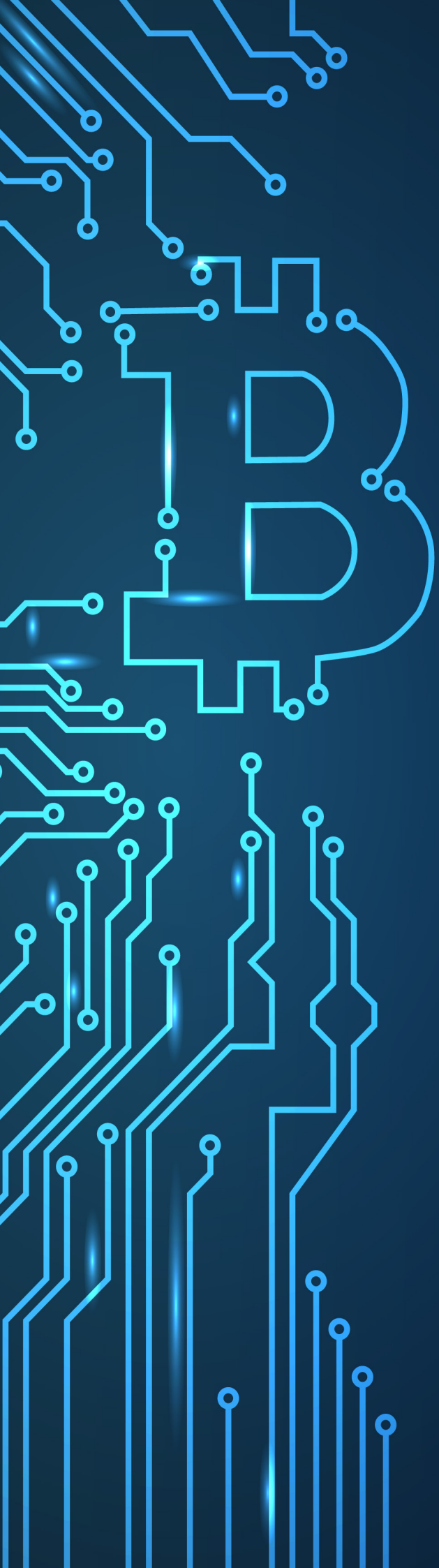


KPMG

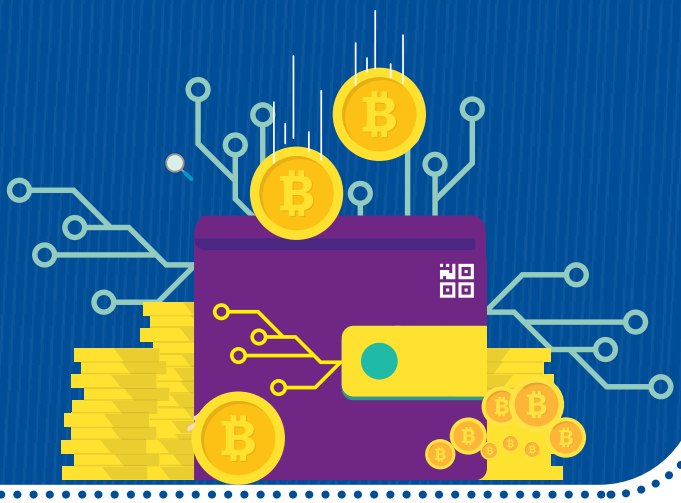
Crypto assets: Imagining the way forward

June 2022

home.kpmg/in

Table of contents

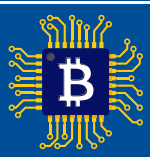
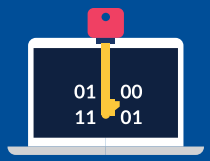
Introduction



In recent times, financial markets across the globe, including India, have been abuzz with words like cryptocurrencies, Central Bank Digital Currencies (CBDC) and Non-Financial Tokens (NFT). In India, the government has been contemplating on 'Cryptocurrency and Regulation of Official Digital Currency Bill' which was scheduled to be tabled during the winter session of the Parliament in December 2021. This has now been postponed amid evolving cryptocurrency regulations across the globe. Government of India is fairly ready with its consultation paper on cryptocurrencies and has consulted domestic and institutional stakeholders[1].

Bitcoin, which came into existence in 2009, is probably one of the first cryptocurrencies in circulation. As of November 2021, there are more than 18.8 million bitcoin tokens in circulation against a total supply of 21 million bitcoins[2]. Apart from bitcoin, there are currently more than 8,000 other cryptocurrencies in existence. While many of these cryptos have little to no following or trading volumes, others enjoy immense popularity among investors. Amongst the biggest and most popular cryptos that exist today are Bitcoin, Ethereum, Solano, Cardano, Binance Coins and Tether.

