Volume 22, September 2022 2581-5504

Cryptocurrency and Money Laundering (Indian)

Ripudaman Singh Tanwar
Ramjas College,
Delhi University

THE RELATIONSHIP: CRYPTOCURRENCY AND MONEY LAUNDERING

Cryptocurrencies, which are mostly based on the peer-to-peer (P2P) mechanism, appeal to money launderers as the whole cost of cashing out is less than 15 percent of the proceeds of crime, compared to traditional money laundering procedures, which may cost up to 50 percent. As a result of the anonymity of the transaction information and the funding source, the PMLA does not cover these transactions. Section 12 of the PMLA, which mandates that banks, financial institutions, and intermediaries preserve and maintain records, forbids the failure to record every transaction data. Because of their anonymity and accessibility, bitcoins are arguably the ideal safe haven for criminal activities such as money laundering.

As a consequence, unless anonymity is eliminated from all cryptocurrency transactions, finding or freezing a digital wallet suspected of containing "proceeds of crime" would become exceedingly difficult for an agency like the Directorate of Enforcement (hereafter "ED"). The PMLA's draught bill attempted to address the problem of anonymity by designating cryptocurrency mining, creation, issuance, ownership, use, sale, transfer, and/or disposal as a "scheduled crime." WazirX, CoinDCX, and CoinSwitch Kuber, three of India's largest cryptocurrency exchanges, joined the Internet and Mobile Association of India to create an advisory council for the development of ethical standards for the crypto industry in India. WazirX was recently slapped with a notice by the ED for allegedly breaking the FEMA in transactions worth Rs 2,790.74 crore. Despite the fact that India has yet to establish a cryptocurrency regulation, particular forms of transactions are more likely to result in fines.

CRYPTOCURRENCY: A MEANS OF MONEY LAUNDERING

1. Criminals use digital currency exchanges to create online accounts that accept fiat cash from conventional bank accounts. “Then they begin a 'cleaning' process (mixing and layering), in which they use mixers, tumblers, and chain hopping to move money into the cryptocurrency system (also called cross-currency). Money is transferred from one cryptocurrency to the next, through digital currency exchanges — the less regulated, the better — to create an almost impossible-to-follow money trail.”[1]
2. According to the "Cryptocurrency Anti-Money Laundering Report," criminals often launder bitcoins via theft and gaming.
3. The creation of the Dark Web or Dark Market, which allows hackers to abuse people.

[1] Nikolei M Kaplanov, ‘Nerdy money: Bitcoin, the private digital currency, and the case against its regulation’ (2012) 25 Loy. Consumer L. Rev. 111, 124.

4. Bitcoin is the world's biggest cryptocurrency, with a market capitalization of $350 billion. A distinguishing characteristic of bitcoin is that all transactions are recorded in a public ledger that is shared among thousands of computers at the same time. Bitcoin proponents argue that it is vulnerable to manipulation or hacking.[2]
5. There is no legal tender for cryptocurrency. As a consequence, it cannot be approved and anybody may subscribe, resulting in money laundering.
6. It is simple to trade across nations since it lacks regulatory power, and this might lead to money laundering disguised as business.
7. Cryptocurrency is highly encrypted, making it difficult to track.[3]
8. Stacking: Cryptocurrencies may be bought using cash (fiat) or other forms of cryptocurrency (altcoin). Online cryptocurrency trading venues (exchanges) differ in their compliance with financial transaction requirements. Legitimate exchanges are Anti-Money Laundering (AML) compliant and meet regulatory criteria for identity verification and money source. Other exchanges do not have the same level of AML compliance. The majority of bitcoin money laundering transactions take done via this vulnerability.[4]
9. Confidentiality: Cryptographic transactions may usually be tracked via the blockchain. Criminals may utilize an anonymizing service to obscure the source of money once a filthy cryptocurrency is in circulation, destroying the linkages between bitcoin transactions. This may be done on standard crypto exchanges or via an Initial Coin Offering (ICO), in which one kind of coin is used to pay for another, obscuring the digital currency's origin.
10. Integration: The integration stage - the ultimate step of money laundering – is when you can no longer simply track filthy cash back to illegal activities. Money launderers still need a means to justify how they got into possession of the cash, even though it is no longer directly linked to crime. That explanation is integration.[5] Presenting the unlawful revenue as the product of a lucrative enterprise or other monetary appreciation is an easy way to legitimize it. In a market where the value of any individual cryptocurrency may vary by the second, this can be difficult to show.
11. Peer to Peer: Many criminals use decentralized peer-to-peer networks, which are usually transnational, to reduce the danger of bitcoin money laundering. They may frequently transmit monies to their future destination via unwitting third parties in this situation.
12. Gaming site: Another option to undertake a crypto money-laundering plan is to engage in online gambling and gaming via sites that accept bitcoin or other cryptocurrencies. Users

[2] Kerry Lynn Macintosh, 'How to encourage global electronic commerce: The case for private currencies on the internet' (1998) 11 Harv J L & Tech 733, 756.
[3] Ibid.
[4] *Supr*a note 1.
[5] The Law Library of Congress, Regulation of Cryptocurrency around the World, Global Legal Research Center, June 2018.

may use cryptocurrency to purchase credit or virtual chips, which they can cash out after a few modest transactions.[6]

NO LEGAL STRUCTURE IN PLACE

The current legal system is ill-equipped to cope with the many controversial policy concerns that surround crypto and its sub-groups, whether it's transaction methods like Bitcoin, tokens like Ethereum, or non-fungible tokens (NFTs).

