Committee: United Nations Economic and Social Council

Issue: Promoting globally legitimate use of cryptocurrencies to combat illicit financial activities

Student Officer: Jiwon Choi

Introduction

The world has been developing at a speed that human society has never observed before. Over the past few decades, electronics and IT devices have been invented, created, and disseminated at a rapid pace. People these days often walk around with their smartphones, listen to music with Bluetooth earbuds, and keep track of their exercise with smartwatches. Not only the lifestyle, but also the economics have also vastly transferred into a new structure. Electronics, IT devices, and semiconductors have emerged as a new mega-industry in terms of trades and productions, and a new form of capital, called 'cryptocurrency' appeared.

Cryptocurrencies (or crypto) are utilized in many fields where physical cash faces its limitations. Physical money possesses issues like security risks, difficulty in tracking transactions, and inconvenience for large payments. Crypto, on the other hand, offers enhanced security through cryptography and its blockchain technology, enabling fast, large, and global transactions without any hindrances and obstacles, such as but not limited to intermediaries like federal, central, and commercial banks. Beyond simple and fast transfers, cryptocurrency offers new possibilities for decentralized applications of money, and this kind of crypto's ability to address physical money's fundamental drawbacks is growing its adoption.

Nevertheless, the anonymous and pseudonymous nature of cryptocurrency, aligning with its unregulated Decentralized Financing (DeFi) platforms, makes these cryptos attractive for money laundering, allowing economic criminals to veil their origin of the funds and to move them globally with speed. Other than laundering, the identity-hiding background allows criminals to exploit those for ransomware payments, sales happening through dark web marketplaces, and even terrorist financing, which poses significant challenges for law enforcement to trace and disrupt these movements.

Thus, the global society is making efforts to hinder the illicit activities regarding the usage of cryptocurrencies. The Financial Action Task Force (FATF) leads the movement by setting up such as but not limited to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) guidelines and publishing "Travel Rule" for Virtual Asset Service Providers (VASPs). INTERPOL also actively works and collaborates with other state and non-state actors to eradicate these movements and

announces red notices to arrest and detain the related personnel. Blockchain-related firms are also developing tools to trace the illicit flow of funds, providing crucial information to worldwide enforcement bodies to tackle the borderless crimes.

Definition of Key Terms

Cryptocurrency

Digital assets exchanged and recorded on public distributed ledgers (known as blockchains) that do not require central intermediaries (e.g., commercial banks, central banks) for clearing and settlement.

Altcoins

Refers to all the other cryptocurrencies other than Bitcoin. Can be created with its specialized purpose, such as but not limited to improved privacy features and transaction speed.

Decentralized Finance (DeFi)

System that utilizes blockchain technology to enable financial transactions without relying on traditional intermediaries like banks or brokerages, aiming to create a more open, transparent and accessible financial ecosystem.

Blockchain

A digital, distributed ledger that securely records transactions across a network of computers, especially those made in a cryptocurrency, is maintained across computers that are linked in a peer-to-peer network and makes it difficult to alter or hack the data.

Money Laundering

The process of illegally concealing the origin of money obtained from illicit activities, such as inter alia terrorism, corruption, economic fraud, and drug trafficking, and converting the funds into a seemingly legitimate source and can be used without detection of the illegal activity that produced them.

Virtual Asset Service Providers (VASPs)

Any business that helps people deal with virtual assets like cryptocurrencies, which includes a wide range of activities include such as but not limited to exchanging virtual assets for regular money, trading virtual assets for other ones, transferring virtual assets, or even holding them securely.

History

Creation of 1st generation cryptocurrency

The first ever cryptocurrency was eCash, developed by the company DigiCash in 1982. The first idea of anonymous electronic money has become a reality. While eCash pioneered the concept of digital anonymity, Bitcoin, the first-ever crypto designed as a decentralized, free-market digital currency, operating on a peer-to-peer network without the need for banks, first emerged in 2009, created by an anonymous identity currently known as Satoshi Nakamoto. Bitcoin experienced a steep success followed by the 2008 global financial crisis, attracting many users and developers through its blockchain technology, which offered enhanced security and speed in transactions.

Rise in supply and demand of cryptocurrency and emergence of its drawbacks

Following Bitcoin's success as one of the early cryptocurrencies, thousands of other cryptocurrencies, often referred to as 'altcoins', have emerged with unique features and usages, leading to the exponential growth of the online-capital market. This has diversified the nature of digital assets beyond a simple concept as online cash, but specialized tokens that can have their own dedicated purpose, each aiming to solve distinct problems. With its rapid growth and powerful anonymity, illicit usages primarily focused on dark web marketplaces have facilitated transactions using Bitcoin and its alternatives.