The most salient nuances associated with cryptos are as follows:

These currencies are not issued, backed, or regulated by a central bank or a sovereign regulatory authority	
These are encrypted (secured) with specialised computer code called cryptography	
They are created using a blockchain or distributed ledger technology and the transactions on the chain are verified through a peer-to-peer review	
As assets, cryptocurrencies are generally stored in digital wallets, commonly a blockchain wallet, which allows users to manage and trade their coins	
All these cryptocurrencies are built upon public-key cryptography, which essentially means usage of pairs of keys called 'public keys' that are publicly known and essential for identification, and 'private keys', which are kept secret and are used for authentication and encryption. Private keys would be known only to the owner. The private key is like a password that is required to access the vault wherein the owner would store his/her crypto coins	

1. Discussion paper on crypto is "fairly ready', says Govt, Indian Express, May 31, 2022
2. Bitcoin mining: Only 10 per cent left of total 21 million BTC that will ever exist to be mined, Financial Express, December 13, 2021

There is another class of cryptocurrencies called ‘stablecoins’. These are backed by a reserve asset like the US Dollar (USD) or some commodity like gold. These coins provide instant processing and privacy of payments as cryptocurrencies, as well as have volatility-free stable valuations like that of a fiat currency, thus combining the best of both worlds. In recent times, stablecoins have gained huge tractions in some markets. In Turkey, for example, following the steep rise of inflation (report from Turkish Statistical Institute, issued on 3 January 2022 pegs inflation at 36 per cent in December 2021[3]) and devaluation of the Turkish Lira by around 44 per cent against USD, usage of two stablecoins- Tether and Turkish New Lira (TRY) - have grown tremendously as citizens tried to move their savings to a safer place against rising inflation.

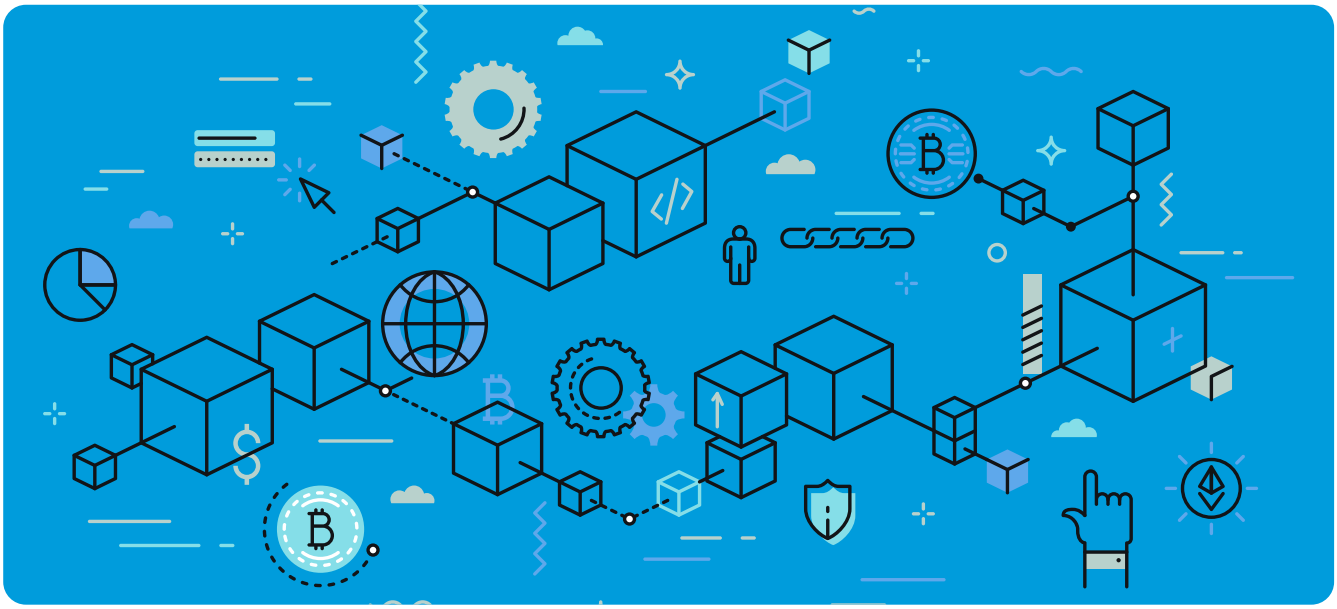
3. Use of stablecoins rises hugely in Turkey as inflation touches all time high, Times of India, Jan 06, 2022

Understanding the technology behind blockchain

As alluded earlier, cryptos are created using blockchains. The basic idea behind a blockchain is to create a distributed ledger that is accessible to anyone around the world. Transactions can be submitted from any place and then verified from elsewhere. Everyone, on the chain can see the balances on this distributed ledger. In other words, no single person controls the ledger, and it exists in a 'decentralised' manner. This in turn, allows value to be transferred directly on a peer-to- peer basis, without involving a central intermediary like a bank.

Invariably this raises a question on how to ensure that the million copies of this ledger floating across multiple machines are identical and updated in a synchronised manner. This is where the concept of a 'bad actor proof consensus' comes in, which is central to any blockchain network. Whenever a transaction is proposed on a blockchain network, the ledger isn't immediately updated. Transactions sit in a 'waiting room' for confirmation and thereafter 'miners' authenticate this transaction and propose them for settlement.

Typically, on a network, a single transaction isn't settled but these are grouped together into what is known as a 'block' or a series of transactions and therefore the name 'blockchain'. Miners compete with each other to solve this block. This entails solving a complex mathematical puzzle. A new block can be proposed only when this puzzle is successfully completed by a miner. As a transaction fee for solving the puzzle, miners get paid in form of a newly minted 'coin'. For example, if this transaction is being conducted on the Ethereum blockchain, miners will get paid in the form of Ether. If the transaction is valid and the puzzle has been solved correctly, the proposed block of transactions gets added to the ledger and the decentralised copies of the ledger get updated to reflect these new transactions. This is then available to be viewed by anyone on the network.



