COMITTEE: Economic and Financial (EcoFin)

QUESTION: Utilizing emerging technologies to combat money laundering in the age of digital currencies and cryptocurrency-based crime.

STUDENT OFFICERS: Michail Panotopoulos and Sophia Maria Danalis

POSITION: President and Deputy President

Table of contents

Personal Introduction

Dear Delegates,

We, Michail Panotopoulos and Sophia Maria Danalis, are honoured to serve as your President and Vice-President for the upcoming session of LFH MUN 2025. Over the course of these three days, our aim is to guide you in engaging discussions and support you in formulating thoughtful and effective resolutions. We trust that this experience will not only strengthen your diplomatic skills but also deepen your understanding of significant global issues.

This report provides essential information on the topic of utilizing emerging technologies to combat money laundering in the age of digital currencies and cryptocurrency-based crime. It is designed to offer you a solid foundation for your research and to help you better understand the perspective of the country you will represent. We encourage you to make full use of this resource to enhance your preparation and contribute meaningfully to the debate.

We look forward to witnessing your dedication, insight, and hard work throughout this conference. If you have any further questions, please do not hesitate to contact us. We wish you all good luck.

Introduction

Money laundering has long posed a significant threat to global financial stability, facilitating criminal activities such as drug trafficking, terrorism financing, and corruption. The United Nations Office on Drugs and Crime estimates that annually, between 2% and 5% of global GDP—approximately $800 billion to $2 trillion—is laundered worldwide.

The advent of digital currencies and the rapid growth of cryptocurrencies have further complicated this issue. In 2023, losses from cryptocurrency-related frauds and scams rose by 45% compared to 2022, totalling over $5.6 billion, according to the U.S. Federal Bureau of Investigation.

Cryptocurrencies offer users a high degree of anonymity and operate across borders with minimal regulation, making them attractive tools for criminals seeking to conceal illicit funds.

The decentralized nature of blockchain technology, while providing benefits such as transparency and security, also presents challenges for authorities in tracking illegal

transactions. As criminals continue to exploit loopholes in cryptocurrency systems, financial institutions and governments face increasing pressure to adopt emerging technologies—such as artificial intelligence (AI), blockchain analytics, and machine learning—to strengthen anti-money laundering (AML) efforts.

These advanced tools can help detect suspicious activities more rapidly, analyse complex transaction patterns, and identify high-risk accounts. However, the global scale of cryptocurrency use necessitates international cooperation to establish unified regulations and address existing gaps in law enforcement. Without a coordinated effort, criminals will persist in exploiting countries with weaker AML policies.

The United Nations and its member states play a crucial role in fostering this global collaboration, promoting the adoption of innovative solutions, and ensuring financial security in the digital age. By integrating technology with regulation, the international community can work toward preventing financial crimes and safeguarding the integrity of the global economy.

Definition of Key Words

Money laundering: The process of disguising the money earned from illegal activities and making it look like it came from a legitimate source.

Digital currency: A digital currency is a form of money that exists only in electronic form and is stored, transferred, and exchanged through computers or the internet.

Cryptocurrency: A cryptocurrency is a type of digital money that uses cryptography to make transactions secure. It works on decentralized networks like blockchain and is not controlled by governments or banks.

Artificial intelligence: known as AI – is a technology that enables machines and computers to mimic human learning and knowledge

Cryptocurrency-based crime: Illegal activities that use digital currencies such as Bitcoin for the transactions seeing as they are harder to track and known for their anonymity.

Blockchain: form of technology that records all transactions made with digital currencies

Blockchain analysis: analysis used by experts to find unusual or illegal activities via blockchain

Distributed Ledger Technology (DLT): the technology from which blockchains are created. It allows users to see what kind of changes were made and by who, this way the data is more reliable

Anti-money laundering (AML): used universally – it means fighting and preventing money related crimes through the process of regulations, law and policies

Financial crime: refers any kind of crime that involves money. Crimes like these are committed through deception, fraud or unlawful transactions making the people behind them gain financial benefits.