Among illicit transactions, money laundering, phishing scams regarding crypto assets have significantly increased in recent days. The total volume of illicit cryptocurrency is estimated to have reached $40.9 billion, with some studies suggesting that it could have reached $51 billion. Cybercrimes asking for cryptocurrency have been increasing behind the anonymity of the capital. Terrorist financing has shown as a trend, with groups like ISIS increasingly utilizing digital assets with privacy-focused cryptocurrencies. Reports also indicate that approximately $31.5 billion and $22.2 billion worth of cryptocurrency was sent to services for money laundering each in 2022 and 2023, showing the scale of this new challenge the world is facing.

With constant expansion of the cryptocurrency system, international groups such as but not limited to Financial Action Task Force (FATF), International Monetary Fund (IMF), and International Criminal Police Organization (INTERPOL) continue to detach guidelines for safe and legitimate use of virtual assets. The FATF sets global Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) standards, including the "Travel Rule" for Virtual Asset Service Providers (VASPs), to align crypto transfers with traditional financial regulations. The IMF assesses crypto's impact on financial

stability and promotes adherence to global rules, while INTERPOL combats crypto-related cybercrime through international cooperation and tracing illicit assets.

Key Issues

The exponential growth in the number of altcoins

The growth in the number of altcoins has dramatically reshaped the landscape of digital assets. This mass creation is driven by the eagerness to address the limitations in the earlier cryptocurrencies, such as but not limited to offering specialized functionalities or unique usages, which makes its role go far beyond simple digital cash, as mentioned before. As a result, the market exploded with mass increase of Decentralized Finance (DeFi) currencies, non-fungible tokens (NFTs), and various other blockchain-based applications, continually diversifying and expanding the overall crypto economy. Nonetheless, mass proliferation of altcoins and specialized tokens has created greater complexity in tracing illicit movements of capital, making it more difficult for regulators to monitor and control the activities, creating more opportunities for such, but not limited to, frauds, scams, and market manipulations.

Inconsistency and lack of global regulations

The absence and shortage of consistent and unified global regulations for cryptocurrencies creates a significant vulnerability for illicit financial activities, such as, inter alia, file recovery fees demanded after ransomware attacks and money laundering through the blind spots of laws. This big sinkhole of global rules causes criminals to take action and move their operations to weaker oversight or even with no crypto regulations at all. This makes it significantly difficult for law enforcement bodies and financial intelligence units to effectively track illicit domestic and international flows, as the legal initiatives, frameworks or such are not created and implemented for international cooperation.

Pseudonymous and anonymous nature of cryptocurrency transactions

The challenge current global society is facing regarding cryptocurrency transactions lies in the anonymous nature, where activity is tied to virtual wallet addresses rather than direct identities, making it difficult to link transactions to real-world individuals without further investigation. The genuinely anonymous cryptocurrencies and services deliberately obscure transaction details, creating significant hurdles for law enforcement trying to trace illicit funds and combat financial crimes.

The existence of the dark web and its usage of cryptocurrency

The dark web complicates efforts to legitimize cryptocurrency use. The dark web is the internet websites where its entry is regulated by a heavy security system, making them inaccessible via standard and normal search engines and requiring specific software. This hidden part of the internet hosts marketplaces for illegal goods and services, where cryptocurrencies are the primary form of payment. The dark web's extreme anonymity, combined with crypto's inherent privacy features, creates a formidable barrier, making it extremely difficult for law enforcement to track and investigate the flows of illicit funds and identify criminals.

Major Parties Involved and Their Views

State Actors

United States of America

As a dominant leader in the cryptocurrency industry, the United States of America maintains a dual stance on cryptocurrencies: fostering responsible innovation while also aggressively combating illicit financial activities. While acknowledging the potential of digital assets, the US government, through various agencies like the Treasury, FinCEN, SEC, and CFTC, prioritizes investor protection, market integrity, and national security. The country aims to address regulatory gaps, enhance law enforcement capabilities in trading illicit crypto, and promote global standards, including the FATF's Travel Rule. The role of the United States emphasizes its goal to fill in the big hole of both domestic and international regulations to address the issue.

Swiss Confederation

Switzerland balances banking secrecy and anonymity with combating illicit crypto finance. Known for its confidentiality and the bank keeping the client's identity secret, Swiss law explicitly removes this protection for funds involved in money laundering. More specifically for crypto, FINMA applies Anti-Money Laundering (AML) standards that go beyond international norms. This includes not only full implementation of the FATF's "Travel Rule" for all crypto transfers but also a notable requirement for regulated entities to verify the identity and ownership of self-hosted wallets when transacting with them, thereby significantly reducing opportunities for anonymous illicit flows.

