GEORGETOWN UNIVERSITY
Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

DECRYPTING CRYPTO: ILLICIT FINANCE

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Kelly Grace Richardson, Research Assistant

KEY INSIGHT

Enforcing AML/CFT regulations in the cryptocurrency industry strengthens financial oversight by requiring KYC procedures, transaction monitoring, and sanctions compliance. However, jurisdictional inconsistencies and evolving tactics by illicit actors present ongoing challenges, requiring continuous adaptation and international collaboration by law enforcement.

SUMMARY

The implementation of **Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)** regulations in the cryptocurrency industry has significantly reduced illicit financial activity by enforcing KYC procedures, transaction monitoring, and sanctions compliance. However, evolving tactics by illicit actors and jurisdictional inconsistencies pose challenges to regulators, requiring constant adaptation and international collaboration. Cryptocurrencies, powered by blockchain technology, allow for decentralized transactions without traditional financial intermediaries. However, their pseudonymous nature has raised concerns regarding illicit financial activities. To combat these risks, regulatory agencies like the **Financial Crimes Enforcement Network (FinCEN)** in the United States have imposed Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) requirements on cryptocurrency businesses, treating centralized exchanges as **money service businesses (MSBs)** subject tofinancial reporting obligations. These regulations require **Know Your Customer (KYC)** procedures, transaction monitoring, and reporting of suspicious activity to detect and prevent financial crimes. However, enforcement remains a complex issue due to the evolving tactics of illicit actors and the global nature of digital assets.

KEY FACTS

Cryptocurrency exchanges operating as money transmitters in the United States are required to implement KYC procedures, collecting personal information such as names, addresses, and government-issued identification to verify customer identities. Exchanges and other **virtual asset service providers (VASPs)** must also file **Suspicious Activity Reports (SARs)** and **Currency Transaction Reports (CTRs)** for transactions exceeding regulatory thresholds. Additionally, the **Office of Foreign Assets Control (OFAC)** enforces compliance with sanctions, requiring crypto exchanges to screen transactions against the **Specially Designated Nationals (SDN) list** to prevent illicit financial flows to sanctioned entities. The transparency of blockchain transactions has enabled the development of analytics tools that assist regulators and law enforcement in

tracking suspicious activity and prosecuting illicit actors. These measures have strengthened financial oversight whilepreserving the benefits of blockchain technology.

Key Institutions

The Financial Crime Enforcement Network (FinCEN), a bureau within the U.S. Treasury Department, enforces AML/CFT regulations, including for the cryptocurrency sector. Blockchain analytics firms like Chainalysis, Elliptic, and TRM Labs have developed tools to trace illicit transactions and support compliance efforts. Other major cryptocurrency exchanges such as Coinbase, Binance, and Kraken have implemented regulatory measures to align with AML/CFT requirements, supporting the interests of both consumers and regulators.

Background

The U.S. has been a pioneer in developing AML/CFT frameworks for the cryptocurrency industry. In 2013, FinCEN released its first guidance clarifying that cryptocurrency exchanges fall under MSB regulations, requiring compliance with financial reporting laws. This early regulatory approach helped shape global AML/CFT policies, influencing the **Financial Action Task Force (FATF)** to establish international standards for virtual asset service providers (VASPs) in 2019. These frameworks have been essential in reducing the percentage of illicit transactions occurring through U.S.-based cryptocurrency platforms compared to global averages.

Policy and Regulation Issues

The primary regulatory challenge in the cryptocurrency space around financial crime is the inconsistency across jurisdictions. Other challenges include the ever-evolving illicit finance methodologies and concerns over balancing financial transparency with user privacy. While the U.S. has led global AML/CFT policy development, regulatory clarity on whether certain digital assets are classified as securities or commodities remains in contention. The industry is also facing the creation of **privacy-preserving technologies** that may complicate enforcement efforts. As regulatory agencies refine their approaches, collaboration between all stakeholders will be essential in mitigating illicit finance risks while supporting the continued growth of the cryptocurrency ecosystem.

Glossary

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT): A set of regulations designed to prevent financial crimes by requiring businesses to implement compliance measures.

Currency Transaction Report (CTR): A mandatory report filed for transactions exceeding a certain threshold.

Financial Action Task Force (FATF): An international organization that sets global AML/CFT standards, including guidance for regulating cryptocurrency businesses and virtual assets.

Financial Crimes Enforcement Network (FinCEN): A bureau of the U.S. Department of the Treasury responsible for enforcing AML/CFT regulations and ensuring financial institutions comply with reporting obligations.

Know Your Customer (KYC): A process that requires companies to verify the identities of their customers by collecting personal information such as names, addresses, and government-issued identification.

Money Service Business (MSB): A category of financial institutions that are required to register with FinCEN and implement AML/CFT compliance programs.

Office of Foreign Assets Control (OFAC): A U.S. Treasury agency that enforces economic and trade sanctions.

Privacy-Preserving Technologies: Cryptographic tools such as privacy coins and decentralized mixing services that enhance user anonymity but may also complicate regulatory enforcement.

Specially Designated Nationals (SDN) List: A list maintained by OFAC identifying individuals and entities subject to economic sanctions due to their involvement in illicit activities or threats to national security.

Suspicious Activity Report (SAR): A report that companies must file with regulators when they detect transactions that may indicate illicit financial activity.

Virtual Asset Service Provider (VASP): A business that facilitates the exchange, issuance, or hold of digital assets.

For more information, please visit our website finpolicy.georgetown.edu or email cfmp@georgetown.edu