KHAITAN &CO

CREBACO

CRYPTO ASSETS IN INDIA

Proposed Regulatory Framework

Representation Before The Government Of India

January 2021

INDEX

A. ABOUT US

About Khaitan & Co

Khaitan & Co is one of India's oldest and largest full-service law firms. Combining a rich heritage of over a hundred years with a modern and cutting-edge practice, the firm offers full service legal solutions to domestic and international clients. Majority of the Firm's practice areas have been consistently ranked in the Tier-I category by leading ranking agencies such as Chambers & Partners, Asialaw, IFLR1000, Legal 500, Benchmark Litigation, etc. Over the course of the last century, our Firm has contributed to various headline M&A deals and successfully represented clients right up to the level of the Supreme Court.

Rashmi Deshpande, Partner
deshpande.rashmi@khaitanco.com
+91 98338 62234

About CREBACO

CREBACO Global Private Limited is a research, intelligence, and rating company focused on Blockchain and Cryptocurrencies. CREBACO follows a systematic approach to analyzing a technology project by keeping in mind all the aspects related to it such as the feasibility of the project, promoters background, technology, user details, audits for security, etc. CREBACO works with Governments, regulators, SEZs, Investors, and projects to build and share the most reliable database and setting new benchmarks for the industry.

Sidharth Sogani, Founder and CEO
sidharth@crebaco.org
+91 98677 60706

B. EXECUTIVE SUMMARY

India is home to over 1.3 billion people with an average age of less than 30 years, making it a land of opportunities and possibilities which the world is looking at with great interest & expectations. We have the cheapest and fastest internet connectivity in the world, one of the best software developers and a great vision of 'Digital India' led by Prime Minister Narendra Modi. Keeping this vision in mind, the Government has openly endorsed the blockchain technology and has made announcements to use it for public purposes such as medical record, land records, individual databases, etc.

Nonetheless, there is currently no regulatory framework to govern the crypto assets market in India. The absence of a regulatory framework not only creates uncertainty for businesses looking to enter this space, but also exposes investors to avoidable frauds. Given the scale of business generated by crypto assets today in India, it has become imperative to regulate this industry with a suitable framework. The purpose of this representation is to shed light on the operations of the crypto asset market and suggest regulations that would safeguard the interest of all stake holders including and especially the Government.

The representation is divided into multiple sections for ease of reference. We have first discussed certain statistics highlighting the growing popularity of crypto assets and their growth potential. Thereafter, we have traced the history of cryptocurrencies in India and identified several key developments since the year 2013. Further, since the subject of this representation is still an emerging technology, we have briefly discussed certain basic concepts and terminologies before proposing a comprehensive regulatory framework governing crypto assets in India. The suggested framework touches upon several key areas and legislations, the roles and responsibilities of authorities such as the Reserve Bank of India and the Securities and Exchange Board of India. In our view, these two authorities have the most important role to play in striking a balance between maintaining the attractiveness of crypto assets and ensuring transparency and accountability in their usage. Finally, we provide a list of countries that have embraced crypto assets and decided to regulate their usage and highlight the role of the Financial Action Task Force as an international regulator.

We earnestly hope that our representation will be looked at favourably by the relevant authorities and that the Government will take steps to embrace and regulate this new technology.

C. MARKET SIZE AND POTENTIAL

A recent webinar organized jointly by Khaitan & Co and CREBACO in July 2020 titled *Cryptocurrency in India: What the Future Holds*[1] saw active participation from Mr. Subhash Chandra Garg, Former Economic Affairs and Finance Secretary and head of the inter-ministerial committee on virtual currencies constituted by the Government of India and from the discourse that took place during the webinar, it became apparent that the Government had given a thought to the idea of using the crypto assets as tradable commodities.

The crypto asset market in India is worth USD 15 billion. The data on the traffic on global crypto asset exchanges between January 2018 and December 2020 from Indian IPs amounted to average 5%., a figure that shows that the size of the Indian crypto community is very large. As per a recent analysis, the Indian crypto community may consist of over 6 million users or approx. 0.5% of the Indian population. However, Indians own only a fraction of the global crypto assets.

It is pertinent to note that there are several companies dealing in crypto assets and blockchain which are incorporated overseas and have persons of Indian origins either as their directors, founders, Chief Technology Officers, or Chief Finance Officers. The future of such companies include investment of approximately USD 6.7 billion in the next 18 to 27 months.

Since the last time CREBACO evaluated the Indian ecosystem, the crypto asset market has gone up by over 40% (based on web traffic, and number of app downloads, market conditions). This means that from the previous estimate of USD 12.9 billion, the current crypto ecosystem has grown to a potential market size of over USD 15+ billion. Despite the COVID-19 situation and the ensuing nationwide lockdown, the number of crypto users in India increased to over 6 million users. It is pertinent to note that the value of crypto assets is a non-correlated asset (*i.e.* not tied to fluctuations in traditional markets).

In fact, the recent rise of the price of bitcoin to record levels (more than $ 42,000 / INR 31 lakh) demonstrates the faith that investors have placed in cryptocurrencies. The scale at which the crypto assets are traded globally point to a very bright future for the industry. As such, the time is ripe for India to embrace this new technology and regulate it for the betterment of its citizenry.

[1] Recording of the webinar can be accessed at https://www.youtube.com/watch?v=anWAdy7haQY

D. TRACING THE HISTORY OF CRYPTOCURRENCIES IN INDIA

December 2013

First crypto exchange in India started operations

December 2014

RBI issued a press release, wherein for the first time, users, holders, and traders of cryptocurrencies were cautioned of its potential risks

2016

October 2016

ICICI Bank and Emirates NRD announced a pilot launch of blockchain network for international remittances and trade finance

November 2016

Demonetisation became a major trigger for India to move towards digitization and a cash free economy

2017

Feb 2017 - Dec 2017

RBI again cautioned users of cryptocurrencies and explicitly stated that no licenses had been granted to operators trading in cryptocurrencies in India

October 2017

Land Records Department and Transport Department of the Government of Andhra Pradesh implemented a blockchain pilot

January 2017

Institute of Development and Research in Banking Technology (established by RBI) released a white paper titled *Applications of Blockchain Technology to Banking and Financial Sector in India*

November 2017

Government of India constituted a high-level Inter-ministerial Committee to study issues related to cryptocurrencies

2018

April 2018

RBI took a definitive stand, issued a circular prohibiting banks and financial institutions from dealing in cryptocurrencies or providing services for facilitating any person or entity in dealing with or settling cryptocurrencies.

April 2018

Several cases filed in the Supreme Court challenging the RBI circular. *Internet and Mobile Association of India*, the lead petitioner, contended that the action of the RBI in issuing the circular was *ultra vires* its powers as laid down in the Banking Regulation Act, 1949

April 2018

The Inter-Ministerial Committee submitted its initial report along with a draft bill known as *Crypto Token and Crypto Asset (Banning, Control and Regulation)* Bill, 2018. This bill was never enacted.

October 2018

First cryptocurrency ATM started in Bengaluru

2019

February 2019

The Inter-Ministerial Committee released its final report recommending a ban on cryptocurrencies, given the risks associated with them and volatility in their prices. A bill known as *Banning of Cryptocurrencies and Regulation of Official Digital Currency Bill, 2019* was proposed prohibiting any person from mining, generating, holding, selling, dealing in, issuing, transferring, disposing of or using cryptocurrency in India. This bill was also never enacted.

2020

March 2020

Supreme Court set aside the RBI circular on the ground that it effectively resulted in paralyzing the cryptocurrency exchanges for an activity that was not banned in India and had not caused an adverse impact on entities regulated by RBI However, power of RBI to operate and regulate the currency and credit system in the country (including cryptocurrencies) was upheld. It was also held that if an intangible property such as cryptocurrency could act under certain circumstances as money, then RBI was authorized to regulate it.

April 2020

Writ Petitions filed before the Supreme Court seeking removal of restrictions on crypto businesses by banks, pursuant to its judgement

June 2020

A note was reportedly moved in the Finance Ministry for inter-ministerial consultations. It was widely reported that the Government of India was seeking to introduce another bill to ban cryptocurrencies

July 2020

A webinar titled *Cryptocurrency in India: What the future holds* was organised by Khaitan & Co and CREBACO. Mr Subhash Chandra Garg, chairman of the Inter-ministerial Committee and former economic affairs / finance secretary, actively participated and explained the Government's position.

October 2020

According to news reports, banks had started lending to crypto businesses

December 2020

Banking operations started with retail crypto apps and physical stores, where people could walk in to trade Bitcoin

2021

January 2021

A comprehensive representation submitted to the Government of India by Khaitan & Co and CREBACO shedding light on the operations of the crypto asset market and suggesting regulations to safeguard the interest of all stake holders, especially the Government.

Source: CREBACO

E. BASIC CONCEPTS

E.1 Bitcoin

Bitcoin is a crypto asset invented in 2008 by an unknown person or group of people using the pseudonym Satoshi Nakamoto. It started in early 2009 when its implementation was released as an open-source software/network. It initiated a decentralized digital currency without a central bank, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries. In other words, transactions are made with no middlemen – meaning, no banks or central/regulating bodies.

There are no physical bitcoins, only balances kept on a public ledger that everyone has transparent access to, that – along with all bitcoin transactions – is verified by a huge amount of computing power. bitcoins are not issued or backed by banks or Governments but are validated by a network of nodes and miners.

In bitcoin, a transaction is a record informing the network of a transfer of bitcoin from one owner to another owner, which is confirmed by a network of decentralized parties. Ownership of bitcoins is established and accessed through digital keys pairs, Bitcoin addresses and digital signatures. Digital keys are created and stored offline (and at times – online) and consist of a mathematically-related Private-Public key-pair, created using the Elliptic Curve Digital Signature Algorithm (ECDSA). When transactions are broadcasted over the network, the SHA-256 hash function (other projects have used other hash functions) is used to verify data integrity (*i.e.* to establish that data has not been corrupted or modified during transmission). All bitcoin transactions are stored in blocks, which are linked (or "chained") together in a chronological sequence to form the "Blockchain". Cryptographic hash functions are generally used to verify block integrity and establish the chronological order of the Blockchain. Furthermore, hash functions are used as part of the Proof-of-Work (PoW) algorithm, which is a way of reaching consensus in a network and forms a prominent part of the bitcoin mining algorithm. There are other hash functions methods of achieving consensus such as Proof of Stake and Proof of Identity which are used in many other Crypto assets and are being experimented upon to achieve a mechanism that is secure, efficient and environment friendly.

E.2 Blockchain

A blockchain is a shared ledger where transactions are permanently recorded by appending 'blocks'. The blockchain serves as a historical record of all transactions that have ever occurred, from the genesis block to the latest block. The blockchain was mainly

incorporated in the Bitcoin network to make transactions incorruptible, validated and more reliable.

E.3 Broker-dealer license

As the industry evolves, there would be opportunities to issue broker-dealer licenses, similar to traditional stock market systems. These licenses can be issued by local or international exchanges, and small brokers who obtain such licenses can run businesses using the issuing exchange's liquidity. Such or similar licenses would be necessary to run portfolio management, consultancy, and advisory services. The regulatory authority can make sure that the broker is compliant enough. These licenses will also be necessary for payment gateways which would use the exchange platform for liquidity.

E.4 Central Bank Digital Currency (CBDC)

CBDC stands for Central bank digital currency. It is a digital form of fiat currency which can be transacted using wallets backed by blockchain and is regulated by the central bank. Though the concept of CBDCs was directly inspired by bitcoin, CBDC is different from decentralised virtual currencies and crypto assets which are not issued by the state and lack the 'legal tender' status declared by the Government.

CBDCs enable the user to conduct both domestic and cross border transactions which do not require a third party or a bank. Since several countries are running pilot projects in this space, it is crucial for India to launch its own CBDC making the Rupee competitive in international financial markets.

E.5 Crypto Assets

Cryptographically signed transmissions which hold a record in a distributed ledger based on consensus, are known as Crypto assets. They have a digital presence and can be accessed through a 'private key'. They are essentially a collection of entries in a ledger, which builds up a mechanism of copy-proof digital assets. The Bitcoin system is based on decentralized trust and heavily relies on cryptographic technologies such as:

a) Cryptographic hash functions (*i.e.* SHA-256, RIPEMD-160, etc);
b) Public Key Cryptography (*i.e.* ECDSA – the Elliptic Curve Digital Signature Algorithm)

E.6 Digital Asset Exchanges

Digital asset exchanges are virtual places where one can buy or sell crypto assets or other digital assets *via* a bank or credit card or from various coins on the open market. These exchanges are very similar to traditional stock exchanges. Currently there are over 400 known exchanges globally who trade digital assets. Exchanges are the gateways to enter and exit the crypto ecosystem. As such, it becomes crucial to regulate and monitor these exchanges.

E.7 Distributed Ledger Technology (DLT)

DLT is a decentralized database managed by multiple participants across multiple nodes. It may or may not be decentralized or open source. It can be an enterprise solution where transactions are recorded with an immutable cryptographic signature called a hash.

E.8 Decentralized Finance (DeFi)

DeFi or Decentralized Finance, is a product of smart contracting features backed by blockchain technology. It is a process of developing smart contracts that allows participants to offer and access financial services in a peer-to-peer format without relying on traditional intermediaries like banks, credit unions, or brokerages. It has the potential to extend benefits of decentralization to the banking space. Decentralized finance is an emerging phenomenon which aims to solve problems faced by many participants in CeFi (Centralised financial systems).

E.9 Ethereum

Ethereum is a blockchain-based decentralized platform for apps that run smart contracts and is aimed at solving issues associated with censorship, fraud, and third-party interference. Ethereum blockchain is cheaper, programmable, and is the most widely used blockchain for developing smart contracts on a decentralised platform. Over 90% of the tokens and smart contracts use Ethereum as their base platform.

