Discussion paper on blockchain technology and competition

April 2021

भारतीय प्रतिस्पर्धा आयोग
Competition Commission of India

Building a better working world

Acknowledgement

We are happy and pleased at the occasion of the publication of the "Discussion paper on blockchain technology and competition". Blockchain is one of the prominent emerging technologies of our times. This paper is intended to shed light on several key aspects around the blockchain technology.

We thank the Competition Commission of India (CCI) for giving us an opportunity to delve deep into this emerging area. We hope this paper will provide useful insights and guidance to all stakeholders.

During the course of developing this discussion paper, we also consulted industry experts and had the benefit of feedback from them.

We wish to thank our team members Chinmaya Goyal, Jincy Francis, Navneeraj Sharma, Natasha Nayak and Sakshi Gupta who spent long hours researching and writing this paper.

Lastly, thanks to all others, whose names may not have been mentioned but who contributed to the paper.

Rajnish Gupta
Associate Partner

Ernst & Young LLP

Introduction

The Competition Commission of India (CCI) is entrusted with the responsibility of preserving and enhancing competition, not just through enforcement, but also through advocacy. Section 49 of the Competition Act, 2002 states that CCI "*shall take suitable measures for the promotion of competition advocacy, creating awareness and imparting training about competition issues*".

Recognising the growing interest of technology firms, businesses and institutions towards blockchain technology, competition authorities in different jurisdictions have shown keenness in understanding how this technology can create opportunities for enhancing competition and lead to efficiencies, and how this technology will interact with competition law.

This discussion paper is an effort to proactively discuss blockchain technology and how the technology interacts with competition law in India. This paper is expected to enable CCI to achieve its objective of promoting and sustaining competition in markets while maximising economic gains from innovation and introduction of new technology by:

- Sensitising stakeholders on the nuances related to blockchain technology, its applications and the potential effects it might have on competition.
- Spreading awareness and providing guidance about competition law and its interface with blockchain technology among the blockchain stakeholders (developers, miners, and users) to encourage these stakeholders to comply with competition law while developing/participating in blockchain applications.

The aim of this paper is to provide broad level information to all stakeholders on the interplay between blockchain applications and competition law. Its contents should, in no way, be treated as the official view of the CCI, or CCI Officers. The examples or possible situations related to competition issues discussed in the paper are purely hypothetical in nature. Any case relating to the blockchain will be assessed on the merits thereof. This paper is merely an intellectual exercise and not a regulatory or investigative guidance. Readers should take appropriate legal and other professional advice, wherever necessary.

Contents

1. Background

Trust and co-operation are the key to prosperity of human being sand nations[1]. Kenneth Arrow also states, "*Virtually every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time. It can be plausibly argued that much of the economic backwardness in the world can be explained by the lack of mutual confidence"*[2].

Building trust between unknown, untrusting third-party has been a long-drawn process. Measures adopted in this regard include: (a) recordkeeping through the creation of double-entry accounting system, (b) introduction of financial statements (based on widely-accepted accounting standards) to trustfully share information,(c) development of standards to ensure product quality, and (d)introduction of credit rating and legal systems to ensure enforcement of contracts and property rights.

One of the reasons for the growing enthusiasm around blockchain technology[3] is the impact that it can have on currencies, record keeping, sharing of information, contracting and verifying identities. This technology has been brought about by progress in the fields of cryptography, computing, economics, and law. While some argue that the blockchain technology is as transformational as capitalism[4]and could change the way governments function[5], speculation regarding the possibility of technology ending with a whimper rather than a big bang[6] also surface. As an evolving technology, one cannot be certain whether blockchain will live up to the expectation, but the technology does accompany some advantages.

Presently, intermediaries mediate between the different individuals, entities and institutions keen to enter into a transaction by providing the necessary trust to the involved parties. Banks, credit card companies, or e-commerce platforms act as intermediaries to resolve the issues pertaining to lack of trust between the two transacting parties, i.e., buyers and sellers. These entities frame the rules that guide entry and exit and set the terms for engagement between the various participants. These entities also act as counterparty to each side, maintain a centralised database/ledger of all the transactions, facilitate sharing of information and verify their identity. Thus, the intermediary provides confidence to two parties for trusting each other while interacting or making a transaction. They act as the channel through which transacting parties transact with an unknown entity/individual and in return charge a fee for the service provided by them.

Blockchain removes the need for such intermediaries as validators of trust and identity and supports transactions between two entities without involving a third-party as an intermediary. Blockchain allows participants to exercise increased control over the transaction, without relying on intermediaries. Since trust is most essential in financial transactions, it is no surprise that the first and the biggest application of blockchain was a crypt ocurrency - Bitcoin - which removes the need for intermediaries in money transactions.

Over time, the benefits of blockchain applications over the existing systems have resulted in businesses exploring new ways of doing business using blockchain technology. There is a growing interest among businesses on how blockchain technologies can be leveraged, both in India and globally. These projects are mainly in pilot or proof of concept stage. However, they have the potential to become more pervasive.

This discussion paper on blockchain and competition gives a background on blockchain, and highlights how the blockchain technology works, its different types and their unique characteristics. It also gives an overview of its applications and the possible regulatory and policy issues. The paper also discusses the interface between blockchain and competition law in India and concludes with some general guidance for blockchain stakeholders.

[1]Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity (Vol. 99)*. New York: Free press.

[2] Arrow, K. (1972). Gifts and Exchanges.*Philosophy and Public Affairs,*Vol. 1 (4), 343-362

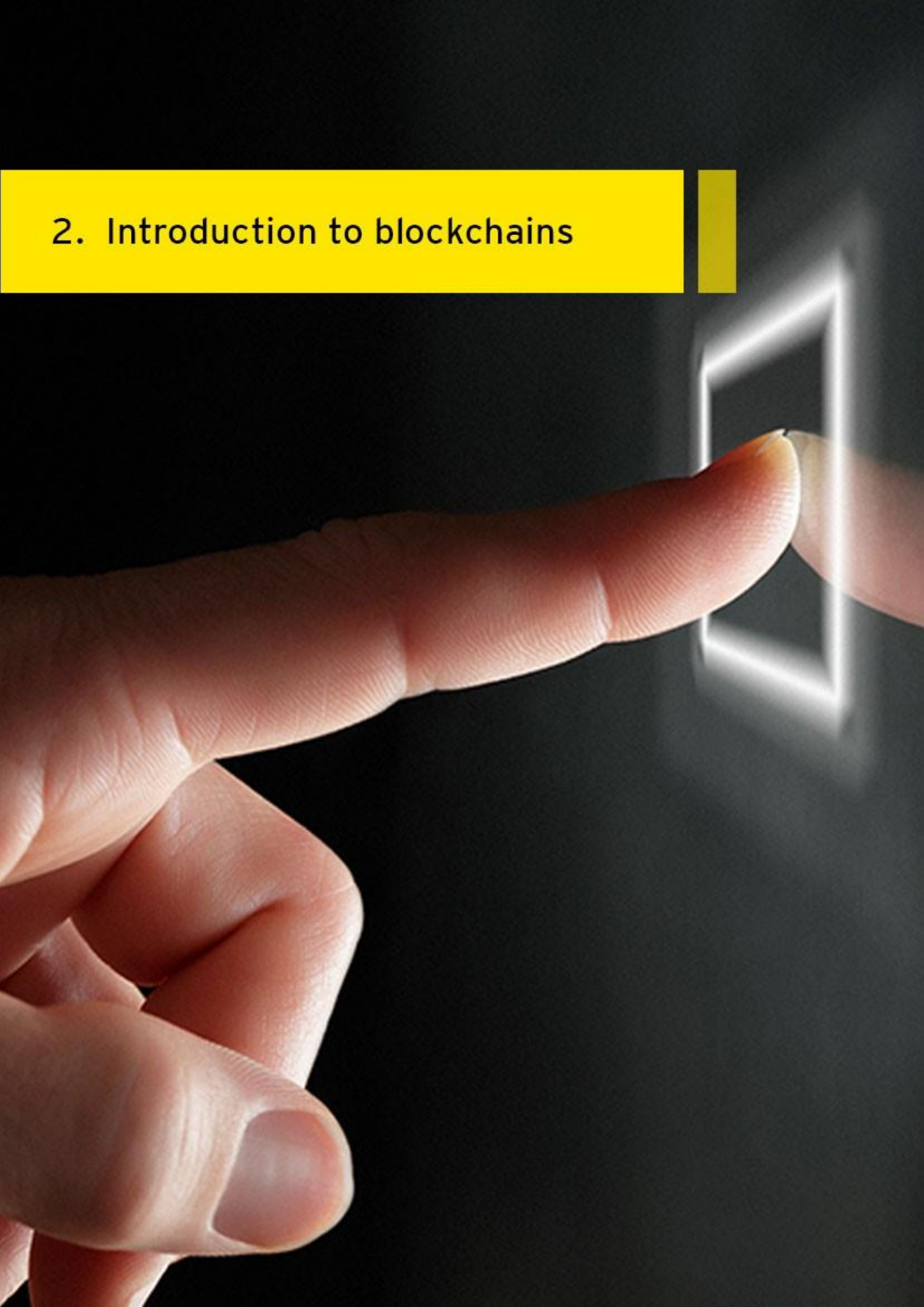
[3]In this paper, the term blockchain covers technologies developed on this concept of a distributed ledger technology (DLT).

[4]Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain. Available at SSRN: https://ssrn.com/abstract=2744751 or http://dx.doi.org/10.2139/ssrn.2744751

[5]Weyl, G. (2018*). A RadicalxChange between Vitalik Buterin and Glen Weyl.* [online] *The Medium*. Available at: https://medium.com/@glenweyl/a-radicalxchange-between-vitalik-buterin-and-glen-weyl-328d8ad088cf

[6] Most of the criticisms are centered around the Bitcoin- the most popular blockchain application. Bloomberg.com. (2019). *Bloomberg - Are you a robot?* [online]. Available at: https://www.bloomberg.com/features/bitcoin-bulls-bears/

2. Introduction to blockchains



2.1 What is a blockchain?

A blockchain is a virtual chain consisting of information on various blocks (transactions) grouped together in a sequential manner. This chain maintains a decentralised, distributed, immutable and secure record (or ledger) of the transactions taking place between different nodes[7] of the blockchain.

Decentralised

The process of adding a new block to the database/ledger is governed by a consensus mechanism[8]where the different nodes on the network participate in the process of deciding whether to add a new block of transactions to the database or not. This decentralised nature of the blockchain (resulting from it being controlled by a group of nodes rather than a single central authority) makes it more secure for the participants since the characteristics of the network cannot be changed by a single entity for its benefit.

Distributed

Each node keeps a copy of the database/ledger containing details of all the past entries. While this creates redundancy in the network, it also provides security to avoid manipulation of records. Specifically, any attempt to corrupt the network (by a hacker) may happen only if the data stored on the majority of the nodes in the network gets altered.

Immutable

Once an entry has been added to a blockchain, it is nearly impossible to edit, correct or delete the entry. This makes the data record of past transactions on a blockchain almost permanent and unalterable. An entry can only be updated by adding a new block instead of changing/deleting the past record.

