VIRTUAL DIGITAL ASSETS DECODED

Understanding Technology, Legality, & Frauds

A CoinSwitch Publication

Foreword

India has emerged as a global leader in grassroots-level crypto adoption, ranking first in the Global Crypto Adoption Index for the third consecutive year in 2025. Millions of Indians today own Virtual Digital Assets (VDAs), using them as a tool to save, invest, and explore emerging technologies.

From small town India to urban metros, this rapid adoption reflects a broader digital transformation fueled by smartphone penetration, affordable internet, intuitive platforms, and growing awareness of digital finance. I am inspired by how these developments are enabling millions to participate in long-term wealth creation, positioning India at the forefront of the global digital financial revolution.

With such growth and adoption, the responsibility lies on us – virtual digital services providers – to safeguard consumer interest, and create a safer and inclusive crypto ecosystem in India. I'd like to dedicate this handbook to that cause.

At CoinSwitch, we view compliance, transparency, and security as non-negotiable. Beyond providing a platform for trading and investing, we are committed to being a trusted partner to the government and the community, fostering trust, awareness, and robust safeguards across India's crypto ecosystem.

– Ashish Singhal, Co-founder, CoinSwitch

With growth comes responsibility. The expansion of the crypto ecosystem has also attracted attempts to exploit its vulnerabilities. While crypto-related incidents are smaller in scale than broader cybersecurity frauds, they frequently involve complex, cross-border transactions requiring specialized expertise, tools, and coordination to track, trace, and resolve.

From an operational standpoint, supporting the ecosystem responsibly means working hand-in-hand with regulators, law enforcement, and industry stakeholders. Strengthening processes, upgrading systems, and adopting advanced monitoring tools are essential to safeguard the integrity of the market and ensure investor confidence.

–Vimal Sagar Tiwari, Co-founder, CoinSwitch

Crypto is a rapidly evolving global asset class, bringing with it inherent complexity. This handbook has been developed to assist police officials, law enforcement, policymakers, and regulatory bodies in navigating the dynamic crypto landscape. It provides practical insights, case studies, and best practices to enhance coordination and support informed, effective decision-making.

Sukant Dukhande, Director, Legal, CoinSwitch

About CoinSwitch

Founded in 2017, CoinSwitch is India's largest crypto trading platform and a pioneer in shaping the country's crypto ecosystem. With over 2.5 crore users, CoinSwitch operates a regulatory-compliant platform that simplifies and enhances crypto trading for both retail and professional investors. CoinSwitch is ISO/IEC 270001: 2022 certified and Financial Intelligence Unit (FIU-IND) registered.

Disclaimer

The tools and other resources mentioned in this document are shared purely for information purposes. Their inclusion does not imply endorsement. Readers are encouraged to independently assess the accuracy, reliability, and applicability of these resources before use.

Index

UNDERSTANDING CRYPTO BASICS

From everyday users to businesses, crypto and blockchain technologies are opening up new possibilities for transactions and investments. In this chapter, we explore the basics of Virtual Digital Assets (VDAs), how these transactions actually work, the difference between legitimate and fraudulent activities, and a clear overview of India's regulatory landscape.

How was Crypto Born?

In 2008, an unknown person or group using the name Satoshi Nakamoto released a white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System.”

The paper introduced Bitcoin as a decentralized digital currency that allowed people to send money directly without banks or intermediaries. In its early days, Bitcoin was often mined on personal computers or even given away in online games. But as awareness and adoption grew, its value began to rise steadily, turning it into one of the most revolutionary financial innovations of the modern era. The true identity of Satoshi remains a mystery to this day.

What is Crypto or VDA?

Cryptos, also called Virtual Digital Assets (VDAs), are a type of digital asset that can be bought, sold, or held as an investment. Today, this has grown into a trillion-dollar industry globally.

VDAs are entirely digital and secured using cryptography, making transactions safe and extremely difficult to tamper with. They operate on a peer-to-peer network, allowing users to send and receive value directly. Transactions are recorded on blockchains, digital ledgers that permanently store every transaction.

Unlike traditional assets, VDAs do not rely on banks or central authorities. This enables direct transfers worldwide, with features like transparency, security, and decentralization, although their value can fluctuate like other investments.

For example, Bitcoin is a cryptoasset. You can hold it like an investment, trade it, or use it to send value globally, while its history of transactions remains public and verifiable on the blockchain.

What is Blockchain Technology?

Think of blockchain as a shared digital notebook or khata book that exists across many computers. In the notebook every page technically records transactions, and when it’s full, it’s sealed and linked to the previous one, forming a chain of blocks. Once every transaction is written into this notebook, and once recorded, it cannot be changed or erased, making it secure and transparent. So, when tracing VDA related crimes, investigators should follow these digital trails block by block.

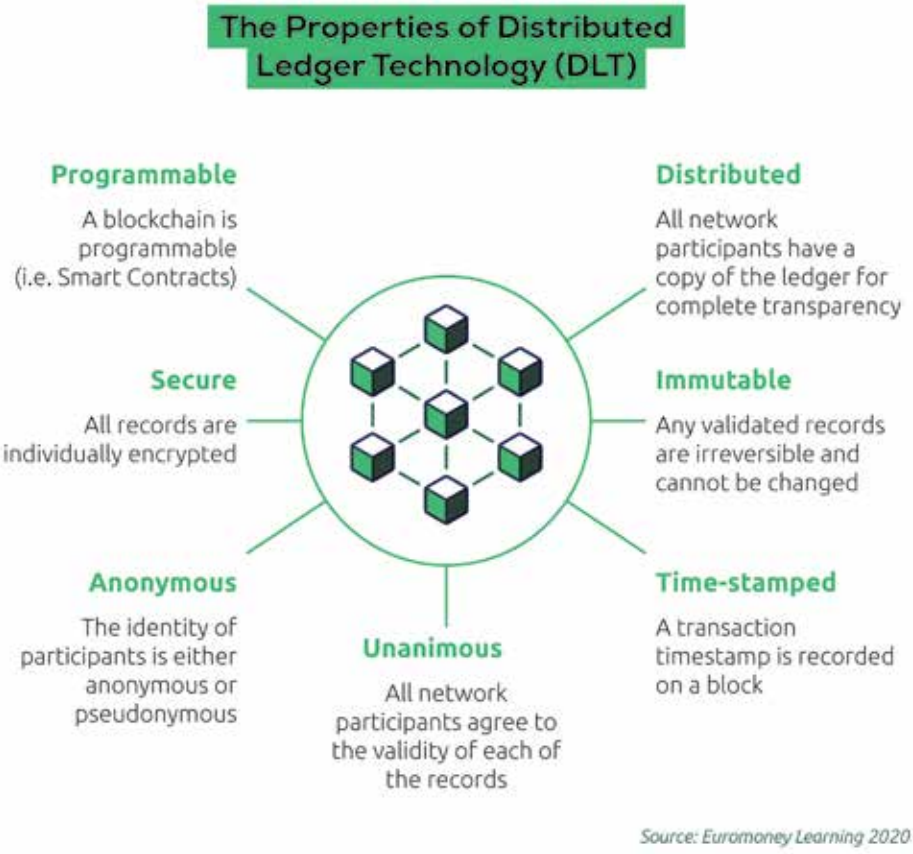
Blockchain allows people to transact directly with each other without a middleman. The network of computers worldwide validates transactions, and only when all participants have verified a transaction, the block is added to the ledger.

Once recorded, the transaction becomes a permanent part of the blockchain, visible to everyone but impossible to alter or delete. This decentralized and transparent system ensures trust, security, and accountability without relying on any single authority.

