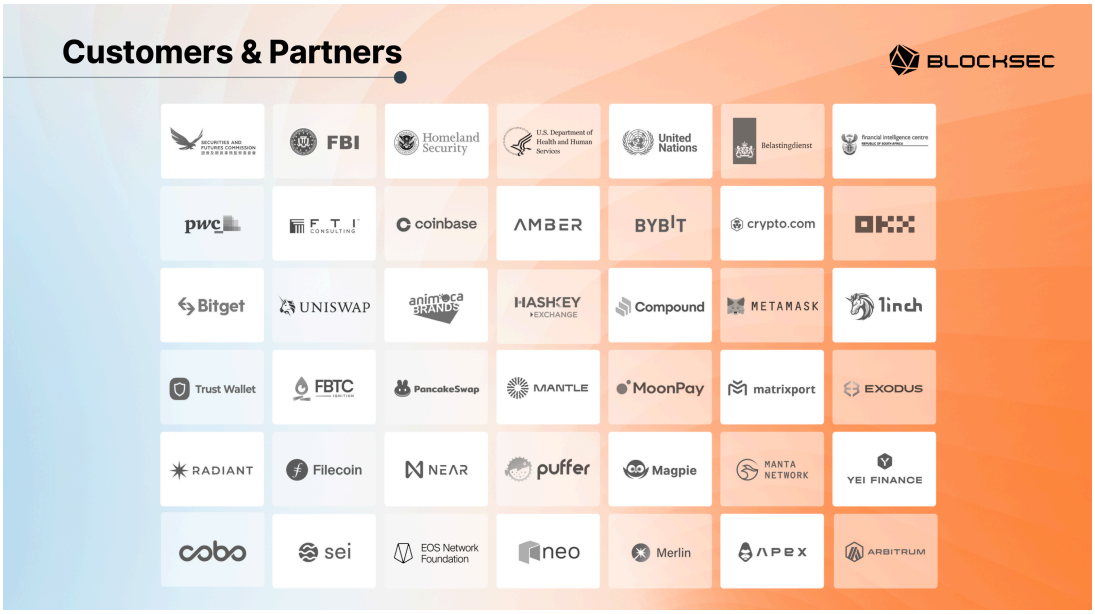
BlockSec was founded in 2021 by a team of world-class blockchain security experts. We believe that **security and compliance** are the bedrock of Web3's path toward mainstream adoption and full potential realization. Accordingly, BlockSec is dedicated to delivering **comprehensive, full-stack solutions** in both security and compliance, encompassing:

- **Smart contract auditing**
- **Real-time threat monitoring and blocking (Phalcon Security)**
- **Intelligent compliance and transaction screening (Phalcon Compliance)**
- **On-chain fund tracing and investigation (MetaSleuth)**

[Figure 5.1-1 – BlockSec Product and Service Matrix]

Our capabilities have earned the trust of top-tier institutions worldwide. To date, BlockSec has provided services to over **500 clients**, ranging from leading Web3 organizations to global regulators and consulting firms. Notable partners include:

- Web3 Entities: **Coinbase**, **Uniswap Foundation**, **MetaMask**, **Compound**, **Amber**, **Bybit**, **Cobo**
- Regulatory and Investigative Bodies: **United Nations (UN)**, **Hong Kong SFC**, **U.S. FBI**, **PwC**



[Figure 5.1-2 – Selected Clients of BlockSec]

5.2. Phalcon Compliance: A Crypto Compliance Solution

Platform Overview

In today's increasingly complex global regulatory landscape, crypto businesses—including stablecoin issuers, payment companies, and exchanges—require a **compliance solution** that not only meets current demands but also anticipates future requirements.

Phalcon Compliance was built to meet this need. It is a **real-time compliance monitoring and risk management platform** designed to help enterprises build effective and scalable AML/CFT systems, transforming compliance challenges into operational advantages.

Website: https://blocksec.com/phalcon/compliance

How We Protect Your Business

Step 1: Accurate Identification – Eliminate Risk at the Source

- **Proprietary Intelligence, Real-Time Updates**: Phalcon Compliance aggregates data from global regulators, industry partners, and proprietary attack/phishing monitoring engines. The platform instantly issues alerts when your platform interacts with flagged addresses, helping you **avoid asset contamination**.

- **Continuous Monitoring to Meet Regulatory Requirements**: The system supports automatic and manual **re-screening** of high-risk addresses and transactions to satisfy strict regulatory expectations for ongoing due diligence.
- **Omni-Channel Alerts**: Risk notifications are pushed instantly to **Email**, **Telegram**, **Slack**, **Lark**, **Discord**, and more—ensuring rapid response and operational coordination.

Step 2: Deep Insight – Empower Faster, Smarter Decisions

- **Smart Risk Engine**: Built-in rules align with **FATF standards**, offering both exposure-based and behavior-based risk assessment modes. AI-driven algorithms detect complex laundering tactics (e.g., fast-in/fast-out, address peeling) even when using newly generated wallets.
- **Visual Investigations**: Intuitive diagrams show fund origins and paths, with **one-click pivoting** to **MetaSleuth** for deeper forensic analysis.
- **Unified Customer Risk Profiles**: Aggregates all related wallets, historical alerts, and risk scores per customer, enabling a **holistic view** of client exposure.

Step 3: Collaborative Response – Stay Audit-Ready

- **Efficient Teamwork**: Assign incidents, comment inline, and track status updates directly within the platform. Support for **tiered response workflows** ensures clarity of responsibility and consistent documentation.
- **One-Click Report Export**: Instantly generate **STRs (Suspicious Transaction Reports)** and **Audit Logs** that comply with major regulatory requirements.
- **Integrated Blacklist/Whitelist Management**: Seamlessly synchronize address lists with business systems and payment rails to automate enforcement of risk policies.

Compliance is not a blocker to growth—it is its foundation.

Phalcon Compliance turns trust into capability, and capability into sustainable scale.By adopting Phalcon Compliance, your organization can:

- **Minimize compliance costs and enforcement risk**
- **Earn the trust of institutional partners**
- **Strengthen your brand through security and transparency**
- **Free up internal teams to focus on innovation**

At BlockSec, our mission is to empower industry builders with the tools to create a **secure and compliant Web3 ecosystem**.

