Crypto Assets and Money Laundering

Analysis of Montenegro and Taiwan Systems with Recommendations

TAIPEI REPRESENTATIVE OFFICE IN HUNGARY

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK | CRNA GORA

BIRN Montenegro

Crypto Assets and Money Laundering Analysis of Montenegro and Taiwan Systems with Recommendations

Publisher:
Balkan Investigative Reporting Network – Montenegro (BIRN Montenegro)

Document Author:
Vuk Maraš
February 2026

Note: Original version of the document is in Montenegrin. Any translation mistakes should be addressed by accessing the original document.

This activity was financed by the Taipei Representative Office in Hungary. The views and opinions expressed in this document are those of the author and cannot be considered as the positions of the donor who financially supported the project.

Summary

The analysis shows that both Montenegro and Taiwan have formally aligned their legislation with international standards, particularly FATF recommendations, but did so in different ways and with different practical results.

In 2025, Montenegro incorporated crypto assets directly into the Law on Prevention of Money Laundering and Terrorism Financing. A registry of crypto asset service providers was established and rules for transfer monitoring were prescribed, including the so-called "travel rule." The system is normatively correct, but in practice there are still no registered service providers.

The Financial Intelligence Unit had only a few crypto asset-related cases during 2024, received through bank reports, while BIRN Montenegro's investigations indicate the existence of large, unregistered and uncontrolled money flows through the crypto market.

Taiwan, on the other hand, significantly tightened its system in 2024. In addition to legislative amendments, a mandatory AML registration regime was introduced for all virtual asset service providers, with clear technical and security standards and strict "fit and proper" criteria. Taiwan also introduced serious criminal sanctions for unregistered operations in the digital asset sector.

The result of this approach was a doubling of suspicious transactions reported by the crypto sector, and the fact that after tightening the rules, two thirds of the previously registered virtual asset service providers (VASPs) lost their right to operate because they failed to meet the new standards.

The key difference between the two systems is not in the existence of legislation itself, but in the level of operational precision and enforcement. Taiwan has built a detailed and technically developed framework with clear sanctions and active supervision. Montenegro has laid the foundation, but without a specific digital asset law, without the criminal offense of unregistered provision of digital asset services, and without specialized supervisory capacities.

The document therefore proposes several concrete steps to improve the situation: introducing criminal liability for unregistered service providers, adopting a specific digital asset law aligned with European regulations, strengthening the supervisory capacities of the Financial Intelligence Unit and the Capital Market Commission, developing crypto-specific guidelines and typologies, and introducing blockchain analytics tools.

The core message of the analysis is clear – crypto assets are not the problem in themselves. The problem arises when institutions lack the capacity to identify, register and control entities trading in them. Taiwan's experience shows that it is possible to build a system that delivers results. Montenegro now has the opportunity to move from the phase of formal compliance to the phase of actual implementation and effective supervision.

Table of Contents

Introduction

The analysis compiled by BIRN Montenegro, comparing the anti-money laundering systems with a focus on digital assets of Montenegro and Taiwan, is the result of months of research aimed at improving Montenegro's legal framework and institutional practices. Research conducted by BIRN has shown that in Montenegro there exists a vast, shadow market of crypto assets that is almost entirely beyond the reach of institutions, with complete monetary flows occurring without any state knowledge.

In a series of investigative articles, we documented numerous cases flying under the radar – from purchases of luxury real estate with cryptocurrencies to street-level dealers through whose accounts millions passed. In just one case, over 17 million dollars were transacted through a single such account in one year.

Given that digital asset transactions are considered a highly sophisticated technological phenomenon, BIRN conducted research on various jurisdictions that have successfully tackled this issue.

In this specific case, we analyzed Taiwan's situation, because like Montenegro, Taiwan recently upgraded its legal framework to improve the effectiveness of anti-money laundering efforts in the digital asset space. In addition to researching the legal and institutional framework, BIRN Montenegro visited all relevant institutions in Taiwan responsible for preventing money laundering, as well as civil society organizations monitoring institutional activities. Through conversations with more than 30 people directly involved in various stages of the process, we obtained concrete and useful information that informed our recommendations for improvement in Montenegro.