For example, Bitcoin, the first and largest crypto, uses blockchain to track every transaction ever made. Anyone can view this public ledger, which helps build trust and prevents fraud, showing how blockchain underpins the security of digital assets.

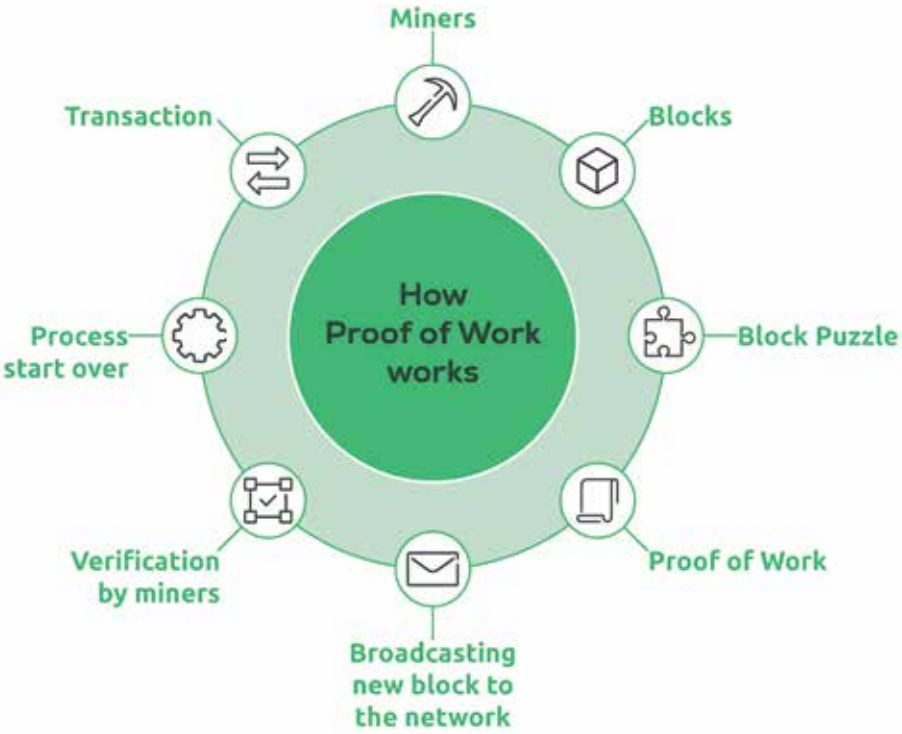
How Does Blockchain Work?

When transactions are verified and a new "block" is added to the blockchain, it happens through a pre-decided consensus mechanism among the participants, known as miners or validators. These are individuals or entities responsible for confirming transactions and maintaining the security and integrity of the blockchain network.



There are two primary types of consensus algorithms:

Proof of Work (PoW): In this system, miners use computing power to solve complex mathematical puzzles. The first miner to solve the puzzle gets the right to add a new block to the blockchain and earns a reward for doing so. This process is called mining. Bitcoin is a well-known example of a blockchain that uses PoW.



Proof of Stake (PoS): In this system, validators are chosen to add new blocks based on the amount of crypto they "stake" or lock up as collateral. Validators don't need massive computing power, instead, they are selected randomly or through delegation, depending on the algorithm. Several factors like wealth, age, number of days currency held for etc are taken into account. Ethereum now uses PoS after its transition from PoW.

Types of Cryptos

Bitcoin: Bitcoin is the first and largest crypto, often considered digital gold. It dominates around 59% of the global crypto market (as of Oct 24th 2025). Bitcoin has a capped supply of 21 million coins, with approximately 19.93 million already in circulation. Its decentralized nature allows peer-to-peer transactions. It is widely used as a store of value, investment, and for cross-border transactions.

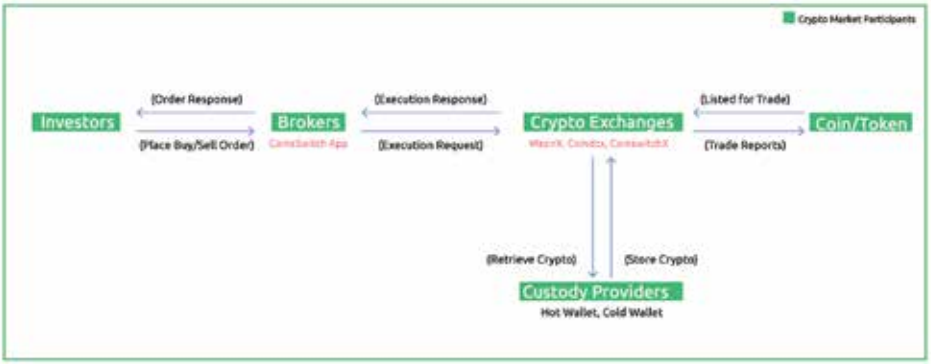
Altcoins: Apart from Bitcoin, other tokens are called altcoins. Be it Ethereum, Ripple, Cardano, Solana, Polygon etc. Ethereum dominates 12% of the crypto market (as of Oct 24th 2025). It is a decentralized platform that enables smart contracts and decentralized applications to build and run without downtime, fraud, control or interference from a third party. Altcoins can serve multiple purposes, from faster payments to decentralized finance, gaming, or governance. Their variety and

innovation make them an important part of the broader crypto ecosystem. Unlike Bitcoin, there are non public ledgers for altcoins.

Stablecoins: These are cryptos designed to maintain a stable value, often pegged to a fiat currency like the US dollar. Examples include USDT (Tether), USDC, and BUSD. They combine the benefits of digital assets, fast, borderless, and decentralized transactions, with the price stability of traditional money. This stability makes stablecoins ideal for trading, remittances, and acting as a safe haven during volatile market periods.

Memecoins: Memecoins are cryptos created mainly for fun, community engagement, or internet culture rather than serious financial purposes. Popular examples include Dogecoin and Shiba Inu. While they often start as jokes or memes, some gain large followings and market value due to social media hype, celebrity endorsements, or community support. Memecoins are highly volatile and speculative, attracting traders looking for short-term gains.

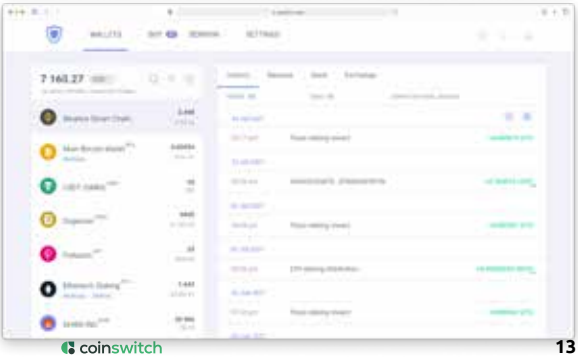
How the Crypto Market Works



A crypto exchange is a digital marketplace where users can buy, sell, or trade VDAs (cryptos). Exchanges act as intermediaries, matching buy and sell orders, executing trades, and safely holding user's assets. They are often preferred by beginners for their ease of use and reliability.

Key Participants in the Ecosystem:

Users: Individuals or institutions who register, complete KYC, fund their accounts, and place buy/sell orders.



Custody Providers: Technology platforms that securely store assets on behalf of exchanges, without exercising any control over them.

Exchanges: Operate the order-matching engine that executes trades efficiently and transparently.

User Flow: Users sign up, complete verification, add funds (fiat or crypto), and place buy or sell orders. The exchange matches these orders and updates balances once trades are executed.

How Exchanges Earn: They charge small trading fees based on order size, type, and volume.