Frictionless Compliance: Instant Screening and Flexible Pricing

Phalcon Compliance is committed to providing crypto payment enterprises with a low-barrier, high-efficiency compliance experience. The Version 3.1 upgrade eliminates traditional industry hurdles like "lengthy onboarding" and "complex payment processes." Built on the pillars of **"Instant Response, Flexible Billing, and Lucrative Incentives,"** we've made compliance screening faster and more intuitive, creating a robust line of defense for both institutional and individual users.

Instant, Out-of-the-Box Screening: Double Your Efficiency

We have completely re-engineered the workflow to remove all operational friction, ensuring your compliance needs are met immediately:

Hassle-Free "Lite Scan": No registration or login required. Simply enter an address or transaction hash on the landing page to get a risk score in seconds. It's the perfect tool for both urgent audits and routine checks.

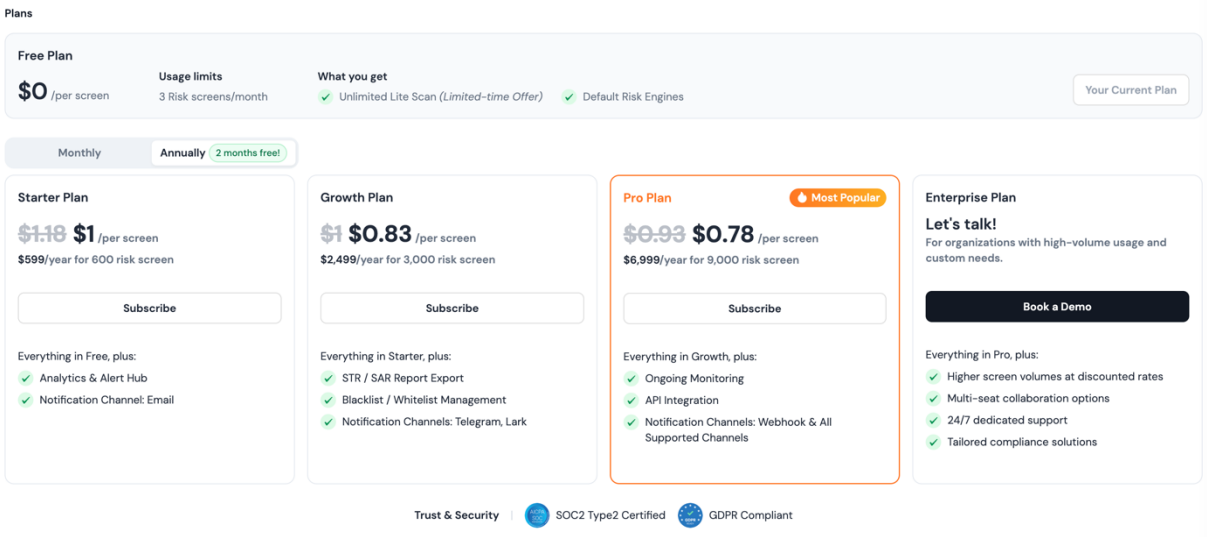
All-in-One Dashboard: Access to all key tools in a single page, including search bar, screening history, and recent alarms.. This eliminates the need for page-hopping, allowing even first-time users to navigate the platform with zero learning curve.

Automated Multi-Chain Support: The system automatically identifies the blockchain (covering mainstream chains like Ethereum, Polygon, and TRON) and matches it with the corresponding risk database, ensuring precise results for each scan.

Flexible Pricing Plans: Manage Budget with Control

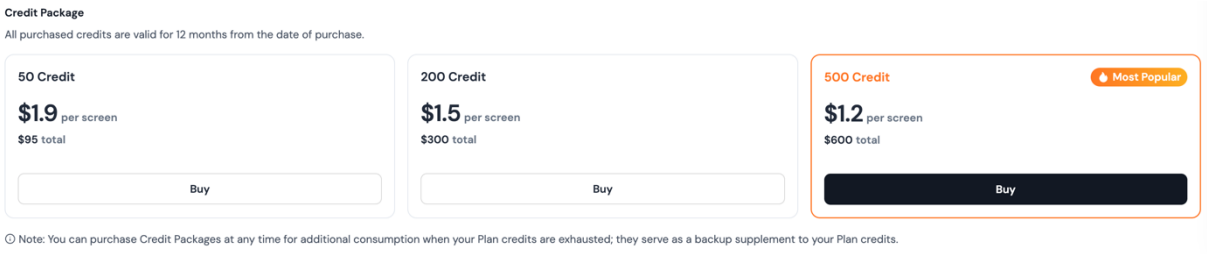
We offer diversified payment solutions tailored to different business scales and usage patterns:

Tiered Subscription Plans: Best for enterprises with stable screening volumes. Choose from Entry-level to Enterprise tiers. Annual plans include **2 months free** (a 16.7% discount). Our **Pro Plan** brings the cost down to just **$0.78 per scan**, including premium features like real-time monitoring and multi-channel alerts.



On-Demand Credit Packages: Ideal for handling temporary surges in volume. These serve as a flexible top-up to your subscription. Our **500-Credit bundle** offers rates as low as **$1.2 per scan** on a "pay-as-you-go" basis to avoid waste.

Global Payment Compatibility: Beyond native **Crypto** settlement, we now support **WeChat Pay** and **Cash App**. This provides a seamless checkout experience for users from various regions, making the financial operations transparent and efficient.



Enhanced Referral Rewards: Grow with the Ecosystem

Our new referral program is designed to be a win-win for our community:

First-Order Discount: New users can claim up to a **20% discount** on their initial purchase by using a partner's exclusive referral code.

Double Incentives: Referrers earn a **cash rebate of up to 20%** on their invitees' payments. Earnings can be withdrawn starting at $100 (up to $10,000 per referrer). Additionally, referrers can unlock **unlimited free scans**, scaling with their advanced screening needs.

Through understanding technical solutions such as BlockSec's Phalcon Compliance APP, we see practical tools for addressing crypto payment compliance challenges. However, the effective use of technical tools requires staying synchronized with the latest regulatory policies. With the successive implementation of regulations such as the EU's MiCAR, Hong Kong's Stablecoin Ordinance, and the US GENIUS Act, the regulatory environment is rapidly evolving.

