ACL
ALLIANCE CENTRE FOR CORPORATE AND COMMERCIAL LAW

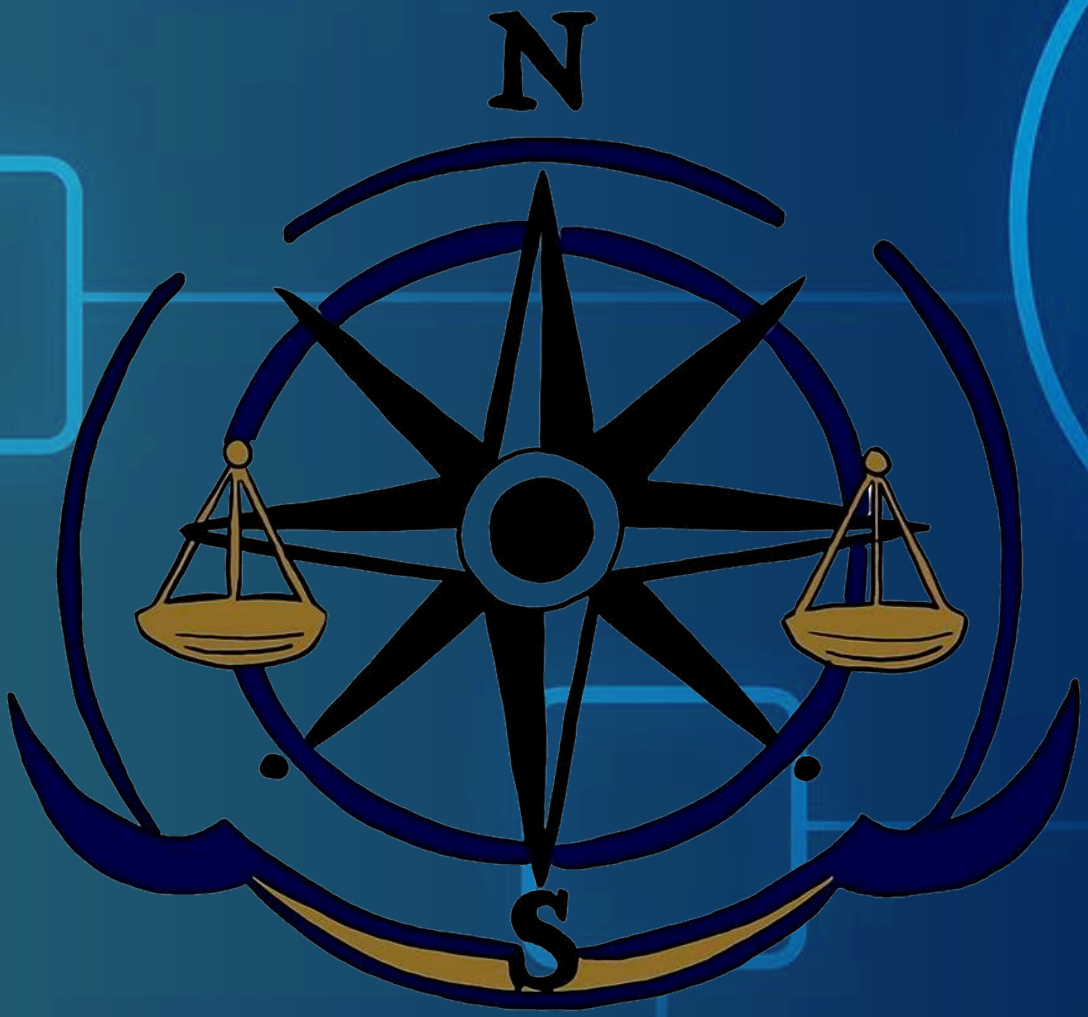
ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

Celebrating 25 SILVER JUBILEE years of Alliance Education

Alliance Centre for Corporate and Commercial Law (ACCL)

NEWSLETTER

VOLUME - IV ISSUE - 1 APRIL 2025



THE CORPORATE COMPASS

Navigating the Future of Corporate Law

Crypto, Compliance & Cashless Futures – The Law Behind the Ledger

EDITORIAL NOTE

We are pleased to present this edition of the Corporate Compass, the official newsletter of the Alliance Centre for Corporate and Commercial Laws. As members of the Faculty Editorial Board, it gives us great pride to witness how this platform has grown into a meaningful space for critical thought and informed dialogue in corporate and commercial law.

This edition reflects the collaborative spirit and intellectual rigour that define our Centre. From insightful articles to timely legal updates, each contribution has been carefully curated to ensure relevance, depth, and academic integrity We extend our sincere appreciation to the student editorial team, contributors, and all those who have supported this endeavour. We hope that the Corporate Compass continues to serve as a guiding resource for students, academicians, and professionals alike.

Warm regards,
Faculty Editorial Board
Alliance Centre for Corporate and Commercial Laws

ACKNOWLEDGEMENTS

Chief Patron

Mr. Abhay G. Chebbi
Pro - Chancellor
Alliance University, Bengaluru

Patron

Dr. B. Priestly Shan
Vice - Chancellor
Alliance University, Bengaluru

EDITOR IN CHIEF

Dr. V. Shyam Kishore
Dean, Alliance School of Law,
Associate Dean (Academic Affairs),
Alliance University, Bengaluru

GUEST EDITOR

Ms. Kiran Patel
Associate, Fox Mandal &
Associates LLP, Bengaluru

FACULTY EDITORS

- Dr. Sujith Surendran P, Professor ASOL
- Dr. Gyanashree Dutta, Assistant Professor ASOL
- Dr. T Jayashree, Associate Professor ASOL
- Mr. Shashank Kumar, Assistant Professor ASOL
- Mr. Rahul Shaw, Assistant Professor ASOL
- Mr. Nikhil A S, Assistant Professor ASOL

STUDENT EDITORS

- Mr. Naveen S M, Convener & Chief ACCL & LEGAL EAGLES CLUB
- Ms. Rapaka Himabindu, Joint - Convener & Deputy Chief ACCL & LEGAL EAGLES CLUB
- Ms. Geethika Katakam, Co-Convener ACCL
- Ms. Nawvi K, Joint - Convener ACCL
- Mr. Yohan S Menen, Joint - Convener ACCL
- Ms. Anoushka Uthaiah, Member ACCL
- Mr. Abhai Sreekumar CA, Research Scholar ASOL
- Ms. Saritha P, Research Scholar ASOL

STUDENT CO-EDITORS

Mr. Jishnu Venkataraman, Mr. Kamal Vibhash Reddy, Ms.Ritisha Sidenur, Mr. Rishiraj Nalte, Mr.Vishnu Gopakumar, Ms. Vrinda Saxena, Ms. Priti Pragyan Pradhan, Ms. Shivani, Ms. Pilla Navya, Ms. Varsha, Ms. Aashna, Ms. Khwaish, Ms. Aastha Jha, Ms. Jaya Mahaty, Mr. Advay, Mr.Agney, Ms. B Dhanusri, Mr. Bhuvaneshwaran, Ms. Nathania Do Rego, Ms. Rania Rifaya, Mr.Siddesh Munghate, Mr. Aziz, Mr. Kishanth.

Table of Contents

CURRENT Affairs–India

1. SEBI Redefines the Investor Experience: ASBA for Secondary Markets

In a bold step towards empowering investors, SEBI has brought about a revolutionary ASBA-like facility in secondary markets. Funds will no longer be shifted pre-trade; instead, investors have control until trades are settled.

Why it matters:

a. It enhances investor confidence through reduced settlement risks.

b. It's a bold nod towards greater financial discipline across the secondary markets.

RBI Tightens the Noose on Digital Lenders

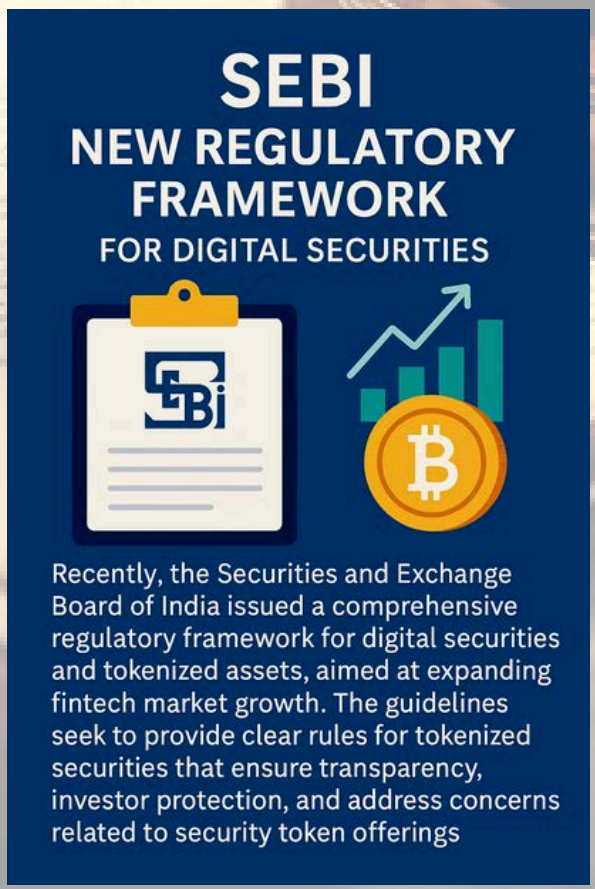
The Reserve Bank of India, in keeping with its larger mission of safeguarding financial dignity, has expanded the ambit of its Digital Lending Guidelines.

This time, it embraces the fast-growing Buy Now Pay Later (BNPL) models, leaving no grey zones untouched.

Why it matters:

a. Clearer guidelines mean reduced consumer exploitation risks.

b. Fintech players now must walk a path of much more regulatory seriousness.



GST Council Lowers the Bar: New E-Invoicing Rules

In what is being referred to by many as a "compliance revolution," the GST Council has made it mandatory that companies with an annual turnover exceeding ₹5 Crore must now issue e-invoices for all B2B transactions from August 1, 2025.