E.10 Exchange Traded Funds

ETFs are advanced financial instruments crucial for institutional investors. ETFs are a type of security, that involves several other securities (in this case, crypto currencies and tokens). Based on the underlying values of the tokens, a tradable index value is derived using a formula-based methodology, which may differ with the type of ETF one is

investing in. There are high risk ETFs and blue-chip ETFs similar to traditional markets. An investor may individually invest in any number of industries or use various strategies, but ETFs ensure that the investor gets a balanced exposure to the entire market. ETFs are in many ways similar to mutual funds. However, they are listed and traded throughout the day and night, similar to other tokens.

E.10 Initial Coin Offering (ICOs)

Initial Coin Offering is an event in which new crypto tokens are issued to raise capital. Unlike an Initial Public Offering (IPO), equity is not diluted under ICOs, but new tokens are issued to raise capital. It is a decentralised way of raising funds through a smart contract. These tokens are usually known as utility tokens which can be used against services of the company. If the token is listed, the investor can trade it on a digital exchange and exit whenever the investor wants.

ICOs are typically used by start-ups to raise funds and fund the development of new cryptocurrencies. ICOs can be of two types- Private ICOs and Public ICOs. Private ICOs allow participation to only a limited number of investors, whereas Public ICOs set the general public as their target and allows anyone to become an investor globally.

E.11 Initial Exchange Offerings (IEOs)

Initial Exchange Offerings are ICOs that are handled by exchanges. The exchange administers the process on behalf of the startup that is looking to raise funds in lieu of the tokens it has issued. All projects that seek to raise funds through an IEO on an exchange's platform are screened by the exchange, thereby creating a verification process. The tokens are not offered to the general public, and only users of the exchange platform administering the IEO are allowed to participate in the process. The exchange platform's established base is beneficial for a company in receiving more funding for their projects. The exchange is responsible for processing the token distribution, sales and other responsibilities.

E.12 Mining and Miners

Mining is solving and record keeping of transactions taking place in near-to-real time by deploying electricity/energy, equipment and time. This is usually done on heavy duty computers equipped with ASICs or graphic cards to be more efficient. Miners (are also nodes) are individuals or group of individuals or organizations who deploy their resources on the crypto assets' blockchain to maintain records of the transactions. In return, they are paid by the newly originated crypto assets rewarded to them in their wallets. These rewards

vary from currency to currency, currently bitcoin gives a reward of 6.25 bitcoins to the miner who successfully mines one block of transactions.

The bitcoin system of trust is based on computation. Transactions are bundled into blocks, which require an enormous amount of computation to "prove" (or "confirm"), but only a small amount of computation to verify as "proven", in a process called mining. Mining serves two purposes in Bitcoin (POW): (i) Mining creates new bitcoins in each block, like a central bank printing new money. The number of bitcoins to be created is fixed and diminishes with time; (ii) Mining creates trust by ensuring that transactions are confirmed only when enough computational power has been devoted to the block that contains them.

Mining difficulty

Bitcoin nodes that mine actively regulate the rate of creation of new blocks. As more miners join, the rate of block creation will go up. As the rate of block creation goes up, the mining difficulty rises to compensate, which pushes the rate of block creation back down. The creation of new blocks must take an average of 10 minutes. The regulation is done by periodically adjusting the hash target value for blocks. Every 2,016 blocks (which ideally spans every 2 weeks, with each block taking 10 minutes to confirm) bitcoin nodes calculate a new difficulty based on the time it took to mine the last 2,016 blocks.

Mining reward

Solving the Proof of Work problem requires a lot of computing power, which costs money. To encourage participants to invest their resources in mining, bitcoin provides a reward in each successfully mined block. When a block is discovered, the discoverer will award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 6.25 bitcoins, Based on bitcoin's algorithm, this bounty halves every 210,000 blocks (*i.e.* approximately every 4 years). Eventually, the reward will be removed entirely when the limit of 21 million bitcoins is reached, by the year 2140. After that, transaction processing will be rewarded solely by transaction fees.

E.13 Over-The-Counter Trade, ATMs and Walk-in shops

Over the counter trades are necessary when transfer takes place between two parties directly. There are several exchanges and private institutions which facilitate transfer which is legally compliant and safe. Many walk-in shops have emerged in the industry globally where individuals can directly go, complete the formalities, and exchange crypto in real time. There are ATMs which issue crypto assets on deposit through cash or bank

transfers to facilitate real time transactions. Many countries like Japan, USA, Germany, etc. have operational crypto ATMs in place.

E.14 P2P Network and Ownership

Bitcoin is run over a peer-to-peer (P2P) network of computers, called nodes. Nodes are responsible for processing transactions and maintaining all records of ownership. Anyone can download the free open-source bitcoin software and become a node. All nodes are treated equally, and no single node is trusted, it must be noted that all miners in the network are nodes but not all nodes are miners. However, the system is based on the assumption that the majority of computing power (*i.e.* at least 51%) will come from honest nodes.

Ownership records are replicated on every node and bitcoin users possess digital keys that allow control over bitcoins recorded in a public ledger (the blockchain). The public ledger records transactions transferring ownership of a quantity of bitcoins from one owner to the another, like a double-entry bookkeeping ledger.

E.15 Pegged Currency

A pegged crypto asset is a crypto asset whose value is pegged to something else to create a stable currency. This means that the currency is stable and not volatile in nature making transactions free of market price volatility. Currently there are many pegged/tether tokens like USDT, USDC, etc which are backed by the US Dollar *i.e. 1 USDT = 1 USD.*

E.16 Public and Private Keys

The Private key (Privkey) is initially generated at random and is always kept secret. It is used by the current owner of bitcoins to digitally sign a bitcoin transaction when the owner authorizes the transfer to the new owner. A transaction's digital signature confirms ownership and can be used to verify that the transaction is authentic.

The Public key (Pubkey) is generated from the Private Key using a one-way cryptographic hash function. It is used by the new owner to validate a transaction's digital signature.

E.17 Security Token Offerings (STOs)

Security tokens are typically digitalized versions of traditional securities; they derive their value from a tradeable external asset. An STO is essentially a process in which a company sells it security tokens to the public in exchange for raising funds. The investors who invest

through an STO, receive direct benefits for holding a platform's tokens, and accordingly gain voting rights, dividends, and revenue shares in some cases.

An existing stock of a listed company can be converted into a token. This would ensure that settlements are done in real time instead of T+2 days and centralized depositories like NSDL or CDSL are not required.

E.18 Smart Contracts

Smart contracts are contracts whose terms are recorded in a computer language, instead of legal language. Smart contracts can be automatically executed by a computing system based on the instructions programmed, such as a suitable distributed ledger system.

E.19 Transaction Block

A collection of transactions on the bitcoin network is gathered into a block that can then be hashed and added to the blockchain.

E.20 Transaction Fee

Crypto asset transactions involve a small transaction fee. These transaction fees add up to account for the block reward that a miner receives when he successfully processes a block. A higher transaction fee enables a faster confirmation of the transaction in the blockchain.

E.21 Valuation of crypto assets

Bitcoin is a debt free instrument, which means that nobody owes the bitcoin to anyone. Bitcoin comes into existence as equity, and not debt - which is usually the mode of creation of currency in the current economic ecosystem. For example: the Reserve Bank of India takes responsibility (owes) value of Rupee thus every rupee note mentions *'I promise to pay the bearer…'*. However, bitcoin is a debt free instrument and belongs to a debt free decentralized network. Bitcoin is not backed by any asset and the absence of any centralized regulatory authority ensures that its price cannot be artificially manipulated.

There are many factors which affect the "value" of crypto assets (*please note that "value" is different than "price", the latter being dependent upon what users are actually willing to pay and is more perception-based*):

a) **Strength of the network:** The more the number of nodes, the stronger the ledger

they will have, adding to the strength of the network which can be global, national or private;

b) **Number of users:** Metcalfe's law of telecommunication states that the value of technology driven networks increases based on the number of users who use that technology. Similarly, with every increase in the number of users who deal in crypto assets, the value of that asset increases;

c) **Technology:** The value of a crypto assets also depends on what kind of technology that crypto asset is using.

d) **Demand and Supply:** Supply of every crypto asset is fixed as per the protocol of that particular crypto asset. Bitcoin's supply is fixed at 21 million coins and since it has a limited supply, it is perceived as more valuable;

e) **Consensus:** When people collectively agree that the value of a certain commodity is INR *x*, that value is automatically attributed to that commodity;

f) **Longer chain of blocks:** The longer the chain of blocks the older and more reliable network is.

How they are transmitted

When we send an email to somebody or forward a WhatsApp image, we send a copy of that content because we already have a copy with us on our devices. But when we transfer somebody a bitcoin, a cryptographically hashed signature is created which moves from one digital wallet to another, which means that the sender has no copy of what he has sent, but just a cryptographic hash code which confirms that the transaction can be verified on the blockchain. This is because bitcoin is not a 'coin' but a mere entry in the distributed ledger. Thus, it becomes a 'push' technology and not a 'pull' technology *i.e.* no third party can charge or debit one's account without one's will or consent, since one is in control of one's own private key. A bitcoin transaction tells the network that the owner of a number of bitcoins has authorized transfer of some of these bitcoins to another owner.

Each transaction contains one or more inputs, which are *debits* against a Bitcoin account. On the other side of the transaction, there are one or more outputs, which are *credits* to a Bitcoin account. The inputs and outputs (debits and credits) do not necessarily add up to the same amount; instead, outputs add up to slightly less than inputs and the difference represents an implied transaction fee, a small payment collected by the miner who solves the mathematical calculation to mine the block which includes his transaction in the blockchain. The transaction block contains proof of ownership of a number of bitcoins whose value is transferred in the form of a journal entry from the owner, secured by a digital signature, that can be independently validated by anyone on the bitcoin network.

E.22 Wallet

A wallet is a file that houses private keys. A wallet usually contains a software client which allows access to view and create transactions on a specific blockchain that the wallet is designed for. A wallet plays a very important role in usability of a token. Wallets are essential to trade, transact and store tokens in handheld or computer devices. Wallets must be regulated since they crypto assets belonging to users.

F. PROPOSED REGULATORY FRAMEWORK

F.1 Digital Asset Exchanges

Digital asset exchanges, being the first layer of protection for users engaging in buying or selling crypto assets, should be notified as "Reporting Entities" under the Prevention of Money Laundering Act, 2002 ("**PMLA**"). Reporting Entities under the PMLA also include financial institutions and payment system operators. This would require them to maintain records of all transactions they facilitate, verify the identity of the clients and identify beneficial owners of such clients.

Global standard-setting bodies such as the Financial Action Task Force ("**FATF**") have recommended that digital asset service providers be regulated under national Anti-Money Laundering laws for purposes of record retention, reporting and Know Your Customer ("**KYC**").[2]

Licensing these exchanges would provide a two-fold advantage. Firstly, it would provide the Government with a high degree of visibility over crypto asset transactions. Each transaction would be traceable to a particular identity if KYC requirements are complied with. Secondly, even consumers would be protected against fraudulent activities carried on through such exchanges since actual identity of each participant will be disclosed. Such regulations could be included under the Payment and Settlement Systems Act, 2007 to cover digital asset exchanges within the ambit of "payment systems"[3], which could be easily monitored by the RBI.

Alternatively, since digital asset exchanges offer an avenue to buy, sell and exchange digital assets, trading on these exchanges is akin to trading in traditional securities, as they face the same risk of market failures. This has been observed by the Securities and Exchange Commission of USA and other countries as well.[4] To mitigate these failures, it is recommended that Securities and Exchange Board of India ("**SEBI**") be the regulating body. The reasons for the same lies in the know-how of the SEBI in regulating and supervising traditional securities.

---

[2] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf

[3] Section 2(i), The Payment Settlement Systems Act, 2007

[4] SEC, *Statement on Digital Asset Securities Issuance and Trading*, November 16, 2018, at https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading; Board of the International Organization of Securities Commissions, *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, May 2019, at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf

SEBI should have the power to regulate digital asset exchanges through a license granted exclusively to such exchanges. Accordingly, amending Sections 11 and 12 of the SEBI Act, 1992 and expanding functions of SEBI to include digital asset exchanges is advisable.

It is recommended that related changes in several sub-clauses of Clause (2) of Section 11 should also be incorporated to empower SEBI to regulate other digital asset service providers including dealers, advisers, investment managers offering services in connection with investment in digital assets or derivative products with digital assets as underlying, so that SEBI has a complete control over such activities.

For the purposes of tax implications, if the platform is considered as providing a service, it would be liable to pay the following taxes under the current Indian laws:

a) **Commission Fee** *i.e.* fees paid for facilitating the transaction. The charge towards facilitations of the transaction is levied on both the parties, buyer as well as seller. If the platform is for facilitating exchange of crypto assets, the aforesaid charge is towards a "service" and would be subject to GST.

b) **Value-Added Service Fee** *i.e.* fee paid for price discovery, security of transactions, customer care, etc. Buyer of bitcoin would be charged a consideration for services rendered by platform and such a charge would be subject to GST. This is because such charges would be viewed as consideration towards supply of taxable services.

Further, as stipulated by section 2(45) of the Central Goods and Services Tax Act, 2017, *any person who owns, operates or manages a digital or electronic facility or platform for electronic commerce is an "electronic commerce operator"*. This would include the operator of digital asset exchange. Such an operator would be required to mandatorily obtain a GST registration. Moreover, such an operator would need to collect tax at source at the rate of upto 1% of the net value of sales made through the exchange by other suppliers, where consideration in respect of such sales is to be collected by the exchange.