Fund Safety: Exchanges typically maintain 1:1 user fund reserves, storing crypto in secure custody wallets and fiat with regulated banks. Multiple approval layers ensure safe fund movement.

How Crypto Transactions Work

Understanding how crypto/VDA moves is important for anyone using or studying digital assets. At a basic level, these transactions involve three key components: wallets, exchanges, and public ledgers.

Wallets: A wallet is a digital tool used to store and manage digital assets. There are two main types:

Hot Wallets: Connected to the internet, easy to access, and convenient for everyday transactions.

Example: Mobile & web wallets

Think of hot wallets like the wallet in your pocket, easy to spend from anytime.

Metamask, Coinbase Wallet, Trust Wallet etc are some of the hot wallets.

Cold Wallets: These are stored offline and are not connected to the internet and are safer for storing large amounts of VDA.

Example: Hardware wallets or paper wallets

Think of cold wallets like a safe at home, secure, but not for daily use.

Exchanges: Exchanges are platforms that let users buy,

sell, or trade crypto/VDA. They act as intermediaries between buyers and sellers.

Examples: CoinSwitch, CoinDCX, Mudrex

Public Ledgers: Every VDA transaction is recorded on a blockchain, which acts as a public ledger. This ensures transparency and immutability, meaning transactions cannot be altered.

For example, Bitcoin's blockchain records all transactions made with the crypto, providing a public ledger that anyone can verify.

What Is Crypto Used For in India?

In India, crypto or VDAs are not legal tender or currency, meaning they cannot be used like the Indian Rupee to buy goods or services. You can't walk into a store and pay with Bitcoin or Ethereum.

Instead, VDAs are treated as a digital asset where people can buy, hold, or sell these assets as part of their investment portfolio to diversify and potentially grow their wealth.

In other words if someone buys Bitcoin or Ethereum in India, they're not using it as money but as an investment, just like buying shares of a company. The value of Bitcoin, like a stock, can go up or down depending on market demand and global trends.

In short, in India, VDAs are an investment option, not a replacement for the Rupee or any government-backed currency.

What are Legitimate Activities?

Legitimate VDA activities are safe and legal ways to use or invest in digital assets. These include:

1. Investment: People purchase VDAs such as Bitcoin or Ethereum to store value or benefit from potential price growth over time and pay taxes as prescribed by the Income Tax Act.

2. Trading on FIU Registered Exchanges: Buying and selling digital assets through FIU registered platforms that follow KYC (Know Your Customer) and AML (Anti-Money Laundering) rules.

Understanding VDA Exchanges and Their Types

As explained earlier, a crypto/VDA exchange is a platform where people can buy, sell, or trade cryptos like Bitcoin and Ethereum. These exchanges allow trading digital assets in a secure and convenient manner.

There are two main types of VDA exchanges:

1. Centralized Exchanges (CEX) – Operated by registered companies that act as intermediaries. They function within a regulatory framework, conduct KYC, and enable data sharing, making them the most secure and reliable option for users.

Example: CoinSwitch, CoinDCX.

2. Decentralized Exchanges (DEX) – Operate without intermediaries, allowing users to trade directly through smart contracts. They offer greater privacy but come with higher risks due to the absence of regulation and KYC processes.

Example: Uniswap, PancakeSwap

3. Peer-to-Peer (P2P) – Enables users to trade directly with one another without an exchange platform. While offering flexibility, P2P trades carry increased risks of fraud and limited recourse in case of disputes.

Example: Binance P2P, Paxful, WazirX P2P

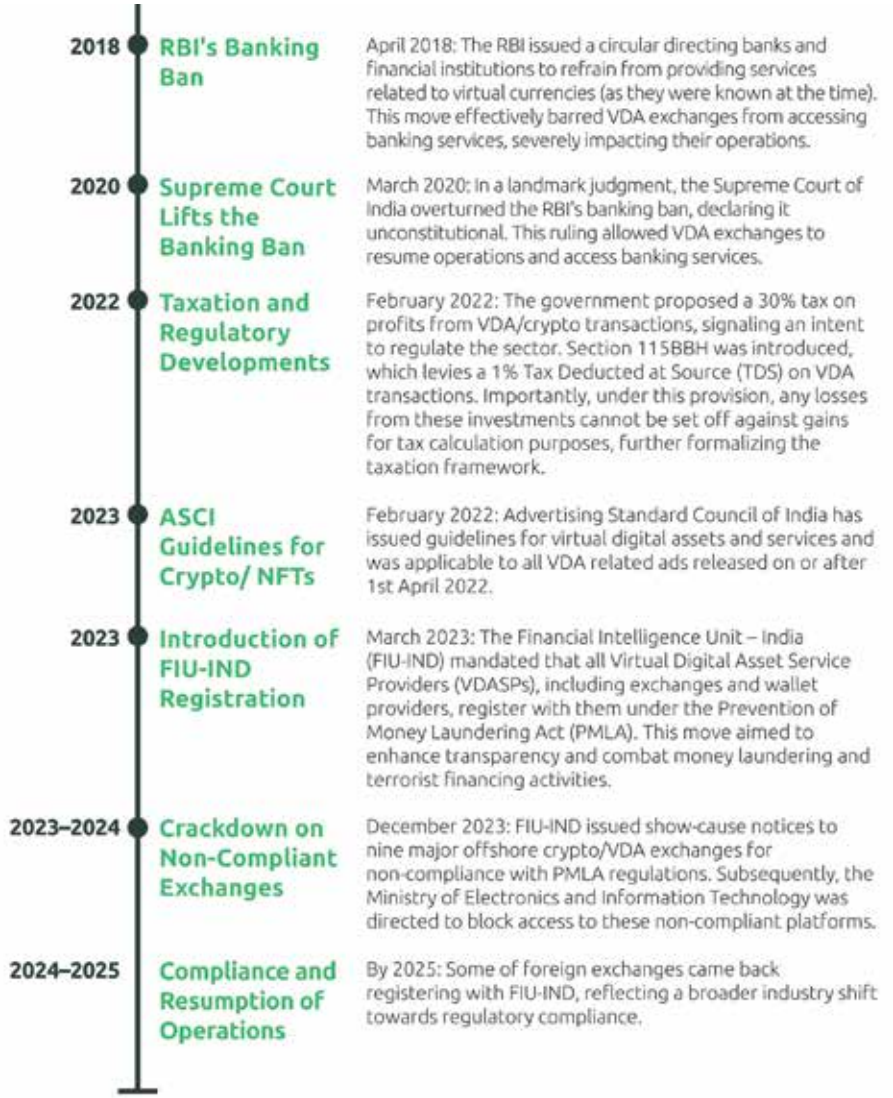
Crypto Adoption in India

India has consistently ranked #1 in the crypto retail led adoption for the third consecutive year according to the TRM Lab's Country Crypto Adoption Index 2025.

India ranks 1 in crypto adoption

Overview of India's Regulatory Landscape

India has taken a cautious and evolving approach to crypto/VDA regulation. The government and regulators aim to protect users, prevent fraud, and curb money laundering, while allowing innovation to continue. Here's a simplified timeline of major developments:



Is There a Regulator for VDA in India?

Currently, in India, VDAs are legal and regulated under the Prevention of Money Laundering Act (PMLA) and do not have a dedicated regulator.However, the Financial Intelligence Unit – India (FIU-IND), a government agency under the Ministry of Finance, plays an important role in overseeing VDA-related financial activities. Its main goal is to monitor transactions to prevent money laundering, terrorism financing, and other illegal activities.