Why it matters:

a. Even small and mid-sized companies must digitize their billing processes now.

b. Tax compliance and real-time reporting of data will be the new standard.

2. Landmark Judgments Redrawing the Business Landscape-

(Supreme Court Delineates a Clear Line on IBC Valuations)

Case: Essar Projects Ltd. v. Edelweiss Asset Reconstruction Co.

In a well reasoned judgment, the Hon'ble Supreme Court has held that valuation issues under the Insolvency and Bankruptcy Code are beyond judicial review.

The CoC's "commercial acumen," the Court stated, should be respected and maintained.

Why it matters:

a. It shields bankruptcy proceedings from perpetual litigation.

b. It provides investors and resolution applicants with renewed faith in India's insolvency system

(Delhi High Court Issues a Warning to Aggregators)

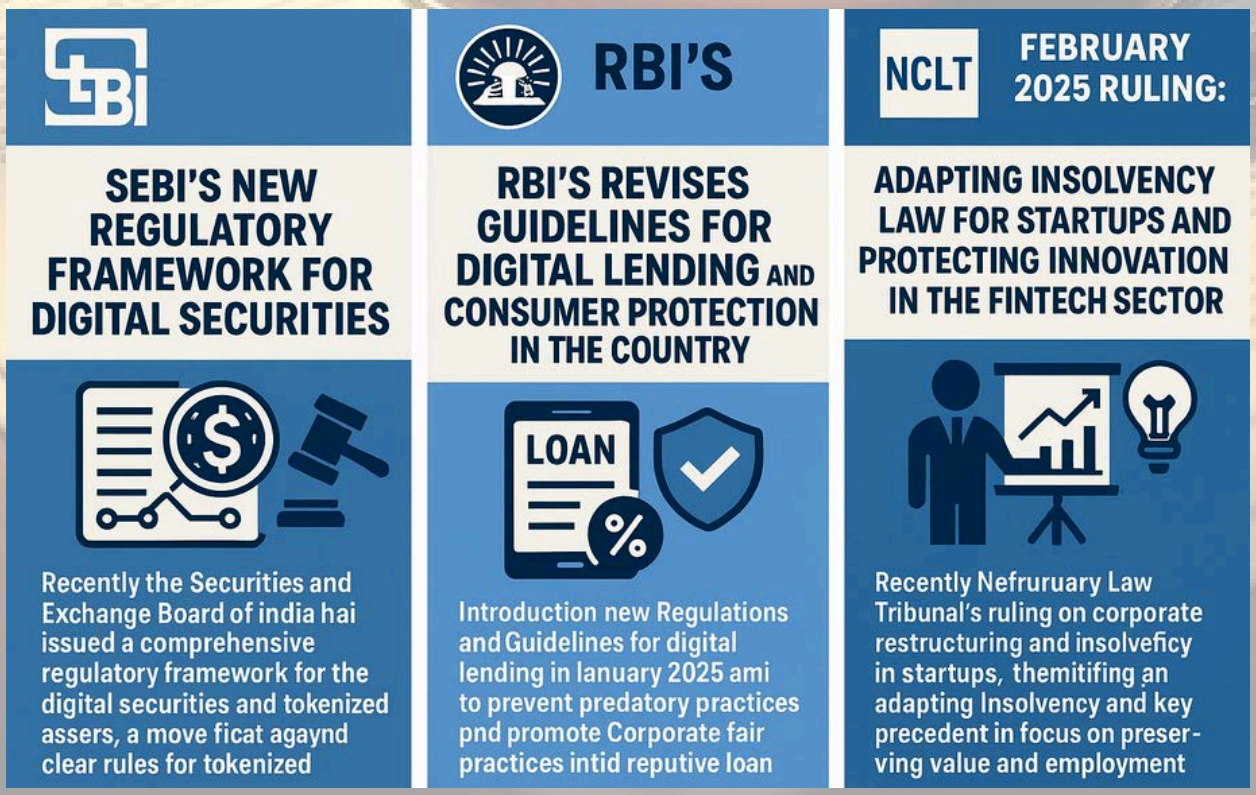
Case: UrbanClap Technologies v. State of Maharashtra

The Delhi High Court, in a pithy and sophisticated ruling, cautioned start-ups that calling themselves mere "aggregators" will not keep exempt them from consumer liability.

Why it matters:

a. Service providers will have to own up fully, no excuses.

b. Customer-friendly contracts and grievance redressal will no longer be discretionary — they will be a matter of survival



3. Government's Policies on Digital Finance & Cryptocurrency: Winds of Change

Digital India Act: A Manifesto for the Future

The government has initiated a public consultation process for with its Digital India Act (DIA) draft.

This isn't a superficial cosmetic makeover — it's a far-reaching redo of India's digital economy.

Highlights:

a. Comprehensive grievance redressal within 72 hours.

b. Unconditional transparency of algorithms and AI-based systems.

c. Strong digital rights and privacy frameworks for consumers.

Why it matters:

For tech majors, fintech, and startups, compliance will no longer be a choice — it will be reputational oxygen.

Cryptocurrency: The Road to Regulation Begins

Following years of diplomatic caution, the Government has finally recognized crypto assets as a separate asset class, not as currencies.

A Crypto Regulatory Authority (CRA) is on the cards, promising much-needed structure and clarity.

Why it matters:

a. Startups that are constructing in blockchain, DeFi, and NFTs should gear up for licensed operations.

b. Taxing structures and disclosure standards will become sharper, and more transparent

The Changing Face of Corporate Law, Crypto, and Compliance

International Corporate Law: A year of strategic recalibration.

a. The UK's Economic Crime and Corporate Transparency Act 2023 is more than a quietly progressing piece of legislation for Parliament. It is a signpost for something greater: an actual wake-up call for corporate governance.

b. Making directors disclose their identities and extending corporate criminal liability — these are not merely adjustments. They are a sign that the corporate culture is being steered towards more transparency and accountability, at a time when trust in the public has become increasingly fragile (UK Government Legislation Website).

c. At the same time, London is shaking off old habits. With the launch of the new prospectus regime, companies can now raise capital without navigating a complex web of paperwork. By simplifying disclosures and going digital-first, the UK is placing a bold bet on entrepreneurial energy over bureaucratic inertia (Womble Bond Dickinson).

d. And then there is PISCES — a nearly poetic appellation for a trading platform — providing a new way for private firms to access investors. For expansion-stage companies shut out of conventional venues, PISCES may be the catalyst they've been hoping for. It's not there yet, but that's true for much innovation.

Crypto, Digital Finance, and the New World Order

It's difficult to discuss 2025 without mentioning crypto — and regulators worldwide are no longer playing catch-up. They're making the rules, and they're establishing them quickly and decisively.

Global Regulatory Alignment Efforts:

a. The FATF is ratcheting up anti-money laundering compliance for crypto companies (FATF).[5]

b. The EU's MiCA regime — arguably the most ambitious crypto regulation to date — is

forcing players across Europe to finally play by one plain rulebook (World Finance Council).
c. Meanwhile, the UK, true to form, is trying to walk a tightrope: to encourage innovation without allowing the shady operators to slip through .
Regional Snapshots:
a. In the US, regulatory bodies are in a battle over who gets to call crypto a "security."
b. Throughout Asia, China's strong move towards the e-CNY contrasts with India's gradual experimentation.
c. The UAE is forging ahead, creating customized blockchain policies that have Silicon Valley taking notice .
d. And in Latin America, El Salvador continues to make its Bitcoin wager, while Brazil makes a quieter, structural blockchain revolution (World Finance Council).[7]

Cross-border crypto payments will hit $4.4 trillion by the end of the decade. That's not a footnote — it's the future of money in action.

a. Fintech, Compliance, and the Race Against Time In the EU, the AI Act has only just come into effect. Artificial intelligence is no longer a unregulated playground; for the first time, it is regulated industry ; it's a regulated industry now subject to actual sanctions for firms that misuse AI (World Finance Council).
b. It's not compliance — it's values. High-risk applications of AI must be informed by rigorous control of bias, transparency, and oversight. It's as if regulators are saying: if computers are to make decisions, shouldn't we at least make sure that they make fair decisions? [8]
c. While this is going on, Payment Services Directive 3 (PSD3) is keeping fintech on their toes. Tighter customer checks, bigger demands on transactions being transparent, and greater focus on safeguarding consumer data are in store. [9]

d. And then there is DeFi — the wild west. Formerly crypto's outlaw fringe, decentralized finance is slowly being pulled into the regulatory mainstream. It's a mess, a patchwork, and full of grey areas, but the trend is clear: DeFi will mature or will be pushed to the fringes. [10]

Final Thoughts: Accepting a Changing World

If there is one message in 2025, it's this: the good times are over. Compliance can no longer be an afterthought. Innovation must no longer outrun ethics. Those businesses that will survive this revolution will be those that discover how to adapt, not fight against change. Because in this new world, it's not about being faster or bigger. It's about being smarter. And wisdom, as ever, is born of knowledge of the rules — and precisely how to flex them without ever shattering them.

Let's Interview

Ashish Chandra

Chief Legal & Risk Officer at Junglee Games

Q1. You have previously spoken about Decentralized Autonomous Organizations (DAOs), covering all aspects, including character of DAO, regulations and its basic foundation. Could you please explain what DAO exactly is and how current regulations impact DAOs? Considering most of the audience lacks knowledge about what DAO exactly is.

A DAO is like a digital company that runs on the internet using blockchain technology. Instead of having a boss or a central office, it's controlled by its members i.e., people who own crypto tokens (like digital shares) and vote on decisions together. The rules of a DAO are written in computer code called "smart contracts" - usually over Ethereum blockchain. These are automatic and transparent, so no one can secretly change them. Think of it as a WhatsApp group of college students where everyone agrees on rules upfront, and a computer ensures those rules are followed without needing a leader.