To tax crypto assets under Income Tax Act, 1961, a uniform approach cannot be taken as the distinction in the usage of crypto assets as 'capital assets' (subject to tax under the income head 'capital gains') or 'business assets / stock-in-trade' (subject to tax under the income head 'profits and gains from business or profession') could be extremely subjective and vary on a case-to-case basis.

F.2 Initial Coin Offering ("ICO")

One of the most ICO friendly countries, Cayman Islands, does not have any specific regulations for crypto assets. They are interpreted within the existing legislative framework

depending upon the nature of the activity and the classification of the respective cryptoasset within the existing laws.[5] Further, the country uses the "*Howey* Test" to categorize an ICO as a 'security'. This is a four-factor landmark test devised by the U.S Supreme Court in 1946[6]. Under this test, a digital asset is identified as an 'investment contract' *i.e.* a 'security', if there is (i) monetary investment (ii) expectation of profit from such investment (iii) investment in common enterprise (iv) profits derived from efforts of other persons. These criteria have been evaluated and analysed for the present digital space by the Securities and Exchange Commission of USA in its statement on "Framework for 'Investment Contract' Analysis of Digital Assets".[7]

Other ICO dominant countries like Singapore have also recognized certain types of ICO within the ambit of their existing securities law. In 2017, the Monetary Authority of Singapore had released a 'A Guide to Digital Token Offerings' that clarifies the application of the present Securities and Futures Act with respect to offers or issues of digital tokens.[8]

One such recommendation to include ICO within the Indian securities law is that certain ICOs which meet all the requirements could be classified under 'collective investment schemes' and be subject to its regulations. As per the SEBI Act, 'collective investment scheme' is where multiple investors contribute into a pool with an aim to receive profits, income, or property, and the scheme is managed by on behalf of the investors who have an extensive level of control over the operation of the scheme and the management.[9] This definition is similar to nature of multiple ICOs and would satisfy the most important criterion of "*Howey* Test" *i.e.* expectation of profits from efforts of others.

Further, certain utility tokens like ICO could be directly covered under the existing definition of securities through a notification. ICOs that satisfy parameters of 'securities' could be notified under Section 2(h)(iia) of Securities and Contract Regulation Act, 1956. This would enable ICOs to get covered under a well-established regulatory regime managed by SEBI.

F.3 Initial Exchange Offering ("IEO")

As classified in the US by the SEC, IEOs are initial offerings of digital assets to raise capital and are offered directly on online trading platforms on behalf of companies for a fee. This

[5] https://www.careyolsen.com/sites/default/files/CO_CAY_Blockchain-and-Cryptocurrency-Regulation-2019-1st-Edition_10-18.pdf
[6] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946)
[7] https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets?hootPostID=7604b0fbb8f5d3e5ac775448e860b4e2
[8] https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Tokens-Offering---23-Dec-2019.pdf
[9] Section 11AA, Securities and Exchange Board of India Act, 1992

means that IEO will be subject to registration requirements and compliances as per the federal securities law of state where it is being offered[10]. Moreover, the SEC requires that in case of an IEO dealing with securities, the online trading platform on which it is offered needs to register as a national stock exchange or obtain an exemption to operate independently as an Alternative Trading System, which shall also be liable to comply with certain legal requirements[11]. India can also consider framing regulations specifically for IEO's not operating as a national stock exchange recognized by SEBI for greater transparency and investor protection, similar to USA's Alternative Trading System.

India lacks such a clear classification, and it can be said that a trading platform that is not a recognized stock exchange and does not comply with the Securities Contract (Regulation) Act, 1956 ("**SCRA**") cannot facilitate trading in securities. IEOs can therefore be regulated if they are made available to all digital asset exchanges covered under the Payment Settlement Systems Act or regulated by SEBI as mentioned above. This would ensure compliance with the mandatory disclosure norms and other requirements under securities law necessary for investor protection. Since IEOs are offered by exchanges, regulating such exchanges would effectively regulate IEOs.

F.4 Security Token Offerings ("STO")

The classification of STOs can be made under the Securities Contract (Regulation) Act, 1956 as they are 'securities' within the meaning of the said act. Only "recognized stock exchanges" may facilitate trading of such tokens.

In the USA, the SEC regulates the trading of STOs. The SEC has made it clear that whether any particular transaction involves offer or sale of a security – regardless of the terminology or technology used – depends on the facts and circumstances. The SEC provides for mandatory registration to ensure that all investors comply with proper disclosures and are subject to regulatory scrutiny.[12]

In Singapore, under the Securities and Futures Act, security tokens have been defined as digital tokens that constitute any capital markets product including securities, shares, debentures, units in a business trust, units in a collective scheme and derivative contracts[13]. As per the Singaporean securities law, security token would include shares, where such shares represent or confer ownership interest in a corporation, represent the liability of the token holder in the corporation and represent the token holder's mutual covenants with

[10] https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_initialexchangeofferings
[11] https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_initialexchangeofferings
[12] https://www.sec.gov/news/press-release/2017-131
[13] https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-3/1230199/singapore

other token holders in the corporation. Another example includes debentures, where such debentures evidence or constitute the indebtedness of the digital token issuer in respect of any money that is or may be lent to such issuer by token holders[14].

In Japan too, ICOs functioning similarly to securities have been subject to securities regulations and must adhere to their strict requirements. These include registration for licensing and following strict staffing and regulations for governance, among others[15].

As seen from the legal position adopted by various countries, security tokens are treated akin to securities. In India, if a similar approach is adopted, SEBI will assume jurisdiction to regulate such trading. Similar standards of scrutiny can be adopted by SEBI to investigate the realities of a transaction irrespective of classification given to it by the company, and whether the tokens involved fall within the meaning of 'securities' under the SCRA. The requirements would include adherence to existing regulations of SEBI that deal with eligibility, issuance and trading of securities.

Accordingly, compliance with related KYC regulations would also be required, ensuring greater transparency. This would also be in line with promoting anti-money laundering approaches under the PMLA and will also create a well-regulated platform, during the offering period as well as post the offering.

F.5 Smart Contracts

The use of smart contracts to automatically execute contracts best suit two types of transactions found in many contracts: (i) ensuring the payment of funds upon certain triggering events; and (ii) imposing financial penalties if objectives are not satisfied[16].

However, the enforceability of smart contracts has still not been conclusively determined even in the USA. Each state in the USA has been left to its own interpretation depending on considerations such as: (i) whether requirements of a 'contract' are fulfilled; (ii) whether the contract can be termed to be in writing; and (iii) determining the 'final agreement between the parties' that is the intent of the parties[17].

[14] Paragraph 2.3.1 and Paragraph 2.3.2 of Guide to Digital Token Offerings, https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Token-Offerings-26-May-2020.pdf
[15] https://www.securities.io/japan-tightens-up-sto-framework/
[16] https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/
[17] https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Since the position in India is even more ambiguous, a general idea can be extracted from one of the notifications released by the Telecom Regulatory Authority of India (TRAI)[18] in 2018. The notification defines smart contracts as *functionality of intelligent and programmable code which can execute pre-determined commands or busines rules to pre-check regulatory compliance without further human intervention and suitable for DLT system to create a digital agreement, with cryptographic certainty that the agreement has been honoured in the ledgers, databases or accounts of all parties to the agreement.*

To fall within the ambit of the Indian Contract Act, 1872, smart contracts will need to fulfil all the criteria under section 10 of the act *i.e.* such contracts would need to be made by free consent of the parties who have attained the age of majority and are of sound mind. Additionally, such contracts need to have a lawful object for a lawful consideration. This would make them valid contracts under the act and protection provisions and penalties would apply. This ensures that only those crypto assets/networks which are to be used as consideration or object of a contract, are recognised as smart contracts, effectively narrowing down their scope and making them easier to regulate.

A recommendation can be made for developers to code Know Your Customer ("**KYC**") and Anti Money Laundering ("**AML**") functionality into smart contracts that allow for asset transfers[19]. Under the Information Technology Act, 2000 analysis will have to be made for authentication of Digital Signatures, as smart contracts use cryptography for coding into the ledger-based system. They also use digital signatures/private keys for authentication and secured limited access. Therefore, digital signatures/private keys created using the blockchain technology will need to be recognized specifically under the said act.

F.6 Wallet

A digital asset-based wallet can be of different types, ranging from physical hardware wallets to web & mobile wallets. To take an example, crypto currency platforms such as ethereum or bitcoin can have several wallets developed using open-source code which provides for transacting of tokens on the blockchain. It has been clarified that such wallets do not function as banks or exchanges and the user is in complete control of its security and privacy[20.]

In India, RBI has powers under the Payment Settlement Systems Act, 2007 to frame regulations and directions for Prepaid Payment Instruments, in which case the wallet

[18] https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf
[19] https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
[20] https://kb.myetherwallet.com/en/getting-started/myetherwallet-an-introduction/

issuers would need to follow the robust KYC requirements and licensing and auditing norms to be regulated for consumer protection. Even if the wallets may not come under the scope of 'payment system' under section 2(i) of the Act, they could clearly be regulated by the RBI's notification for governing intermediaries in digital transaction, *Directions for opening and operation of Accounts and settlement of payment for electronic payment transaction involving intermediaries*.[21] Under this notification, intermediaries are broadly defined as those related to transfer of "monies". AML rules should be extended to cover crypto asset wallet providers that go unregulated.

Further, since wallet service providers store crypto assets for consumers, they should be made answerable to consumers as they share a fiduciary relationship with them. Such providers could be regulated under the Consumer Protection Act, 1986 with respect to 'deficiency in services' and 'unfair trade practices', if found defrauding the consumers or not being able to perform their functions adequately by being easily susceptible to hacking, etc.

Hosted wallets

Here the wallets are hosted on a platform by a service provider. The private keys also remain with the service provider, who takes the responsibility of broadcasting the transaction on the network. Hosted wallets may be vulnerable to hacking or other risks and hence it is not advisable to store larger amounts of funds in such wallets. New and emerging solutions involving a multi-factor authentication may eliminate these risks to some extent. Hosted wallet providers from India shall follow minimum compliance requirements.

Un-hosted wallets

These wallets are standalone wallets, and the private keys are in possession of the user. The user is responsible for broadcasting the transaction on the network every time using the public and private key functions. These wallets are also available in hardware form, wherein the private key of the wallet is stored on a device (similar to a USB pen drive), which makes its use simple. Here the responsibility of the keys remain with the user at all times

[21] https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=5379

F.7 Risk avoidance and safeguarding interests of users

The below table lays down certain instances and concerns surrounding the operation and use of crypto assets, along with the corresponding legal provision and our recommendations.

S. No	Incident	Current Legal Provisions	Recommendation
1.	Hack of crypto exchange/back-end software (i) What happens to the seized currency? (ii) How to safeguard the users of the crypto exchange?	Sections 43 and 66 of the Information Technology Act, 2000. Section 378 of the Indian Penal Code, 1860 ("**IPC**") relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. Section 424 of IPC- Dishonest or fraudulent removal or concealment of property.	Under S. 2(o) of Information Technology Act, 2000, the definition of "data" should be amended to include specific crypto assets to extend the benefits of the act to digital assets. Assuming this amendment is carried out, S.43 and S.66 of the act would then cover all activities related to hacking, data theft, damaging computers or computer programs, etc. Also, under S.43, damages by way of compensation are mandated so the owner will be appropriately compensated. Under S.2(i) of Payment and Settlement Systems Act, 2007 ("**PSS Act**"), the explanation to definition of "payment system" should be amended to include systems enabling crypto asset operations, to better

S. No	Incident	Current Legal Provisions	Recommendation
			safeguard the users of exchange as they will be monitored by RBI.
2.	Wrong transaction between parties (i) Who is responsible for typing the wrong address?	S. 22 of Indian Contract Act, 1872- Mistake as to matter of Fact. This talks about Mistake of identity or other essential matters of fact. Section 25, Payment and Settlement Systems Act, 2007- grounds for dishonour of transaction.	Under the Indian Contract Act, 1872, contract will not be void if mistake is caused by only one party. Thus, the person entering the wrong transaction address will be responsible. However, if the transaction is between regulated exchange(s), then the funds may be recoverable (subject to conditions). Amendment suggested above in the PSS Act would make the digital asset exchanges regulated by RBI.
3.	International payment outwards International payment inwards	Foreign Exchange Management (Current Account Transaction) Rules, 2000 Master Direction- Liberalised Remittance Scheme by RBI, 2016 – Permitting the Authorized Persons (mostly banks) under Foreign Exchange	This scheme permits the authorized persons to allow a resident to transact up to USD 2,50,000 per financial year. Under FEMA rules, there are specific instances only under which remittances could be made like studying abroad, overseas employment, etc.