List of Abbreviations

FATF – Financial Action Task Force – https://www.fatf-gafi.org

AML – Anti-Money Laundering

CFT – Combatting the Finance of Terrorism

VASP – Virtual Asset Service Providers

DLT – Distributed Ledger Technology

STR – Suspicious Transactions Report

ZoSPNiFT – Law on Prevention of Money Laundering and Terrorism Financing (Montenegro)

MCLA – Money Laundering Control Act

FSC – Financial Supervisory Commission

SFB – Securities and Futures Bureau

CFTA – Counter-Terrorism Financing Act

MJIB – Ministry of Justice Investigation Bureau

How the System is Structured

Montenegro and Taiwan have both moved toward compliance with FATF standards in the area of anti-money laundering and counter-terrorism financing, particularly regarding the control of digital assets, but they have done so in entirely different ways, creating different legal systems and institutional solutions.

Montenegro's current approach incorporates crypto asset obligations directly into the primary Law on Prevention of Money Laundering and Terrorism Financing[1] through amendments made in 2025. This includes the statutory "travel rule" model for crypto transfers and a specific registry of crypto asset service providers under the supervision of the capital market regulator.

Taiwan, by contrast, tightened its framework in 2024 through the Money Laundering Control Act[2] and Financial Supervisory Commission (FSC) regulations, establishing a set of measures including a mandatory AML registration regime for VASPs, with clear rules on classification, custody, transactions, and information security, and ensured their active enforcement.

---

[1] Zakon o sprječavanju pranja novca i finansiranja terorizma Crne Gore ("Službeni list Crne Gore", br. 110/23 od 12.12.2023, 065/24 od 05.07.2024, 024/25 od 12.03.2025

[2] Money Laundering Control Act (Adopted on 23.10.1996 and amended 10 times, last one on 31.07.2024. godine)

Montenegro's Anti-Money Laundering System with a Focus on Crypto Assets

The core of the system in Montenegro is the Law on Prevention of Money Laundering and Terrorism Financing, last amended in 2025, which contains a dedicated chapter on crypto assets. The Law broadly defines "crypto assets" as a digital representation of value or rights that can be transferred and stored electronically using distributed ledger technology (DLT) or similar technology, and explicitly recognizes the concept of "electronic money tokens," i.e., the definition of stablecoins pegged to fiat currencies. The system also recognizes NFTs, defined as unique and non-fungible crypto assets.

The function of the financial intelligence unit (FIU) is performed by the Montenegro Police Directorate through a dedicated sector for financial intelligence operations. This sector receives suspicious transaction reports (STRs) and other reports from obligated entities, conducts operational and strategic analyses, and, when suspicion thresholds are met, submits analytical reports to the competent prosecution. By law, this Police Directorate sector is operationally independent and autonomous in exercising its powers and making decisions relating to financial intelligence activities.

Supervision is divided among several bodies. Sectorally, the Central Bank of Montenegro supervises banks and certain financial institutions, while the Capital Market Commission of Montenegro supervises capital market participants and, most importantly for this analysis, providers of crypto asset-related services (VASPs).

Market Entry and Supervision of the Crypto Sector (VASP)

Montenegro requires that any entity intending to provide crypto asset-related services in Montenegro be entered into a specific registry (the "Registry of Crypto Asset Service Providers") prior to commencing operations.

The Capital Market Commission of Montenegro maintains the registry, and the FIU and other supervisory bodies have direct electronic access, while the public has access to information on the identity of the provider and the types of crypto asset-related services offered. Documentation required for registration includes identification data, appointment of an AML officer, evidence of compliance with owner and management criteria ("fit and proper"), and a business plan describing the crypto asset services to be offered.

Montenegro's law defines data-sharing obligations for crypto transfers – identification data of the sender and recipient that accompanies the transfer – and contains a specific risk-based rule for transfers involving self-hosted (unhosted) wallets. Specifically, when a crypto transfer occurs between a VASP and a self-hosted address and exceeds EUR 1,000, the VASP is required to assess whether that self-hosted address is owned or controlled by the sender or recipient. This architecture closely mirrors the model of the EU Funds Transfer Regulation as applied to crypto transfers.