Cybercrime: refers to all criminal activities involving computers, networks, or digital systems. These types of crimes are committed to steal, manipulate, destroy data or even stop something from happening. Cybercrime can target individuals, businesses, and even governments and often uses advanced technology to evade detection.

Dark Web: it is the opposite of the surface web – it is only accessible through specialized tools like Tor Browser. Used mostly by criminals seeing as authorities have a hard time tracking and identifying anyone because of anonymity and the resistance of surveillance in the dark web.

Cross-chain interoperability: refers to the ability of different blockchain networks to communicate, share data, and execute transactions with one another

Stablecoin: A type of cryptocurrency that is tied to a real-world asset (like the U.S. dollar or gold) to keep its value stable.

KYC (Know Your Customer): A rule that requires businesses to check the identity of their customers to prevent fraud or crime.

General overview

There are different ways to scam people using cryptocurrencies. Seeing as it is a hard topic involving advanced technology, newcomers and trusting people are usually more likely to get scammed. And there are countless ways to do so.

- Fraud & Scams

The Ponzi scheme consists of taking investments from people with the promise of making huge profit but instead you use that money to repay debt you have to others, leaving many investors with nothing. The scheme works as long as there are investors

so eventually, the whole thing falls apart. For example, BitConnect (2016-2018) was a fraudulent cryptocurrency platform that promised investors high returns through an "automated trading bot." BitConnect claimed that their mysterious AI trading bot could predict Bitcoin's volatility and generate risk-free profits. Investors earned commissions for recruiting others to BitConnect. In January of 2018, BitConnect shut down and its token dropped by 99% in value leading to investors losing everything overnight. The aftermath consists of investors losing over $2.4 billion in total. BitConnect's promoters, were arrested and in September 2021, U.S. authorities charged Satish Kumbhani, BitConnect's founder, with wire fraud, conspiracy, and money laundering. Another type of fraud is the Fake Initial Coin Offering, projects claim to launch new cryptocurrencies and collect funds from investors, but they never deliver the promised product. For instance, PlexCoin raised over $15 million before being forced to shut down by the SEC. Scammers also uses rewarding systems based on a lie such as sending tokens to wallets, luring users to connect their wallets to malicious sites that drain their funds or promising victims free cryptocurrency if they send a certain amount first.

- Hacks & Cybercrimes

Cryptocurrency attracts hackers and cybercriminals due to its decentralized nature, pseudonymity, and the irreversibility of transactions. These criminals exploit weaknesses in exchanges, wallets, smart contracts, and even users' personal security to steal millions -- sometimes billions -- of dollars. Stolen funds are often laundered through mixing services or moved across multiple blockchains to evade tracking. bad coding or security flaws lead to major hacks; they find bad bags or a flaw in the coding to hack the system and get what they want. For example, the Poly Network, a cross-chain interoperability platform, allowing users to transfer tokens between different blockchains. Seeing as it is a bridge it holds large amounts of assets making it a prime target. A hacker discovered a flaw in the smart contract code which allowed them to authorize transactions without proper approval, replace the contract owner, in other words full control of the funds and the ability to drain Poly Network's reserves resulting to a $611 million theft. Hackers sometimes use ransom meaning, they encrypt a victim's files and demand payment in cryptocurrency to unlock them, if unpaid the files are usually leaked or permanently lost. Moreover, cryptocurrency is often used on the dark web for illegal activities, including money laundering, drug trafficking, and cybercrime services. It's very difficult to track transactions but not impossible so criminals must find ways to make their money look legitimate: mixers (tumblers) break up the crypto into smaller pieces, mix them with others and send them back or swapping money across different blockchains, in doing so, erasing some of the tracking trails, some currencies such as Monero hide all transactional details making it impossible to know anything about the transaction. Some transactions such as P2P (peer-to-peer) trading don't require KYC (Know Your Customer) so it's a "no questions asked" type of transaction,

other times a criminal creates a fake online business and accepts Bitcoin for services that don't exist.