Chapter 7 Appendix will provide interpretations of the latest regulatory policies across major jurisdictions, helping practitioners maintain forward-looking compliance in a changing regulatory environment.

Chapter 6 Appendix: Latest interpretation of regulatory policy

This appendix compiles in-depth regulatory policy analyses recently published by the BlockSec team on their official WeChat account, providing readers with timely and comprehensive policy insights and practical guidance. Developed through our continuous monitoring and professional analysis of global regulatory developments, these articles serve as an essential supplement to the core manual content.

BlockSec will continue to monitor global regulatory policy changes in the crypto industry and provide professional interpretation and compliance guidance to the industry at the earliest opportunity. Follow our WeChat official account (Search: BlockSec) for the latest regulatory interpretations.

6.1. Hong Kong regulatory analysis

The Evolution of OTC regulation: from "coin shop" to full management

Article source: BlockSec WeChat account **Release time:** August 2025

As a globally significant financial hub, Hong Kong's virtual asset regulatory framework serves as a prime example of international best practices. This study provides an in-depth analysis of three pivotal phases in the evolution of Hong Kong's OTC (Over-The-Counter) market regulation from 2023 to 2025, revealing the strategic shift from "pilot programs" to "comprehensive implementation".

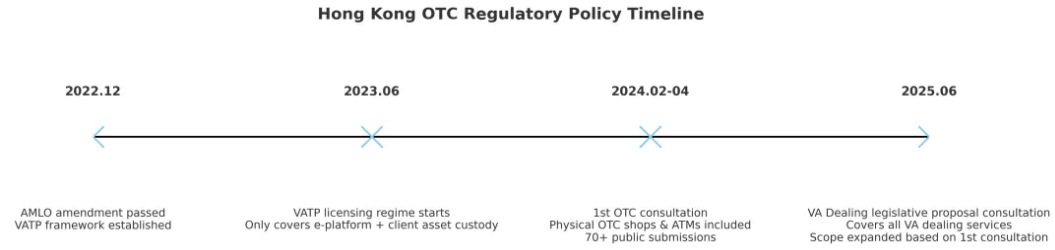
In May 2025, Hong Kong police busted a virtual asset money laundering ring worth $15 million (about HK $117 million), which was involved in splitting and transferring funds through the OTC channel located in Tsim Sha Tsui.

Earlier in the Hong Kong sensation JPEX case, the Commercial Crime Bureau (CCB) revealed that much of the money involved was exchanged and transferred through OTC stores in Hong Kong, becoming an important part of the fraud chain.

In June 2025, the Hong Kong government released a public consultation document titled "Legislative Proposal to Regulate Dealing in Virtual Assets" (the "Virtual Asset Trading Services Regulation Bill"), proposing to integrate all virtual asset trading services—including over-the-counter (OTC) transactions—into a unified licensing and regulatory framework. Although this

proposal remains in the consultation phase without formal legislation yet, it has outlined a clear roadmap for the next steps in Hong Kong's virtual asset regulation——**From the early licensing of VATP platforms, to the regulation of coin stores, and then to the full coverage of VA Dealing services.**

In a word: **in three years, Hong Kong's regulation has moved from the "vacuum zone" of OTC to the full chain management.**



Phase 1 (2023)

VATP is regulated, but OTC is a "loophole"

At the end of 2022, Hong Kong passed the Anti-Money Laundering and Terrorist Financing (Amendment) Ordinance, which will implement a licensing system for virtual asset trading platforms (VATP) from June 2023 under the supervision of the Securities and Futures Commission (SFC).

VA Dealing Consultation Paper, 1.3

“In December 2022, ... a licensing regime for VA trading platforms (“VATPs”) ... commenced operation in June 2023 ... must be licensed by the SFC unless otherwise permitted by the law.”VADEALING_consultation_...

According to the definition of VA exchange:

- Virtual asset transactions between buyers and sellers are facilitated through electronic facilities;
- Access to client assets (holdings, control or arrangements in custody)

Therefore, the system at that time only targeted the business of "electronic platform + access to customer assets",**OTC scenarios such as physical coin stores, counters and ATMs are not included,**This has led to a regulatory vacuum.

Phase 2 (2024)

Customs licensing, cryptocurrency OTC also requires a license

From February to April 2024, the Financial Services and Treasury Bureau (FSTB) launched the first round of consultation on the Licensing Scheme for Off-exchange Trading Services in Virtual Assets, bringing physical OTC into regulation for the first time.

Primary coverage：

- All persons operating physical trading of virtual assets (physical or online) in Hong Kong are required to hold a licence;
- The Hong Kong Customs (CCE) is responsible for licensing;
- Including the exchange and transfer of legal tender such as USDT and BTC;

VA Dealing Consultation Paper, 1.6(a)-(b)：

“Scope and coverage: Any person … services of spot trade of any VAs … would have to be licensed by the Commissioner of Customs and Excise (“CCE”).Eligibility: A licensee would be required to be a locally incorporated company …”

Phase 3 (2025)

The OTC is incorporated into the VASP family and SFC is under unified supervision

In June 2025, Hong Kong issued the second round of《Legislative Proposal to Regulate Dealing in Virtual Assets》,Double upgrade of regulatory scope and depth:

- **Expanding the scope:**Covering complex services such as block trading, brokerage, settlement and exchange, asset management;
- **Regulatory adjustments:**Banks licensed by the SFC and regulated by the HKMA/SVF;
- **Principle of continuity:**Same business, same risk, same rules;
- **Exemption arrangements:**Issuers that issue/redeem stablecoins only in the primary market and have been licensed by the HKMA are exempt.

VA Dealing Consultation Paper, 1.10：

“Under the proposed regime, any person … providing the VA service of dealing in any VAs in Hong Kong is required to be licensed by or registered with the SFC… including conversion, brokerage, block trading…”

Reasons for change: This round of recommendations is based on more than 70 written comments received during the first round of consultations, which the government said reflected concerns about the high risk of OTC, loopholes in cross-border money laundering and inadequate regulatory coverage, **therefore, the original OTC regulatory recommendations are expanded to a broader "VA Dealing" framework.**

VA Dealing Consultation Paper, 1.8：

“Following the conclusion of the first round of consultation, we received over 70 written submissions from various stakeholders... We have refined our proposal to expand the scope to VA dealing services to better address AML/CFT risks.”

