"Fighting Money Laundering and Terrorist Financing

in the Era of Digital and Cryptocurrencies: Reality and Ways of Combating."

The 18th Meeting of the INTOSAI Working Group on Fight Against Corruption and Money Laundering – WGFACML

Warsaw - Poland
1st to 4th of July 2025

CRYPTOCURRENCIES AND FINANCIAL CRIME

INTRODUCTION

- Cryptocurrencies have evolved into a transformative force in modern finance, reshaping how value is transferred and stored.
- Yet, this innovation has introduced major vulnerabilities in the global financial system.
- Regulatory agencies currently face a dual challenge: fostering innovation and reducing misuse.
- The Financial Action Task Force (FATF) has extended its standards to include crypto assets; however, compliance remains limited globally.

The Dual Nature of Cryptocurrencies

OPPORTUNITIES

- Enable financial inclusion for the unbanked individuals.
- Reduce transaction costs and eliminate intermediaries.
- Accelerate cross-border trade and remittances.

RISKS

- Anonymity enables illicit finance.
- Lack of regulation creates safe havens for criminal activities.
- Technological complexity makes detection more difficult.

KEY TYPES OF
CRYPTO-FINANCIAL CRIMES

1. MONEY LAUNDERING

- Converting illegal profits into clean money via crypto platforms.
- Uses pseudonymous wallets and layering methods to obscure sources.

2. TERRORIST FINANCING

- Crypto is used to circumvent sanctions and banking bans.
- Often relies on small, decentralized donations raised through online platforms.

HOW CRYPTO MONEY LAUNDERING HAPPENS?

PHASE 1: PLACEMENT

1

- Conversion of cash to crypto via irregular brokers or trading platforms that are not subject to strict supervision.
- Direct acquisition of crypto through cybercrime such as electronic extortion or exchange hacks.

PHASE 2: LAYERING

2

- Create a huge number of digital wallets for free and anonymously.
- Using mixers: Cryptocurrencies from multiple sources are mixed and then redistributed, making it difficult to link the incoming to the outgoing of each user.
- Privacy coins which are specified designed to hide the transactions details which makes tracking them almost impossible using traditional tools.

PHASE 3: INTEGRATION

3

Returning laundered funds to the formal economy in a usable form without raising suspicions , for example :

- Purchasing assets (real estate, NFTs).
- Using exchanges, gaming platforms, or gift cards.

TOOLS

USED BY CRIMINALS

Mixing Services:

- Obfuscate transaction trails by pooling funds.
- Example: Tornado Cash laundered $7B+ (sanctioned in 2022).

Privacy Coins:

- Cryptocurrencies like Monero and Zcash conceal sender/receiver info.

Darknet and DeFi:

- Peer-to-peer exchanges and decentralized platforms with no oversight.

DIGITAL TRACKING TOOLS

➤ Blockchain Analytics Platforms

- Chainalysis, CipherTrace, Elliptic track suspicious flows.
- Identify links between wallets, exchanges, and real-world actors.

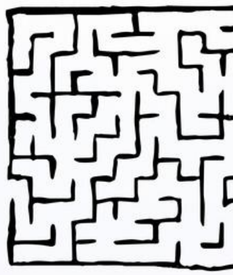
➤ Red Flag Indicators

- Sudden wallet creation + large inflows.
- Repeated micro-transfers.
- Use of high-risk jurisdictions or anonymization tools.

➤ Public-Private Cooperation

- IRS, FBI, and others now partner with forensic firms.
- Example: Silk Road BTC recovery via blockchain trace in 2020.

Challenges in Crypto Oversight



DeFi Protocols

No centralized authority → hard to regulate or subpoena.

Cross-chain Bridges

Facilitate moving assets between blockchains without transparency.

Un hosted Wallets

Not tied to an exchange; ownership difficult to attribute.

KEY OVERSIGHT ENTITIES

Legislators

- Define virtual assets in law.
- Criminalize illicit activities.

Regulators & Central Banks

- Issue licenses.
- Monitor compliance.
- Enforce rules.

KEY OVERSIGHT ENTITIES

Financial Intelligence Units (FIUs)

- Monitoring suspicious transactions.
- Regulation of virtual asset service providers.
- Use advanced analysis tools to analyze digital money sources and assess risks.

Supreme Audit Institutions (SAIs)

- Monitoring the effectiveness of the institutional framework to combat money laundering and terrorist financing.
- Assess the adequacy of national laws and regulations and their ability to fill gaps.

INTERNATIONAL COOPERATION

1- FATF, INTERPOL, Egmont Group support information sharing.

2- Regional frameworks (e.g., EU, Arab League) for joint action.

3- Encourage alignment of national laws to international standards.

SUPREME AUDIT INSTITUTIONS (SAIS)

Institutional Assessment

- SAIs evaluate how well government bodies (e.g., ministries, financial authorities) are prepared to handle crypto-related risks.
- They identify gaps in oversight, resource allocation, and coordination among agencies.

Legal and Regulatory Review

- SAIs examine whether national legislation and regulations effectively address the challenges of digital assets.
- They propose amendments or new laws to close legal loopholes.

Capacity Building and Policy Recommendation

- SAIs recommend training programs for auditors, regulators, and law enforcement in blockchain and digital forensics.
- They advise on investments in tools and infrastructure required for crypto oversight.

EFFECTIVE TOOLS & STRATEGIES

1. Legal Reforms

- Licensing for Virtual Asset Service Providers (VASPs).
- Clear definition of digital assets.

2. Supervision

- KYC (know your customer).
- transaction monitoring.
- inspections.
- Real-time alert systems for suspicious activity.

3. Technical Investment

- AI tools, forensic blockchain labs.
- Training and capacity building.

Recommendations and Moving Forward Ensuring adaptive and dynamic oversight

1- Closing Global Regulatory Gaps

Countries behind on crypto AML implementation must accelerate efforts following FATF's roadmap, sharing best practices and results for mutual progress. Unregulated zones present ongoing risk to all participants.

2-Building Human and Technical Capacity

Governments must allocate sufficient funding for specialist units, analytics tools, and expert training in cyber and blockchain investigations. Personnel shortages remain a bottleneck for enforcement, as exemplified by US IRS cyberunits.

3-Targeting High-Risk Technologies

National strategies should focus specifically on mixers, privacy coins, and unregulated DeFi services, instituting restrictions or enhanced monitoring to counter their disproportionate threat.

4-Proactive and Flexible Regulatory Approaches

Continuous monitoring of new tech trends (e.g., metaverse, Web3), ongoing legislative updates, and research into leveraging blockchain for public asset tracking are needed for sustainable, forward-thinking AML/CTF regimes.

Conclusion:

Balancing innovation and security: The rise of cryptocurrencies has presented enormous opportunities and unprecedented challenges in the fight against financial crime.

Success does not require a blanket ban, but clear and flexible regulation; well-enabled and trained authorities; and strong international cooperation. SAIs play a pivotal role in assessing national AML/CFT frameworks and recommending improvements to them, ensuring that they keep pace with evolving threats.

Ultimately, maintaining the delicate balance between innovation and secure, exploitation-resistant financial systems requires collective vigilance, regular policy updates and mutual knowledge sharing among all stakeholders.

Thank You