Financial stability and how to safeguard consumers and investors are the most pressing public policy concerns. Other issues like as money laundering and terrorist financing continue to be a source of worry. Furthermore, the private crypto-exchanges that enable the selling and purchase of cryptocurrencies are unregulated. And the blockchain technology that underpins cryptography is not immune to theft, and it also carries the danger of no support or assurance in the event of a system failure or hacking.

Poly Network, a blockchain platform, disclosed that its system has been hacked. Other options exist. For example, can consumer and investor protection be guaranteed if crypto assets are taxed? All of these factors are said to be being examined by the government in order to safeguard the financial system's security and avoid the exploitation of technology-based financial products.

The BitConnect Ponzi scheme fraudulently swindled thousands of individuals out of more than $2 billion in bitcoin, making it "the biggest single recovery of a cryptocurrency fraud by the US to date."[7]

The contradiction that various governments and significant economic leaders are grappling with is the danger to the security of financial institutions vs the promise of crypto assets. It's also a divisive investment topic. Gary Gensler, the chairman of the United States Securities and Exchange Commission, compares them to the "wild west." "I wouldn't go invest in crypto, not because I wouldn't spend my own money, but because I don't believe people purchase Apple shares to have exposure to crypto," Apple CEO Tim Cook said.[8]

The administration of the European Union has said that Bitcoin and other cryptocurrencies will not be recognized as legal money at this time. It's reasonable that you're wary. The relationship between the price of Bitcoin and world events is poorly understood. Because crypto assets are anonymous, they generate data gaps that are used for money laundering and terrorist funding. Even if exchanges collaborate with law enforcement, authorities may not be able to decipher the data and accurately identify the participants to questionable transactions.

[6] Supra note 4.
[7] Ibid.
[8] Novak, Julie, 'The end of money as we know it' (October 2012) Review- Institute of Public Affairs, Vol 64, Issue 3, pg 19-21.

The disappearance of Bitcoins in Bengaluru has drawn attention to the police's lack of standards and competence in dealing with new age crimes involving crypto currency and the dark web. This incident may not have had a substantial effect on financial stability, but as trade volume rises in tandem with the number of unique visitors, the relevance of crypto assets in terms of possible repercussions for the broader economy is only going to grow.[9]

The government has a challenging policy formulation task in making this 'India's Techade' a leader in the area of electronics and information technology. It must strike the appropriate balance between enjoying the advantages of a big crypto-market and preserving the interests of investors.

THE INDIAN STANCE ON ANTI-MONEY LAUNDERING

On a global scale, India has previously ratified a number of United Nations (UN) Conventions:

1. International Convention on the Suppression of Terrorist Financing (1999);
2. The United Nations Convention Against Corruption.
3. The United Nations Convention Against Transnational Organized Crime and;

Since 2010, India has been a member of the Financial Action Task Force (FATF), which was founded in 1989 at the G7 meeting in Paris.[10] The Prevention of Money Laundering Act, 2002, was similarly designed and implemented in India (PMLA)

Despite the fact that there are no mandatory processes for cryptocurrency exchanges, several have taken it upon themselves to verify that all of their customers complete their KYC and provide their PAN card information.[11] The Penny Drop technique is used by these exchanges to undertake KYC for its members. Penny Drop is a technique of transferring Rupees 1 from a user's bank account to the exchange's wallet to verify that the bank account data are correct and that the name registered with the bank matches the name registered with the exchange.[12] Many exchanges also use anti-money laundering software to identify cryptocurrency addresses that have already been blacklisted.[13] However, because the blockchain is decentralized and allows users to exchange cryptocurrency on a peer-to-peer basis, criminals can easily exchange their cryptocurrency through multiple hands.[14] But, at the end of the day, when a user withdraws their cryptocurrency, law enforcement agencies are able to keep track of any funds that have been

[9] Shobhit Seth, "The 6 Most Private Cryptocurrencies" (Investopedia, 5-1-2021) <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/>.
[10] Robert Skildelsky, 'The euro in a shrinking zone' (cnn.com, 20 December 2011).
[11] Nikolei M Kaplanov, 'Nerdy money: Bitcoin, the private digital currency, and the case against its regulation' (2012) 25 Loy. Consumer L. Rev. 111, 118.
[12] Ibid.
[13] Brett Wolf, 'Senators seek crackdown on 'BITCOIN' currency' (Reuters.com, June 8, 2011).
[14] Edward Southall, Mark Taylor, 'Bitcoins' (2013) 19(6) C.T.L.R 177, 177

withdrawn and are linked to the blacklisted address because blockchain, with its transparent structure, makes all transactions available in the public forum.[15]

CONCLUSION

Incorporating new-age machine learning technology that enables transactions to be monitored using software that employs artificial intelligence (A.I.) to effectively filter through strings of meta-data to keep a watch on probable instances of money laundering is one such way that may be implemented. Because A.I.'s machine learning skills will enable it to detect patterns in massive volumes of data while also reacting to changes in criminal behavior over time, this might be a viable option. Even, if necessary, precautions are put in place, criminal elements will continue to exist; they will just find new methods to achieve their mission, which is to abuse the system.

As a result, legislation, monitoring, and the use of cutting-edge technology to combat such crimes is the way to go in order to limit the number of victims.

Due to the ambiguity in this field about the RBI's position on cryptocurrency and the tensions that occur as a result of technical gaps and the absence of regulations that may control the technology employed, there is a continuing need for consideration and swift adoption of such laws.

[15] Ibid.