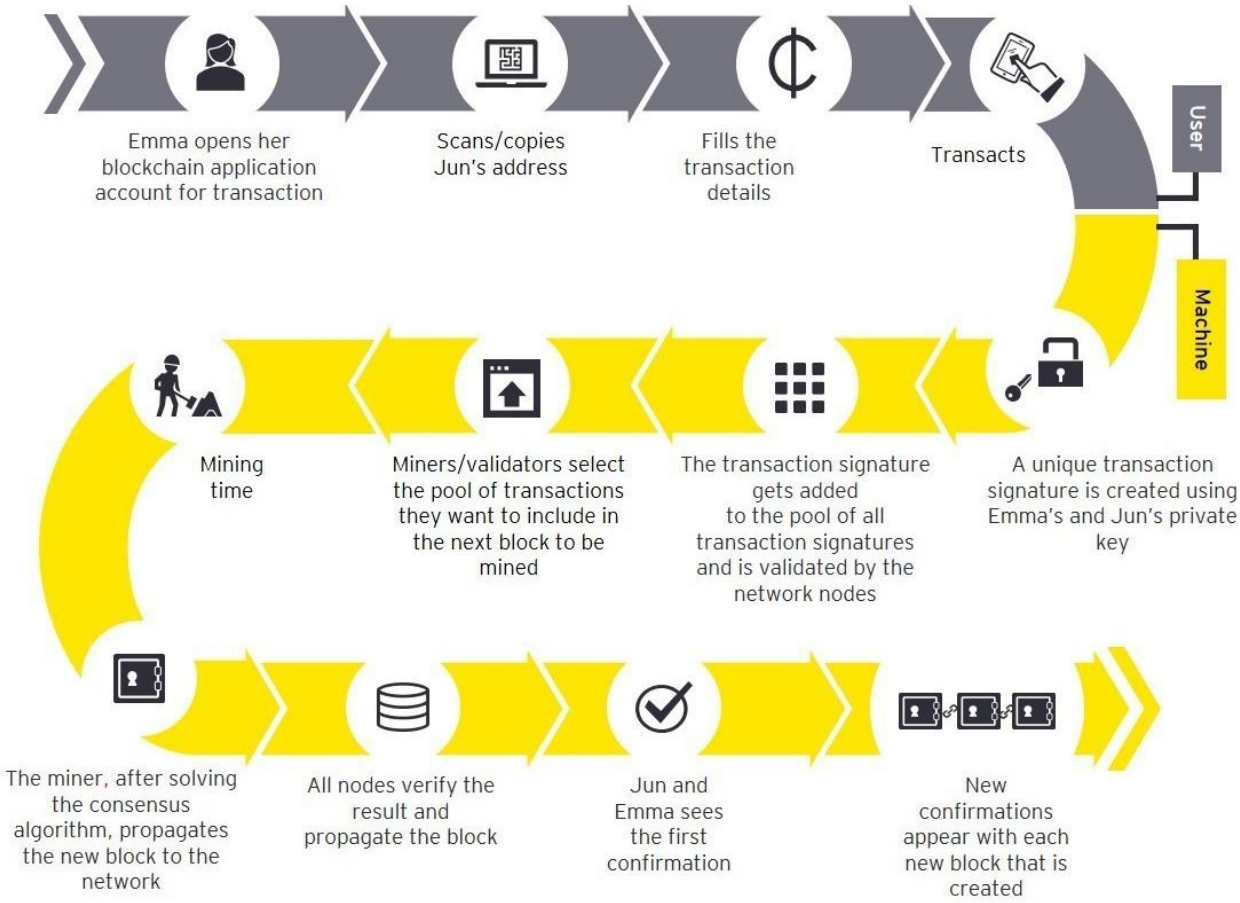
Secure

The process of adding a block to the database involves cryptography (a mathematical algorithm to encode information for security purposes) and economic incentive mechanisms which do not require trusting the other nodes involved in the network. This is the emergent property of maintaining a distributed and decentralised database by involving a consensus mechanism. The absence of the need to trust the other nodes involved creates an opportunity to transact and interact with greater confidence.

[7]Individual/entity/computing machine on a network.

[8]Consensus mechanism is a computer algorithm where all the nodes decide whether to add a new row to the database or not, after verification.

Figure 1: How a transaction takes place on a blockchain



Source: European Payments Council. (2014). Blockchain: a short-lived illusion or a real game changer? [online]

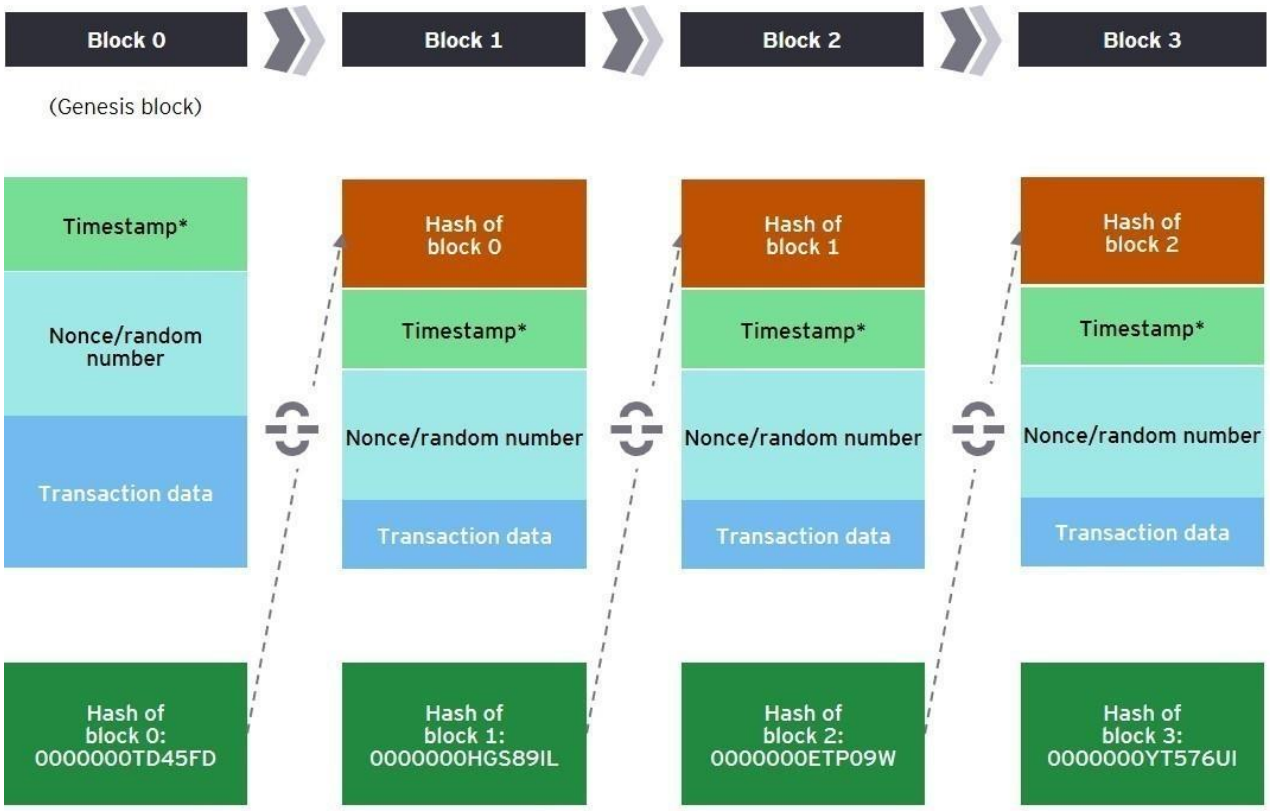
The following steps illustrate how a transaction is recorded on a blockchain[9] and verified by the different nodes:

1. All the nodes on the blockchain are free to transact between themselves. For security purposes, all the nodes have a public key (akin to an address) and a private key (akin to a password). When two nodes transact between themselves, they record the transaction using their keys to create a signature. All such transactions (along with their signatures) get pooled together in a repository.
2. In case of a centralised database, a neutral intermediary verifies these transactions and updates the database with the record of new transactions. However, a blockchain ledger is updated in a decentralised fashion. This process includes the following steps:
    a. A subset of nodes on the network, i.e., miners start the verification process (called mining) by selecting a pool of transactions they want to include in the next block. The following inputs are required for this process:
        i. Hash function: It is a mathematical algorithm which takes input data and outputs a string (hash) of a pre-specified length. This function is very sensitive to the input data and even a minor change in the input data can completely change the output hash. It is almost impossible to predict the input from the output. This feature acts as the key security mechanism in a blockchain.
        ii. Hash of the previous block: In a blockchain, a chain is created by linking a new block with the previous block. In this case, the output (hash) of the previous block is included in the next block added to the blockchain.
        iii. Signatures of the various transactions to be validated: When two nodes initiate a transaction, the block created contains the signatures of the nodes. This can be used to identify the entities involved in a transaction.

[9]We describe attributes of Bitcoin and Ethereum to explain the different mechanisms and algorithms involved in a blockchain. They are the two biggest applications of blockchain. They fall under the category of public permissionless blockchains (discussed in section 2.2).
The Government of India has banned holding and trading of cryptocurrencies like Bitcoin and Ethereum. Nonetheless, we have used their mechanisms and algorithms for elucidation purpose as they help in explaining the full-scale power of the blockchain technology. The other types of blockchain applications have similar and simpler algorithms.

iv. A random number generator for the nonce[10]: To ensure that the output hash of a new block cannot be guessed beforehand, a random number is generated and included in the block.

Figure 2: Data structure of a blockchain



*Timestamp marks the time for each transaction on the blockchain.

b. No node has the prior knowledge of the exact hash value which the hash function generates. However, certain attributes such as the number of the prefix zeroes of the hash output are known to all the nodes. Different miners compete to produce an output hash with the desired 0s by changing the nonce repeatedly through a brute computation[11] process. In return for this computation and energy-intensive work, miners collect a transaction fee.

c. The miner who discovers the desired hash first broadcasts the necessary information required to check the accuracy of the hash with the other nodes.

d. Once the other nodes agree on the value of the hash calculated by the miner, the new block gets linked to the previous block on the blockchain and the updated ledger is shared with all the nodes. Once the block is added, it is almost impossible to change its content.

2.2 Types of blockchains

There are two main dimensions on which blockchains can be segregated:

- Who can read the information stored on the blockchain?
  a. Anyone can access the information in a **public blockchain**.
  b. If only an individual entity or a consortium of entities access the information on a blockchain, then it is classified as a **private blockchain**.
- Who can participate (submit/verify transactions) on the blockchain?

[10]Jargon for a random number.
[11]This is the **Proof-of-Work**consensus mechanism. Other consensus mechanisms like Proof-of-Stake are similar but are inefficient in terms of computation and energy spent to achieve consensus. See Box 1 for further details.

c. In case, authorisation is not required to participate in a blockchain (i.e., anyone in the public can submit and verify transactions), then the blockchain is referred to as a **permission-less blockchain**.

d. If authorisation is required to participate in a blockchain (i.e., submit and verify transactions), then the blockchain is referred to as a **permissioned blockchain**.

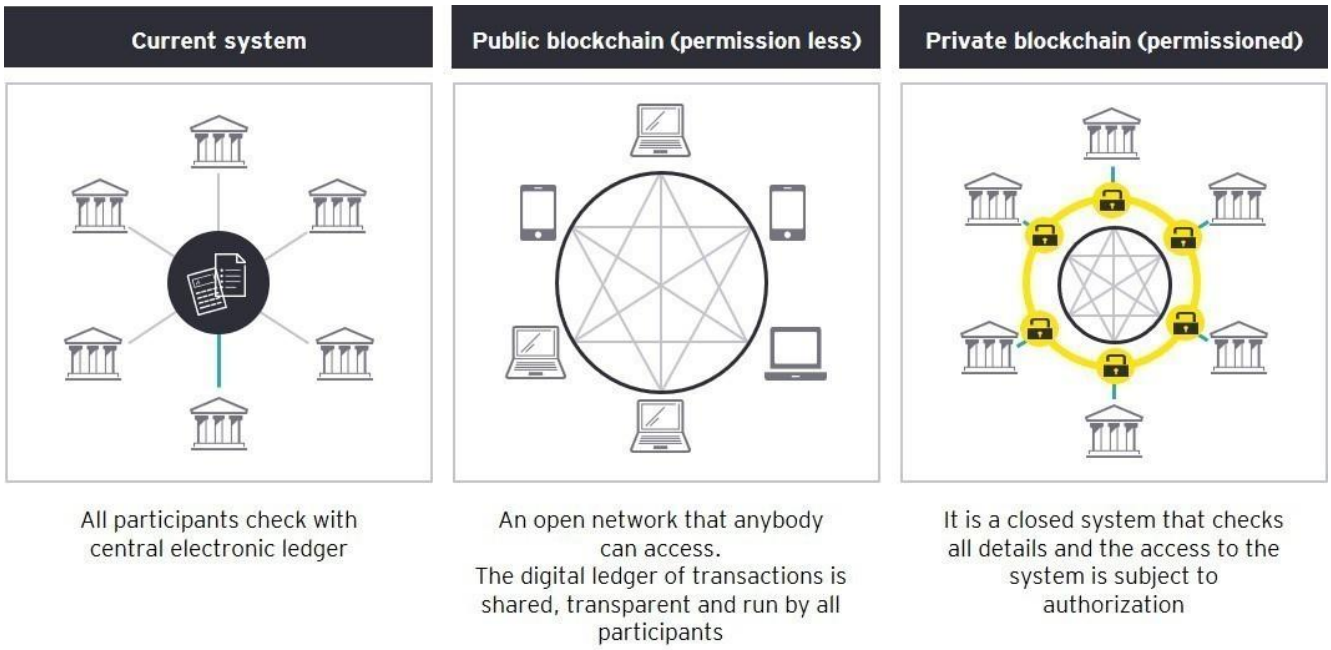
Therefore, there are four principal categories of blockchains. These are public permissioned, public permission-less, private permissioned and private permission-less. The selection of these categories depends on the needs and requirements of the participants who want to use the blockchain.