Important: The content of this stage is still in the public consultation stage and has not been formally legislated. Final details may be adjusted during the legislative process.

What drives policy change

The three evolution of Hong Kong's OTC regulatory policy is not an isolated occurrence, but the result of multiple factors superimposed on each other. There are at least three core drivers behind it：

Driver 1: Major cases occur frequently, exposing regulatory vacuum

In the $15 million money laundering scheme uncovered in May 2025, criminal groups employed over-the-counter (OTC) fund splitting techniques to bypass bank monitoring systems and execute multiple cross-border transfers within a short timeframe. The Joint Proceeds Exchange (JPEX) case revealed that the Commercial Crime Investigation Division (CCB) discovered numerous investors' defrauded funds were converted into cash or stablecoins through local OTC exchanges before being swiftly transferred to offshore wallets.

These cases expose a problem: even if platform regulation is tightened, the anonymous and instant settlement characteristics of offline OTC can still bypass regulation and become a risk channel for the "last kilometer".

Driver 2: International regulatory pressure and FATF standards

Since updating Recommendation 15 in 2019, the Financial Action Task Force (FATF) has explicitly required all jurisdictions to fully integrate Virtual Asset Service Providers (VASPs) into their anti-money laundering and counter-terrorism financing (AML/CFT) frameworks. While Hong Kong initially met some FATF requirements when introducing its first VASP license, international evaluation agencies and partners repeatedly highlighted the oversight of OTC operations. To preserve Hong Kong's reputation as an international financial hub, regulators must address this gap and **ensure the principle of "same business, same risk, same rules" is effectively implemented.**

To become an international virtual asset center, Hong Kong must address the hidden dangers of AML/CFT.

Driver 3: Local public opinion drives policy upgrading

During the first round of OTC consultations in 2024, the government received over 70 written public submissions from banks, compliance agencies, crypto firms, and law enforcement departments. The majority of feedback highlighted three key concerns: high anonymity risks in

OTC transactions; challenges in tracking cross-border capital flows; and OTC's significant role as an intermediary in fraud and money laundering cases.

In the legislative proposal of《VA Dealing》 released by the government in 2025, it is clearly pointed out that based on these feedback, the regulatory scope which was originally only covering OTC exchange will be expanded to a more complete full chain business of VA Dealing.

VA Dealing Consultation Paper, 1.8：
“Following the conclusion of the first round of consultation, we received over 70 written submissions from various stakeholders... We have refined our proposal to expand the scope to VA dealing services to better address AML/CFT risks.”

Summary

The OTC market, once the "underground network" of Hong Kong's cryptocurrency sector, is now being brought into the spotlight. From platform regulation in 2023 to the 2024 regulatory integration of crypto exchanges, and further to the full-chain "VA Dealing" framework proposed for 2025, Hong Kong's virtual asset supervision is evolving toward systematic and internationalized governance.**The latest chapter of this is in the public consultation period, awaiting final legislation.**

Highlights of Phalcon Compliance APP upgrade

Phalcon Compliance APP is built by BlockSec, a team that has long focused on cutting-edge research in blockchain security and compliance, and has made breakthroughs in phishing attack defense, crypto asset tracking, and anti-money laundering analysis.

Three new risk indicators: keep up with the latest FATF requirements

The Phalcon Compliance App continues to follow the latest FATF regulatory standards with three new key risk indicators:

Terrorist Financing- Critical

- Identify addresses associated with terrorist organizations or the financing of terrorist activities
- Integrated into the existing illegal entity risk engine
- Trigger the highest level of risk alert

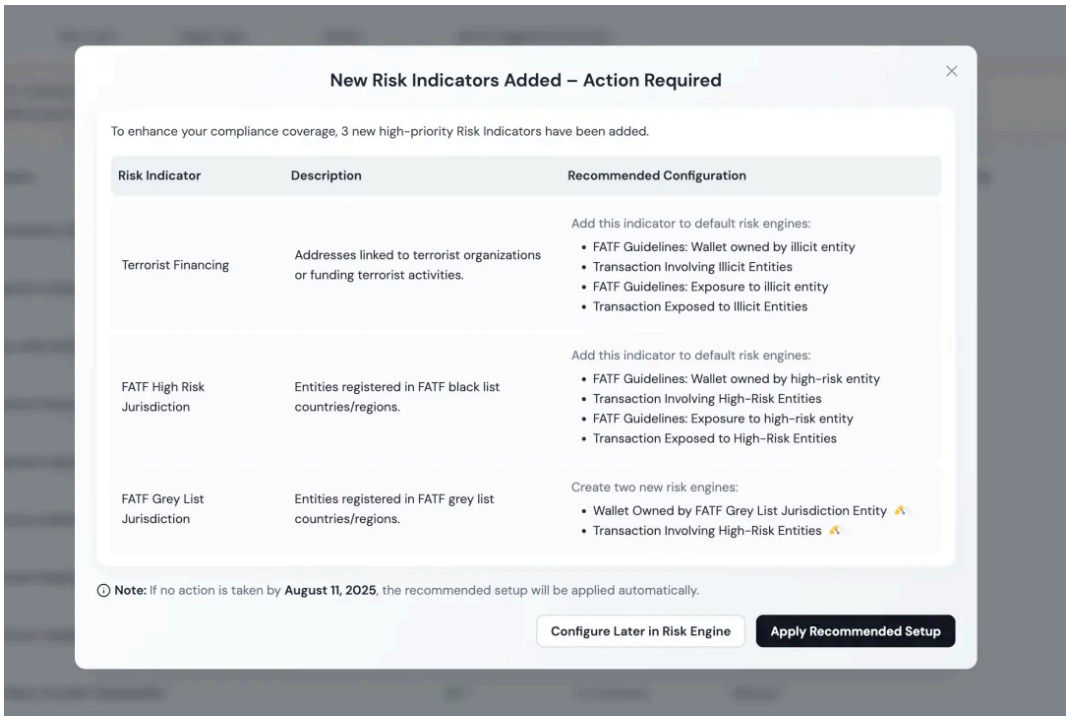
FATF High Risk Jurisdiction -High Level

- Automatically identify entities from blacklisted countries such as North Korea, Iran and Myanmar
- Transactions involving high-risk entities will be closely monitored

Support real-time risk rating updates

FATF Grey List Jurisdiction -Medium level

- Entity identification covering 24 gray list jurisdictions
- Create a dedicated gray list risk engine
- Provide progressive risk management strategies



This product integrates core capabilities including over 400 million address tags, unlimited hop tracking, and customizable risk rules. By simply importing addresses and transactions, users can automatically identify risks related to money laundering, terrorist financing, phishing, fraud, and other illegal activities through risk exposure analysis and on-chain behavior monitoring. The system supports automated alerts, team collaboration, blacklist management, and one-click export of STR reports compliant with regulations in the United States, Singapore, Hong Kong, and other regions. This empowers efficient identification, management, and response to complex compliance risks, achieving dynamic risk control and full-process compliance implementation.