In the context of VDA, the FIU performs several key functions. It collects and analyzes financial data, receiving reports of suspicious transactions from banks, exchanges, and other entities. This helps detect patterns of fraud, money laundering, or other illicit activity. The FIU also ensures that crypto/VDA exchanges comply with regulations such as KYC (Know Your Customer) and the Prevention of Money Laundering Act (PMLA).

The FIU also coordinates with other agencies, sharing information with law enforcement, regulatory bodies, and international authorities to prevent financial crimes. By monitoring transactions, it promotes transparency and maintains trust in the financial system, ensuring that digital asset movements can be traced if needed.

For example, if someone tries to move large amounts of digital assets through multiple exchanges to hide the source of funds, the FIU can analyze reports from these exchanges, identify suspicious patterns, and take appropriate action.

Registered Entities with FIU

The Financial Intelligence Unit – India (FIU-IND) maintains a list of registered Virtual Digital Asset Service Providers (VDA SPs), ensuring compliance with KYC, AML, and other regulatory requirements. CoinSwitch, CoinDCX, Mudrex, ZebPay etc are some of the registered entities with FIU.

S. No	Entity Name	Trade Name
1	Neblio Technologies Private Limited	CoinDCX
2	ANQ Digital Finserv Private Limited	ANQ Finance
3	Unocoin Technologies Private Limited	Unocoin
4	Buyhatke Internet Private Limited	Onramp
5	Giottus Technologies Private Limited	Giottus

S. No	Entity Name	Trade Name
6	Bitbns Internet Private Limited	Bitbns
7	Awlencan Innovations Private Limited	Zebpay
8	Zanmai Labs Private Limited	WazirX
9	Bitcipher Labs LLP	CoinSwitch
10	Nextgendev Solutions Private Limited	CoinSwitchX
11	RPFAS Technologies Private Limited	Mudrex
12	Iblock Technologies Private Limited	BuyUCoin
13	Wollfish Labs Private Limited	Coindhan
14	Rario Digital Private Limited	Rario
15	Angelic Infotech Private Limited	Suncrypto
16	CarretX Technologies Private Limited	Carret
17	Ante Multimedia Private Limited	-
18	Abhibha Technologies Private Limited	Onmeta
19	Smartliving Digital Technologies Private Limited	Cryptosmartlife
20	Ucy Technology Private Limited	Pyor
21	Digital Collectibles Private Limited	Rario
22	Veeratva Technologies Private Limited	Valr
23	Transak Technology India Private Limited	Transak
24	Remizo Technologies India Private Limited	Getbit
25	FinGenie Tech Private Limited	Bytex
26	Ardour Labs Private Limited	-
27	Inocyx Technologies Private Limited	Inocyx
28	Metatoken Technologies Private Limited	Fanztar
29	Excellium Technologies Private Limited	Delta Exchange
30	Rovi91 Innovations Private Limited	-
31	Longreen India Private Limited	Bitbse.com
32	Flitpay Private Limited	FlitPay
33	Fincrypt LLP	Stable Pay
34	Arthbit Private Limited	ArthBit
35	Pagarpay India Private Limited	Density Exchange
36	Lightningnodes Technologies Private Limited	Pi42
37	Kooz Advisors and Technologies Private Limited	KoinBX

S. No	Entity Name	Trade Name
38	Mindless Pandora Tech Solutions Private Limited	-
39	FanzCraze Technologies Private Limited	-
40	SUBHX Infotech (OPC) Private Limited	BIT24HR
41	Peken Global Limited	KuCoin
42	ALSD Technologies Private Limited	Alpyne
43	Damsol Private Limited	Square
44	First Answer India Technologies Private Limited	Liminal
45	Eclipton Technologies Private Limited	Eclipton
46	Blockoville OU	Blockoville
47	Binance International Limited	Binance

Further information can be found on https://fiuindia.gov.in/

Why was VDA Included in PMLA?

Crypto is a global asset, which means it can move quickly across borders without the involvement of banks or other intermediaries. Because of this, it becomes challenging for authorities to track and monitor suspicious transactions.

To address this issue, the government included VDA under the Prevention of Money Laundering Act (PMLA). By doing so, digital assets are brought under a legal framework, requiring Virtual Digital Asset Service Providers (VDASPs), such as exchanges and wallet providers, to register with the Financial Intelligence Unit (FIU-IND), maintain proper records, and report any suspicious activity.

This framework ensures that, while the regulator can prevent the misuse of crypto, individuals and businesses can still use, invest, and innovate with digital assets safely.

What is the Travel Rule in Crypto/VDA?

The Travel Rule is a global anti-money laundering (AML) requirement that ensures certain key information “travels” along with a VDA transaction, just like it already does for traditional bank transfers.

It was introduced by the Financial Action Task Force (FATF), the global watchdog for AML/CFT (Anti-Money Laundering / Countering the Financing of Terrorism).

When someone sends crypto (like Bitcoin or USDT) from one exchange or wallet to another, the sending exchange must share identifying details about both the sender and receiver with the receiving exchange.

This ensures that authorities can track who is sending money to whom, preventing the

use of crypto for money laundering, terror financing, or other illegal activity.

The Indian government is strengthening tax transparency and regulatory oversight in the Virtual Digital Assets (VDAs) sector. The Finance Bill 2025, tabled on February 1, updates the definition of VDAs and mandates reporting of crypto transactions. This aligns with the G20-endorsed OECD Crypto-Asset Reporting Framework (CARF) for automatic information exchange between tax authorities. In India:

- The Financial Intelligence Unit (FIU-IND) monitors compliance under the Prevention of Money Laundering Act (PMLA).
- All registered VDA exchanges are "Reporting Entities", meaning they must:
  - Conduct full KYC.
  - Maintain records of all transactions.
  - Report suspicious activity (STRs).
  - Ensure information is shared when digital assets move between platforms.

Even if a transaction moves from an Indian exchange to a foreign exchange, the Indian platform must maintain sender/receiver records as per the Travel Rule.

How is VDA Taxed in India?

In India, VDA's are under Section 2(47A) of Income Tax Act, 1961, and profits from selling or exchange or conversion of one VDA into another VDA are taxable. The provisions are introduced to track VDA transactions and collect tax, while simplifying compliance.

30% Tax on Profits: 30% Tax on Profits: Any profit or gain from selling or conversion of one VDA into another VDA is taxed at flat 30%, irrespective of the holding period (i.e no distinction between short term and long term gain).

On top of the 30% rate, an additional tax of surcharge (as per income income level) and cess at the rate of 4% are payable, slightly increasing the effective tax rate.

1% TDS on VDA Transactions: In order to track the VDA transaction, 1% TDS deducted at source is applied on every sale transaction. This is deducted by broker or exchange or buyer (depending on who facilitates the transaction).

Losses Cannot Be Set Off or Carry Forward: If you incur a loss from VDA investments, it cannot be used to reduce taxable gains from other VDA transactions or from other Income (like salary, house property, business income, interest income). Further, such loss cannot be carried forward to future years.

VDA Tax on Different Activities

Transaction	Taxation
VDA to INR	Selling VDA at a profit is taxed at 30%, while buying VDA with INR is not taxed
VDA to VDA	Treated as gifts, airdrops are taxable at individual slab rate if the value exceeds INR 50,000 in a financial year
Crypto Gifts	Receiving crypto gifts valued over INR 50,000 in a financial year is subject to a 30% tax.
VDA Airdrops	Treated as gifts, airdrops are taxable at 30% if the value exceeds INR 50,000 in a financial year.
DeFi Income	Selling, swapping, or spending tokens earned from DeFi activities is taxed at 30%. Receiving new tokens is taxed upon receipt at your individual tax rate.
HODLing	Simply holding crypto without selling or exchanging incurs no tax.
Wallet Transfers	Moving crypto between your own wallets does not attract any tax.