Figure 3: Comparison between four types of blockchains

Source: Drawn by authors based on McKinsey & Company. (2018). *Blockchain beyond the hype: What is the strategic business value?* [online], Tjark Friebe (2017). *Is Blockchain equal to Blockchain?* [online] *Medium*, and Daniels, A. (2018). *The rise of private permissionless blockchains — part 2*. [online] *Medium.*

Figure 4 highlights how centralised databases, public permission-less blockchains and private permissioned blockchains are different from each other.

Figure 4: Difference between centralised system and public blockchain



Source: Financial Times.

One of the challenges in a permission-less blockchain is designing the economic incentives for miners to verify the transactions and the time taken for conducting such verifications. The relatively easier scalability and ease of implementation of permissioned blockchains have made them popular than permission-less blockchains. This is because when a group of entities come together to explore a blockchain application within themselves, there is a certain level of pre-existing trust between them. Therefore, the consensus algorithm is generally simpler in this case.

Box 1: Main consensus mechanisms in blockchains

Blockchain applications may use various consensus mechanisms to authenticate inclusion of a new block into the blockchain ledger. The permission-less mechanisms need more rigorous processes as they allow anyone to verify the transactions on the blockchain (refer Figure 3).

The two most popular mechanisms currently in use for permission-less networks are:

- **Proof-of-Work (POW)**: The legitimacy of a proposed new block is verified by nodes competing and spending their computation power to solve a complex hashing algorithm. This approach involves a significant cost in terms of electric power consumed as well as computer hardware and storage space required. The challenge with this mechanism is in terms of energy inefficiency and difficulty in scalability because of the large time periods required to solve the hash functions. Both Bitcoin and Ethereum use this consensus mechanism.
- **Proof-of-Stake (POS):** Any node wanting to be the verifier can stake its assets (currency token of the platform) as collateral for being considered and appointed as the verifier. There are two main mechanisms for choosing a verifier and achieving consensus:
  - *Chain-based Proof-of-Stake*: The algorithm randomly selects a verifier during each time slot and assigns that verifier the right to create a single block. This block must be built on a previous block (normally the block at the end of the previously longest chain), so that over time, most blocks converge into a single constantly growing chain. For e.g., Peercoin and Ethereum Casper.
  - *Byzantine Fault Tolerance (BFT)*[12]*style Proof-of-Stake*: Verifiers are randomly assigned the right to propose blocks but agreeing on which block is final involves a multi-round process wherein every verifier sends a "vote" for some

[12]Byzantine Fault Tolerance (BFT) is the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making (both – correct and faulty nodes) which aims to reduce to influence of the faulty nodes. Source: Geeks for Geeks. (2019). *Practical Byzantine Fault Tolerance (pBFT) – Geeks for Geeks* [online]. Available at: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/ [Accessed 30 Aug. 2019]

specific block during each round, and at the end of the process all (honest and online) verifiers permanently agree on whether or not any given block is part of the chain. For e.g., Hedera.

The consensus mechanisms for permissioned networks are simpler and utilise the implicit trust of the nodes involved in transactions. The main types of consensus mechanisms used are:

- **Proof of authority/proof of identity:** The publishing nodes reveal their (verified) real-world identity within the blockchain network and thus stake their identity/reputation to publish new blocks. For e.g., VeChain
- **Round-robin:** Nodes take turns to create blocks (often with a time limit in case a node is unavailable to include a block on its turn). For e.g., MultiChain
- **Proof of elapsed time**: Random wait times are provided to every publishing node, who then must remain idle for the stipulated time. After this time, when a node becomes active, its block is added to the blockchain and all the other nodes are accordingly notified, starting the process again. For e.g., Hyperledger Sawtooth.

Source: Scarfone, K., Roby, N., Mell, P., Yaga, D. (2018). "Blockchain Technology Overview." National Institute of Standards and Technology. US Department of Commerce.

Private blockchains can further be classified into two categories – those involving a single organisation or its subsidiaries (hereafter referred to as private blockchain) and those involving a group of different firms (hereafter referred to as consortium blockchain).

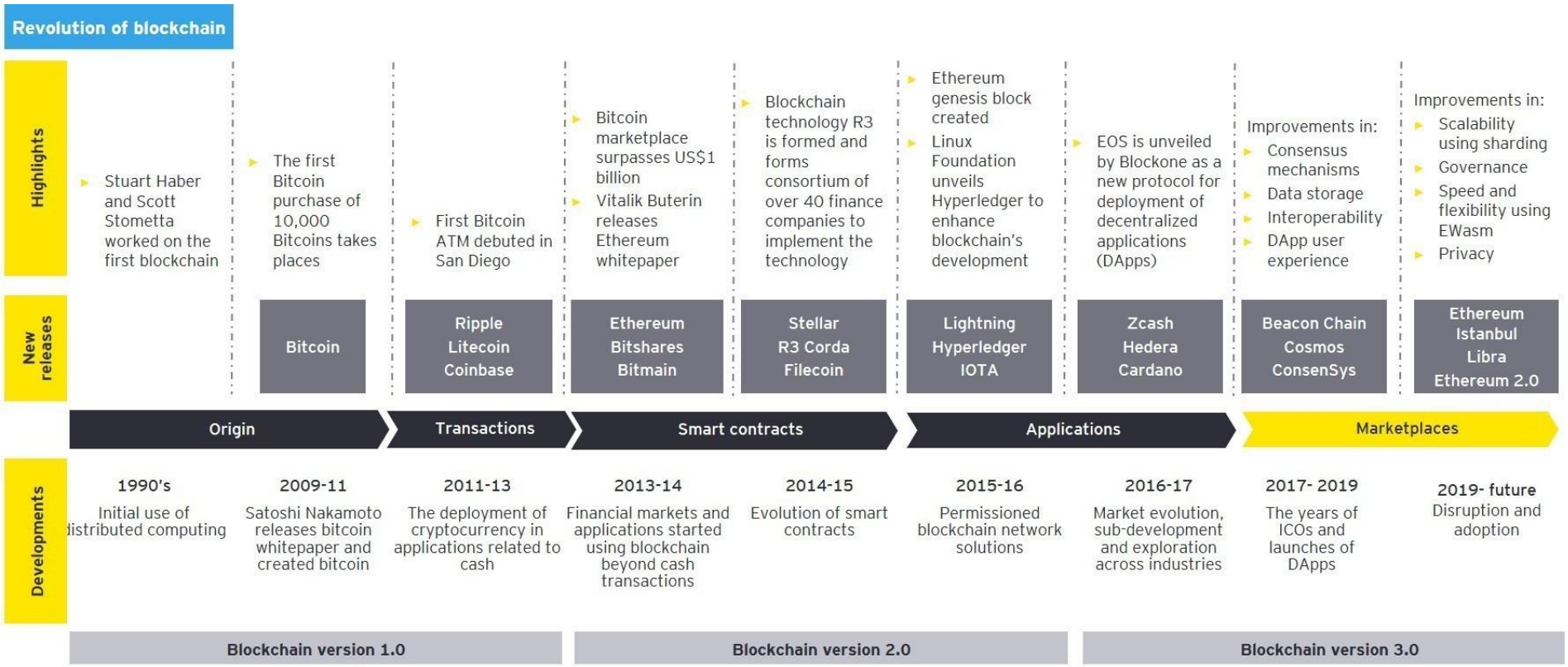
2.3 Evolution and development of blockchains

The parallels between the development of blockchain and internet are quite similar. The internet layer[13], by itself, was not end-user centric and required the development of web browsers, website hosting platforms and services, search engines, application development tools, etc., which enabled the provision of services such as social networks, ride-hailing applications, video platforms, etc. Similar dynamic is at play with blockchains as well: developers first develop the very basic architecture of blockchain technologies which may then be leveraged to create new applications and services.

Figure 5 highlights the structural developments of blockchains over time. Blockchain version 1.0 involved Bitcoin and the basic tools around it. Most of the applications were centered on financial applications of Bitcoin and helped a user transact in Bitcoin. This changed with the advent of Blockchain version 2.0, which saw the emergence of Ethereum, smart contracts, etc., and building of the tools which the developers themselves needed to build consumer-focused applications. It also saw the proto-app developments as proof-of-concept, which highlighted the gaps in the tools and the further indicated the development required to explore other applications. Blockchain 2.0 also saw the development of permissioned blockchain tools such as Hyperledger. This was followed by Blockchain version 3.0, which is trying to solve the problem of scalability, identity and creating tools for the developers. New ways are being explored to make the consensus mechanism more efficient (for example, Ethereum's decision to move from Proof-of-Work to (POW) to Proof-of-Stake (POS) consensus mechanism).

[13] The internet layer is responsible for the logical transmission of data packets over the internet.

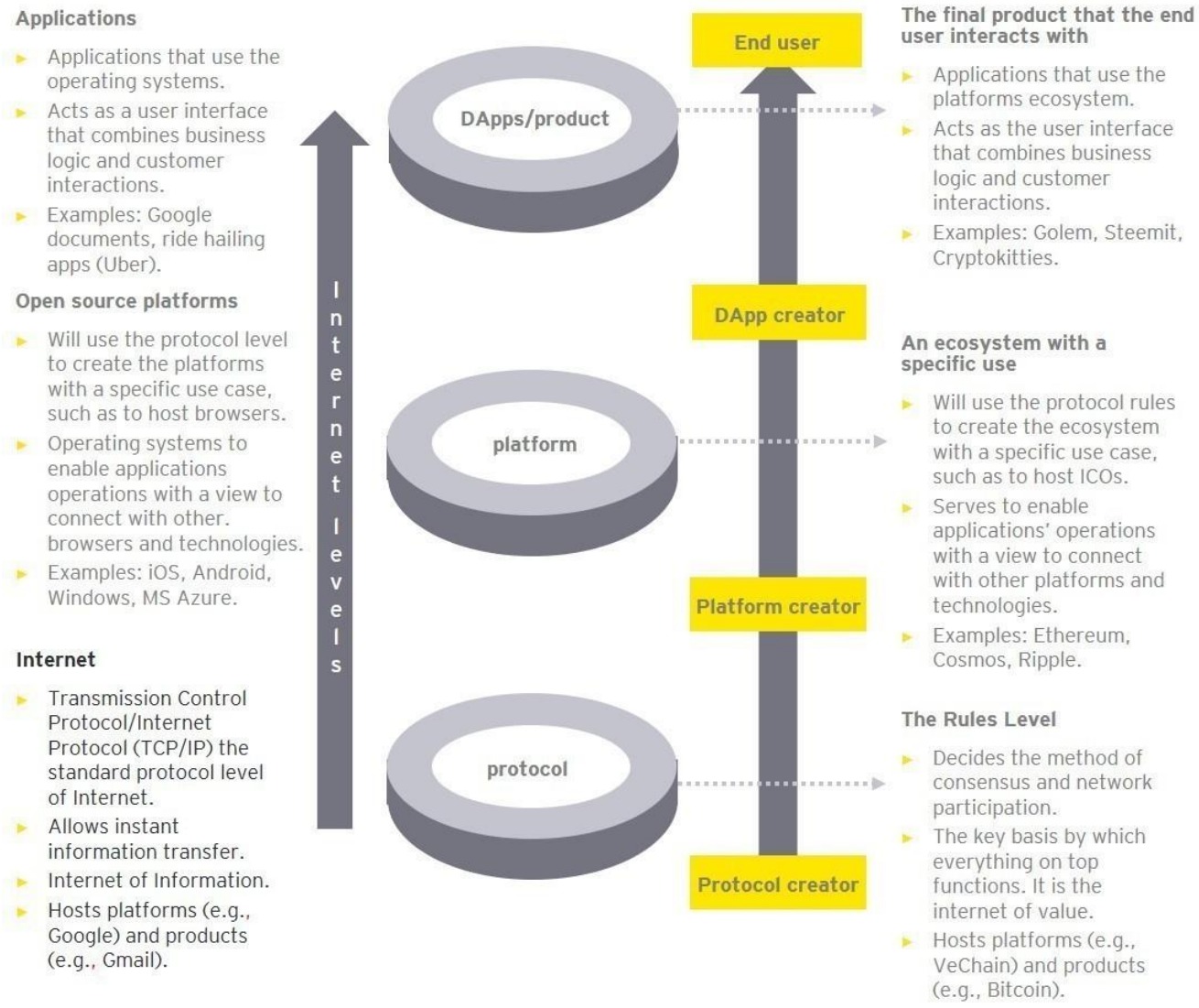
Figure 5: Blockchain structural developments



Source: Goyal, S. (2018). *The History of Blockchain Technology: Must Know Timeline.* [online], Accenture, Reddit.

Figure 6 shows the structural evolution in the blockchain technology space, which can be viewed in three levels. Level 0 is the base layer of blockchain technology akin to internet and web. Level 1 includes the platforms and tools which need to be developed to leverage the full power of blockchains. Ethereum is the primary example of this level. Level 2 includes the customer-facing decentralised applications (DApps) and smart contracts. Figure 6 highlights further details about the levels of blockchain technology andalso shows comparison with the internet levels.