DAOs use blockchain, a secure digital ledger, to record all decisions and transactions like a public, unchangeable notebook. Members propose ideas (e.g., how to spend money or start a project), and everyone with crypto tokens votes. These interactions usually happen over the traditional Web2.0 environment over websites. The smart contract executes the decision automatically if the vote passes, and such voting and automatic execution of the decision happens over the new Web3.0 environment.

For example, a DAO could be a group of students pooling money to fund a college participation in an international moot court competition. They vote on which legal issues to cover and who will represent the college, and the funds are automatically released to a pre-designated wallet of the contesting students only when 60% agree.

How Do Current Regulations Affect DAOs?

Most countries, including India, don't have specific laws for DAOs yet. This creates confusion viz., are DAOs companies, partnerships, or something else? On the liability side, if a DAO does something wrong (like breaking a contract), it's unclear who's responsible whether the members, the coders, or no one or all. This uncertainty makes people hesitant to join or invest.

DAOs usually deal with digital currencies / digital assets (like crypto). In India, laws on crypto are strict, and DAOs might need to follow rules for money laundering and taxes, which can be tricky to apply to a digital group with no office and no identified individual at the helm of the DAO, where participants are identified by their 64 alpha-numeric blockchain wallet address. Lastly, from a consumer protection standpoint, if someone loses money in a DAO (e.g., due to a hack), there's no clear law to protect them, unlike traditional companies.

Q2. DeFI platforms often operate without traditional intermediaries or clear jurisdictional oversight. From a legal standpoint, how do you see the enforcement of regulatory compliances evolving in this space and what challenges does that pose?

DeFi (Decentralized Finance) platforms, which offer crypto assets based financial services like staking, yield farming, lending or trading without regulated intermediaries like banks, stock exchanges or brokers, challenge traditional regulations due to their global, anonymous, and intermediary-free nature. DeFi, being run on smart contracts, is also not flexible to evolve ever changing regulatory landscape as the smart contracts can't be easily altered to meet new laws, and moreover, to make any such change, a majority of token holders need to vote for such alterations. For eg: think of a smart contract like a vending machine- once it's set up to dispense snacks for ₹20, you can't easily change it to charge ₹25 or add new snacks. But if you design the machine with a "settings panel" (like upgradable contracts or governance votes), you can update it without breaking the whole system. The challenge is making those updates fast and fair while keeping users' trust.

The Indian government has tightened rules under the PMLA and tax laws, requiring DeFi platforms to verify users (with KYC), monitor and report transactions.

To test the business models of DeFi, SEBI or RBI or IFCA may create "regulatory sandboxes" (like in Gift City) to test DeFi under controlled rules, balancing innovation and oversight.

Q3. Could NFTs become the new-age art collectibles—replacing traditional paintings in terms of prestige and value? And how is the legal system preparing to tackle issues like money laundering in the NFT trade?

NFTs are unique digital assets stored on a blockchain, like a digital certificate proving you own something (e.g., a piece of art, a video, or even your law degree). Unlike a painting, they exist online, not on a wall. NFTs - esp representing arts and entitlements - are valuable in a fully Web3 or Metaverse world. Bollywood celebrities sold their NFTs for crores of rupees, during the peak NFT euphoria in 2021. Younger generations value digital experiences (think gaming skins or Instagram filters). NFTs can include perks, like access to exclusive events or royalties for artists when the NFT is resold.

NFT buyers and sellers often use pseudonymous crypto wallets (e.g., "User123"), making it hard to trace who's trading, which can hide illegal funds. NFTs can sell for crores, making them attractive for laundering money e.g., NFTs' global nature lets someone in India buy from Dubai, complicating oversight, but India's PMLA and blockchain tracing help track such trades.

Indian law classifies NFTs as Virtual Digital Assets (VDAs), taxing NFT profits at 30% and requiring 1% TDS on transfers. Further, PMLA applies to crypto / NFT exchanges, requiring KYC verification. This helps track transactions. Law enforcement agencies in India are increasingly using tools to trace blockchain transactions, and are actively collaborating with their international counterparts to conduct thorough investigations.

Q4. What shift do you visualize in Indian Crypto policy in near future?

There was a prohibition from 2018 to 2020 on the RBI regulated entities e.g., banks, credit cards, etc. to provide services to the crypto transactions and crypto exchanges. After the Supreme Court quashed those restrictions, a second attempt was made in November 2021 - as per media reports - to bring in a crypto banning bill while acknowledging the benefit of public blockchains. However, this bill was never placed before the parliament. Since 2022, the government has been attempting to bring the virtual assets industry into the mainstream but with a cautious approach. It started with taxation, cyber security requirements and then PMLA compliance framework.

Under India's presidency of G20 Summit 2023, Indian leaders highlighted crypto assets as a new subject for social order, monetary, and financial stability and urged G20 leaders to establish global standards for its regulation. India emphasized that crypto assets, underpinned by blockchain, require international cooperation due to their borderless nature, which impacts terrorism financing, tax evasion, and financial stability.

Therefore, India is likely to adapt G20 recommendations to its unique context, balancing strict oversight while fostering innovation. Gift City's sandbox could test tax-friendly crypto models, fostering DAOs and NFTs while ensuring AML compliance, that could position India as a Web3 hub.

Q5. On linkedin you posted, and I quote "Tulips are not durable, not scarce, not programmable, not fungible, not verifiable, not divisible, and hard to transfer. This analogy has made us hodlers and not builders." What message were you aiming to convey?

Various key critiques of Bitcoin in the past have made frequent comparisons between Bitcoin and the Dutch Tulip Mania of the 1630s, where tulip bulbs became a speculative bubble and then crashed spectacularly.
These critics argued that Bitcoin is just another "bubble", like tulips and are based only on irrational speculation, with no inherent value. This wide-spread criticism has deterred the development of a favorable business and regulatory eco-system for crypto assets and blockchain in India.

For the believers of Bitcoin, it is not just a speculative "tulip flower", it has fundamental, durable technological properties, unlike the tulips. Thus, my statement claims that Bitcoin is a radical financial innovation, not a mere "speculative bubble". And, because of analogies like tulips, instead of building applications and innovations on Bitcoin, people have been reduced to passively holding (popularly called as HODL in the Web3.0 which means "Hold On for Dear Life" i.e. never sell) it for speculative gains which in my view is a missed opportunity to foster deeptech innovation in India.

Q6. If Bitcoin is to become the future of the money, how should it be taxed to ensure a sustainable government revenue?

The Supreme Court of India, in its landmark judgment in Internet and Mobile Association of India v. Reserve Bank of India (2020 SCC Online SC 275), delivered on March 4, 2020, addressed the classification of Bitcoin and other virtual currencies (VCs). The Supreme Court broadly classified VCs as (a) medium of exchange, (b) store of value, and (c) unit of account, while noting that VCs (including Bitcoin) are not "legal tenders".

The taxation of Bitcoin should reflect how the Bitcoin is being used by the tax assessee, and whether Bitcoin is considered as "money" or remains "money equivalent". Further, the tax policy should also reflect India's international competitiveness to attract and retain talents, entrepreneurs and large investors in the blockchain space.

The present tax structure supports dealing in Bitcoin as a "store of value" as potential long term appreciation of its price will not hurt the holder of Bitcoin to pay 30% tax. However, any short term decision by the holder of Bitcoin to sell it and later buy it - to manage the risk and return in a volatile market, will impact that tax outflow as any losses in Bitcoin trade will not be offset against any potential gains.

Q7. Do you believe Bitcoin has the potential to replace gold as the primary "store of value" in global trade?

In the recent global volatility seen due to tariff war, Bitcoin price dropped by approx 30% from its December 2024 peak however, Gold price has touched its lifetime high. Therefore, Gold is a clear winner over Bitcoin in this round of global trade volatility.

However, Bitcoin could potentially challenge (or, I would say co-exist with) gold as a store of value in global trade due to its digital ease, fixed 21-million-coin supply, and appeal to tech-savvy investors, unlike gold's physical bulk. In India, where gold is culturally vital (large holdings by households), Bitcoin's volatility, regulatory scrutiny, high taxes, and tech reliance limit its dominance. Gold's stability and RBI's backing ensure its edge.

Q8. What's your take on meme coins? How does Indian law currently view their legitimacy as a crypto asset, if at all?

Meme coins, such as Dogecoin and Shiba Inu, are crypto assets inspired by internet memes, pop culture, or social media trends, and are often created as jokes or community-driven projects. Unlike Bitcoin or Ethereum, which aim for utility in decentralized finance (DeFi) or smart contracts, meme coins typically lack intrinsic value or functionality, deriving worth from speculation, hype, and community sentiment.

Meme coins thrive on virality, often propelled by celebrity endorsements or social media buzz. Their volatility and lack of fundamentals make them akin to digital collectibles that are prone to pump-and-dump schemes.

Presently, tax laws and PMLA guidelines in India do not distinguish between a Stablecoin, Utility Coin or a Meme Coin.

With gratitude, we conclude this exchange

Right to Privacy in Digital Transactions

Anurima Biswas

One of the most treacherous data breaches that the world has seen is the infamously dubbed 'Mother of All Data Breaches'(MOAB) that floated to the surface in January 2024. The world saw a number that couldn't be fathomed, it was the breach of 26 billion records! This was the culmination of breaches that occurred anywhere between the period of 2007 and 2021. To notice, right when digital transactions was sitting down as the norm. This database carries with it over 3,800 folders, each holding data from individual data breach. What alarms is that within the list of breached entities were listed names of trusted brands. The list did not stop at Adobe, going further up to LinkedIn and ultimately Twitter/ X from where 28.1 crores of records were transgressed. These are one of the most popular platforms where information is shared and received and sensitive data is collected. But the company that shot up to the top of the charts with data breaches was Tencent, with an incredible figure of 150 crores of data breach incidents. The leak extended to records from government departments from countries like U.S.A, Turkey, Germany and Brazil among others.