The true boundaries and technical paths of KYC obligations for stablecoins

Article source: BlockSec WeChat account **Release time:** August 2025

In view of the widespread controversy in the industry on KYC requirements for Hong Kong stablecoin, this paper clarifies the definition criteria of "customer" and "non-customer" based on an in-depth study of regulatory documents, and analyzes the alternative relationship between technical risk control and KYC requirements.

The recent debate about the regulation of Hong Kong's stablecoin has intensified. There has been a lot of interpretation on the Internet that "stablecoin holders need to be authenticated (KYC)", which has sparked widespread controversy:

"KYC is required for on-chain transfers. How can it be decentralized?"

"Is regulation too conservative to be conducive to financial innovation?"

While these arguments hold water, do they truly capture the Hong Kong Monetary Authority (HKMA)'s regulatory intent? After conducting an in-depth analysis of two pivotal documents——the "Guidelines for Supervising Stablecoin Issuers" and the "Anti-Money Laundering and Terrorist Financing Guidelines", we have uncovered a more nuanced answer that delves into technical specifics and legal boundaries.

Not all holders are required to KYC, provided that the issuer can demonstrate that its risk control mechanisms are sufficiently effective.

This article will start from the division of customers vs non-customers and Primary vs Secondary markets, sort out the applicable logic of KYC for stablecoins, clarify the true bottom line of regulation, and provide a judgment framework applicable to both project parties and compliance teams.

Who is the customer, who is not the customer?

First of all, we need to make it clear that in the HKMA regulatory framework, "stablecoin holders" are not the same as "customers of stablecoin issuers".

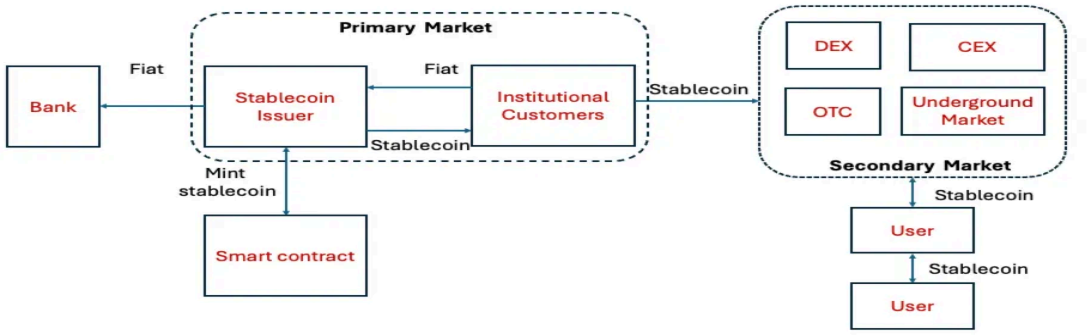
4.1. The term “stablecoin holder” in this Guideline refers to a person who has possession of the specified stablecoin issued by a licensee. A person should be treated as a customer of the licensee if (i) a business relationship7 has been established between the person and the licensee; or (ii) the licensee carries out an occasional transaction8 for a person (both (i) and (ii) hereafter referred to as “customer” or “customer stablecoin holder”). Other stablecoin holders that are not the licensee’s customers are referred to as “non-customer stablecoin holders”.

According to the definition in Chapter 4 of the Anti-Money Laundering and Anti-Terrorist Financing Guidelines, only when a user directly requests an issue or redemption of a stablecoin from the issuer, or establishes a business relationship, will be considered a "customer", who is required to strictly enforce the KYC/KYB process.

6.42 For the avoidance of doubt, a licensee does not need to observe paragraphs 6.40 to 6.41 for peer-to-peer transfers of stablecoins between unhosted wallets of non-customer stablecoin holders. It should however undertake adequate ongoing monitoring of stablecoins in circulation following the guidance in paragraphs 5.9 to 5.12.

Users who receive, transfer, and trade stablecoins on the chain but never interact directly with the issuer (e.g., those who acquire stablecoins through DEX purchases or wallet transfers) are classified as "non-customer stablecoin holders" and are generally not required to undergo KYC.

As shown in the figure below, only institutional users in the Primary Market are considered customers (customer), while participants in the Secondary Market are not defined as customers in the HKMA regulatory framework.



However, this does not mean that they are completely out of sight. Chapter 5 of the guidelines makes it clear that publishers have an obligation to continuously monitor all stablecoins in circulation, including those held by customers and non-customers.

5.9 A licensee, as an AML/CFT-obliged entity, has a responsibility for maintaining effective functioning of its stablecoins and guarding against the risk of their misuse for unlawful purposes. Ongoing monitoring of stablecoins in circulation is crucial for the licensee to discharge its AML/CFT responsibilities. The extent of such ongoing monitoring should be proportionate to the associated ML/TF risks identified in the licensee's institutional risk assessment (see paragraph 2.2), taking into account the nature of the licensee's business model (e.g. open or closed-loop).

KYC is not the only way, but it is the regulatory bottom line

Many of the interpretations that have led to misunderstanding often ignore an important premise set by the HKMA：

"Non-customer stablecoin holders may not do KYC, provided that the issuer has established an effective on-chain risk control mechanism and can demonstrate to regulators that it is adequate to prevent money laundering and terrorist financing risks."

In other words, KYC is not the only tool, but it is the bottom line.