What are Advertising Guidelines for Crypto/VDA?

The Advertising Standards Council of India (ASCI) has issued guidelines for promoting virtual digital assets (VDAs), including cryptos and NFTs.

All crypto/VDA ads must include the following disclaimer:

“Crypto products and NFTs are unregulated and can be highly risky. There may be no regulatory recourse for any loss from such transactions.”

This ensures that potential investors are aware of the risks before engaging with VDA products.

Further guidelines can be found on ascionline.in.

COMMON VDA FRAUDS IN INDIA

Crypto's rapid adoption in India has also attracted malicious actors exploiting the lack of regulatory oversight and the general public's limited understanding of digital assets. Let's understand some of the very common kinds of frauds in India.

Type of Fraud	How it Works	Real Example
Investment Scams / Ponzi	Fake projects promise high returns (e.g., “Double your Bitcoin in 10 days”).	2024: Telangana police busted a ₹6.4 crore fake investment app using Bitcoin
Fake Exchanges	Fraudsters build fake trading platforms. Victims deposit crypto but can’t withdraw.	2023: Delhi cyber cell tracked a fake site mimicking Binance.
Pump & Dump	Groups artificially inflate the price of a token and dump it later.	Telegram groups run coordinated scams.
Phishing & KYC Frauds	Fake messages asking users to “verify KYC” or “update wallet.”	When users click on fake KYC link or sophisticated link, money is lost
Rug Pulls	Developers create a new token, attract investors, then vanish.	Several meme coins have disappeared overnight.
Impersonation & Deepfakes	Scammers use celebrity or influencer videos to promote fake crypto giveaways.	Fake Elon Musk videos on YouTube used to steal Bitcoin
Hacks	Exploiting system flaws or malware to access wallets or databases and steal money or sensitive information.	In 2024 WazirX was hacked at $235 M and in 2025, CoinDCX was hacked for $44M.

VDA frauds are often an extension of regular cybercrime, same methods, but the money ends up in a digital wallet.

TRACING AND INVESTIGATION OF VDA FRAUDS

Effective tracing and investigation are essential to identify perpetrators, recover lost funds, and safeguard the ecosystem. Leveraging advanced tools, collaboration, and specialized expertise ensures robust protection for investors and the broader crypto market.

1. Tracing and Investigating Frauds

VDA frauds often use schemes like Ponzi scams, phishing attacks, or fake investment platforms to deceive people. Investigating these frauds requires special tools and expertise to track the digital trail left on the blockchain, since every transaction is recorded but not always easy to trace.

2. How VDA Transactions Can Be Tracked On-Chain

Blockchain technology offers transparency, allowing investigators to trace transactions from one wallet to another. Tools like Chainalysis and TRM Forensics enable the visualization of transaction paths, helping to identify the flow of illicit funds.

3. Importance of KYC, IP Logs, and Exchange Cooperation

Know Your Customer (KYC) procedures are vital for verifying the identity of users on VDA exchanges, aiding in the prevention of fraudulent activities. Additionally, IP logs provide crucial information about the geographical location and device used during transactions. Cooperation from exchanges is essential in accessing these records and tracing the perpetrators.

4. How to Gather Digital Evidence

Digital evidence can be collected from various sources, including mobile devices, computers, and online platforms. Forensic experts employ techniques like data extraction, memory analysis, and cloud investigations to retrieve and analyze this evidence. In one case, police uncovered a China-based scam through analysis of bank transactions, IP logs, and WhatsApp chats.

5. Steps for Approaching VDA Exchanges During Investigations

When investigating VDA/crypto frauds, law enforcement agencies should:

Identify the Exchange: Determine which platform was used for the fraudulent transactions.

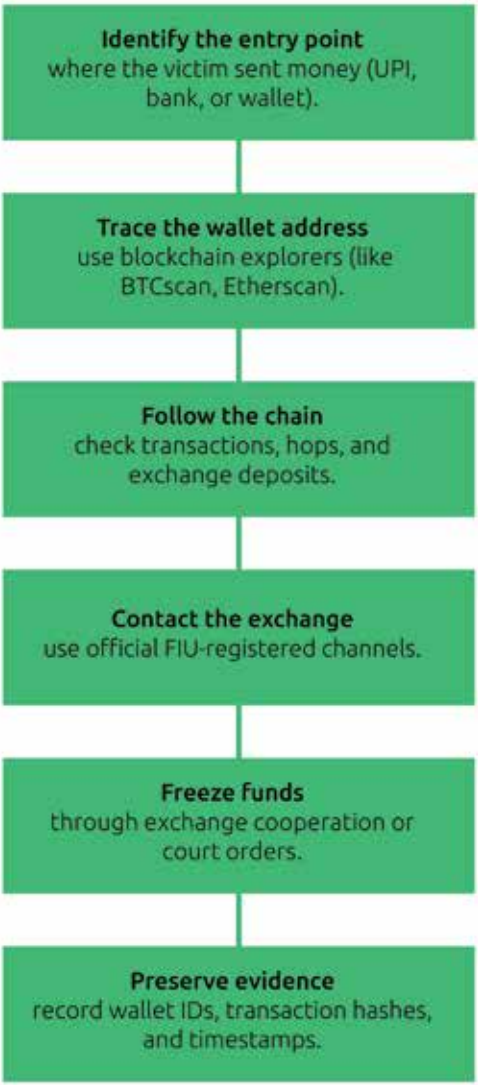
Request Information: Formally request user data, transaction history, and IP logs from the exchange.

Analyze Data: Examine the provided information to trace the flow of funds and identify suspects.

Collaborate with Other Agencies: Work with cybercrime units and other relevant authorities to coordinate the investigation.

6. Sample Investigation Flowchart

A typical VDA fraud investigation follows these steps:



Example:

A victim reports ₹2 lakh stolen via fake Bitcoin investment. Police traced the USDT wallet, found it deposited on Binance, contacted Binance via the FIU channel, and froze funds within 24 hours.

The rise in VDA fraud cases in India necessitates a comprehensive approach to investigation, combining technological tools, legal procedures, and inter-agency cooperation.

COLLABORATION BETWEEN POLICE, LEAS & EXCHANGES

As crypto or VDA adoption accelerates in India, the need for effective collaboration between police, law enforcement agencies (LEAs) and crypto exchanges has become paramount. The necessity for strong regulatory frameworks and cooperative efforts to prevent misuse of digital assets for illicit activities is crucial.

Why Collaboration Between Law Enforcement and VDA Exchanges is Important

Preventing Financial Crimes: Digital assets, due to their digital and often anonymous nature, can be misused for money laundering, fraud, and terrorism financing. Collaboration ensures that suspicious activities are detected early and investigated effectively.

Enhancing Regulatory Compliance: By working with exchanges, law enforcement can ensure that platforms adhere to KYC, AML, and other regulatory requirements. This strengthens the integrity of the VDA ecosystem and aligns it with national and international standards.

Protecting Users and the Market: Collaboration helps protect investors from scams or fraudulent schemes, while maintaining trust in the digital asset market, encouraging safe adoption of digital assets.

Efficient Investigations: Exchanges hold critical transaction data. Partnering with law enforcement allows for timely and accurate access to information, enabling faster investigations and resolution of cases.

Building a Safe and Transparent Ecosystem: Continuous dialogue between LEAs and exchanges fosters a secure, transparent, and responsible VDA environment, supporting both market growth and legal oversight.

How CoinSwitch Supports Law Enforcement

As India's largest VDA platform, CoinSwitch is deeply committed to supporting law enforcement and ensuring that the digital asset ecosystem remains transparent, safe, and compliant.