Point of view of countries across the globe

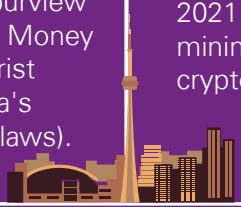
The world has been strongly divided in the opinion around cryptocurrencies - a group strongly supporting the development and further technological investments into advancing cryptocurrencies while the other group being wary of the decentralised nature, extreme volatilities, and Know Your Customer (KYC) and Anti Money Laundering (AML) related concerns. Some noteworthy positions in this context are as listed below:

1. The European Union (EU) recognises bitcoin and other cryptocurrencies as crypto assets.

2. While transacting in bitcoin is legal in the United Kingdom (the U.K.), Bank of England (BoE) has been wary of the use of cryptocurrencies and in a statement issued in November 2021 had said that bitcoins can become 'worthless', and investors need to be cautious when investing in cryptos.

3. The banking regulator in USA is expected to clarify rules/regulations on cryptocurrency in 2022.

4. While bitcoin trading is legal in Canada, it is not considered as legal tender. However, these are recognised as commodities for income tax purposes. Crypto exchanges are considered as money service businesses, which need to be registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and are regulated under the purview of Proceeds of Crime Money Laundering and Terrorist Financing Act (Canada's version of AML/ CFT laws).



5. China had been one of the early countries to embrace cryptocurrencies and was once the bitcoin trading and mining hub of the world. However, the Chinese government in September 2021 issued a blanket ban on mining and trading of private cryptos in the country.

6. The Australian Taxation Office, similar to Canada, considers cryptos as a financial asset class and taxes any buy-sell transactions under the capital gains tax.

7. Currently, the only country in the world to declare bitcoin as a legal tender is El Salvador. In June 2021, the country's Congress approved the proposition to formally adopt bitcoin as a form of payment. However, as recently as January 2022, the International Monetary Fund (IMF) has urged the local government to reverse its decision on accepting bitcoin as a legal tender alongside USD. Crypto has been accepted as currency in Central African Republic - announced on 27 April 2022; second country to do so now.

Cryptocurrency landscape in India

In India, crypto mining has been a challenge due to uncertainties around laws and regulations along with the huge infrastructure and power costs associated with the mining setup. However, there has not been any explicit law that bans crypto trading related activities. With the rise of the blockchain industry, crypto trading has gained tremendous traction in the Indian market. On the back of two important events in 2020 - the COVID-19 pandemic outbreak and the overrule of an RBI ban on cryptos by the Honorable Supreme Court of India - the crypto market has seen a dramatic rise in the number of retail investors. According to crypto research and intelligence business CREBACO, as of October 2021, 105 million Indians or 7.90 per cent of the population has invested in some form of digital token. Though there is no official data available, according to a Thomson Reuters report, it is estimated that cryptocurrencies held in India could be about INR400 billion or USD5.40 billion[1].

Backed by the strong demand, the cryptocurrency exchanges in India have also witnessed a meteoric rise in number of new user sign ups over 2021. According to a press release in November 21, WazirX is said to have facilitated trading volume worth over USD38 billion in the past 12 months, with a month-on-month growth rate of 44 per cent. The company reported growth of 2,648 per cent in user sign-ups from Tier II and Tier III cities - in other words, large cities in the country except the six biggest: Mumbai, Delhi, Kolkata, Chennai, Bengaluru and Hyderabad.[2] Zebpay, another crypto exchange platform based in India, has witnessed a 300 per cent rise in its trading volume over 2021, coupled with an increase in its user base by 130 per cent to over 5 million in a year's time.[3] Another exchange, namely Coin store, which started active operations in June 2021 has seen daily trading volumes jump from USD10,000 to USD40 million in a period of 6 months' time.

While India now has 15 homegrown crypto exchange platforms that enable trading of cryptos, the market largely has been unregulated with no specific consumer protection laws or redressal mechanism yet. Further, most of these exchanges are privately owned and there is no designated financial regulator who oversees their operations or regulates any settlement risks.

Further, past trends have shown extreme price volatilities across all cryptos due to the fluctuating demand and supply dynamics.To put things in perspective, the daily price volatility for bitcoin over the past three years is 75 per cent. In comparison, the S&P 500 daily volatility over the past three years has been 22 per cent, thereby making bitcoins almost thrice as volatile as S&P 500[4]. Without any "safety net" or check on the trading activities, this can potentially wipe off significant investor wealth.

1. India may create obstacles to crypto trading and holding -sources, Reuters, Nov 19, 2021
2. Indian crypto exchange WazirX registers $38-bn trading in a year, Business Standard, Nov 12, 2021
3. Crypto round up: Zebpay's user base grows 130%, Rohit Sharma will launch his own NFT, Times of India, Dec 24, 2021
4. 'Crypto: A new asset class?' -Goldman Sachs, Global Macro Research, May 21, 2021

Implementation roadmap: A possible approach

Regulators around the globe have been grappling with the twin issues - controlling the mining as well as trading around cryptos. For long, the mining activities have been associated with concerns such as concentration of power among relatively few operators and owners, market opacity, significant price volatility, and environmental impacts of such activities. To make this process transparent and develop a governance framework around it, there is an ever-growing need for a regulator to monitor all mining activities. There are also significant concentration risks as well, since today approximately 70 percent of the hash rates are controlled by top 5 mining pools[1].

