INDEX

ANKIT VERMA ADVOCATE
Email- advocateankit.v@gmail.com
Contact no - +91-9999197883.

Ch No. 3, Patiala House Court,
New Delhi -110001.
Office at:- GL-5, Ansal Bhawan,
K.G. Marg, New Delhi -110001.

To,

07.11.2023

Mr. R. Venkataramani
Attorney General of India
Supreme Court of India
New Delhi -110001.

Sub- Sharing my views/Opinion regarding Whether Cryptocurrency should be regulated in India or not in the matter of W.P (Crl) no. 15 of 2023 Titled as Ganesh Shiv Kumar Sagar vs Union of India & ors.

Respected Sir,

I, Ankit Verma Advocate counsel in the above captioned matter request you examine my sense of knowledge for regulating cryptocurrency in India. You being a highest law officer of this land may also concern about Crypto regulation in India. Thereafter I also being a citizen and a law officer also deeply concern about scams or manipulation being done in India in non-identical forms of Schemes in cryptocurrency in India. Before going into the aspect of Cryptocurrency we need to understand the technology, the history of the technology and future of the technology.

INTERNET -A DECENTRALIZED SYSTEM

Decentralization means the Internet is controlled by many. Its millions of devices linked together in an open network. No one can own it, control it, or switch it off for everyone.

The Internet and the World Wide Web remain the biggest decentralized communication system humanity has ever seen. This was very much a part of the design: the inventors of the Web wished for all people to be able to create and access information.

But the benefits of a decentralized Internet are eroding. When we concentrate our online activity on just a few social networks and messaging apps – as billions of us do – it narrows our experience of the Web to one where we are pointed only at content that appeals to our likes in search results and social media streams. Here, we are consumers rather than creators.

The Internet remains decentralized, but the things we do on it every day are controlled by just a handful of global technology giants. The companies are starting to look more and more like monopolies of the past. Given the importance of the Internet in our lives, this is not healthy.

Now, we need to understand the evolution of internet and various versions of webs, which have evolved over period of time. Since, cryptocurrency is a key feature of WEB.3.0.

WEB 1.0, WEB 2.0 AND WEB 3.0

Web 1.0[1] is the ancestor of the internet that we use today. It was a static web, where users could only read or view the content and had no ability to interact with it. Websites were designed using HTML and CSS, and it was a one-way communication with web pages composed of plain text and images. There was no database connectivity and the pages were not interactive. The search engines

[1] https://www.linkedin.com/pulse/evolution-internet-web-10-20-30-deepak-lyngdoh

of this time like Yahoo operated as web directories as they were manually analyzed and categorized by human editors.

WEB 2.0

Web 2.0 websites are more dynamic, collaborative and feature-rich. With Web 2.0 sites, one can do so much more online than anyone could before. Sites such as Wikipedia, Facebook, YouTube, and Twitter are all examples of Web 2.0 sites. They are built with the user in mind, allowing the user to easily create, collaborate and share content. But what distinguishes Web 2.0 from its earlier counterpart. Web 2.0 uses dynamic content, whereas Web 1.0 uses static content. Web 2.0 also encouraged participation and collaboration with other users, allowing for more user-generated content. Web 2.0 sites are also characterized by their use of open-source software and web applications that operate without the need to install software on a user's device. This allows for increased convenience and mobility, as the user can access their accounts on other devices. Overall, Web 2.0 has revolutionized the way we interact online. From social media to job networking, e-commerce, and digital marketing, Web 2.0 sites have transformed the internet landscape beyond recognition.

WEB 3.0

Web 3.0 is characterized by machine-based intelligence, natural language processing, and ontology-based metadata. It uses web crawling and other types of artificial intelligence to create comprehensive databases of information that can be easily accessible and understandable by machines. The technologies that power Web 3.0 include Blockchain, Artificial Intelligence, and the Internet of Things. Blockchain technology is used to create a secure and decentralized database that eliminates the need for intermediaries in transactions. AI is used in various forms such as chatbots, voice assistants, and image recognition to improve search results and provide a more personalized experience for the user.

