Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
April 2022 10(4), 56-70

DIGITAL CURRENCY VS. CRYPTOCURRENCY AND BLOCKCHAIN

Dr. Sarita Mishra Kolhe [1]

[1] Commissioner of Income Tax, Interim Board for Settlement I, II & III, Ministry of Finance, Government of India, New Delhi, India

Received 15 March 2022
Accepted 01 April 2022
Published 03 May 2022

Corresponding Author
Dr. Sarita Mishra Kolhe,
dr.saritamishra9@gov.in

DOI
10.29121/granthaalayah.v10.i4.2022.4528

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Despite the Reserve Bank of India consistently raising concerns over the dangers of cryptocurrencies primarily its use in facilitating money laundering and terror financing–India has emerged as a blossoming crypto market contributing billions of dollars in trading volume. In recent years, though cryptocurrencies have gained momentum with various investors, yet they have not made any significant impact due to the volatility of the transactions. The fact that cryptocurrencies require various kinds of tools like wallets, computer, internet connectivity and various other services, their usage have been restricted to only those who are technologically sound. As a result, a vast majority of the population do not have the technological know-how and hence are unable to use them. Furthermore, the complexities involved in these transactions have lessened their trust and acceptability. One of the major shortcomings is that the cryptocurrency network can validate the payment only but is unable to ensure the delivery of various products and services. Hence, buyer of products and services are helpless as the network does not at the same time, validate both sides of the transactions. The sharp volatility in the value of cryptocurrencies which changes rapidly in a short time period is a major issue due to which, maintaining price stability becomes extremely difficult. Furthermore, the absence of regulatory mechanisms and the decentralized nature of the transactions raises various fears as well as apprehensions that cryptocurrencies may be used for illegal activities. The solution to get over few of the shortcomings of cryptocurrencies lies in the issue of digital currency by the Central Bank. The International Monetary Fund (IMF) has voiced grave concerns due to the risks posed by the cryptocurrencies, mainly in emerging and developing nations and has suggested the need for coordinated action to put in place global standards for cryptocurrencies. The IMF has reiterated that "Determining valuation is not the only challenge in the crypto ecosystem: identification, monitoring, and management of risks which defy regulators and firms are also areas of concern. These include operational and financial integrity, risks from crypto assets exchanges and wallets, investor protection, inadequate reserves and inaccurate disclosure for some stable coins and that capital flow management needs to be fine-tuned to digital currencies." The IMF has further emphasized that "Crypto's cross-sector and cross-border remit limits the effectiveness of national approaches. Countries are taking very different strategies, and existing laws and regulations may not allow for national approaches that comprehensively cover all elements of these assets. Importantly, many crypto service providers operate across borders, making the task for supervision and enforcement more difficult. Uncoordinated regulatory measures may facilitate potentially destabilizing capital flows". In the Union Budget of 2022-23 it has been proposed that, the Reserve Bank of India would be issuing Digital Currency which would go a long way for identifying, monitoring, regulating, management of risks, and capital flow management as well as in mitigating the crisis due to financial instability emanating from the crypto eco-system. Furthermore, a structured taxation regime of 30 % on virtual digital assets, as well as 1 % TDS would have the potency to know the trail of investments or profits generated / losses incurred in this type of trading of virtual digital assets. The issuance of Digital Currency by RBI as well as bringing the same within the ambit of a structured taxation regime would lead to regulation of liquidity as well as volatility and would ensure stability in the economy.

Keywords: Digital Currency, Cryptocurrency, Bitcoin

1. INTRODUCTION

Cryptocurrencies involve transactions which are validated or verified by decentralised nodes in a peer-to-peer electronic payment network like computers. Blockchain is a form of distributed ledger technology which is used to validate payment transactions in cryptocurrencies. Blockchain is a cryptographic mechanism by which information is stored in blocks which are chained together. New data on transactions are filled in blocks which are chained to the previous one in a chronological order in decentralised computer nodes on the network that are outside the purview or regulation of a central authority. This implicates that the payment transactions once made are irreversible and permanently recorded, and no single node can make any changes in the block without a consensus.

1.1. CENTRAL BANK DIGITAL CURRENCY (CBDC)

What is a CBDC? A Central Bank digital currency would be a legal tender to be issued by the Reserve Bank of India but will only be indistinguishable from fiat currency in circulation and tradable on a one-to-one basis. However, a CBDC is distinguishable from Cryptocurrencies like Bitcoin or Ethereum as CBDC's value will be controlled by the Central Bank's sovereign reserves. Virtual currencies do not have any intrinsic value and their markets are often prone to extreme volatility. A CBDC, on the other hand, will function as a stable coin alternative to fiat currency. The concerns on the private virtual currencies are immense with respect to volatility and stability in the economy. A CBDC in contrast, provides significant benefits such as reduced dependency on cash, higher seigniorage due to lower transaction costs and reduced settlement risks. When one pays from one's bank account or digital wallet which stores value corresponding to the actual fiat money, via an electronic transfer mechanism for any product or service, one is basically using digital currency. When one withdraws money from an ATM, the digital currency is turned into liquid cash. CBDC would be a legal tender to be issued by RBI in a digital form. It would be like a fiat currency and would be exchangeable one-to-one with the fiat currency. Only its form would be different being a digital one. As digital currency is the electronic form of fiat money, it is always backed by a centralised authority unlike the Cryptocurrencies. CBDC is a digital currency or virtual currency, but it is not comparable to the private virtual currencies i.e., Cryptocurrencies. Private virtual currencies are different from the usual concept of money. They are not commodities or claims on commodities as they have no intrinsic value. There has been a phenomenal increase in transactions in virtual digital assets in cryptocurrencies. The magnitude and frequency of these transactions have made it imperative to provide for a specific tax regime. Accordingly, for the taxation of virtual digital assets, the Union Budget 2022-23 has proposed that any income from transfer of any virtual digital asset shall be taxed at the rate of 30 per cent. The other salient features regarding taxation of the virtual digital assets are as under:

