INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 12 | ISSUE - 2 | MARCH - 2022

INTRODUCTION TO CRYPTOCURRENCIES

Prof. Dr. Lengare K.B.
M.Phil, Ph.D. Professor, Shri Chhatrapati Shivaji College, Omerga, Tq. Omerga
Dist. Osmanabad, Maharashtra.

ABSTRACT

With the growing popularity of the crypto industry and the vast number of unregulated cryptocurrencies (thousands), governments and other stakeholders around the world are paying more attention. Between May 2021 and June 2021, the total market capitalization of cryptocurrencies is predicted to have dropped considerably, as digital coins became less likely to be used as an investment tool. This was ascribed to China's efforts to limit cryptocurrency mining and expansion within the country. According to data from coinmarketcap.com, the biggest crypto-badge, Bitcoin, set an all-time high of $68,530.34 earlier today. Its market capitalization was hovering around $1.29 trillion, representing for 43% of the o... There hasn't been a clear consensus on how to accomplish it up until now. In any case, there are strong reasons for regulators and supervisors to pay closer attention to cryptocurrencies. Price volatility, speculative trading, hacking, money laundering, and terrorist financing are all threats that necessitate tighter regulation.

The latter is the subject of this study. Many believe that, in addition to the volatility of cryptocurrency prices, these digital assets require more governmental control to prevent unlawful activities and illegitimate use. Aside from the volatility of cryptocurrency values, regulators are concerned about criminals who are increasingly exploiting cryptocurrencies for crimes such as fraud and manipulation, tax evasion, hacking, money laundering, and terrorism financing (trading outside of official channels). The issue is significant: while the full scope of virtual currency misuse is unknown, its market worth has been estimated to be in excess of EUR 7 billion globally.

KEYWORDS: *Cryptocurrencies, Badges, Token, Cryptosecurities, Blockchain, Trading platforms, Wallet providers, Coin inventors, Bitcoin, etc.*

1. INTRODUCTION:

It's not easy to come up with a definition for cryptocurrencies. Cryptocurrencies, like blockchain, have become a "buzzword" to describe a wide range of technological breakthroughs that use a method known as cryptography. In simple terms, cryptography is the process of encrypting (or converting) information into an unreadable format that can only be decoded (or decrypted) by someone who has a secret key. Cryptocurrencies like Bitcoin are secured using this method, which employs a clever system of public and private digital keys. Following that, we will attempt to provide an appropriate description of cryptocurrencies based on a critical review of the definitions already provided by various concerned policymakers at the European and worldwide levels. [1]

The initial application of blockchain technology was cryptocurrency, which was introduced as a financial tool. Once a payment transaction is generated on the internet, cryptocurrencies can use

blockchain technology to create a distributed system with certification and integrity. Unlike traditional fiat currency, which relied on a central trusted party (such as a central bank) to guarantee the value of national currencies or transactions, cryptocurrency, which is based on blockchain technology, creates a digital online distributed system of certification for payment transactions that does not require a central authority. Criminals are increasingly exploiting cryptocurrencies for illegal operations such as money laundering, terrorism financing, and tax avoidance, according to regulators. The problem is significant: while the full scope of virtual currency misuse is unknown, its market worth has been estimated to be in excess of EUR 7 billion globally. The use of cryptocurrencies for financial crime, money laundering, and tax evasion is the focus of this Policy Department A study, which examines the phenomenon from a legal standpoint. It includes policy suggestions for future European Union standards. [2]

2. CRYPTOCURRENCIES – BADGES:

In practise, the term "cryptocurrency" is frequently misused in a broad meaning. It should be separated from both badges and cryptosecurities, as indicated below. [3]

CRYPTOCURRENCIES – BADGES:

To begin, cryptocurrencies should be distinguished from cryptographic "badges," which have a purpose other than and beyond serving as a general-purpose means of trade. Badges are issued as part of an Initial Token Offering, or "ITO," in order to raise capital for a certain project or business. They are a new type of crypto-asset (digital assets recorded on a distributed ledger and secured by cryptography) that represent a claim against an entity (or its cash flows, assets, residual value, future goods or services, etc.) arising from the usage of blockchain technology. Some badges are referred to as "security tokens" or "investment tokens" because they resemble traditional securities like stocks or bonds. Other tokens, referred to as "utility tokens," give their holders (future) access to specific products or services. They can be used to purchase certain products or services, but they are not a general-purpose means of exchange because they are often exclusively usable on the token platform.