Web 3.0 sites provide more sophisticated applications that can integrate with various devices, browsers, and even web services.

KEY FEATURE OF WEB 3.0 ARE AS FOLLOWS:

Several key Web 3.0 features define what this third generation of the web will likely be all about:

Decentralized Unlike the first two generations of the web, where governance and applications were largely centralized, Web 3.0 will deliver applications and services through a distributed approach that doesn't depend on a central authority.

Blockchain-based Blockchain decentralization is the enabler for Web 3.0's distributed applications and services. With blockchain, data is managed and validated on a broadly distributed, peer-to-peer network. Blockchain also employs a theoretically immutable ledger of transactions and activity, which helps to verify authenticity and build trust among blockchain participants.

Cryptocurrency-enabled Cryptocurrency is a key feature of Web 3.0 that is expected to largely replace the "fiat currency" issued by government central banks.

Semantically organized The idea behind the Semantic Web is to categorize and store information in a way that helps "teach" an AI-based system what data means. Websites will be able to understand the words in search queries the same way a human would, enabling them to generate and share better content.

Autonomous and artificially intelligent:- More overall automation is a critical feature of Web 3.0, and it will largely be powered by AI. Websites equipped with AI will filter through and provide the data individual users need.

INTRODUCTION OF CRYPTOCURRENCY

A virtual currency is a digital representation of value only available in electronic form. It is stored and transacted through designated software, mobile, or computer applications. Transactions involving virtual currencies occur through secure, dedicated networks or over the Internet. They are issued by private parties or groups of developers and are mostly unregulated. Virtual currencies are a subset of digital currencies and include other types of digital currencies, such as cryptocurrencies and tokens issued by private organizations. The advantages of virtual currencies include faster transaction speeds and ease of use. The disadvantages of virtual currencies are that they can be hacked and do not provide much legal recourse to investors because they are not regulated.

As an Individual user, one can get started with Crypto currency without understanding the technical details. Once you've installed a Crypto wallet is installed in computer or mobile phone, it will generate your first wallet address and you can create more whenever needed. One can disclose his/her addresses to anyone so that they can pay or vice versa and the cost of the transaction is low. In crypto wallets a user can only store Digital currencies.

i. **Decentralized Digital currency** :

Cryptocurrencies are, by their nature, decentralized forms of money. That's because the work required to validate transactions is performed by a network of anonymous users from across the world. It is very difficult for a single entity to exert influence over the network, meaning that the

whole thing is leaderless. Decentralization is at the opposite end of the spectrum of the Centralized coin like the Canadian or US dollar. over which governments maintain monopolies.

ii. **Centralized Crypto Exchange :**

Centralized Digital Currency: A centralized cryptocurrency exchange is a site that maintains an orderbook and holds reserves within its own vaults. Examples of centralized platforms include Coinbase. Binance. and kraken. A decentralized crypto exchange, or DEX, is a protocol for swapping coins that doesn't take control over your funds. DEXes run entirely on computer scripts and decentralized governance. Decisions are not made by companies and their executives.

Centralizing comes with legal risks for the developers. The Centralization reserves controlled by the companies, not by code. Some coins are controlled and stable coins like USDT (TETHER) and USDC is a frequent source of tension for the Cryptocurrency market. TETHER i.e. USDT is a Cryptocurrency is a stable coin, launched by the company namely Tether limited inc.in 2014. Tether is used to trade other Decentralized cryptocurrencies like Bitcoin. The USDT (Tether) is not fully backed by fiat reserves, despite false claims by the company to the contrary. The USDT (Tether) has failed to present audits showing that the amount of tether outstanding are backed one-to-one by U.S. Dollar on deposit despite repeated claims that they would.

Centralised Cryptocurrency used to trade decentralised Cryptocurrency which was backed by the developer itself with false token/coin. Thereafter the manipulation is being manipulated by the group of developers and

using that kit in multi-level marketing, money laundering , terrorism and in other financial crime.