- There will be no deduction in respect of any expenditure or allowance while computing such income except cost of acquisition. Further, loss from transfer of virtual digital asset cannot be set off against any other income.
- Further, in order to capture the transaction details, it has been proposed to provide for TDS on payment made in relation to transfer of virtual digital asset at the rate of 1 per cent of such consideration above a monetary threshold.

- Gift of virtual digital asset is also proposed to be taxed in the hands of the recipient.

2. CRYPTO TAX AS PER THE BUDGET OF 2022

The Finance Bill, 2022 has proposed a new scheme of taxation of "**virtual digital assets**" **(VDA).** The Bill inter alia has proposed to insert a new section 115BBH in the Income Tax Act, 1961 which provides that where the total income of an assessed includes any income from transfer of any VDA, the income tax payable shall be the aggregate of the amount of income tax calculated on income due to the transfer of any VDA at the rate of 30 %. However, no deduction in respect of any expenditure (other than the cost of acquisition) or allowance or set off any loss shall be allowed to the assessed under any provision of the Act while computing income from the transfer of such asset. Also, no set off any loss arising from the transfer of VDA shall be allowed against any income computed under any other provision of the Act and such loss shall not be allowed to be carried forward to subsequent assessment year(s). The Finance Bill, 2022 has several new provisions pertaining to the new tax on virtual digital assets w.e.f. 1st April 2022. Any transfer of virtual digital asset to a resident will attract 1 % TDS (Tax Deducted at Source). The surplus which is to be computed on a trade in a virtual digital asset has been very briefly stated. The manner in which it will be computed is that the surplus will be carried out or will be worked out only by reducing one item which is the cost of acquisition, which means it is the bare cost of acquisition. It would not include any loadings such as incidental charges, brokerage fees, exchange fees etc. TDS has been the most potent mechanism for the Tax authorities to know the trail of investments or profits generated or losses incurred in this kind of trading. There would be obligation to withhold TDS at the time of payment and not at the time of receipt. In other words, the payer will have to deduct TDS at 1 %. If the exchange bears the responsibility it has to deduct the tax, TDS.

3. CRYTPO TAX AND ITS AFTERMATH

After a 30 % tax on virtual digital assets was announced in the Budget of 2022, the crypto industry and crypto exchanges have rolled out various plans/ financial products to enable investors to navigate volatility and manage taxes efficiently. Cryptocurrency exchange **Coin Switch** in February 2022 has launched a SIP (Systematic Investment Plan) called Recurring Buy Plan for investors which is aimed at users who want to beat high volatility in crypto assets. Fintech SaaS firm **Clear** has launched a crypto tax and portfolio management platform for enterprises and individual users. Clear's initiative is aimed to help the investors with their TDS reporting as well as their taxes and GST level invoices and deposits so as to integrate these with the crypto exchanges. This would enable the investors to get a bird's eye view of the crypto trading, investment and holding patterns which would help the investors to declare their asset-liability and automatic calculation of tax. The investors would have access to the live portfolio performance dashboards and tax reports, would be able to make real-time decisions so as to adhere to the new tax norms.

4. CRYPTO MARKETS IN INDIA

Despite the Reserve Bank of India consistently raising concerns over the dangers of cryptocurrencies – primarily its use is facilitating money laundering and terror financing –India has emerged as a blossoming crypto market contributing

billions of dollars in trading volume. According to some estimates, for the June –July 2021 period the volume of trading across three of the largest India crypto exchanges Wazir X, Coin DCX and Zipay – was pegged at a staggering $ 3.1 billion (Rs.23,000 crore). The fact that cryptocurrencies require various kinds of tools like wallets, computer, internet connectivity and various other services, their usage have been restricted to only those who are technologically sound. As a result, a vast majority of the population do not have the technological know-how and hence are unable to use them. Furthermore, the complexities involved in these transactions have reduced their trust and acceptability. One of the major shortcomings is that the cryptocurrency network can validate the payment only but is unable to ensure the delivery of various products and services. Hence, buyer of products and services are helpless as the network does not at the same time, validate both sides of the transactions. The sharp volatility in the value of cryptocurrencies which changes rapidly in a short time period is a major issue due to which, maintaining price stability becomes extremely difficult. Furthermore, the absence of regulatory mechanisms and the decentralised nature of the transactions raises various fears as well as apprehensions that cryptocurrencies may be used for illegal activities. The solution to get over few of the shortcomings of cryptocurrencies lies in the issue of digital currency by the Central Bank. The real cause of concern is that Cryptocurrencies would interfere with the regulation and coordination by the Central Bank which guides the monetary policy, suggests measures to the Central Govt. regarding incorporating suitable steps / measures so as to safeguard the economic health of the nation. If cryptocurrencies are not regulated, then the Central Bank would have no control/ regulation over the number of cryptocurrencies in circulation this would pose various difficulties for the Central Bank to control inflation and hence the total liquidity in the economy. As cryptocurrencies are global currencies, buying and selling of cryptocurrencies by the Central Bank to regulate liquidity would also not help. Their regulation in one country can affect their circulation and use in other countries and destabilise various activities outside the targeted economy. The solution to overcome some of the problems of cryptocurrency is the issue of digital currencies by the Central Bank which has been proposed by the Union Budget 2022-23.

