



LEGALITY OF CRYPTOCURRENCY: REGULATION VS. PRIVACY

Manas Saxena* Harsh Tiwari*

ABSTRACT

This article contributes to the digital debate about the legality of cryptocurrency. It explores the legal implications of cryptocurrency, dwelling into the digital dilemma of regulation of financial transactions by legal regulatory bodies, which is opposed by individual entities concerned about anonymity and privacy breaches leading to global conflict. It talks about 'privacy coins and the issues that regulatory bodies face while dealing with them. It talks about global trends and perspectives on cryptocurrency. It critically questions the necessity of KYC (Know Your Customer) and AML (Anti-Money Laundering) laws. With the help of legal precedents and case laws, it discusses the current scenario of cryptocurrency in India. Furthermore, it explains the current scenario of cryptocurrency in India and predicts upcoming legal frameworks and regulations for it. It also offers potential solutions to balance out the volatile issue of regulation vs. privacy, advocating for laws and policies that are just, fair, and reasonable while ensuring financial transparency and consumer protection.

INTRODUCTION

Being a modern challenge for law, cryptocurrency has reshaped the global financial system. The First Cryptocurrency, bitcoin, was introduced in 2008 by a pseudonymous developer, defining it as a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution.¹ Cryptocurrency, being decentralised in nature, does not require a central authority; its state is maintained through distributed consensus, which keeps an overview of cryptocurrency units and their ownership. Unlike other digital forms of currency, cryptocurrency is anonymous, making it hard to trace or track, making it tricky for legal frameworks to deal with.

*BA LLB (HONS), SECOND YEAR, FACULTY OF LAW, JAGRAN LAKECITY UNIVERSITY.

*BA LLB (HONS), SECOND YEAR, FACULTY OF LAW, JAGRAN LAKECITY UNIVERSITY.

¹ Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008), <https://bitcoin.org/bitcoin.pdf>

GLOBAL PERSPECTIVES ON CRYPTOCURRENCY REGULATION

The perspectives on cryptocurrency regulation can be roughly classified into 2 groups: Supporters and Opposers. Supporters being conservative in nature regarding cryptocurrency regulation, contend that regulation is required to maintain financial stability across the state whereas opposers advocate for the fact that anonymity is an essential force, required for the smooth functioning of digital transactions.

Following are the opinions and decisions of regulatory bodies of global giants:

- **United States of America:** The scenario in the USA regarding cryptocurrencies is quite fragmented. Certain cryptocurrencies are treated as securities, whereas CFTC treats Bitcoin and Ethereum as commodities. The IRS is stringent with Money Laundering laws regarding cryptocurrencies.
- **Canada:** Canada is quite liberal with cryptocurrencies, has clear cryptocurrency guidelines, and requires exchanges to register with financial regulators.
- **European Union:** Markets in Crypto-Assets (MiCA) regulation will establish a uniform legal framework throughout the European Union and is set to take full effect by 2024.
- **United Kingdom:** The U.K. prioritizes consumer protection and compliance. Post-Brexit, cryptocurrencies need to register with the Financial Conduct Authority (FCA).
- **China:** China has declared a complete banned cryptocurrency trading and mining to promoting its own central bank digital currency (CBDC), the digital yuan.

PRIVACY COINS AND THEIR LEGAL IMPLICATIONS

Privacy coins are cryptocurrencies that use techniques such as ring signatures, zero-knowledge proofs, and conjoin to enhance user data privacy. Being nascent, Privacy coins are hard to understand, making it difficult to present them as evidence. Privacy coins provide nearly no financial oversight for legal agencies, making them the perfect tool to carry out illegal activities such as terrorism funding, tax evasion, and money laundering. This forces regulatory bodies to often impose restrictions on privacy coins, which defeats the purpose of privacy coins. However, despite these restrictions, the misuse does not stop as the regulatory bodies are incapable of enforcing these restrictions. The anonymity of privacy coins remains undefeated, even by legal bodies, as there is a lack of technology available to penetrate their technical

security or defences. Regulators are trying to renovate their monitoring techniques, but Privacy Coins are far ahead in the race and are difficult to catch.

