REGULATING CRYPTO-ASSETS FOR ANTI-MONEY LAUNDERING AND TERRORIM FINANCING - INTERNATIONAL EXPERIENCE AND POLICY IMPLICATIONS FOR VIETNAM

Assoc.Prof.PhD. Nguyen Le Cuong* - PhD. Tran Thi Lan* - PhD. Nguyen Thi Thuy Dung*
PhD. Phung Thanh Loan*

Abstract: ***The rapid rise of crypto-assets has transformed the financial landscape, providing new opportunities for investment and innovation. However, this growth has also introduced significant risks related to money laundering and terrorist financing. In 2023, Vietnam was included in the "grey list" of FATF mainly because Vietnam's regulatory response to risks arising from crypto-assets has been deemed insufficient. The paper reviews the latest FATF recommendations concerning crypto-assets and examine how different countries have implemented these guidelines. The research will analyze the effectiveness of various regulatory strategies in addressing ML/TF risks associated with crypto-assets and will subsequently propose relevant implications for the Vietnamese government.***

• Keywords: *crypto assets, regulation, anti-money laundering, terrorism financing, Vietnam.*

Date of receipt: 03rd Feb., 2025
Date of delivery revision: 27th Feb., 2025
Date of receipt revision: 12th Mar., 2025
Date of approval: 15th Mar., 2025
DOI: https://doi.org/10.71374/jfar.v25.i3.32

1. Introduction

The rapid rise of crypto-assets has transformed the financial landscape, providing new opportunities for investment and innovation. Vietnam is indexed in the top 5 countries in the world with the highest crypto-assets adoption in 2024 (Chainalysis, 2024). However, this growth has also introduced significant risks related to money laundering and terrorist financing (ML/TF). In 2023, Vietnam was included in the "grey list" (aka jurisdictions under increased monitoring) of The Financial Action Task Force (FATF) mainly because Vietnam's regulatory response to risks arising from crypto-assets has been deemed insufficient. Being included in the grey list could lead to several adverse consequences such as decreased foreign investment and economic activity. This explains why the Vietnamese government issued Decision No. 194/QD-TTg dated February 23, 2024 in promulgating the National Action Plan to remove Vietnam from this "grey list"; particularly, Action 6 specifies "*Building a legal framework to ban or regulate virtual assets and organizations providing virtual asset services, and demonstrate the implementation of regulations including measures to ensure compliance*", which needs to be completed before May 2025.

The primary objective of this study is to review the latest FATF recommendations concerning crypto-assets and examine how different countries have implemented these guidelines. The research will analyze the effectiveness of various regulatory strategies in addressing ML/TF risks associated with crypto-assets and will subsequently propose relevant implications for the Vietnamese government. This study employs a qualitative research methodology, involving a literature review of FATF reports, regulatory documents from multiple jurisdictions, and academic articles on crypto-assets. Comparative analysis will be used to identify best practices and challenges faced by different countries in implementing FATF recommendations.

2. International ML/TF regulation related to crypto-assets

2.1. FATF rules on regulating virtual assets

The latest guidance from the FATF on virtual assets (VAs)[1] and virtual asset service providers (VASPs) emphasizes the need for robust regulatory frameworks to combat money laundering and terrorist financing risks associated with these assets. FATF recommends the following points in regulating virtual assets:

[1] *There has not been a consersus in defining crypto-assets and virtual- assets; but generally, these two terms are used interchangeably.*

* *Academy of Finance*

+ Risk-Based Approach: Authorities are encouraged to implement a risk-based approach to VAs and VASPs, tailoring regulation based on the specific risks posed by different types of assets and activities.

+ Regulatory Frameworks: Countries should ensure that VASPs are subject to the same AML/CFT obligations as traditional financial institutions, including registration, licensing, and compliance with customer due diligence (CDD) requirements.

+ Travel Rule Compliance: The guidance reiterates the importance of the travel rule, requiring VASPs to collect and transmit information about the originator and beneficiary of transactions, similar to traditional banking systems.

+ Definition Clarity: VAs and VASPs should be clearly defined within national legislation to ensure comprehensive coverage under AML/CFT regulations.

+ Supervisory Practices: Effective supervision of VASPs is crucial. Authorities are advised to develop supervisory practices that are adaptable to the rapidly evolving nature of the cryptoasset market.

Despite FATF's efforts and detailed guidelines on this matter, BIS (2021) still report that the adoption of these recommendations especially the Travel Rule widely vary across jurisdictions. Additionally, jurisdictions also differ in their approach to implementing AML/CFT measures for crypto-asset service providers. Some apply existing frameworks, while others have developed new, tailored regulations. Generally, crypto-asset service providers are required to comply with AML/CFT preventive measures similar to traditional financial institutions. This includes conducting customer due diligence (CDD), maintaining records, applying a risk-based approach, and reporting suspicious transactions to the relevant financial intelligence units.