5.10 All on-chain stablecoin transactions 37 are recorded instantaneously and automatically on the blockchains on which they take place, and such records provide some traceability of transactions which can aid in identification of potential illicit activities, as well as wallet addresses involved in such activities. Subject to paragraph 5.11, a licensee may apply various measures to guard against the risks of stablecoins being used for illicit activities. Examples of possible measures include:

5.11 As the effectiveness of these risk mitigating measures is yet to be proven, the HKMA expects licensees to adopt a cautious approach in determining whether their systems are adequate for mitigating ML/TF risks associated with licensed stablecoin activities, in particular as regards peer-to-peer transfers between unhosted wallets. Unless a licensee can demonstrate to the HKMA's satisfaction that these risk mitigating measures are effective in preventing and combating ML/TF and other crimes, the identity of each individual stablecoin holder should be verified (i) by the licensee even if the holder has no customer relationship with the licensee; (ii) by an appropriately supervised FI or VASP; or (iii) by a reliable third party.

If issuers adopt methods such as blockchain analysis tools, address blacklists, transaction risk scoring, wallet profiling and freezing mechanisms (5.10) to monitor the flow and use of coins, and can make the HKMA "satisfied" (to the HKMA's satisfaction-5.11), then these technical risk control measures can be used as alternatives without forcing a KYC check on every coin holder.

However, if these measures prove insufficient to mitigate risks in practice or fail to achieve this objective, regulatory expectations will automatically revert to the most conservative option——requiring all cryptocurrency holders to undergo identity verification (KYC), regardless of whether they are clients. It should be noted that even when KYC is required for crypto holders, stablecoin issuers may delegate the KYC process to Virtual Asset Service Providers (VASPs) and trusted third parties.

For publishers, it's a "either/or" choice

For stablecoin issuers, this is really a "either/or" compliance choice:

Or establish a set of risk monitoring system covering the whole chain, including real-time address portrait, suspicious transaction identification, blacklist interception, freezing mechanism and STR reporting process;

Or accept a more straightforward but costly option: KYC for all holders, even if they just received a stablecoin on the chain.

From a regulatory perspective, this design isn't conservative at all—it ties technical capabilities to regulatory obligations. You can skip real-name verification for every user, but you must have the ability to manage risks. Otherwise, you'll end up reverting to the original approach—— of KYC.

This is also the focus of this paper:

"Whether stablecoin holders need KYC": It's not a one-size-fits-all question, but depends on whether the issuer's risk control ability is trustworthy.

Bottom line: The regulation is clear, and the technology is due

Regulating stablecoins is not about blocking technology, but about setting a clear red line:

You can choose a technical solution to replace real-name registration, but you can not avoid the responsibility of risk control.

For publishers, the key question is not "do you want to do KYC" but —— do you have the ability to convince HKMA that you can do it without.

Under the principle of "same activity, same risk, same regulation", stablecoins as quasi-payment tools are now facing the same compliance requirements as traditional finance. For Web3 projects, this is not the end but a new starting point: with regulations clarified, it's time for technology to deliver its performance.

If you're designing a stablecoin product, participating in compliance reviews, or struggling to balance KYC and user experience, hopefully this will help you clarify your thinking.

6.2. FATF Global Regulatory Assessment interpretation

Article source: BlockSec WeChat account **Release time:**August 2025

As the global standard-setter for anti-money laundering, the Financial Action Task Force (FATF) annual assessment report serves as a key indicator of regulatory standards worldwide. This article provides an in-depth analysis of FATF's 2025 latest report, revealing the current state and future trends of global crypto regulation.

In June 2025, the FATF released its sixth targeted update on the regulation of crypto assets, and the conclusion is shocking:

Only one jurisdiction worldwide has achieved the Financial Action Task Force (FATF)'s "full compliance" standard in virtual asset regulation, while a staggering 20% of countries remain in non-compliance. Meanwhile, North Korean hackers have made history by stealing $1.46 billion in crypto assets, stablecoins have become the new darling for money laundering activities, and regulatory frameworks for the DeFi sector continue to remain a foggy area...

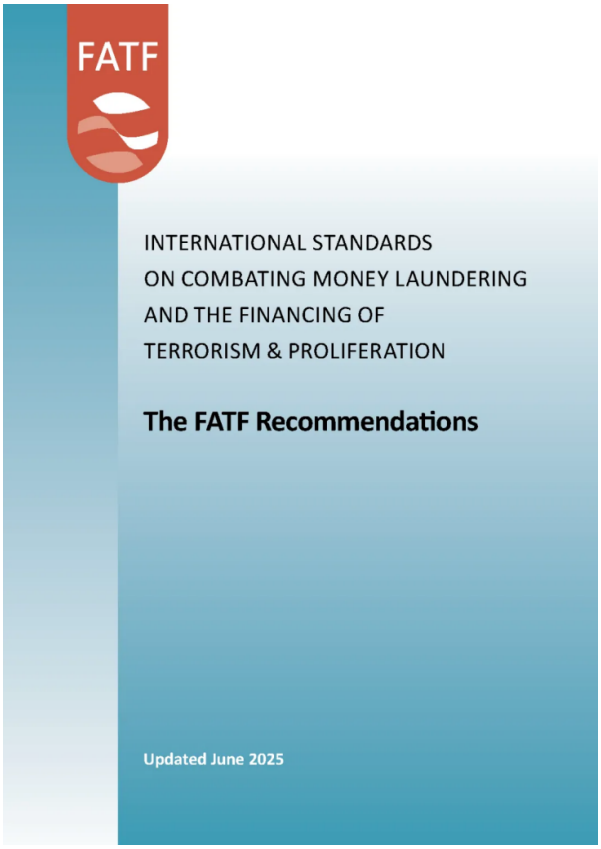
Behind this seemingly chaotic global crypto regulatory landscape, there is an invisible hand quietly shaping the rules of the game for the entire industry—— and that is the FATF.

This article will provide an in-depth analysis of the six key findings of the FATF's latest report, reveal the latest "black and grey list" countries in 27 countries, and look ahead to important changes in crypto regulation in 2026. It will help you understand the "source code" of global regulation.