S. No	Incident	Current Legal Provisions	Recommendation
	International investment outwards International investment inwards (i) How should the RBI Intervene in this transaction? (ii) How to declare the export of goods and services? If payment is received directly to an Indian exchange, how shall it be declared?	Management Act, 1999 ("**FEMA**") to facilitate transaction RBI Circular of 2016- Rupee Drawing Arrangement ("**RDA**")- for 'Authorized Dealer Category-1' banks RBI Master Direction- Money Transfer Service scheme for authorized persons as Indian agents under S.10(1) of FEMA, 1999 Foreign Exchange Management (Transfer or Issue of any Foreign Security) (Amendment) Regulations, 2004 RBI Master Direction- Direct Investments by Residents in Joint Venture/ Wholly Owned Subsidiary Abroad, 2016 Foreign Direct Investment (FDI) Policy	S. 10(1) of FEMA, 1999 should be amended to allow digital asset exchanges to be considered as 'Authorized Person' to deal in foreign exchange limited to proceeds from trading in crypto assets, thereby making digital asset exchanges governed and regulated by the RBI. This would enable digital asset exchanges to accept inward payments. Under the RDA, there is no limit for transfer. Whereas, for MTS, a limit of USD 2,500 per transaction is imposed. This only for authorized dealers under FEMA as approved by RBI. This lays out the guidelines for Overseas Direct Investment monitored and set by the RBI. The 'authorized dealers' are empowered to handle the investments. However, the Master Directions on Export of Goods and Services require that full value of exports should be received through authorized banking channels only and any set-off import payments should also be undertaken through

S. No	Incident	Current Legal Provisions	Recommendation
		RBI Master Direction- Foreign Investment in India, 2019	banking channels. Accordingly, receipt of payment against export of goods or services in cryptocurrency is not permitted.
4.	Short-term or Long-term investment/ profit or loss through trading	Securities and Exchange Board of India Act, 1992 ("**SEBI Act**") Securities Contract (Regulation) Act, 1956 Income Tax Act, 1961	Digital assets under STO and IEO arising in India need to be regulated like other securities on stock exchange and monitored by SEBI. However, these will be traded on a separate Digital Asset Exchange. Under S.2(h)(iia) of SCRA, the definition of "securities" can include certain STOs, IEOs, cryptocurrencies and other crypto assets as notified by the Government. Under S.4 of SCRA, digital asset exchanges should be included as a recognized similar to commodities or stock exchanges. Under S.11(2)(a) of SEBI Act, an explanation could be provided to deem crypto assets as securities which are to be regulated by the SEBI.

S. No	Incident	Current Legal Provisions	Recommendation
			If the above amendments are carried out, then under the Income Tax Act, 1961, tax implications on sale of crypto assets would be the same as for other securities, *i.e.*, if held for less than 12 months, short term capital gain shall arise on their transfer and if held for more than 12 months, long term capital gain shall arise on their transfer. However, if crypto assets are not considered to be "securities" and crypto exchanges are not considered to be "recognised" stock exchanges, short term capital gain shall arise if such assets are held for less than 36 months and long-term capital gain shall arise if they are held for more than 36 months. In certain cases, depending upon the frequency and volume of transactions, income from trading in crypto assets may be characterised as business income, taxable under the head "Profits and Gains from Business of Profession".

S. No	Incident	Current Legal Provisions	Recommendation
			A model Code of Conduct for this purpose would be shared separately by us.
5.	Use of crypto assets for money laundering	Prevention of Money Launder Act, 2002 ("**PMLA**") RBI Master Direction- Know Your Customer (KYC) Direction, 2016	To completely make use of this legislation and deter money laundering, the digital asset exchanges need to be included or monitored by Reporting Entities that are mandated to follow KYC norms with all of its participants. Under S. 2(wa) of PMLA, the definition of 'Reporting entity' should include digital asset exchanges or any organisation which can monitor the digital asset exchanges and report it to the regulator as per the compliances. Under S.3(xiii) of RBI Directions, 'Regulated Entities' should include digital asset operators to ensure transparency and trackability.
6.	Use of crypto assets for tax evasion (i) What if the transactions are mis declared?	Income Tax Act, 1961 Under Section 271(c) of the Income Tax Act, 1961, penalty of up to 300% of tax evaded could be levied in cases of concealment of income	If crypto assets are covered under the Income Tax Act, 1961, they may be subject to inquiries and scrutiny by the income tax department.

S. No	Incident	Current Legal Provisions	Recommendation
	(ii) How shall they get tracked?		
7.	Use of crypto assets for other illicit activities	Information Technology Act, 2000 Indian Penal Code, 1860	These two legislations cover a wide range of illicit activities. The Information Technology Act, 2000 specifically targets computer / digital offences while IPC covers offences in general.
8.	Use of crypto assets for trade manipulation Use of crypto for multilevel marketing or ponzi schemes	SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations 2003 S.12A of SEBI Act,1992- Prohibition of Manipulative and Deceptive Activities Securitisation and Reconstruction of Financial Assets and Enforcement of Securities Interest Act, 2002 Section 3, Competition Act, 2002- Anti Competitive Practices The Payment and Settlement Systems Act, 2007	All these Acts presently do not specifically govern trade manipulation for digital assets but govern general manipulation in the market. If crypto exchanges and crypto assets are regulated by SEBI (as above), these legislations would automatically apply. Thus, if the relevant amendments to SCRA and PSS Act, SEBI and RBI would be able to regulate them.

S. No	Incident	Current Legal Provisions	Recommendation
9.	Purchase/sale/investment of crypto assets in cash/off the books	Income Tax Act, 1961 Under Section 271(c) of the Income Tax Act, 1961, penalty of up to 300% of tax evaded could be levied in cases of concealment of income	Strong KYC/AML measures are suggested to prevent evasion of taxable income. As suggested, suitable amendments in PMLA, RBI KYC Norms, PSS Act, SCRA and SEBI Act will help overcome this.
10.	GST on sale, purchase, investment of crypto assets Other GST related considerations	Central Goods and Services Tax Act, 2017, respective State Goods and Services Tax Act, 2017 and Integrated Goods and Services Tax Act, 2017	If crypto assets are considered as "securities" under SCRA (as suggested above), trading in such assets would not attract GST. This is because the definitions of "goods" and "services" both exclude "securities", as defined under SCRA. A model Code of Conduct for this purpose would be shared separately by us. However, if crypto assets are not classified as "securities", then they would most likely be classified as "goods". Presuming that crypto assets would be considered as "goods" under GST, we wish to highlight the following areas of concern:

S. No	Incident	Current Legal Provisions	Recommendation
			(i) Levy of GST at each leg of purchase and sale would make crypto assets unattractive as investment options; (ii) GST is applicable only on supplies made "in the course or furtherance of business". This may reasonably lead one to the conclusion that casual trading or investment in crypto assets will not attract GST. (iii) Persons who supply goods through e-commerce operators are *mandatorily required to obtain GST registration*. Crypto exchanges would qualify to be e-commerce operators and as such, every individual selling crypto assets on such exchanges would technically require GST registration. Once registered, GST will have to be discharged on every sale transaction. (iv) Every e-commerce operator who collects consideration against sales made through it is liable to collect GST at source

S. No	Incident	Current Legal Provisions	Recommendation
			(@1%), which is available as a credit to the supplier. As such, crypto exchanges would technically be liable to collect GST on every sale transaction routed through them – which would represent an additional cost for the users. (v) A risk of double taxation exists if cryptocurrencies are used as a mode of payment (*i.e.* in exchange for goods and services). Presently, opportunities in India to settle payments through cryptocurrencies are limited. However, once their use becomes commonplace, this would become a far greater problem since cryptocurrencies would attract GST at the time of their purchase and also at the time of their use in exchange for goods or services that are subject to GST. This would result in the same value being taxed twice. Since the above issues represent major concerns and directly impact day-to-day trade, the Central Board of Excise Customs ("**CBIC**")

S. No	Incident	Current Legal Provisions	Recommendation
			should intervene and issue necessary guidance / clarification.
11.	Other tax considerations	Securities Transaction Tax Act, 2004	Since the act borrows and applies the definition of "securities" and "recognized stock exchanges" from the SCRA, the relevant amendments made in SCRA would make specified crypto-assets (which are similar to securities) taxable as "other securities" as per S.98 of the act. Other decentralised assets may not fall under the same.
12.	Mismanagement in exchange (i) How to safeguard interests of consumers?	SEBI Act, 1992. Consumer Protection Act, 1986.	It is suggested to cover Digital Asset Exchanges under the purview of SEBI so that SEBI could ensure investor protection. Wallets may not be directly regulated by SEBI but could be made liable for 'deficiency of services' / 'unfair trade practices' under the Consumer Protection Act, 1986 as they provide a service directly to consumers. Consumer Protection (E-Commerce) Rules, 2020 focus on transparency and contain provisions to make e-commerce entities

S. No	Incident	Current Legal Provisions	Recommendation
			(including those issuing e-wallets) liable along with the sellers. This would mean that both, Digital Asset Exchanges/e-Wallet issuers, would be liable for tokens sold/traded on such exchanges. Minimum compliance and third party approval (from a recognized institution) must be made mandatory for each token. The rules also focus on prevention of unfair trade practices. In the context of crypto assets, this may include putting up misleading statements, misrepresenting utility benefits of tokens, manipulating their value, etc. Further, these rules require sellers to provide an undertaking about their products, ensuring that the description guaranteed on the ecommerce platform matches with that of the actual product. In the context of crypto assets, this would mean that the benefits and uses of tokens/assets must match up to their actual uses. This would be particularly relevant for security tokens backed by a tangible asset since investors would seek to invest in these tokens based on the value they perceive out of that asset.

S. No	Incident	Current Legal Provisions	Recommendation
13.	Ransom in crypto assets	Section 364A of IPC- Kidnapping for ransom S.503 of IPC- Criminal Intimidation S.66-67, Information Technology Act, 2000- Computer Related Offences	Under S.503 of IPC, an explanation should be added to include digital property like crypto assets as "property" under the said provision.

G. CRYPTO ASSETS – TREATMENT AROUND THE WORLD

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF launched regulations for virtual assets in June 2019, called *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. This guidance aimed to help countries and virtual asset service providers understand their AML and counter-terrorist financing obligations, and effectively implement the FATF's requirements as they apply to the virtual asset sector. The FATF strengthened its standards to clarify the application of AML and counter terrorist financing requirements on virtual assets and virtual asset service providers. Countries are now required to (i) assess and mitigate their risks associated with virtual asset financial activities and providers; (ii) license or register providers; and (iii) subject them to supervision or monitoring by competent national authorities. Virtual asset service providers are subject to the same FATF measures that apply to financial institutions.

In view of the above, countries are now obligated to comply with all FATF requirements, as otherwise there is a risk of being included in the *grey list* of countries.

The below table provides a list of countries which have introduced regulations governing crypto assets, and names of the regulatory authorities in such countries[22]:

S. No	Country	Primary Regulatory Body	Status [as of 31 December 2020]
1.	Argentina (G20)[23]	Comisión Nacional de Valores (CNV) / Central Bank of Argentina	Partly Regulated
2.	Australia (G20)	Australian Government (AUSTRAC)	Regulated
3.	Brazil (G20)[24]	Comissao De Valores Mobiliarios	Unregulated

[22] https://en.wikipedia.org/wiki/List_of_financial_regulatory_authorities_by_country; https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory; https://www.bis.org/regauth.htm
[23] https://www.loc.gov/law/help/cryptocurrency/argentina.php
[24] https://www.loc.gov/law/help/cryptocurrency/brazil.php#:~:text=Cryptocurrencies%20have%20yet%20to%20be%2

S. No	Country	Primary Regulatory Body	Status [as of 31 December 2020]
		(CVM) / Central Bank of Brazil (BACEN)	
4.	Canada (G20)	Canadian Securities Administrators (CSA)	Regulated
5.	China (G20)	The National Internet Finance Association (NIFA)	Partly Regulated (Several banking restriction. Coin offerings are prohibited)
6.	Estonia	The Estonian Government	Regulated
7.	France (G20)[25]	Autorité des Marchés Financiers (AMF)	Regulated
8.	Germany (G20)	Germany's Federal Financial Supervisory Authority (BaFin)	Regulated
9.	Gibraltar	Gibraltar Financial Services Commission	Regulated
10.	Hong Kong	Hong Kong's Securities and Futures Commission (SFC)	Regulated
11.	India (G20)	RBI, Ministry of Finance, Supreme Court of India	Unregulated and await regulation
12.	Indonesia (G20)	Financial Services Authority	Partially Regulated
13.	Italy (G20)	Italian Ministry of Economic	Regulated
14.	Japan (G20)	Payment Services Act (PSA) / Financial Instruments and Exchange Act (FIEA)	Regulated
15.	Malaysia	Securities Commission of Malaysia (SC)	Regulated (IEOs) Further regulations awaited in 2021
16.	Malta	Malta Financial Services Authority (MFSA) Malta Digital Innovation Authority	Regulated

0regulated%20in%20Brazil.&text=Recently%2C%20the%20Brazilian%20Securities%20and,be%20acquired%20by%20investment%20funds

[25] https://www.loc.gov/law/help/cryptocurrency/france.php; https://news.bitcoin.com/france-new-cryptocurrency-measures-fight-anonymous-transactions/

S. No	Country	Primary Regulatory Body	Status [as of 31 December 2020]
		(MDIA)	
17.	Mexico (G20)[26]	CNBV - Comision Nacional Bancaria y de Valores	Regulated
18.	Philippines	Philippines Securities and Exchange Commission (SEC)	Partially Regulated
19.	Russia (G20)	Ministry of Finance of the Russian Federation	Regulated
20.	Saudi Arabia (G20)[27]	Saudi Arabian Monetary Authority (SAMA)	Partly Regulated
21.	Singapore	The Monetary Authority of Singapore (MAS)	Regulated
22.	South Africa (G20)	South African Reserve Bank (SARB)	Unregulated, Bill proposed and awaiting regulations 2021
23.	South Korea (G20)	Financial Action Task Force (FATF)	Regulated
24.	Spain	Spain's National Securities Market Commission (CNMV)	Regulated
25.	Sweden	Sweden's Financial Supervisory Authority (FSA)	Partly regulated, Waiting for further guidelines in 2021
26.	Switzerland	Swiss Federal Tax Administration (SFTA)	Regulated
27.	Thailand	Thailand's Security Exchange Commission (TSEC)	Regulated
28.	Turkey (G20)[28]	Banking Regulation and Supervision Agency (BRSA) / Capital Markets Board of Turkey	Unregulated

[26] https://www.loc.gov/law/help/cryptocurrency/mexico.php#:~:text=In%20March%202018%2C%20Mexico%20enacted,as%20a%20means%20of%20payment; https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/mexico

[27] https://hackernoon.com/saudi-arabias-ban-on-bitcoin-is-unlikely-to-last-lo1y3xjg

[28] https://www.mondaq.com/turkey/fin-tech/985690/will-cryptocurrencies-be-regulated-in-turkey-soon

S. No	Country	Primary Regulatory Body	Status [as of 31 December 2020]
		(CMB) / Financial Crimes Investigation Board of Turkey (MASAK)	
29.	United Arab Emirates	Securities and Commodities Authority	Regulated
30.	United Kingdom (G20)	Financial Conduct Authority (FCA)	Regulated
31.	United States (G20)	Securities & Exchange Commission (SEC)	Regulated in majority states

Countries marked as "regulated" in the table above, have major guidelines in place for crypto assets, covering aspects such as taxation, settlement and process of declaration. Countries marked as "partly regulated" do not yet have in place guidelines for a few of these aspects.

