On Loan apps and Crypto Criminals*

C. P. Chandrasekhar

India's enforcement directorate, still preoccupied with unearthing corruption and money laundering among opposition politicians, has decided to turn its attention to those involved in the crypto business in the country as well. Raids on the offices of crypto-exchanges (which manage trades in and movements of these virtual coins) and a freeze on the assets of companies controlling them, have stalled crypto activity in the country. The Economic Times recently reported that the Enforcement Directorate (ED) is probing at least ten cryptocurrency exchanges for allegedly laundering more than Rs. 1,000 crore of money criminally acquired. Coming in the wake of a one per cent capital gains charge (to be deducted at source) on digital transactions, that had eroded trading volumes in crypto markets, these moves are expected to cripple the crypto business.

Such a setback is no cause for concern, given the role of this sector as a site for speculation and illegal activity. But the fact that this possible outcome is not the result of a ban, which the government and the Reserve Bank of India (RBI) have on occasion favoured, but of taxation and investigations relating to criminal activities, points to the lack of clarity with regard to the government's cryptocurrency policy and the ineffectiveness of whatever intervention is being adopted.

The investigation of criminal activity that led up to the raids on the cryptocurrency exchanges were not originally targeted at this industry, but at the app-based online lending business. The story is one of crude and predatory extortion of huge sums from misinformed or foolish borrowers by loan-app businesses, using a combination of deceit, fraud and coercion. Attracted by offers made through online apps of instant loans that required no documentation or collateral, cash-strapped or pathological borrowers logged in and obtained loans, for which they had to reveal information varying from digital identity markers to their social media profiles, contact lists and photo galleries. Often such data was accessed without informing the client, once permission to access some data stored on the user's phone was obtained. In some instances, loan app managers even engaged illegal call centres to hack into the user's phone and steal data.

The loans advanced by these apps are given for short periods of time at interest rates that are usurious, making repayment near impossible. When the much-too-early repayments fall due and default is a possibility, the lenders unleash a barrage of online weapons aimed at threatening or shaming clients into finding ways of extricating themselves from the situation after paying hefty sums inflated because of absurdly high interest rates and penalties imposed. The attack included threatening calls often at unearthly hours, disparaging and defamatory messages to relatives, friends and colleagues demanding their intervention to ensure payment, and the use of morphed images even of an obscene kind to shame the victim, all with the aim of pressurising borrowers to pay up huge sums. According to reports, the sums demanded for loans advanced for a few weeks were exorbitant multiples of the original amount borrowed, and on occasion payments were demanded from individuals who had just made enquiries and not resorted to any borrowing. Unable to suffer the bullying, some of the victims paid up by liquidating every available asset, a couple committed suicide because of the harassment, and a few turned to the police.

When the number of such complaints mounted and investigations began, the trail of the huge sums of money extracted from these borrowers not only faded but went beyond the jurisdiction of Indian agencies. It turned out that shell companies set up to manage these apps received their capital and their returns in rupee wallets that were used to convert profits into digital cryptocurrency tokens. Those tokens were then transferred to cryptocurrency wallets outside the country. To transform rupees into cryptocurrency equivalents and to transfer those cryptocurrency sums abroad, the operators used the legal crypto-exchanges operating in the country, whose lax know-your-customer practices allowed the transactions to go through without any difficulty. According to the investigating agencies, the operators of many of these loan apps were foreign agents from multiple locations, predominantly Chinese. In most cases the individual beneficiaries of the foreign wallets remain unidentified.

A typical example is Yellow Tune Technologies Ltd, a Bengaluru-based 'fintech' firm. The ED's investigations reportedly revealed that Yellow Tune was a shell company that had Chinese nationals on its board. Entities engaged in predatory lending deposited funds in the rupee wallets of Yellow Tune, which were then converted into cryptocurrency tokens and transferred to crypto wallets outside the country. The ED's raid revealed that Yellow Tune had transferred abroad through transactions in the exchange Flipvolt, a crypto exchange that is the Indian arm of Singaporean Vauld, a sum of at least Rs. 370 crore that had been deposited into its rupee wallets by as many as 23 entities engaged in predatory lending. But, searches conducted at various premises of Yellow Tune Technologies to locate the owners of the company and the recipient wallets found them untraceable, because: "Lax KYC norms, loose regulatory control of allowing transfers to foreign wallets without asking any reason/declaration/KYC, non-recording of transactions on blockchains to save costs etc, has ensured that Flipvolt is not able to give any account for the missing crypto assets."