We implement stringent Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols, thereby ensuring compliance with the Prevention of Money Laundering Act (PMLA). These measures not only enhance the integrity of the digital asset market but also facilitate LEAs in tracing and investigating suspicious activities.

a. Compliance-first Approach

- CoinSwitch complies with PMLA regulations and is registered with the Financial Intelligence Unit – India (FIU-IND).
- It has robust KYC (Know Your Customer) and AML (Anti-Money Laundering) policies aligned with FATF and Indian legal frameworks.
- Suspicious transaction reports (STRs) and large-value transactions are regularly filed with FIU-IND as part of its commitment to transparency.

KYC, AML & PMLA Processes at CoinSwitch

- Name screening for PEP and GWL
- Verify PAN using NSDL database
- Robust KYC of Users on the app. Seamless KYC process
- Verify email and mobile using OTP
- Travel rule generation for VDA in/out from our platform and travel rule integration
- Penny drop verification for beneficial ownership identification
- Chainalysis implementation for VDA transaction investigation
- Signzy for transaction monitoring
- Employee training via Fintelekt
- Data storage as per regulatory requirements
- Policy management for PMLA
- Principal officer and designated director for management of PMLA requirements
- Deposit and withdrawal investigation to ensure the safety of user funds
- Only adult resident Indian customers are allowed on the platform

b. User Protection Initiatives

- 24x7 security monitoring for fraud detection.
- Dedicated Law Enforcement Helpdesk: nodaldesk@coinswitch.co
- Awareness campaigns and in-app safety messages to educate users about scams, phishing, and fake investment schemes.Partnerships with government and cybersecurity agencies to strengthen the industry's safety net.

c. Capacity Building Support

CoinSwitch collaborates with state police and investigative agencies through:

- Workshops and training programs on blockchain tracing and crypto fraud investigation.

- Resource sharing, including data analysis support for ongoing cases (subject to legal protocols).

- Advisory partnerships to help shape balanced and effective crypto regulation in India.

How to Freeze Funds?

Law Enforcement Agencies (LEAs) may consider approaching the concerned platform or exchange to request the freezing of a specific user's funds, rather than freezing the exchange's entire account.

CoinSwitch has established a streamlined process for LEAs to submit official requests at—nodaldesk@coinswitch.co

CoinSwitch Wallet & Liquidity Services

CoinSwitch offers secure wallet and liquidity services to support Law Enforcement Agencies (LEAs) in managing seized virtual digital assets during investigations.

In addition, CoinSwitch offers liquidity and conversion support, allowing authorized agencies to convert seized crypto assets into fiat currency when directed by competent authorities. This process is executed in compliance with existing legal and regulatory frameworks, maintaining full transparency and auditability.

LEGAL & REGULATORY FRAMEWORK IN INDIA ON VDAS

The legal and regulatory landscape governing VDA in India is multifaceted, involving a combination of existing laws, evolving guidelines, and international best practices. This chapter delves into the Indian legal framework applicable to these frauds, the role of key regulatory bodies like the Reserve Bank of India (RBI) and the Ministry of Electronics and Information Technology (MeitY), and global enforcement practices that influence India's approach.

Indian Laws Applicable to VDA Fraud

1. Indian Penal Code (IPC)

The IPC serves as the cornerstone for criminal law in India. While it does not specifically address VDAs, provisions under sections such as 420 (cheating), 406 (criminal breach of trust), and 120B (criminal conspiracy) have been invoked in cases involving VDA fraud. For instance, in 2021, a Delhi court ruled that transactions in digital assets must comply with the general laws in force in India, including the IPC, highlighting the applicability of these provisions to VDA-related offenses.

2. Information Technology Act, 2000 (IT Act)

The IT Act addresses cybercrimes and electronic commerce. Sections 66C (identity theft), 66D (cheating by personation), and 66E (violation of privacy) are pertinent in cases where VDA are used for fraudulent activities. The Act provides a legal framework for addressing offenses committed through digital means, including those involving virtual currencies.

3. Prevention of Money Laundering Act, 2002 (PMLA)

In 2023, the Indian government amended the PMLA to include Virtual Digital Assets (VDAs), bringing these transactions under its purview. This amendment mandates that exchanges and intermediaries report suspicious activities, aligning with global anti-money laundering standards.

Global Best Practices for VDA Enforcement

India's approach to VDA regulation is influenced by international standards and practices. The Financial Action Task Force (FATF), a global financial crime watchdog, has urged countries to intensify efforts to regulate digital assets, citing persistent risks and regulatory gaps. As of April 2025, only 40 out of 138 jurisdictions evaluated were "largely compliant" with FATF's crypto standards, highlighting the need for enhanced global cooperation.

In the European Union, the Markets in Crypto-Assets (MiCA) regulation, effective from 2024, provides a comprehensive framework for crypto assets, including licensing requirements for issuers and stringent anti-money laundering measures. This serves as a model for countries like India in developing robust regulatory frameworks.

Example 1: United States (DOJ)

- In 2023, the U.S. recovered $3.4 billion from a Silk Road-linked crypto wallet.
- Lesson: Blockchain transparency allows recovery even after years.

Example 2: Singapore (MAS)

- Every exchange must be licensed and reported to MAS.
- Lesson: Strict licensing reduces cross-border fraud.

Example 3: UK (FCA)

- Enforces Travel Rule for crypto, all transactions must carry sender details.
- Lesson: Transparency helps trace suspects faster.

Crypto regulation at a glance

The table provides a summary of digital asset legislative, regulatory, and licensing status as of January 2025. It factors in the implications of the EU's Markets in Crypto-Assets Regulation (MiCAR), which entered into force in June 2023 becoming fully operational in December 2024.

	Regulatory Framework	Licensing / Registration	Travel Rule	Stablecoins
United States	🟢	⚫	⚫	🟢
European Union	⚫	⚫	⚫	⚫
United Kingdom	🟢	⚫	⚫	🟢
Argentina	🟢	⚫	🟢	🟡
Australia	🟢	🟢	🟢	🟢
Bahamas	⚫	⚫	⚫	⚫
Bahrain	⚫	⚫	⚫	🟢
Brazil	🟢	🟢	🟢	🟢
Canada	🟢	⚫	⚫	🟢
Cayman Islands	⚫	⚫	⚫	⚫
Gibraltar	⚫	⚫	⚫	⚫
Guernsey	⚫	⚫	⚫	⚫
Hong Kong SAR	⚫	⚫	⚫	🟢
India	🟢	🟡	⚫	🟡
Isle of Man	⚫	⚫	⚫	⚫
Japan	⚫	⚫	⚫	⚫
Kenya	🟢	🟢		🟡
Liechtenstein	⚫	⚫	⚫	⚫
Mauritius	⚫	⚫	⚫	🟢

	Regulatory Framework	Licensing / Registration	Travel Rule	Stablecoins
Norway	●	●	●	●
Qatar	●	●	●	●
Saudi Arabia	●	●	●	●
Singapore	●	●	●	●
South Africa	●	●	●	●
Switzerland	●	●	●	●
Taiwan	●	●	●	●
Turkey	●	●	●	●
UAE	●	●	●	●
Ukraine	●	●	●	●

Credit: PwC, March 2025

● **Legislation/regulation in place**

Signifies that extensive crypto legislation/regulations have been established.

● **Active legislative/regulatory engagement**

Indicates that there is ongoing activity, such as regulatory discussions, consultations, or pending implementation of crypto-related laws and regulatory frameworks.

● **Legislative/regulatory process not initiated**

Implies that the jurisdiction has not yet started formulating or considering specific crypto asset legislation or regulatory frameworks.