Who is FATF? The global "standard-setter" on anti-money laundering

FATF（Financial Action Task Force)，Established in 1989, it is the world's authoritative standard-setting body for anti-money laundering and counter-terrorism financing (AML/CFT). This intergovernmental organization, comprising 39 member states and regional organizations, has developed anti-money laundering recommendations that are widely regarded as the "gold standard" of global AML/CFT.

For the crypto industry, the FATF's most critical document is Recommendation 15 (R.15), which for the first time in 2019 included virtual assets and VASP in the anti-money laundering regulatory framework: VASP is required to perform compliance obligations such as customer due diligence, transaction monitoring, and suspicious transaction reporting, just like traditional financial institutions.



The FATF is not a police force, yet it has made Binance pay a $4.3 billion fine; the FATF has no military, yet it can "isolate" entire countries from the international financial system; the FATF does not make laws, yet it has 205 jurisdictions legislate according to its standards.

Why can an international organization without law enforcement power play such a key role in global encryption regulation?

The answer is simple: In this decentralized crypto world, the FATF has ironically become the "centralized" global standard-setter. While national regulators are still figuring out how to manage this emerging industry, FATF's R.15 framework has emerged as their shared "gold standard". Whether it's FinCEN in the US, the EU's AMLD6, Singapore's Monetary Authority (MAS), or Hong Kong's recently enacted Stablecoin Ordinance, the FATF standards leave an unmistakable mark on these regulatory frameworks.

Interestingly, through its unique **"soft law" mechanism**—— peer review and "greylist" system——, the FATF has transformed non-binding recommendations into mandatory "hard rules" that all countries must follow. What does being placed on the FATF greylist mean? Turkey and Cambodia should be well aware—— of the consequences: blocked international remittances, foreign capital withdrawal, and credit rating downgrades... No country would willingly bear such costs.

For crypto practitioners, understanding the FATF is understanding the "source code" of global regulation. When you know that national regulations are "localized" based on the same FATF standards, you can better anticipate regulatory trends, plan your compliance system in advance, and conduct business globally.

Interpretation of the latest FATF report 2025:

Six key findings

In June 2025, FATF released its sixth "Targeted Update Report on the Implementation of FATF Standards for Virtual Assets and Virtual Asset Service Providers".

Through an in-depth survey of 163 jurisdictions, the FATF decodes the true state of global crypto compliance through six key findings.

Discovery 1: Global compliance progress is slow but steady

As of April 2025, in 138 jurisdictions that have been assessed:

- Only one jurisdiction fully compliant: The Bahamas
- 29% were basically compliant, up slightly from 25% in 2024, including the United States, The United Kingdom, Germany and Singapore
- 449% partial compliance, including: Hong Kong, Netherlands, Turkey
- 21% non-compliant, down from 25% in 2024, including Cambodia, Vietnam

BlockSec explains: Compliance lists are constantly changing. For businesses using crypto payments, how to adjust their strategies in a timely manner according to FATF guidelines and identify wallet addresses and users belonging to non-compliant countries is a new challenge that must be faced.

Discovery 2: How to deal with risk is the main challenge

76% of the jurisdictions surveyed reported having performed a ML/TF risk assessment for VA/VASP, up from 71% in 2024. But here's the catch:

- While risk assessments have been completed in many jurisdictions, there are still difficulties in implementing prevention measures
- Only 40 jurisdictions met the "assess risks and take a risk-based approach" criteria, including Switzerland, Japan and others

BlockSec explains: Risk assessments in many countries remain at the reporting level, lacking mechanisms to translate findings into concrete implementation measures. Both nations and crypto companies need to establish a dynamic, flexible, and actionable risk management system.

Discovery 3: Diverging regulatory paths

- 62% of jurisdictions chose to allow VAs and VASPs to operate, including the US, major EU countries
- 20% chose to completely ban crypto activities, a significant increase from 14% in 2024, including China and Egypt.
- Eighteen percent have yet to decide on regulatory direction, including some in Southeast Asia and Africa

Of particular note, partial bans (rather than total bans) are becoming the trend: 48% of jurisdictions with bans choose to partially ban specific VA/VASP activities rather than a one-size-fits-all approach.

BlockSec explains: Regulatory fragmentation means cross-border compliance will become more complex. Companies need to develop differentiated compliance strategies for different markets.

Discovery 4: Breakthrough progress in the implementation of Travel Rule

While the 73% of jurisdictions (85) that have passed legislation to implement the Travel Rule may seem flat in 2024, the absolute number has increased from 65 to 85, indicating substantial progress.

Travel Rule requires VASPs to obtain, maintain and transfer specific remitter and recipient information when transferring virtual assets, which is equivalent to extending traditional financial KYC requirements into the crypto space.

BlockSec Analysis: While the global adoption of Travel Rule represents a significant trend, it still faces substantial challenges in the crypto world. The anonymous nature of blockchain technology allows individuals to easily create multiple wallet addresses without real-name verification. Although clients using centralized services (e.g., crypto exchanges) may submit KYC documents, self-custody users face difficulties in obtaining identity information, and even when such data is obtained, verifying its authenticity remains challenging.

Discovery 5: Stablecoins are the new favorite for money laundering

In particular, the report notes that stablecoins are becoming the tool of choice for all kinds of illegal actors:

- Most illegal activities on the chain now involve stablecoins
- Criminals use stablecoins in conjunction with anonymity enhancement tools (such as coin mixers, cross-chain bridges) to stratify funds
- The use of USDT on the Tron network is particularly favored by illegal actors

BlockSec Analysis: Stablecoin Regulation to Become a Key Focus in 2025-2026. Issuers 'freezing and monitoring capabilities will play an increasingly vital role. For details on the KYC controversy surrounding Hong Kong's stablecoins, check out our in-depth analysis: Does Holding Coins

Require Real Name Verification? The True Boundaries of Hong Kong Stablecoin KYC Obligations

Discovery 6: North Korean hackers set new record

North Korean hackers stole $1.46 billion worth of virtual assets from the crypto exchange ByBit in 2025, a record single theft. Ultimately, less than 4 percent of the stolen funds were recovered.