Till 2021, China has controlled a majority share of these mining pools, till Chinese government's crackdown on mining operations. Since then, most of hashing power has moved to US and Canada. However, given relative opacity around this activity, it is difficult to exactly track the hashing power usage or the volumes of newly minted coins across multiple networks. The presence of a global regulator and access to the distributed ledgers for the various networks would ensure accurate estimation of the number of coins produced vis-a-vis coins in circulation.

1. Bitcoin mining pools, Buybitcoinworlwide, March 10, 2022

Crypto transactions executed on public blockchains, might not have a very well-defined central management or governance. In case, there are hacks or compromises on the network, the crypto asset owner might not have any recourse action available as there are no trusted intermediaries like a bank to capture, confirm, clear/settle and conduct the transactions.

The crypto eco-system, as it operates currently, is very different from a traditional financial ecosystem involving banks, financial intermediaries, regulators and customers (wholesale and retail), which is highly centralised. While there are obviously certain parallels that one can draw between the crypto ecosystem and the traditional financial ecosystem, there are newer components that need to be brought in and enhanced roles that existing components need to play to give this ecosystem certain stability that may soften the regulatory stance towards it.

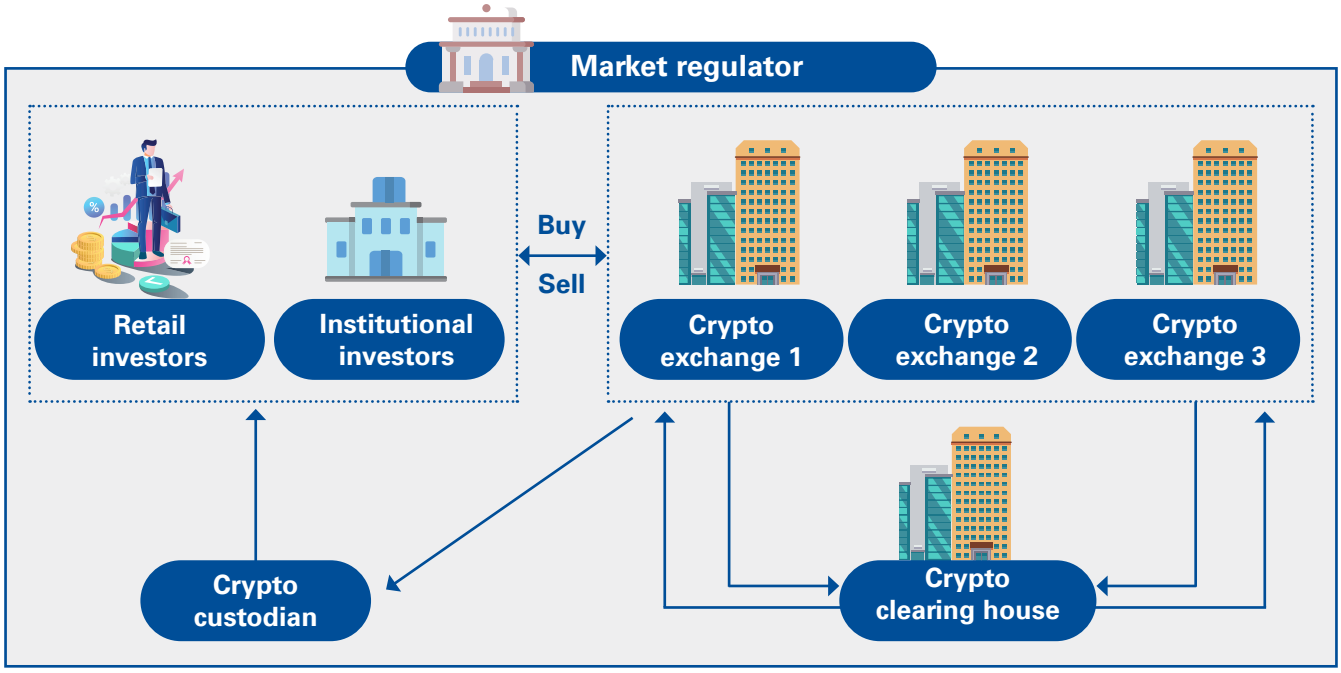


Figure 1: *How the key players may interact in a re-imagined crypto marketplace*

Just as the Registrar and Transfer Agent (RTA) tracks a company's authorised shares vis-a-vis outstanding shares in the share market and determines the float, for a crypto network, an independent agency should track transactions occurring on a mining blockchain and help assess the trading volumes, along with liquidity of a particular crypto trading in the market.
Currently, to the best of our knowledge, such an agency is not existent but if it can be created, that would act as a powerful mitigant against the information asymmetry that exists in this ecosystem. It is difficult to accurately determine the total number of various cryptocurrencies in circulation[1] but around 18,000 different crypto currencies are in circulation today. Not all of these are actively traded and some of them are 'dead' but at any point, determination of this number is a challenge in itself. With Initial Coin Offerings (ICOs) happening almost on a weekly basis, its highly possible to underestimate this number at any given day. It is even more difficult to determine the number of coins in circulation across each of these networks. These RTAs, specific to each network, would need to act as registrars that can track exactly how many coins get mined vs to-be-mined and track it against the network limit, if any. They would also need to work in conjunction with the regulators as well as market participants to provide them with timely information to improve the ease and transparency of the overall ecosystem. The crypto exchanges (discussed later in this section) need to make this information available to the users on their platform to enable them to assess the liquidity and tradability of the coin they are holding and/or intend to purchase/sell/hold.