Taiwan's Anti-Money Laundering System with a Focus on Crypto Assets

Taiwan's framework is based on the Money Laundering Control Act (MLCA), last amended on July 31, 2024, and accompanying sectoral regulations. The MLCA defines categories of regulated financial institutions and other entities subject to supervision and, following the amendments, explicitly extends AML obligations and market access controls to "enterprises or persons providing virtual asset services," including the requirement that domestic and foreign providers register for AML compliance and service capacity with the central competent authority.

The law also prescribes clear criminal sanctions for providing digital asset services without the required AML-related registration – a penalty of up to two years imprisonment and/or a fine of up to five million New Taiwan Dollars for natural persons (approximately EUR 135,000) or up to 50 million New Taiwan Dollars for legal persons (approximately EUR 1.35 million).

The institutional system in Taiwan is more complex, but in practice delivers visible results in the digital asset area. The central competent authority for AML registration and AML supervision of VASPs is the Financial Supervisory Commission (FSC), and operational enforcement is carried out by the Securities and Futures Bureau (SFB), a dedicated, independent agency of the FSC.

Suspicious transaction reports (STRs), cash transaction reports, and reporting under the Counter-Terrorism Financing Act (CTFA) within the VASP rules are submitted to the MJIB – Ministry of Justice Investigation Bureau, which in practice functions as the financial intelligence unit (FIU) for these obligations. The MJIB is the key law enforcement and intelligence agency responsible for national

security, the most important criminal investigations, and money laundering prevention (often referred to in literature as Taiwan's FBI; in Montenegrin terms, this institution represents a blend of the competencies of the Special Police Department and the National Security Agency). In Taiwan, the MJIB is the institution that exchanges operational data with the US FBI.

Taiwan has established a two-tier regulatory package for VASPs, implemented through VASP registration regulations and AML/CFT obligations for VASPs[3]. Under the registration regime, a VASP must be registered with the FSC before commencing operations, and foreign VASPs must have a registered company or branch in Taiwan before applying for AML registration.

The registration regulation defines virtual assets and explicitly lists a set of VASP activities aligned with international standards. In addition, through so-called "fit and proper" criteria, certain persons are excluded from positions as responsible officers and beneficial owners if, for example, they have prior convictions for a range of financial and predicate offenses.

Taiwan also introduces structured self-regulation – the registration rules stipulate that a VASP cannot begin operations until it becomes a member of the Virtual Asset Service Provider Association (VASP Association). This is institutionally significant as it provides an additional layer of oversight and alignment with various policies that raise the quality of services and reporting.

AML/CFT rules applicable to VASPs contain clear thresholds and timelines. Customer due diligence measures are mandatory when

---

[3] Regulations Governing Anti-Money Laundering Registration of Enterprises or Persons Providing Virtual Asset Services, 26.11.2024.
https://law.fsc.gov.tw/EngLawContent.aspx?id=2734&lan=E

establishing a business relationship and for occasional transactions of 30,000 New Taiwan Dollars (approximately EUR 800) or more (or multiple related transactions reaching that threshold), and anonymous accounts are prohibited.

The regulations also require sanctions list screening and periodic assessments of money laundering and terrorism financing risk.

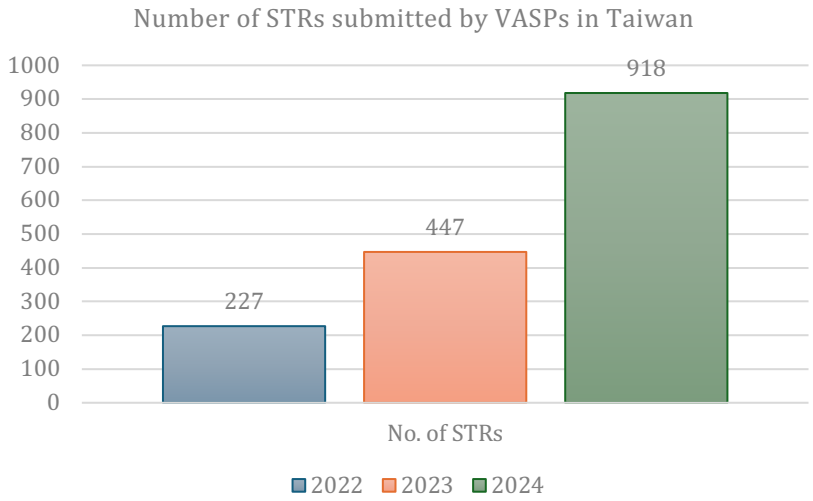
Taiwan's VASP registration rules include mechanisms for safeguarding client funds held in official currencies (e.g., separate deposit accounts, fiduciary arrangements or guarantees of full performance of obligations), as well as broader obligations for information security system management.