Non-state Actors

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) plays a crucial global role in combating illicit crypto finance. This intergovernmental body sets Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) standards for countries worldwide. A key initiative for crypto is the "Travel Rule" which requires Virtual Asset Service Providers (VASPs) to share transaction information, mirroring rules for traditional wire transfers. FATF also guides countries on identifying risks by providing specific guidelines, licensing VASPs, and reporting suspicious activities, ensuring a unified approach against the misuse of digital assets.

International Criminal Police Organization (INTERPOL)

INTERPOL, as the world's largest international police organization, plays a critical role in combating international cryptocurrency crime through global cooperation. Lacking direct arrest powers, INTERPOL facilitates information sharing among its member countries, issues Red Notices and much more for wanted individuals in crypto-related cases, and provides expertise, guidelines, and analytical tools to national law enforcement. They also coordinate major operations, like "HAECHI", to disrupt cyber financial crime networks that exploit cryptocurrencies for money laundering, scams, and terrorist financing, aiming to enhance cross-border investigations and asset recovery.

International Monetary Fund (IMF)

The International Monetary Fund (IMF) primarily addresses the macroeconomic and financial stability risks of cryptocurrencies. While supporting AML/CFT efforts, the IMF focuses on how widespread crypto adoption could impact national monetary policy, capital flow management, and fiscal stability for member countries. It advocates for comprehensive, consistent, and coordinated global crypto regulation to ensure financial stability and improve data collection, rather than advocating for bans, and is actively involved in integrating crypto into global economic reporting frameworks.

Timeline of Relevant Resolutions, Treaties and Events

Date	Description of event
May 27, 1994	The first electronic payment with eCash has been made.
January 3, 2009	Bitcoin software was made available to the public.
May, 2017	The ransomware 'WannaCry' has infected and spread through numerous devices, which demanded a wire transfer of $300 and $600 worth of Bitcoins to multiple

	anonymous Bitcoin wallets, which are well protected from tracing by investigation bodies.
June, 2019	FATF's update of its guidance on Anti Money Laundering and Counter-Terrorist Financing (AML/CFT) measures to virtual assets (VA) and virtual asset service providers (VASPs) to prevent criminal and terrorist misuse of the sector.
February 23, 2023	IMF Executive Board discussed "Elements of Effective Policies for Crypto Assets", outlining guidance for member nations on managing the macroeconomic and financial stability risks posed by crypto, emphasizing the need for comprehensive regulatory frameworks.
September 7, 2023	The IMF and Financial Stability Board (FSB) released a joint paper and roadmap for global crypto-asset regulation, promoting a coordinated international approach.
November 27, 2024	INTERPOL's operation HAECHI V conducted a major global investigation on cyber-enabled financial frauds, including a significant amount of seizures of virtual assets, demonstrating ongoing, active international law enforcement efforts.
January 10, 2025	First publications of Silver Notice, which targets criminal assets, have been issued by INTERPOL.

Evaluation of Previous Attempts to Resolve the Issue

While the FATF's "Travel Rule" and increased global regulations have helped trace some funds, implementation remains significantly uneven, with the global agreements still only partially compliant as of the current date. This creates regulatory gaps that criminals exploit using privacy coins and cross-chain transfers. Moreover, vulnerabilities in DeFi platforms and the pervasive use of crypto on the dark web mean that illicit financial activities, estimated at over $40 billion in fraud and scams alone in 2024,

continue to pose a growing challenge despite ongoing international efforts, necessitating a more harmonized and active global response.

Some nations have also taken actions to combat the issue. The Republic of Korea has implemented strict real-name verification requirements and mandated information sharing between all exchanges, leading to a decrease in local crypto-related fraud. Similarly, the European Union implemented MiCA (Markets in Crypto-Assets Regulation), which includes AML measures and regulations for crypto firms, and aims to create a region-wide regulatory framework. The United States has collaborated with private firms, such as but not limited to Chainalysis, to recover and freeze funds from ransomware by operations through the FBI (Federal Bureau of Investigation), utilizing blockchain forensics. This partnership well demonstrates the positive utility of public-private collaboration. These actions from the global society highlight the need for coordinated international enforcement and regulatory collaboration, as these actions show the globally uneven adoption of legal enforcement, which leads to the limitation of the overall effectiveness of combating borderless fraud.

Possible Solutions

The complex and borderless background of illicit cryptocurrency activity requires a multifaceted approach to globally promote a secure and legitimate digital asset system. To address the current challenges, potential solutions must prioritize enhanced global cooperation and legal enforcement. This includes urging all enforcement bodies to fully implement and enforce the FATF's AML/CFT standards for Virtual Assets and VASPs, and to work towards consistent interpretation to close existing regulatory blanks.