1. How many cryptocurrencies are there in 2022? Exploding Topics, Mar 22

Once, the number of coins is accounted for, next one needs to have a closer look at who would be holding these coins in custody. Herein comes in the crypto custody solution providers/ custodians, the second building block of this eco system. On a blockchain network, the cryptographic private key owner has control of crypto assets that can then be used to unlock a public key wallet address, which in turn is used to execute transactions and move the assets and/or tokens across the network. Typically, these keys are combinations of alphanumeric characters, thereby making it challenging for the users to remember them. The crypto custodians provide independent storage and security systems and hold large quantities of tokens on behalf of the investor. The primary objective of these custody solutions is to ensure that the private keys are safe and are not accessible to anyone except the rightful owner of the asset/ token.

There could be two types of storage options

Hot Custody: This is a crypto custody with connection to the Internet thereby offering ease of liquidity but are also prone to hacks due to online connectivity.

Cold Custody: This is a crypto custody that is not connected to the Internet and hence is more secure, but at the same time comes with the challenge if the owner must generate liquidity at a short notice.

For a traditional asset, banks and trusts authorised by a regulatory body are allowed to act as the custodian for an institutional investor. There are specific regulatory requirements on aspects such as infrastructure, governance and controls, risk management and reporting that these banks and/or the trusts are subject to. Similarly, for crypto assets, these qualified custodians will need to be well-equipped with storage, network and technological requirements that will need to be defined, as well as there would be policy requirements on risk management, cyber security, know your customer (KYC) norms. This would significantly bring down the apprehensions that investors have with respect to safeguarding their crypto assets once they own them.

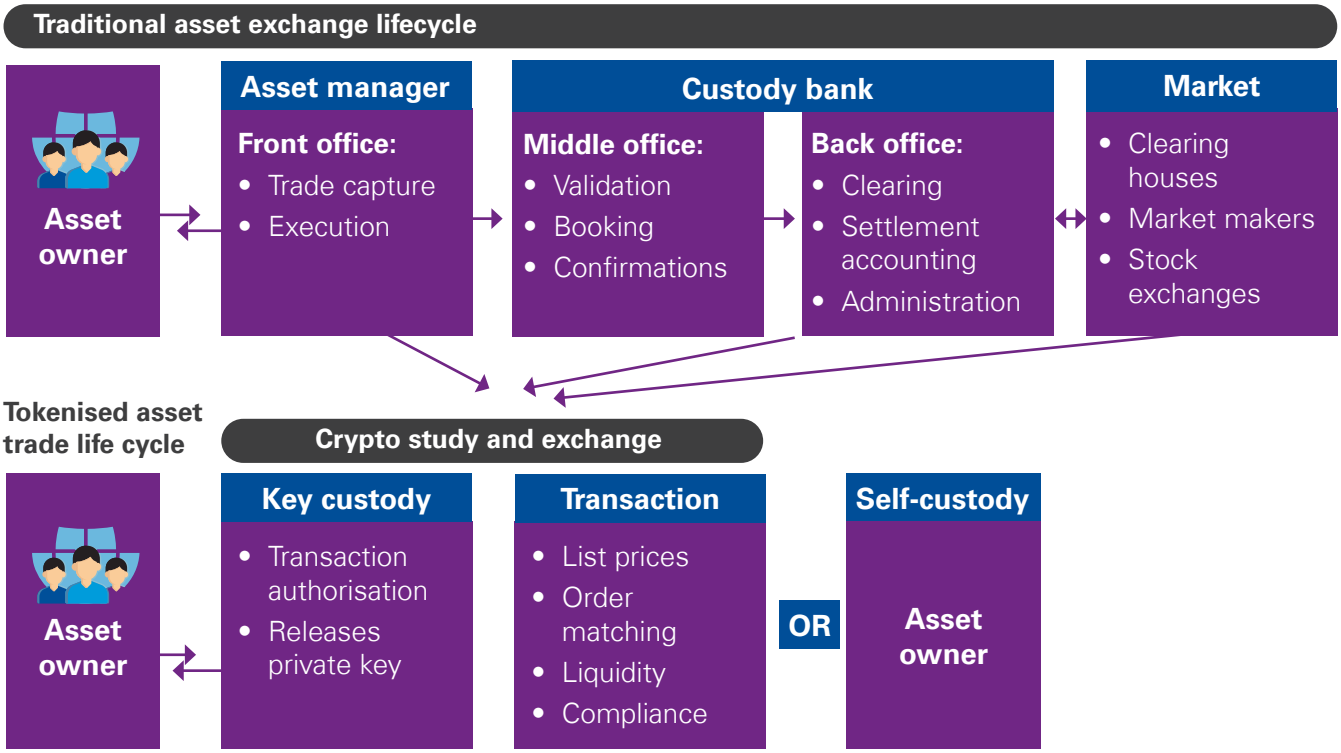


Figure 2: *Traditional asset exchange lifecycle vs Tokenised asset trade lifecycle; Source: KPMG International*

While for institutional investors, custodial services are of paramount importance, for a retail investor it would be difficult to access such a service. In such situations, the crypto wallets can be used by retail investors to store their coins. A crypto wallet behaves similarly to that of a digital wallet; however, they are used primarily to store the user's 16-digit alphanumeric private key. This ensure that the investor has custody of the crypto without storing the coin.