Taiwan has also issued an official interpretation prescribing minimum ratios of hardware wallets (cold wallets) to software wallets (hot wallets) for storing client digital assets. At least 70% of assets must be held in hardware devices if service providers have met a high level of information security, or at least 80% if they have not. Accordingly, storage in digital wallets (applications) can account for a maximum of 30% or 20% respectively.

The analysis shows that the level of operational precision in Taiwan is dramatically more detailed than Montenegro's approach based on the Law on Prevention of Money Laundering, which primarily focuses on controls in that area and less on everything else connected with digital assets.

Data from Practice

In 2024, when Taiwan strengthened its money laundering monitoring system with a particular focus on digital assets, the number of suspicious transaction reports (STRs) from virtual asset service providers (VASPs) doubled compared to the previous year, from 447 to 918. However, the total number of reports across all entities decreased slightly, showing that improvements in the digital asset area produced significant results.



Source: 2024 Annual Report on Money Laundering Prevention, Investigation Bureau, Ministry of Justice, Taiwan

Following the tightening of the legal framework, of the 27 registered VASPs in Taiwan, only nine managed to meet the new legal criteria for AML registration and continue providing services, while 18 – two thirds – lost their registration.

Also, according to data obtained during our institutional visits in Taiwan, prosecutors have charged dozens of individuals for criminal

offenses related to unregistered VASP operations worth billions of New Taiwan Dollars. In just one case in April 2024, 32 people were charged with fraudulent, unregistered crypto activities worth nearly 800 million New Taiwan Dollars, or nearly EUR 22 million.

On the other hand, Montenegro's Financial Intelligence Unit (FIU) has received no reports from VASPs in Montenegro, as there are still no such registered entities in the country[4].

However, the FIU reports that during 2024 it handled five crypto asset cases received through suspicious transaction reports from commercial banks. In three cases, individual purchase amounts were below EUR 3,000, and it was concluded that no elements of criminal offense were present. The remaining two cases, reported at the end of 2024, involved amounts of approximately EUR 300,000 and related to transactions connected with online gambling and cryptocurrencies derived from gambling proceeds; these cases are currently under review[5].

Through its own investigations, BIRN Montenegro has identified multiple cases where cryptocurrency exchange services are being provided without any oversight and in large amounts[6].

In just one case identified by a BIRN journalist, a street-level dealer had transacted over USD 17 million through a single digital account over the course of one year, demonstrating that institutional efforts to detect illegal cryptocurrency trading and potential money laundering are out of step with reality.

---

[4] More information at: https://birn.me/vijesti/registar-kripto-usluga-bez-ijedne-prijave/
[5] Report on Work of FIU, Police Directorate, Ministry of Internal Affairs - https://wapi.gov.me/download/75a14a75-1718-4741-876a-fe7dbdea7729?version=1.0
[6] More information at: https://birn.me/istrazivanja/kripto-dileri-i-telegram-mjenjacnice-milionske-transakcije-prolaze-ispod-radara/

Recommendations for Improvement

1. **Montenegro should amend its Criminal Code to introduce the criminal offense of unregistered provision of digital asset services.** According to the data obtained through our comparative analysis, it was precisely a strict sanctions policy that led to the registration of a larger number of service providers in Taiwan.