Figure 6: Blockchain structural evolution



Source: Snapper (2018). *Protocols Platforms and DApps - blockchain layers explained – Origin Trail community* [online]. OriginTrail community.

2.4 Key relevant blockchain technology related concepts

Governance

Governance of a blockchain refers to the process through which the nodes agree to implement changes to the blockchain. The process also covers which stakeholders are involved in the decision-making and the way they come to a consensus.

Forking

One of the features of blockchain is that it allows all transactions to be conducted in accordance with the governance provisions developed at the time of a blockchain's commencement. But, do blockchains have the flexibility to adapt to changing circumstances? Forking can enable such change, depending upon the type of blockchain and its governance rules.

If a group of nodes wish to change the governance rules, they can split these rules from the original blockchain, thereby creating a fork. If the changes are accepted by all the nodes, then all participants can move to the new fork. However, if only a minority of the nodes agree to implement the change, then they can split into a different blockchain from the point of forking. Forked blockchain generally has access to the ledger/data till the point of forking.

Forks that are incompatible with older versions of the protocols and algorithms are called **"hard forks".** Hard forks typically change consensus rules (such as block size, mining algorithm and consensus mechanism) in a way that makes previous versions of the blockchain incompatible. **Soft forks**, on the other hand, are compatible with older versions of the blockchain

Smart contracts

A smart contract is a programmable code that is executed on a blockchain, after meeting certain pre-defined terms and conditions, thereby self-enforcing an agreement between two or more parties[14]. They are based on the "if and then" logic, i.e., if the parties to a transaction comply with the pre-agreed conditions, then the transaction is validated by a smart contract, else it is rejected. It is a computer protocol intended to digitally facilitate, verify and enforce performance of an agreement. Platforms like Ethereum provide setting up of a programming logic for executing transactions between the nodes.

With the advent of 5G, the Internet of Things (IoT) and Artificial Intelligence (AI), smart contracts play an important role in the world of technology and commerce. Today, most of the trading on stock exchanges is algorithmic in nature where AI plays a key role in deciding whether to buy or sell securities.

Crypto-tokens and initial coin offerings (ICOs)

Crypto-tokens are medium of exchange for executing transactions on a blockchain. They are analogous to loyalty points, flying miles or credit card points used by a select group of individuals, who have them. They do not have a universal usage like fiat currencies.

They are created using the standard templates like that of Ethereum network that allows an application to create its own crypto-tokens. Such blockchains work on the concept of smart contracts or decentralised applications (DApps), where the programmable, self-executing code is used to process and manage the various transactions taking place on the blockchain.

ICO refers to the creation and sale of crypto-tokens. In an ICO, a blockchain application creates a certain number of crypto-tokens and sells them to the public. The public could be interested in the crypto-tokens on offer for either or both of the following reasons:

- Crypto-tokens have an inherent benefit of granting the holder access to a service, a say in an outcome or a share in a project's earnings.
- Crypto-tokens could appreciate in value, depending upon the demand and supply.

Crypto-tokens are usually listed on crypto exchanges, where initial buyers sell their holdings and new buyers join in at any time. As a type of digital crowd funding, crypto-token sales enable start-ups not only to raise funds but also to bootstrap the project's adoption by incentivizing its use bycrypto-token holders.

Decentralised autonomous organisation (DAO)

One of the questions in economic theory has been "Why do firms exist?"[15] and why the same objectives cannot be met through contracts between individuals. The explanation given for a firm's existence is that it is very difficult to manage contracts between individuals for completing the work efficiently and the economic cost associated with managing these contracts may be high.

[14]Sadiku, M. N. O., Eze, K. G., &Musa, S. M. (2018). Smart Contracts: A Primer. *Journal of Scientific and Engineering Research*, 5(5): 538-541.

[15]Coase, R.H. (1937). The Nature of the Firm.*Economica*, 4(16), pp.386–405;Williamson, Oliver E. (1985).*The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting.* London: MacMillan,; and Williamson, Oliver E. (1975) *Markets and Hierarchies.* New York: Free Press.

However, with the advent of digital technologies, internet and now, blockchain as well as smart contracts and ICOs, many people believe that the firms can be organised in a different fashion, where rather than having a hierarchical centralised structure, these technologies can be used to reduce frictions and allow the firms to run in a decentralised way. The idea of a DAO is born out of this philosophy and background.

DAO is a business or organisation whose decisions are made electronically by written computer code or through the vote of its members. In essence, it is a system of hard-coded rules that defines an organisation's actions.

2.5 Conclusion

To conclude, while evaluating a blockchain-based application, the following needs to be understood / defined:

- Who can participate in a blockchain application and who can get access to the information, i.e., whether the blockchain application is permissioned/permission-less and private/consortium/public?
- What is the consensus mechanism that is being adopted?
- What are the governance rules, i.e., how can the source code/algorithms be changed?
- What is the application, i.e., what records are being maintained?
- What is the medium of exchange, i.e., fiat money, cryptocurrency, crypto-tokens, etc.?

3. Application of blockchains

Blockchain technology clears one of the major constraining dimensions for economic activity – the need for individuals or entities to know and trust each other – before executing a transaction. This, together with the ability of blockchains to store and distribute information securely, has resulted in them being heralded by some as the next big disruptive technologies. Enthusiasts believe that the possibilities for blockchain are abundant and it may even disrupt the established digital economy platforms. Some commentators refer to blockchain as the new internet[16], comparable to what it was three decades ago. However, there is no consensus on whether blockchains will become pervasive or not. Research and development are currently underway to address some of the present challenges that the technology is facing, for instance, how can the rate of verifying transactions be increased and how can common technical standards be adopted, to name a few.

Other applications of blockchain are also built around each or a combination of these attributes. Blockchains have the highest potential in markets or business situations where trust, transparency and high level of decentralised information is required. The power of tokenisation – the process of embedding data related to a real-world asset (product or service) on a digital token stored on a blockchain – can play a key role in unleashing the potential of blockchain applications beyond cryptocurrencies.

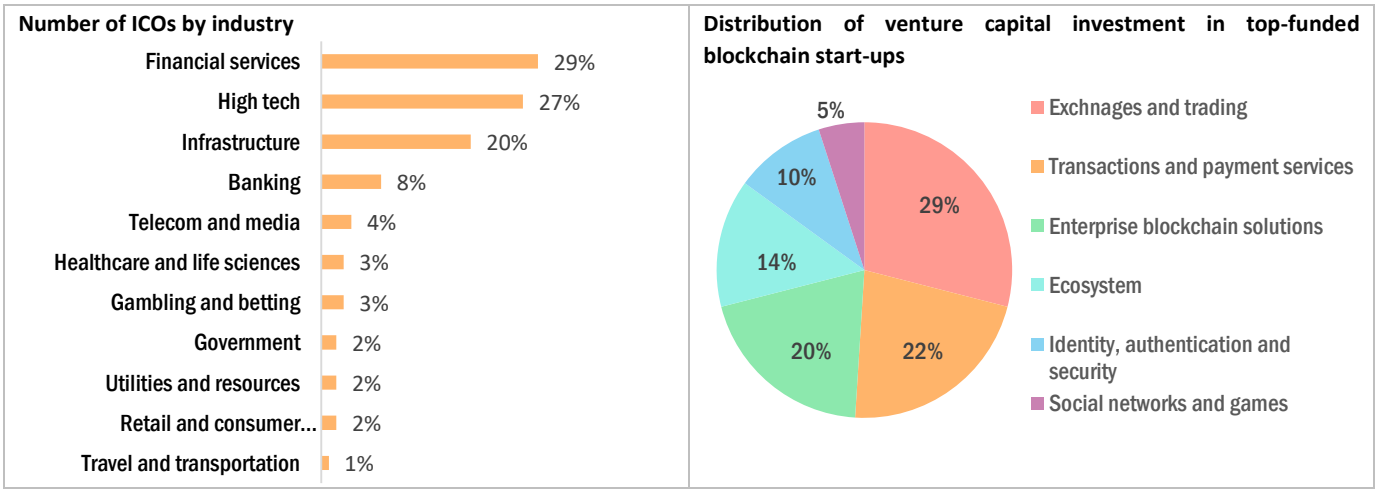
3.1 Current state of blockchain applications globally

A study by the National Association of Software and Service Companies (NASSCOM) and Avasant on blockchains highlighted the following points:

- Fifty countries have embarked on initiatives to integrate blockchains in their economies.
- Global blockchain investments through venture capital (VC) and ICO was over US$20 billion in 2018.
- Blockchain development is still at an early stage – over 90% of the reported cases are at the level of either proof of concept or at a pilot stage.
- Blockchain technologies are evolving and some of the areas of focus are interoperability between platforms, cost-effective and faster transactions.[17]

The following figures illustrate the distribution of blockchain investment in terms of ICOs and venture capital investment across major industries and solutions.

Figure 7: Investment in blockchain industry globally



Source: Avasant. (2019). *NASSCOM Avasant India Blockchain Report 2019.* [online]

To summarise, given the vast potential of the technology, there is a growing interest in exploring blockchain-based applications across geographies and industries.

[16]Cretin, A. (2018). *It's 2018 — Blockchain is on its way to Become the New Internet* [online].*Medium*. Available at: https://medium.com/@andrewcretin/its-2018-blockchain-is-on-it-s-way-to-become-the-new-internet-7055ed6851ec
[17]Avasant. (2019). *NASSCOM Avasant India Blockchain Report 2019* [online].

3.2 Value addition through use of blockchain technology

Pro-competitive effect of blockchains

Blockchains can lead to various pro-competitive effects including providing a way for more efficient growth of firms and increasing competitiveness in markets[18]. For instance,

- They may enable individuals and entities to bypass intermediaries, provide consumers with greater information, and enable more efficient transactions[19]. Better functioning markets may thus be promoted as a result of the decentralised and transparentnature of blockchains[20].
- They can reduce transaction cost between unrelated entities, as a result of which it may be possible for firms to disaggregate their different departments and outsource the related functions to external individuals/entities. As a result, competition for these functions may increase[21].
- They can provide small and medium enterprises (SMEs) with an efficient and trusted way of transacting with consumers, thereby removing any barriers that may result from the existing economies of scale[22].

The most prominently discussed pro-competitive effect of blockchains relate to their possibility to increase competition by lowering barriers to entry and creation of new products and services. An example is a digital marketplace created on a blockchain that does not assign control (over both price and access to data) to a single entity[23]. Such a marketplace by enabling individuals and firms to transact without an intermediary may be able to increase competition in the market[24].

Increasing efficiency through decentralisation and disintermediation

One of the key features of a blockchain is its ability to verify transactions collectively, without relying on a centralised intermediary. As a result, in some markets such as payments systems, blockchain can enable peer-to-peer transactions without involving an intermediary to bear counter party's risk, maintaining ledgers and updating and sharing information. Such markets are potentially at risk of disruption by blockchain-based applications.

Smart contracts are an application of blockchain that is gaining increasing attention, given its decentralised nature. For instance, in 2017, AXA had launched a flight delay insurance service, Fizzy, which processed claims using a smart contract[25]. Under Fizzy, once a customer recorded his flight, selected his cover and paid the premium, a smart contract was created in the form of code[26]. From public sources, the smart contract collected information about flight delays and automatically made payments to a consumer in case his/her flight was delayed[27]. This example also illustrates how IoT and 5G can lead to new applications of blockchains.

Smart contracts have applications in various sectors such as insurance, healthcare, automobiles, real estate, insurance, lotteries, supply-chain management, cryptocurrency exchanges, financial exchanges, covenants, law (including creating a will) and government (e-voting system)[28]. Smart contracts do not require manual intervention, such as raising a claim request or processing it, thereby saving time and cost for both parties. For instance, in the clearance and settlement of accounts, blockchains allow near real-time transactions between two parties directly, thereby reducing cost and the time involved.

In existing markets, where transaction costs are high and many intermediaries are required to consummate transactions, or where the exchange of information or transaction involves significant time delays, smart contracts save costs and time involved in a transaction.

[18] Directorate For Financial and Enterprise Affairs Competition Committee, OECD. (2018). Blockchain Technology and Competition Policy-Issues paper by the Secretariat [online]. Available at: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf
[19]ibid
[20]Nissen, Morten. (2018). Blockchain technology and competition law - issues to be considered[online]. Bird & Bird. Available at: https://www.twobirds.com/en/news/articles/2018/global/blockchain-technology-and-competition-law-issues-to-be-considered
[21] Directorate For Financial and Enterprise Affairs Competition Committee, OECD. (2018). Blockchain Technology and Competition Policy-Issues paper by the Secretariat [online]. Available at: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf
[22]ibid
[23]Catalini, C. (2017). Why Blockchain Can Be Good For Competition. *Forbes.*[online] Available at: https://www.forbes.com/sites/christiancatalini/2017/10/30/why-blockchain-can-be-good-for-competition/#165ec1d768ec
[24]ibid
[25]Temperli, Daniel. (2018). Why is blockchain so interesting for insurance companies? [online] *AXA Schweiz* Available at: https://www.axa.ch/en/unternehmenskunden/blog/start-ups-and-innovation/blockchain-insurance-switzerland.html
[26] Ibid
[27] Ibid
[28]Sadiku, M. N. O., Eze, K. G.,& Musa, S. M. (2018). Smart Contracts: A Primer. *Journal of Scientific and Engineering Research*, 5(5):538-541.

Leveraging the ability to authenticate or verify the identity of an individual or origin of a product

In markets or business processes where verification of the identity of an individual or the origin of products is critical, blockchains may be effectively used as they create an immutable database to authenticate identity in a short time and possibly at a lower cost. This benefit of blockchain technology helps firms across industries to increase the efficiency and transparency of their supply chains, i.e., from tracing the procurement of raw material to manufacturing, warehousing, delivery and payment.

For instance, an Italian food and wine producer, developed a proof of concept for a blockchain wherein the producer and customers, with the help of a smart label, were able to see all the information about the winery and the entire process of cultivation, production and wine-making (represented with story-telling) of each bottle, maximising both the trust and the user experience. Blockchain applications, in addition to enabling users to trace the distribution of the product, may also overcome counterfeiting (with a strong potential in the pharmaceutical sector to verify the authenticity of medicines).

Similar blockchain-based solutions may also be used to facilitate international trade and improve customs processes. For instance, Maersk and IBM introduced a blockchain-enabled shipping solution, TradeLens, that enables efficient, predictable and secure exchange of information and fosters greater collaboration and trust across the global supply chains.[29] The solution involves enabling shippers, shipping lines, freight forwarders, port and terminal operators, inland transportation and customs authorities to interact more efficiently by providing them with real-time access to shipping data and shipping documents, including IoT and sensor data ranging from temperature control to container weight[30].

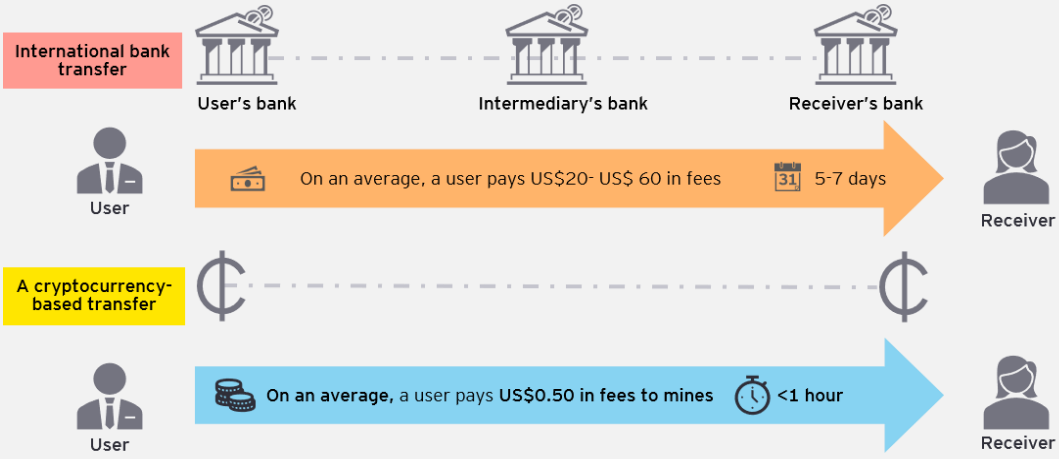
Box 2: World Food Programme uses blockchain

The World Food Programme (WFP), the food-assistance branch of the United Nations is the world's largest humanitarian organisation addressing hunger and promoting food security. It provides food assistance to an average of 91.4 million people in 83 countries each year. Traditionally, the idea of providing social assistance has been to be physically present and distribute resources, or through costly intermediaries, if distributed virtually.

However, since 2016, WFP has been using blockchain technology to make cash transfers more efficient, while protecting beneficiary data, controlling financial risks and reducing costs. WFP's initiative, Building Blocks, runs on a private, permissioned blockchain with a Proof-of-Authority consensus algorithm. So far, it has successfully transferred more than US$23.5 million worth of entitlements and helped 106,000 Syrian refugees in Jordan.

After a trial phase of four months in Pakistan, a pilot project was initiated in Jordan's Azraq and Zaatari refugee camps. Here, WFP's biometric authentication system allowed the refugees to buy food from supermarkets, set up across the camp, by simply looking at the iris scanner. Through this process, the biometric system was able to accurately verify the identity of the refugees and their spending using WFP food vouchers that were linked from their accounts.

As compared to the days when refugees had to wait for days for local banks to validate their identity and transfer money, this system is time-saving as it encrypts refugees' data and enables workers to transfer vouchers almost instantaneously once refugees are registered. This innovative IrisGuard eye-scanning technology virtually eliminates identity fraud, excessive bureaucracy and systemic corruption usually present in refugee camps across the globe.



Blockchain has disrupted the idea of providing social assistance from traditional bank transfers by offering:

- Lower transaction fees and real-time reconciliation of accounts.

[29]TradeLens. (2018). Solution Brief [online]. Available at: https://www.tradelens.com/wp-content/uploads/2018/12/TradeLens-Solution-Brief_Edition-One.pdf

[30]IBM website. (2018). Maersk and IBM Introduce TradeLens Blockchain Shipping Solution [online]. Available at: https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution

- More secured and reliable route to record identities.
- Safer mode to transfer money and maintain records of the transactions done.
- Lower dependence on any national authority, thereby reducing latency.

In addition to money transfers, WFP is already looking to experiment with blockchain for supply chain management and may offer its technology to others as a basic accounting system, for tracking disbursements for food and entries for land ownership, educational credentials and travel history.

Source: Wfp.org. (2018). *Blockchain for Zero Hunger.*

Creating trust through a repository of verified immutable records

Blockchain technology may be useful in cases where control over data or maintenance of verified records is extremely important. The technology may contribute significantly in exercising control over data or maintaining a registry of verified records for a variety of purposes, such as education, health or land titles[31].

For instance, the Republic of Georgia developed a pilot blockchain-based land titling project[32], which made it the first country to covert the data pertaining to land registry to a blockchain[33]. In addition to providing a transparent and immutable register of land titles, the pilot project also reaped the benefit of reducing cost and time involved. This example can also be used by the potential recruiters to verify a candidate's information, such as identity, academic or employment records.

The healthcare sector can also reap the benefits in terms of the security and accuracy of records. Clinical and medical data, such as vaccination and medication records, patients' data, genetic histories, insurance policies and clinical trial results can be securely stored and shared with relevant parties through a blockchain. For instance, the Taipei Medical University Hospital and Digital Treasury Corporation (DTCO) developed a blockchain-based personal healthcare record operating system, phrOS, and tested it in their hospital[34]. The system ensured that medical data is collected and stored securely, protecting it from being hacked. At the same time, it provided patients with greater control of their healthcare data enabling them to own and share it easily[35].

Increasing efficiency in public services

Blockchain's ability to provide security, transparency and verification of the identity of an individual makes it attractive for the governments for digital record keeping, facilitating cross-departmental coordination or providing public services or aid. The government in the City of Vienna, for instance, has developed a public blockchain to validate and secure the city's Open Government Data (OGD)[36]. The OGD included data such as public transport routes, train schedules and surrounding communities' voting results.

[31]A point to note is that a blockchain confirms ownership (of property or land) but cannot enforce its possession by the owner (an intermediary such as the government continues to be important for the same).

[32]Shang, Q. and Price, A. (2018). A Blockchain-based Land Titling Project in the Republic of Georgia. Blockchain for Global Development II.*Innovations: Technology, Governance, Globalization,*Vol. 12, No.¾.

[33]Nimfuehr, Marcell. (2017).Blockchain application land register: Georgia and Sweden leading. (December). *The Medium.* Available at: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c

[34] Lu, N. (2017). "Taipei Medical University Hospital and Digital Treasury Corporation Jointly Release "phrOS"- The First Healthcare Blockchain Platform Worldwide."*The] Medium* [online]. Available at: https://medium.com/blog-ipseeds-net/taipei-medical-university-hospital-and-digital-treasury-corporation-jointly-release-phros-the-7e80cdfa87b9

[35]Chatterjee, K. (2018). Blockchain enabled Personal Health Record OS — Challenges & Opportunities in Health Care Informatics. *The Medium.* Available at: https://medium.com/dtco/blockchain-enabled-personal-health-record-os-challenges-opportunities-in-health-care-55161e3a5a32

[36] Ey.com. (2018). EY and City of Vienna collaborate on public blockchain networks. [online] Available at: https://www.ey.com/en_gl/news/2018/08/ey-and-city-of-vienna-collaborate-on-public-blockchain-networks

3.3 Blockchain in India

In India, cryptocurrencies have received a great deal of regulatory attention over the past several years, culminating in a recent recommendation by an inter-ministerial committee to ban trading and holding of cryptocurrency. Since 2018, banks have been barred by the Reserve Bank of India (RBI) from dealing with cryptocurrency firms and their exchanges.[37] Several petitions have been filed before the Supreme Court to overturn the RBI's ban. On 4 March 2020, the Supreme Court while recognising that the RBI is empowered to take action since cryptocurrencies are a medium of exchange and a unit of value, set aside the circular by the RBI on grounds of proportionality[38].

Further, the Government of India had set up an inter-ministerial committee to determine the legality of cryptocurrencies and blockchain. In its report submitted to the Finance Ministry on 23 July 2019, a ban on private cryptocurrencies is recommended in India[39]. The committee also formulated a draft law, namely, Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019, which mandates a fine and imprisonment of up to 10 years for dealing in private cryptocurrencies[40].

The committee, however, said the government should keep an open mind on the potential introduction of an official cryptocurrency. The committee also recognised that there is a difference between cryptocurrency and its underlying technology, i.e., Distributed Ledger Technology (DLT) or blockchains. The report has identified various applications of blockchain technology for financial services such as cross-border payments, loan issuance and tracking, insurance, securities and commodity trading, collateral and ownership registries, such as land records. Earlier in 2017, the RBI had issued a white paper on applications of blockchain technology for the banking and the financial sector in India, which identified blockchain as one of the three pillars to drive digital transformation and innovation in the Banking, Financial Services and Insurance (BFSI) sector (Artificial Intelligence and Internet of Things, being the other two pillars)[41].

The potential application of blockchain technology in India, however, extend beyond cryptocurrencies, with various firms exploring ways to leverage the technology to address business issues in a wide range of sectors. The following chart highlights some of the sectors and the applications where blockchain technology is being applied in India.

