SHIS MUN 2025

UNITED NATIONS OFFICE ON DRUGS AND CRIME

BACKGROUND GUIDE

LETTER FROM THE EXECUTIVE BOARD

Greetings Delegates!

It gives us immense pleasure to welcome you to this simulation of the United Nations Office on Drugs and Crime at SHIS MUN 2025. We look forward to an enriching and rewarding experience.

This study guide is by no means the end of research, we would very much appreciate it if the leaders were able to find new realms in the agenda and bring it forth in the committee. Such research combined with good argumentation and a solid representation of facts is what makes much as possible, as fluency, diction or oratory skills have very little importance as opposed to the content you deliver. So just research and speak and you are bound to make a lot of sense. We are certain that we will be learning from you immensely and we also hope that you all will have an equally enriching experience. In case of any queries feel free to contact us. We will try our best to answer the questions to the best of our abilities.

We look forward to an exciting and interesting committee, which should certainly be helped by the all-pervasive nature of the issue. Hopefully we, as members of the Executive Board, do also have a chance to gain from being a part of this committee. Please do not hesitate to contact us regarding any doubts that you may have.

Regards,

Mr. Bhavya Bhardwaj
(+91 72178 44642)

Beginner’s Guide to Model UN

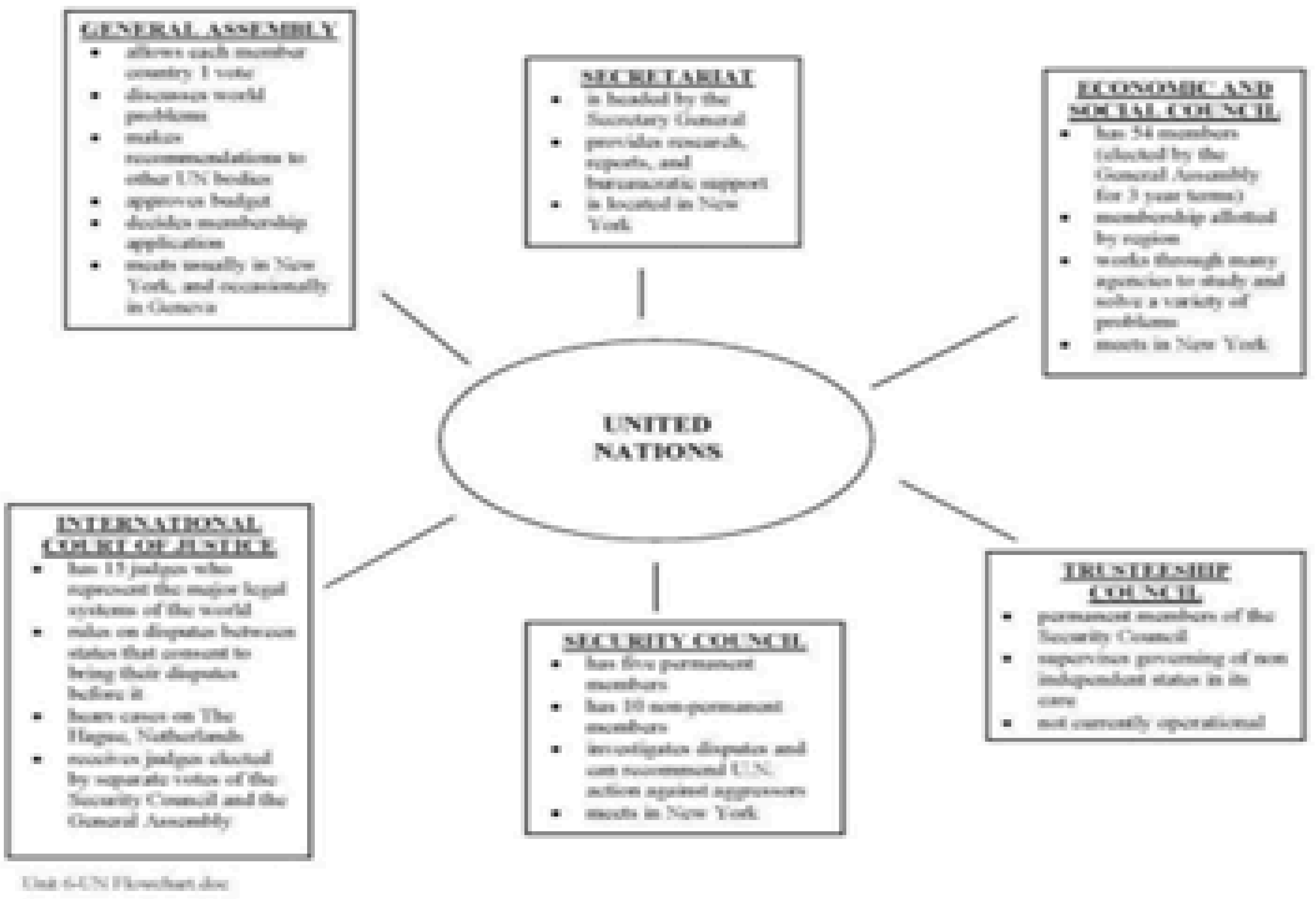
Question 1 What is the United Nations?

The United Nations is an international organization founded in 1945 to maintain international peace and security, developing friendly relations among nations and promoting social progress, better living standards and human rights by 51 countries. The United Nations has 6 principle organs.

<u>The UN has 4 main purposes</u>

- To keep peace throughout the world;
- To develop friendly relations among nations;
- To help nations work together to improve the lives of poor people, to conquer hunger, disease and illiteracy, and to encourage respect for each other’s rights and freedoms;
- To be a centre for harmonizing the actions of nations to achieve these goals

PRINCIPLE ORGANS OF UNITED NATIONS



GENERAL ASSEMBLY
- allows each member country 1 vote
- discusses world problems
- makes recommendations to other UN bodies
- approves budget
- decides membership application
- meets usually in New York, and occasionally in Geneva

SECRETARIAT
- is headed by the Secretary General
- provides research, reports, and bureaucratic support
- is located in New York

ECONOMIC AND SOCIAL COUNCIL
- has 54 members (elected by the General Assembly for 3 year terms)
- membership allotted by region
- works through many agencies to study and solve a variety of problems
- meets in New York

INTERNATIONAL COURT OF JUSTICE
- has 15 judges who represent the major legal systems of the world
- rules on disputes between states that consent to bring their disputes before it
- hears cases on The Hague, Netherlands
- receives judges elected by separate votes of the Security Council and the General Assembly

SECURITY COUNCIL
- has five permanent members
- has 10 non-permanent members
- investigates disputes and can recommend U.N. action against aggressors
- meets in New York

TRUSTEESHIP COUNCIL
- permanent members of the Security Council
- supervises governing of non independent states in its care
- not currently operational

Unit 6-UN Flowchart.doc

Question 2 What is the Model United Nations?

Model United Nations is a simulation of the actual United nation which is done to enhance knowledge about pressing International issues. It is called Model United nation not mock United nation because it does not work as an exact replica of the United Nations, it is just an attempt to understand the working of the United Nations by practicing some of its working mechanisms. Every person who participates is given a country to represent and are called Delegates of their respective committees. There are some rules that we follow in MUNs to facilitate the debate called rules of procedure. The procedure that is closest to what is followed in the actual UN is UN4MUN.

Question 3 What is considered to be valid evidence in the Model United Nations?

Evidence or proof that is acceptable from sources

1. News Sources

a. REUTERS – Any Reuters article which clearly makes mention of the factor is in contradiction of the fact being stated by a delegate in council. http //www.reuters.com/

b. State-operated News Agencies – These reports can be used in the support of or against the State that owns the News Agency. These reports, if credible or substantial enough, can be used in support of or against any Country as such but in that situation, they can be denied by any other country in the council. Some examples are,

i. RIA Novosti (Russia) http //en.rian.ru/

ii. IRNA (Iran) http //www.irna.ir/ENIndex.htm

iii. BBC (United Kingdom) http //www.bbc.co.uk/

iv. Xinhua News Agency and CCTV (P.R. China) http //cctvnews.cntv.cn/

2. Government Reports These reports can be used in a similar way as the State Operated News Agencies reports and can, in all circumstances, be denied by another country.

a. Government Websites like the State Department of the United States of America (http //www.state.gov/index.htm) or the Ministry of Defense of the Russian Federation (http //www.eng.mil.ru/en/index.htm)

b. Ministry of Foreign Affairs of various nations like India (http //www.mea.gov.in/), People's Republic of China (http //www.fmprc.gov.cn/eng/),

France (http //www.diplomatie.gouv.fr/en/), Russian Federation (http //www.mid.ru/brp_4.nsf/main_eng)

c. Permanent Representatives to the United Nations Reports http //www.un.org/en/members/ (Click on any country to get the website of the Office of its Permanent Representative)

d. Multilateral Organizations like the NATO (http //www.nato.int/cps/en/natolive/index.htm), ASEAN (http //www.aseansec.org/), OPEC (http //www.opec.org/opec_web/en/), etc.

3. UN Reports All UN Reports are considered credible information or evidence for the Executive Board of the Security Council.

a. UN Bodies Like the SC (http //www.un.org/Docs/sc/), GA (http //www.un.org/en/ga/), HRC (http //www.ohchr.org/EN/HRBodies/HRC/Pages/HRCIndex.aspx) etc.

b. UN Affiliated bodies like the International Atomic Energy Agency

5 (http //www.iaea.org/), World Bank (http //www.worldbank.org/), International Monetary Fund (http //www.imf.org/external/index.htm , International Committee of the Red Cross (http //www.icrc.org/eng/index.jsp), etc.

c. Treaty Based Bodies like the Antarctic Treaty System (http //www.ats.aq/e/ats.htm), the International Criminal Court

(http //www.icccpi.int/Menus/ICC)

*Some of the links might get replaced so type the keywords for research.

IMPORTANT NOTE THIS BACKGROUND GUIDE ISN'T A VALID SOURCE FOR PROOFS. IT IS JUST FOR REFERENCE, DON'T RESTRICT YOUR RESEARCH TO SAME.

Question 4 How to prepare for the Model United Nations overview?

General Research and Preparation guidelines

There are three consistently significant parts of representative planning. They are useful; meaningful; and positional planning. Practical readiness outfits the representatives with essential apparatuses, including a comprehension of the guidelines important to act in board of trustees. The meaningful component gives preparation of explicit data on the subject regions. At long last, positional planning requires the understudies to embrace viewpoints that are not their own. In light of this, the EB gives three instruments to help you this Guide to Delegate Preparation, Background Guides, and position papers. Together, these will guarantee you will be prepared for the gathering. Past perusing and understanding the material we have given, the more pragmatic experience you can gain through banter, goal composing, making introductions, and so forth, the more ready you will be.

Meaningful Preparation

The Background Guides are a consequence of broad exploration and exertion with respect to the Executive Board and are the establishment of considerable groundwork for every advisory group. We recommend that you read them, talk about them, and read them once more. On the off chance that an agent has not perused and ingested the data in the Background Guide, the person won't contribute adequately to the board. An ambitious beginning on the Background Guides will empower you to completely comprehend the subjects and start to tissue out your own thoughts. Advise yourself that you should go about as policymakers, dissecting and shaping the data you have gotten into arrangements and goals. Conversations with different representatives will likewise assist you with fostering your thoughts. While the Background Guide will give a large portion o omf your meaningful readiness, autonomous exploration is valuable, fulfilling and important for a fruitful gathering.

Positional Preparation

We expect representatives to receive the situation of a particular country all through the UN reproduction. This is a vital component of the "global" experience of a model UN as it powers representatives to analyze the points of view, issues, and arrangements of one more country at an exceptionally major level. It is additionally quite possibly the most troublesome parts of MUN on the grounds that understudies should go up against natural inclinations of their own public viewpoints and authentic data. The position papers are the focal point of positional planning before the meeting. Albeit generally short, we request that you invest energy and exertion on investigating and keeping in touch with them.

Materials arranged by the EB are not intended to fill in for your individual exploration. All things being equal, they ought to give a beginning stage, motivating you to ask yourself inquiries about the current issues. The best-arranged agents are those that accept the gave materials as the start of their exploration and dig further into the theme regions. Past these materials are a large group of data administrations, starting with United Nations sources. UN's assets regularly have ordered measurements, outlines, and charts which you may discover supportive in understanding the issues. Most UN report communities convey records of UN gatherings; maybe the most ideal approach to comprehend your nation's position is to see it iterated by its diplomat.

Explicit assets to research include

•**Yearbook of the United Nations** The Yearbook is a decent beginning stage for your examination. The Yearbook will furnish you with general data on what has been done on your theme during a specific year. It likewise gives exceptionally accommodating references to past articles and goals.

•**United Nations Chronicle** This magazine gives you general data on the procedures of the UN. Watch out for exceptional reports on your theme region, which will advise you about the point and countries' situations on it.

•**UN Document Index** This record for all UN reports comes in three distinct renditions UNDI (1950-1973), UNDEX (1970-1978), and UNODC (1979-present). Contingent upon which of the three you are utilizing, you will track down a subject record, a nation file, and an alphanumeric rundown of all reports distributed (this is helpful in light of the fact that each panel has its own novel alphanumeric prefix and accordingly you can track down every one of the records put out by a board of trustees during a specific year paying little heed to the particular theme.

●**UN Resolutions** This arrangement is both significant and extremely simple to utilize. The record is aggregate from 1946, which implies that you need just check the most current list to track down every one of the goals on your point that the UN has at any point passed.

•**Other UN Sources** Depending on the subject, there may be extra pertinent UN sources. Check for books and exceptional reports put out by the WHO. Past United Nations sources, notwithstanding, are general wellsprings of data. Explore your school and nearby libraries. Look at diaries, periodicals, and papers for more current sources. Remember to ask the curators for help.

•**Books** Up-to-date books are probably going to give you a profundity and exactness that is hopeless from UN sources or periodicals. Try to check library postings for bound materials. Book research, in any case, can take a decent arrangement of time, so use prudence when choosing books.

•**Periodicals** Periodicals are valuable for straightforward, current data on points (the Reader's Guide to Periodical Literature and InfoTrack fill in as a record for these materials). Try not to anticipate that they should supply you with the profundity of data you will require for the Conference.

•**People** A regularly ignored source; individuals can help you extraordinarily in your exploration. A few groups to remember are bookkeepers, individual agents, personnel counselors, and your board of trustees' Director, Moderator, and Assistant Directors. Not exclusively can these individuals help you discover what you are searching for, yet they may likewise suggest new sources that you had not thought of. Try not to spare a moment to call or email your advisory group Director.

•**Embassies and Consular Offices** Contact the government office or consular office of the country that you are addressing. These spots are happy to help you in your exploration via mailing factual information and other unclassified data.

RESEARCH AID

(This is just a suggested pattern, you can research your way, individual differences makes us all special but these suggestions may aid you in understanding where to start)

1. Start from knowing
   a. United Nations
   b. Your committee
   c. Mandate of the committee (functions and power)
   d. Bodies it works with
   e. Final result of your committee
   f. Funding channels

2. Know your Agenda
   a. Historical background
   b. Current trends
   c. Future aims

d. International legal instruments

3. Within the agenda cover the following areas
    a. Political
    b. Economic
    c. Social
    d. Technology and its role
    e. Arms and army strength
    f. Legalities
    g. Impacts and implications of (a-f) on historical background, current trends, future aims and international legal instruments.

Note International legal instruments are applicable on Nations for them to reach individuals they should be incorporated in domestic law as individuals are subjects of it i.e. domestic law is applicable on citizens. So it is crucial to understand the relationship between the two and bridge and the gap for effective implementation.

4. Know your country
    a. Historical background, Current trends, Future aims of the agenda from your country's perspective.
    b. Political, Economic, Social, Technology and its role, Arms and army strength and Legal aspect related situation in your nation. (emphasis on High value resources, crisis, support services, governance, political system and administrative conditions)
    c. Membership and participation in regional organizations
    d. International organizations other than UN
    e. Allies and non allies (friends and enemies) of your nations

NOTE Research alone is not enough, as it would be simply reading out from the internet what is needed is to **"Analyze"** i.e. to present your understanding of the research. For eg you read it on the internet about stress

RESEARCH " Depression is leading cause of disability"

ANALYSIS It can cover why depression is on a hike, mental health status, stigma around it and need for change, merits or demerits.

At sneak peak analysis includes your interpretation and understanding of the agenda.

Introduction

In this committee, we will consider the agenda topic **"Contemplation on the Role of Cryptocurrency in Transnational Organized Crime, with Special Emphasis on Blockchain Transparency Tools for Law Enforcement."** Cryptocurrencies (digital or virtual currencies secured by cryptography) have become an important global phenomenon in the 21st century. Originally conceived as a decentralized digital cash, cryptocurrency now underpins a multi-billion-dollar industry including financial services, technology innovation, and speculation. But it has also attracted the attention of criminals. Transnational organized criminal groups – networks involved in drug trafficking, money laundering, cybercrime, and other illicit activities – have found cryptocurrency appealing for moving money across borders, financing illegal operations, and evading law enforcement. At the same time, cryptocurrency technology (especially the public "blockchain" ledger that records transactions) offers new tools for detecting crime.

The dual nature of cryptocurrency – a source of anonymity for criminals and a source of traceable data for investigators – is at the heart of this debate. Delegates will explore how criminals misuse blockchain and digital currencies, and how law enforcement around the world is using innovative techniques to follow the money. This background guide will walk through the technical foundations of cryptocurrency, survey how it has been exploited in crime, examine real-world case studies of both success and failure in enforcement, outline existing legal frameworks, and highlight international challenges. It will also examine how global stakeholders (from nations to international bodies to private companies) are cooperating or conflicting, consider unresolved legal and ethical dilemmas, and describe UNODC's role in shaping the global response. The guide ends with forward-looking recommendations to consider. The goal is to give delegates the full context needed to engage critically and craft effective solutions. Remember, this guide is a starting point delegates should consult additional sources such as UNODC reports, FATF guidelines on virtual assets, law enforcement press releases, and academic analyses. Use this information to ask incisive questions, challenge assumptions, and debate rigorously.

Origins and Evolution of Cryptocurrency

Cryptocurrency's story begins with a search for a new form of money that could operate without central banks or governments. In October 2008, an individual or group using the pseudonym Satoshi Nakamoto published a paper titled "Bitcoin A Peer-to-Peer Electronic Cash System." This revolutionary document proposed a decentralized digital currency called Bitcoin. Unlike traditional currencies, Bitcoin would use a distributed ledger (the blockchain) maintained by a network of computers around the world. Transactions would be recorded publicly on this blockchain, secured by cryptographic techniques. When Bitcoin launched in early 2009, it was a niche project among cryptography and computing enthusiasts. Its creator(s) aimed to enable online payments that were secure, verifiable, and independent of any single authority.

Bitcoin and other early cryptocurrencies were rooted in ideas from the "cypherpunk" community of the 1990s, which valued privacy, free expression, and technological solutions to reduce government control. Early enthusiasts believed that cryptography could empower individuals, protect privacy, and provide financial freedom. Bitcoin's original design focused on anonymity (pseudonymous transactions with no real-world identity) and on a proof-of-work process where computers competed to validate blocks and earn new coins. Over time, Bitcoin grew beyond its early user base. During the 2010s it experienced speculative booms and busts. Other cryptocurrencies (often called "altcoins") were launched, each experimenting with different features. For example, Litecoin introduced faster transaction confirmations; Ethereum (launched in 2015) added smart contracts and decentralized applications; privacy coins like Monero and Zcash introduced enhanced anonymity techniques; and stablecoins like Tether or USDC aimed to peg digital currency to real-world assets like the US dollar.

The cryptocurrency ecosystem also diversified in use. In some markets it became an investment, with exchanges and trading platforms. In other regions it offered banking services to unbanked populations. It enabled crowdfunding via Initial Coin Offerings (ICOs) and fueled entirely new sectors like decentralized finance (DeFi). While Bitcoin often called itself "digital gold", other tokens became utility tokens or security-like offerings. The technology advanced with developments like blockchain interoperability, non-fungible tokens (NFTs), and decentralized autonomous organizations (DAOs). By 2025, tens of millions of people hold or trade cryptocurrencies, and their total market value fluctuates in the hundreds of billions of dollars.

Key features of cryptocurrency from its origin remain transactions happen peer-to-peer using digital wallets and cryptographic keys (private/public keys). A wallet is like a digital address on the network; a private key is a secret number allowing spending from that wallet, and a public key (or address) is where others can send coins. The blockchain is an append-only ledger, where each block contains recent transactions and a link (hash) to the previous block. The decentralized network verifies and records transactions without any central server. In principle, this means that no single entity can unilaterally control or shut down the network. It also means that, unlike cash or bank transfers, there is a permanent public record of every transaction ever made on that blockchain (though identities behind addresses can be unknown).

For delegates new to cryptocurrency, it helps to imagine it as a software-driven financial system. Users create a wallet (essentially generating a key pair). They buy or earn crypto, then broadcast transactions, which are grouped by miners or validators into blocks, secured by cryptographic proof-of-work or proof-of-stake. Nodes around the world keep copies of the ledger. The system's transparency means anyone can verify transactions, balances, and flows. For example, on the Bitcoin network, you can look up any wallet's history and see its incoming and outgoing payments. This transparency can deter fraud in open markets. Yet it also means that if a user's identity ever becomes linked to a wallet, their entire transaction history is exposed.

Delegates should note that cryptocurrency is still evolving. New innovations continually change how it works. For example, mixers (also called tumblers) emerged as services to blend coins together to reduce traceability. New protocols aim to improve speed and privacy. Meanwhile, governments are exploring Central Bank Digital Currencies (CBDCs) – digital versions of their fiat money – which could be seen as the state's response to crypto's innovation. The cultural perception of crypto also shifted from libertarian experiment, to investment fad, to suspected criminal tool. Understanding this history and these changes will ground any discussion of crime and regulation.

Mechanisms of Criminal Misuse of Blockchain

Cryptocurrency's technical features give criminals both opportunities and obstacles. On one hand, decentralized digital currencies allow quick, cross-border transfers without traditional intermediaries like banks. Criminal networks have exploited this to obscure financial trails. On the other hand, the very transparency of blockchain records can undermine criminals if law enforcement can link transactions to real identities. In practice, criminals have adopted various techniques to misuse blockchain and cryptocurrency. These techniques can be grouped into categories like money laundering, darknet market operations, ransomware, fraud schemes, and more.

One major mechanism is **money laundering**. Organized crime profits from activities such as drug trafficking, arms dealing, human trafficking, and corruption generate large amounts of illicit cash. Criminal organizations must "clean" this money by moving it through various channels so it appears legal. Traditionally they used offshore shell companies or smuggled cash, but cryptocurrency offers a new vehicle. For example, a drug trafficker might exchange cash for Bitcoin (perhaps at a non-compliant exchange or peer-to-peer platform), then send that Bitcoin through a series of transactions or across borders, converting eventually to another cryptocurrency or fiat currency. Each stage of this process – placement (introducing into crypto), layering (moving through chains and services), and integration (bringing back to usable form) – can be conducted digitally and globally.

In these money-laundering schemes, criminals often use specific tools

- **Mixers (Tumblers)** Services like the now-defunct Bitcoin Fog or ChipMixer (recently disrupted by law enforcement) pooled together coins from many users. These services break the link between sender and receiver by shuffling coins and returning equivalent amounts from the pool. By using mixers, criminals attempt to obscure the origin of funds. They deposit Bitcoins into the mixer and later withdraw "clean" Bitcoins. Mixers can be built-in smart contracts or independent websites. However, running such a service carries legal risk operators of mixers may be prosecuted if authorities trace transactions. The recent conviction of the Bitcoin Fog operator, who laundered hundreds of millions of dollars, shows law enforcement can eventually break the anonymity of mixers.
- **Privacy Coins** Some cryptocurrencies, like Monero or Zcash, have privacy features by design. Transactions on Monero use ring signatures, stealth addresses, and RingCT to hide sender, recipient, and amount. If criminals exchange their Bitcoin into Monero, they can take advantage of those anonymity features. This can be part of chain-hopping

(moving value across different blockchains to complicate tracing). Privacy coins make illicit flow harder to detect on public blockchains.

- **Chain Hopping** Even without specialized coins, criminals may convert between multiple cryptocurrencies (Bitcoin to Ether to privacy coin to stablecoin, etc.). This multiplies steps and can use many exchange platforms, hoping to evade simple tracking.
- **Decentralized Exchanges (DEXs)** These are platforms where users trade crypto directly without centralized authorities. Some criminals turn to DEXs to swap coins without identity checks. On a DEX, one cryptocurrency can be directly traded for another via a smart contract on a blockchain. Because there is no company to subpoena for records, tracing funds may be harder, though public ledgers can still show how coins moved through contracts.

Another avenue is **darknet markets**. These are online black markets (often on the Tor network) where illegal goods and services are sold – drugs, weapons, stolen data, even hitman services. Cryptocurrencies became the dominant payment method on these marketplaces. The original Silk Road (launched 2011) famously used Bitcoin to facilitate drug sales. Even though law enforcement shut down Silk Road in 2013, many other dark markets emerged (Silk Road 2.0, AlphaBay, Hydra, etc.). Criminal buyers and sellers trade for Bitcoin or other cryptocurrencies, trusting that online wallets provide some shield of pseudonymity. Payments on a blockchain replace cash drops or bank transfers in the old days. If law enforcement monitors darknet forums, they can discover addresses or patterns, but criminals continually adapt with new addresses and platforms.

Ransomware is another high-profile misuse. In a ransomware attack, criminals hack computers (individuals, hospitals, corporations, governments) and encrypt data, demanding payment for decryption. Cryptocurrencies are the primary ransom payment method because they can move value anonymously and are hard to seize ahead of time. For example, the WannaCry attack (2017) demanded Bitcoin payments. More recently, ransomware strains like Conti or REvil have extorted millions, typically in Bitcoin or Monero. Even governments like the U.S. have faced such attacks (e.g. Colonial Pipeline in 2021). Although private keys can sometimes be discovered (allowing police to recover payments), often victims pay in untraceable crypto. The decentralized nature of crypto means once criminals have the private key, they control the coins and can cash out or further launder them.

Other **fraud and scam schemes** exploit cryptocurrency. "Pig butchering" scams (romance or investment scams) involve fake online relationships or trading apps to trick victims into sending crypto. Initial Coin Offering (ICO) fraud – promising a new cryptocurrency project – was rampant in 2017-2018, defrauding investors. Ponzi schemes (promising high returns on crypto investments) lure people to send coins and use new funds to pay earlier victims. These schemes often collapse, leaving trails of stolen crypto. In one case, an international crypto Ponzi scheme defrauded over 50,000 victims of more than half a billion dollars (as reported by Spanish police in 2025), showing the massive scale of such frauds.

It is often said criminals treat cryptocurrency like cash. They like that it is borderless and does not require traditional banking. But criminals also face **challenges** every transaction on many blockchains is permanently logged, even if names aren't attached. If two addresses are ever linked to the same person (for example, through an exchange that follows Know Your Customer rules), past transactions become evidence. Some criminal groups also exploit the anonymity of cash or barter rather than crypto; thus, crypto is just one tool in a broader illicit ecosystem. Importantly, authorities have repeatedly shown that they can penetrate many of the apparent anonymity features. Tracing tools and international co-operation have identified mixers, seized ransomware funds, and arrested operators of illicit services.

Delegates should consider how these mechanisms work in practice. It is useful to look at the stages of money laundering applied to cryptocurrency placement (buying crypto with dirty cash), layering (using chains of transactions or services to blur origins), and integration (exchanging crypto back to legitimate assets). Each stage has both opportunities and vulnerabilities. For example, if criminals use a regulated exchange to cash out, regulators may alert authorities. Delegates might research real examples of laundering chains to understand both sides. Moreover, consider how innovations like decentralized finance (DeFi) – where loans or investments happen with crypto collateral – open new channels. Criminals have begun using DeFi protocols for laundering, by using theft or fraud proceeds as collateral, though this remains an emerging challenge.

Case Studies

Concrete case studies highlight how these dynamics play out. Some operations demonstrate law enforcement triumphs using blockchain tools; others illustrate criminals exploiting gaps. Delegates should analyze both to understand what works and what remains difficult.

One landmark example is the **Silk Road case**. In 2013, U.S. authorities shut down the Silk Road marketplace and arrested its operator, Ross Ulbricht. Silk Road ran on Tor and exclusively accepted Bitcoin for transactions. Initially, investigators traced Bitcoin payments on the blockchain from Ulbricht's account. In one move, Ulbricht paid a known public key with Bitcoin at a café, which linked his identity. Once law enforcement knew his public key, they could see years of Silk Road transactions on the Bitcoin ledger. This proved two things (1) that the transparent nature of Bitcoin made it possible to connect seemingly anonymous criminals to their funds, and (2) that even seasoned criminals can slip up. Ulbricht's case is a classic success of blockchain tracing.

Another major example is the **Bitfinex hack case**. In 2016, hackers stole about 120,000 Bitcoins (then worth some $70 million) from the Bitfinex exchange. The thieves laundered large amounts of Bitcoin through dozens of transactions and mixed them, trying to cover their tracks. For years, law enforcement struggled to find them. Then in 2022, the U.S. Department of Justice announced the arrest of Ilya Lichtenstein and Heather Morgan for conspiring to launder this stolen cryptocurrency (then valued at around $4.5 billion). The FBI had traced many hops through the blockchain and linked the suspects to certain transactions. Ultimately agents seized over 94,000 Bitcoin by discovering the private keys on cloud storage linked to the suspects. This operation shows that even very large, complicated laundering schemes can be unraveled with persistence. In the Bitfinex case, authorities used blockchain analysis, investigation of online identities, and search warrants to recover funds. The lesson is that while criminals can multiply steps (like chain-hopping or using mixers), law enforcement can follow the digital trail with the right tools and collaboration.

The **Spanish Operation Bonanza** (2025) demonstrates international cooperation and analytics success. Spanish police uncovered a global cryptocurrency Ponzi scheme defrauding 50,000 victims for about $500 million in crypto. By 2023, authorities arrested key suspects, froze bank accounts, and seized luxury assets. With the help of a blockchain analytics firm (Chainalysis), investigators traced transactions and froze around $21 million in cryptocurrency. They worked with other countries (for example, Seychelles, where the fraudulent platform was registered) to seize funds. In this case, detectives started from the fiat money side (bank records) then followed the crypto path, demonstrating how governments can jointly turn blockchain data into evidence and recovered value. The success hinges on public-private partnership and cross-border police work. Delegates might ask how similar frameworks could be extended globally.

Ransomware incidents illustrate mixed results. The 2021 Colonial Pipeline attack saw hackers demand Bitcoin, which the company paid. The FBI was able to track a portion of that Bitcoin. In one publicized move, FBI agents located a wallet holding a large share of the ransom and obtained the private keys, recovering about $2.3 million. However, they acknowledged that much of the ransom had already moved through alternative assets or wallets. Ransomware criminals often switch payments into privacy coins or cash out quickly, so although law enforcement scored a win in Colonial Pipeline, it is not always possible to recover funds. Some strains of ransomware have shifted to payments exclusively in Monero or other privacy tokens, which are much harder to trace.

Darknet market takedowns also provide lessons. In 2021 the U.S. took down Hydra Market (a large dark web marketplace) by seizing its infrastructure. The FBI recovered some cryptocurrency and arrested administrators. This shows again that law enforcement can unmask hidden marketplaces. Yet new markets quickly reappear. When a market is taken down, criminal vendors often migrate to other platforms or set up shop on new technology (for example, some markets now use the Ethereum blockchain to trade certain contraband via smart contracts). Delegates should consider the “whack-a-mole” problem does taking down one marketplace significantly deter crime, or do resilient networks simply switch to the next platform?

There are also failures or ongoing challenges. One cautionary example is the continued operation of **privacy-focused laundering services**. Despite major takedowns like Bitcoin Fog, some mixing services remain active or re-emerge under new names. The ChipMixer case (2023) shows that even after law enforcement seized domain names and arrested an operator, millions of dollars in mixing persisted in other forms. Criminals responded by quickly moving to alternative mixers or decentralized tumblers. The enforcement action set a precedent that mixers face consequences, but it has not eliminated the problem.

Another difficulty is **cross-border legal gaps**. For instance, one country may seize cryptocurrency linked to crime, but if the criminals or assets are in another country with lax law, enforcement stalls. In the Bonanza case, cooperation with Seychelles was crucial because that is where the platform was registered. If Seychelles authorities had refused to cooperate, the funds might have been hidden overseas. Similarly, some countries have little regulatory framework, making them attractive for criminals to park crypto. A delegate should examine how legal differences can undermine global cases.

In contrast, certain crypto-related crimes remain unsolved. For example, several years after massive initial coin offering (ICO) scams (where billions were raised fraudulently), many perpetrators have not been caught. Or consider some cryptocurrency-themed thefts (like the 2021 Poly Network hack, where $600 million in tokens was stolen – ironically the hacker returned most of it, but only after claiming to expose security flaws). Even though blockchain analysis could trace such large transfers, prosecuting the culprit (a self-confessed hacker) proved challenging because it involved multiple jurisdictions and legal questions about finding someone on the internet.

In summary, case studies teach that blockchain transparency is a double-edged sword. It has enabled unprecedented law enforcement successes, but criminals adapt quickly. Delegates should critically assess each example to see patterns. For instance, successes often involve collaboration across agencies (police, prosecutors, regulators, intelligence) and countries; partnerships with technology firms skilled in analytics; legal tools like asset seizure laws or mutual legal assistance; and sometimes a bit of luck (like finding private keys). Failures or challenges often involve anonymity tools (mixers, coins) that still largely mask users; lack of cooperation from jurisdictions; and rapid shifts by criminals to new platforms. Thinking through these real-world stories helps frame the debate do we rely on blockchain's transparency as a policing tool, or try to minimize it to protect privacy? How do we fill the gaps criminals exploit?

Legal and Regulatory Frameworks

Cryptocurrency operates in a complex legal environment with no single global standard. Delegates should survey how international agreements and national laws have evolved to meet cryptocurrency's challenges, and where gaps remain.

At the global level, the **United Nations conventions** on crime and trafficking provide a backdrop. The Palermo Convention (2000) obliges parties to criminalize money laundering and improve international cooperation, but it does not specifically address digital currencies. Similarly, the UN Convention Against Transnational Organized Crime (UNTOC) and related protocols (like the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms) date from before cryptocurrencies, so delegations often interpret their provisions (such as those requiring seizure of "proceeds of crime") as applying to crypto. UNODC's role is to clarify that these treaties cover virtual assets under existing principles of asset forfeiture, mutual legal assistance, and cross-border law enforcement. UNODC also works on new guidance. For instance, it has published tools on cryptocurrency investigations and training manuals for law enforcement. In 2019 the UN General Assembly adopted a resolution on strengthening international cooperation in criminal matters related to cybercrime and terrorism that explicitly mentioned cryptocurrency as an emerging challenge.

The **Financial Action Task Force (FATF)** is a crucial international body setting standards on money laundering and financing of terrorism. Since 2013, FATF has issued guidelines on virtual assets. It defines "virtual assets" broadly to include cryptocurrencies, and "virtual asset service providers" (VASPs) as businesses that exchange or transfer these assets. Under FATF standards (published in 2014 and revised in 2019), countries must regulate VASPs and require them to implement Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) controls, such as customer identity verification (Know Your Customer, KYC) and transaction monitoring. The FATF's "Travel Rule" (2019) requires that when virtual assets are transferred, sending and receiving VASPs must share sender/receiver information, akin to banks. Nations agreeing to FATF rules must adapt their laws accordingly. This has led many countries to license or register cryptocurrency exchanges and enforce KYC.

Regionally, the **European Union** has been proactive. The EU's Fifth Anti-Money Laundering Directive (5AMLD, in effect from 2020) explicitly includes cryptocurrency exchanges and wallet providers under AML rules. The directive also prohibits anonymous crypto transactions above small limits and creates public registries of crypto operators. On top of AML laws, the EU adopted a major framework called **Markets in Crypto-Assets (MiCA)** in 2023. MiCA sets uniform rules for crypto issuers and service providers in the EU. It creates a licensing regime for crypto-asset issuers and exchanges, demands transparency in stablecoins, and aims to protect consumers. For example, MiCA may require reserves for stablecoins and higher capital requirements. It also distinguishes between different crypto-asset categories (utility tokens, asset-referenced tokens, e-money tokens, etc.). MiCA is seen as a model for balancing innovation and investor protection. Delegates should note how EU integration contrasts with the US's patchwork of regulations or China's bans.

In the **United States**, no single federal law on cryptocurrency exists, so multiple agencies share oversight. The Treasury's Financial Crimes Enforcement Network (FinCEN) treats many crypto businesses as "money transmitters," requiring registration and AML programs. The Internal Revenue Service (IRS) classifies crypto as property, meaning capital gains tax applies. The Securities and Exchange Commission (SEC) has acted against certain crypto projects as unregistered securities offerings. In 2021-2023, U.S. Congress debated laws on crypto tax reporting (e.g. a provision in the Infrastructure Investment Act for brokers to report transactions over $10,000, though this was controversial and partly rolled back). There are also new specialized enforcement units – for example, the Department of Justice formed a "National Cryptocurrency Enforcement Team" (NCET) to prosecute crypto-related crimes. Some U.S. states, like New York, created license requirements (the "BitLicense") for crypto businesses. Overall, U.S. regulation is evolving, with tension between wanting to foster the tech sector and cracking down on illicit finance.

Other countries vary widely. **China** has adopted a hardline approach it banned crypto trading and mining domestically, citing financial risks. Chinese authorities also penalize any crypto-related fundraising as illegal. This draconian stance contrasts with countries like **Japan** and **South Korea**, which have established licensing regimes and consumer protections after early scams, allowing regulated exchanges to operate. **India** considered an outright ban on cryptocurrencies, but instead settled on heavy taxes (for example, a 30% tax on crypto gains and 1% tax collected on transactions) to discourage speculation. **African nations** show a mix Nigeria (which has high crypto adoption rates) banned crypto trading on regulated platforms to curb fraud, yet the central bank also piloted a digital naira currency. **El Salvador** famously made

Bitcoin legal tender in 2021, encouraging crypto adoption with legal status, although critics question the use case in everyday transactions. These national approaches affect crime by either restricting or inadvertently pushing illicit activity into less regulated venues. Delegates should compare these models to see what incentives they create for criminals.

Within legal frameworks, several measures are common

- **Asset Forfeiture Laws** Many jurisdictions have updated laws to allow seizing crypto assets. For example, prosecutors may obtain warrants to seize a suspect's cryptocurrency wallet or freeze accounts on exchanges. However, because crypto is digital, authorities also need technical methods (or co-operation from exchanges) to actually take control. Some countries have developed rules on what to do with seized crypto – whether it can be sold or used for public benefit.
- **Regulating Privacy Tools** Laws may target the tools criminals use. For instance, after sanctioning Tornado Cash (an Ethereum mixer) in the U.S. in 2022, authorities treated sending crypto through it as money laundering. Germany explicitly banned privacy coins like Monero for anti-money laundering law in 2021. These legal gaps arise from trying to adapt old laws to new technology.
- **Cybercrime and Fraud Laws** Traditional laws on hacking, fraud, and extortion apply to crypto crimes. Ransomware is charged under extortion statutes; online fraud under cybercrime laws. But prosecutors must build cases with digital evidence from blockchains and computers.
- **International Cooperation Agreements** Legal regimes now emphasize extradition and mutual legal assistance treaties (MLATs) that cover virtual assets. Many nations have negotiated MLATs to obtain data from exchanges or to pursue suspects across borders. Still, not every country easily assists with crypto cases – some may lack laws requiring VASPs to keep records.

Despite these laws, **gaps** remain. For one, not all countries have incorporated FATF standards. A Transnational Organized Crime group might exploit a country with no VASP regulations to launder money through that jurisdiction's platforms. Also, the legal status of crypto itself is unsettled in some places – is it a currency, a commodity, or a security? This affects how it's taxed and policed. For example, if an exchange in one country is unlicensed by its home regulator but operates online globally, should other countries accept service to or from it? Furthermore, new crypto technologies (like decentralized autonomous organizations or non-fungible tokens) don't fit neatly into existing legal categories. Delegates should ask do we need new treaties specifically about virtual assets? Or can we rely on existing ones? How can legal frameworks keep pace without stifling beneficial innovation? It will be important to consider both law enforcement needs and those of legitimate users who value privacy and new financial tools.

Enforcement Challenges and Technologies

On the enforcement side, cryptocurrency brings unique challenges, but also novel solutions. Understanding the technical battlefield is key for delegates what can investigators do today, and what obstacles do they face?

A central challenge is **anonymity and pseudonymity**. Although blockchain transactions are public, the real-world identities behind wallets can be hidden. Users can generate unlimited wallet addresses without revealing personal information. Criminals exploit this by moving small amounts through many addresses (a technique called "peeling chains") or by using chain-hopping through multiple blockchains. While blockchain data is static, linking an address to a person often requires off-chain information (like KYC data from an exchange, or surveillance). Investigators overcome this by targeting the "gatekeepers" – cryptocurrency exchanges, brokers, or money services. For example, when a suspicious wallet sends coins to a regulated exchange, law enforcement can subpoena the exchange for the account's identity. This shows a dichotomy blockchain itself is trustless, but legal compliance relies on institutional players. Delegates should weigh is it possible or desirable to force decentralized services to comply with anti-crime laws? What if criminals never touch regulated channels?

Privacy-enhancing technologies also make tracing harder. Mixers, as noted, combine coins to hide flows. Hashing and cryptography mean investigators often can only guess how coins were shuffled. However, investigators have sophisticated tools. **Blockchain analytics software** like Chainalysis, Elliptic, CipherTrace, and others use algorithms to cluster addresses, identify patterns, and link them to known entities. For example, if multiple addresses send coins to the same exchange within a short time, analytics can suggest they belong to one user. These companies maintain databases of wallet tags from past investigations, KYC leaks, or cryptocurrency patterns. They use graph analysis to detect laundering patterns. Public block explorers allow anyone to track transactions, but commercial tools add layers of intelligence. Several companies and even public agencies have developed proprietary solutions to trace complex flows. Delegates might explore how open-source vs commercial tools are used by law enforcement, and whether public funding for such analysis is needed.

Another technological challenge is **decentralized finance (DeFi)**. DeFi platforms operate on smart contract chains (mostly Ethereum) where users can lend, borrow, and swap without a central authority. Criminals have begun exploiting DeFi for instance, in some money laundering cases, illicit funds are passed through decentralized exchanges (DEXs) or through automated market maker (AMM) pools. Because DEXs don't have a company behind them, there is no one to subpoena for user information. Enforcement relies on blockchain tracing through the contract calls, which is complex but possible with tool upgrades. Also, some DeFi uses cross-chain bridges (to move assets between blockchains), which add another layer of obfuscation. This is a rapidly evolving area. Delegates may want to research how enforcement is responding to decentralized platforms for example, law enforcement has begun obtaining data from known DEX smart contracts or pursuing DEX developers who facilitate theft.

International collaboration and intelligence sharing is itself a kind of technology – a network of law enforcement cooperation. Groups like INTERPOL and Europol have set up cryptocurrency and blockchain working groups. For example, INTERPOL runs a Virtual Assets and Forensics Unit, offering training on blockchain analysis to police worldwide. Europol's European Cybercrime Centre has partnerships with analytics firms to support operations. Countries also share data through agencies like INTERPOL I-24/7 network or via regional task forces. The U.S. maintains an FBI unit and provides outreach to other countries. But this cooperation can be hampered by different legal standards or lack of trust. Diplomacy plays a role in building these networks. Delegates should consider structures like "Operation Sky ECC" or "Operation Dark HunTor" (2021, which targeted a crime messaging network), which were multi-national crackdowns involving crypto tracking.

A critical enforcement process is **asset seizure**. Seizing digital assets can be both easy and hard. Once authorities identify a wallet's private key, they can transfer coins to government wallets. But finding that key is difficult unless it is voluntarily handed over or found in a physical location. For example, the UNODC toolkit advises that searches of suspects' properties often focus on finding written or digital wallet "seed phrases" (a string of words that can recover a wallet). In some operations, police confiscated laptops or phones containing wallet keys. If a suspect is arrested with a hardware wallet (a physical device storing keys), authorities can retrieve funds by accessing it. But if criminals keep keys only in their memory or on hidden devices, funds are inaccessible. Hence, despite knowing where illicit coins are, law enforcement sometimes cannot seize them.

Law enforcement also relies on **traditional investigative methods** adapted to crypto. This includes undercover operations (posing as buyers on dark markets), tracking IP addresses of suspicious activity, and working with tech companies. The FBI's Virtual Asset Unit, for instance, was created to focus on crypto crimes. Special units like "Virtual Currency Task Force" may exist in some agencies. Training is crucial an untrained officer might mistakenly convert crypto evidence or overlook metadata. UNODC and other bodies run training courses (as cited earlier) on techniques like using blockchain explorers, extracting wallet data, and understanding private keys and recovery phrases.

One enforcement challenge is speed. Cryptocurrency transactions are fast, but law enforcement operates slowly with warrants and bureaucracy. If investigators wait too long for a court order, perpetrators may liquidate or move assets to untraceable places. Delegates should discuss whether laws should allow quicker action (e.g. emergency freezes) on digital assets, and what safeguards are needed. Another issue is **jurisdiction** if a crime spans multiple countries, who leads the investigation? UNODC can facilitate dialogues, but ultimately one nation's laws govern arrests. Crypto complicates this by being purely digital. For example, a hacker in Country A could launder stolen crypto through wallets hosted anywhere. Unless Country A's authorities find evidence linking to a person, they cannot arrest. Even with evidence, extradition treaties and politics intervene. This makes global frameworks essential for coordinated actions.

Regarding **technology**, delegates should also note advanced forensic methods. Investigators sometimes use network data (like blockchain network node information) to trace users. Timing analysis (inferring user location from transaction timestamps), or even machine-learning on transaction patterns, can give clues. Some researchers have proposed "steganography detection" (finding hidden messages or instructions in blockchain data). However, criminals counter with encryption, VPNs, and by subdividing transactions to make patterns less clear. The technological arms race is ongoing. It may be useful for delegates to think beyond pure tech encryption is a legitimate privacy tool but can hide criminals; how do we balance tech rights with security needs?

Finally, a point about **data retention and privacy** as investigators gather KYC data from exchanges, or use surveillance to identify wallet owners, they hold sensitive personal information. How that data is managed raises privacy concerns. Some countries have strict data protection rules (e.g., GDPR in Europe) that might complicate sharing of crypto-related personal data. Delegates should consider the legal interplay between privacy rights and crime prevention.

Global Stakeholders and Cooperation

Fighting crypto-related crime is inherently international. Key stakeholders range from nation-states to intergovernmental bodies to private industry. Understanding their roles and interactions is vital.

International Organizations UNODC is central, as this committee simulates. UNODC's Global Programme on Cybercrime or Financial Crime supports capacity building. It often works with UN Office of Counter-Terrorism or UNODC's Corruption and Asset Recovery Unit when crypto touches those issues. Beyond the UN, **Interpol** runs global operations on crypto crime (e.g. "Operation Kobalos" in 2017 tackled dark web child abuse networks and involved crypto tracing). **Europol** has an Innovation Lab for blockchain and has coordinated cross-border investigations like "Operation Tonya" (2017) on darknet forums. Groups like FATF, World Bank, IMF, and the **Financial Stability Board (FSB)** watch crypto's financial risks. Regional bodies (ASEAN, EU, African Union) also form working groups. The **Egmont Group** (an association of Financial Intelligence Units) encourages member nations to exchange information about suspicious crypto transactions.

National Law Enforcement and Regulatory Bodies Each country has its own agencies involved. For example, the U.S. Federal Bureau of Investigation, Homeland Security Investigations, and Drug Enforcement Administration all pursue crypto criminals. The Treasury's FinCEN and IRS get involved via financial monitoring. Other countries have analogous units (e.g., Germany's Bundeskriminalamt, Japan's NPA cybercrime units, India's Cybercrime Cells). Regulators like the U.S. Securities and Exchange Commission or EU's European Banking Authority set rules. Critical are national **Financial Intelligence Units (FIUs)**, which collect reports of suspicious transactions from banks and (increasingly) from crypto platforms. FIUs in one country may share tips with their counterparts about cross-border flows.

Private Sector Cryptocurrency exchanges and wallet services are on the front lines. Companies like Coinbase, Binance, or Kraken (global platforms) must follow laws and often alert police to shady accounts. Some exchanges voluntarily scan transactions for illicit links. Another major private role is blockchain analytics firms (Chainalysis, Elliptic, TRM Labs, etc.) that provide tools to law enforcement. These firms sometimes offer joint training sessions or "Open Source Intelligence" teams for agencies. Private sector also includes crypto payment companies, which might flag large suspicious transfers. On the other hand, some private crypto players lobby against heavy regulation, arguing it could stifle innovation. Delegates should consider how to encourage beneficial partnership while regulating malfeasance.

Civil Society and Academia NGOs and think tanks study crypto crime, offering independent analysis and recommendations. For example, some NGOs advocate for privacy rights of ordinary users, warning against blanket surveillance laws. Others focus on financial crime prevention. Academic researchers (like the author Andy Greenberg or studies by Stanford or Cambridge universities) publish on tracing methods and policy analysis. Delegates should not overlook these voices when considering solutions.

Cooperation Structures Successful crypto enforcement relies on organized cooperation. There are joint working groups like the **Global Cryptocurrency Enforcement and Asset Recovery Team (GCERT)**, involving dozens of countries, which share intelligence. Interpol's ICCC (International Cybercrime Coordination Cell) serves as a 24/7 contact point for urgent crypto-related investigations. The **Financial Action Task Force (FATF)** itself is a platform where member countries agree on standards – not law-making, but guidance with persuasive power. For example, when FATF issues an updated guidance (such as the Travel Rule), most major economies try to comply, creating a pseudo-global standard. The **United Nations General Assembly** has also hosted discussion panels on cryptocurrency and national security. Delegates should explore how binding or influential these bodies are, and how effective they have been at resolving disputes or gaps.

In addition to formal structures, **informal networks** matter. Law enforcement often relies on liaison officers, backchannels, and joint task forces. For instance, after a major crypto bust in Europe, investigators might leak details to counterparts in other nations to coordinate raids within hours. Private-public dialogues also exist. For example, some countries have "Crypto Councils" where the central bank, finance ministry, industry representatives, and law enforcement discuss policy.

However, cooperation is not guaranteed. Some stakeholders may be uncooperative if politics or economics intervene. For example, a country known to host a popular exchange might be reluctant to fully disclose user data if it fears hurting its crypto industry. Or a tech company outside law enforcement might claim that privacy concerns prevent it from handing over data. Disagreements can also arise over how to classify cryptocurrency – is it a security or not? – which affects which agencies have jurisdiction. Delegates should debate how to incentivize cooperation should there be international funding for crypto crime units, or penalties for non-cooperating states? Is it feasible to create a treaty on cryptocurrency investigation cooperation?

Ethical Dilemmas and Unresolved Legal Gaps

Cryptocurrency exists at the intersection of technology, finance, and individual rights. As delegates consider regulation and enforcement, ethical questions and legal gaps inevitably arise.

A primary tension is **privacy vs. surveillance**. Crypto was designed to give users autonomy and pseudonymity. Many law-abiding citizens use cryptocurrency to avoid censorship, bank discrimination, or to hold savings outside unstable local currencies. But these same features appeal to criminals. If governments clamp down too hard – for example, by requiring backdoors in blockchains or banning privacy coins outright – innocent users could lose legitimate privacy. Delegates should consider is it just to punish all users for the actions of a few? Can we differentiate legal privacy (e.g., political dissidents using crypto) from illegal? In discussions of blockchain transparency tools, remember that using these tools sometimes means monitoring many users' transactions.

Civil liberties also come into play. Should law enforcement have the right to freeze someone's cryptocurrency wallet without a warrant if they suspect wrongdoing? Some countries have explored using "sweeps" where crypto windows are required to report suspicious activity akin to cash thresholds. This raises legal due process concerns. Also, the sharing of KYC data across borders could conflict with data protection laws or human rights norms in some jurisdictions. Delegates should explore where to draw lines maybe create clear legal standards requiring judicial oversight for crypto surveillance, similar to wiretapping laws.

Another dilemma is **the line between regulating crime and stifling innovation**. For many entrepreneurs, cryptocurrency and blockchain are legitimate fields promising economic growth. Heavy-handed rules might drive projects offshore or curtail technological development. For example, banning DeFi could hurt financial inclusion efforts. On the flip side, lack of regulation has allowed scams and frauds to proliferate (as in ICOs). How can delegations balance fostering innovation and protecting the public? Should governments, for instance, provide "regulatory sandboxes" for crypto startups, or should they simply ban any suspicious entities?

Trust in institutions is also an issue. Some communities adopt cryptocurrency because they distrust banks or governments (e.g., in countries with high inflation). If international bodies push for strict crypto regulation, will this generate backlash? Could it even inadvertently fuel underground alternatives (like a private, unregulated blockchain created by criminals)? Delegates should not assume that more enforcement always leads to more compliance. They should weigh social and economic contexts.

In terms of legal gaps, delegates must confront that many laws were written before crypto existed. For instance, in some legal systems, no law explicitly makes cryptocurrency theft a crime separate from general theft. If someone hacks a crypto exchange and takes Bitcoin, should the prosecutor use theft laws, fraud laws, or some new statute? Similarly, when exchanging cryptocurrency is done peer-to-peer without a regulated middleman, it can slip through AML regulations. These grey areas give criminals loopholes. For example, consider a person who pays a hacker with Bitcoin what is that transaction legally? In some places, there is no clear answer, complicating prosecution.

Criminals also exploit diplomatic tensions. If law enforcement in Country A wants crypto data from Country B but that nation has poor relations with A, aid may be withheld. This is an unresolved political challenge. On a technical front, quantum computing (still nascent) may one day break current cryptography, which is another future ethical dimension – how to handle a situation where all crypto becomes insecure?

Finally, there are ethical questions about **recovery of stolen cryptocurrency**. When authorities seize coins, should they return them to victims, or hold them for investigations, or use them as bait in other cases? Some jurisdictions allow seizing assets and selling them with proceeds going to law enforcement budgets, which raises questions about incentivizing seizures. Delegates should discuss policies for seized crypto that balance justice for victims and accountability for bad actors.

VIII. Role of UNODC in Shaping Global Policy

The UNODC is uniquely positioned to address cryptocurrency and organized crime on the global stage. Delegates should consider how this body – and the UN system as a whole – can influence norms, policies, and capacity building.

First, UNODC is a knowledge hub. It routinely publishes research on organized crime trends, drug trafficking, and cybercrime. The office's **World Drug Report** sometimes highlights cryptocurrency's role in drug networks (for example, the 2024 report noted the use of crypto to buy illicit substances online). UNODC can use its analytical resources to inform member states about emerging threats. Delegates should be aware of UNODC's analytical work (for instance, its "Global Study on Cybercrime") and consider whether UNODC might create a dedicated task force or panel on cryptocurrency.

Second, UNODC assists in **capacity building**. It offers training modules (like the Synthetic Drugs Crypto Toolkit we referenced) on how to investigate crypto crimes. It organizes workshops and delivers technical assistance in drafting legislation. For example, UNODC's global programs have helped countries develop legal frameworks to freeze cryptocurrency. Delegates might explore how UNODC could expand these efforts, such as by funding joint training exercises for prosecutors and police from multiple countries, or by developing a UNODC-certified cryptocurrency analyst training program.

Third, UNODC plays a policy coordination role. Through the Commission on Crime Prevention and Criminal Justice (CCPCJ) and the Commission on Narcotic Drugs (CND), UNODC helps member states negotiate resolutions. In recent years, the CCPCJ has held sessions on cybercrime, including cryptocurrency. Delegates should track UNODC-led discussions or resolutions for instance, there may be calls for encouraging the sharing of blockchain forensics among countries. UNODC's role could be to draft model laws or template language for countries to adopt.

Fourth, UNODC can foster **international cooperation frameworks**. While FATF sets AML standards, there is no global law enforcement treaty solely for cryptocurrency. UNODC could spearhead the creation of an international convention or a protocol to UNTOC specifically addressing virtual assets, if member states see a need. Even without new treaties, UNODC can convene informal task forces or commissions. For example, it might assemble a "Global Crypto Crimes Task Force" of experts from different regions to propose unified strategies or early warning systems.

Fifth, UNODC can advocate for balanced solutions. It must weigh both crime-fighting and development. For instance, UNODC recognizes that banning cryptocurrency altogether could drive it underground. Instead, it might promote proportionate measures like requiring identification for high-value crypto transactions, or encouraging VASPs to be licensed without shutting down blockchain innovation. Delegates should assess how UNODC's mandate – which includes promoting human rights – informs its stance on crypto. UNODC has also called for safeguarding privacy and preventing the misuse of personal data in anti-crime initiatives.

Finally, as a UN body, UNODC can serve as an honest broker among nations. If certain states are reluctant to share data or harmonize laws, UNODC can use its neutral, multilateral forums to bridge gaps. For example, it can encourage regional solutions (like ASEAN guidelines or EU-style codes of conduct) if global consensus is out of reach. UNODC's existing relationships with bodies like INTERPOL, the World Bank (on anti-corruption) and the IMF (on financial stability) position it to integrate crypto considerations into broader strategies. Delegates should ask how can UNODC leverage these networks? Should UNODC partner with the FATF to jointly issue guidance, or coordinate with the G20's Financial Stability Board when they consider crypto risk? The answers could shape how international policy evolves.

Comparative National Approaches

Countries' policies toward cryptocurrency range from welcoming to hostile, which creates a patchwork landscape affecting crime. Delegates should review examples from different regions to see patterns and implications.

- **China** In 2021, Chinese authorities banned all cryptocurrency mining and trading, aiming to eliminate what it saw as speculative bubbles and financial risk. Domestic crypto businesses were shut, and banks instructed not to process crypto transactions. This comprehensive ban forced Chinese crypto users to offshore platforms. The likely aim was to make money laundering harder domestically, but critics argue it drove crypto activity into underground channels or overseas markets. From an organized crime perspective, Chinese criminal networks may now rely on neighboring jurisdictions or alternative methods (like smuggling hardware wallets) to access crypto. Delegates should debate whether a strict ban approach lowers crime or simply pushes it beyond reach.
- **European Union** Through MiCA and AML directives, the EU opts for regulation over prohibition. Exchanges and crypto service providers in EU countries must register, conduct KYC, and report suspicious transactions. The EU also cooperates via Europol. This approach tries to balance growth of fintech with crime control. However,

enforcement sees gaps not every crypto transaction involves a licensed entity; peer-to-peer trades and foreign unregulated platforms remain. Crime groups may exploit the gray areas by using DEXs or unlicensed overseas exchanges. Still, EU regulators have started fintech-vetting crypto innovators (for example, requiring compliance with AML for DeFi protocols). Delegates should consider whether standardizing across EU is a model for global alignment, or if its complexities slow response.