BLOCKCHAIN[2]

The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. It allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring they're actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

BUIDING A BETTER BLOCKCHAIN[3]

Imagine banking systems, social networks and even public organizations that are completely autonomous, transparent and without individual ownership. No one lender could create a mortgage crisis. No government could shut down a service. This dream is part of what motivates a new generation of software developers who are building on the success of the cryptocurrency Bitcoin to create broader applications for the underlying technology.

Bitcoin is based on the computing concept of the "blockchain."Blockchains are databases on peer-to-peer computer networks (where machines pool together their powers) made of time-stamped entries called "blocks" that are encrypted and unchangeable, and describe transactions such as money transfers. No one person or system holds the entire ledger of transactions, and no one can falsify a transaction. because everyone in the network helps validate and run the database. In short: ownership is decentralized, and security is bolstered

[2] http://bitcoin.org/en/how-it-works
[3] internethealthreport.org/v01/stories/building-a-better-blockchain

TRANSACTION

A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a *private key* or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The *signature* also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process called *mining*.

MINING PROCESS

Mining is a distributed consensus system that is used to *confirm* pending transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a *block* that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively to the block chain. In this way, no group or individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

DIGITAL LEDGER TEHNOLOGY

The Financial Action Task force developed a framework for centralised ledger system, owned and operated by a single trusted entity. DLT in its blockchain form

was first used in Bitcoin to facilitate peer-to-peer payments without a central third party. Blockchain is a type of DLT that has a specific set of features, organising its data in a chain of blocks. Each block contains data that are verified, validated and then 'chained' to the next block. Blockchain is a subset of DLT, and the Bitcoin Blockchain is a specific form of a blockchain. Today, all crypto assets utilise various forms of DLT (be it blockchain or otherwise), although the use cases of DLT extends far beyond financial services. We have previously shared our position on DLT as part of a Feedback Statement that we published in December 2017. DLT was also covered in the recent Crypto asset Taskforce report.

DIFFERENT TYPES OF CRYPTOCURRENCIES IN WORLD

BITCOIN is a Decentralized Digital Currency. Bitcoin transactions are verified by network nodes through cyptography and recorded in a public distributed ledger called a Blockchain. The Cyptocurreny was invented in 2008 by an unknown entity under the name Satoshi Nakamoto. The currency began use in 2009, when its implementation was released as open- source software. The word " Bitcoin" was defined in a white paper published on 31st October,2008. It is a compound of the words bit and coin.

There are also different types of crytocurrency which are design by some Private developers which are like Dogecoins, Shibu and others. There are thousands of Digital Currencies utilising blockchain technology being used for an incredibly diverse list of application within the digital economy. There are four types of crypto currencies 1. Payment cryptocurrency. 2. Utility tokens. 3. Stablecoins. 4. Central Bank Digital.

Now, with the entry of Cryptocurrency in the domain digital currency and sense the vulnerabilities attached to it, brought into pictures FATF and actions takers by it. FATF was the first inter-government body ,which has started discussing and recommendations regarding Cryptocurrency.

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force[4] (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

In June 2013, the Financial Action Task Force (hereinafter, "FATF"), also known by its French name, Groupe d'action financière, which is an inter-governmental organization founded in 1989 on the initiative of G-7 to develop policies to combat money laundering, came up with what came to be known as "New Payment Products and Services Guidance" (NPPS Guidance, 2013). It was actually a Guidance for a Risk Based Approach to Pre-paid cards. Mobile Payments and Internet-based Payment Services. But this Guidance did not define the expressions 'digital currency', 'virtual currency', or 'electronic money', nor did it focus on virtual currencies, as distinct from internet based payment systems that facilitate transactions denominated in real money (such as Paypal, Alipay,

[4] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

and Google Checkout etc.). Therefore, a short-term typologies project was initiated by FATF for promoting fuller understanding of the parties involved in convertible virtual currency systems and for developing a risk matrix.

A report titled "Virtual Currencies – Key Definitions and Potential AML/CFT Risks" was issued in June 2014 by FATF, highlighting, both legitimate uses and potential risks associated with virtual currencies. What is of great significance about this FATF report is that it defined 2 important words. The FATF report defined 'Virtual currency' as a digital representation of value that can be traded digitally and functioning as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but not having a legal tender status. The FATF report also defined 'Cryptocurrency' to mean a math-based, decentralised convertible virtual currency protected by cryptography by relying on public and private keys to transfer value from one person to another and signed cryptographically each time it is transferred.