- Identity theft & Impersonating

Phishing attack is a type of identity theft where criminals trick you into giving away personal information by posing as a trusted source or create a fake wallet app, hackers also use information from your social media, for example if you follow a certain team they will pose as that team and ask for information for a giveaway. Scammers also use SIM swapping where they trick your mobile to change SIM cards giving them access to anything associated with the new SIM card or they simply hack your email, reset your cryptocurrency exchange passwords and gain full access to them. Furthermore, impersonation is used in multiple case, scammers pretend to be celebrities, government officials, or exchange representatives to trick users into sending them cryptocurrency, sometimes they build relationships with the victims through dating platforms convincing them to invest in fake crypto schemes often leaving them with nothing.

- Regulatory Violations

Regulatory violations in the cryptocurrency world refer to breaches of national or international financial rules designed to ensure transparency, accountability, and the safety of economic transactions. Because cryptocurrencies are decentralized, fast-moving, and relatively new, many individuals and businesses exploit gaps in existing laws or simply ignore them. This creates a wide range of violations that authorities struggle to detect and punish. Below is a closer look at the main areas where violations occur:

1. Money Laundering Violations

Money laundering is the most pressing regulatory concern in the crypto space. Criminals use digital assets to disguise the illegal origin of funds and reintegrate them into the legitimate economy. Violations in this area include:

- **Failure to report suspicious activities**: In many jurisdictions, businesses, such as crypto exchanges must report suspicious transfers, especially when they involve unusually large amounts or patterns inconsistent with normal financial behaviour. Ignoring or neglecting this duty constitutes a direct violation. For instance, if an exchange fails to flag multiple transfers from wallets previously associated with drug trafficking, it can be held accountable (fines, criminal charges) damaging its reputation.
- **Ignoring Know Your Customer (KYC) requirements**: KYC rules oblige financial institutions and crypto businesses to verify the identity of their clients.

Skipping these checks allows anonymous users to launder funds with ease. This is a frequent violation in small, unlicensed exchanges or peer-to-peer platforms.

- **Use of mixers and privacy coins**: Some individuals deliberately attempt to obscure the origin of illicit funds by using coin mixers, tumblers, or privacy-focused cryptocurrencies like Zcash. In certain jurisdictions, knowingly using or providing these services is classified as a regulatory violation, since they are strongly linked to money laundering schemes.

2. Tax Evasion Violations

Cryptocurrencies generate income, whether through trading, mining, or staking. In most countries, this income is taxable. However, because crypto transactions are hard to trace, many individuals and companies attempt to avoid paying taxes. Violations include:

- **Failure to declare cryptocurrency earnings**: Selling Bitcoin at a profit or earning interest on digital assets should be reported as taxable income. Many users deliberately leave out these declarations, committing tax evasion.
- **Wash trading**: Traders sometimes engage in buying and selling the same asset repeatedly to artificially inflate trading volume or create fake losses for tax benefits. This practice misleads tax authorities and financial regulators, and it is considered a violation in most regulated markets.
- **Cross-border avoidance**: Because crypto can move across countries instantly, some individuals exploit regulatory loopholes by shifting assets to jurisdictions with weaker tax enforcement. This practice, though harder to detect, is increasingly flagged as tax evasion.

3. Consumer Protection Violations

Cryptocurrencies are not only a tool for criminals but also a source of risk for ordinary investors and users. Regulatory violations in this field occur when companies fail to respect the rights and safety of consumers:

- **False or misleading claims**: Crypto businesses often advertise exaggerated or even false promises of profit. For example, platforms claiming “guaranteed returns” or “risk-free investments” mislead users and breach consumer protection laws.
- **Failure to disclose risks**: Legitimate investment products must clearly outline potential risks, including volatility, hacking, and fraud. When crypto companies present only the benefits without the risks, they commit a violation. This was

evident in the collapse of several platforms that misrepresented their financial stability before suddenly shutting down.

- **Negligent security practices**: Some exchanges fail to implement proper cybersecurity standards, leading to hacks and thefts. Regulators increasingly consider the lack of proper safeguards a violation of consumer rights, since users lose their assets due to negligence rather than personal error.