This was a global breach. Speaking of the Indian Landscape, in early 2018, one of the largest 'Identity' databases in the world – Aadhaar was infiltrated by harmful actors. This breach disclosed data beyond that of 110 crore Indian citizens. The details included their name, photos, emails, addresses along with biometric data like fingerprints and iris scans. The cherry on top was that since this database was connected to UIDAI in the year 2009, it also contained data on bank accounts connected with distinctive 12-digit numbers, and with that Aadhaar Breach of Data became a credit breach too.

Statistics have shown that the annual average toll of cybercrime is forecasted to reach more than 23 trillion US dollars in 2027, and increase from 8.4 trillion US dollars in 2022, in line with data mentioned by Anne Neuberger, U.S. Deputy National Security Advisor for Cyber and Emerging Technologies, in 2023. Over FY24, India's average data breach damage hit an all-time high of Rupees 19.5 crore, a 7% up from the preceding year, as per an IBM report2. This is where the question arises — Is our financial privacy buried six-feet down in the age of digital transactions?

Digital transactions are explained as transactions where the customer authorizes the transfer of money online that is by using electronic means, and the money/funds are transferred directly from one account to the other. These accounts are held with banks or entities/ providers. They are done by way of cards, net banking, mobile apps and wallets, National Electronic Fund Transfer (NEFT), Immediate Payment Service (IMPS), pre-paid instruments etc.

With the world leaning increasingly towards digital transactions, privacy stands as the most vulnerable and eroding hook. On the Global frontier, the European Union's General Data Protection Regulation (GDPR) has robust methods to deal with data breaches and ensuring maximum privacy. It is done through making comprehensive rules for collecting, storing and managing personal data, also further granting individual rights like access, rectification and erasure rights. Lastly, it also imposes obligations on the organizations to be fair, ensure transparency in all actions and being accountable. The GDPR also works on data minimization that is collecting only important data. We also have California Consumer Privacy Act (CCPA) of 2018 where under this Act, the consumers are given more control over the personal information that corporates and businesses collect and the CCPA guidelines gives rules for the implementation of the act. The act secures present-day privacy rights like Right to Know, Delete, Non-Discrimination and Opting-Out. This was further improved and from 2023 two more rights were added called, 'right to limit' and 'right to correct'. One of the most used privacy framework is the OECD Privacy Principles which is part of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Globally these Laws have proved to be effective in ensuring privacy of its consumers and handle responsibilities in an incident like data breach. In the Indian Landscape however, privacy got the recognition of fundamental right under the ambit and spirit of Article 21 only in 2017 through the landmark case on privacy of Justice K. S. Puttaswamy v. Union Of India. Herein, the Hon'ble Apex Court pronounced thus, 'Right to Privacy' is part and parcel of Articles 14, 19, and 21 and included within the list of fundamental rights.
While the Data Privacy Acts are not as comprehensive as the GDPR, India does have the Information Technology Act, 2000, and RBI guidelines on cybersecurity to protect against data leaks and the exposure of sensitive information. India in 2023, also came up with the Digital Personal Data Protection Act, 2023 (DPDP Act) with the objective of regulating and processing digital personal data in a manner that individual rights of privacy are not compromised. In China, we have Personal Information Protection Law and in the U.S.A we have the Gramm-Leach-Bliley Act, that ensures and regulates privacy in digital transactions.

Though legislative acts safeguard privacy, the true test lies in whether these measures to protect hold firm when governments and corporations possess the power of surveillance. Under the Indian Telegraph Act, 1885, the government is allowed surveillance of data only in two exceptional circumstances that is any 'public emergency' and 'public safety'.

Under The Indian Post Office Act, 1898, government surveillance is allowed though in restricted capacity but nevertheless there. Under The IT Act, 2000, the government is given the power to issue directions in cases of [monitoring, decryption, and interception of any information transmitted, received or stored through a computer resource.] Surveillance is given for in cases of criminal acts in India but when an individual merely wants to use a cashless service to effect the transfer of money, do they also acknowledge and permit leak of the data collected through surveillance? Both the corporate and government should take definitive measures to address security and privacy concerns because if not the threat to individual rights is apparent. India is a signatory to the UDHR 1948 declaration (Article 12) and International Convention on Civil and Political Rights (Article 17), whereby both recognizes privacy as a fundamental rights. Though part of these conventions India does not have suitable legislation to guarantee privacy.

Now, how do we keep private in the steadily growing world of digitalization? To protect our data and privacy and both in the online and electronic medium? One of the leading digital payments platforms in India, Paytm, on 20th of August in 2020 battled a significant breach in cybersecurity which compromised records of tens of lakhs of users. The platform was invaded into and the Hackers secured unauthorized gateway to Paytm Mall's database leading to evident concerns about privacy and security of digital transactions in India. Paytm later successfully bounced back from financial losses and gained trust through its robust policies at this critical juncture.

The fear of losing privacy over financial data is worth losing sleep over. More so when, data is shared with Third-Parties. This process is called "open banking" and the global movement is termed as "open financial data". Is it an innovation in digital transactions or only means of data leaks is the argument. The significant risks it poses more than the effectiveness of transactions and handling online banking is the competency risks, data breach and data control. When the 2nd part is requested services the intervention of 3rd party affects the quality of data. Further, data breach of the 3rd party affects not the 3rd party alone but every account associated with it. Third party vendors swim in an ocean of data because they gather data from multiple sources and hence the foremost peril is that of data breach.

The modern-day mode of transactions has been eased with the use of Cryptocurrencies. Though not widely used to replace cash, it is widely used as a form of currency in the trade and investment market. Therefore taking privacy in the context of Cryptocurrencies becomes essential.

Cryptocurrencies works to promote privacy from the very nature it is designed in the context of technology because it combines secure encryption protocols, decentralised storage systems and user-managed access permissions. The characteristics of these currencies are, decentralization, immutability, cryptographic security, and transparency with control. Firstly Cryptocurrencies are made with blockchain technology and privacy is made possible through its anonymization procedures, employing cryptographic methods containing hashing in addition to public-private key pairs which makes such secured and protected data that unauthorized access is nearly impossible. Through its decentralised identity management feature one need not reveal any information beyond their age. However, no technology is free from limitations for example in Cryptocurrencies because of their immovable blockchain ledger difficulties arise in fulfilling 'right to be forgotten' conditions as under GDPR guidelines. To further protect Privacy Cryptocurrencies have Anonymity- Enhanced Coins (AECs) called Privacy Coins. These make the transaction details opaque through cryptographic techniques as the flow of money itself is concealed. Crypto Trading and Privacy go hand in hand as the technology leaves no trace of where the money is transferred.

From this is the shift of dilemma between privacy and compliance. How does privacy work with Anti-Money Laundering Regulations and how for financial institutions, being one step ahead of money laundering and menaces requires walking through a comprehensive set of international and domestic guidelines and regulations while taking advantage of technology to adjust to emerging risks. Fintechs are challenged through regulatory compliance adherence whereby these companies must stick to an expanse of banking regulations, data privacy laws among others. Keeping up the compliance is made necessary as even if hackers won't attack or get unauthorized access but merely the non-adherence with the requirements with levy heavy penalties if a breach occurs due to this non-compliance. In the guidelines issued by RBI under KYC in February 2005, has become benchmark for international standards. These guidelines give for privacy while taking KYC for opening an account. Having made comments on this, the remaining leg is to address the gaps and loopholes, and outline the way forward.

India as mentioned above did not have robust laws on data privacy until recently. In 2019, DPDP bill was tabled. This was the first instance of data protection laws to call for stricter guidelines to collect, process and store data. The act was released in 2023, however India still walks behind the GDPR laws of the European Union. This gap should be bridged through stronger and detailed laws and regulations while imposing responsibilities upon the culprit.

Lastly, here are some high-tech methods and technologies that will reshape the future of digital transactions and privacy in the upcoming years. The Homomorphic encryption algorithm method which is designed to permit execution of mathematical computations encrypted datasets. Next are the Wallets! Two of which are the Samourai Wallet and the Wasabi Wallet. Samourai Wallet is the Bitcoin-only wallet intended to sequence user privacy. Features of this wallet involves Stealth Mode that is hiding wallet from device screens and apps plus makes the sender's and receiver's identity anonymous. This can be a great leap in ensuring privacy over anything. Further one of its features also includes using new bitcoin address for every transaction. Next is the Wasabi wallet which is also a privacy focused Bitcoin wallet and uses breakthrough cryptographic techniques to make the transactions anonymous. It obscures transaction history.

There are also introduced new privacy layers in Decentralized Finance (DeFi) and Web3. Them being Zero-Knowledge Proofs (ZKPs) which is a privacy layer. This is a cryptographic method used to prove information about a piece of data, without showing the data itself. Other privacy layers include, Tornado Cash, Aztec Protocol, Secret Network, Railgun, Orchid Protocol, Manta Network, Panther Protocol, Firo (formerly Zcoin), and Oasis Network. There are also upcoming innovations in Central Bank Digital Currencies (CBDCs) that promise privacy. Therefore, the right to privacy in digital transactions follows follows advanced rules and directives and the commitment to improved technologies to privatize and prioritize privacy gives for and upholds right to privacy.

Article Written by:

Anurima Biswas- B.A. LL.B. (Hons.)

4th SEMESTER, 2023-2028.

Insufficient Legal and Regulatory Framework for ICO and Hard Fork Fraud in India

Bhoomika Suthar

"There Are Three Era Of Currency: Commodity Based, Politically Based And Now, Math Based" by Cris Dixon. We get our Currency from the Central Government and RBI issues it, while Crypto currency is not a type that can be used by the people in this real world, it is used to do transaction in the Digital World. Crypto currency in India has evolved significantly over the last decade, with ICOs and hard Fork emerging as popular trends. What started out as a digital currency experiment on the digital market in 2009 by Satoshi Nakamoto4 has developed into an innovative and rising ecosystem. Bit coin was the first to use block chain technology, which requires an unchangeable and transparent record system that permits transactions between individuals without the involvement of banks or other authorities. This concept as how we view money, and how it created a completely new method of doing any kind of online transaction.