Beyond the consistent adaptation of FATF standard implementations, further actions have to be taken in order to ensure that the cryptocurrency society to make legitimate moves and transactions. This involves considering strategies for improving information sharing among nations. Such collaboration is crucial given how quickly the illicit crypto funds can cross borders and cover their origin, making it vital for diverse law enforcement and international financial intelligence units to collect data and insights.

Another solution involves the global development and adoption of advanced blockchain analytics tools, supported by public-private partnerships of parties. These tools will help the governments and international parties to track and trace illicit transactions across multiple blockchains, identify suspicious patterns, and indicate bank accounts linked to illicit activities. Governments and global regulatory bodies must collaborate with global blockchain firms to access the data of real-time transactions, which would

significantly enhance the ability to detect and disrupt illicit flows. Encouraging VASPs to take these tools into action in their operations can boost risk management across the digital world.

Furthermore, the debate should also reach out to fulfill the need to adapt legal frameworks to match up with rapidly evolving crypto technologies, including those used in the DeFi system and privacy-enhancing tools. This includes exploring and applying "same activity, same risk, same regulation" principles for crypto transactions and developing specific guidance for privacy coins to prevent their misuse. Discussions on capacity building for law enforcement to back the adaptations of legal initiatives will be vital alongside efforts to increase public awareness about safe crypto usage. The overall direction must focus on creating a globally cooperative regulatory environment that can effectively counter the current illicit finance.

Ultimately, the committee needs to direct its debate towards striking a crucial balance: promoting the legitimate benefits of cryptocurrencies while also combating the misuse of cryptocurrencies for illicit finance, such as darkweb transactions, as mentioned above.

Bibliography

United Nations, Department of Economic and Social Affairs. "Cryptocurrency." *Un.org*, 2018, www.un.org/development/desa/dpad/tag/cryptocurrency/

US Congress. "Introduction to Cryptocurrency." *Congress.gov*, 2025, www.congress.gov/crs-product/IF12405

United Nations Office on Drugs and Crime. "Money Laundering through Cryptocurrencies." *United Nations : UN Toolkit on Synthetic Drugs*, 2023, https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

FATF. "Virtual Asset", www.fatf-gafi.org/en/topics/virtual-assets.html

FATF, "Guidance of Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures", 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf

Conyers. “Virtual Asset Service Providers and the Travel Rule”, 28 Nov. 2024, www.conyers.com/publications/view/virtual-asset-service-providers-and-the-travel-rule/

Cryptopolitan. “$40 Billion in Crypto Received by Illicit Addresses in 2024: Chainalysis.” *Mitrade.com*, Insights, 28 Feb. 2025, www.mitrade.com/insights/news/live-news/article-3-667472-20250228

Aurelien Sage. “Crypto Money Laundering Drops to $22.2B in 2023.” *Bitget*, Bitget Exchange, 20 Mar. 2025, www.bitget.com/news/detail/12560604653665

Tangem. “How Many Cryptocurrencies Are There in March 2025? | Tangem Blog.” tangem.com/en/blog/post/how-many-cryptocurrencies-exist/

IMF. “IMF Executive Board Discusses Elements of Effective Policies for Crypto Assets.” *IMF*, 23 Mar. 2023 www.imf.org/en/News/Articles/2023/02/23/pr2351-imf-executive-board-discusses-elements-of-effective-policies-for-crypto-assets

INTERPOL. “INTERPOL Publishes First Silver Notice Targeting Criminal Assets.” *interpol.int*, 2025, www.interpol.int/en/News-and-Events/News/2025/INTERPOL-publishes-first-Silver-Notice-targeting-criminal-assets

INTERPOL. “INTERPOL Financial Crime Operation Makes Record 5,500 Arrests, Seizures Worth over USD 400 Million.” *interpol.int*, 2022, www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million

FSB. “FSB and IMF Outline Comprehensive Approach to Identify and Respond to Macroeconomic and Financial Stability Risks Associated with Crypto-Assets.” *www.fsb.org*, 7 Sept. 2023, www.fsb.org/2023/09/fsb-and-imf-outline-comprehensive-approach-to-identify-and-respond-to-macroeconomic-and-financial-stability-risks-associated-with-crypto-assets/

FSB. “FSB Global Regulatory Framework for Crypto-Asset Activities.” *www.fsb.org*, 17 July 2023, www.fsb.org/2023/07/fsb-global-regulatory-framework-for-crypto-asset-activities/

FSC. “Press Releases - Financial Services Commission.” *fsc.go.kr*, 2018, www.fsc.go.kr/eng/pr010101/22173

ESMA. “Markets in Crypto-Assets Regulation (MiCA).” *www.esma.europa.eu*, 2023, www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica