

# CRIMINAL LAW & YOU

**DAILY LIFE CRIMINAL LAW  
EXPLAINED**

**JULY 2025**

HEARD OF BITCOIN?  
KNOW WHAT THE LAW  
SAYS ABOUT IT? YOU  
WILL IN UNDER 5  
MINUTES

READ  
BEFORE YOU  
INVEST,  
ARGUE, OR  
EXPLAIN.

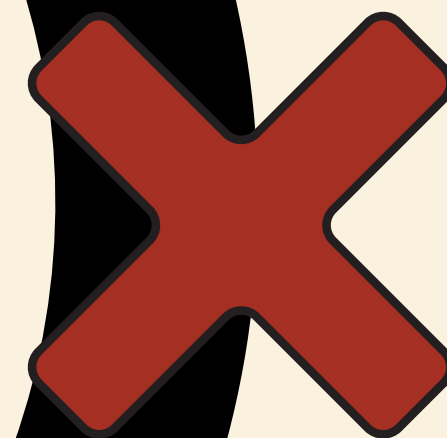
Faculty in charge -  
Dr. Geeta Kubsad  
Mentored by-  
Suha Shaikh

Content and Editing by -  
Arin Indurkhya - 3<sup>rd</sup> Year  
Divya Ichhaporia - 3<sup>rd</sup> Year





# TOPIC 3: cryptocurrency and Money laundering





# why this handbook? whom will it help?

Cryptocurrency was originally created to allow people to make secure, direct transactions without needing banks or middlemen. But over time, its value began to grow fast.

By 2011, new cryptocurrencies started popping up, and people began to see them not just as digital money, but also as investment opportunities. Many software developers launched their own versions, hoping to create the next big thing like Bitcoin.

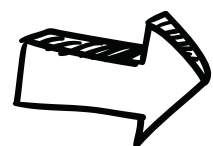
Bitcoin's success was massive. In 2017, it had a market value of around \$535 billion. By 2024, the price of a single Bitcoin had skyrocketed to \$100,000. A huge leap from where it began.

This handbook is designed for students, law enthusiasts and anyone who is inquisitive about cryptocurrency, helping one understand how money laundering occurs through cryptocurrency, and keeping one updated and informed about legal, technical and practical aspects in an easy-to-understand way.



# Bitcoin & the birth of crypto

Who is Satoshi Nakamoto?



Click to reveal theories

In 2009, the world saw the launch of the first cryptocurrency, Bitcoin, created by someone using the name Satoshi Nakamoto. To this day, no one knows who they really are.

Cryptocurrency is a type of digital money. What makes it special is that it's protected by a technology called cryptography, which keeps it secure and nearly impossible to copy or fake.

Cryptography is a way of hiding information so that only the right people can read it. It turns messages into secret codes, and only someone with the key can unlock and understand them. Think of it like a secret language that protects your data that is used in things like online banking, passwords, and cryptocurrencies.

Cryptocurrency in WhatsApp too?  
WhatsApp doesn't support cryptocurrency because of Regulatory challenges that lead to halting of efforts of integrating blockchain technology for payment.

Cryptocurrency allows users to share digital money through secure codes without a bank as a middleman. It uses a process called Blockchain wherein the transactions are transparent and secure. It is a quick and more direct process.



# The Dark Side of cryptocurrency:

As cryptocurrency grew, so did its misuse. Crimes like money laundering, fraud, scams, and other financial tricks have become more common. Why? Because many criminals are simply looking for ways to make illegal money look clean, and crypto is being used to facilitate it.



## How is crypto misused?

Tax evaders use crypto to hide income and assets, bypassing conventional banking systems and avoiding reporting requirements imposed by tax authorities.

Criminals use cryptocurrency to launder money by hiding the source of illegal funds through anonymous wallets and complex blockchain transactions.

Terrorist organizations use crypto to receive international donations anonymously, avoiding detection by governments and financial monitoring agencies.



# What is money laundering?

Money laundering is the process of hiding money that was earned through illegal activities, so it looks like it came from a legal source. Once the money is "clean," it can be used in the real economy for investing in businesses or even donating to charities.

This process happens in **three main steps**:

1. Placement – The illegal money is put into the system, often by converting it into assets or depositing it into bank accounts through shell companies or middlemen.
2. Layering – The money is moved through many accounts or used to buy things like real estate, art, or other valuable items. This step is meant to hide where the money really came from.
3. Integration – Finally, the money reenters the legal economy and reaches the criminal again, now looking like clean, legitimate income.

This cycle often involves not just criminals, but sometimes wealthy business people or corrupt officials, making it very hard to track how much money is actually being laundered.





## Case study: The 2016 Bitfinex Hack- Crypto Heist

In 2016, Lichtenstein hacked into Bitfinex's system and stole around 120,000 Bitcoins worth billions of dollars today. He used advanced hacking tools and approved over 2,000 automated transactions, which moved about 119,754 Bitcoins into his own multiple crypto wallets with fake identities. He practiced chain hopping- converting Bitcoin into other cryptocurrencies to avoid being caught and even converted some funds into gold coins. He later deleted network access credentials and removed the digital log files that could link him to the theft, to cover his tracks. At last, using blockchain analysis, the law enforcement through financial investigation tools identified the movement of the stolen crypto and the criminals were arrested.







# How crypto is used to Launder Money:

## Why crypto appeals to criminals?

The three steps of money laundering makes the whole process even easier for some people. It allows people to move large amounts of money quickly and across borders, and it can be difficult to trace the person behind the transaction. In 2024 alone, over \$40.9 billion in cryptocurrency was linked to money laundering.

That said, the way money is laundered using crypto is a bit different from traditional methods.

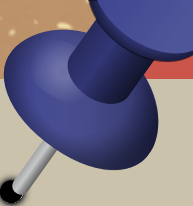
## Blockchain vs Traditional Tracing

Even though crypto is often linked to secrecy, it's actually easier to trace than traditional ("fiat") money. This is because every crypto transaction is recorded on something called the blockchain, a public digital record that cannot be changed or erased.

A blockchain is a shared online ledger that records every crypto transaction. It's open for anyone to see and keeps a permanent history of all activity. People can use it to track the movement of money or other assets across a network. Money generated through real world crimes such as extortion, drug trade, weapon trade or trafficking is fiat money and criminals convert these into cryptos with the intent of laundering them







# How criminals try to clean dirty money:



## 1. Acquiring Digital Tokens

Criminals buy digital tokens during ICO- Initial coin offering sales held by crypto companies to raise funds which they later using the coin mixing method combine legal and illegal cryptocurrencies from different users to hide the origin of the coins. Later using peel chain method they shuffle crypto coins into mini wallets to convert a part of the coins into dollars.



## 2. NFTs

Non Fungible Tokens are digital assets like art, music, or video clips that are recorded on blockchain. Criminals create fake non fungible tokens, use multiple wallets and get people to buy them at higher prices, and then resell them to convert them into clean money.



## 3. Metaverse


Metaverse, a 3D virtual world has virtual land, clothes or art that can be bought using cryptocurrencies. Criminals create fake avatars, trade digital within themselves to make their money clean. Since the nature of metaverse is anonymous and global, it is hard to track ownership, making it easier for criminals to hide in plain sight.





# Legal and Regulatory Frameworks:

## Global Legal Response:



But is this actually  
minimizing money  
laundering?

The Financial Action Task Force (FATF) is the global watchdog that sets rules to fight money laundering and terrorist financing. It was created in 1989, with its headquarters in Paris, to tackle financial crime in banks and other financial systems.

FATF has introduced 40 recommendations to help countries fight money laundering.

As crypto became more common, FATF issued its first crypto guidelines in 2019, and finalised them in 2021.

One major rule is the Travel Rule (Recommendation 16): Crypto companies and platforms must collect and share information including wallet addresses, account numbers, names, national ID details, and more about both the sender and receiver of crypto when the amount sent is \$1,000 or more.

However, despite the FATFs efforts, the implementation of the recommendations remains ineffective due to inconsistency across jurisdictions. This regulatory gap is often exploited by criminals who make transactions with weaker enforcement mechanisms.



# Indian Legal Framework:



## Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 is the legislation that deals with money laundering in India. It has a total of 75 sections within it, that manage the offence of money laundering, its penalties, and create a defined framework to control and further prevent these activities.

This act was introduced to help abide by India's global undertakings, that were set by the Financial Action Task Force (FATF), the global authority for fighting money laundering. PMLA has also been amended multiple times to broaden the spectrum of the possible offences and to reinforce the implementation systems with a stronger legal framework, displaying India's growth against monetary offences.

## Anti Money Laundering

In India, Anti-Money Laundering (AML) laws are governed by the Prevention of Money Laundering Act (PMLA). This law requires banks, financial institutions, and even crypto businesses to take steps to identify, control, and prevent money laundering.

To meet these goals, several tools and systems are used to detect suspicious activity and reduce financial crimes.







### Key AML tools in Crypto Monitoring:

- 1.KYC-Strengthen the Know Your Customer system to confirm user's identity, prevent fake accounts and track illegal activity
- 2.Screening and Monitoring-Observing crypto transactions to spot suspicious behaviour like large transactions, unusual frequency of transactions and activity from high risk countries.
- 3.Risk Based Approach-Focusing more on high risk customers, risky locations and large/complex transactions to reduce missing illegal activities.



### Key AML Enforcement Agencies

- 1.Enforcement Directorate (ED)- It enforces the PMLA by investigating financial crimes, foreign exchange violations and money laundering.
- 2.Financial Intelligence Unit-India(FIU-IND)-It monitors and analyses suspicious financial transactions, collaborates with national and international agencies and overall plays a huge a major role in building strong strategies to detect and prevent money laundering



### Key AML Regulators in India

- 1.Securities and Exchange Board of India (SEBI)- Regulates India's securities market, ensures KYC compliance for investors and maintains safe & transparent financial transactions
- 2.Reserve Bank of India-Formulates AML rules for banks and financial institutions, monitors transactions and issues guidelines to maintain integrity in the banking sector
- 3.Insurance Regulatory and Development Authority of India(IRDAI)- It regulates the insurance sector, decides specific AML rules for insurance companies and aims to prevent financial fraud and prevent trust in the insurance market



## Case Study- The E-Nugget App Scam

A mobile gaming app called E-Nugget lured users by offering games with money wagering and the promise of high returns on investment. Once people invested their money, the app stopped all withdrawals, deleted user data and vanished, leaving users with no way to recover their funds. The Enforcement Directorate (ED) began investigating based on an FIR filed at the Park Street Police Station in Kolkata.

## Legal Action:

The scam involved-

- 90 crores worth of crypto assets across 70 accounts on platforms like Binance, ZebPay and WazirX
- 2500 fake bank accounts used to launder money
- Additional 19 crores in cash and accounts seized during the investigation

The case was handled under various sections of the Prevention of Money Laundering Act (PMLA):

- Section 3 – Defines the offence of money laundering involving the use of illegally obtained money
- Section 5 – Allows the ED to attach property involved in money laundering
- Section 17 – Grants power for search and seizure during investigations
- Section 19 – Gives the ED the right to arrest persons involved in the offence

Two individuals were arrested in connection with the scam: Aamir Khan and Romen Agarwal.





# Challenges in cryptocurrency Regulation

1. Anonymity and Decentralization-Cryptocurrencies have no central authorities or intermediaries which allows people to make transactions anonymously making it hard for FIU-IND to trace activities.
2. Cross Border Transactions-Digital currencies can easily be used for international transfers making it difficult for FIU-IND to operate or manage them quickly. Coordinating with countries and institutions becomes challenging due to varying rules and regulatory gaps
3. Rapid Technological Advancements-Criminals use sophisticated systems to hide their activities. FIU-IND struggles to keep pace with the speed of technological advancements and complexity of these developments.

## The Way Forward

1. Strengthen KYC (Know Your Customer) rules and promote cryptocurrencies that include built-in security and compliance features.
2. Enhance global cooperation, advocate for a unified international reporting framework to monitor cross-border crypto flows.
3. Invest in advanced tech tools, including Blockchain analysis, Artificial Intelligence (AI) and Machine Learning (ML)
4. Work towards a standardised global regulatory system for cryptocurrency to reduce loopholes and confusion

## Quiz

**Imagine this:** You find a great deal on a used laptop, half price, brand new listed on a marketplace that only accepts crypto.

The seller says:

"No worries, I don't do PayPal or bank, just send Bitcoin to this address."

No reviews, no refund policy, but it's a really good price.

What would you do?

- A. Buy it crypto is just the future of payments
- B. Ask the seller for more proof and customer feedback
- C. Refuse this sounds like it could be tied to fraud or stolen goods
- D. Offer to use an escrow service or crypto marketplace with buyer protection

👉 Choose your move and learn why it matters.

What Could Happen if It's Crypto Fraud?

1. You Lose Your Money Permanently ❌

Crypto transactions are irreversible once you send it, it's gone.

No bank, no chargeback, no refund. If the seller disappears, you're out of luck.

Even if you track the wallet, that doesn't help you get the funds back.

2. You Might Unknowingly Participate in a Crime ?

If the goods are stolen or linked to illegal activity, you could be buying stolen property.

In worst cases, your wallet or identity could be flagged in investigations if the funds are traced as part of a laundering operation.

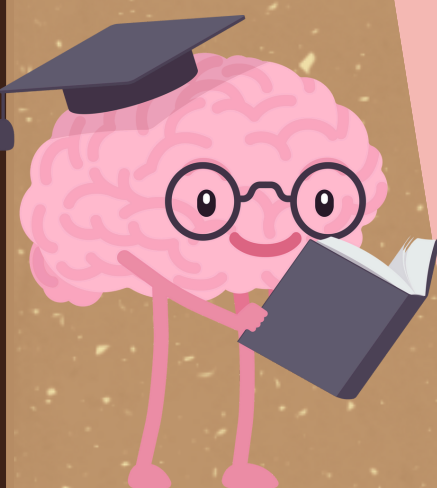
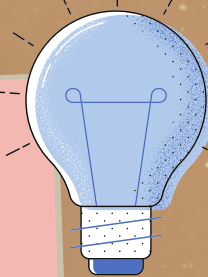
3. Your Identity Could Be Exploited 📄

If you shared any personal details (email, ID, wallet info), the fraudster might use or sell that data.

This opens the door to phishing, impersonation, or future scams.

Bottom Line: If you can't verify the seller, and there's no protection walk away.

Your crypto safety is your responsibility.





# THE END

*A Project by the "Criminal Law Forum" of  
Pravin Gandhi College of Law*



*July 2025*