Safekeeping a customer's assets is the primary job of a custodial service provider, and therefore such an entity would have certain obligations when it comes to transparent operations specifically around record keeping, information security, separation of duties, segregation of customer assets, physical security, risk, controls and accounting. Typical custodial service providers also provide a range of value-added services (VAS) around account administration, post-trade processing and settlement transactions (including DvP), collection of dividends and interest (on assets that bear them), collateral management, tax support, and foreign exchange.

The most effective way to monetise a crypto post mining it, is through over the counter (OTC) transactions, wherein crypto currency exchanges come in. They would need to provide a verifiable and trustworthy marketplace wherein investors can exchange different cryptos or buy-sell them against fiat currencies, or transfer the ownership of a crypto from one person to another. Currently across the globe, there are both domestic and international private exchange players that facilitate trading of cryptos. Following are certain key considerations when dealing with these crypto exchanges:

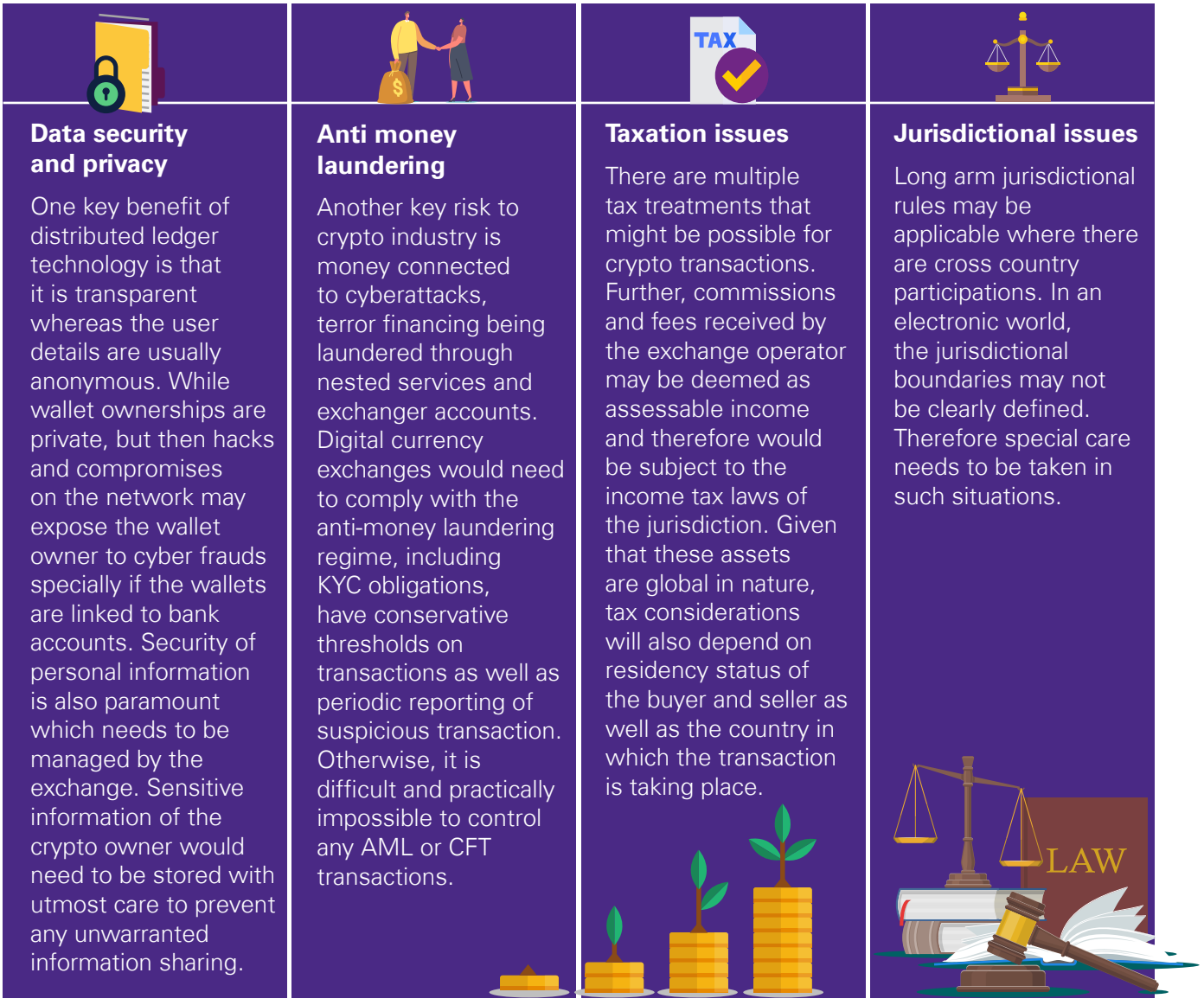


Figure 3: *Challenges that private crypto exchanges face*

Currently there are very limited rules that are applicable to these exchanges, and it varies widely across countries. For example, in the US, they fall under the regulatory scope of Bank Secrecy Act (BSA). These exchanges need to register with FinCEN, implement an AML/CFT program, maintain appropriate records, and submit reports to the authorities. FINCEN expects exchanges to comply with the "Travel Rule" (refer to FATF, June 2019 guidance) and gather and share information about the originators and beneficiaries of cryptocurrency transactions. Similarly the European Commission has also proposed draft travel rules to improve traceability of crypto coins. All Virtual Asset Service Providers (VASP) would need to collect details of senders and recipients to help authorities track transaction and thwart attempts at money laundering. The role that a crypto exchange plays in this ecosystem is enormous, and therefore, also need to shoulder great responsibility in improving the data security, privacy and AML/ CFT concerns around cryptos.

Given that cryptos can be traded across the globe, a payment network system needs to be also developed, specially if investors aren't transacting on international exchanges. Domestic exchanges in a country need to have a messaging system like SWIFT developed with its counterpart in a foreign jurisdiction to enable the buy and sell transactions. The key would be to ensure that this messaging system is fast, secure, and reliable. This could lead to the emergence of a central counterparty to facilitate the clearing of these transactions. For instance, the central counterparty may possibly be like a clearing house that guarantees clearing and settlement functions for transactions in financial markets. There would also be the requirement to set up a settlement guarantee fund which would have margin contributions from all members to maintain enough liquidity to meet all end of day settlements.

Considering these challenges inherent in the crypto trading transactions, a market regulator may need to have an oversight on the entire crypto ecosystem. Strong internal safeguard mechanisms using advanced AI/ML investigative techniques might be required to be employed by exchanges to identify any fraudulent or AML/CFT transactions and delist the associated accounts. The presence of such a regulator will mean that the private crypto exchanges build in appropriate mitigants and safeguards to early detect and report such transaction, block, and delist such accounts and work back with law enforcement agencies. Further, investor protection related laws would need to be strongly enforced by the regulatory authority to create a safe marketplace for retail and institutional investors.