2.2. Case studies

KOREA

In 2020, South Korea passed an amendment to the Act on Reporting and Using Specified Financial Transaction Information, which took effect on March 25, 2021 (FSC, 2021). The law establishes direct regulations on anti-money laundering and counter-terrorism financing for Virtual Asset Service Providers (VASPs). The law defines VASPs as entities engaged in the buying/selling, exchanging, transferring, storing, brokering, and managing virtual assets. Thus, VASPs include cryptocurrency exchanges, wallet operators, and cryptocurrency custodians. The main obligations that VASPs must fulfill include:

+ Registration: VASPs must register with the Korea Financial Intelligence Unit (KoFIU). They are required to provide detailed information about the company and its legal representatives to KoFIU.

+ Information Security Management System (ISMS) Certification: VASPs must obtain ISMS certification from the Korea Internet & Security Agency (KISA) under the Act on Promotion of Information and Communications Network Utilization and Information Protection to verify that they can protect the important assets and information of investors.

+ ML/TF Obligations: VASPs have specific anti-money laundering and counter-terrorism financing responsibilities and must comply with three main obligations: (i) customer identification (KYC); (ii) reporting suspicious transactions (STR); and (iii) data retention. VASPs must verify the identity of customers when they open accounts and further verify the purpose of transactions and the sources of funds involved.

+ Obligations for Financial Institutions: The Act on Reporting and Using Specified Financial Transaction Information also imposes obligations on financial institutions when transacting with VASPs. When financial institutions engage with VASPs, they must verify the identity of the VASP by requiring them to open real-name accounts and check whether the VASP's assets/deposits are segregated from their customers' deposits.

SINGAPORE

Singapore's Anti-Money Laundering and Counter-Terrorist Financing Notice PSN02 guidance provides that the board of directors and senior management of Digital Payment Tokens service providers have strong and sound governance responsibilities to control money laundering and terrorist financing risks. The board of directors and senior management of the payment service provider are ultimately responsible for ensuring compliance with anti-money laundering and terrorist financing laws, regulations and notices (MAS, 2024).

Under Guidance PSN02, DPT service providers must establish three lines of defense to combat the use of DPTs for money laundering and/or terrorist financing.

+ The first line of defense consists of business units (e.g., departments that directly interact with customers at the business premises of payment service providers). Payment service providers are obligated to ensure adequate resources, including IT, to detect illegal transactions and to train employees so that they are fully aware of their obligations and avoid legal violations when interacting with customers.

+ The second line of defense is the anti-money laundering and counter-terrorism financing compliance department, which continuously monitors compliance with all anti-money laundering and counter-terrorism financing obligations. The compliance department is responsible for reporting to the board of directors or senior management when employees are struggling or not adequately addressing risks and concerns related to money laundering and terrorist financing.

+ The third line of defense is the internal control department of the payment service provider or an independent auditing firm. This department plays a crucial role in independently assessing the framework for managing money laundering and terrorist financing risks.

The three lines of defense of the payment service provider must ensure the implementation of the following requirements: Risk Prevention; Customer Due Diligence, enhanced Due Diligence, Transaction Monitoring, Reporting Suspicious Transactions; Record Keeping.

TURKEY

Similar to Vietnam, in 2021, the FATF placed Turkey on the "grey list" due to the fact that Turkey only "partially compliant" with FATF standards regarding new technologies such as cryptocurrencies. In 2021, the Amendment Regulation on Imposing Specific Obligations on Virtual Asset Service Providers (VASPs) under Law No. 5549 on the Prevention of Laundering of the Proceeds of Crimes (Law No. 5549) was introduced. Then, Financial Crimes Investigation Board (FCIB) published Guidelines on the Main Principles Regarding the Prevention of Money Laundering and Financing of Terrorism for VASPs (AML Guidelines). According to the definition in the aforementioned Guidelines, VASPs "intermediate transactions of virtual assets through electronic trading platforms." (Global Insight, 2025)

The key compliance obligations of VASPs include:

+ The primary obligations of VASPs are (1) customer identification (KYC), (2) reporting suspicious transactions, and (3) providing information and documentation.

+ The KYC process must be completed before entering into a contract (establishing a business relationship) or conducting a transaction. The accuracy of the name, surname, date of birth, identification number (for Turkish citizens), and type and number of identification documents must be verified with documentation.

+After submitting the original or notarized copy of the identification documents to be verified to the VASP, a copy or electronic image or identity information will be recorded for submission to the competent authority upon request.