[37]Business Today. (2018, July 3). RBI cracks down on Bitcoin; bans banks from dealing with cryptocurrency traders.)[online]. Available at: https://www.businesstoday.in/current/economy-politics/rbi-bans-cryptocurrency-trade-banks-transaction-bitcoin-exchanges/story/274214.html

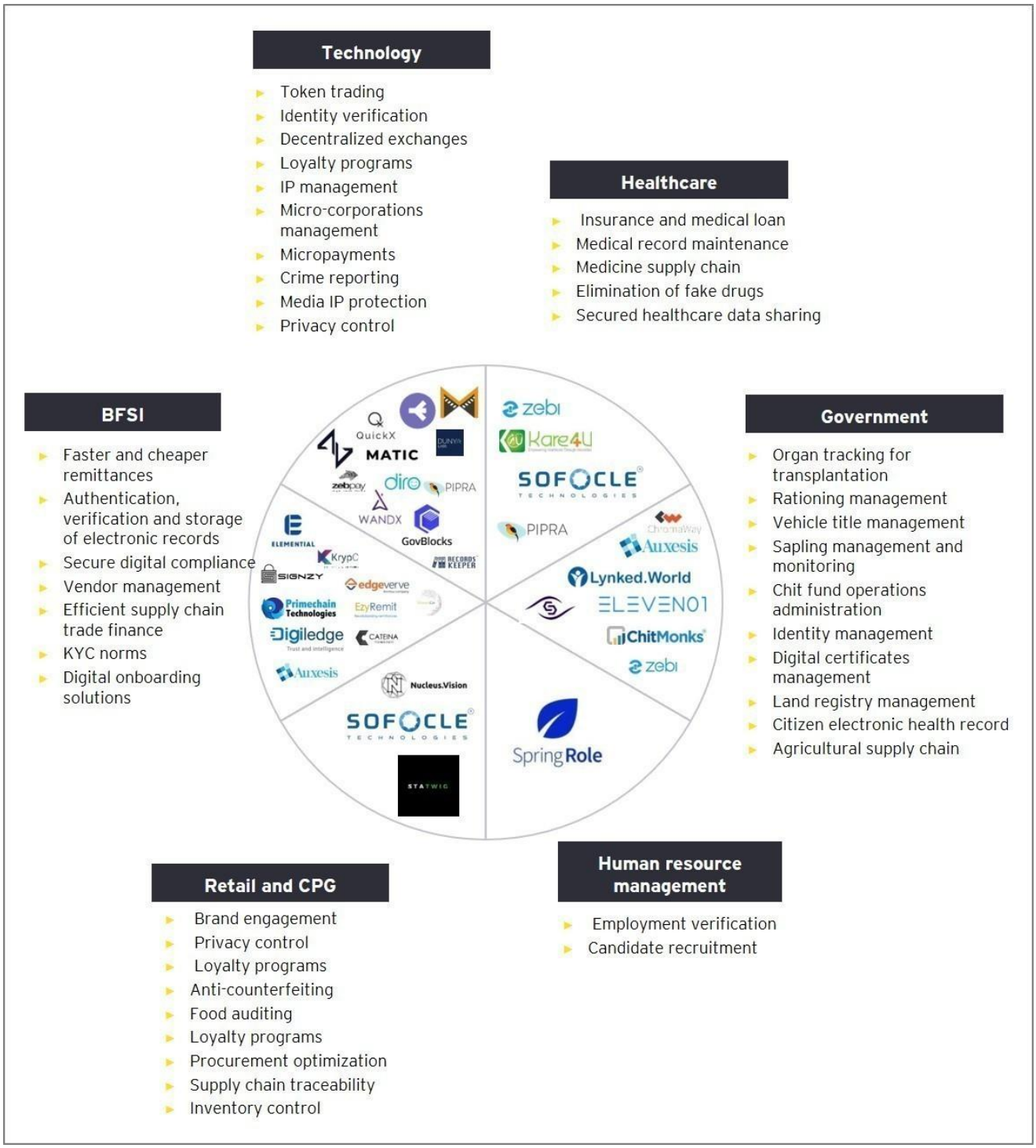
[38] Supreme Court of India Order dated March 4, 2020. Bench: Rohinton Fali Nariman, Aniruddha Bose, V. Ramasubramanian. Delivered by V.Ramasubramanian

[39] Mishra, Asit Ranjan. (2019). Panel favours cryptocurrency ban in India. [online]*LiveMint*. Available at: https://www.livemint.com/industry/banking/government-panel-suggests-ban-on-private-cryptocurrencies-1563796292369.html

[40]PRSIndia. (2019). *Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019*. [online] Available at: https://www.prsindia.org/billtrack/draft-banning-cryptocurrency-regulation-official-digital-currency-bill-2019

[41]Whitepaper by IDBRT, established by Reserve Bank of India.*Applications of Blockchain Technology to banking and financial sector in India* (2019). [online] Available at: https://idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf.

Figure 8: Blockchain technology in India



Source: Avasant. (2019). *NASSCOM Avasant India Blockchain Report 2019.* [online]

Some examples of blockchain applications in India are discussed in the Box 3 below. This is not an exhaustive list but provides an understanding on how organisations and individuals are thinking of leveraging the technology.

Box 3: Examples of blockchains initiatives in India

Technology firms in India have introduced various pilot projects and proof of concepts based on blockchain technology across various sectors and geographies. Following are some select examples of blockchain solutions introduced in India:

- Coffee Board, in collaboration with Eka Plus's blockchain-based marketplace application, Eka Blockchain Marketplace, launched a pilot blockchain-based coffee e-marketplace to integrate Indian coffee growers with global markets in a transparent manner and ensure fair price realisation for the producers[42]. While Indian coffee is highly-valued globally and is sold at a premium, the small size of producers and the presence of various intermediaries lowers the earning for the coffee growers[43]. This blockchain application is expected to improve the transparency in the trade of Indian coffee and maintain the traceability of Indian coffee from bean to cup to provide the consumers' authentic taste. The application also ensures fair payment to the coffee grower for the produce[44]. It also ensures reliable traceability, may minimise middlemen between coffee producers and buyers, and may help farmers increase their income[45]. It also allows coffee farmers, traders, coffee curers, exporters, roasters, importers and retailers to access the blockchain sharing details about the place where the coffee is grown, details of the crop, elevation, certificates (if any), etc.[46]According to reports, the number of Indian coffee farmers registered on the platform increased from just 23 since its launch in the early 2019 to 30,000 in November 2019[47].

- Edu Chain, a blockchain-based digital credential management solution developed by Zebi Data India Pvt Ltd., enables students and universities to store, retrieve and verify their data online[48]. Various universities, including IIT Basara, had adopted this solution[49].This application allows students to securely store their academic records and educational certificates in their wallets[50]. Additionally, it enables quicker verification of their records by employers and universities. It also provides universities the protection from fraudulent activities, enhances the credibility of their educational certificates' and helps in tracking the fee collection and payment by supporting an audit trail for each transaction[51].

- In 2018, NITI Aayog, Oracle, Apollo Hospitals and Strides Pharma Sciences announced a plan to pilot a blockchain-based real drug supply chain solution[52]. The solution permanently registers a drug's record, including its serial number, labelling and scanning, through its movement from a manufacturer to logistics, from stockist to hospital, or from pharmacy to consumer, limiting the scope for the record to be deleted or tampered[53]. The Internet of Things (IoT) software also enables tracking critical information such as chemical ingredients of the drug or maintenance of temperature control in case of life-saving drugs or vaccines[54].It is expected that this solution may support governments and healthcare experts to detect fake drugs sooner and enable them to penalise offenders with easy, proof-based data[55].

- In 2018, Cognizant and a consortium of leading life insurers in India (including SBI Life Insurance, Max Life Insurance, Canara HSBC OBC Life Insurance, Edelweiss Tokio Life, IDBI Federal Life Insurance, Birla Sun Life Insurance, HDFC Life, Kotak Life, Tata AIA Life, PNB MetLife, India First Life Insurance, ICICI Prudential Life Insurance, Bharti AXA, Aegon Life, and Star Union Dai-ichi Life Insurance) announced that they have developed a blockchain-based solution for exchanging insurance-related

[42] Ledger Insights.(2019). India's Coffee Board unveils blockchain based marketplace. Available at:https://www.ledgerinsights.com/blockchain-coffee-food-traceability-india/
[43] Ibid
[44] Ibid
[45] Ibid
[46] Ibid
[47] Ledger Insights. (2019). India's Coffee Board registers 30,000 farmers on blockchain marketplace.. Available at:https://www.ledgerinsights.com/india-coffee-board-blockchain-marketplace/
[48]Zebi website <https://zebi.io/edu-chain/>
[49] Ibid
[50] Ibid
[51] Ibid
[52]The Economic Times (2018, September 28). NITI Aayog, Oracle, Apollo Hospitals, Strides Pharma team up for real drug supply. Available online at: //economictimes.indiatimes.com/articleshow/65997772.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
[53] Ibid
[54] Ibid
[55] Ibid

information between the firms[56]. The solution, built on Corda, a platform developed by R3 and hosted by Microsoft's Azure infrastructure, enables insurers to overcome the risk of data breaches, fraud and money laundering and improves their process efficiently, through record-keeping and minimising the turnaround time[57]. The blockchain is expected to make the records available on a near real-time in a transparent and consistent manner, thereby making the audit easier. This is likely to reduce operating costs for insurers by avoiding duplication of procedures and streamlining the approvals[58].

Besides these, various other blockchain applications are also developed in India. For instance, the National Stock Exchange (NSE) tested the use of blockchain for know your customer (KYC) process along with some Indian banks[59] and undertook a pilot for e-voting using blockchain[60].

Further, state governments in India are working at leveraging the inherent benefits of blockchain. Some of these are:

1. The Government of Andhra Pradesh announced plans to use blockchain technology for hosting land records and for streamlining the process of maintaining records pertaining to vehicles' ownership[61].
2. The Municipal Corporations of Bankura and Durgapur districts in West Bengal partnered with the Netherlands-based company Lynked. World to work towards building a blockchain-based platform for issuing birth certificates[62].
3. The state governments in Rajasthan and Uttar Pradesh also announced the intent of implementing a blockchain solution in managing land ownership records[63].

In July 2018, the Telecom Regulatory Authority of India (TRAI) passed the Telecom Commercial Communications Customer Preference Regulations (2018), mandating telecom companies in the country to adopt blockchain technology (permissioned and private/consortium) to (a) ensure that all necessary regulatory pre-checks are carried out for sending commercial communications; and (b) operate smart contracts among entities for effectively controlling the flow of commercial communication. Further, the telecom companies are also required to establish blockchains to record (a) user's complaints and reports of violations of the regulations in an "immutable and non repudiable manner"; (b) details of the users; and (c) history of complainants and senders and details of all complaints (including their resolution) over the last three years. The blockchain also enables interaction and exchange of information between relevant entities in a safe and secure manner. The regulation also talks about the possibilities of setting up regulatory sandboxes for the blockchain solutions.

[56]The Economic Times. (2018, April 16). Indian life insurers' consortium and Cognizant build industry-wide blockchain solution. Available online at:https://cio.economictimes.indiatimes.com/news/digital-security/indian-life-insurers-consortium-and-cognizant-build-industry-wide-blockchain-solution/63782077

[57] Ibid

[58] Ibid

[59] Coindesk. (2017, February 8). India's Biggest Stock Exchange is Testing Blockchain KYC. Available online at:https://www.coindesk.com/india-stock-exchange-blockchain-kyc

[60] The Hindu Business Line. (2018, September 28). "NSE to test e-voting using blockchain." Available online at:https://www.thehindubusinessline.com/markets/nse-to-test-e-voting-using-blockchain/article25058651.ece

[61]*Andhra Pradesh Cybersecurity Summit Post Event Coverage Dossier*

[62]Avasant. (2019). *NASSCOM Avasant India Blockchain Report 2019.* [online]

[63]Ibid

3.4 Centralised databases vs blockchains

Blockchains provide benefits such as the creation of new markets, increasing the efficiency of existing markets by decreasing transaction costs and processing times, streamlining business processes, etc. Table 1 compares traditional databases with permissioned and permission-less blockchains.

Table 1: Key differences between different kinds of databases

	Traditional centralised database	Permissioned blockchain	Permission-less blockchain
Type of network	Centralised	Semi-centralised	Decentralised
Cost of transaction	High (Depending on the fee charged by the intermediary)	Low	Low to medium (depends on the associated cost of the consensus mechanism)
Speed of transactions	High	High	Low to medium (depends on the consensus mechanism)
Ease of implementation	Can use the existing system	Requires wider network of bandwidth	Requires wider network of bandwidth
Logical Decentralisation*	Low	High	Low
Political Decentralisation*	Low	Medium	High
Architectural Decentralisation*	Low	Medium	High
Mutable history of records and ownership	Mutable	Immutable	Immutable
Consensus mechanism	None	Varies across blockchains	POW, POS
Crypto-token use	Not required	Not required	Used
Identity	Known identities	Known identities	Anonymous
Scalability/ability to change	High	High	Low

Source: **Buterin,Vitalik (2017). "The Meaning of Decentralization" [online].*The Medium*. Available at:https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274**

While blockchain has its benefits over centralised databases in certain applications, scalability is realised as a major challenge for blockchain technology. The two biggest financial transaction applications of blockchain, Bitcoin and Ethereum, have far slower[64] transaction processing speeds than centralised platforms. The failure to scale up the speed has also led to increased transaction charges[65], which further constrains the usage of the blockchains. This also explains why businesses are exploring permissioned applications of blockchain increasingly.

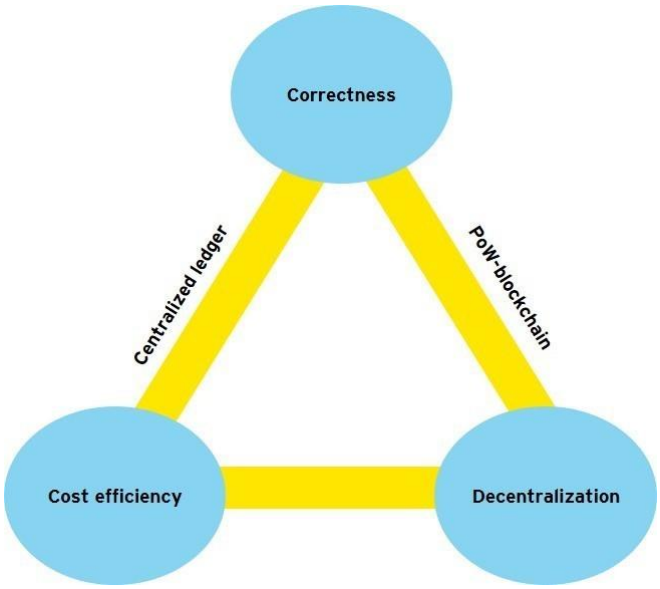
Blockchain technology, as it exists today, suffers from central trilemma[66], which could explain its slow growth till date. Being a decentralised distributed ledger technology, compared to a centralised database, a blockchain application has a trade-off between either achieving correctness or speed of consummating transactions (leading to cost efficiency). The Ethereum blockchain platform's future transition to POS consensus from its original POW consensus is a step to solve the issue of the speed. However, it is yet to ascertain its success untilits implementation.