5. CRYPTOCURRENCIES

Cryptocurrencies are in essence a Ponzi scheme which holds the promise of alchemy turning lead into gold that appears bewitching. They are seductive with their get-rich-quick schemes in which seven out of ten vulnerable consumers lose their money / virtual assets. Cryptocurrencies are a dangerous and retrograde bait for gullible and vulnerable consumers. Cryptocurrencies are today's South Sea Bubble- one of the earliest recorded financial bubbles that took place in 1720's Britain, which was intended to raise money "for carrying on an undertaking of great advantages but none knowing what it is". Cryptocurrencies if unregulated would only reap financial disaster. The financial disasters are to be avoided at all costs as they lead to poverty and inequality.

The current system is highly vulnerable to cyberattacks because money is little understood. History is witness to the fact that private money or money tied to a rigid formula in the 19th century was marked with frequent financial instability and little or no growth (pedestrian growth). In order to bring stability, the **Gold Standard** was adopted but after 50 years it was abandoned when it deepened and spread as the **Great Depression**. As compared to these cryptocurrencies, the benefits of regulated fiat money are numerous as it has been associated with far more growth,

is much more distributed and has led to more growth and stability than that of the Gold Standard era. Cryptocurrencies are a retrograde step socially, politically, and economically. Cryptocurrencies cannot kill inflation, moreover it is anti-democratic which has led RBI to voice its strongest concern.

While cryptocurrency is often associated with shady deals on the dark web, it is a digital form of money that anyone can use. It is virtually immune from counterfeiting or governmental interference, but the main appeal is the potential profit from trading it, making cryptocurrency more commodity than cash. There are more than 7,000 kinds of cryptocurrencies, most popular being Bitcoin. The value of Bitcoin has grown nearly 12,000 percent over the past five years. In order to trade in cryptocurrency, one would need an individual investment account with a crypto-exchange. Popular exchanges include **Coinbase**, **Kraken** and **Gemini** all of which charge fees just as traditional brokerages do. Another key difference is that investors are responsible for storing their cryptocurrencies, which is easier said than done. Because the coins aren't insured, one would lose them (**through theft, system failures or simply by forgetting one's key code to access them**) and thus lose one's investment. Once cryptocurrency is lost, it is nearly impossible to recover, which then makes the remaining accessible coins even more valuable. The way to store cryptocurrency is in a digital wallet. These wallets can either be '**hot**' (meaning that they're stored online), '**cold**' (stored on an external device that isn't connected to the Internet). Cold wallets are more secure since hackers can't use the Internet to access them. Until now, cryptocurrency was neither formally recognised nor regulated, in India. In the 2022 budget, however, it has been proposed to tax all '**virtual assets**', which includes cryptocurrency at 30 percent. Additionally, one percent of tax will be deducted at source (TDS) on these investments.

6. BLOCKCHAIN TECHNOLOGY

"All blockchains are distributed ledger but not all distributed ledgers are blockchain.'' Blockchain is a specific type of distributed ledger with a distinct set of features or operational processes. Often blockchain is confused with DLT, but the former is nothing but a subset of the latter. A blockchain is a sequence of blocks, whereas a DLT does not need such a chain. One of the earliest mentions of the blockchain technology can be found in a paper written by Satoshi Nakamoto as to how financial transactions can take place without the need for centralized financial institutions. In his paper "**Bitcoin: A peer-to peer Electronic cash system**", Nakamoto (2008) talks about a peer– to peer node system in which transactions taking place on digital forum are to be verified by other nodes, thus creating an immutable system under which the transactions are made public. Changes in a blockchain is possible only if the other nodes verify such change, which is logically hard to achieve. Once a block of information gets hashed in the blockchain, tampering with it is next to impossible. However, there have been many instances where blockchain-run system has been attacked.

7. CRYPTO MARKET SUFFERS $ 1 TRILLION LOSS AS BITCOIN CRASHES GLOBALLY

As per reports, Bitcoin along with other digital cryptocurrencies crashed to its lowest level in last week of January 2022 and wiped out over $ 1 trillion from the global crypto market. Other digital currencies, **Ethereum**, **Finance Coin** and **Cardano** also witnessed similar meltdowns. Crypto assets such as Bitcoin have raised financial stability concerns. According to **IMF research**, "Given their high

volatility and valuations, cryptocurrencies could soon pose risks to financial stability. It is high time to adopt a comprehensive coordinated global regulatory framework to guide national regulation, supervise, so as to mitigate the financial stability risks stemming from the crypto ecosystem. The retail and institutional investors need to exercise caution in this regard."

8. SHORTCOMINGS

Some of the major shortcomings of Blockchain and Cryptocurrencies are as under:

8.1. IMMUTABLE CHARACTERISTICS

One of the shortcomings, of a blockchain is its immutable characteristic. The fact that every transaction under a blockchain needs to be verified creates an immutable system; So, if a mistake is committed by any of the nodes in making a payment to an individual, and once it has been validated, there is no going back for the transaction. That does not happen in a three-party transaction system, mostly including a bank, where a bank takes care of the transaction and also provides the means of delegitimising a transaction if a genuine mistake has been committed on behalf of the customer.

8.2. PRIVACY ISSUES

The other shortcoming of cryptocurrency lies in its open- ended ledger that can easily be a gateway of understanding someone's transacting pattern, more specifically the behaviour-mining. Anyone who creates a wallet through a platform is laying a root to the origin of the transactions as to where it originated. Creation of a digital wallet requires an email ID, thus also exposing the internet protocol address of the user, thereby the nodes.

8.3. STABILITY

The idea of a **''fiat currency**'', which means currency backed by a government promise, stands in contrast to the **''commodity currency**'' backed by some physical substances such as gold or silver. In today's world, most of the Government have fiat currency, and the Government's promise of backing the currency gives it a legitimate existence. Coming to cryptocurrency, it too is not backed by any substance and the use of cryptocurrency does not per se bring in the required stability and security. Governments across the globe have been using the argument of volatile nature of cryptocurrency as the reason for not recognising it. The '' Cryptocurrency and Regulation of Official Digital Currency '' Bill, 2021 to regulate the working of cryptocurrency which is yet to be finalised would be a step forward till a comprehensive, coordinated global regulatory framework is put in place to diminish and alleviate the financial stability risks stemming from the crypto eco-system. Since 2013, the RBI has taken a dim view of cryptocurrencies. RBI's concerns on cryptocurrencies by comparing them to Ponzi Scheme and that private cryptocurrency could wreak havoc on India's currency, banking system and the government ability to effectively monitor and regulate the economy are valid. As cryptocurrencies are devoid of underlying cash flows, they have no intrinsic value hence they pose a risk to financial sovereignty. One of the chief concerns of the RBI stems from the degree of anonymity that cryptocurrencies facilitate. The concerns of RBI seem legit.

9. DATA PROTECTION REGIME IN INDIA

India does not have any specific legislation for data protection. It only has the Information Technology Act (2000) (IT ACT), which is also applicable for validating e–transactions. The applicability of the IT Act to blockchain is questionable. The Information Technology Act is applicable only on an intermediary (favoring a three-party structure), which again is in contrast to the blockchain technology (a peer-to-peer structure). However, the Information Technology (Reasonable Security Practices and Procedures and Sensitive personal Data or information) Rules, 2011 made in pursuance of Section 43A (7) of the IT Act might have some relevance. The rules were made for monitoring the practice of data profiling done at different stages and were more of a nascent attempt at data protection but again as Section 43A is governed by the IT Act, it also suffers from the same lacunae of three- party structure and the jurisdictional limits of the IT Act.

10. CRYPTOCURRENCIES: TIMELINES OF EVENTS IN INDIA

In India, Cryptocurrency came into light in 2013, when a restaurant in Mumbai announced that it was accepting payments in Cryptocurrencies. In the year 2013, cryptocurrency exchange **Uno coin** was launched, making it accessible for Indians to buy and sell Bitcoin. Bitcoin price rose from $ 100 to $1000 in 2013. The RBI issued an advisory against Cryptocurrencies, warning the public against its use. The RBI stated, "Virtual Currencies are not backed by a Central bank and their value isn't underpinned by an asset and thus a matter of speculation." Between 2012 and 2017, Cryptocurrencies had started to gain momentum. The price of Bitcoin reportedly touched $ 20,000 in 2017, from a mere $ 5 in 2012. In 2018, the RBI made an announcement restricting banks from dealing in Cryptocurrencies or providing any services to anyone dealing with Crypto exchanges. This hit the industry and exchanges hard, as prices of Cryptocurrencies plummeted. A Government formed committee issued its report in July 2019, proposing a complete ban on Cryptocurrencies. The Honourable Supreme Court of India in March 2020 nullified the RBI's circular and subsequently the ban. Revoking the ban, the Supreme Court stated that while Cryptocurrencies are unregulated, they are not illegal in India. The price of Bitcoin reportedly jumped more than 700 % between April 2020 and February 2021. While the industry has expressed that cryptocurrency should be brought under a structured taxation regime, the RBI is in favour of a complete ban on cryptocurrencies. The year 2022 started with global cryptocurrency super app, **Crypto wire** launching a crypto index in India, known as **IC 15**, the index reportedly aims to monitor the performance of the 15 most traded Cryptocurrencies, listed on leading exchanges in the world.

11. STABLE COINS

The escalation in volatility of **Bitcoin** and other altcoins like **Ethereum, Solano, Polkadot** and **Shiba Inn** has pushed Indian crypto Investors towards stable coins that are comparable to real world currencies like US dollars. Stable coins have been a major point of discussion through much of 2021, especially the ones pegged to the US dollar, and researchers have opined that the total supply of US dollar stable coins is now touching $ 140 Billion. The RBI has cautioned investors against stable coins, stating that any Cryptocurrency assets pegged to the US dollar would be a threat to the Indian Rupee. The RBI is of the view that stable coins if allowed in India could impact the RBI's ability to control currency fluctuations and volatility. Experts are

of the view that RBI's concerns seem legit. It is feared that wider adoption of such dollar or gold-pegged digital assets for domestic payments could have repercussions outside the control of the Central Bank. Global regulatory agencies are struggling to churn out rules regarding stable coins as they are more volatile as compared to fiat currencies due to demand and supply dynamics. The **Blockchain and Crypto Assets Council (BACC)** is of the opinion that digital tokens should not be banned but should be regulated. However, RBI has voiced its strong disagreement with Cryptocurrency trading, dubbing it a threat to the financial stability of the country, since they are unregulated.

12. IMF: COORDINATED ACTION TO PUT IN PLACE GLOBAL STANDARDS FOR CRYPTOCURRENCIES

The International Monetary Fund (IMF) has voiced grave concerns due to the risks posed by the cryptocurrencies mainly in emerging and developing nations and has suggested the need for coordinated action so as to put in place global standards for cryptocurrencies. The IMF has reiterated that "Determining valuation is not the only challenge in the crypto ecosystem: identification, monitoring, and management of risks which defy regulators and firms are also areas of concern. These include operational and financial integrity, risks from crypto assets exchanges and wallets, investor protection, inadequate reserves and inaccurate disclosure for some stable coins and that capital flow management needs to be fine-tuned to digital currencies." The IMF has further emphasized that "Crypto's cross-sector and cross-border remit limits the effectiveness of national approaches. Countries are taking very different strategies, and existing laws and regulations may not allow for national approaches that comprehensively cover all elements of these assets. Importantly, many crypto service providers operate across borders, making the task for supervision and enforcement more difficult. Uncoordinated regulatory measures may facilitate potentially destabilizing capital flows".

13. CRYPTO AIRDROP

An airdrop involves giving out free coins or tokens issued by a Crypto company or platform to establish crypto holders, usually in exchange for marketing-related tasks such as blog posts or promotional content or social media. It is always prudent to approach an airdrop critically, since the tactic has been previously used by malicious actors to dupe crypto users out of their coins or tokens, users in order to receive their coins or tokens are required to have wallets based on the same blockchain as that being used by the platform for instance, **My Ether Wallet** is used for coins or tokens built on the **Ethereum** blockchain.

Why should the Crypto users be careful about Airdrop?

- A scam artist may send malicious tokens to a particular set of users to spur their curiosity. When these users seek out what these tokens are on the internet, they will, inevitably, be directed to the scammer's website and could fall prey to phishing schemes.
- In other cases, scammers may request users to transfer some of their own Cryptocurrencies to a wallet, promising a transfer of new tokens.
- Another red flag to exercise caution is if the airdrop amount is extremely high.
- Users are advised to conduct their own background research around specific Crypto platforms before engaging in an airdrop.

- The lure of free tokens or coins from a platform that could explode in value can be difficult to quell but staying vigilant will ensure that the Crypto user's holdings are not compromised.

14. CYBERATTACKS ON CRYPTOCURRENCY

The instances of cyberattacks on cryptocurrencies is on the rise globally. As per news reports, cryptocurrencies valued over $ 326 million were stolen from, the Blockchain bridge **Wormhole,** a platform that allows users to transfer Cryptocurrencies across different blockchains. Further, cryptocurrencies worth $ 80 million were stolen from **Qubit Finance**, a **decentralised finance (DeFi)** platform. According to **Cyrptobriefing,** since the launch of **Binance Smart Chain (BSC)** in 2020, several DeFi projects have faced cyberattacks and hacking including a $ 50 million hack from **Uranium Finance** in April 2021, and $ 88 million hack from **Venus Finance** in May 2021. The greatest security concern for many people investing in Cryptocurrencies is the risk of Hacking and fraud. Crypto scams have become common these days. According to reports, scammers posing as Elon Musk have stolen over Rs 14.63 crore in digital currencies since October 2020. Also, crypto crimes involve scammers requesting payment in Cryptocurrency or sending unsolicited offers to persons to make money or increase their holdings.

In the largest incident of cryptocurrency theft, Hackers have allegedly stolen more than $ 600 million in Cryptocurrencies, having breached the blockchain-based platform, **Poly Network** and extracted thousands of tokens. Poly Network took to Twitter to confirm the breach, saying "We are sorry to announce that # Poly Network was attacked on @ **Binance** chain @ **Ethereum** and @ **Ox polygon**". Poly Network is a decentralised finance (**DeFi**) platform i.e., it acts as a financial application that runs on blockchain technology that aims to cut out intermediaries like brokerages and exchanges in enabling cryptocurrency holders to convert tokens from one currency to another. Poly Network has also urged cryptocurrency exchanges to 'blacklist tokens' from the IP addresses found to be linked to the Hackers. As per news reports, **Tether**, the company responsible for the world's third largest cryptocurrency by (market capitalisation) has frozen $ 33 million in USDT tokens related to the hacker's wallet addresses, according to the Chief Technology Officer of Tether. Blockchain- based security firm, **Slow Mist** has issued a statement claiming that it had identified the hacker's email, IP address and device fingerprints and that it was working on uncovering further forensic clues. Although the Poly Network hack is the largest Cryptocurrency hack, it is by no means the first. According to cryptocurrency compliance outfit **Cipher Trace**, DeFi-related hacks have totalled roughly $ 361 million USDT between the start of 2021 to July 2021. This amounts to a three-fold increase from 2020. DeFi fraud have also escalated during the period (July 2021 to January 2022) which accounted for 54% of all crypto frauds compared to 3 % in 2020.