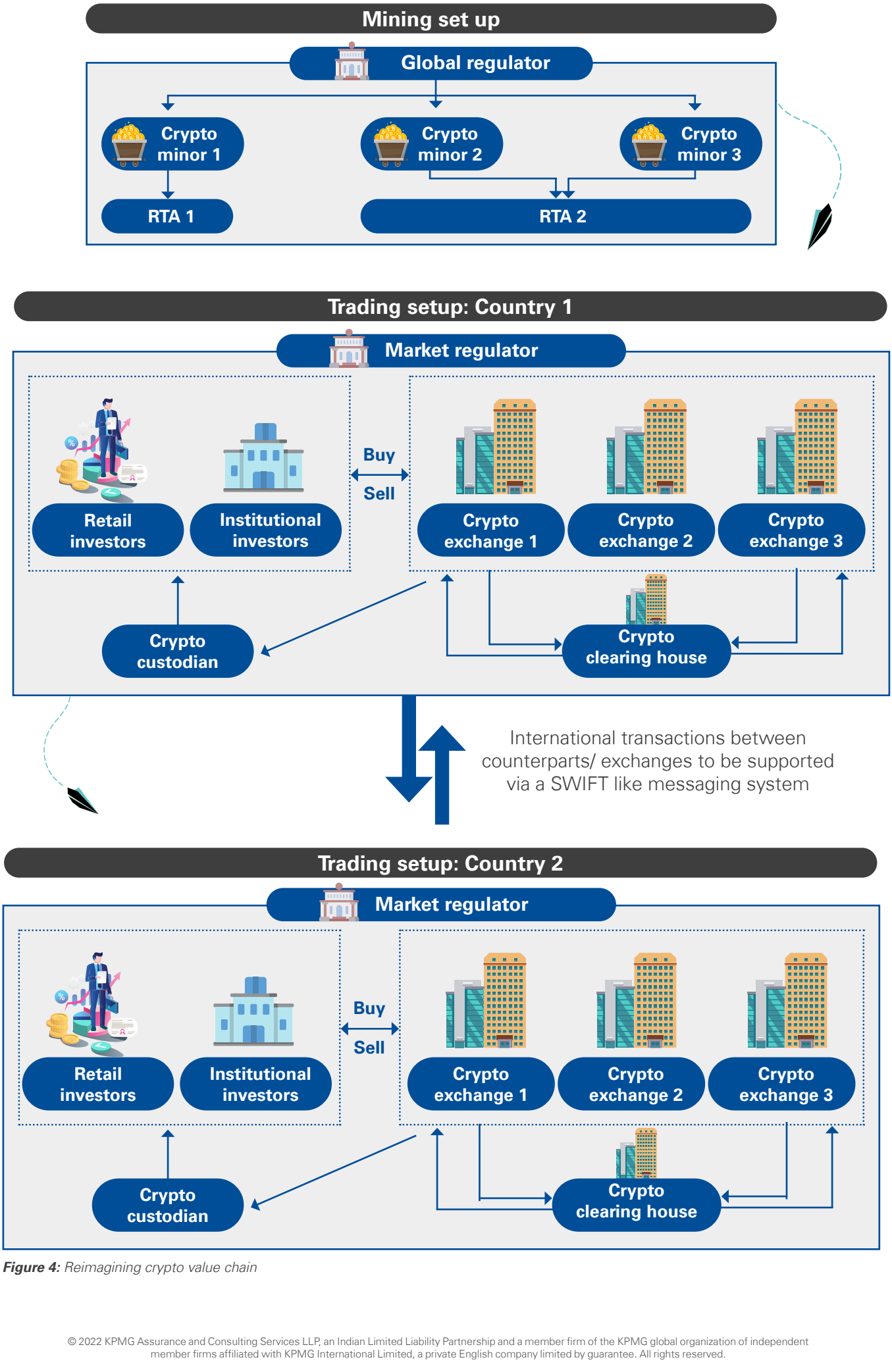


Figure 4: *Reimagining crypto value chain*

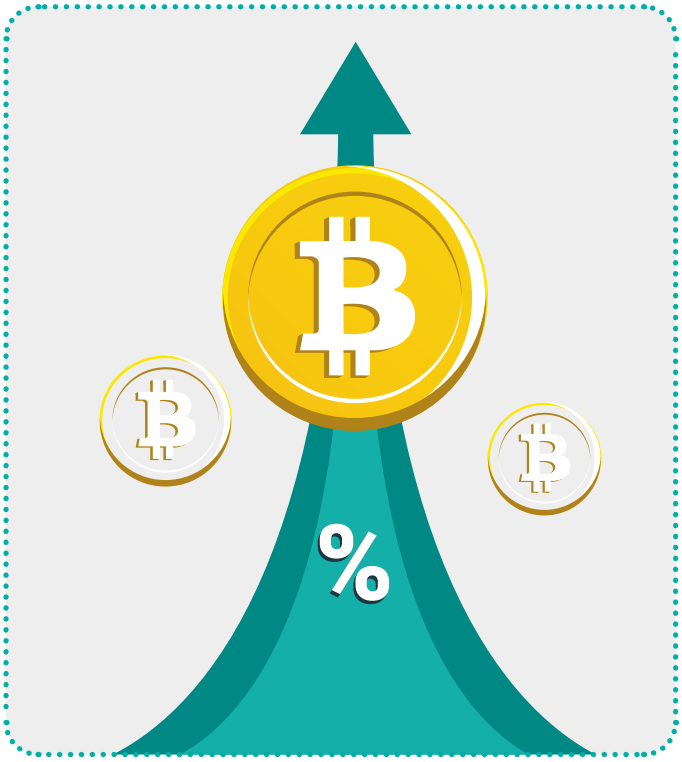
Way forward

The world of cryptos is evolving fast, and so are the points of view of various governments, regulatory bodies, and market participants. Recently, the Honorable Union Finance Minister Nirmala Sitharaman in her fourth budget speech announced that the Reserve Bank of India (RBI) will issue India's digital Rupee in financial year 2022-23. The digital Rupee is popularly known as CBDC. CBDC is the digital form of fiat currency that can be transacted using wallets based on blockchain technology and in the Indian context, it will be regulated by the RBI.

While the cryptocurrency bill is yet to be issued, the Honorable Union Finance Minister announced a flat tax rate of 30 per cent for any income from transfer of digital assets. Also, Tax Deducted at Source (TDS) of 1 per cent has been introduced to track transactions in crypto assets.

In 2022, the Federal Reserve (FED) is expected to come up with policy sprints focused on cryptos and would provide a roadmap of their future work on cryptos. This roadmap is expected to provide clarity on whether banks would be legally permitted to support crypto-assets-related activities, elaborate on consumer protection laws and how compliance needs to be enhanced. Further, the roadmap is expected to provide clarity in areas such as crypto safe-keeping and custodian solutions, crypto collateralised loans, landscape around stablecoins and treatment of crypto