Again, in June 2015, FATF came up with a "Guidance for a Risk Based Approach to Virtual Currencies", which suggested certain recommendations, as follows:
A. Countries to identify, assess and understand risks and to take action aimed at mitigating such risks. National authorities to undertake a coordinated risk assessment of VC products and services that:

(1) Enables all relevant authorities to understand how specific virtual currency products and services function and impact regulatory jurisdictions for Anti Money Laundering ('AML' for short)/combating the Financing of Terrorism ('CFT' for short) treatment purposes;

(2) Promote similar AML/CFT treatment for similar products and services having same risk profiles.

B. Where countries are prohibiting virtual currency products and services, they should take into account among other things, the impact a prohibition would have on local and global level of money laundering/terrorism financing risks, including whether prohibition would drive such payment activities underground, where they will operate without AML/CFT controls.

2.8. The FATF submitted a report in October 2015 on "Emerging Terrorist Financing Risks". The report was divided into four parts, under the captions (i) introduction (ii) financial management of terrorist organisations (iii) traditional terrorist financing methods and techniques and (iv) emerging terrorist financing threats and vulnerabilities. Even while acknowledging in part 3 of the report that the traditional methods of moving funds through the banking sector happens to be the most efficient way of movement of funds for terrorist organisations, the report acknowledged the emergence of new payment products and services in part 4 of the report. The report took note of different methods of terrorist financing, such as self-funding, crowd funding, social network fund raising with prepaid cards etc. Coming to virtual currencies, the report noted the following:

'Virtual currencies have emerged and attracted investment in payment infrastructure built on their software protocols. These payment mechanisms seek to provide a new method for transmitting value over the internet. At the same time, virtual currency payment products and services (VCPPS) present ML/TF risks. The FATF made a preliminary assessment of these ML/TF risks in the report Virtual Currencies Key Definitions and Potential AML/CFT Risks. As part of a staged approach, the FATF has also developed Guidance focusing on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers.

Virtual currencies such as bitcoin, while representing a great opportunity for financial innovation, have attracted the attention of various criminal groups, and may pose a risk for TF (terrorist financing). This technology allows for anonymous transfer of funds internationally. While the original purchase of the currency may be visible (e.g., through the banking system), all following transfers of the virtual currency are difficult to detect. The US Secret Service has observed that criminals are looking for and finding virtual currencies that offer: anonymity for both users and transactions; the ability to move illicit proceeds from one country to another quickly; low volatility, which results in lower exchange risk; widespread adoption in the criminal underground; and reliability.

Law enforcement agencies are also concerned about the use of virtual currencies (VC) by terrorist organisations. They have seen the use of websites affiliated with terrorist organisations to promote the collection of bitcoin donations. In addition, law enforcement has identified internet discussions among extremists regarding the use of VC to purchase arms and education of less technical extremists on use of VC. For example, a posting on a blog linked to ISIL proposed using bitcoin to fund global extremist efforts." (emphasis supplied).

Cryptocurency Trading by India & other Countries. Before, we dwell into Cryptocurrency trading, mere is a need to first have a look at the Forex Trading in India.

FOREX TRADING

Forex trading, also known as currency trading, is decentralized worldwide market in which all of the currencies of various economies are traded, sold and bought. The Foreign exchange market is a world largest financial market and heavily regulated by governments and banks through their influence factors like

Economic indicators. Central bank policies. There are also risks factors in Forex Trading like Exchange risks and Economic events. However, after that events where risk factor is involved it is permissible to trade Forex Trading in India through Indian forex Exchanges such as BSE, NSE and MCX -XXX. The Foreign Exchange Management Act (FEMA) mix binary trading illegal. While dealing in Foreign currency is legal with several restrictions.