15. CRYPTOCURRENCY THEFT IN THE US

The US Department of Justice has made arrests in the biggest cryptocurrency theft worth $ 4.5 billion. In 2016, **Bitfinex**, one of the largest cryptocurrency exchanges at the time was hacked, with Hackers stealing roughly $ 70 million worth of Bitcoin. The value of the stolen bitcoin has since risen to $ 4.5 billion. In order to be anonymous in cyberspace the Hackers laundered stolen funds through a maze of cryptocurrency transactions. The Hackers infiltrated the Bitfinex exchange platform and laundered Bitcoins through over 2000 unauthorised transactions. Through

these transactions, the stolen cryptocurrencies were sent to a digital wallet operated by the Hackers. In the five years that followed, the Hacker couple transferred roughly 25000 of the stolen Bitcoin out of the wallet into other financial accounts through a convoluted money laundering process. The remaining 94,000 Bitcoin remained in the original wallet. The criminal complaint claimed that the hacker couple made various fictitious identities to set up financial accounts, employed software to automate quick transactions, deposited funds into different cryptocurrency exchanges and used the darknet markets to withdraw funds. In a process known as '**chain hopping**', the two allegedly also converted "bitcoin to other forms of virtual currency including "**Anonymity-Enhanced Virtual Currency (AEC)**". As the criminals always leave some clues, the FBI Investigative teams were able to uncover the sources of even the most sophisticated cyberattack scheme in the above case.

16. OPEN SEA PHISHING ATTACK

One of the largest global non-fungible token marketplaces, **Open Sea** found itself at the centre of a public relations storm, when reports emerged of a hack that saw nefarious actors walking away with $ 1.7 million worth of NFTs. In the Open Sea case, the perpetrators exploited a flexibility in the **Wyvern protocol**, an open-source standard upon which most NFT smart contracts are made. The targets of the attacker were tricked into signing partial contracts with a general authorisation, leaving several positions empty. Once they had the signature, the attackers then filled in the contracts to include a call to their own contract, facilitating the transfer of ownership of NFTs without any payment. To put it in layman's terms, the targets were essentially fooled into signing a blank cheque which the attackers then filled in, giving them access to their digital assets. The timing of the attack is also significant. Open Sea was in the process of updating its contract protocol when the attack happened. Taking advantage of the small window offered to users to update their accounts, the attackers reportedly, sent a false link claiming to be an Open Sea upgrade to their attackers. The latest attack is yet another example of the vulnerabilities that continue to prevail in the NFT ecosystem. Open Sea itself was the subject of a report from cybersecurity firm **Check Point** in October 2021, that flagged a platform vulnerability that allowed actors to create a malicious NFT, gift it to targets, gain permission to access their wallets and claim ownership of their holdings. Phishing attacks are also not the only way attackers can exploit users among these communities. In December 2021, a fake bot was found to have stolen digital assets worth $ 15,00,00 from a Discord server seen by another NFT marketplace **Fractal**. Additionally, malicious actors have often posed as fake buyers or sellers to secure access to a target's wallet during the transfer of NFT ownership.

As per news reports,

- Cyberattacks on Indian Cryptocurrency exchanges have been doubled in recent months.
- Criminals use DDoS and Social Engineering attacks to gain access to the Wallets of Investors and exploit vulnerabilities in security architecture of exchanges.
- Exchanges are rushing to strengthen their frameworks, systems, and protocols so as to build defences against such sophisticated attacks.

As prices of cryptocurrencies rise, exchanges are facing increased attacks from Cyber crooks and Hackers to get inside their systems. Criminals are using clever tactics like impersonating or spoofing social media profiles in order to deceive

investors and sneak into their Cryptocurrency Wallets. Not just Cryptocurrency investors, Cybercriminals are also increasingly attacking Cryptocurrency Exchanges. Such attacks have doubled in recent months with digital coins touching all-time high levels. Cryptocurrency Exchanges are placing robust frameworks, systems, and protocols to insulate themselves from such rising threats. According to an Economic Times report, one of the largest Cryptocurrency Exchanges in India **Zeb pay** faces at least two Sophisticated **Distributed Denial of Service (DDoS)** attacks whereby crooks try to overwhelm the exchange's system to disrupt service or search for vulnerabilities. However, more sophisticated of the lot are security threats emanating from fraud from a combination of **Social Engineering and Computer Intrusion**. The frequency of such attacks is increasing. According to the Chief Technology Officer at Zeb pay "**Zeb pay is constantly under attack. Whether it is from white-hat hackers to find issues they can submit to our bug-bounty programme or nefarious black-hat hackers trying to overload our system to cause disruptions and find holes in our defences. As Cryptocurrency becomes more mainstream, the frequency of these attacks is increasing, meaning we must develop more sophisticated methods to quickly identify and neutralise them"** Some exchanges have even reached out to their lawyers on the way forward in case their customers are duped of their investments through such frauds.