CRYPTOCURRENCIES – CRYPTOSECURITIES:

Second, cryptocurrencies should be separated from a concept known as "cryptosecurities" that has recently gained popularity. In summary, it has been proposed that blockchain technology be used to register, issue, and transfer regular shares and other corporate securities, ensuring that a company's capitalization table is always accurate and current. Because this technological process would be protected by cryptography, cryptosecurities have been proposed as a classification for these securities. The only thing that connects this new notion of "cryptosecurities" to cryptocurrencies is that they both use blockchain technology.

2.1. Cryptocurrencies – Blockchain:

In recent years, cryptocurrencies and blockchain have become trendy issues. Despite the fact that the two are frequently used in the same sentence and are plainly related, one should never confuse the two. The backbone of the cryptocurrency market is blockchain, a type of distributed ledger technology. It is the technology that underpins the wide range of cryptocurrencies currently in use. Its scope and applicability, however, are not confined to that. As previously said, blockchain may be used in a variety of industries and has a wide range of applications. It's critical to distinguish between these applications and cryptocurrencies, which are just one type of blockchain application. In light of this, regulators need not be concerned about limiting innovation when it comes to cryptocurrency. [4]

3. WHO CONCERNED?

The bitcoin market is a new stage on which many players take on different roles. To provide a better understanding of how the market operates, and without aiming to be thorough, we will identify the important participants in the following sections. [5]

Cryptocurrency users:

The "cryptocurrency user" is the first and most important player. A cryptocurrency user is a natural person or a legal entity who acquires cryptocurrencies for the purpose of using them.

- to buy real or virtual products or services (from a select group of merchants),
- to make peer-to-peer payments, or
- to keep them as an investment (i.e. in a speculative manner).

A cryptocurrency user can earn his coins in a variety of methods, without attempting to be exhaustive: To begin, he can simply purchase his coins using fiat money or another cryptocurrency on a cryptocurrency exchange. Second, he can purchase his coins directly from another cryptocurrency user (through a trading platform - this type of transaction is known as a "P2P exchange"). Finally, if a cryptocurrency uses a PoW consensus method, he can mine a new coin (that is, participate in transaction validation by solving a "cryptographic problem" and be paid with a new coin); Fourth, he may be able to obtain his coins directly from the coin offeror, either as part of a free initial coin offering (for example, on the Stellar network, Lumens (XLM) are given away for free) or as part of a crowd sale organised by the coin offeror (for example, a large amount of ether (cf. Ethereum) was sold in a crowdsale to cover certain development costs). [6] Fifth, he can get coins as payment for things or services he sells in exchange for cryptocurrencies. Finally, if a coin's blockchain undergoes a "hard fork," he will instantly receive an amount of the newly minted coin; and finally, he can accept coins as a gift or donation from another cryptocurrency user.

Miners:

The "miner" is a second person who validates transactions on the blockchain by solving a "cryptographic puzzle." Mining, as previously stated, is related to cryptocurrencies that use the PoW consensus mechanism. A miner contributes to the network by using processing power to validate transactions in exchange for newly minted currency (i.e. through an automatic decentralised new issuance). Miners can be cryptocurrency users or, more typically, parties that have started a new business mining coins to sell for fiat currency (such as the US dollar or the Euro) or other cryptocurrencies. To pool computer power, some miners form so-called pools of miners. The hazards associated with so-called "mining firms" appear to be underappreciated at the moment. We'll go through this in more detail later. [7]

Cryptocurrency exchanges:

The so-called "cryptocurrency exchanges" are a third important category of companies. Cryptocurrency exchanges are individuals or organisations that provide cryptocurrency customers with exchange services in exchange for a fee (i.e. a commission). They enable cryptocurrency users to exchange their currencies for fiat currency or to purchase new coins with fiat currency. They usually serve as a bourse as well as a type of exchange office. Bitfinex, HitBTC, Kraken, and Coinbase GDAX are examples of well-known cryptocurrency exchanges.

It's crucial to note that some exchanges are pure cryptocurrency exchanges, meaning they only accept payments in other cryptocurrencies, most often Bitcoin (for example, Binance), whereas others accept payments in fiat currencies like the US dollar or Euro (for example Coinbase). Furthermore, several cryptocurrency exchanges restrict their consumers to purchasing only a limited number of coins. [8]

It's also worth noting that many cryptocurrency exchanges (both traditional and pure cryptocurrency exchanges) also serve as custodian wallet providers (for example Bitfinex). In general, cryptocurrency exchanges provide a wide range of payment alternatives to their consumers, including wire transfers, PayPal transfers, credit cards, and other coins. Some cryptocurrency exchanges additionally provide market statistics (such as trading volumes and volatility of the coins traded) and conversion services to merchants who accept cryptocurrency payments.

Trading platforms:

Aside from bitcoin exchanges, so-called "trading platforms" play an essential role in cryptocurrency trade (and, most notably, allow cryptocurrency users to buy coins with cash). Trading platforms are marketplaces that bring together cryptocurrency users who are eager to purchase or sell coins and provide them with a platform on which they may trade directly with one another (think of it as a cryptocurrency version of eBay).

"P2P exchanges" or "decentralized exchanges" are terms used to describe trading platforms. In several aspects, they differ from bitcoin exchanges. They don't buy or sell coins themselves, for starters. Second, they are not administered by a single body or firm that controls and executes all trades, but rather by software (i.e. there is no central point of authority). Trading systems merely connect buyers and sellers, allowing them to transact business online or in person (i.e. a face-to-face trade, often executed in cash). Local Bitcoins is a well-known example of a Bitcoin trading site. [9]

Wallet providers:

The so-called "wallet providers" are another important category of businesses. Wallet providers are companies that offer digital wallets, also known as e-wallets, to cryptocurrency users. These wallets are used for holding, storing, and transferring coins. Simply simply, a wallet stores the cryptographic keys of a cryptocurrency user (see above). A wallet provider converts a cryptocurrency user's transaction history into an easily viewable format that resembles a traditional bank account. There are various types of wallet providers in reality: [10]

- The so-called "wallet providers" are another significant category of stakeholders. Wallet providers are companies that offer digital wallets, also known as e-wallets, to cryptocurrency users.
- These wallets are used to hold, store, and send cryptocurrencies. Simply described, a wallet is a storage device for the cryptographic keys of a cryptocurrency user (see above).
- A wallet provider converts a cryptocurrency user's transaction history into a readable format that resembles a traditional bank account.

Coin inventors:

There are also "coin inventors," or players who create their own coins. Individuals or groups that created the technical basis of a cryptocurrency and established the first rules for its use are known as coin innovators. In certain situations, their identity is known (for example, Ripple, Litecoin, and Cardano), but they are frequently unknown (eg. Bitcoin, Monero). Others simply vanish, while others continue concerned in maintaining and refining the cryptocurrency's code and underlying algorithm (in theory without administrator's powers) (e.g. Bitcoin). [11]

Coin offerors:

The "coin offerors" are a last group of important actors to note. Coin offerors are individuals or organisations that offer coins to cryptocurrency users upon the coin's initial release, either for a fee (through a crowdsale) or for free (through a specific (sign-up) programme (e.g. Stellar – see below), typically to fund the coin's further development or boost its initial popularity. These coin offerors produce or pre-mine the coins they offer to cryptocurrency consumers before the token's formal release / genesis. These currencies are either partially pre-mined or pre-created (i.e., cryptocurrency users can still generate more coins after the release) or entirely pre-mined or pre-created. The coin offeror normally keeps a considerable share of the coins in the latter case (e.g. this is the case with Stellar). It's vital to remember that not all coins have a known coin offeror, and not all coins are pre-mined or have their whole supply pre-created. A coin offeror can be the same person or a different person or organisation than the coin inventor. [12]

4. GRADING CRYPTOCURRENCIES:

After experiencing consistent growth over the previous few years, the cryptocurrency market exploded in 2017, appreciating more than 1,200 percent. Hundreds of coins are currently in circulation

(with a total market capitalization of well over EUR 300 billion), and new ones are appearing on a regular basis. To fully comprehend this developing market and conduct a thorough investigation, we chose to examine the essential attributes of the most well-known cryptocurrency, Bitcoin, before moving on to the primary features of a select group of alternative cryptocurrencies, often known as "Altcoins." [13]

Alternative coins to Bitcoin are known as altcoins. In a nutshell, Altcoins are divided into two categories:

- Altcoins are based on Bitcoin's original open-source system, but with a variety of modifications to the underlying code, resulting in a new coin with a unique set of attributes. Litecoin is an example of an Altcoin.
- Altcoins are digital currencies that are not based on Bitcoin's open-source system and instead have its own protocol and distributed ledger. Ethereum and Ripple are two well-known examples of Altcoins.

We chose these Altcoins not only because of their current popularity within the "crypto-community," but also because they demonstrate a diverse set of characteristics. Some are based on Bitcoin's original open-source protocol, while others are a whole different platform and/or ecosystem. Some use a PoW mechanism, while others use a different type of consensus process. Most are described as pseudo-anonymous, but some are described as completely anonymous (i.e., the quantity of coins their users own, transmit, and receive is not visible, traceable, or linked through the blockchain's transaction history).

#	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	$12,346,014,952	$770.52
2	Ethereum	ETH	$679,896,251	$7.85
3	Ripple	XRP	$236,220,241	$0.006564
4	Litecoin	LTC	$191,152,116	$3.92
5	Monero	XMR	$112,380,759	$8.34
6	Ethereum Classic	ETC	$67,603,454	$0.781504
7	Dash	DASH	$60,960,690	$8.80
8	Steem	STEEM	$43,627,481	$0.192984
9	Augur	REP	$36,887,245	$3.35
10	MaidSafeCoin	MAID	$31,768,623	$0.070199
11	NEM	XEM	$30,870,455	$0.003430
12	Waves	WAVES	$24,153,355	$0.241534
13	Dogecoin	DOGE	$23,078,949	$0.000215
14	Factom	FCT	$18,478,091	$2.11
15	DigixDAO	DGD	$15,760,516	$7.88
16	Iconomi	ICN	$15,653,710	$0.179928
17	Lisk	LSK	$15,278,474	$0.152785
18	Peerplays	PPY	$15,257,877	$15.26
19	GameCredits	GAME	$14,743,851	$0.249644
20	Gulden	NLG	$12,702,417	$0.037773

Figure: Overview of coins (Source: https://in.pinterest.com/pin/85216617933849185/ accessed on 09/03/2022)

5. BITCOIN (BTC):

5.1 What is Bitcoin?

Bitcoin (BTC) is a virtual, decentralised, and (at first look) anonymous currency that is not backed by the government or any other legal body and cannot be exchanged for gold or any other commodity.

The text "Bitcoin: a Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto, released on the internet in 2008, lies at the heart of Bitcoin's invention. The development of Bitcoin was accelerated as a result of this article and the principles it expressed. The fact that it is still unknown if Satoshi Nakamoto is a genuine person, a pseudonym, or even a group of hackers adds to the mystique around Bitcoin.