CRYPTOCURRENCY TRADING

Cryptocurrency trading means taking up financial position on the prize directions of individual cryptocurrencies against the dollar or against another crypto, via crypto to crypto pairs. Contracts for difference (CFD) are a particularly popular way to trade cryptocurrency as they allow for greater flexibility. The Cryptocurrency exchange market is a most popular and upcoming world largest financial market which was not regulated by any governments or any financial institutions. Cryptocurrency can be traded in several ways. The first way is to deal in the Digital crypto coin itself by buying and selling it on cryptocurrency exchange. Cryptocurrency trading , just like all forms of financial trading, requires relevant knowledge, skills, available capital and relevant skills for analysing market because it is more volatile than traditional instruments and hence, risker than more people are used to.

Even though cryptocurrencies are not recognised as legal tender in the global economy, they have the potential of changing the financial landscape and this makes them hard to ignore. At the same time, the blockchain technology, which forms the foundation of cryptocurrency creation, has opened up new investment opportunities for traders to capitalise on. There are several risk factors also involved such as market volatility, regularity risk, security etc.

THE BLACK MARKET

After Trading there are no special laws in respect to start a cryptocurrency business in India. Apart from this, in light of paying the taxes applied to VDAs. There were several formalities among which are to obtain a permanent account number (PAN), apply for a tax deduction and collection account number, to obtain goods and services identifications account number (GSTIN). However, cryptocurrencies are also variously referred to as Crypto assets which raise concern of Consumer Protection Market Integrity, Tax- invasion and Global Money laundering which rendered their very existence questionable.

However, on the other hand, there are currently many cryptocurrencies which are developed and designed by private developers and promoted in MLM companies. These kinds of crypto token have been subjected to several major scams and issued or launched by private developers with unlimited supply of cryptocurrency/coin and also be used in money laundering , terrorism and other financial crime.

RISKS TO CONSUMER

Crypto assets pose a range of substantial risks to consumers, which stem from consumers purchasing unsuitable products without having access to adequate information. This can include fraudulent activity, as well as the immaturity or failings of the market infrastructure and services.

1.1 Consumers may experience unexpected or large losses. While this is true of many types of investments, cryptoasset investors should be particularly aware of the volatility that many tokens experience, and the limited information available on how these tokens work. Preliminary findings from

our consumer research suggest that consumers can overestimate their knowledge of cryptoassets and the underlying technology, with some respondents believing that, due to language such as 'mining' and 'coins', they were investing in tangible assets.

1.2 Leveraged derivatives, like Contracts for Differences (CFDs) and futures, referencing cryptoassets carry a high risk of loss due to the volatility of cryptoassets and the impact of product fees such as financing costs and spreads,. They can also be difficult to value due to a lack of transparency in the price formation of the underlying cryptoasset. The potential to misunderstand the nature of these assets can be compounded by poor practices in relation to advertising. Adverts often overstate benefits and rarely warn of volatility risks, the fact consumers can lose their investment, the absence of a secondary market for many offerings, and the lack of regulation. These often play on consumers' aspirations for 'easy money and wealth' and 'fear of missing out'. Often social media plays a significant role in influencing consumers' behavior.

1.3 Whitepaper' documents that typically accompany ICOs are not standardised and often feature information considered to be exaggerated or misleading. Given the lack of clear information, consumers may not understand that many of these projects are high-risk and at an early stage, and therefore may not suit their risk tolerance, financial sophistication or financial resources. These documents are not prospectuses, are not approved by a regulatory authority and do not, generally, provide the level of detail contained in a prospectus in relation to the company, the business and the product.

1.4 Consumers may buy cryptoassets without being aware of the limited regulatory protections for those cryptoassets that fall outside the FCA's regulatory remit like the lack of recourse to the Financial Services Compensation Scheme (FSCS), and the Financial Ombudsman Service (FOS). This can be more problematic when firms offer both regulated and unregulated products at the same time, as it can be harder for consumers to determine which products provide recourse. We would always expect a regulated firm selling unregulated products to be clear with consumers about this. Where products are regulated, recourse is only available in limited circumstances like mis-selling – losing money in an investment does not automatically mean recourse is available.