Given the failure to prevent the original predatory actions that constitute the crime, and to bring to book the loan app operators who are the principal perpetrators of the crime, the subsidiary role of the crypto-exchanges became the focus of attention. Action against them followed. For example, to cover the Rs. 370 crore transferred abroad through Flipvolt, its bank and payment gateway balances worth Rs 164.4 crore and crypto assets in pool accounts worth Rs 203.26 crore were frozen. But the real damage is not the frozen assets of the exchange but the reputation loss. In fact, in the more high-profile instance of an ED raid on crypto exchange WazirX, only Rs. 64.67 crore of bank assets could be frozen, whereas the show cause notice issued to the company under the Foreign Exchange Management Act questions it "for allowing outward remittance of crypto assets worth Rs 2,790 crore to unknown wallets". But the reputational damage following the raid has frozen almost all activity on the exchange.

According to the ED, "the exchange has 'actively' assisted around 16 fintech companies under investigation on charges of money laundering to divert their alleged proceeds of crime using the crypto route. The agency probe has found that the exchange has a complicated ownership structure making it 'obscure'. The exchange was in alleged violation of KYC norms and has failed to conduct any enhanced due diligence (EDD) or has raised any suspicious transaction reports (STRs)." This is one more instance of the conduit for flow of proceeds from criminal activity rather than the perpetrators of the activity being made the principal target.

Part of the reason is because the law on online lending by fintech firms is ambiguous, because of the conflict between the need for regulation and the government's commitment to encouraging fintech of various kinds. Till recently the Reserve Bank of India's views regarding online lending were not clearly stated. It was only in November 2021 that the RBI formulated a regulatory framework based on the report of a Working Group on "digital lending including lending through online platforms and mobile apps" constituted for the purpose. It classified the universe of digital lenders into three groups: (1) entities regulated by the RBI and permitted to engaged in the lending business; (2) entities authorized to carry out lending as per other statutory/regulatory provisions but not regulated by RBI; and (3) entities outside the purview of any statutory/regulatory provisions and engaged in lending activities. The RBI's framework recommended that lending using digital lending apps (DLAs) be restricted to regulated entities registered under any law. With regard to the third group of entities, which are the ones involved in the predatory lending scam, the RBI recommended that the government may consider framing legislation for banning of unregulated lending activities and the setting up of a Digital India Trust Agency to verify DLAs. Clearly, as of now that recommendation has not been put into practice. With the law on digital lending unclear, the companies tracked down for illegal online lending practices are being charged under sections relating to extortion, cheating, and forgery of the Indian Penal Code and sections of the Information Technology Act relating to dishonest or fraudulent hacking of a person's computer or of circulating obscene material.

Meanwhile, the threat to the crypto-exchanges has triggered dissension within some of these entities, as former partners want to individually absolve themselves of the responsibility for the transactions being scrutinised by the investigating agencies. This has led to a spat on Twitter between Nischal Shetty, the founder of WazirX and co-founder of Zanmai Labs that originally owned the crypto exchange, and Binance chief executive Changpeng Zhao (often referred to as CZ). In 2019, Binance had reported that it had acquired WazirX from Zanmai. But, following the ED raids, CZ declared that "Binance does not own any stake in Indian cryptocurrency exchange WazirX" and that "Binance does not own any shares in Zanmai Labs, the entity operating WazirX and established by the original founders." In essence Binance was denying any role in WazirX's trading operations. But, Shetty insists that "WazirX was acquired by Binance," and that "Zanmai Labs is a separate entity that has a licence from WazirX (owned by Binance) to operate INR/Crypto pairs on WazirX. Crypto-to-crypto transactions and withdrawals are being operated under Binance through their ownership of WazirX." Shetty wants to hold Binance responsible for the transfer abroad of "the proceeds of crime".

In appears that the absence of clarity on what to permit in the fintech space and how to regulate permitted operators has created a situation where the cryptobusiness is imploding, while the government prevaricates and postpones the decision on what to do with it.

*** This article was originally published in the Frontline Print edition: August 30, 2022.**