H. BHARATCHAIN – INDIA'S OWN DECENTRALISED NETWORK

In a country as large as India, managing data among various departments, jurisdictions and States is a major challenge. Indian Government is taking strong steps to maintain data privacy based on the General Data Protection Regulation ("GDPR") introduced by the European Union. Our country is moving strongly towards digital innovation under the guidance of Prime Minister Narendra Modi with the digital India project. We believe that Indian developers are always ahead when it comes to innovation in technology.

Blockchain is a solution to many of the problems which our country faces relating to data privacy and development. We propose **BharatChain**, an India-centric decentralized blockchain which ensures that all nodes are maintained within the country, while being open-source for our citizens and other developers globally, making it truly decentralized and immutable. This blockchain will also enable development of advanced decentralized applications that our developer community can leverage upon.

As per the data received by CREBACO, India has over 35,000 blockchain developers who are using over 5+ languages to develop smart contracts based on blockchain. However, when it comes to development, there are a few expensive international blockchains that provide a platform for DAPPs and a few public blockchains that burn a lot of 'gas fee' (processing fee) for each contract or transaction.

This limits development and puts data privacy at risk, despite it being encrypted, and restricts the opensource aspect at several stages due to regulations. BharatChain would be completely open-source and used for storing Government data, business transactions, banking, smart contracts, etc.

We propose that all nodes and the data remain within India and at the same time we propose to install a surveillance node exclusively for the regulatory authority so that it can monitor transactions and make sure that there are no illicit activities, and the network is not misused. This concept is not very new, as several countries like Estonia and UAE have already installed it and many others are exploring possibilities or running pilot projects.

Key features

Enables CBDC

The key feature of this chain will be that it will easily enable the Central Bank Digital Currency which is expected to be a bold step towards digital payments. Many countries are already running pilots on this and in the next 24 months CBDCs are expected to be widely used by many platforms. Development of India's own digital currency is a must to be a part of the global CBDC ecosystem. We must not forget that with the strength of the Indian population, India's CBDC could easily be a global leader in digital currencies.

Other Features

- Decentralized (within India): All the nodes will remain within India.
- Open-source: Global developers can develop on this blockchain, on account of it being open source
- Surveillance & Forensics node(s) for the regulatory authority: The regulatory authority established by the Government will possess a forensic node having higher authority. This node can amend transactions or block smart contracts, subject to acceptance by other nodes and other conditions.
- Easy monitoring: Government may monitor the activities and transactions taking place on the blockchain platform, thereby maintaining a pre-determined minimum compliance standard.
- Reduction in illicit activities: Any fraudulent or suspicious smart contract can be frozen.
- Controlled node behavior: Minimum requirements must be met if a node wants to join the network.
- Compliance and prerequisites for development: Certain development and compliance standards must be met if a financial smart contract is to be issued using BharatChain.

Opportunities and Advantages

- Development of a community
- Will support skill development

- Many start-ups and businesses will be born around this chain
- An estimated 25000 jobs could be created in the first year itself
- Developer funding and grants
- Will enable India's own Central Bank Digital Currency.

We hope the Government of India encourages this ecosystem and initiates the BharatChain project at the earliest. Khaitan & Co and CREBACO would be happy and privileged to partner with the Government for development of BharatChain and submit a detailed project report for this purpose.

I. CONCLUSION

The suggestions and recommendations put forth in this representation aim at balancing the interests of all stakeholders. Considering that the domain of crypto assets is complex and evolving, any attempt at regulation would require a concerted effort from the Ministry of Electronics and Information Technology, Ministry of Finance as also regulatory bodies such as the RBI and SEBI.

A regulatory framework could go down one of two routes. Suitable amendments could be made in existing regulations so as to make them applicable to crypto assets (*regulation by analogy* method). This would entail conferring additional powers upon existing institutions so as to enable them to regulate providers and users of crypto assets. Alternatively, the Government may decide to formulate a separate and dedicated legislation to govern crypto assets. This legislation would be a self-contained code and may provide for establishment of an independent regulatory body at a central level to govern the crypto industry. In the meantime, the Government may also consider issuing circulars and guidelines to existing players in the crypto industry to ensure that safeguards and compliances at a preliminary level are put in place.

Decentralised ecosystems are unprecedented and hold great potential. We must learn from the leading countries of the world who have regulated this space, also highlights a fact that banning something like this is not even an option. The leading nations are encouraging startups arising in this industry to research, develop and scale. India is mainly looking at the Blockchain technology and the possibilities of crypto assets cannot be ignored.

The apprehensions surrounding this new technology need to be objectively pegged against its benefits and any legislation on the subject should be drafted from the touchstone of advancing the greater economic good. Effective and robust regulations governing crypto assets would ensure that benefits of this new technology are harnessed, and the associated risks are minimized.

J. VOICES FROM THE INDUSTRY

Achyuta Ghosh
Head of Research, NASSCOM

NASSCOM®

The good news is that enterprises and Governments have started pragmatic evaluation of potential use cases before implementing blockchain solutions. This is already resulting in credible and encouraging results which have helped drive commercial and developmental adoption. Blockchain applications have also evolved, become much easier to implement and manage, and are opening the door for more enterprises to consider them as part of their large-scale digital transformation investments.

Leading blockchain jurisdictions are driving growth and innovation in the ecosystem through a light touch, collaborative and consultative regulatory approach. A consultative and enabling regulatory approach by India can help drive the growth of the ecosystem.

Ankit Gaur
Founder & CEO, EasyFi Network

easyfi

India is poised at the cusp of an innovation explosion in the blockchain technology space. We are witnessing this in the Fintech industry with "DeFi", which is opening new horizons and changing the way we know finance. We are moving towards decentralization in a big way, where we are seeing participation from authorities as well. It is evident by in the manner in which discussions are taking place, that digital assets could soon become mainstream, a case in point being CBDCs.

Jagdish Pandya
CEO, BlockOn

Block On

India is now crawling. Cryptocurrency is still in its nascent stages in India. Once regulated, it will become a credible profession and the Government can stop its misutilization by scammers.

Innovation and technology should not be controlled or banned. If they are banned, the country of the ban is usually punished, whereas other jurisdictions expedite development. Cryptocurrencies are here to stay – Better regulate than ban them.

Manoj Jain
Co-Founder and CEO, Bitfia Labs

bitfia

Indian crypto industry needs a regulatory framework to operate, and common Indians need protection in law from unscrupulous elements operating in this space. With the global crypto market cap crossing 1 Trillion, the decentralised economy is here to stay. I believe it is the best time for India to introduce a regulatory framework starting from clear taxation rules to compliances for entities operating in this space.

Clear laws in this year's Union Budget will give a boost to a lot of young blockchain startups and help them access capital. Also, the bitcoin grey market will move to a regulated form helping both, the Indian crypto startups and the Government of India, who can collect taxes.

Nischal Shetty
Founder and CEO, WazirX

Crypto industry has been one of the fastest growing industries globally. Countries across the world are moving towards positive regulation in order to grab the early mover advantage in this industry. US has several billion-dollar crypto startups and has attracted billions in investments. India hasn't been able to attract any sizeable capital investments in crypto due to lack of regulatory clarity.

Rahul Pagidipati
CEO, ZebPay

We estimate that Indians currently own less than 1% of the world's Bitcoins. We risk facing a *Bitcoin gap*, where we lag behind countries like China, US, Japan, and others who have moved ahead on regulation. If Bitcoin becomes a reserve asset by 2030, when India may be the 3rd largest economy, would we have the 3rd largest bitcoin holding? Passing healthy regulation in 2021 would protect and reassure investors and allow Indians to claim their fair share of this vital asset. Regulation would also unleash innovation in blockchain and bring new solutions to poverty and inequality.

Rashmi Deshpande
Partner, Khaitan & Co

Lack of regulation always leads to uncertainty for any business. However, if the laws are very much in place, the business is recognised by the Government and a sudden banishment is out of question. Moreover, investors and other stakeholders are assured of continuity of the business. The State gets another source of revenue with a business that legitimately adds to the GDP of the country.

The intended representation aims to propose, among other things, a modification in existing laws such as FEMA and SEBI to regulate flow of money and the option of raising capital. Similarly, amendments in the Income tax and GST laws would provide clarity on applicability of taxes and finally the Indian Penal Code along with the Information Technology laws would recognise specific acts as offences, in order to impose penalties.

Sandeep Nailwal

Blockchain technology has the potential to bring in a high level of transparency into any process which involves multiple parties. A good example of this is "DeFi", a USD 18 billion industry, in which

Co-Founder and COO, MATIC Network

blockchain technology removes middlemen in financial transactions and gives maximum benefit of borrowing or lending to individuals transacting with each other.

The need of the hour is to have a proper legal framework around blockchain technology and cryptocurrencies so that India can become the world leader in this technology. Other countries like China are already experimenting with a nationwide cryptocurrency and we too, should create the environment to allow companies in India to build the same.

Sathvik Vishwanath
CEO, Unocoin

Cryptocurrencies and blockchain technology are at the forefront of manifesting investment, employment, and innovation opportunities in developed countries. India has lagged when it comes to technology in the past few decades and the circular from RBI in April 2018 pushed the industry back by 21 months. It is very important to acknowledge and understand that this technology is here to stay and will lead to new ways of doing transactions and storing information in the future.

Regulations need to catch up so that bad actors will not take advantage of it. On the other side, a promising future can be ensured by embracing the change and staying abreast with this developing industry.

Sidharth Sogani
Founder and CEO, CREBACO Global

India had lost the opportunity to be a global leader once before – global internet and personal computer industry flourished between 1985 to 1995, but India did not have any regulations till the Information Technology Act was enacted in 2000s. I do not want the same to happen with Blockchain and Crypto industry; this can be considered to be another opportunity to shine. Stopping or banning it is not even an option. The earlier the Government regulates this space, the faster we can grow globally. Indian developers and entrepreneurs have the potential to be at the forefront of this industry worldwide, while operating from India.

Regulations are important, but they are always followed by innovation. India should encourage this decentralized technology to evolve. Remember, the *Wright Brothers* did not have a pilot's license.

Sumit Gupta
Co-Founder and CEO, CoinDCX

We are happy to support CREBACO and the prominent law firm Khaitan & Co, who are together submitting a representation on cryptocurrency regulations to the Government of India. We believe, as the cryptocurrency market is growing and gaining more prominence, it is important that the Indian Government should consider adopting smart and sensible crypto regulations. Indian lawmakers need to share Indian crypto industry insights, suggestions on how adopting certain regulations will benefit the Indian economy and discourage bad actors. The combination of such insights and findings in the representation will act as an important tool to lawmakers, as it will help them to better evaluate the benefits of positive crypto regulation.

K. GLOSSARY

Airdrop	A marketing campaign that distributes a specific cryptocurrency or token to an audience.
All-Time-High (ATH)	The highest point (in price, in market capitalization) that a cryptocurrency has been in history.
All-Time-Low (ATL)	The lowest point (in price, in market capitalization) that a cryptocurrency has been in history.
Addresses	(Cryptocurrency addresses) are used to receive and send transactions on the network. An address is a string of alphanumeric characters but can also be represented as a scannable QR code.
Agreement Ledger	An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.
Alt Coin	An alt coin is a Bitcoin alternative. There are many hundreds of alt coins currently being marketed.
Attestation Ledger	A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.
ASIC	ASIC is an acronym for "Application Specific Integrated Circuit". ASICs are silicon chips specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.
Arbitrage	Arbitrage is the practice of quickly buying and selling the same asset in different markets to take advantage of price differences between the markets.
Ashdraked	A situation where you lose all your money, more specifically when you lose all your money shorting Bitcoin trading against the trend.
Atomic Swap	A way of letting people directly exchange one type of cryptocurrency for another on a different blockchain or off-chain without a centralized intermediary such as an exchange.
Automated Market Maker (AMM)	An automated market maker (AMM) is a system that provides liquidity to the exchange it operates in through automated trading.
Block	Blocks are packages of data that carry permanently recorded data on the blockchain network.
Blockchain	A blockchain is a shared ledger where transactions are permanently recorded by appending blocks. The blockchain serves as a historical record of all transactions that ever occurred, from the genesis block to the latest block, hence the name blockchain.
Block Height	Block height refers to the number of blocks connected in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.
Block Reward	A form of incentive for the miner who successfully calculated the hash in a block during mining. Verification of transactions on the blockchain generates new coins in the process, and the miner is rewarded a portion of those.
Bagholder	A person who holds large quantities, or bags, of a cryptocurrency. Often used to describe such a person when the price of that cryptocurrency is declining.
Bear	A person who is pessimistic about market prices and expects them to decline. This person is also known to be "bearish" about the market or price.
Bear Trap	A technique played by a group of traders, aimed at manipulating the price of a cryptocurrency. The bear trap is set by selling a large amount of the same cryptocurrency at the same time, fooling the market into thinking there is an upcoming price decline. In response, other traders sell their assets, further driving the price down. Those who set the trap then release it, buying back their assets at a lower price. The price then rebounds, allowing them to make a profit.
BitLicense	A business license issued to cryptocurrency companies in New York, created and provided by the New York State Department of Financial Services (NYSDFS).
Bitcoin ATM (BTM)	A machine from which you can withdraw bitcoin.
Bitcoin Improvement Proposal (BIP)	A technical design document providing information to the Bitcoin community, describing new proposed features, processes or environments affecting the Bitcoin protocol. Suggested changes to the protocol are submitted as a BIP. The BIP author is responsible for soliciting feedback and consensus for his or her suggested improvements within the community and documenting dissenting opinions.
Bits a.k.a mBTC	A sub-unit of one bitcoin's widely known as satoshi. There are 1,000,000 bits in one bitcoin.
Block Explorer	An online tool to view all transactions that has taken place on the blockchain, network hash rate and transaction growth, among other useful information.
Bollinger Band	A tool developed by Bollinger to help in the recognition of systemic pattern recognition in prices; it is a band that is plotted two standard deviations away from the simple moving average, or exponential moving average in some cases.
Bonding Curve	A bonding curve is a mathematical curve that defines the relationship between the price and the supply of a given asset.
Bots	Automated trading software bots that execute trade orders extremely quickly, based on a preset algorithm of buy-and-sell rules.
Brute Force Attack (BFA)	A method of trial-and-error in which automated software generates and tries many possible combinations in order to crack a code or key.
Bubble	A bubble describes a situation where market participants drive prices up above their value, which is usually followed by a steep, rapid drop in prices as the market corrects.
Bug Bounty	A reward offered for finding vulnerabilities and issues in computer code. It is often offered by