17. THREATS TO INDIA'S CYBERSECURITY

India as one of the fastest growing markets for digital technologies fuelled by the **Digital India Mission,** has in the past five years seen rapid adoption of Digital Technology in various areas like, creation of broadband highways, Digi Lockers and in various schemes under the aegis of **e-governance**. Presently, India has as many as 1.15 billion mobile phones and 700 million internet users making it a large pool of targets who are digitally vulnerable. The pandemic has only compounded this problem due to heavy dependence on these digital technologies. Due to the Pandemic induced lockdowns, people have resorted to online payment, e-shopping, WFH which have led to greater adoption of interconnected devices and hybrid work networks. Against this rapid expansion of digital assets and dependence on digital technology, there have also been a meteoric rise in cyber-attacks by various malicious actors and adversaries. The rise in cyberattacks on electricity grids and financial institutions have highlighted the potentially grim and dangerous scenarios. There are a variety of Cyber threats the notable ones include i) Malware, Viruses, Trojans, Spywares, ii) Backdoors, which allow remote access, iii) DDoS (Distributed Denial of Service), which floods servers and networks and makes them unusable, iv) DNS (Domain Names System), poisoning attacks, which compromises the DNS and re-direct websites to various malicious sites.

18. CHALLENGES FOR A COHESIVE CYBERSECURITY POLICY

There are several challenges to a cohesive Cybersecurity Policy. The problem stems from the use of hardware and software being of foreign origin, terabytes of data that is parked on servers outside India which compounds the grim situation and lead to a slew of hurdles for the lawmakers while trying to draw up concrete policies. Additionally, the fast-paced digitisation in almost every sector has led to an increase in the collaboration with application service providers, so as to avail of the best apps and services in the shortest possible time. However, the requisite attention to the security aspects as well as a cautious approach is often neglected and missed in the process. Furthermore, various infrastructure that needs to be

under the ambit of the law belongs to the private sector, which make it difficult for the lawmakers to implement policies so as to secure the digital environment.

19. THE PATH AHEAD

There is a need for a central coordinating agency which would enforce laws strictly and penalise entities if they do not comply with cybersecurity norms and which do not take the requisite steps and safeguards to secure the cyberspace. This approach would be very much akin to what the RBI does with Financial Institutions and Banks. A National Cybersecurity Cell can leverage the resources (both for the Centre and the States) so as to tackle the threats and breaches. There is a need for the government, business organisations, companies as well as other entities to create defences against acts of cybercrime by educating their employees to be vigilant and avoid becoming vulnerable targets for cyber-criminals. There is an urgent need for strict guidelines and SOPs which can be put in place for all the entities, so as to have a proper threat analysis and which would help in building increased awareness about the risk factors and make an honest analysis of an organisation's preparedness in the event of a breach by the cyber-criminals. India needs a robust cybersecurity strategy that safeguards government systems, citizens, and the business ecosystem. These measures if implemented appropriately with proper checks and balances would not only help protect the citizens from cyber-threats, but also boost investor confidence in the economy. Furthermore, there would be generation of employment opportunities in the field of cybersecurity for those persons who successfully complete a certified programme in cybersecurity so as to take up the role of cybersecurity expert as well as various other jobs such as that of a cybersecurity analyst, network security specialist, cybersecurity manager, cybersecurity architect and other C-suite positions such as Chief Information Security Officer etc.

20. SMART TIPS TO PROTECT AGAINST CRYPTO FRAUDS

The rapid growth of various cryptocurrencies such as **Bitcoin**, **Ethereum** and **Dogecoin**, have attracted many new investors to join the crypto bandwagon. Being unaware of the blockchain and crypto technologies, new investors or prospective investors can always become subjects of scams. Due to non-existence of a regulator to govern the functioning of cryptocurrency exchanges, new investors can fall prey to fraudsters and scamsters. Below are listed few smart tips to protect oneself from fraudsters.

- As there are many fake apps, having closed resemblance with legitimate cryptocurrency apps, it is always advisable to watch and observe the ratings, customer reviews, as well the authenticity of the logo, to weed out the fake apps from the real ones.
- It is advisable to double-check the websites and their URL's. Spoofing is one of the most common technological attacks which is prevalent even in the world of cryptocurrency. One needs to be doubly certain/sure that one is making transactions only on recognised, secured and approved platforms. Even while following a link, care should be taken that the user/person is not being redirected to a fake site by the fraudsters.
- It is advisable to avoid an offer which is too good to be true. If any deal which promises the returns manyfold with no real explanation in sight, there are chances that one is buying into a scam. It is advisable to skip such deals.

- Fraudsters often use various modus operandi and strategies to trick the users by sending phishing e–mails that exactly look like an official communication from a credible cryptocurrency site or exchange. Such emails often give money-spinning offers and deals to trap the users.
- There is a need to double – check the phone number, social media handle or email– id that are being used to contact the person, or the contact which one uses for availing technological support and troubleshooting.