Ethereum was introduced by Vitalik Buterin in 2015, following the creation of Bit coin. While Bit coin was created as a means of commerce and value storage, Ethereum introduced the idea of smart contracts—digital agreements that are directly programmed into the block chain.

This made it possible for decentralized apps to be developed, increasing the block chain's usefulness. This led to the creation. of initial coin offerings (ICOs),6 which will be further be explained below in a detailed way, is a way for developers to generate money for block chain projects by exchanging digital tokens for well-known crypto currencies like Bit coin or Ether. The phenomenon of hard forks emerged as block chain networks evolved. A hard fork happens when modifications to a block chain protocol cause the network to permanently diverge, givingrise to a new crypto currency version. As an example, this was seen in the split between Ethereum and Ethereum Classic, or between Bit coin and Bit coin Cash. Hard forks sometimes cause legal and financial uncertainties, especially for inexperienced investors, even though they may be motivated by technical advancements or ideological disagreements within a community.

Whereas an ICO serves as a platform for startups to obtain funding by issuing digital tokens, a hard fork refers to blockchain split that results in the creation of new cryptocurrencies. Despite their unique appeal, the emergence of these systems has coincided with a huge increase in fraud, scams, and other illegal activities, resulting in significant financial losses for investors When it comes to India, where cryptocurrency legislation is still in its early stages, concerns regarding the country's legal and regulatory structure remain.The paper studies the lack of adequate and regulatory structure in India to address the difficulties posed by ICO and hard fork frauds, focusing on the necessity for a complete

framework to safeguard investors and maintain transparency in the crypto currency ecosystem.

Understanding ICO And Hard Forks

Before we go further, it is crucial to understand ICO and hard fork.

Initial Coin Offerings (ICOs) are everywhere now look left, Right, Straight and then cross the road, where you look you will find a prospect of ICO there. It is a type of crowd funding in which a new coin is sold to investors seeking to invest. Does it make similar to an IPO? NO! As, IPO gives investors ownership in a company through shares, an ICO offers digital tokens with future value often without regulatory safeguards. The major purpose is to collect funding for the development of projects, which are generally blockchain-based applications. ICO allows enterprises to sidestep traditional venture capital fundraising, allowing investors the opportunity to purchase tokens that may later be sold for other crypto currencies. However, the lack of regulation around ICOs has led to numerous cases of fraud, with scammers misrepresenting their projects and stealing funds from unsuspecting. There is no clear rules on people running ICOs are genuine. As per the Reports more than 80% of the ICOs in 2017 were scams.

What is a Block chain? It refers to digital ledger which stores, connect the information and verifies whether the information is genuine using the blocks which are generated from the computers. One of the famous use of block chain is bit coin.

Hard Forks occurs when a block chain's protocol undergoes a significant change, resulting in a split in the block chain. Think of it like a road path that suddenly split into two paths and people and choose which to follow. One path continues the old rules, while the other follows new rules. Both share same history till the point where they split, they became different crypto currencies after that. The new version of the blockchain operates according to a different set of rules, creating a new cryptocurrency. Hard forks are often contentious and can lead to market confusion, especially if the fork occurs without sufficient transparency or communication from the original project developers. While hard forks themselves are not inherently fraudulent, they can be used as a tool for misleading investors, especially if the developers of the original project abandon or mismanage the new block chain. Hard forks happens to fix a bug, security flaws in system, to improve features or speed. Bitcoin cash was created from a hard fork of bit coin in 2017 due to a disagreement between the communities on handling the transactions. The ethereum classic was created from the hard fork of ethereum in 2016 after a major hack.

Regulatory Gaps in India's Legal Framework

In March 2020, the Supreme Court overturned the banking ban that the RBI had first placed on crypto currency-related businesses in 2018. This was a major win for the crypto currency community. Since then, there has been a demand for more precise laws to safeguard investors and promote creativity. However, the legal foundation for ICO has not yet been established.

When it comes to India, there are no particular rules that regulate it. Since there is little protection for ICO initiatives, it is challenging to handle concerns like responsibility, transparency, and investor protection. Additionally, given the absence of a clear structure, ICO fraud is thriving as project creators ignore venture disclosures. Although there has been progress in developing tax regulations for crypto currencies, it is still unclear how tokens created with ICOs would be taxed. Although the Indian Income Tax Department has released recommendations for the taxation of crypto currency, several concerns, such as the taxation of tokens created through ICOs and hard forks, are not entirely addressed by these rules. Investors find it challenging to comprehend their tax responsibilities due to the absence of laws, which may result in legal problems.

Indian investors are left without any defence against crypto currency frauds and scams in the absence of governmental oversight. Scammers can simply start an initial coin offering (ICO) to commit fraud, and as there is no investor protection, investors are at risk of suffering significant financial losses. Investor uncertainty can also result from hard forks because stakeholders might not understand the ramifications of a fork or might lose access to their assets as a result of subpar project team management or miscommunication.

Crypto currency as a legal grey area in India

Crypto currency remains a murky issue in India even after the Supreme Court's decision to overturn the RBI banking ban. Digital assets are not classified as securities or legal tenders, which causes ambiguity for both businesses and investors. A safe environment for Initial coin offerings (ICOs) and hard forks is hampered by the ambiguity surrounding the status of crypto currencies. Nevertheless, the hard forks and ICOs frameworks has not yet been created.

Key Challenges Associated with ICO and Hard Fork Fraud:

One Coin is a prime example of an ICO scam that duped Indian investors as well as many others throughout the world. The fraudsters created phony initial coin offerings (ICOs) that promised larger returns on investments before vanishing with the money they had gathered. These deceptive schemes frequently lack transparency, which makes it challenging for investors to assess a project's credibility. The reason for all of this is that this ICOs is not governed by any regulatory framework. When we discuss hard forks, it might result in disputes between investors and developers, particularly if the fork creates new coins without adequate notification. The initial project may occasionally be abandoned by the developers, leaving the investors with assets that are mishandled and of little value. Investors have limited options for recovering money or resolving conflicts in the absence of adequate regulation. Additionally, because different exchanges may handle the distribution of fork tokens differently, they cause confusion surrounding token ownership.

The Pump and Dump schemes, where the price of a crypto currency token is inflated through coordinated efforts, which can only be sold when there is profit unsuspecting the investors has entered the market and this creates a unstable market where the investors are left holding worthless assets with them, after the prices of those assets have been crashed.

The 2016 Ethereum DAO hack is a classic example of the dangers of this technology. Using Ethereum, Dao is a crowd funded project that aims to raise $150 billion. But because of the loophole, the hacker was able to take 60 billion ether. It resulted in a contentious problem. Unfortunately, the community's plan to reverse the block chain and recover the victims' assets was unsuccessful. The block chain's history is known as Ethereum Classic.

Icos and hard forks are frequently vulnerable to security flaws, such as phishing and hacking attempts by scam artists. Because project developers have less incentive to put security measures in place in the absence of governmental monitoring, investors are more vulnerable to cyber-attacks.

The Need for a Comprehensive Legal and Regulatory Framework

India must establish particular legislation to control their behaviour and identify the ICO as a type of fundraising. This entails mandating that the ICO projects register with the regulatory body, reveal all pertinent project details, and even go through a vetting procedure that guarantees accountability and openness. This should be accompanied by the implementation of required disclosure and the creation of accounts for funds raised.

Laws protecting investors should be implemented to prevent fraud and scams. This might mean the creation of a regulatory agency charged with monitoring crypto currency operations generally and a dispute resolution procedure. They may even be investor education programs designed to raise awareness of the dangers of hard forks and ICOs.

Since tax laws are crucial to every corporate operation, the government should give ICOs and hard forks thorough tax rules. Issues like capital gains taxes on crypto currency profits,26 taxation of tokens created through ICOs, and tax treatment of hard forks should all be covered by these rules. These unambiguous tax laws would reduce legal ambiguities and give entrepreneurs and investors certainty.

When it comes to hard forks, investors should be made aware of the implications and the treatment of their assets. To safeguard investors' money, developers should make sure that security measures are in place and communicate openly with all parties involved. India should establish cyber security guidelines for crypto currency projects in order to lower the danger of hacking and cyber-attacks. This would assist in motivating developers to implement security measures for their platforms and safeguard investors from cybercrime.

Conclusion

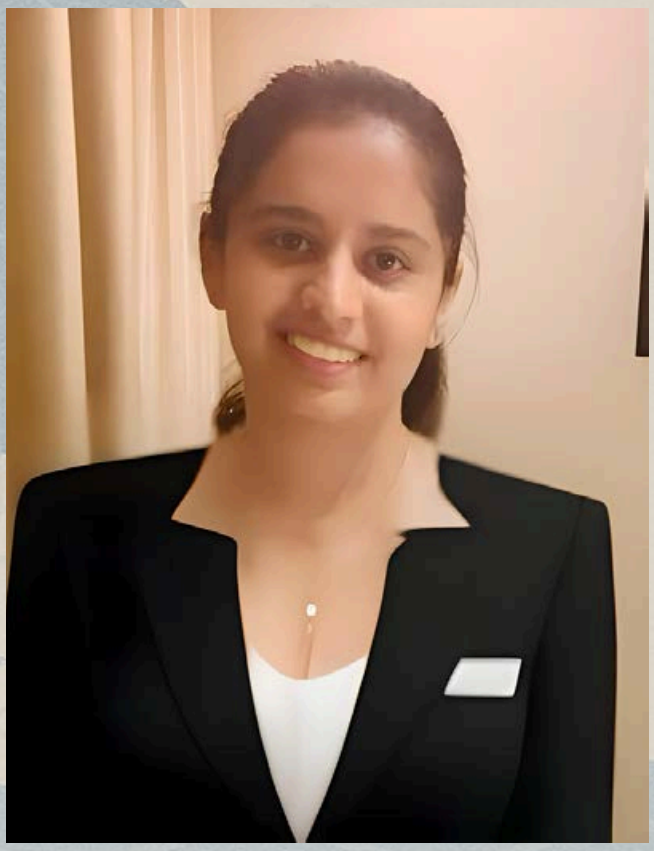
ICO and Bitcoin are the Next big thing in this demanding era, we do agree there are no or less regulatory framework, which controls the functioning of this digital currencies, which makes it easier and make them available to the world. Unlike, the other currencies where regulatory bodies govern them, but here we are the owners. But every new thing brings some fears here as well. The lack of Regulations for them, makes it difficult for the investors dealing in it. Some countries like South Korea and china has banned ICO, while some are attempting to regulate it. Since Bitcoin introduced block chain technology to the world, crypto currency has advanced significantly. New ideas like as hard forks and initial coin offerings (ICOs) gained popularity as digital currencies like Bit coin and Ethereum expanded. While hard forks allowed for the creation of new coins and improvements, and initial coin offerings (ICOs) gave entrepreneurs the opportunity to acquire capital without the help of traditional banks, they also carried significant dangers. Because there are currently no clear rules pertaining to crypto currencies in India, many investors have been duped and defrauded.