THE DILEMMA OF REGULATION, PRIVACY, AND LEGAL RIGHTS

Privacy provides comfort and security to an individual entity, whereas Regulation provides stability at a broader level. Both of them are inversely proportional to each other as they lie at opposite ends of the spectrum, which makes establishing harmony between the two a challenge. In the digital age, financial transactions are vulnerable to cyber-attacks, putting valuable assets at risk. Due to this fear of loss, people lean towards safe and secure modes of transactions, which are sparse. When cryptocurrency came into motion, people who valued their privacy shifted to it. Anonymity provides privacy, which assures people of safety, which is the core philosophy of cryptocurrency.

However, it is not privacy that's the problem but rather the misuse of it. Privacy can be a headache for legal frameworks as privacy provides no data to the regulatory bodies as well. The intention of regulatory bodies to collect data is not malicious, but cryptocurrency does not differentiate. Therefore, with near to no data, regulatory bodies cannot monitor or control illegal activities taking place with cryptocurrency. Regulation provides crime prevention; a state where there is no regulation will ultimately harm the entities in it. However, some people believe that the Regulatory Bodies are no better than the data pirates themselves as there have been countless breaches and infiltrations within the regulatory bodies, leaking private data. People are fed up with such attacks and, therefore, believe that regulation will only harm their financial security, causing non-compliance.

Setting the balance between regulation and privacy relies on the question of whether Privacy is a legal right. If it is, then cryptocurrency transactions should be legal, but if it is not a legal right, then it can be regulated. Privacy is required for day-to-day activities where a person must have the right to conceal his sensitive information. Privacy may not be a legal right in every country, but it is a human right. However, rights are not absolute and, therefore, can be restricted for the benefit of the collective good and general welfare. To establish control over cryptocurrency, regulatory bodies might bring up laws that require compromising some of the private data of a person, but the data must be safely and securely stored with the regulatory bodies. The laws should be brought up to prevent illicit activities and not for any other malicious reason. The data laws must be 'just, fair and reasonable' and not arbitrary.

KYC (KNOW YOUR CUSTOMER) AND AML (ANTI-MONEY LAUNDERING) LAWS: NECESSARY OR OVERREACHING?

What are AML Laws: Anti-Money Laundering (AML) laws describe a range of compliance actions that financial institutions must take to ensure that they do not become a part of any illegal activity through their platform services. Complying with AML laws has many benefits for business, which include:

1. Keeping customer data secure.
2. Creating automated fraud detection services.
3. Using global customer databases to check the background of new customers.
4. Close monitoring of transactions.
5. Reporting illegal activities.

What is KYC: Know your customer is a subset of AML compliance focused on customer identity verification. KYC consists of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD). CDD includes collecting personal information to identify the real identity of the person, collecting business information and regular customer monitoring. EDD includes taking extra steps for customers who may be a high risk for money laundering. These steps may include collecting more customer information, documenting detailed customer reports, and closely monitoring politically exposed persons.

Is there money laundering in crypto transactions? According to a 2022 report from the leading blockchain analytics company Chainalysis, criminals laundered \$8.6 billion in cryptocurrency in 2021, a 30% increase over the previous year. The report says that “while billions of worth of cryptocurrency are transferred annually from illicit addresses, the majority of it ends up at a surprisingly small number of services, many of which appear to be purpose-built for money laundering.”²

These AML laws and KYC do not infringe upon the privacy of the customers, but on the other side, they protect private information and maintain the security of the customers. It takes up only the necessary information from the customers that is required to identify genuine customers. These laws and procedures are made to minimize illegal and fraudulent transactions

² Notabene, *What Is Anti-Money Laundering (AML) & How Does It Apply to Crypto?* Notabene (2024), <https://notabene.id/crypto-travel-rule-101/aml-crypto>

so that no one becomes the target of scammers around the web. Moreover, these laws are made with a Bonafide intention of overall safety of the customers and the financial activities.

LEGAL POSITION OF CRYPTOCURRENCIES IN INDIA

In India, cryptocurrencies are currently unregulated. Earlier, the Reserve Bank of India and the Government of India banned dealings in cryptocurrency. Its notification on 6th April 2018 titled “Prohibition on dealing in Virtual Currencies (VCs). According to the RBI, cryptocurrencies are “stateless digital currencies” that use encryption techniques for trading and enjoy immunity from state intervention, leading to chances of illegal transactions.