Bitcoin is a virtual currency, which means that it does not have a physical form. As a result, a reasonable representation of a Bitcoin is most likely a computer file saved on a personal computer or in a digital wallet via an internet service. However, Bitcoins' purely virtual nature should be qualified. It is rumoured that it is feasible to print the combination of characters that make up Bitcoin and then transfer that print as a bearer instrument. However, because this is believed to be a minor occurrence, it will not be discussed further here. [14]

A PoW consensus method underpins Bitcoin. Bitcoins are created through a process known as "mining" (see also above). To clarify, such a method – the entirety of which is open-source software – comprises individuals willingly making their own computers available to the Bitcoin network in order to solve complex mathematical problems. Bitcoins are awarded to computers that are able to solve such issues (and, as a result, construct so-called transaction "blocks"). The total number of Bitcoins that may be made by mining is limited: the Bitcoin system is set up so that the creation of blocks over time is rewarded with fewer and fewer Bitcoins, with no more than 21 million Bitcoins ever being created. The fact that the generation and increase of Bitcoins is automated and limited by the system itself suggests that a central institution / authority is not required to issue Bitcoins. [14]

The restricted number of Bitcoins, along with the fact that Bitcoin conversion rates are set by supply and demand, with no government agency able to intervene (for example, by printing more money), leads in extreme price volatility.

Bitcoin is based on permission less, open blockchain:

A typical example of an open, permissionless blockchain is the Bitcoin blockchain. Without needing to be (pre-)approved by any (central) authority, anyone can join or quit the public Bitcoin network at any time. To join the Bitcoin network and add transactions to the ledger, all that is required is a computer with the necessary software installed.

Bitcoin is a digital currency that may be exchanged for fiat money.

On a variety of cryptocurrency exchanges, Bitcoin may be purchased and converted straight into fiat currency. Bitcoin is one of the easiest cryptocurrencies to convert into fiat currency out of all the ones currently in circulation.

Bitcoin is a digital currency:

A rather high number of (online) businesses, including numerous large companies (e.g. Microsoft, Expedia, Playboy, Virgin Galactic, LOT Polish Airlines, etc.), accept Bitcoin (BTC) as a valid source of money. As a result, it is considered a means of exchange.

Bitcoin is a pseudo-anonymous coin:

Bitcoin is frequently referred to as an anonymous currency because, while anybody can verify the chain of transactions using the public ledger, nothing in the system appears to link Bitcoins to specific individuals at first glance. This anonymous character, however, is far from perfect. It is technically possible – albeit extremely difficult and expensive – to identify the parties concerned in a

Bitcoin transaction by combining various indicators. In other words, Bitcoin is a pseudo-anonymous coin rather than a totally anonymous currency. [14]

6. CONCLUSION:

The fundamental conclusion that can be derived from the many points of view presented above is that there is no widely agreed meaning of the term cryptocurrency in the regulatory environment. Furthermore, most policymakers have avoided defining the phrase entirely. Only the World Bank and the FATF have provided a clear definition among those mentioned above. Most policymakers, on the other hand, treat cryptocurrencies as a subset or a type of virtual or digital currencies. To summarise all of the above definitions, a cryptocurrency is "a digital representation of value that I is intended to serve as a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by cryptography, and (iv) can be converted into legal tender and vice versa." We will discuss the notion of cryptocurrencies (or coins; we will use both terms interchangeably hereafter), in particular the dividing line between cryptocurrencies and other, closely related concepts that should be distinguished from cryptocurrencies.