+ The accuracy of the declared address in the long-term business relationship must be verified through (i) a residence certificate, (ii) a bill in the name of the individual related to subscription services such as electricity, water, natural gas, or telephone issued within three months from the date of the transaction, or (iii) other documents and methods deemed appropriate by the FCIB.

+ Reporting suspicious activities to the FCIB is another crucial principle for preventing money laundering and terrorist financing. VASPs are also obligated to provide ongoing information to the FCIB, in addition to reporting suspicious transactions as described above.

3. Policy implications for Vietnam

Based on global experiences and FATF guidance on regulating crypto-assets for anti-money laundering and terrorism financing (AML/TF), here are several recommendations for Vietnam:

Establish a Clear Regulatory Framework

The first step is to develop clear definitions for crypto assets and crypto asset service providers within Vietnamese legislation to ensure comprehensive regulatory coverage. Currently, a Draft Law on Digital Technology Industry is proposing definition for "digital assets", "crypto

assets"; but there has not been a definition for "crypto asset service providers". Additionally, the framework should adopt a risk-based classification system for different types of crypto-assets, considering their functionalities and risks. For example, if a crypto asset has a function being similar to a financial instrument, it should be subject to related financial regulation like the traditional financial assets. if a crypto asset does not meet this criterion, should alternative classifications be considered. Likewise, some activities or certain types of assets need to be considered and managed immediately due to many potential risks for investors. For example, the public issuance of security token; transaction activities including storage services (hot and cold wallets), activities with potential risk of money laundering to finance terrorism.

Conduct Risk Assessment and Review over risks arising from crypto-assets.

Vietnam should conduct a comprehensive national risk assessment (NRA) focusing on the potential risks posed by crypto-assets and VASPs to inform regulatory measures. The latest NRA was 2018-2022; the next round of this assessment should include the risk arising from crypto-assets. The assessment should identify potential risks from crypto-assets, including market volatility, fraud, and systemic risks to the financial system. The assessment should evaluate how these risks could affect various sectors, including finance, consumer protection, and national security. To ensure the proper assessment, the government involve relevant stakeholders, including government agencies, financial institutions, and industry experts, to gather diverse perspectives and insights.

Implement AML/CFT Obligations applied to crypto-asset service providers

Various countries have fully adopt different requirements KYC Requirements. Currently, in line with the Law on Anti-money laundering issued in 2022, there are various organizations being subject to apply AML/CFT requirement. Hence this requirements should be also applied to cryto-asset service providers in the future. The key requirements include: mandate cryto-asset service providers to perform robust customer due diligence (KYC) during onboarding and ongoing monitoring of transactions; require cryto-asset service providers to report suspicious transactions to the relevant financial intelligence unit store relevant data similarly to other organizations responsible for the administration of the Anti-Money Laundering Law. Some stringent requirement could specify all cryptocurrency transactions to be made through a bank account registered with a real name. Investors can only deposit and withdraw money between real-name bank accounts.

Enhance Supervisory Capacity

Vietnam should establish a dedicated regulatory body to oversee the crypto-assets market, ensuring it has the expertise and resources to monitor compliance effectively. It is important to provide guidance and training for regulatory staff to understand the complexities of crypto-assets and associated risks.

Promote International Cooperation

The regulatory bodies should engage in international cooperation with other jurisdictions to share best practices, intelligence, and resources for combating ML/CFT risks in the crypto sector. It would be helpful to collaborate with international organizations such as the FATF and World Bank to gain insights and assistance in crafting regulatory frameworks.

4. Conclusion

As Vietnam continues to embrace the digital economy, addressing the ML/TF risks associated with crypto-assets is critical. By learning from the FATF recommendations and the regulatory experiences of other countries, Vietnam can develop a robust framework that promotes innovation while safeguarding its financial system. This research contributes to the ongoing discourse on effective regulation of crypto-assets, offering practical insights for policymakers in Vietnam.

References:

BIS (2021), Supervising cryptoassets for anti-money laundering. Accessed via https://www.bis.org/fsi/publ/insights31.pdf

Chain Analysis, 2024: 2024 Global Crypto Adoption Index. Truy cập tại https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

FATF (2025), Virtual Assets. Accessed via https://www.fatf-gafi.org/en/topics/virtual-assets.html

FSC (2021), FSC Proposes Additional Rules Change on Virtual Asset Service Providers- Press Release. Accessed via https://www.fsc.go.kr/eng/pr010101/75410

Global Insight (2025), Turkey Blockchain & Cryptocurrency Laws and Regulations 2025. Accessed via https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/turkey-turkiye/

MAS (2024), Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service. Accessed via https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service