In the case of Internet and Mobile Association of India v. Reserve Bank of India (AIR 2021 SC 2720),³ The judgement on 4th March 2020 set aside the ban on cryptocurrency by the Reserve Bank of India. The court said that the ban would take away the rights of trading people, which is a fundamental right. The court also emphasized that there are no legal provisions for banning cryptocurrency trading and that cryptocurrency did not affect the functioning of banks under the Reserve Bank of India. This judgment paved the way for trading companies and investors for future options related to cryptocurrency trading.

MODERN TRENDS AND FUTURE PREDICTIONS

Cryptocurrency is evolving rapidly, transforming financial systems and challenging traditional institutions. The trends include the integration of Artificial Intelligence (AI), the tokenization of Real-World Assets (RWA), and the developments related to Non-Fungible Tokens (NFTs).

Artificial Intelligence and Blockchain Integration: Artificial Intelligence (AI) is improving the cryptocurrency industry by improving trading techniques and analysing market trends with high precision. Artificial Intelligence (AI) is enhancing security by identifying vulnerabilities and detecting fraudulent activities. Artificial Intelligence’s integration with blockchain has made several advancements, including:

1. Improved decision-making through predictions.
2. Real-time fraud detection and prevention.
3. Smart automated contract auditing for enhanced security.

³Author Unknown, *Regulating Cryptocurrency in India*, INT’L BAR ASS’N (Jan. 12, 2023), <https://www.ibanet.org/article/2e4fb646-4ffd-4660-a5be-5e41e79c5576>

Real-World Asset Tokenisation (RWA): The tokenisation of Real-World Assets (RWA) is one of the most progressive applications of blockchain technology. Converting assets like real estate, commodities, or fine art into digital tokens, enables investors of all scales to participate in markets reserved for the wealthy elite.

Benefits of RWA tokenisation:

- Allowing investors to buy smaller shares of high-value assets.
- Enhanced transparency and security.
- Global accessibility and participation.

NFTs and Digital Identity: By enabling tokenized ownership of digital assets, NFTs facilitate innovative applications in gaming and intellectual property management. In addition to NFTs, digital identity solutions powered by blockchain are systems that provide individuals with secure, verifiable identities that are portable across platforms.

Applications of NFTs and digital identity include:

- Personalised content delivery based on NFT ownership.
- Enhanced user engagement.
- Decentralised authentication for privacy.

POTENTIAL SOLUTIONS

Blockchain technology can be used to ensure privacy, where only authorized parties have visibility to reports carrying information about the users. The data could be made selectively visible only to authorized law enforcement authorities, subject to clear policies while ensuring the protection of personal information from data miners and criminal actors. Compliance policies, established by regulators and within organizations, could be used to enforce rules for which digital transactions may be allowed and what information should be stored with each transaction. Using such on-chain compliance, privacy can be guaranteed with each transaction. The on-chain compliance can protect confidential information along with enforcing privacy and financial confidentiality for all.

On-chain compliance is an opportunity to modernize AML rules utilizing consensus rules running on a blockchain. Instead of struggling to harmonize KYC practices or exposing the financial system to a central panopticon with implications on cybersecurity, on-chain crypto compliance provides an opportunity for financial institutions to rely on other institutions'

attestations and use them for risk management without moving information or exposing it to the user. Sanctions can be enforced on-chain and updated in real-time to prevent any transaction from going through absent compliance. Reports can be administered automatically off-chain, saving important time and providing law enforcement with better chances to prevent crime from happening.⁴

CONCLUSION

The debate of regulation vs privacy regarding cryptocurrency is an evolving dispute. On one hand, privacy and anonymity are essential human rights, but the misuse of such rights causes problems for regulatory bodies in preventing financial crimes. Maintaining a balance between regulation and privacy is essential for the future of cryptocurrency. Regulatory bodies must adopt policies that maintain financial transparency without undermining fundamental privacy rights. Global perspectives remain diverse, with some countries accepting cryptocurrency with open arms, whereas others outright reject its concept. The legal status of cryptocurrency in India remains uncertain and volatile, with the Indian Judiciary playing a critical role in shaping its future, yet a comprehensive legal framework is yet to be implemented.

⁴Angela Angelovska-Wilson et al., *On-Chain Privacy and Compliance: Can They Co-Exist?*, STAN. J.L. BUS. & POL'Y (June 24, 2023), <https://stanford-jblp.pubpub.org/pub/onchain-privacy-compliance/release/1>.