We arrive at a taxonomy and history of cryptocurrencies based on the preceding overview and analysis, allowing us to undertake a more detailed regulatory study and warn the regulatory framework's shortcomings in the future. We'll begin with taxonomy. The overview makes it evident that THE cryptocurrency does not exist. Although some are similar, there is a lot of variety in terms of how they are structured, which technology they use, the level of anonymity they provide, and so on. The table below attempts to demonstrate this diversity. The chosen cryptocurrencies are compared based on a number of factors, including whether they run on permissioned or permissionless technology, their decentralised nature, whether they were first offered by an identifiable person or entity, whether they are electronically traded, directly convertible into fiat currency, serve as a medium of exchange, and whether they are pseudo-anonymous or fully anonymous. These factors are not picked at random, but rather to help determine whether cryptocurrencies are caught by AMLD, which crypto players are included in AMLD's scope, whether relevant players that are not (yet) in scope can be regulated, and so on. Our understanding of the selected cryptocurrencies is reflected in the table. It should be read with the understanding that distinguishing between cryptocurrencies is difficult. The scarcity of available information, as well as the often very technical nature of it, are complicating problems. Cryptocurrencies are also a moving objective. For example, a cryptocurrency that is not now used as a medium of exchange may become one in the future. As a result, the overview does not claim to be the only means of representing or classifying the cryptocurrencies in question.

More work and research, in order to get a complete picture of cryptocurrencies and all of its various aspects in order to provide the best possible policy guidance, is arguably required. Nonetheless, we believe that the table below is a useful tool for the purposes of this study, allowing us to draw certain conclusions throughout the regulatory examination.

REFERENCE:

1. Hill, J. (2018). Fintech and the remaking of financial institutions. doi: 10.1016/C2016-0- 03863-9 Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain
2. Adhami, S., Giudici, G., & Martinazzi, S. (in press). Why do businesses go crypto? An empirical analysis of Initial Coin Offerings. Journal of Economics and Business. doi: 10.1016/j.jeconbus.2018.04.001
3. Bhaskar, N. D., & Chuen, D. L. K. (2015). Bitcoin mining technology. In Chuen, D. L. K (Eds), Handbook of digital currency. (pp. 45-65). doi: 10.1016/B978-0-12-802117- 0.00003-5
4. Casey, M., & Wong, P. (2017). Global supply chains are about to get better, thanks to blockchain. Harvard business review. Retrieved from https://hbr.org/2017/03/globalsupply-chains-are-about-to-get-better-thanks-to-blockchain CB Insights. (2018).

5. Chan, S., Chu, J., Nadarajah, S., & Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies. Journal of Risk and Financial Management, 10(2), 12. doi: 10.3390/jrfm10020012
6. Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. Business Horizons, 61, 567-575. doi: 10.1016/j.bushor.2018.03.006 Coindesk. (2018).
7. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6-10. Retrieved from https://j2-capital.com/wpcontent/uploads/2017/11/AIR-2016-Blockchain.pdf
8. Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain enabled applications: Understand the blockchain ecosystem and how to make it work for you. doi: 10.1007/978-1-4842- 3081-7
9. Drescher, D. (2017). Blockchain basics: A non-technical introduction in 25 steps. doi: 10.1007/978-1-4842-2604-9 Elbahrawy, A., Alessandretti, L., Kandler, A., Pastorsatorras, R., & Baronchelli, A. (2017).
10. Nian, L. P., & Chuen, D. L. K. (2015). Introduction to bitcoin. In Chuen, D. L. K (Eds), Handbook of digital currency. (pp. 5-30). doi: 10.1016/B978-0-12-802117-0.00001-1
11. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of blockchain technology: pros, cons and SWOT. Cluster Computing, 1-15. doi: 10.1007/s10586-018- 2387-5
12. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187. doi: 10.1007/s12599-017-0467-3
13. Nolan, A. R., Dartley, E. T., Baker, M. B., ReVeal, J., & Rinearson, J. E. (2018). Initial coin offerings: Key US legal considerations for ICO investors and sponsors. Journal of Investment Compliance, 19(1), 1-9. doi: 10.1108/JOIC-02-2018-0016
14. Pierro, M. D. (2017). What is the blockchain?. Computing in Science & Engineering, 19(5), 92-95. doi: 10.1109/MCSE.2017.3421554

Prof. Dr. Lengare K.B.
M.Phil, Ph.D. Professor, Shri Chhatrapati Shivaji College, Omerga, Tq. Omerga Dist. Osmanabad, Maharashtra.