India requires strict and unambiguous regulations to regulate cryptocurrency use, safeguard investors, and stop fraud in order to proceed securely. India can embrace the advantages of cryptocurrency while avoiding its risks with the right legal framework, improved security, and increased public knowledge. Innovation should be promoted, but not at the expense of investor confidence and safety.

Article written by:

Bhoomika Suthar- B.B.A. LL.B. (Hons.)

6th SEMESTER, 2022-2027.



Anti-Money Laundering And Know-Your-Customer Crypto Transactions

Dondapati Naga Siva Durgaprasad

The introduction of cryptocurrencies fundamentally changed the very idea of currency, expanding and redefining the international financial landscape, and has gained popularity among individuals, investors, and businesses. Because of the launch of cryptocurrency on January 3, 2009, in the past 15 years, there has been a high rise in high-profile financial crimes. The very anonymity, privacy, easy borderless transfers, absence of central authority oversight, and decentralized nature of cryptocurrency transactions have rendered them especially susceptible to money laundering and other illegal practices. A fully undeveloped regulatory structure on cryptocurrencies has been opening loopholes for financial criminals to take advantage of this emerging market. Weak Anti-Money Laundering (AML) guidelines and regulations in some countries have allowed the perpetrators to use the anonymity and distributed nature of cryptocurrencies to commit criminal activities. Securities and Exchange Commission v. Ripple Labs Inc,The SEC accused Ripple of its sale of XRP as an unregistered securities offering. The matter presented significant crypto regulatory issues, highlighting openness and legal token dissemination. If this continues, the crypto market will see an escalation in money laundering and financing to terrorists, which is harmful to state sovereignty, bribery, fraudulent activities, and numerous other financial crimes., AML and Know Your Customer (KYC) regulations are very important in protecting the cryptocurrency market from misuse in a view to prevent money laundering, terrorism financing, and also from fraud. They are ensuring user identity verification and helping to identify illicit fund flows. These types of measures build investor trust, support market legitimacy, and promote long-term stability. As the digital economy grows, balancing innovation with effective oversight and effort to fight against illicit activities, the regulatory authorities, including governments, financial institutions, and law enforcement agencies, are required to have mandatory “Anti Money Laundering (AML) and Know Your Customer (KYC) policies in place.

This article is intended to determine the importance of AML and KYC policies and their function in the promotion of legitimacy and integrity within the cryptocurrency market.

Anti-Money Laundering (AML). Anti-Money Laundering (AML) targets a set of procedures and practices employed by financial crime institutions and other regulated bodies to curtail economic crimes. Such procedures include analyzing customer profiles and transactions against ascertainable benchmarks

maintaining appropriate books and records, reporting any suspicious activities concerning money laundering that may necessitate immediate action to the appropriate authorities, and many more. United States v. Delo, Hayes, and Reed (BitMEX), No. 20-cr-500 (S.D.N.Y. 2020), BitMEX founders were sanctioned for BSA violations because of missing AML/KYC despite U.S. customers. It confirmed that crypto exchanges should register and abide by U.S. AML regulations.

In cryptocurrency, AML deals with the legal boundaries restraining lawbreakers' attempts to convert cryptocurrencies attained through illicit means into cash. At present, it is the Financial Action Task Force (FATF) that sets the thresholds of AML law policy on an international level. In United States v. Larry Dean Harmon, the court decided that running a Bitcoin mixing service without a proper license was contrary to anti-money laundering laws. This case established that crypto mixers are not exempt from FinCEN regulation and KYC.

The FATF is a 39-member organization that establishes international standards to ensure national authorities are capable of effectively pursuing illicit funds that are crime proceeds. The FATF first started issuing cryptocurrency AML guidance in 2014, and the FATF's member jurisdictions followed swiftly with policy responses. The Financial Action Task Force (FATF) completed an interpretative note on Recommendation in 2019, amending and clarifying the recommendation to give more guidance on the application of FATF standards to virtual assets or cryptocurrency activities.

Coincheck Hack and Regulatory Fallout (Japan, 2018), Following a $530M hack, Japan's FSA enforced more stringent AML/KYC regulations on crypto exchanges. While not a court ruling, it turned out to be a regulatory milestone in crypto regulation in Japan. The note broadens existing regulatory requirements already imposed on other regulated products. After taking inputs from the private sector players, the Interpretation Note document was formally taken on board as part of the FATF Standards in June 2019.

Due to this new recommendation, virtual assets and Virtual Asset Service Providers (VASPs) will be fully regulated in the context of money laundering prevention and counter-terrorist financing, just like any other financial instrument. Currently, many regulatory bodies have legislated most of FATF's cryptocurrency AML recommendations. Securities Exchange Commission v. Binance Holdings Limited Binance was ordered to pay over $4 billion and CEO CZ pleaded guilty to not putting adequate AML/KYC controls in place. The case helped bolster international crypto exchange compliance standards.

AML controls demand financial institutions to scrutinize customer transactions for unusual conduct, which may prove money laundering or other economic offences, and to disclose the same in a timely manner. While so doing, financial institutions are also compelled to make confirmations on customer identification in a system of KYC steps.

Know Your Customer (KYC)

In financial operations, the verification process would involve having customers present certain credentials to organizations and businesses in order to be identified. It then becomes the organizations and businesses responsibility to verify that the submitted credentials are not false and that the customers are as claimed.

KYC is the process of collecting information on a customer and verifying their identity. The particular information to be used for verification purposes can differ according to jurisdiction. Businesses are generally required to obtain, at least, the customer's name, date of birth, and address.

For Cryptocurrency, KYC means the collection of a person's identity verification processes that are mandated by law for Virtual asset service providers (VASPs). This involves gathering personal details, for example, name, address, and government-issued identification documents. KYC is a minimum requirement that makes financial institutions responsible for due diligence and knowing the nature of their customers. FTX Collapse (2022) SBF was found guilty of fraud following FTX's inability to protect user funds and disregard for AML controls. The collapse highlighted the necessity for compliance and internal controls in leading crypto companies. By applying KYC checks, institutions are able to assign a risk value to persons or entities and flag potentially risky accounts and transactions beforehand. That type of procedure is in need as it directs or enables law enforcement authorities to link "ostensibly anonymous cryptocurrency addresses to real-world entities in crucial cases where all the addresses will be linked to criminality". This significantly enhances the ability to track and investigate criminality within the realm of cryptocurrency.

For traditional finance, acceptable credentials are ID card verification, face verification, biometric verification, and address proof, like a copy of a recent utility bill. In the cryptocurrency space, KYC is less uniform. The majority of crypto exchanges are asking their new customers to provide their full legal name, date of birth, government-issued ID, and current address details during onboarding, but it depends on where the exchange is based and what services it is offering.

In October 2021, FATF, under its updated member jurisdiction guidance, clarified that NFT marketplaces, DeFi protocols, and stablecoin issuers, subject to the activity they conduct, may also need to implement KYC measures.

How does KYC work in cryptocurrency?

1. Customer Identification Program (CIP)

CIP is the starting step in the process of KYC, which concentrates on customer identification verification. In the case of individuals, it is about obtaining information such as their full legal name, date of birth, home address, and official documents such as a passport or driver's license. In the case of businesses, business licenses or articles of incorporation are necessary. This step authenticates the customer and prevents fraud that is based on identity.

2. Customer Due Diligence (CDD)

CDD majorly involves assessing the level of risk posed by a customer or business relationship. Financial institutions collect and analyze information like customer background, transaction history, and survey responses. From here, a risk profile is developed to determine the level of scrutiny that will be required. The Customers facing high risk can be exposed to increased due diligence with tighter compliance and well-developed protection against financial crime.

3. Continuous Monitoring process

This process involves the real-time checking of the customers' transactions to identify unusual or suspicious behavior and patterns. In the cryptocurrency industry, Virtual Asset Service Providers (VASPs) are mandated by law to check accounts and report on any suspicious activities by submitting Suspicious Activity Reports (SARs). Continuation of monitoring is the supreme process for the detection and resolution of potential financial crimes. Examples are money laundering or fraud within the virtual assets platform.

Suggestions

- Incorporate guidelines from international bodies like the Financial Action Task Force (FATF), including the "Travel Rule" for information sharing between Virtual Asset Service Providers (VASPs).
- Institute harsh punishments for non-adherence to AML/KYC regulations, such as fines, revocation of licenses, or criminal charges where necessary.
- It is more desirable to invest in technology solutions such as blockchain analytics software and artificial intelligence to increase AML and KYC capacities and strengthen the effectiveness of regulation.
- Encouraging global collaboration and coordination of regulators and law enforcement authorities in order to really understand cross-border issues overlap with cryptocurrencies and money laundering.

Conclusion

Cryptocurrencies are changing how money works, making it crucial to have strong and long-lasting systems to stop money laundering and verify customer identities. While groundbreaking, the spread-out and semi-anonymous nature of these digital assets creates special weak spots that criminals are eager to take advantage of. The recent crackdowns and punishments, like what happened with FTX falling apart and Binance getting fined, show that the crypto world is entering a new phase where people are held responsible for their actions.