CASE STUDIES & LEARNINGS

This chapter compiles real-world studies and insights drawn from Indian and international experiences in tracing, investigating, and resolving crypto-related offenses. Each case highlights practical challenges, investigative approaches, and the learnings that can help strengthen future responses to crypto crimes.

Case Study 1

The Fake Exchange App Scam (Telangana, 2025)

Background

The victim's ordeal began on a popular matrimonial website, where he connected with a profile named 'Nanditha Reddy'. Over several months, the scammer, who later claimed to have relocated to Malaysia, built trust before introducing a seemingly lucrative crypto investment opportunity.

Investigation

After receiving the complaint, the Telangana Cyber Security Bureau (TGCSB), with the help of a specialised crypto investigator, traced the digital footprint of the stolen funds. The probe revealed that 2,703 USDT had been transferred to a wallet registered to a Chinese national, Jiang Chuanxuan, on the international crypto exchange OKX.

Acting swiftly, TGCSB issued a notice to OKX to freeze the suspect's wallet. Following a court order, the exchange was directed to refund the frozen assets.

Outcome

TGCSB successfully recovered a portion of the stolen crypto, marking one of the few instances where funds lost to an international crypto scam were traced and refunded to an Indian victim.

Key Learnings

- Early reporting and blockchain tracing tools are critical in recovery.
- Coordination with global exchanges enables effective fund freezes.
- Cross-border cooperation remains essential for crypto-related investigations.

Source: *https://www.ndtv.com/india-news/cryptocurrency-stolen-in-online-fraud-recovered-from-foreign-wallet-in-telangana-9156897*

Case Study 2

Crypto Rug-Pull (Himachal Pradesh, 2023)

Background

Starting around 2018, a fraudulent network in Himachal Pradesh launched several cryptocurrency coins, notably "KRO" (Korvio Coin) and "DGT". They lured thousands of investors in the Kangra and Hamirpur districts with promises of high short-term returns, built a recruitment network, and operated a ponzi-style architecture.

Investigation

The scheme involved initial activation fees, manipulated coin pricing, and repeated launches under different names (such as the companies "Hypenext" and "Aglobal") once earlier schemes slowed down.

A special investigation team (SIT) was formed after the matter was raised in the state legislative assembly, and at least five arrests were made while the main kingpin remained at large.

Outcome

Authorities estimate that over ₹200 crore (more than 2 billion INR) was swindled from victims in Himachal Pradesh over the period. The exact amount remains under verification, and investigations are ongoing.

Key Learnings

- Encourage victims to report promptly to local cyber police stations or cybercrime.gov.in. Quick reporting greatly improves the chances of fund recovery.
- Regulatory and enforcement frameworks need to be proactive and coordinated at both state and national levels.
- Equip district-level cyber units with training on crypto tracing, wallet identification, and blockchain verification to decentralize response and reduce investigation delays.

Source: *https://www.indiatoday.in/india/story/crypto-investment-fraud-thousands-lose-over-rs-200-crore-in-series-crypto-rug-pulls-2443594-2023-10-03*

Case Study 3

Chinese-Linked Crypto Fraud (Gorakhpur, 2025)

Background

In Gorakhpur (Uttar Pradesh), a fraud network operating under the guise of NGOs, fake business accounts, and mule-bank accounts orchestrated large-scale cyber-fraud. The gang's mastermind, Shailesh Chaudhary, maintained direct contacts with Chinese hacker-handlers. Funds acquired via online scams were routed through mule accounts, converted into cryptocurrency (USDT on TRC-20), and forwarded via hawala networks to Dubai, Singapore and Hong Kong.

Investigation

The gang had opened current accounts in the names of NGOs and front companies. Fraud proceeds were deposited to these accounts, withdrawn via ATMs and bank branches, then converted into cryptocurrency and transferred abroad.

Investigation uncovered: ₹70.54 lakh of suspicious transactions traced, ₹9.60 lakh funds frozen.

The crypto wallet addresses (e.g., TLbuG…, TYzp…) and foreign-linked digital wallet transfers were also identified.

Outcome

Five accused persons including Chaudhary, Adil Shafiq, Shubham Rai, Vishal Gupta and Anuj Sahu were arrested by Gorakhpur Cyber Crime Branch. Investigations revealed the network was part of a larger international chain linked to China, Singapore and Dubai.

Key Learnings

- Fraudsters are using NGO/business front accounts to mask illicit funds and convert them into crypto.
- Mule bank accounts continue to be a primary conduit for entering illicit proceeds, followed by crypto conversion.
- Identifying wallet addresses and tracking digital transfer chains is crucial for asset-freeze and recovery.

Source: *https:///the420.in/chinese-hackers-cyber-fraud-ngo-business-gorakhpur/*

CLOSING NOTE: CALL FOR CO-OPERATION AND CAPACITY BUILDING

Crypto and blockchain technology have introduced immense opportunities for innovation, but they have also brought new challenges for law enforcement, regulators, and policymakers. As digital assets grow in India, collaboration across public institutions, private platforms, and global agencies has become critical to ensuring user safety, market integrity, and national security.

1. The Need for Co-operation

A crypto transaction can move across countries and exchanges in seconds. This complexity demands strong inter-agency coordination and public–private partnerships to prevent misuse of the technology.

- **Law Enforcement Collaboration:** Crypto exchanges, investigative agencies, and cyber cells must work together to share intelligence and act swiftly. Joint efforts between the FIU-IND, RBI, CERT-In, and leading exchanges have helped prevent fraud and recover lost funds.

- **Cross-border Intelligence Sharing:** Participation in global networks such as the Egmont Group and adherence to FATF's Travel Rule strengthen India's role in international crypto enforcement.

- **Unified Legal Understanding:** Regular training sessions, handbooks like this one, and centralized helpdesks for law enforcement help ensure consistent interpretation of laws.

2. Capacity Building and Knowledge Empowerment

As more Indians use crypto, building technical and legal capacity among enforcement and regulatory professionals is essential.

- **Training & Workshops:** Dedicated blockchain investigation training modules should be introduced for police academies and cyber labs across metro cities.

- **Knowledge Sharing Platforms:** Setting up centralized crypto fraud reporting dashboards and intelligence databases will enable faster information flow across agencies.

- **Public Awareness:** Educating users on safe investment practices, recognizing scams, and verifying platforms before transacting is equally vital.

3. The Road Ahead

The future of India's digital economy depends on how responsibly the country manages emerging technologies. To that end, trust and transparency will be key to progress.

CoinSwitch believes that India can set a global benchmark for a safe, inclusive, and innovation-friendly crypto ecosystem.

RESOURCES & KEY INVESTIGATION TOOLS

Investigating crypto-related crimes requires specialized tools and methodologies that allow enforcement agencies to trace, analyze, and link transactions on the blockchain. This chapter highlights key tools, their functions, and how Indian and global agencies use them to investigate crypto frauds, money laundering, and cybercrime.

1. Blockchain Analysis Tools

These tools allow investigators to trace transactions, identify wallet patterns, and link blockchain activity to real-world identities or exchanges.

a. Chainalysis Reactor (Paid Tool)

Used globally by enforcement bodies like the FBI, Interpol, and India's Directorate of Enforcement (ED).

Function: Visual mapping of crypto transactions, identification of illicit wallets linked to darknet, integration with exchanges on KYC databases to identify real users.

https://www.chainalysis.com/solution/crypto-investigations/

Arkham Intel (Free Tool) https://intel.arkm.com/

b. TRM Labs (Paid Tool)

Risk assessment and compliance monitoring for exchanges and banks.