4. International Compliance Violations

Because cryptocurrency transactions cross borders instantly, they often fall under multiple legal frameworks. Many violations occur when individuals or companies ignore international requirements:

- **Operating in banned jurisdictions**: Countries like China have banned crypto trading outright. Businesses that continue to operate in these regions, or target their citizens, are in violation of national bans. Penalties range from fines to imprisonment.
- **Failure to comply with cross-border rules**: When funds move internationally, they must comply with both the sending and receiving countries' AML, KYC, and tax regulations. Violations occur when companies ignore these obligations, creating blind spots for authorities.
- **Unlicensed operations**: In most countries, crypto businesses must register with financial regulators and obtain licenses before offering services. Many companies operate without the required licenses, especially offshore exchanges that serve global clients without authorization. This is considered a serious international compliance violation.

In summary, regulatory violations in the cryptocurrency sector highlight the ongoing struggle between technological innovation and financial governance. While cryptocurrencies offer speed, efficiency, and anonymity, these same features create opportunities for crime and misconduct. Governments, regulators, and international bodies continue to tighten their frameworks, but the pace of innovation often outstrips regulation, leaving gaps that criminals and dishonest actors exploit.

Concerned countries and organizations

UNITED STATES: The U.S. is a global leader when it comes to crypto currency, they have made multiple moves against it passing major laws such as the GENIUS Act (Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025). It is a centre for blockchain innovation but also a target for hidden funds and crimes.

UNITED KINGDOM: The UK is a global financial centre. A home to many crypto startups, fintech companies, and major banks. Furthermore, it's also a target for dirty money, including crypto-based money laundering. The UK is pushing to make the sector safer through strong AML laws and crypto regulations while also using AI financial monitoring to detect things such as suspicious transaction patterns.

FRANCE, GERMANY (EU): The EU is part of the MiCa regulation to control crypto assets France is home to major crypto players and Germany recognizes Bitcoin as legal tender. Both countries support AI-based financial monitoring.

SWITZERLAND: The Swiss government is crypto-friendly with strong financial rules it is, like the U.S, is a target for hidden funds and a centre for blockchain innovation.

JAPAN: One of the first countries to regulate crypto exchanges, the Japanese is known for high tech investment in blockchain security and traceability with strict AML checks.

CHINA: China has banned crypto trading but plays a big role in digital currency development for example the Digital Yuan. The government focuses on state surveillance tech and AI to prevent capital flight and illicit transfers.

RUSSIA: In Russia, Crypto is used for sanctions evasion and illicit transactions. It is under increasing global pressure to track and control crypto usage. Russia doesn't openly share information about how it handles cryptocurrencies or financial crime. Its crypto regulations are unclear, and enforcement is weak. It's hard for other countries to track criminal activity happening inside or through the country. The government has been accused of letting hackers and money launderers use crypto with little punishment.

PHILIPPINES: Central bank supports regulation and tech to detect fraud. The Philippines are important for tracing cross-border crypto payments.

NIGERIA: Africa's biggest crypto market, it faces high levels of crypto fraud and scams. The country introduced the Nigeria a digital currency and needs stronger monitoring tools and fund.

VENEZUELA & ARGENTINA: High inflation drives crypto use for both survival and crime for example tax evasion and scams although they need better tools and regulations to ensure safety and less crimes through digital currencies.

LEBANON: Lebanon faces a severe financial crisis, with its national currency having lost most of its value. Many citizens have turned to cryptocurrencies to protect their savings and bypass strict capital controls. However, the lack of a strong regulatory framework makes the country highly vulnerable to money laundering and fraud. Lebanese authorities have expressed concern about the growing use of crypto for illicit transactions but have limited resources to monitor or regulate the sector effectively.

SYRIA: Syria, being a conflict-affected country, is particularly vulnerable to illicit financial flows through cryptocurrencies. With weak institutions and ongoing instability, crypto is sometimes used to bypass sanctions or finance illegal activities. The lack of a functioning regulatory system means violations go largely unchecked, making Syria a concern for international organizations trying to curb crypto-related crime.

KENYA: Kenya has one of the most active crypto markets in Africa, driven by a tech-savvy population and the popularity of mobile money services like M-Pesa. Cryptocurrencies are increasingly used for cross-border payments and remittances, but weak regulation leaves the market open to scams and fraud. Kenyan authorities have begun drafting laws to regulate the industry, but enforcement capacity remains limited. This makes Kenya both a promising market for crypto innovation and a potential hotspot for regulatory violations.