assets on the balance sheet. The agencies would also evaluate application of bank capital and liquidity standards to crypto assets for activities involving U.S. banking organisations[1]. In January 2020, European Commission had announced a public consultation initiative pertaining to where and how crypto assets fit into the EU's existing regulatory framework. This was followed by a proposal in September 2020, called Markets in Crypto-Assets Regulation (MICA). In July 2021, the European Commission published a set of legislative procedures around Transfer of Funds regulations (TFR) and information collection of senders and recipients that would be applicable to all VASPs across the EU.

It also remains to be seen how these developments in the international arena impact RBI's policy stance on cryptos and CBDCs and in general on its monetary policy. It is likely that factors such as utility of blockchain technology, security and acceptable levels of decentralisation will influence the way crypto-related transactions are permitted and how regulations evolve in the country.



1. Crypto regulation: Fed announces roadmap for 2022 — What it means for investors and developers, Yahoo Finance, Dec 01, 2021

KPMG in India contacts:

Rajosik Banerjee
Partner, Head of Department
Financial Risk Management
E: rajosik@kpmg.com

Venkateswaran Narayanan
Partner
Financial Risk Management
E: vnarayanan4@kpmg.com

Sunil Badala
Partner and National Head
Financial Services - Tax
E: sunilbadala@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.