	cryptocurrency companies like protocols, exchanges and wallets to identify potential security breaches or bugs before they are exploited by unfriendly parties.
Bull	A person that is optimistic and confident that market prices will increase, this person is also known to be "bullish" about the market or price.
Bull Trap	A bull trap occurs when a steadily declining asset appears to reverse and go upward, but soon resumes its downward trend.
Burned	Cryptocurrency tokens or coins are considered “burned” when they have been purposely and permanently removed from circulation.
Buy The Dip (BTD/BTFD)	An enthusiastic exclamation by supporters of a cryptocurrency to buy while prices are at a low point. When a coin is rallying higher and there is a dip in price, you should buy all such dips as the price is expected to keep going higher.
Buy Wall	A buy wall is a disproportionately large buy limit order placed on a cryptocurrency exchange.
Byzantine Fault Tolerance (BFT)	Byzantine Fault Tolerance (BFT) is the property of a computer system that allows it to reach consensus regardless of the failure of some of its components.
Byzantine Generals' Problem	A situation where communication, that requires consensus on a single strategy from all members within a group or party, cannot be trusted or verified.
Central Ledger	A central ledger refers to a ledger maintained by a central agency. Bitcoin is decentralised because it is not maintained by a central body but a community on the internet.
Confirmation	The successful act of hashing a transaction and adding it to the blockchain.
Consensus	Consensus is achieved when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other.
Cryptographic Hash Function	Cryptographic hashes produce a fixed-size and unique hash value from variable-size transaction input. The SHA-256 (Signature Hash Algorithm) computational algorithm is an example of a cryptographic hash.
Candlesticks	A candlestick chart is a graphing technique used to show changes in price over time. Each candle provides 4 points of information opening price, closing price, high, and low. Also known as "candles" for short.
Capitulation	A period of strong selling activity, where investors give up their positions and sell their holdings as quickly as possible.
Cash	Cash is the most liquid form of money: physical coins and banknotes in the narrowest sense of the term.
Central Bank Digital Currency	CBDCs are digital currencies issued by a central bank whose status as legal tender depends on Government regulation or law.
Centralized	A centralized organizational structure is one in which a single node or a small number of them are in control of an entire network.
Centralized Exchange (CEX)	Centralized exchanges (CEXs) are a type of cryptocurrency exchange that is operated by a company that owns it in a centralized manner.
Chain Split	Chain splits are another term used to describe cryptocurrency forks — the separation of a single original coin into several independently managed projects.
Cipher	A cipher is any algorithm that can be used to encrypt and decrypt information.
Circulating Supply	The best approximation of the number of coins that are circulating in the market and in the general public's hands.
Cloud Mining	Cryptocurrency mining with remote processing power rented from companies.
Co-Signer	A person or entity that has partial control and access over a cryptocurrency wallet. Usually a multi-sig wallet.
Coin	A coin can refer to a cryptocurrency that can operate independently or to a single unit of such cryptocurrency.
Coinbase	In mineable cryptocurrencies, a coinbase is the number of coins that are generated from scratch and awarded to miners for mining every new block. Coinbase is also a name of a crypto exchange in the US
Confirmation Time	The time elapsed when a transaction is submitted to the network and the time it is recorded into a confirmed block.
Cold Storage	Offline storage of cryptocurrencies, typically involving hardware non-custodial wallets, USBs, offline computers, or paper wallets.
Cold Wallet	A cryptocurrency wallet that is in cold storage, *i.e.* not connected to the internet.
Collateralized Debt Position (CDP)	A collateralized debt position is held by locking collateral in smart contracts to generate stablecoins.
Consortium Blockchain	A privately owned and operated blockchain where a consortium shares information not readily available to the public, while relying on the immutable and transparent properties of the blockchain.
Correction	A correction is a pullback of an asset's price of at least 10% to adjust for over-valuation.
Cryptoasset	A cryptoasset is any digital asset that uses cryptographic technologies to maintain its operation as a currency or decentralized application.
Cryptocurrency	Cryptocurrencies are digital currencies that use cryptographic technologies to secure their operation.
Cryptographic Hash Function	Cryptographic hash functions produce a fixed-size hash value from a variable-size transaction input.
Cryptography	A field of study and practice to secure information, preventing third parties from reading information to which they are not privy.
Cryptojacking	The use of another party's computer to mine cryptocurrency without their consent.

Custodial	Custodial cryptocurrency businesses are the ones that are in possession of their customers' funds for the duration of the use of their services.
Cypherpunk	The cypherpunk movement promotes the use of cryptography and other privacy-focused technologies to advance social and political progress.
Dapp	A decentralized application (Dapp) is an application that is open source, operates autonomously, has its data stored on a blockchain, incentivised in the form of cryptographic tokens and operates on a protocol that shows proof of value.
DAO	Decentralized Autonomous Organizations can be thought of as corporations that run without any human intervention and surrender all forms of control to an incorruptible set of business rules.
Distributed Network	A type of network where processing power and data are spread over the nodes rather than having a centralized data center.
Difficulty	Difficulty, in Proof-of-Work mining, is how hard it is to verify blocks in a blockchain network. In the Bitcoin network, the difficulty of mining adjusts verifying blocks every 2016 blocks. This is to keep bitcoin block verification time at ten minutes.
DeFi	DeFi (decentralized finance) is the creation of an ecosystem of financial tools built on blockchain.
Dead Cat Bounce	A temporary recovery in prices after a prolonged decrease.
Decentralized	Decentralization refers to the property of a system in which nodes or actors work in concert in a distributed fashion to achieve a common goal.
Decentralized Exchange (DEX)	A peer-to-peer exchange that allows users to buy and sell cryptocurrency and other assets without a central intermediary involved.
Decryption	The process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.
Delisting	The removal of an asset from an exchange either as a request from the project team or as a decision made by the exchange.
Deflation	Reduction of the general level of prices in an economy. May also refer to deflationary monetary policy, such as Bitcoin, where there is a fixed supply of coins.
Delegated Proof-of-Stake (dPOS)	A consensus mechanism where users can vote for delegates producing blocks on the blockchain, with votes proportional to their stake. It aims to increase efficiency and environmental friendliness of blockchain consensus protocols.
Depth Chart	A graph that plots the requests to buy (bids) and the requests to sell (asks) on a chart, based on limit orders. The chart shows the point at which the market is most likely to accept a transaction.
Derivative	A contract deriving its value from the performance of an underlying asset, index or interest rate.
Derivatives Market	A public market for derivatives, instruments such as futures contracts or options, which are derived from other forms of cryptocurrency assets.
Deterministic Wallet	A type of wallet that derives keys from a starting point called a seed. As long as you have this seed, you are able to backup and restore any wallet.
Digital Commodity	An intangible asset that is transferred electronically and has a certain value.
Digital Currency	Digital currency, also known as digital money or electronic money or electronic currency, is a type of currency available only in digital form, allowing for instantaneous transactions and borderless transfer-of-ownership.
Digital Identity	Digital representations and storage of personal information such as name, address, social security number and more; on the blockchain, digital identity can be decentralized and used for identity verification in a secure manner.
Digital Signature	A digital code generated by key encryption that is attached to an electronically transmitted document to verify its contents and the sender's identity.
Distributed Denial of Service (DDoS) Attack	A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable, disrupting services of a host connected to the internet, by overloading the system with requests so that legitimate requests cannot be served.
Distributed Ledger	Distributed ledgers are ledgers in which data is stored across a network of decentralized nodes. A distributed ledger does not necessarily involve a cryptocurrency and may be permissioned and private.
Distributed Ledger Technology (DLT)	The technology underlying distributed ledgers. This term is most often discussed in the context of enterprise use cases around adoption of distributed ledger technology.
Dominance	Also known as BTC Dominance or Bitcoin Dominance, it is an index that compares the market capitalization of Bitcoin with the overall market cap of all other cryptocurrencies in existence.
Double Spending	A situation where a sum of money is (illegitimately) spent more than once.
Dump	To sell off all your coins.
Dumping	The action of collective market selloffs, creating downward price movement to sell off all your coins.
Dust Transactions	Minuscule transactions that flood and slow the network, usually deliberately created by people looking to disrupt it.
Dusting Attack	When a scammer sends tiny amounts of a cryptocurrency to random users' wallets, and then analyzes and tracks the subsequent transactions to identify the specific users behind each address.
Eclipse Attack	When majority of peers on the network are malicious and monopolize the network to prevent specific nodes from receiving information from honest nodes.

Ethereum	"The Other Blockchain" Ethereum is a blockchain-based decentralized platform for apps that run smart contracts, and is aimed at solving issues associated with censorship, fraud and third-party interference.
Exchange	Where you Buy or Sell bitcoin and altcoins to or from your bank or credit card or from various coins on the open market. There are internal wallets, yet the exchanges have the private keys to the wallets so it's never safe to store the cryptocurrency on these Exchanges for a long period of time.
ERC-20	A token standard for Ethereum, used for smart contracts implementing tokens. It is a common list of rules defining interactions between tokens, including transfer between addresses and data access.
ERC-721	A token standard for non-fungible Ethereum tokens. An Ethereum Improvement Proposal introduced in 2017, it enables smart contracts to operate as tradeable tokens similar to ERC-20 tokens.
Enterprise Ethereum Alliance (EEA)	A group of Ethereum developers, startups and large corporations working together to commercialize and use Ethereum for business applications.
Escrow	An escrow is a contractual arrangement in which a third party receives and disburses money or documents for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties. This is possible to be automated using smart contracts on the blockchain.
Ether	The form of payment used in the operation of the distribution application platform, Ethereum, to incentivize machines into executing the requested operations.
Ethereum Improvement Proposal (EIP)	Ethereum Improvement Proposals (EIPs) describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards.
Ethereum Virtual Machine (EVM)	A Turing-complete virtual machine that enables execution of code exactly as intended; it is the runtime environment for every smart contract. Every Ethereum node runs on the EVM to maintain consensus across the blockchain
Exchange Traded Fund (ETF)	A security that tracks a basket of assets such as stocks, bonds, and cryptocurrencies but can be traded like a single stock.
Fakeout	A situation where a trader enters a position betting on a price movement that quickly reverses or ultimately does not happen.
FOMO	An acronym that stands for "Fear of Missing Out" and in the context of investing, refers to the feeling of apprehension for missing out on a potentially profitable investment opportunity and regretting it later.
FUD	An acronym that stands for “Fear, Uncertainty and Doubt.” It is a strategy to influence perception of certain cryptocurrencies or the cryptocurrency market in general by spreading negative, misleading or false information.
Faucet	A cryptocurrency reward system usually on a website or app, that rewards users for completing certain tasks. It is mostly a technique used when first launching an altcoin to interest people in the coin.
Fiat Currency	A legal tender issued by a Government or a central bank such as Federal Reserve which issues US Dollars and Reserve Bank of India which issues Indian Rupees
Flipping	The term for constantly rotating your AltCoins on a trading platform trying to catch the raising percentages as the coins constantly go up in value.
Fork	Forks create an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network
Fiat-Pegged Cryptocurrency	Also known as "pegged cryptocurrency,"" it is a coin, token or asset issued on a blockchain that is linked to a Government- or bank-issued currency. Each pegged cryptocurrency is guaranteed to always have a specific cash value in reserves.
Full Node	Nodes that download a blockchain’s entire history to observe and enforce its rules.
Futures	A futures contract is a standardized legal agreement to buy or sell a particular commodity or asset at a predetermined price at a specified time in the future. They are different from forward contracts, which can be customized for each trade and can be conducted over-the-counter, instead of being traded on an exchange.
Gains	Gains refer to an increase in value or profit.
Gas	A term used on the Ethereum platform that refers to a unit of measuring the computational effort of conducting transactions or smart contracts or launch DApps in the Ethereum network. It is the "fuel" of the Ethereum network.
Gas Limit	A term used on the Ethereum platform that refers to the maximum amount of gas the user is willing to spend on a transaction.
Gas Price	A term used on the Ethereum platform that refers to the price you are willing to pay for a transaction. Setting a higher gas price will incentivize miners to prioritize that transaction over others.
Genesis Block	The first block of data that is processed and validated to form a new blockchain, often referred to as block 0 or block 1.
Gold-Backed Cryptocurrency	A coin or token issued that represents a value of gold; for example, one physical gram of gold equals one coin. The gram of gold is stored in a safe and can be traded with other coin holders.
Governance Token	A governance token is a token that can be used to vote on decisions that influence an ecosystem.
Graphical Processing Unit (GPU)	More commonly known as a graphics card, it is a computer chip that creates 3D images on computers but has turned out to be efficient for mining cryptocurrencies.
Gwei	The denomination used in defining the cost of gas in transactions involving Ether.