- **United States** The U.S. approach is mixed. Federal agencies treat crypto with scrutiny, and major exchanges comply with AML. For example, U.S. Treasury has sanctioned cryptocurrency addresses connected to illicit activities (like North Korean cyber thefts). At the same time, U.S. regulators face issues like unclear crypto-company classifications. Different states have different rules (some friendly, some skeptical). This patchwork can be exploited. For instance, criminals may use a foreign crypto exchange blocked from U.S. oversight to launder money, then bring small amounts into U.S. systems. The U.S. also pursues innovative deterrents for example, offering bounties for info on stolen crypto (like the $10 million on North Korean cybercriminals' stolen funds). Delegates might ask if targeted sanctions on crypto addresses (like those done under anti-terrorism laws) are an effective tool, and whether they should be coordinated internationally.
- **Russia** Russia has had an evolving stance. It legalized cryptocurrency as property in 2020, allowing trading, but banned its use for payment by 2021. This means criminals can hold and trade crypto, but cannot legally use it to pay in Russia. Russia has used crypto to circumvent some sanctions, while facing internal crime some Russian criminal groups use crypto to move funds abroad. The government may be ambivalent it could use crypto to move around global systems, but it also worries about unsupervised capital flows. Delegates should note how a country facing sanctions might rely on crypto networks, which complicates international law enforcement.
- **Singapore** An example of proactive regulation. The Monetary Authority of Singapore (MAS) established clear licensing for crypto exchanges (the Payment Services Act) and promotes Singapore as a fintech hub. It also requires strict AML compliance. By having clear rules, Singapore aims to attract legitimate business while deterring criminals. The government even invested in blockchain startups. For crime, Singapore has been relatively successful; police actively trace crypto and have convicted individuals in major money-laundering cases. Delegates could examine Singapore's model clear rules, plus strong enforcement, plus a tech-friendly stance.
- **El Salvador** Unique in making Bitcoin legal tender. The government has built infrastructure (even offering wallets called "Chivo"). The official narrative is that this empowers citizens. But critics point out that crypto volatility risk might hurt ordinary Salvadorans more than it aids them, and questions remain about AML enforcement. Interestingly, some illicit actors began using El Salvador's system; this prompted the government to consider imposing limits or stricter checks on large transfers. Delegates should explore whether such adoption encourages more crypto use by criminals (or just by citizens), and how this might change if most countries still do not treat crypto as currency.
- **Developing Countries** In regions of Africa, Latin America, and parts of Asia, the crypto situation is mixed. Some people in these countries use crypto as a hedge against weak local currencies (e.g., Argentina, Nigeria). Others experience tech-forward adoption (like Kenya's M-Pesa influence). Many African countries have yet to develop comprehensive

policies. This regulatory vacuum can attract criminal exploitation. For example, criminals from Nigeria or South Africa might find it easier to operate local crypto mixers or exchange services without oversight. Delegates should consider how capacity-building (a UNODC role) could help such countries craft effective laws, and how criminal flows might shift from developed to developing nations as crypto crime hotbeds.

Across these examples, a common theme is that **coordination is crucial**. Where one jurisdiction has gaps, criminals will gravitate there. Delegates should debate mechanisms to align national approaches perhaps through international standards (like FATF) or bilateral agreements. They might also consider incentives for instance, richer nations could offer aid or tech transfer to help poorer countries develop crypto surveillance capabilities, thus discouraging the use of their jurisdictions by criminals.

Forward-Looking Recommendations

In preparing for debate, delegates should outline innovative and feasible proposals for addressing the complexities above. These recommendations could be technical, legal, or policy-oriented.

1. **Enhance International Legal Instruments** Consider advocating for a UN-led convention or protocol specifically on virtual assets and cyber-enabled crime. This could clarify definitions (what is cryptocurrency, who is considered a VASP) and oblige cooperation on blockchain evidence sharing. Delegates could propose model clauses for extradition treaties covering crypto crimes or for mutual legal assistance requests specifically mentioning digital assets.
2. **Standardize Global AML/CFT Rules** Expand FATF-style standards. For example, promote universal adoption of the Travel Rule for crypto and a public registry of licensed crypto entities. Encourage countries that have not yet done so to enact AML laws for VASPs. Delegates might suggest an international framework for licensing exchanges, much like Cross-Border Payment Regulations, or propose international sanctions on uncooperative platforms.
3. **Invest in Law Enforcement Technology and Training** Recommend establishing a UNODC crypto-forensics fund or training program. Funding could help police in developing countries purchase blockchain analysis software and train analysts. UNODC could certify instructors or facilitate sharing of open-source tools. Delegates might suggest partnerships between governments and academic research on investigative technology.
4. **Public-Private Partnerships** Encourage formalized cooperation between tech firms and law enforcement. For instance, propose that major blockchain analytics companies share anonymized risk assessments via a secure channel to trusted agencies. Or that social media/communication platforms report networks of crypto fraud. Delegates could also call for joint exercises (like cyber drills) between the crypto industry and police to simulate investigations.
5. **Regulatory Sandboxes and Innovation Zones** Recognize that over-regulation could stifle good uses of blockchain (e.g. for supply chain tracking or identity verification). Recommend that governments create "regulatory sandboxes" allowing crypto projects to

operate under supervision and study their risks. This dual approach ensures crime is addressed without killing beneficial innovation.

6. **Focus on Education and Victim Support** Beyond enforcement, delegates should think of preventing victimization. Propose international campaigns to educate the public about crypto scams and financial literacy. Also suggest ways to help victims recover losses – for instance, by recommending that seized crypto be used to partially compensate victims of fraud under court orders.
7. **Balance Privacy and Investigative Needs** Work toward legal safeguards that allow tracing transactions while protecting legitimate users. For example, implement warrant requirements for data requests, as in traditional banking searches. Or establish an oversight body (like a "Crypto Freedom Ombudsman") that monitors law enforcement crypto investigations for abuse. Delegates should aim for solutions that protect human rights, possibly by setting global norms on data protection in crypto investigations (akin to UN privacy treaties).
8. **Encourage Research on Emerging Crypto Trends** Technology moves faster than policy, so propose funding for ongoing research. This could mean supporting international academic working groups on DeFi crime or sponsoring think tanks to study anonymity tools. Awareness of future tech (e.g., quantum computing) should be part of policy planning.
9. **Leverage UNODC's Leadership** Finally, delegates can recommend that the committee (UNODC) takes a lead by issuing a resolution encouraging member states to integrate cryptocurrency considerations into existing UN crime conventions, or to hold a special forum on virtual assets. UNODC might also coordinate an annual "Global Crypto Crime Conference" to share knowledge.

These recommendations combine technical measures (tracking tools, training) with legal/policy reforms (laws, treaties) and strategic approaches (education, innovation support). Delegates should defend each by weighing benefits and costs. The aim is a well-rounded set of strategies that push global action.

What is Expected of Delegates

As delegates in the UNODC committee, you are expected to engage deeply with this complex, evolving issue. You should

- **Understand Key Concepts** Make sure you grasp the basics of blockchain and cryptocurrency. Know terms like wallet, private key, exchange, mixer, etc. This guide provides a foundation, but you should also look up current definitions, perhaps through UNODC publications or reputable financial sources.
- **Research National Perspectives** Even though country positions are not in this guide, delegates should consider the stance of the country you represent. Is it a cryptocurrency-friendly nation, or does it have strict controls? What is its capacity to enforce crypto laws? This will influence your arguments on regulation vs innovation.
- **Prepare Policy Proposals** Use the analysis in this guide to outline realistic solutions. Think of draft resolution language. For example "Urges member states to incorporate

virtual assets into national anti-money laundering legislation in accordance with FATF recommendations; encourages public-private partnerships for blockchain analytics." Be creative maybe your country proposes hosting an international symposium on crypto or launching a UNODC working group.

- **Think Multilaterally** Remember UNODC's cooperative nature. Propose measures that could gain broad support. Avoid solutions that only protect national interests at the expense of others. For example, suggesting your country build a unilateral blockchain surveillance program is less likely to pass than advocating cross-border data sharing protocols.
- **Balance Perspectives** This agenda has two sides – criminals and law enforcement. You need to advocate for controlling illicit use of crypto, but also consider legitimate uses. For instance, a developing country delegate might stress that crypto allows financial inclusion and suggest targeted regulation rather than outright bans. Another delegate might focus on tech support for investigators. Both views can be part of your country's position.
- **Engage with Others** Listen to fellow delegates' arguments. Some may question privacy issues, or worry about costs of enforcement. Come prepared to counter or compromise. For example, if someone says blockchain tracing is too intrusive, you could propose strict oversight mechanisms. If someone downplays crypto crime, cite real data (like seizure amounts or increasing trends from 2016 to 2025) to demonstrate the problem's scale.
- **Negotiate Constructively** Like any MUN, this committee seeks consensus on recommendations. You will work to draft clauses that multiple countries can accept. Use the facts and ideas from this guide to back up your positions but be ready to adjust based on others' input. In debate, clearly state your country's stance and reason for any demands or support.
- **Stay Updated** Cryptocurrency evolves rapidly. New events may have occurred even since this guide was written. Keep an eye on recent news (for example, any new crypto laws passed in 2025 or new hacking incidents). This will give you an edge in informed discussion.