Function: Real-time monitoring of suspicious wallet activity, traces funds across blockchain, alerts on wallets associated with sanctioned entities or terror financing.

https://www.trmlabs.com/

c. Elliptic Navigator

Blockchain analytics platform used by financial institutions and regulators.

Function: Transaction risk scoring, identifying links between wallets, exchanges, and darknet entities.

https://www.elliptic.co/

d. Etherscan (Free Tool)

Checks Ethereum wallet transactions, contract activity, and token transfers.

https://etherscan.io/

e. Tronscan (Free Tool)

Displays transactions and wallet data on the Tron network.

https://tronscan.org/#/

f. Blockchair.com (Free Tool)

The Explorer is an open source block explorer providing detailed blockchain data.

https://blockchair.com/

2. OSINT (Open Source Intelligence) Tools

Open-source tools help investigators gather publicly available data from social media, forums, or blockchain explorers.

a. VirusTotal (free)

Search files, URLs, and IPs for reuse in scams; submissions show related metadata.

https://www.virustotal.com/

b. Maltego Community Edition

limited free edition for link analysis and visual mapping.

https://www.maltego.com/use-for-free/

c. SpiderFoot (CE)

automated OSINT collection across domains, IPs, emails, social profiles.

https://github.com/smicallef/spiderfoot

d. OSINT Framework (website)

curated directory of OSINT resources and search techniques.

https://osintframework.com/

e. Whois (command line) / free Whois lookups

domain owner lookups (useful with DNS history services).

f. Shodan (free account) and Censys (free)

discover internet-exposed assets (useful for phishing infrastructure).

https://www.shodan.io/

3. Dark Web & Cyber Forensics Tools

Many crypto scams are coordinated on dark web forums or through phishing campaigns. Specialized tools help law enforcement trace digital footprints and extract wallet evidence.

a. Cellebrite & Oxygen Forensics

› Purpose: Mobile and device forensics tools that can extract data from confiscated smartphones or laptops.

› Functions:

- Recover private keys, seed phrases, and wallet backups.
- Identify crypto exchange apps and transaction history.

› Example: Used by the Delhi Cyber Cell in multiple cases involving hacked Binance and MetaMask accounts.

b. DarkOwl & CipherTrace Dark Web Intel

› Purpose: Monitor dark web activity for leaked crypto wallets, stolen NFTs, or ransomware payments.

› Function: Real-time alerts for investigators when suspect wallet addresses appear in dark web databases.

4. Indian Government & Legal Tools

a. CERT-In (Computer Emergency Response Team – India)

› Mandate: Investigates cyber incidents including those involving digital assets.

› Crypto Role: Coordinates with exchanges for data requests and traces crypto-linked phishing sites.

b. FIU-IND (Financial Intelligence Unit – India)

› Mandate: Collects and analyses information on suspicious financial transactions.

› Crypto Regulation:

- Registered over 47+ Virtual Asset Service Providers (VASPs) under PMLA as of 2025.
- Uses data analytics to identify unregistered exchanges or non-compliant wallet operators.

c. State Police Cyber Crime Units

- Maharashtra, Telangana, and Delhi have dedicated cyber labs for blockchain investigation training.
- Telangana Police's Cyber Forensics Division successfully traced a ₹6.4 crore crypto Ponzi scheme in 2024 using blockchain data.

5. Global Enforcement Frameworks and Cooperation

- Interpol & Europol Crypto Task Forces: Facilitate intelligence sharing on transnational crypto crimes.
- FATF (Financial Action Task Force): Sets global AML/CFT standards for Virtual Asset Service Providers (VASPs).
- Egmont Group: International body that connects FIUs across 160+ countries, including India, for cross-border crypto case coordination.

6. Practical Example – Tracing a Crypto Fraud

Case Example (Simplified):

1. A victim reports losing ₹5 lakh to a "crypto investment app."
2. Investigators obtain the wallet address where funds were sent.
3. Using Etherscan, they identify the transaction hash and destination wallet.
4. Chainalysis Reactor shows the wallet connected to a foreign exchange.
5. The exchange provides KYC data, leading to an arrest of the Indian operator running the scam.

GLOSSARY OF CRYPTO TERMS

Understanding crypto requires familiarity with a specialized vocabulary. This chapter provides a glossary of commonly used crypto terms, simplifying concepts for investigators, law enforcement, and legal professionals. Clear comprehension of these terms can aid in investigations, reporting, and regulatory compliance.

A

- Address: A unique string of characters used to send or receive crypto. Similar to a bank account number but for digital assets.
- Altcoin: Any crypto other than Bitcoin (e.g., Ethereum, Ripple).
- Airdrop: Distribution of free crypto tokens to multiple wallet addresses, often for promotional purposes.

B

- Blockchain: A decentralized digital ledger that records all crypto transactions in a secure, immutable manner.
- Bitcoin (BTC): The first and most widely recognized crypto, created in 2009.
- Block: A package of transaction data recorded on the blockchain.

C

- Cold Wallet / Cold Storage: Crypto stored offline to prevent hacking or unauthorized access.
- Cryptography: The practice of securing communication and data using codes, fundamental to blockchain and crypto security.
- Custodial Wallet: A wallet managed by a third-party service where the provider holds the private keys on behalf of users.

D

- Decentralization: Distribution of control from a central authority (like a bank) to a network of users.
- DEX (Decentralized Exchange): A platform that allows users to trade cryptos directly without intermediaries.
- DeFi (Decentralized Finance): A platform that allows to lend, borrow money using smart contracts

E

- ERC-20 Token: A standard for tokens built on the Ethereum blockchain. Many DeFi and crypto projects use this standard.
- Exchange: A platform where users can buy, sell, or trade cryptos. Examples: WazirX, CoinDCX, Binance.

F

- Fiat Currency: Government-issued currency like INR, USD, or EUR.
- FOMO / Fear of Missing Out: Market-driven behavior where investors buy crypto assets out of fear of missing profit opportunities.

H

- Hard Fork: A significant blockchain upgrade that is not backward-compatible, resulting in two separate chains. Example: Bitcoin Cash forked from Bitcoin in 2017.

I

- ICO (Initial Coin Offering): A fundraising method where new crypto projects sell tokens to early investors.
- Immutable Ledger: A ledger that cannot be altered once a transaction is confirmed, ensuring transparency.

K

- KYC (Know Your Customer): A regulatory requirement for exchanges and financial services to verify user identities to prevent fraud and money laundering.

M

- Mining: The process of validating blockchain transactions and adding them to the ledger, often rewarded with new crypto.
- Market Cap: The total value of a crypto, calculated by multiplying the price per coin by total circulating supply.

P

- Private Key: A secret alphanumeric key that grants access to a crypto wallet. Must be kept confidential.
- Public Ledger: A blockchain database visible to all users, ensuring transparency of transactions.

S

- Smart Contract: Self-executing contracts with terms coded directly into software on the blockchain.
- Stablecoin: A crypto pegged to a stable asset like the USD to reduce volatility.

Examples: USDT, USDC.

T

- Token: A digital asset created on an existing blockchain, representing value or utility within a specific ecosystem.
- Transaction Hash (TXID): A unique identifier assigned to each blockchain transaction for tracking purposes.

W

- Wallet: Software or hardware used to store, send, and receive crypto.
- Whitepaper: A detailed document issued by a crypto project explaining the technology, use case, and roadmap.

Credits

Editorial

Shivani Muthyala, Jayadevan P K

Design

Rajesh Subramanian

Contribution

Sukant Dukhande

Om Prakash Pandey

Venkatesh Ramakrishna

Mathang Seshagiri

Monya