[64] Funcas (2018). The future of blockchain in the European banking system. *Funcas - SPANISH AND INTERNATIONAL ECONOMIC & FINANCIAL OUTLOOK (SEFO).* [online] Sefofuncas.com. Available at: http://www.sefofuncas.com/Spains-near-and-medium-term-economic-outlook-Progress-and-challenges/The-future-of-blockchain-in-the-European-banking-system

[65] Bitinfographics website. Available at: https://bitinfocharts.com/comparison/transactionfees-btc-eth.html; The Star Business Journal (2019, August 19). Multimillionaire 25-year-old crypto king Vitalik Buterin speaks to the Star about the future of Ethereum. Available at: https://www.thestar.com/business/2019/08/19/ethereums-vitalik-buterin-on-reducing-cryptocurrencys-risks.html

[66]Voxeu.org. (2018). The economics of blockchains. VOX, CEPR Policy Portal. [online] Available at: https://voxeu.org/article/economics-blockchains

Figure9: Public blockchain trilemma[67]



Source: Voxeu.org. (2018). The economics of blockchains. VOX, CEPR Policy Portal. [online] Available at: https://voxeu.org/article/economics-blockchains

[67]Abadi, J., & Brunnermeier, M. (2018). *Blockchain economics* (No. w25407). National Bureau of Economic Research.

4. Policy and regulatory aspects

Development of any new technology raises the following fundamental questions:

- Will the existing regulation act as a barrier in adopting the new technology? How will the technological application be interpreted by the existing legal systems?
- Are new regulations needed to facilitate the use of the new technology?
- Are new regulations needed to protect the public interest or prevent misuse by the new technology?

While evaluating policies and regulations related to new technology, it is important that there is a balance between innovation and concerns regarding potential threats emanating from its misuse.

An example is the Information Technology Act, 2000 (IT Act), enacted by the Government of India, to facilitate the use of IT in India. The facilitating changes incorporated by the IT Act included giving legal recognition to digital signature and providing for safe harbor rules on intermediary liabilities. Enactment of this law, therefore, facilitated the usage of information technology in India.

In the case of blockchains, some of the key regulatory challenges relate to jurisdictional issues, data protection and privacy, and competition issues.

Jurisdictional issues and anonymity

Given the decentralised nature of blockchains, there may not be any identifiable host, or an operator and the nodes may be spread across the globe with transactions occurring between the nodes located in different jurisdictions. Therefore, in case of any legal, policy or regulatory issue, it is difficult to understand which jurisdiction's policies and regulations may apply.

In the case of permission-less blockchains, network participants may be anonymous or pseudonymous, i.e., their identities are not known fully. In such a scenario, policymakers and regulators are likely to face enforcement challenges in terms of identifying liable entities and penalising them for wrongful conduct.

Ambiguity about legal status and classification of organisational structure of blockchains

A legal entity can be defined as one that can own assets and property, enter into agreements or contracts, assume obligations, incur debts, can sue or be sued, and be accountable for illegal activities[68].

The organisational structure of an entity is, therefore, key in determining whether or not an organisation qualifies as a legal corporate entity (i.e. as a company, partnership or a limited liability partnership). In a blockchain, authority can be totally decentralised, with consensus playing a key role in decision-making. Therefore, it is difficult to understand who is responsible for the actions of a blockchain.

Current discourse on this presents a few possible alternatives:

- Blockchains may be treated as partnerships: If blockchains are to be considered general partnerships, individual participants can be reached for service and/or liability. Anyone using a blockchain could attempt to obtain jurisdiction over the organisation by serving any human participant. In a general partnership, each partner would be held jointly and severally responsible for all liabilities of the business and all personal assets of each partner are subject to seizure or lien by creditors. Thus, the parties to a blockchain may have unlimited potential liability for the entity's actions. If such an approach is followed, it would raise the level of risk of participating in a blockchain[69].
- Alternatively, the blockchain could be considered as a multi-party contract (or joint venture), with the group that sets up the code design and its nodes under a contractual obligation to maintain the system's security and operations.
- Under the Indian law, a blockchain could be potentially understood to be an "association of persons" for legal classification (and possibly taxation as well). This terminology is expressly recognised within certain legislations such as the Competition Act, 2002, and the Income Tax Act, 1961[70]. This interpretation may impose unlimited liability on the participants due to a lack of a structure.

Compliance with data privacy and protection laws

All the data recorded on a blockchain is stored in a distributed ledger, thereby eliminating the need for a central data repository. Most data breaches have taken place by getting access to the central data repository, which represents a single point of failure. In case of a

[68]The Law Dictionary. (2017). *What is LEGAL ENTITY? definition of LEGAL ENTITY (Black's Law Dictionary)*. [online] Available at: https://thelawdictionary.org/legal-entity/

[69]Rodrigues, Usha R. (2019). *Law and the Blockchain. Iowa Law Review.* [online] Available at: https://ilr.law.uiowa.edu/print/volume-104-issue-2/law-and-the-blockchain/; Metjahic, L. (2018). *Deconstructing the Dao: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*. *Cardozo Law Review*.[online] Available at: http://cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf

[70]Nishith Desai Associates. (2018). *The Blockchain Industry Applications And Legal Perspectives*. [online] Available at: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/The_Blockchain.pdf

blockchain, a hacker may have to target at least a majority of the nodes on a blockchain. As a result, blockchain-based applications are assumed to be more secure[71].

Despite this inherent strength, blockchains may not be fully compatible with the current privacy and data protection frameworks:

- Privacy laws have been designed on the basis that data is centrally collected, stored and processed, i.e., privacy laws assume that a singular entity is responsible for data management. Blockchains, on the other hand, are decentralised and a particular entity is not responsible for ensuring that an individual's data stays confidential. Further, data can be understood to be of different types such as personal data, sensitive personal data, anonymised or pseudonymised data. There are different obligations on how each of these data should be stored and shared under the privacy laws.
- Privacy laws such as the European Union's General Data Protection Regulation (EU GDPR) enforce the "right to erasure" or the "right to be forgotten". These rights (and corresponding obligations) include:
  - The right to have the personal data erased immediately when it is no longer needed[72].
  - The right to request a controller (a third-party) to rectify inaccurate or incomplete personal information[73].
  - The right to object to data processing based on a data controller's legitimate interests (including profiling) unless the controller can demonstrate compelling legitimate grounds that override the interests or rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.
  - The right to withdraw consent.

Similarly, at the time of writing this paper, the draft Personal Data Protection Bill, 2018, in India, has a section on the "right to be forgotten". Section 27 of the bill has listed out three scenarios in which an individual has the "right to restrict or prevent continuing disclosure of personal data" or the "right to be forgotten"[74].

However, in the case of blockchains, data is generally immutable and not erasable. There may be a need for harmonisation of the data protection laws and blockchain technology.

Localised data processing

Some countries may also require the data from the country to be stored and processed locally. For instance, India's draft Personal Data Protection Bill, 2018, mentions that in case of critical personal data, the data should be processed within India (data localisation) only. However, a blockchain can run across multiple jurisdictions. Any resulting cross-border transfer of critical personal data could stand to violate the law.

Issues related to smart contracts

The following are some of the challenges that could arise in case of smart contracts:

- One of the challenges may be a smart contract's inability to address contingencies. For instance, provisions with respect to the frustration of contracts due to change of law, impossibility, Force Majeure, and Act of God, etc., can be built into traditional contracts but may not be possible in smart contracts. Immutability and irreversibility of such contracts could be a challenge[75]. Under contract law, a contract is not just a set of instructions to be automatically executed; rather they are interpreted in the context of ever-changing real scenarios. Spirit of law supersedes the letter.
  - There may be further challenges related to validity of smart contracts. Under the existing provisions, contracts need signatures. Similarly, digital signatures are required for contracts that are executed digitally. The Indian IT Act, 2000 puts a limitation on obtaining these digital signatures, and says that only a government-designated certifying authority can provide these signatures[76]. This conflicts with blockchain technology as it uses a hash-key for authorisation. This disparity is also vis-à-vis the Indian Evidence Act (1872), Section 85B, which states that an electronic agreement would be considered valid only if it has been authenticated with a digital signature. These two provisions raise issues around validity and admissibility in case of a dispute[77].

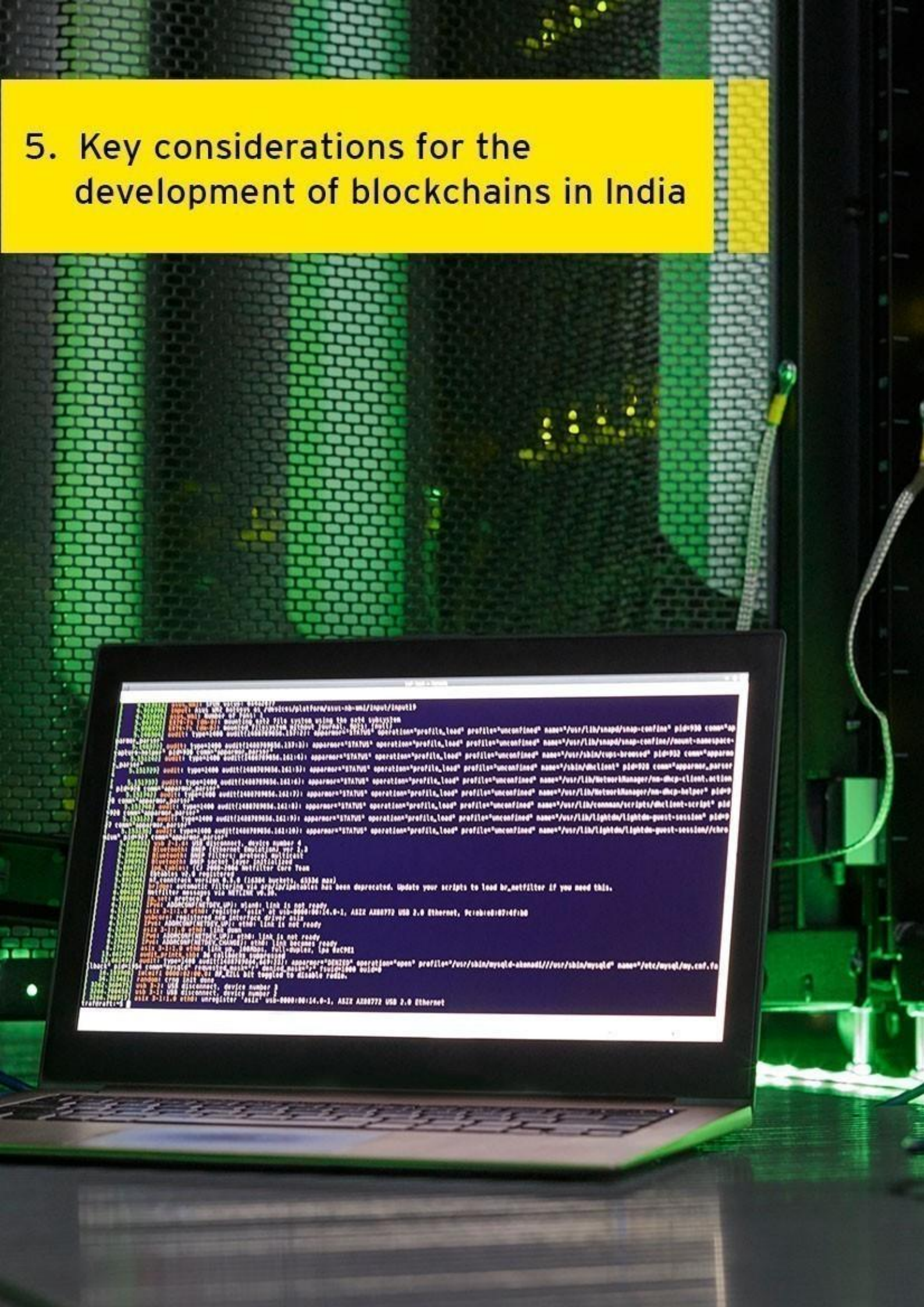
[71]Distributed Ledger Technology, Blockchains and Identity A Regulatory Overview. (2018). [online] Available at: https://www.gsma.com/identity/wp-content/uploads/2018/09/Distributed-Ledger-Technology-Blockchains-and-Identity-20180907ii.pdf.
[72]General Data Protection Regulation (GDPR). (2013*). Art. 17 GDPR – Right to erasure ('right to be forgotten')* [online] Available at: https://gdpr-info.eu/art-17-gdpr/
[73]General Data Protection regulation (GDPR) (2013). Art 16
[74]Saleem,Shaikh Zoaib. (2018, August 14). What is the right to be forgotten in India. [online]LiveMint. Available at: https://www.livemint.com.
[75]Supra note 41.
[76]Section 35 of the IT Act (2002). Mondaq.com. (2018). *Smart Contract In The Indian Crucible - Fin Tech - India*. [online] Available at: http://www.mondaq.com/india/x/711102/fin+tech/Smart+Contract+In+The+Indian+Crucible
[77]Ibid

Lack of a medium of exchange for executing transactions through permission-less blockchains

Transactions through permission-less blockchains may require a crypto-token or a measure for exchanging value. One of the objectives of ICOs and cryptocurrencies has been to create a medium for exchange of value. Since the usage of crypto currencies has been restricted[78]in India till the recent Supreme Court order, lack of a medium was a hinderance in its adoption.