2. **Montenegro should adopt a Law on Digital Assets, which would link obligations and activities related to digital assets from the Law on Prevention of Money Laundering and the Law on Tax Administration, and would define all aspects of digital assets in line with new European regulations.** This law should provide clear powers and mechanisms to the institutions responsible for detecting and prosecuting unregistered crypto asset service providers (VASPs).

3. **The mechanism for verifying all transactions leading to the conversion of digital assets into movable and immovable property must be fully operationalized,** with a particular focus on purchase contracts where only a declaration of prior payment is submitted, without any proof of the payment itself.

4. **Given that Montenegro until recently had a complete absence of any regulation in the digital asset space, a sectoral risk analysis should be conducted** to identify concrete short-, medium- and long-term priorities in this area that would lead to the detection and better monitoring of all entities providing digital asset-related services in Montenegro who are currently doing so illegally.

5. **Strengthening the capacities of the Financial Intelligence Unit (FIU) of the Police Directorate for monitoring and investigating digital assets, suspicious transactions and related persons in this area.**

6. **Strengthening supervisory capacities for the VASP sector within the Capital Market Commission.** A specialized unit for VASP oversight needs to be established, along with a supervisory strategy, risk assessment model, and annual inspection plan. This is necessary because the law assigns VASP supervision and registry management to this institution, and effective implementation is a key expectation under international standards.

7. **Developing crypto-specific supervisory guidelines and typologies.** Based on cases identified by the FIU (e.g. gambling, conversion to crypto assets, bank STRs linked to crypto assets), guidelines should be published with indicators and red flags for obligated entities and VASPs.

8. **Introducing blockchain analytics and sanctions-screening tools.** The FIU and supervisory bodies should implement blockchain transaction monitoring tools to support suspicious transaction analysis, supervision and detection of evasion of international sanctions.

References

- Zakon o sprječavanju pranja novca i finansiranja terorizma Crne Gore *("Službeni list Crne Gore", br. 110/23 od 12.12.2023, 065/24 od 05.07.2024, 024/25 od 12.03.2025*
- Money Laundering Control Act of Taiwan (Adopted on 23.10.1996 and amended 10 times, last time on 31.07.2024. godine)
- Securities and Futures Bureau - https://www.sfb.gov.tw/en/index.jsp
- Financial Supervisory Commission - https://www.fsc.gov.tw/en/
- Ministry of Justice Investigation Bureau - https://www.mjib.gov.tw/en
- Regulations Governing Anti-Money Laundering Registration of Enterprises or Persons Providing Virtual Asset Services, 26.11.2024. https://law.fsc.gov.tw/EngLawContent.aspx?id=2734&lan=E
- Taiwan Virtual Asset Service Provider Association - https://twvasp.org.tw
- *Godišnji izvještaj o sprječavanju pranja novca za 2024, Istražni biro, Ministarstvo pravde Tajvana - https://www.mjib.gov.tw/userfiles/files/35-洗錢防制處/files/洗錢防制處-EN/2024yearbook.pdf*
- Izvještaj o radu Finansijsko-obavještajne jedinice za 2024. godinu, Uprava policije, Ministarstvo unutrašnjih poslova - https://wapi.gov.me/download/75a14a75-1718-4741-876a-fe7dbdea7729?version=1.0

BIRN Montenegro Articles

- https://birn.me/istrazivanja/kripto-dileri-i-telegram-mjenjacnice-milionske-transakcije-prolaze-ispod-radara/

- https://birn.me/vijesti/registar-kripto-usluga-bez-ijedne-prijave/
- https://birn.me/vijesti/crna-gora-kao-kripto-cvoriste-na-darknetu/
- https://birn.me/analize/kripto-donacije-ostale-van-domasaja-izborne-reforme/
- https://birn.me/istrazivanja/drzava-ne-kontrolise-kupovinu-nekretnina-kriptovalutama/
- https://birn.me/crypto-ai/bez-zakona-raste-opasnost-od-kripto-prevara/
- https://birn.me/vijesti/novac-od-kokaina-pere-se-kroz-nekretnine-i-kriptovalute/
- https://birn.me/vijesti/birn-trazi-bolju-kontrolu-kripto-imovine-funkcionera/