1.5 Fraudulent activity is likely to exist across the range of cryptoassets, but evidence suggests there are significant risks associated with ICOs, particularly around high failure rates, or fraudulent ICOs. Recent research looked at listed tokens in 2017 with data provided for those ICOs with over $50 million in market capitalisation and found that 78% of these listed tokens were scams.

1.6 The FCA works closely with other authorities such as the police, Advertising Standards Authority and Trading Standards in order to reduce fraudulent activity. We may also consider other laws and non-financial rules and regulations which may also apply to authorised and unauthorised firms, like the Advertising Codes, general common law, criminal law, and the General Data Protection Regulation (GDPR) amongst others.

1.7 Poor cyber security can also lead to hackers taking advantage of systems and stealing cryptoassets through cybercrime. Cryptoassets are now viewed as high-value targets for theft. Both users, and service providers like custodians/wallet providers and exchanges are increasingly being

targeted by cybercriminals to obtain the private keys which enable consumers to access and transfer their cryptoassets.In the first half of 2018 alone, $731 million worth of cryptoassets were stolen from exchanges. This included $500 million from a hack on the Coincheck exchange and $40 million from a hack on the Coinrail exchange.22 By October 2018, hacking of exchanges increased to $927 million.23 2.29 Monitoring operational harms is demanding given the cyber environment and large scale technological changes taking place within the cryptoasset industry. Mitigating operational harms, including ensuring operational resilience, is a vital part of protecting the UK's financial system, institutions and consumers.

REGULATION OF CRYPTOCURRENCY AROUND THE WORLD.[5]

This report surveys the legal and policy landscape surrounding cryptocurrencies around the world. While not dissimilar in form to the 2014 Law Library of Congress report on the same subject, which covered forty foreign jurisdictions and the European Union, this report is significantly more comprehensive, covering 130 countries as well as some regional organizations that have issued laws or policies on the subject. This expansive growth is primarily attributable to the fact that over the past four years cryptocurrencies have become ubiquitous, prompting more national and regional authorities to grapple with their regulation. The resulting availability of a broader set of information regarding how various jurisdictions are handling the fast-growing cryptocurrency market makes it possible to identify emerging patterns, some of which are described below. The

[5] Regulation of Cryptocurrency Around the World – Mexico, Report of The Law Library of Congress, Global Legal Research Center (June 2018) available at https://www.loc.gov/law/help/cryptocurrency/world-survey.php#mexico (Last accessed on 27-02-2020).

country surveys are also organized regionally to allow for region-specific comparisons.

One interesting aspect of the fast-growing cryptocurrency market is the fluidity of the terms used to describe the different products that fall within its ambit. While the various forms of what are broadly known as "cryptocurrencies" are similar in that they are primarily based on the same type of decentralized technology known as blockchain with inherent encryption, the terminology used to describe them varies greatly from one jurisdiction to another. Some of the terms used by countries to reference cryptocurrency include: digital currency (Argentina, Thailand, and Australia), virtual commodity (Canada, China, Taiwan), crypto-token (Germany), payment token (Switzerland), cyber currency (Italy and Lebanon), electronic currency (Colombia and Lebanon), and virtual asset (Honduras and Mexico).

One of the most common actions identified across the surveyed jurisdictions is government-issued notices about the pitfalls of investing in the cryptocurrency markets. Such warnings, mostly issued by central banks, are largely designed to educate the citizenry about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not. Most government warnings note the added risk resulting from the high volatility associated with cryptocurrencies and the fact that many of the organizations that facilitate such transactions are unregulated. Most also note that citizens who invest in cryptocurrencies do so at their own personal risk and that no legal recourse is available to them in the event of loss.

Many of the warnings issued by various countries also note the opportunities that cryptocurrencies create for illegal activities, such as money laundering and terrorism. Some of the countries surveyed go beyond simply warning the public

and have expanded their laws on money laundering, counterterrorism, and organized crimes to include cryptocurrency markets, and require banks and other financial institutions that facilitate such markets to conduct all the due diligence requirements imposed under such laws. For instance, Australia, Canada, and the Isle of Man recently enacted laws to bring cryptocurrency transactions and institutions that facilitate them under the ambit of money laundering and counter-terrorist financing laws.