The main things are global regulatory harmonization, advanced blockchain analytics, AI-driven compliance systems, and the universal adoption of FATF guidelines, including the "Travel rule" which will be main pillars in combating illicit activities. The Virtual Asset Service Providers (VASPs), DeFi platforms, NFT marketplaces, and stablecoin issuers must proactively integrate compliance by design not as a regulatory obligation but as a cornerstone of trust and sustainability.

In the present evolving landscape, the integration of innovation with responsibility will lead to the legitimacy of the crypto industry. Those who adopt good and accurate AML/KYC practices will not only protect themselves from legal risks but also gain the trust of investors, regulators, and the public at large. The future of cryptocurrency depends not only on technological advancement but on the integrity with which that technology is governed. In the present and in the future scenario, the trend might continue toward stricter global regulations and improved scrutiny. Those who fail to comply with regulations will face heavy penalties, but more importantly and specifically, they risk losing the trust of their customers.

Article Written by:

Dondapati Naga Siva Durgaprasad - B.B.A. LL.B. (Hons.)

6th SEMESTER, 2022-2027.

LET'S SEE
Past Events

1. Offline Quiz by Krida Dharma and Legal Eagles Clubs (January 9, 2025):

Krida Dharma Club and Legal Eagles Club jointly organized an engaging offline quiz on January 9, 2025, helping students enhance their knowledge, critical thinking, and teamwork skills in a competitive environment.

2. Legal Crossword & Puzzle Solving Competition:

The Legal Crossword & Puzzle Solving Competition held on 5 February 2025 tested participants legal knowledge, analytical skills, and quick thinking. Winners A Shree Nidhi, Lingala Moksha, and Raghavi A G were recognized for their speed and accuracy. The event promoted learning, collaboration, and excitement among all participants.

3. Seminar on Taxation Law:

On February 4th and 6th, 2025, ACCL and AULSC hosted a guest lecture on GST by Adv. M.G. Kodandaram, a veteran taxation expert. He provided students with practical insights and real-world applications of Goods and Services Tax through engaging case studies. The session was a great success, enhancing students understanding and interest in taxation law.

4. Seminar on Practical Aspect of GST

The Alliance Centre for Corporate and Commercial Law (ACCL) organized a session on February 7, 2025, with CA Roy Sudeep D'Souza.

Students gained practical insights on GST compliance, real-world applications, and engaged actively in an interactive Q&A session.

5. Model GST Council Competition

The ACCL hosted the three-day Model GST Council Competition from April 1–3, 2025, simulating real council proceedings.

Participants debated GST on health insurance and education, proposed amendments, and reached a consensus after detailed discussions.

6. Article Writing Competition: "Crypto, Compliance & Cashless Futures – The Law Behind the Ledger"

An article writing competition was conducted on the theme Crypto, Compliance & Cashless Futures – The Law Behind the Ledger, encouraging analytical writing on contemporary legal-financial issues. Submissions were received by April 10, 2025, and the results were announced on April 26, 2025.

Crypto Compliance and Cashless Futures – The Law behind the Ledger

Crypto compliance and cashless futures are reshaping the global financial landscape, propelled by digital advancements and changing regulatory frameworks. Crypto compliance pertains to adhering to legal standards for the use and exchange of digital assets, ensuring safety, transparency, and responsibility. a cashless future provides an entirely digital economy where physical money is replaced by electronic transactions. Further they signify a transition toward a more effective and transparent financial system, redefining how value is stored and exchanged internationally. India has taken a leading role in this transition, managing regulatory hurdles and technological progress. In 2018, the Reserve Bank of India prevented banks from supporting crypto enterprises, but this was deemed "unconstitutional" and overturned by the Supreme Court in 2020 (Live Law, 2020). Since that time, India has enacted a 30% tax on crypto profits and a 1% TDS in 2022 (Mint, 2022), indicating a shift toward regulation instead of prohibition. The movement toward a cashless economy has also gained momentum, with UPI surpassing 10 billion monthly transactions by August 2023 (NPCI, 2023). At the same time, the RBI initiated pilot study for the Digital Rupee (CBDC) and began retail experiments with selected banks (TOI, 2023), contributing to India's developing digital payment ecosystem.

The Unified Payments Interface (UPI) has played a crucial role in this development, with transaction volumes soaring from 2,071 crore in FY 2017-18 to 18,737 crore in FY 2023-24, indicating a Compound Annual Growth Rate (CAGR) of 44%. Importantly, UPI transactions accounted for 83% of the total payment volume by 2024, an increase from 34% in 2019. In the realm of cryptocurrency, India has positioned itself as a leading force in adoption. As per Chainalysis, India in top position for usage of cryptocurrency, employing both

centralized and decentralized exchanges. This expansion is especially noticeable in non-metro locations like Nagpur, Jaipur, and Lucknow, where retail traders are progressively participating in crypto trading to enhance their earnings. Despite facing regulatory challenges, including a 30% tax on cryptocurrency gains, the Indian crypto market is projected to exceed $15 billion by 2035, featuring an 18. 5% CAGR. This growth underscores the resolve and enthusiasm of Indian investors in the digital asset market.

-By Jayshree T

The meteoric rise of cryptocurrencies and the accelerating pivot to cashless economies have ignited a seismic shift in global finance, exposing the fragility of outdated legal and regulatory frameworks. As faculty immersed in this paradigm shift, we assert that the future hinges on crafting dynamic, ironclad compliance systems that harness innovation without sacrificing systemic integrity. Blockchain-based cryptocurrencies offer unparalleled transparency and efficiency, yet their pseudonymous architecture poses a direct challenge to anti-money laundering (AML) and know-your-customer (KYC) mandates. Regulators must move beyond reactive patchwork solutions and proactively design frameworks that anticipate the next wave of decentralized financial tools failure to do so risks ceding control to unaccountable actors and undermining public trust.

Equally critical is the role of legal education in this cashless frontier. The law behind the ledger is not merely a technicality but a battleground where economic power, individual rights, and state authority collide. We urge academics and practitioners to prioritize interdisciplinary fluency marrying expertise in cryptography, financial regulation, and ethical governance to equip the next generation of lawyers and policymakers. The stakes are high: as digital currencies erode the monopoly of fiat cash, questions of taxation, cross-border enforcement, and consumer protection demand bold, principled answers. Faculty must lead by example, fostering rigorous debate and research to ensure that the rule of law evolves as swiftly as the technologies it seeks to govern.

-By Abhishek Thommandru

As the Faculty Coordinator of the Newsletter Committee at Alliance School of Law, it gives me immense pleasure to extend my heartfelt congratulations to the entire team on the release of this edition of our newsletter. The dedication, research, and creative effort that goes into each publication are truly commendable, and I am proud to witness the continued growth and excellence of this initiative. The newsletter serves as a platform for students to critically engage with pressing legal developments, and it is heartening to see the level of intellectual curiosity and professionalism reflected in every issue.

This edition's theme: cryptocurrency and its legal implications, is both timely and thought-provoking. As digital currencies continue to reshape global financial landscapes, they raise complex questions surrounding regulation, security, and legal accountability. Exploring these issues is essential for aspiring legal professionals, and I am confident that this edition will spark important conversations and deepen our understanding of this evolving field. I wish the entire team continued success and hope this publication inspires readers to delve further into the fascinating intersection of law and technology.

-By Nikhil A S

From Cowries to Cryptocurrencies

In the village of Kishangarh, nestled beside the Vindhya hills, life revolved around the rhythm of the harvest and the skill of the artisans. Trade was the lifeblood, but it flowed like a clogged stream. Meera the farmer had sacks of wheat and needed a sturdy tool from Sunil the blacksmith. Sunil had fine tools, but he didn't need wheat right then; his store was full. He needed cloth from Priya the weaver. Priya, in turn, needed wheat.

So, Meera couldn't simply trade with Sunil. She had to find someone who needed wheat and had something Sunil might accept for his tools – perhaps dried fish from Rohan by the river? If she traded wheat for fish, she then had to find someone who needed fish AND had cloth that Priya would weave with. It was a dance of inconvenience, a never-ending search for a 'double match'. At the weekly market, people spent more time trying to find the right trading partner than actually exchanging goods. Bartering a large item, like a sturdy bullock cart built by Ramesh the carpenter, was nearly impossible; who had enough different things Ramesh needed to equal its value? Saving was tricky too; extra grain could rot, and extra pottery might break.

The village elders, led by wise Devi Maa, sat under the ancient banyan tree, troubled. "Our efforts are great", sighed Devi Maa, "but our trade is bound by chains of need. We need something... a way to make every exchange simple". They needed something portable, something everyone valued, something divisible.

Young Arjun, known for his sharp eyes, who often played by the riverbank, brought forth a small leather pouch. Inside were smooth, white, spiral shells – Cowrie shells. "Devi Maa", he offered, "after the floods, we find these by the river. They are hard, they are beautiful, and you can count them easily. And you never find too many in one place".

Devi Maa picked one up, its surface cool and smooth. "What if", she said, her voice soft but clear, "we all agree that these cowries represent the value of things? What if anyone will accept cowries for their goods, knowing they can use the cowries to get whatever they need from anyone else?"

Skepticism mingled with hope. But the frustration of barter was great. They agreed to try.

The next weekly market was different. Meera took her wheat, and instead of searching for a direct swap, she sold it for a set number of cowries to a family needing grain. With her cowries, she walked directly to Sunil's stall and bought the tools. Sunil took the cowries and bought cloth from Priya, who used them to buy wheat later from Meera or another farmer. Ramesh the carpenter set a price in cowries for his bullock cart, and buyers saved up cowries from selling their own goods until they had enough.

Life in Kishangarh blossomed. People specialized, knowing their goods could be exchanged for cowries, the universal key that unlocked any trade. The little white shells, born of communal agreement and trust, had replaced the cumbersome chains of barter, becoming the heart of Kishangarh's simple, flowing economy – its first currency.