Hard Fork	A type of fork that renders previously invalid transactions valid, and vice versa. This type of fork requires all nodes and users to upgrade to the latest version of the protocol software.
Halving	Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. This is called "halving". The final halving will take place in the year 2140.
Hash	The act of performing a hash function on the output data. This is used for confirming coin transactions.
Hashrate	Measurement of performance for the mining rig is expressed in hashes per second. Mh/S (mega hash per second) is the speed that a graphics processor, GPU, can hash per second.
Hard Cap	The maximum amount that an ICO will raise. If a hard cap is reached, no more funds will be collected.
Hidden Cap	Hidden cap is an unknown limit to the amount of money a team elects to receive from investors in its initial coin offering (ICO). The purpose of a hidden cap is to even the playing field by letting smaller investors put in money, without the large investors forming an accurate understanding of the total cap and adjusting their investment as a result.
Hierarchical Deterministic Wallet (HD Wallet)	A wallet that uses Hierarchical Deterministic (HD) protocol to support the generation of crypto wallets from a single master seed using 12 mnemonic phrases.
Hosted Wallet	A wallet managed by a third-party service.
Hot Storage	The online storage of private keys allowing for quicker access to cryptocurrencies.
Hot Wallet	A cryptocurrency wallet that is connected to the internet for hot storage of cryptoassets, as opposed to an offline, cold wallet with cold storage.
Hybrid PoW/PoS	A hybrid PoW/PoS allows for both proof-of-stake and proof-of-work as consensus distribution algorithms on the network. This approach aims to bring together the security of PoW consensus and the governance and energy efficiency of PoS.
Hyperledger (Hyperledger Foundation)	Hyperledger is an umbrella project of open source blockchains and blockchain-related tools started by the Linux Foundation in 2015 to support the collaborative development of blockchain-based distributed ledgers.
Iceberg Order	A conditional order to buy or sell a large amount of assets in smaller predetermined quantities in order to conceal the total order quantity.
Immutable	A property that defines the inability to be changed, especially over time.
Impermanent Loss	Impermanent loss is when a liquidity provider has a temporary loss of funds because of volatility in a trading pair.
Index	A financial instrument used to track the price value of a given asset or basket of assets
Inflation	A general increase in prices and fall in the purchasing value of money.
Initial Coin Offering (ICO)	An Initial Coin Offering (also called an ICO) is an event in which a new cryptocurrency sells advance tokens from its overall coinbase, in exchange for upfront capital. ICOs are frequently used for developers of a new cryptocurrency to raise capital.
Initial Exchange Offering (IEO)	An initial exchange offering (IEO) refers to a fundraising event where a cryptocurrency exchange raises money on its own platform, as opposed to an ICO, where a team conducts the fundraising.
Instamine	A period in time, shortly after launch, when a large portion of total mineable coins or tokens are mined in a compressed time frame and may be unevenly and quickly distributed to investors.
Internet of Things	Internet of Things (IoT) is a global interconnected network of devices, sensors and software that can collect and exchange data with each other in real-time over the Internet.
KYC	Acronym for "Know Your Customer," this process refers to a project's or financial institution's obligations to verify the identity of a customer in line with global anti-money laundering laws.
Leverage	A loan offered by a broker on an exchange during margin trading to increase the availability of funds in trades.
Ledger	An append-only record store, where records are immutable and may hold more general information than financial records.
Litecoin	A peer-to-peer cryptocurrency based on the Scrypt proof-of-work network. Sometimes referred to as the silver to bitcoin's gold.
Lightning Network	The Lightning Network is a "second layer" payment protocol that operates on top of a blockchain. Theoretically, it will enable fast, scalable transactions between and across participating nodes, and has been touted as a solution to the Bitcoin scalability problem.
Limit Order / Limit Buy / Limit Sell	Orders placed by traders to buy or sell a cryptocurrency when a certain price is reached. This is in contrast with market orders at which a cryptocurrency is sold at the current best available price.
Liquidity	How easily a cryptocurrency can be bought and sold without impacting the overall market price.
Liquidity Pool	Liquidity pools are crypto assets that are kept to facilitate the trading of trading pairs on decentralized exchanges.
Liquidity Provider	Liquidity providers are decentralized exchange users who fund a liquidity pool with tokens they own.
Listing	The addition of an asset to an exchange either as a request from the project team or as a decision made by the exchange.
Liveness	Liveness is the guarantee that a system will continue to provide data and that no central party can just shut

	down their servers or censor data going to a smart contract.
Long	A situation where you buy a cryptocurrency with the expectation of selling it at a higher price for profit later.
Mainnet	An independent blockchain running its own network with its own technology and protocol. It is a live blockchain where its own cryptocurrencies or tokens are in use, as compared to a testnet or projects running on top of other popular networks such as Ethereum.
Margin Call	When an investor's account value falls below the margin maintenance amount. The broker will then demand that the investor deposit additional money or securities to meet the minimum required maintenance amount to continue trading.
Margin Trading	A practice where a trader uses borrowed funds from a broker to trade a cryptocurrency, which forms the collateral for the loan from the broker. It can be relatively risky for inexperienced traders who may receive a margin call if the market moves in the opposite direction of their trades.
Margin Bear Position	The position you are taking if you are going "short" on margin.
Margin Bull Position	The position you are taking if you are going "long" on margin.
Mempool	A node's mechanism for keeping track of unconfirmed transactions that the node has seen (but have not yet been added to a block).
Mining	The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.
Multi Signature	Multi-signature addresses provide an added layer of security by requiring more than one key to authorize a transaction. Multi signature addresses have a much greater resistance to theft.
Market Capitalization / Market Cap / MCAP	Total capitalization of a cryptocurrency's price. It is one of the ways to rank the relative size of a cryptocurrency.
Market Order / Market Buy / Market Sell	A purchase or sale of a cryptocurrency on an exchange at the current best available price. Market orders are filled as buyers and sellers are willing to trade. This is in contrast with limit orders at which a cryptocurrency is sold only at a specified price.
Masternodes	Masternodes are a server maintained by its owner, somewhat like full nodes, but with additional functionalities such as anonymizing transactions, clearing transactions, and participating in governance and voting. It was initially popularized by Dash to reward owners of these servers for maintaining a service for the blockchain.
Max Supply	The best approximation of the maximum number of coins that will ever exist in the lifetime of the cryptocurrency.
Merkle Tree	A tree structure in cryptography, in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of blockchains, as each change propagates upwards so verification can be done by simply looking at the top hash.
MicroBitcoin (uBTC)	One millionth of a bitcoin or 0.000001 of a bitcoin. Often confused as a fork of Bitcoin.
Microtransaction	A business model where very small payments can be made in exchange for common digital goods and services, such as pages of an eBook or items in a game.
Mineable	Some cryptocurrencies have a system through which miners can be rewarded with newly created cryptocurrencies for creating blocks by contributing their hash power. Cryptocurrencies with this ability to generate new cryptocurrencies through the process of confirmation is said to be mineable.
Not Mineable	Some cryptocurrencies are generated only through other mechanisms, such as annual inflation through staking. These cryptocurrencies are said to be not mineable.
Miners	Contributors to a blockchain taking part in the process of mining. They can be professional miners or organizations with large-scale operations, or hobbyists who set up mining rigs at home or in the office.
Mining Contract	Another term for cloud mining, where users can rent or invest in mining capacity online.
Mining Pool	A setup where multiple miners combine their computing power to gain economies of scale and competitiveness in finding the next block on a blockchain. Rewards are split according to different agreements, depending on the mining pool. Another term for this is Group Mining.
Mining Reward	The reward resulting from contributing computing resources to process transactions. Mining rewards are usually a mix of newly minted coins and transaction fees.
Mining Rig	A computer being used for mining. A mining rig could be a dedicated piece of hardware for mining, or a computer with spare capacity that can be used for other tasks, only mining part time.
Mixing Service	Also known as a tumbler, it is a service to improve the privacy and anonymity of cryptocurrency transactions by mixing potentially identifiable or "tainted" cryptocurrencies with other unrelated transactions, making it harder to track what the cryptocurrency was used for and who it belongs to.
Mnemonic Phrase	A mnemonic phrase (also known as mnemonic seed, or seed phrase) is a list of words used in sequence to access or restore your cryptocurrency assets. It should be kept secret from everyone else. It is a standard in most HD wallets.
Moon	A situation where there is a continuous upward movement in the price of a cryptocurrency. Often used in communities to question when a

	cryptocurrency will experience such a phenomenon, saying "When moon?" It is usually combined with "When Lambo?"
Moving Average Convergence Divergence (MACD)	A technical analysis method, it is a trend-following momentum indicator that shows the relationship between two price moving averages. The calculation is done by subtracting the 26-day exponential moving average (EMA) from the 12-day EMA.
Network	A network refers to all nodes in the operation of a blockchain at any given moment in time.
No-coiner	A no-coiner is someone who has no cryptocurrency in his or her investment portfolio and firmly believes that cryptocurrency in general will fail.
Node	A copy of the ledger operated by a participant of the blockchain network.
Non-Fungible Token	Non-fungible tokens (NFTs) are cryptocurrencies that do not possess the property of fungibility.
Non-custodial	Usually referring to the storage of keys, in relation to wallets or exchanges, a non-custodial setup is one in which private keys are held by the user directly.
Nonce	When a transaction is hashed by a miner, an arbitrary number meant to be used only once is generated, called a nonce.
Off-Ledger Currency	A currency that is created (minted) outside of the specified blockchain ledger but is accepted or used.
On-Ledger Currency	A currency minted on-ledger and used on-ledger. An example of this would be the cryptocurrency, Bitcoin.
Oracles	Oracles work as a bridge between the real world and the blockchain by providing data to the smart contracts.
Offline Storage	The act of storing cryptocurrencies in devices or systems not connected to the internet.
One Cancels The Other Order (OCO)	A situation where two orders for cryptocurrency are placed simultaneously, with a rule in place to enforce that if one is accepted, the other is cancelled.
Online Storage	The act of storing cryptocurrencies in devices or systems connected to the internet. Online storage offers more convenience but also increased risk of theft.
Open Source	Open source is a term that originally referred to open-source software (OSS). In crypto, open-source contracts/code that is designed to be publicly accessible—anyone can see, modify, and distribute the code as they see fit.
Open/Close	The price at which a cryptocurrency opens at a time, for example at the start of the day; the price at which a cryptocurrency closes at a time period, for example at the end of the day. In general, these terms were more useful in traditional financial markets as there are fixed hours of the day in which trading occurs.
Option	A contract giving the buyer the right, but not the obligation, to buy or sell an underlying asset or instrument at a specified strike price. There are American and European options, the former of which may be exercised at any time before expiration, and the latter exercised only at the expiration date.
Options Market	A public market for options, giving the buyer an option to buy or sell a cryptocurrency at a specific strike price, on or before a specific date.
Oracles	An agent that finds and verifies information, bridging the real world and the blockchain by providing data to smart contracts for execution of said contracts under specified conditions.
Orphan	A valid block on the blockchain that is not part of the main chain. They may come into existence when two miners produce blocks at similar times or caused by an attacker attempting to reverse transactions. This is sometimes also known as a "detached block."
Over The Counter (OTC)	Over-the-counter is defined as a transaction made outside of an exchange, often peer-to-peer through private trades. In jurisdictions where exchanges are disallowed or where amounts traded will move the markets, traders will go through the OTC route.
Overbought	When a cryptocurrency has been purchased by more and more investors over time, with its price increasing for an extended period. When this happens without any justifiable reason, the cryptocurrency is considered overbought, and a period of selling is expected
Oversold	When a cryptocurrency has been sold by more and more investors over time, with its price decreasing for an extended period. When this happens without any justifiable reason, the cryptocurrency is considered oversold, and a period of buying is expected.
Peer to Peer Exchange	A person who owns bitcoin or other cryptocurrencies willing to sell it to you or you buy/sell to them.
Plasma	An Ethereum off-chain scaling solution which may allow Ethereum to greatly increase the transactions per second capabilities.
Ponzi	Where a lending platform is set up to accept payment but eventually disappears before fully paying back their investors. Usually when they claim to payout more than they can afford to. Always look for red flags with investing platforms before investing or you could potentially risk losing your entire investment.
P2P Peer to Peer	Peer to Peer (P2P) refers to the decentralized interactions between two parties or more in a highly interconnected network. Participants of a P2P network deal directly with each other through a single mediation point.
Public Address	A public address is the cryptographic hash of a public key. They act as email addresses that can be published anywhere, unlike private keys.
Private Key	A private key is a string of data that allows you to access the tokens (cryptocurrency)in a specific wallet. They act as passwords that are kept hidden from anyone but the owner of the address.
Proof of Stake	A consensus distribution algorithm that rewards earnings based on the number of coins you own or