Some jurisdictions have gone even further and imposed restrictions on investments in cryptocurrencies, the extent of which varies from one jurisdiction to another. Some (Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam) ban any and all activities involving cryptocurrencies. Qatar and Bahrain have a slightly different approach in that they bar their citizens from engaging in any kind of activities involving cryptocurrencies locally, but allow citizens to do so outside their borders. There are also countries that, while not banning their citizens from investing in cryptocurrencies, impose indirect restrictions by barring financial institutions within their borders from facilitating transactions involving cryptocurrencies (Bangladesh, Iran, Thailand, Lithuania, Lesotho, China, and Colombia).

A limited number of the countries surveyed regulate initial coin offerings (ICOs), which use cryptocurrencies as a mechanism to raise funds. Of the jurisdictions that address ICOs, some (mainly China, Macau, and Pakistan) ban them altogether, while most tend to focus on regulating them. In most of these latter instances, the regulation of ICOs and the relevant regulatory institutions vary depending on how an ICO is categorized. For instance, in New Zealand, particular obligations may apply depending on whether the token offered is categorized as a debt security, equity security, managed investment product, or derivative. Similarly, in the Netherlands, the rules applicable to a specific ICO

depend on whether the token offered is considered a security or a unit in a collective investment, an assessment made on a case-bycase basis. Not all countries see the advent of blockchain technology and cryptocurrencies as a threat, albeit for different reasons. Some of the jurisdiction surveyed for this report, while not recognizing cryptocurrencies as legal tender, see a potential in the technology behind it and are developing a cryptocurrency-friendly regulatory regime as a means to attract investment in technology companies that excel in this sector. In this class are countries like Spain, Belarus, the Cayman Islands, and Luxemburg.

Some jurisdictions are seeking to go even further and develop their own system of cryptocurrencies. This category includes a diverse list of countries, such as the Marshall Islands, Venezuela, the Eastern Caribbean Central Bank (ECCB) member states, and Lithuania. In addition, some countries that have issued warnings to the public about the pitfalls of investments in cryptocurrencies have also determined that the size of the cryptocurrency market is too small to be cause for sufficient concern to warrant regulation and/or a ban at this juncture (Belgium, South Africa, and the United Kingdom). One of the many questions that arise from allowing investments in and the use of cryptocurrencies is the issue of taxation. In this regard the challenge appears to be how to categorize cryptocurrencies and the specific activities involving them for purposes of taxation. This matters primarily because whether gains made from mining or selling cryptocurrencies are categorized as income or capital gains invariably determines the applicable tax bracket. The surveyed countries have categorized cryptocurrencies differently for tax purposes, as illustrated by the following examples:

Israel → taxed as asset Bulgaria → taxed as financial asset Switzerland → taxed as foreign currency Argentina & Spain → subject to income tax Denmark →

subject to income tax and losses are deductible United Kingdom: → corporations pay corporate tax, unincorporated businesses pay income tax, individuals pay capital gains tax. Mainly due to a 2015 decision of the European Court of Justice (ECJ), gains in cryptocurrency investments are not subject to value added tax in the European Union Member States.

In most of the countries surveyed for this report that have or are in the process of devising taxation rules, the mining of cryptocurrencies is also exempt from taxation. However, in Russia mining that exceeds a certain energy consumption threshold is taxable.

In a small number of jurisdictions surveyed cryptocurrencies are accepted as a means of payment. In the Swiss Cantons of Zug and a municipality within Ticino, cryptocurrencies are accepted as a means of payment even by government agencies. The Isle of Man and Mexico also permit the use of cryptocurrencies as a means of payment along with their national currency. Much like governments around the world that fund various projects by selling government bonds, the government of Antigua and Barbuda allows the funding of projects and charities through government-supported ICOs.

Should We Regulate Cryptocurrency Or Should Allow Cryptocurrency Trading In India Like Countries Or How We Support Recommendations Of FATF

Cryptocurrency trading should be allowed but with some limitations from approval from any Government Body like SEBI, only through approval platforms and exchanges officially recognized by the government only. There may be new regulators or cryptocurrencies may be acquired by the Central Bank of India (RBI).