21. TAX IMPLICATIONS OF CRYPTOCURRENCIES IN INDIA

There is a difference of opinion among tax experts as to whether the returns from crypto assets must be categorized as capital gains or business income.

In the Indian Context, Cryptocurrency exchanges have to be mandated to share their KYC data with the regulators and Government agencies including the SEBI, RBI, and the Income Tax Department. The KYC data could help regulators to zero in on transactions across platforms, check that against bank deposits and even calculate or scrutinize gains and other discrepancies. Several investors in Cryptocurrency operate through multiple accounts not just across platforms, but even with multiple banks and NBFCs where their money is eventually deposited. Some investors in India are already paying Capital Gains Tax on income from Cryptocurrencies. As per the new Income Tax Declaration forms, taxpayers are required to disclose all their assets to the Income Tax Department in India. Any potential cryptocurrency framework should be formed after consulting all stakeholders amid an evolving global consensus on the matter. A structured taxation regime of 30% on virtual digital assets as well as 1 % TDS would mitigate the financial stability crisis and would go a long way in identifying, monitoring, regulating, and tracking of investments.

22. CONCLUSION

In recent years, though cryptocurrencies have gained momentum with various investors, yet they have not made any significant impact due to the volatility of the transactions. The fact that cryptocurrencies require various kinds of tools like wallets, computer, internet connectivity and various other services, their usage have been restricted to only those who are technologically sound. As a result, a vast majority of the population do not have the technological know-how and hence are unable to use them. Furthermore, the complexities involved in these transactions have lessened their trust and acceptability. One of the major shortcomings is that the cryptocurrency network can validate the payment only but is unable to ensure the delivery of various products and services. Hence, buyer of products and services are helpless as the network does not at the same time, validate both sides of the transactions. The sharp volatility in the value of cryptocurrencies which changes rapidly in a short time period is a major issue due to which, maintaining price stability becomes extremely difficult. Furthermore, the absence of regulatory mechanisms and the decentralised nature of the transactions raises various fears as well as apprehensions that cryptocurrencies may be used for illegal activities. The solution to get over few of the shortcomings of cryptocurrencies lies in the issue of digital currency by the Central Bank. The sharp volatility in the value of cryptocurrencies over relatively short period of time are a major issue due to which, maintaining price stability becomes extremely difficult. Furthermore, the absence of regulatory mechanisms and decentralised nature of the transactions raises various fear and apprehension that cryptocurrencies may be used for illegal activities. The

solution to get over some of the shortcomings of cryptocurrencies is the issue of digital currency by the Central Bank. In the Union Budget of 2022-23 it has been proposed that, the Reserve Bank of India would be issuing Digital Currency which would go a long way for identifying, monitoring, regulating, management of risks, and capital flow management as well as in mitigating the financial stability crisis stemming from the crypto eco-system. Furthermore, a structured taxation regime of 30 % on virtual digital assets, as well as 1 % TDS would have the potency to track investments or profits generated/ losses incurred in this type of trading of virtual digital assets. The issuance of Digital Currency by RBI as well as bringing the same within the ambit of a structured taxation regime would lead to regulation of liquidity as well as volatility and would ensure stability in the economy.

REFERENCES

Avinash, D. (2022). Economic and Political Weekly, 11(7). https://www.epw.in/

Data Protection Regulation in India (2022). Economic and Political Weekly of 2021 and 2022.

Elon Musk (n.d.). CEO and Chief Engineer of SpaceX, CEO and product architect of Tesla, Inc. Founder of The Boring Company and X.com (now part of PayPal), Co-founder of Neuralink, OpenAI, and Zip2, President of Musk Foundation

Garg, S.C. (2019). Report of the Committee to propose Specific Actions to be Taken in Relation to Virtual Currencies. https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf

Haber, S and W. S. Stornetta (1991). How to Time -Stamp a Digital Document," *Journal of Cryptology*, Vol 3, No 2 https://www.anf.es/pdf/HaberStornetta,

Information Technology Act, (2000). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Irina, B. P, Adriana, D. (2020). Blockchain- the accounting perspective, Proceedings of the International Conference on Business Excellence. https://www.researchgate.net/publication/343703545_Blockchain_-_the_accounting_perspective#:~:text=This%20paper%20explores%20the%20potential,to%20enhance%20the%20accounting%20activity.

Avinash, A. (2021). Cybersecurity and Data Protection Regulation in India: An uneven Pathwor. Springer Science and Business Media LLC. https://link.springer.com/chapter/10.1007/978-3-030-56405-6_4

Kuner, C. (2018). Blockchain versus Data Protection," International Data Privacy Law, 8(2). https://academic.oup.com/idpl/article/8/2/103/5047578?login=false

Ministry of Communications and Information Technology Information Technology (2011). (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011," Notification No GSR 313(E), 11 April.

Nakamoto, S. (2008). Bitcoin A Peer- to peer Electronic Cash System. file:///C:/Users/lenovo/Downloads/21260-bitcoin-a-peer-to-peer-electronic-cash-system%20(1).pdf

Regulations (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union.

https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679

Supreme Court of India, (2017). Judgment of 24 August 2017, Justice K S Puttaswamy (retd) v Union ofIndia, Case No WP(C) N0 -000494-000494/2012, H= https://sci.gov.in/pdf/LU/ALL%20to%20 to Privacy pdf