PAKISTAN: Pakistan has a rapidly growing crypto user base despite legal uncertainty surrounding digital assets. Authorities have warned against unregulated crypto trading, but enforcement has been inconsistent. Crypto is sometimes used for tax evasion and cross-border money laundering, especially due to the country's proximity to regions affected by terrorism financing.

INDIA: India has one of the largest cryptocurrency markets in the world, with millions of users investing in Bitcoin, Ethereum, and other digital assets. However, the government has struggled to establish a clear regulatory framework. While crypto trading is not banned, it is subject to heavy taxation and strict reporting requirements.

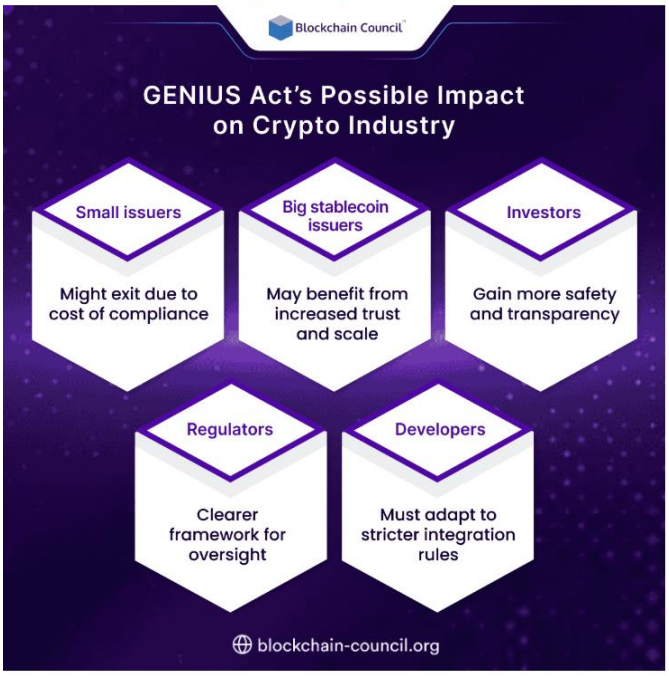
Latest Developments

Case study 1

CASE STUDY 1: THE GENIUS ACT, (UNITED STATES,2025)

The GENIUS Act (Guiding and Establishing National Innovation for U.S. Stablecoins Act), which was officially passed on 17 June 2025, represents an important turning point in the way the United States regulates cryptocurrency. Stablecoins, which are a special kind of digital asset connected to a stable reference such as the U.S. dollar, had for many years been operating in a kind of unclear or grey legal space. Before the GENIUS Act was created and approved, many of the companies that issued stablecoins often said that they held reserves to back up the value of the coins, but they were not actually required by law to prove or clearly show that those reserves really existed. Because there were no strict rules or systems of control, this situation created openings for serious problems such as money laundering, different types of fraud, and even large-scale manipulation of the market. The GENIUS Act therefore stands out as a major step because it directly addresses these long-standing gaps and begins to set clear expectations for how stablecoins should be issued and managed.

GENIUS Act's Possible Impact on Crypto Industry



This could lead to market consolidation, where only the most compliant, well-capitalized players survive.