Second, since cryptocurrencies involve cross-border transactions, a body similar to the Security and Exchange Board of India (SEBI) will be needed to monitor transactions.

"Investor protection comes first. To avoid fraud, a system of checks and balances is required, and in the case of fraud targeting investors, there must be a penalty. Government of India Defines Private cryptocurrency in India which refers to all cryptocurrencies that are not regulated or issued by the government, such as Bitcoin, Ethereum and Doge Coin. However, the official definition of a private cryptocurrency is not clear. There is unnecessary confusion with the use of the phrase 'private cryptocurrency". This confuses crypto developers and investors because a blockchain is a verification of crypto transaction which has been done and is a ledger of wallet owner and there is no such thing as private crypto.

Therefore, there should be a definition of Private Cryptocurrency but as reference to the above definition should not be allowed of defining Private Cryptocurrency. In my views The Definition of Private cryptocurrency should not be that a decentralized currency should be allowed by the Government through exchanges such as Bitcoin, Ethereum & few other but Utility Tokens, Security Tokens or any other Token or coin which was design by the Developer in any part of the world should be called Private Cryptocurrency because a Decentralized Currency or a coin is Bitcoin, Ethereum and other cryptocurrencies are not controlled or managed by private institutions, transactions are on a public ledger and are recognized as public cryptocurrencies in all major economies.

In my views, Private Cryptocurrency should in the meaning of centralized developed crypto tokens/coins which shall be developed by some developers who may have control over it and selling it by Decentralized coin to the people that's called Private cryptocurrency. The Private cryptocurrency is managed or

governed by a Specific set of developers or community, then it can be termed as Private Cryptocurrency.

CONCLUSION

Need of Proactive approach by the Government.

Since 1995 almost all traffic is carried over PCP/IP. The first public ally available internet service in India was launched by State – owned Videsh Sanchar Nigam Limited (VSNL) on 15th, August 1995. ***At the time, VSNL had a monopoly over international communication in the country and private enterprise was not permitted in the sector. It takes ten years to give access of internet to the general public and it takes twenty years for the outcome of providing Digital India which was launched on 1st July, 2015 initiative taken by the Government of India.***

Whether existing acts are equipped enough to cover cryptocurrency?

It requires lot of deliberations, which is not an overnight process. Mere is an urgent need to provide over the existing acts like SEBI, FEMA , PMLA, IT laws and their capacity to deal with cryptocurrency, which may require meetings/session with various experts of the above -mentioned fields. Since, the wideness of the cryptocurrency is so much, it may require a creation of a separate act, rather than making it to adjust in the existing acts which may require the itself a cumbersome process.

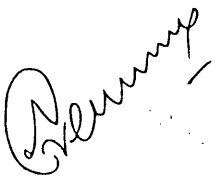
However, as far as the Answer comes out for Cryptocurrency which is concerned to be regulated or not regulated. Considering the facts and circumstances, giving my opinion with the aforesaid observation we should travel the path to become a

Digital and Blockchain operated economy. We should embrace the change and try to adapt and govern it. The Government of India should adopt or store Decentralised Cryptocurrency i.e. BITCOIN only for the future and more importantly understand the creative technology of upcoming web 3.0 which give rapid acceptance and indulgence in the technology. The government should ring fence Crypto entities by creating a licensing framework and bring them under the preview of existing PMLA, FEMA Regulations to bring compliance as far as Money Laundering and Foreign Exchange Violations are concerned.

The Government of India should make Proper forum and department from where a mandatory Permission is to be granted for selling of such coins with some security. Security has be deposited before selling it to the investors if Failure of such coins happen then that Department or forum should return claim amount to the investors.

It may require a separate department like SEBI/or ministry of information and technology with the qualified I.T experts, cyber experts in National Investigation Agency. Since, it's a new concept of a trading that may be required to be given to the investors involved in it.

Thanking You
Yours Sincerely



ANKIT VERMA
(ADVOCATE)