	hold. The more you invest in the coin, the more you gain by mining with this protocol.
Proof of Work	A consensus distribution algorithm that requires an active role in mining data blocks, often consuming resources, such as electricity. The more 'work' you do or the more computational power you provide, the more coins you are rewarded with.
Pyramid	Where an organization is set up on a referral-to-referral basis constantly accepting investments with locked contracts in order to hold onto investors' money. The more people underneath each other investing in the system, is the only fuel for maintaining these infrastructures until they can no longer withstand the demand for payouts. At this time, they will generally disappear or crumble.
Pair	Trade between one cryptocurrency and another, for example, the trading pair BTC/ETH.
Paper Wallet	A physical document containing your private key or seed phrase.
Permissioned Ledger	A ledger designed with restrictions, such that only people or organizations requiring access have permission to access it.
Permissionless	Often used to describe blockchains, a system is said to be permissionless when there is no entity that can regulate who can use it and how it can be used.
Phishing	When a scammer pretends to be a trusted institution or person to trick people into revealing sensitive information such as Social Security numbers, passwords, banking details, etc., often through a malware link disguised as legitimate.
Portfolio	A collection of cryptocurrencies or crypto assets held by an investment company, hedge fund, financial institution or individual.
Pre-mine	When some or all of a coin's initial supply is generated during or before the public launch, rather than being generated over time through mining or inflation. They may be used for legitimate purposes, such as crowdfunding or marketing.
Pre-sale	A sale that takes place before an ICO is made available to the general public for funding.
Proof-of-Authority (PoA)	A blockchain consensus mechanism that delivers comparatively fast transactions using identity as a stake.
Proof-of-Burn (PoB)	A blockchain consensus mechanism aiming to bootstrap one blockchain to another with increased energy efficiency, by verifying that a cost was incurred in "burning" a coin by sending it to an unspendable address.
Proof-of-Developer (PoD)	Any verification that provides evidence of a real, living software developer who created a cryptocurrency, to prevent an anonymous developer from making away with any raised funds without delivering a working model.
Proof-of-Replication	Proof-of-replication (PoRep) is the way that a storage miner proves to the network that they are storing an entirely unique copy of a piece of data.
Proof-of-Spacetime	In simplest terms, PoSt means that someone can now guarantee that they are spending a certain amount of space for storage.
Protocol	The set of rules that define interactions on a network, usually involving consensus, transaction validation, and network participation on a blockchain.
Public Blockchain	A blockchain that can be accessed by anyone.
Pump and Dump (P&D) Scheme	A form of securities fraud involving the artificial inflation of the price of a cryptocurrency with false and misleading positive statements to sell previously-cheaply purchased stock at a higher price.
QR Code	A machine-readable label that shows information encoded into a graphical black-and-white pattern. For cryptocurrencies, it is often used to easily share wallet addresses with others.
Raiden Network	An off-chain scaling solution aiming to enable near-instant, low-fee and scalable payments on the Ethereum blockchain. It is similar to Bitcoin's proposed Lightning Network.
Rank	The relative position of a cryptocurrency by market capitalization.
Relative Strength Index (RSI)	A form of technical analysis that serves as a momentum oscillator, measuring the speed and change of price movements, developed by J. Welles Wilder. It oscillates between zero and 100, where a cryptocurrency is considered overbought when the indicator is above 70 and oversold when below 30.
Relative Strength Index (RSI)	A form of technical analysis that serves as a momentum oscillator, measuring the speed and change of price movements, developed by J. Welles Wilder. It oscillates between zero and 100, where a cryptocurrency is considered overbought when the indicator is above 70 and oversold when below 30.
Replicated Ledger	A copy of a distributed ledger in a network that is distributed to all participants in a cryptocurrency network.
Ripple	A payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships. The banking industry is adapting this platform.
SIM-Swap	SIM-swaps, sometimes referred to as port-out scams, have come into the spotlight as a major concern for cryptocurrency holders in recent years.
Satoshi (SATS)	The smallest unit of bitcoin with a value of 0.00000001 BTC.
Satoshi Nakamoto	The individual or group of individuals that created Bitcoin. The identity of Satoshi Nakamoto has never been confirmed.
Scam	A fraudulent or deceptive cryptocurrency or ICO.
Scrypt	An alternative proof of work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC

	miners. A fraudulent or deceptive cryptocurrency or ICO.
SHA-256	SHA-256 is a cryptographic algorithm used by cryptocurrencies such as Bitcoin. However, it uses a lot of computing power and processing time, forcing miners to form mining pools to capture gains.
Smart Contracts	Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.
Soft Fork	A soft fork differs from a hard fork in that only previously valid transactions are made invalid. Since old nodes recognize the new blocks as valid, a soft fork is essentially backward compatible. This type of fork requires most miners upgrading to enforce, while a hard fork requires all nodes to agree on the new version.
Second-Layer Solutions	A set of solutions built on top of a public blockchain to extend its scalability and efficiency, especially for micro-transactions or actions. Examples include Plasma, TrueBit, Lightning Network and more.
Second-Layer Solutions	A set of solutions built on top of a public blockchain to extend its scalability and efficiency, especially for micro-transactions or actions. Examples include Plasma, TrueBit, Lightning Network and more.
Secure Asset Fund for Users (SAFU)	Secure Asset Fund for Users is an emergency insurance fund. On 3 July 2018, Binance announced the Secure Asset Fund for Users.
Securities and Exchange Commission (SEC)	An independent agency of the United States federal Government, responsible for enforcing federal securities laws, proposing securities rules, and regulating the securities industry, the nation's stock and options exchanges, and other related activities and organizations.
Seed	A single starting point when deriving keys for a deterministic wallet. It is usually presented as a series of words to enable the owner to quickly backup or restore a wallet.
Segregated Witness (SegWit)	SegWit was an update to the Bitcoin protocol and stands for "segregated witness consensus layer", a technological feature created to optimise transactions in 2015. SegWit is the process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions. When certain parts of a transaction are removed, this frees up space or capacity to add more transactions to the chain. A single starting point when deriving keys for a deterministic wallet. It is usually presented as a series of words to enable the owner to quickly backup or restore a wallet.
Sell Wall	A situation where a large limit order has been placed to sell when a cryptocurrency reaches a certain value. This can sometimes be used by traders to create a certain impression in the market, preventing a cryptocurrency from rising above that value, as supply will likely outstrip demand when the order is executed.
Sharding	Sharding is a scaling approach that enables splitting of blockchain states into partitions containing states and transaction history, so that each shard can be processed in parallel.
Shilling	The act of enthusiastically promoting a cryptocurrency or ICO project.
Short	A trading technique in which a trader borrows an asset to sell it, with the expectation that the price will continue to decline. If the price does decline, the short seller will then buy the asset at this lower price in order to return it to the lender of the asset, making the difference in profit.
Side Chain	A blockchain ledger that runs in parallel to a primary blockchain, where there is a two-way link between the primary chain and sidechain. This allows the sidechain to operate independently of the primary blockchain, using their own protocols or ledger mechanisms.
Simplified Payment Verification (SPV)	A lightweight client to verify blockchain transactions, downloading only block headers and requesting proof of inclusion to the blockchain in the Merkle Tree.
Smart Contract Audit	A smart contract audit is a security check done by cybersecurity professionals meant to ensure that the on-chain code behind a smart contract is devoid of bugs or security vulnerabilities.
Soft Cap	The minimum amount that an initial coin offering (ICO) wants to raise. Sometimes, if the ICO is unable to raise the soft cap amount, it may be called off entirely.
Solidity	Solidity is Ethereum's programming language for developing smart contracts.
Spot	A contract or transaction buying or selling a cryptocurrency for immediate settlement, or payment and delivery, of the cryptocurrency on the market.
Spot Market	A public market in which cryptocurrencies are traded for immediate settlement. It contrasts with a futures market, in which settlement is due later.
Stablecoin	A cryptocurrency with extremely low volatility, sometimes used as a means of portfolio diversification. Examples include gold-backed cryptocurrency or fiat-pegged cryptocurrency.
Staking	Participation in a proof-of-stake (PoS) system to put your tokens in to serve as a validator to the blockchain and receive rewards.
Staking Pool	A pool where stakeholders combine their staking power to increase their chance of successfully validating a new block.
Stale Block	A block which was successfully mined but not included on the current longest blockchain, usually because another block at the same height was added to the chain first. A pool where stakeholders combine their staking power to increase their chance of successfully validating a new block.

State Channel	A second-layer scaling solution that reduces the total on-chain transactions necessary, moving the transactions off-chain and letting participants sign to the main chain after multiple off-chain transactions.
Storage (Decentralized)	Decentralized storage refers to the concept of storing files online by splitting them into encrypted fragments and delegating these fragments to multiple nodes on a distributed network, *e.g.* a blockchain.
Symbol	The ticker of a cryptocurrency; for example, bitcoin's symbol is BTC.
Tangle	The Tangle is a blockchain alternative developed by IOTA, using directed acyclic graphs which only builds in one single direction and in a way that it never repeats, and is quantum-computing resistant.
Technical Analysis / Trend Analysis (TA)	An evaluation method involving statistical analyses of market activity, such as price and volume. Charts and other tools are used to identify patterns to underpin and drive investment decisions.
Testnet	A test blockchain used by developers to prevent expending assets on the main chain.
Transaction Block	A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.
Transaction Fee	All cryptocurrency transactions involve a small transaction fee. These transaction fees add up to account for the block reward that a miner receives when he successfully processes a block.
Ticker	An abbreviation used to uniquely identify cryptocurrencies.
Timelock / Locktime	A condition for a transaction to only be processed at a certain time or block on the blockchain.
Timestamp	A form of identification for when a certain transaction occurred, usually with date and time of day and accurate to fractions of a second.
Token	A digital unit designed with utility in mind, providing access and use of a larger crypto economic system. It does not have a store of value on its own but is made so that software can be developed around it.
Token Generation Event	The time at which a token is issued.
Token Swap	Token swaps can refer to one of two things: 1. Direct exchange of a certain amount of one cryptocurrency token for another between users facilitated by a special exchange service. 2. Migration of a cryptocurrency token built on top of one blockchain platform to a different blockchain. Example - Mainnet Launch.
Tokenize	The process by which real-world assets are turned into something of digital value called a token, often subsequently able to offer ownership of parts of this asset to different owners.
Total Supply	The total amount of coins in existence right now, minus any coins that have been verifiably burned.
Trade Volume	The amount of the cryptocurrency that has been traded in the last 24 hours.
Transaction (TX)	The act of exchanging cryptocurrencies on a blockchain.
Trustless	A property of the blockchain, where no participant needs to trust any other participant for transactions to be enforced as intended.
Unconfirmed	A state in which a transaction has not been appended to the blockchain.
Unspent Transaction Output (UTXO)	An output of a blockchain transaction that has not been spent and can be used as an input for new transactions.
Validator	A participant on a proof-of-stake (PoS) blockchain, involved in validating blocks for rewards.
Vanity Address	A cryptocurrency public address with custom letters and numbers, usually picked by its owner.
Venture Capital	A form of private equity provided to fund small, early-stage firms considered to have high growth potential.
Volatility	A statistical measure of dispersion of returns, measured by using the standard deviation or variance between returns from that same security or market index.
Volume	The amount of cryptocurrency that has been traded during a certain period, such as the last 24 hours or more. Volume can show the direction and movement of the cryptocurrency as well as a prediction of future price and its demand.
Wash Trade	A form of market manipulation in which investors create artificial activity in the marketplace by simultaneously selling and buying the same cryptocurrencies.
Wallet	A file that houses private keys. It usually contains a software client which allows access to view and create transactions on a specific blockchain that the wallet is designed for.
Watchlist	A watchlist is a feature of the website where users can create their own lists of cryptocurrencies to follow. Alternative definition A watchlist is a set of pages a user has selected to monitor for changes.
Wei	The smallest fraction of an Ether, with each Ether to 1000000000000000000 Wei.
Whale	A term used to describe investors who have uncommonly large amounts of crypto, especially those with enough funds to manipulate the market.
Whitelist	A list of interested participants in an ICO, who registered their intent to take part or purchase in a sale.
Whitepaper	A document prepared by an ICO project team to interest investors with its vision, cryptocurrency use and crypto economic design, technical information, and a roadmap for how it plans to grow and succeed.

Yield Farming	Yield farming involves earning interest by investing crypto in decentralized finance markets.
Zero Confirmation Transaction	Alternative phrasing for an unconfirmed transaction.
Zero Knowledge Proof	In cryptography, a zero-knowledge proof enables one party to provide evidence that a transaction or event happened without revealing private details of that transaction or event.
Zk-SNARKs	Zcash is the first widespread application of zk-SNARKs, a novel form of zero-knowledge cryptography. Shielded transactions in Zcash can be fully encrypted on the blockchain, yet still be verified as valid under the network's consensus rules by using zk-SNARK proofs.

CREBACO

India

CREBACO Global Pvt. Ltd.
TC Gupta Compound Kherani Road, Saki Naka
Andheri East, Mumbai 400072.

Singapore

CREBACO Global Pte Ltd.
9, Temasek Boulevard, #04-03, Suntec Tower
Two, Singapore 038989

USA

CREBACO Global Inc.
8 The Green, Ste A, Dover, Delaware (DE)
USA 19901.

Malaysia

CREBACO Global Sdn.Bhd.
1-04/05, Medini 7 Jalan Medini Sentral, 5,
Bandar Medini Iskandar, 79250, Iskandar
Puteri, Johor Bahru Malaysia 79250.

KHAITAN &CO

Mumbai

One World Centre, 10th & 13th Floor, Tower
1C, 841 Senapati Bapat Marg, Mumbai
400 013. India

Delhi-NCR

Ashoka Estate, 11th Floor, 1105 & 1106,
24 Barakhamba Road, New Delhi 110 001,
India

Bengaluru

Embassy Quest, 3rd Floor, 45/1,
Magrath Road
Bengaluru 560 025 India.

Kolkata

Emerald House
1B Old Post Office Street
Kolkata 700 001 India