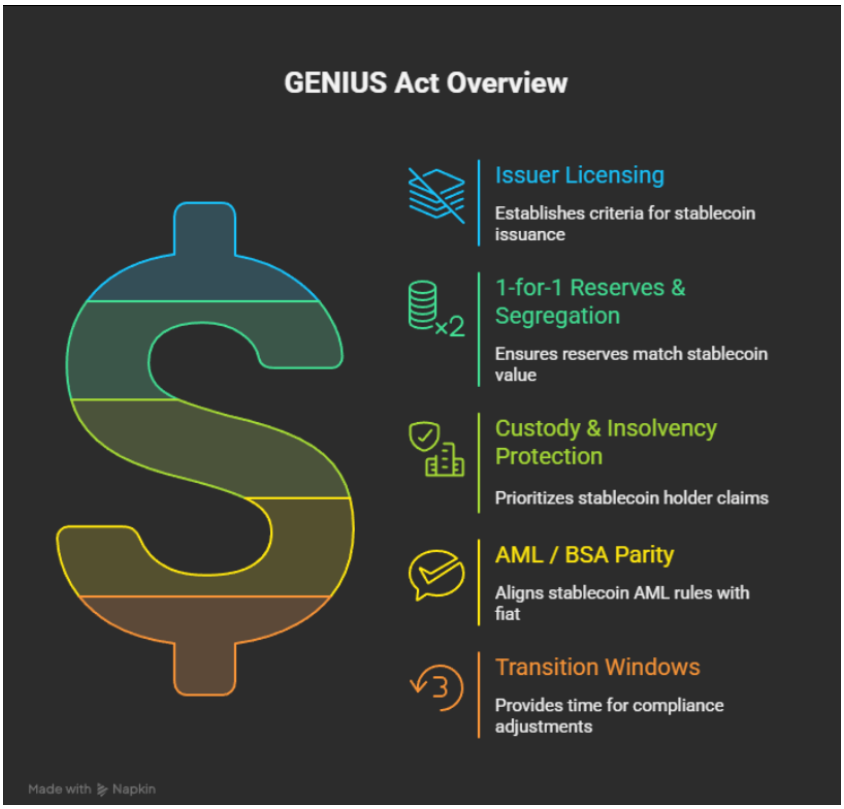
The new law establishes a **federal framework** for stablecoin issuance:

- Only companies approved by U.S. regulators can issue stablecoins.
- Each digital dollar must be backed by one real U.S. dollar in reserve.
- Companies must publish monthly reports on their reserves and undergo annual independent audits.
- Issuers are required to comply with anti-money laundering (AML) and Know Your Customer (KYC) regulations.

This legislation significantly reduces the risk of fraudulent practices in the stablecoin market. By creating transparency and requiring companies to prove their solvency, the GENIUS Act strengthens consumer protection while making it harder for criminals to exploit stablecoins for illicit purposes. It also signals a broader shift: governments worldwide are moving toward stricter rules and oversight in the digital currency space, recognizing the potential risks to financial stability if crypto remains unregulated.

The GENIUS Act has been hailed as a **model for international regulation**, as many other countries are considering adopting similar frameworks for stablecoins. However, critics argue that excessive regulation may drive innovation out of the United States and into jurisdictions with looser rules. This tension between regulation and innovation remains a central issue in the global debate on digital currencies.

Infographic: Key features and implications of the GENIUS Act for stablecoin regulation.



UN involvements / Previous attempts to solve the issue

UN Involvement:

The United Nations (UN) and its affiliated bodies have played a **central role** in addressing money laundering and financial crime in the digital era. As cryptocurrencies grow in importance, the UN has expanded its programs to include crypto-related crime, using training, partnerships, and policy guidance to help member states adapt to this new challenge.

UN Office on Drugs and Crime (UNODC):

The UNODC works closely with governments to fight money laundering linked to organized crime, corruption, and drug trafficking. With the rise of cryptocurrencies, the UNODC has developed specialized programs to trace illicit funds through blockchain technology. It provides:

- **Training for law enforcement officers** on how to track cryptocurrency transactions.
- **Forensic tools and software** to follow the flow of funds on blockchain networks.
- **Workshops on dark web investigations**, where cryptocurrencies are often used to buy and sell illegal goods.

The UNODC emphasizes international cooperation, as money laundering schemes almost always cross borders. By connecting law enforcement agencies from different countries, it helps create a global network capable of responding more effectively to digital crime.

UN Counter-Terrorism Centre (UNCCT):

The UNCCT focuses on preventing the financing of terrorism, which increasingly involves cryptocurrencies. Terrorist groups have experimented with Bitcoin and other digital assets to raise funds anonymously and transfer money across borders without detection. To address this, the UNCCT:

- Works with governments to design monitoring systems that track suspicious crypto transactions.
- Develops AI tools that identify patterns linked to terrorist financing.

- Provides training for financial intelligence units to understand how terrorist groups misuse cryptocurrencies.