The transition from traditional, often government-issued fiat currencies to exploring and utilizing cryptocurrencies is a complex evolution driven by technological innovation and changing societal trust. As the global economy became increasingly digital, the need for native digital forms of value exchange grew. This was accelerated by events like the 2008 financial crisis, which eroded confidence in centralized financial institutions and monetary authorities. The advent of blockchain technology, first popularized by Bitcoin in 2009, offered a novel alternative: a decentralized, distributed ledger for tracking transactions, eliminating the need for intermediaries like banks or central governments. Cryptocurrencies emerged as digital assets built on this technology, designed to function as a medium of exchange, potentially a store of value, and a unit of account, fundamentally different from fiat due to their decentralized nature and cryptographic security. This represents a movement towards digitally native currencies that aim to offer greater transparency (on the public ledger) and resistance to censorship or central control, pushing the boundaries of what 'currency' can be in the 21st century.

-By Rahul Shaw

MESSAGE

Cryptocurrency Recognition

The Indian government has shifted its position on cryptocurrency, acknowledging its existence and has introduced measures to tax it, by classifying it as virtual digital assets. However, cryptocurrency has not been granted the status of legal tender, and no specific laws or regulations have been established to fully regulate its use in the country. In November 2022, the Reserve Bank of India launched the Central Bank Digital Currency (CBDC) or the Digital Rupee on a pilot basis. While CBDC is an electronic/digital version of the national currency, it is not an alternative to cryptocurrency but will provide benefits in a legal and secure manner. While cryptocurrency is decentralised, RBI will control and regulate the supply and usage side of CBDC. Moreover, CBDC is an electronic form of cash, whereas cryptocurrency trading involves investment in cryptocurrency as an asset class. The current attitude of the Indian Government suggests their acceptance of the usage of blockchain technology; however, it is limited to treating cryptocurrency as a currency being regulated by a central authority. Cryptocurrency has also been put under the purview of the Prevention of Money Laundering Act (PMLA) and the crypto exchanges are mandated to report suspicious transactions to the Financial Intelligence Unit of India. Furthermore, entities dealing in crypto have to follow stringent KYC norms and conduct due diligence being 'reporting entities' under PMLA. The Indian Government still remains reluctant to accept and regulate cryptocurrency as an asset class due to its volatility and the tendency of users to be attracted to the facet of speculative trading of cryptocurrencies.

The popular opinion stipulates the acceptance of cryptocurrency as an investable asset class, the acceptance of which will lead to a systemic risk-based approach and the focus would be on governing and regulating this asset class. Nevertheless, the ongoing debate remains on whether crypto has to be categorised as an asset, commodity or security. Japan is a good example of where cryptocurrency is officially recognised as a valid form of payment method with specific regulations. However, cryptocurrency is still classified as an "asset" and not a legally recognized currency or legal tender. In Japan, the Payment Services Act (PSA) only

permits companies with a high financial capacity and operations to function as cryptocurrency exchanges. One can only buy and sell cryptocurrencies on exchanges approved by regulators. Entities wanting to enter cryptocurrency trading, need to register with the Japanese Financial Services Agency, following stringent cybersecurity and anti-money laundering requirements. Along with AML, crypto-asset exchanges are required to undertake counter-terrorism funding measures. The Japanese government doesn't consider cryptocurrency as a legal tender, as it isn't issued by a central bank. However, the Japanese Government recognises the power of a decentralised ledger to increase purchasing power. Banks in Japan can only work with entities handling cryptocurrencies after having completed stringent KYC checks. This reflects that different jurisdictions categorise and treat crypto for varying purposes. Some have recognised and accepted digital assets by legislating over them, while others are regulating them through enforcement. However, this split approach by regulators around the world will create disharmony in the global financial ecosystem.

The current imperative calls for a common consensus among regulators across the world. This consensus must establish clear guidelines pertaining to cryptocurrencies. This should primarily include its classification, regulatory framework to be adopted keeping in line with the framework applicable to banks and differentiating or amalgamating rules and regulations governing securities trading and crypto trading. It is paramount to accept and adopt a unified definition of cryptocurrency and its legitimacy to ensure standardised operations on a global scale.

THE LEISURE LOUNGE

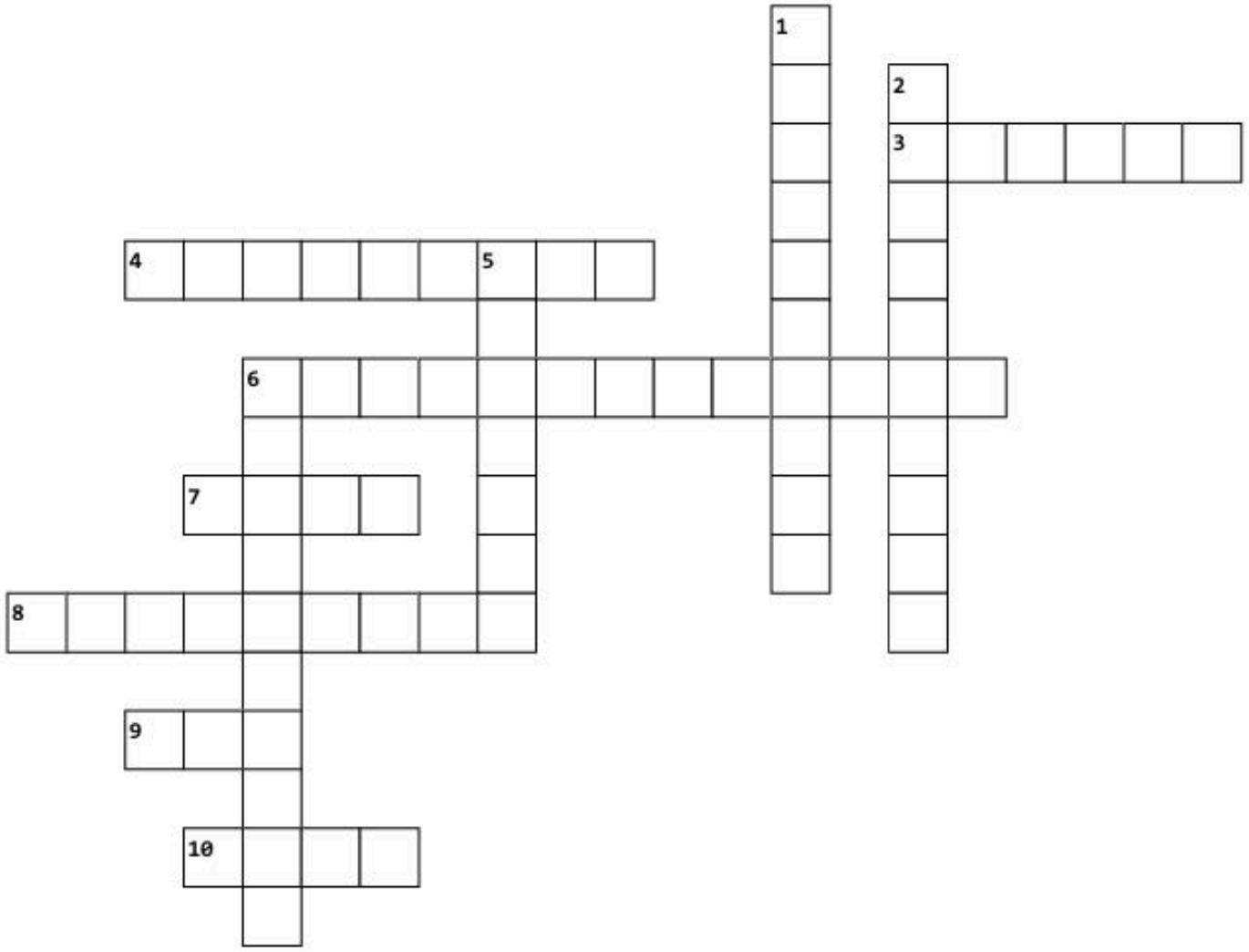
WORD SEARCH PUZZLE

K	N	E	N	O	A	T	N	D	P	N	C	F	B
I	E	E	E	C	N	O	N	I	W	S	B	C	C
I	K	I	C	A	L	I	S	G	A	N	L	D	A
I	O	I	F	O	O	O	F	I	L	C	O	C	S
N	T	Q	C	C	M	R	K	T	L	A	C	M	H
N	A	K	T	A	A	M	C	A	E	C	K	E	L
O	K	I	C	U	I	C	E	L	T	N	C	E	E
V	B	O	D	R	U	D	A	R	E	E	H	D	S
A	Y	T	A	N	P	I	E	C	C	C	A	O	S
T	D	D	T	M	I	I	O	N	A	E	I	C	I
I	A	T	A	O	L	R	O	N	T	G	N	R	S
O	E	D	K	A	I	C	R	R	O	I	L	Q	I
N	B	L	C	R	Y	P	T	O	I	O	T	Y	C
B	E	E	F	I	N	T	E	C	H	S	A	Y	L

Find these words

IDENTITY, TOKEN, WALLET, FRAUD, QRCODE, UPI, INNOVATION, ECOMMERCE, AML, BITCOIN, CASHLESS, BLOCKCHAIN, FINTECH, DIGITAL , CRYPTO

CROSS WORD PUZZLE QUIZ



Across

3. The type of ledger that records all transactions in a decentralized network.

4. A common term for transactions that cannot be undone or altered on the blockchain.

6. A type of digital contract that executes automatically when conditions are met.

7. A global organization that sets anti-money laundering (AML) standards.

8. The maximum supply of Bitcoin, making it a scarce digital asset.

9. The process of verifying a customer's identity to prevent fraud and financial crimes.

10. The name of the legal framework regulating crypto exchanges in the European Union.

Down

1. The act of disguising illegal funds to make them appear legitimate.

2. The technology that powers cryptocurrencies, ensuring transactions are secure and transparent.

5. The digital currency that started it all in 2009.

6. A digital asset pegged to a stable value, often the US dollar.

SHARE YOUR ANSWERS TO ACCL@ALLIANCE.EDU.IN AND GET A SURPRISE


TO BE CONTINUED....