BlockSec's Interpretation: **Cybersecurity and AML/CFT compliance must be equally prioritized.** Organizations with only compliance frameworks but lacking security measures remain vulnerable to cyberattacks. Cryptocurrency enterprises should implement a "double insurance" system: On the cybersecurity front, deploy real-time monitoring and automated attack-blocking systems (e.g., Phalcon Security App) to detect and intercept threats at their earliest stage; on the compliance front, adopt comprehensive KYA solutions that analyze blockchain activities to identify wallet addresses associated with North Korean hacker groups.

Looking at these six findings, a clear thread emerges: **global crypto regulation is moving from a "chaotic period" to an "orderly period," but the process is far more tortuous than expected.**

The striking contrast between "knowledge and action" reveals a critical gap—— While 76% of countries understand their regulatory objectives (with risk assessments completed), only 29% achieve near-compliance. This highlights the fundamental challenge in crypto regulation: How to establish an effective yet innovation-friendly framework that balances oversight with technological progress in this fast-evolving field?

The Financial Action Task Force (FATF) has outlined a framework of **progressive reform and global coordination**. By establishing unified standards with localized adaptations and combining soft compliance measures with binding consequences, FATF is steering the world toward a new regulatory paradigm characterized by "harmony in diversity." For crypto enterprises, this transformation means compliance is no longer optional but a prerequisite for market entry; it's no longer a cost center but a source of competitive advantage.FATF

Countries also get black and grey? 27 countries on the list

If the FATF is the "gatekeeper" of the global financial system, then the black and grey lists are the "wanted notices" in its hands. The annual update of the list will trigger a chain reaction in the global financial market.

What is the FATF Grey List?

The FATF Grey List is formally known as "Jurisdictions under Increased Monitoring" and includes countries and territories with strategic deficiencies in anti-money laundering, counter-terrorism financing, and counter-proliferation financing. These countries have committed to quickly resolve identified strategic deficiencies within agreed timeframes and are subject to increased monitoring.

Grey List Countries by Region

Africa (12 countries)


Algeria


Angola


Burkina Faso


Cameroon


Côte d'Ivoire


DRC


Kenya


Mozambique


Namibia


Nigeria


South Africa


South Sudan

Americas (4 countries)


Bolivia


Haiti


Venezuela


Virgin Islands UK

Europe (2 countries)


Bulgaria


Monaco

Asia (3 countries)


Lao PDR


Nepal


Vietnam

Middle East (3 countries)


Lebanon


Syria


Yemen

June 2025 List Changes

- Countries removed from the list: Croatia, Mali, Tanzania
- Countries newly added to the list: Bolivia, British Virgin Islands

Search in Wechat

BlockSec

BLOCKSEC

The "Big Three" of the blacklist

- North Korea: "Nail Households" Since 2011, the mastermind behind $1.46 billion ByBit theft
- Iran: Nuclear issue combined with terrorist financing risk, financial system completely isolated
- Myanmar: Listed after 2022 coup, regulatory vacuum becomes money laundering haven

Any financial dealings with countries on the blacklist are "high-voltage lines" —— ranging from regulatory penalties to account freezing and settlement interruption.

Three trends on the grey list

- Africa is the hardest hit: 12 countries on the list, South Africa still on the list as Africa's light
- The crypto hot spot is awkward: Nigeria (the world's second largest P2P transaction volume) and Vietnam (one of the top three crypto adoption rates) are lagging behind in regulation
- The offshore centre dilemma: The British Virgin Islands and Monaco are paying the price for their past lax regulation: international remittances are 30-50 per cent higher, foreign investment is 20-40 per cent lower and credit ratings are downgraded

FATF 2026 regulatory "spoiler"

Looking back at the FATF's reporting history:

Travel Rule Directive 2019:50+ countries to legislate within 2 years

The 2020 stablecoin report has triggered a wave of global regulation

Just like a regulatory "script",—— knowing the focus 6-12 months in advance gives you a head start on regulatory changes.

Three major FATF reports coming out

1. Special Report on Stablecoin (Q12026)

Core points: reserve transparency standards, off-anchoring responsibility definition, cross-chain supervision

2. Offshore VASP Report (2025-2026)

Key points: "long-arm jurisdiction" boundaries, data localization, cross-border enforcement

3. DeFi Regulatory Guidelines (2025-2026)

Core points: identification of responsible subjects, legal status of DAO, smart contract audit

An interesting discovery

The FATF report tends to follow a "seasonal pattern" —— with major reports released in June and October.

A savvy compliance team closely monitors both timelines, swiftly gathering intelligence and responding to developments. In the regulatory race, information is time, and time is advantage. Companies that anticipate regulatory shifts first naturally gain a first-mover advantage in market competition. The FATF's latest report clearly indicates a trend: global crypto regulation is transitioning from "wild growth" to "regulated development". Although only one jurisdiction has achieved full compliance, this highlights the vast potential and market opportunities within the crypto world.

The latest FATF report reveals a clear trend: global crypto regulation is transitioning from "wild growth" to "regulated development". While only one jurisdiction has achieved full compliance, this highlights the vast potential and market opportunities within the crypto sector.

Highlights of Phalcon Compliance APP upgrade

In the face of FATF's escalating regulatory requirements, VASP faces huge compliance challenges: How to navigate between the regulatory requirements of different jurisdictions? How to identify high-risk transactions from black and grey list countries in a timely manner? How to establish a risk assessment and monitoring system that meets FATF standards?

Phalcon Compliance APP is built by BlockSec, a team that has long focused on cutting-edge research in blockchain security and compliance, and has made breakthroughs in phishing attack defense, crypto asset tracking, and anti-money laundering analysis.

This product integrates core capabilities including over 400 million address tags, unlimited hop tracking, and customizable risk rules. By simply importing addresses and transactions, users can automatically identify risks related to money laundering, terrorist financing, phishing, fraud, and other illegal activities through risk exposure analysis and on-chain behavior monitoring. The system supports automated alerts, team collaboration, blacklist management, and one-click export of STR reports compliant with regulations in the United States, Singapore, Hong Kong, and other regions. This empowers efficient identification, management, and response to complex compliance risks, achieving dynamic risk control and compliance implementation throughout the entire process.

Contact Us

Book A Demo:

https://blocksec.com/book-demo

Website:

https://blocksec.com

X(Twitter):

@BlockSecTeam

@phalcon_xyz

@MetaSleuth

@MetaDockTeam

Email:

contact@blocksec.com