By focusing on both prevention and detection, the UNCCT ensures that governments can stop these transactions before they are used to fund attacks.

Global Programme on Cybercrime (UNODC):

Another important initiative is the UNODC's **Global Programme on Cybercrime**, which assists countries in investigating online crimes, including crypto-related fraud and laundering. This program:

- Offers both online and in-person training for police officers.
- Teaches digital forensics, enabling investigators to recover evidence from seized devices.
- Promotes collaboration across borders, since cybercriminals rarely operate within a single jurisdiction.

This program is particularly important for developing countries that lack the resources and expertise to combat advanced cybercrimes on their own.

Other Partnerships:

The UN also collaborates with organizations such as **INTERPOL**, the **International Monetary Fund (IMF)**, and the **World Bank** to strengthen global responses to cryptocurrency crime. These partnerships provide:

- Tools for detecting illicit flows.
- Technical support for creating crypto regulations.
- Capacity-building in poorer countries so they can track crypto activity effectively.

Previous Attempts and Challenges:

Despite these efforts, progress has been uneven. Some countries have adopted strong regulations and technologies, while others lag behind due to lack of resources, political instability, or unwillingness to enforce strict rules. Moreover, criminals continually adapt to new regulations by exploiting loopholes, developing new privacy technologies, or shifting operations to jurisdictions with weaker enforcement.

The UN's challenge remains **coordination**: ensuring that all member states adopt at least a minimum level of regulation and monitoring. Without consistent global standards, criminals will continue to exploit the weakest links in the system.

Possible solutions

- **Fund technology to track cryptocurrency while defunding terrorist groups**
  To stop criminal activity, especially by terrorist groups, it's important to support the development of tools that help track cryptocurrency transactions. By funding this kind of technology, governments and organizations can follow where the money goes and act quickly when something looks suspicious. This makes it harder for terrorists to hide or move money online.

- **Secure the Dark Web, so it is not an easy way to commit crimes**
  The Dark Web is often used for illegal activities because it's harder to trace. Making it more secure and better monitored can limit how easily people can use it to break the law. This doesn't mean removing it completely but rather making it less attractive for criminals by increasing the risks and reducing their chances of staying anonymous.

- **Educate the public on the risks**
  Many people don't realize how new technologies—like cryptocurrency or the Dark Web—can be misused. By informing the public, we can help them avoid falling into risky situations or unknowingly supporting illegal activity. Public education also builds a culture of responsibility and helps everyday people become part of the solution.

- **Use the advantages technology and tools provide**
  We already have powerful technologies—like data analysis, machine learning, and tracking software—that can help fight crime. These tools should be used as much as possible to spot illegal financial activity faster and more accurately. They give authorities a real advantage in staying ahead of those who try to abuse the system.

Bibliography

Lang, H. (2025). US Senate passes stablecoin bill in milestone for crypto industry. *Reuters*. [online] 17 Jun. Available at: https://www.reuters.com/sustainability/boards-policy-regulation/us-senate-passes-stablecoin-bill-milestone-crypto-industry-2025-06-17/.

United Nations (2025). *United Nations*. [online] Un.org. Available at: https://www.un.org/en/.

Chavez-dreyfuss, G. and Price, M. (2021). Explainer: How hackers stole and returned $600 mln in tokens from Poly Network. *Reuters*. [online] 13 Aug. Available at: https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/.

BDO Canada LLP (2022). *Fraud Deconstructed: Cryptocurrency execs charged for $2.4 billion Ponzi scheme*. [online] BDO Canada. Available at: https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme.

Drylewski, A.C., Evangelista, A.D. and Cohen, A.J. (2025). Keeping crypto clean: risk-based controls for stablecoins. *Reuters*. [online] 24 Jun. Available at: https://www.reuters.com/legal/legalindustry/keeping-crypto-clean-risk-based-controls-stablecoins-2025-06-24/.

BlockChain Co :GENIUS Act's Potential Impact on Crypto - Blockchain Council

Loffa Interactive Group: The GENIUS Act: Transforming Stablecoins from Crypto Experiment to Regulated Cash Rail - Loffa Interactive Group