[78]Reserve Bank of India circular dated 6th April 2018

5. Key considerations for the development of blockchains in India



India may derive economic benefits from the use of blockchain technology. Research and development on blockchains, including their different applications, their scaling up and future development are already underway.

Theoretically, it is expected that once blockchain applications cross the pilot and proof of concept stage, they will compete with other systems/technologies providing similar services that may not be based on blockchain technology. This is already being experienced to some extent in the financial services sector where blockchain technology was first applied. An example could be the market for providing cross-border payments where traditional banks may have to compete with solutions such as Ripple[79], which is a blockchain concept-based tool that enables users to make cross-border payments in various currencies. Ripple may put competitive pressure on the traditional banking system given that it is faster, cheaper and transparent.

Blockchain technology is an important innovation that can promote competition across different sectors of the Indian economy. Given the nascent stage of its development, removal of regulatory uncertainties and addressing policies that put blockchain applications at a competitive disadvantage may help in fostering the growth of this technology.

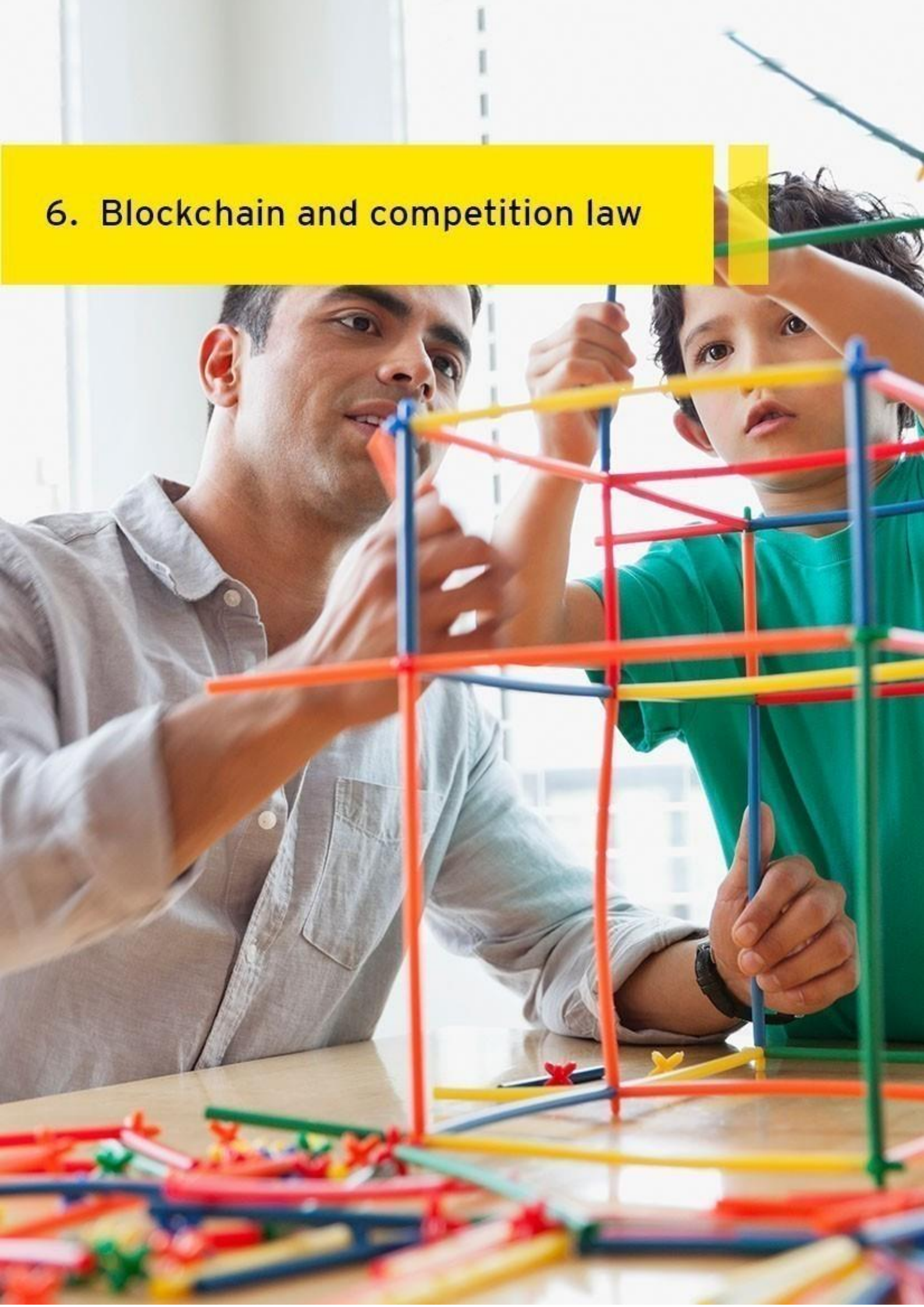
Acknowledging the pro-competitive benefits of blockchain applications, the following are certain relevant questions that are likely to determine the future of blockchain applications in India.

Box 4: Issues for further deliberation (Part 1)

1. What is the likelihood that blockchains will deliver on the expectation that they will change the way businesses operate in India?
2. In what ways can blockchain applications promote greater competition in India and what would be its benefits for consumers?
3. Are there any concerns about the ways in which incumbents may impede the use of blockchain applications?
4. What are the changes in the legal and regulatory framework (if any) that should be considered while promoting blockchain applications?

[79] Ripple. (2015). *Solutions To Send Money Globally, Using Blockchain Technology*.[online] Available at: https://www.ripple.com/ripplenet

6. Blockchain and competition law



Blockchains are an evolving technology and most applications based on this technology are at a proof of concept or pilot stage, thus there is very little empirical information on the conduct of blockchain applications, especially from a competition law perspective. However, the technology is attracting interest and there is a possibility for blockchains to become more pervasive, on the same scale that the Internet was a few decades ago.

The advent of the internet and the digital economy had also raised questions about the ability of competition law to address new competition concerns that rose as digital platforms became more pervasive. Some commentators felt that with the advent of the internet, a new set of rules may be required for assessing competition issues in the cyberspace[80]. However, the same principles of competition law are applied to digital markets[81], after understanding the concepts such as multi-sided markets and network effects, which are relevant to these markets. Similarly, acquiring an understanding on the blockchain technology may help competition authorities address competition issues related to blockchain applications. Discussions among blockchain stakeholders and the competition authorities on new market nuances and paradigms may help in getting an analytical understanding.

This section aims to educate blockchain stakeholders on:

- How competition issues could be evaluated under competition laws.
- The possible benefits from blockchain in terms of competition law enforcement.

6.1 Overview of Indian competition law and blockchain

Participation in a blockchain and agreements

One of the factors influencing applicability of the competition law to blockchain applications is whether participation in a blockchain can be defined as an agreement. For instance, in a case of an alleged collusion wherein competitors are hypothetically accused of havingexchanged competition-sensitive information through a blockchain application, the first question that would arise is whether the participation in the blockchain application can be construed as an "agreement" as defined in the Competition Act, 2002 ('Act'). The Act defines an agreement as "*any arrangement or understanding or action in concert*" irrespective of whether it is written or not and legally enforceable or not[82]. Thus, one could argue that when two firms or individuals participate in a blockchain application with pre-defined rules, they have entered into an "agreement". This suggests that any anti-competitive conduct emerging from participation in a blockchain application may be construed as a contravention of the Act.

Blockchain as an "enterprise"

Unlike traditional enterprises, blockchain applications are decentralised, i.e., there is no single entity that takes decisions. Rather multiple entities are involved in decision-making. This raises the question if a blockchain application can be viewed as a dominant enterprise. One possibility could be to consider all participants together as collectively dominant. However, collective dominance[83] is not yet recognised in India[84]. Even in jurisdictions such as the UK, the European Union and Singapore, where the concept of collective dominance is recognised, negligible enforcement has been made under this concept.

Under the Act, a blockchain may be considered as an enterprise. The Act defines an enterprise as "*a person or a department of the Government…"*[85] and a "person" to include, among others, "*an association of persons or a body of individuals, whether incorporated or not, in India or outside India*"[86]. Thus, a blockchain application may be taken as an enterprise (involved in the provision of the service of distributed ledger technology (DLT) under the scheme of the Act).

[80] Schrepel, T. (2018). Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.*SSRN Electronic Journal.* [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576
[81] Ibid
[82] The Competition Act, 2002 (12 of 2003) Section 2(b). (2012). [online] Available at: https://www.cci.gov.in/sites/default/files/cci_pdf/competitionact2012.pdf
[83] Collective dominance refers to a position of market power possessed jointly by a group of competing firms
[84] Competition Commission of India. (2019). [online] Available at: https://www.cci.gov.in/sites/default/files/17-of-2019.pdf
[85] Section 2(h), Competition Act of 2002.
[86] Section 2(l), Competition Act of 2002.

Enforcement

A competition authority's ability to apply competition law on blockchain applications may be influenced by certain features of a blockchain. For instance, in a permissioned blockchain access to the blockchain's data is restricted, while in a public permission-less blockchain data encryption and the pseudonymous nature of nodes may influence the authority's ability to analyze the data from a blockchain application. As a result, it may be challenging for the competition authority to identify if there is any economic evidence of anti-competitive conduct, also referred to as opacity effect of a blockchain.

Further, while assessing the allegation of collusion, the pseudonymous nature of the nodes in a public blockchain application may imply that even if the authorities are able to analyze the data on the blockchain to detect possible evidence of collusion, it may still be unable to determine the real-world identity of the specific nodes that are alleged to have colluded. This issue is relevant to other areas of competition law as well. Without being able to identify the firms engaged in the anti-competitive conduct, the authorities may be hindered from undertaking necessary measures to address the competition concern and penalise the concerned parties.

Moreover, the decentralised and distributed nature of a blockchain implies that there is no central authority that has control over its decision-making. This may make it challenging for a competition authority to enforce an order against any anti-competitive conduct especially in a public blockchain application wherein the nodes are pseudonyms. For instance, if the governance rules of a blockchain application, that is assessed to be dominant, are such that it provides a bundled product/service (without any acceptable justification), then even if there are orders that the products (or services) be unbundled and provided separately, it may not be possible to change the rules. In this regard, the Act futuristically enables the CCI to pass suitable remedies by enabling it to issue any such order or directions under the residual clause of Section 27 of the Act , as it may deem fit. To incorporate any change, it needs to be accepted by multiple/all nodes (depending on the consensus mechanism adopted). While some node(s) may implement the order by forking, all nodes may not necessarily move to the new fork. Additional issues may be raised by smart contracts if the contract is coded such that there is no way to stop its execution[87].

Jurisdiction

As has been discussed earlier, blockchain applications can exist across geographies. This could raise the jurisdictional issue for competition authorities around the world when nodes/market participants of a blockchain application are located across different countries. This challenge can be overcome by co-operation between competition authorities in different parts of

the world. Therefore, effective competition enforcement would hinge upon timely and accurate information sharing, communication and co-ordination between competition authorities around the globe.

Concerning India, Section 32 of the Act enables India to inquire into anti-competitive agreements, abuse of dominance, and mergers and acquisitions that occur outside India but are likely to have an appreciable adverse effect on competition in India. As mentioned above, international co-operation between competition authorities will play a key role in addressing the jurisdictional challenges arising from global blockchain applications.

Way forward

Awareness about competition issues that may emerge in the case of blockchains may help in the development and use of blockchain applications in line with the principles of the competition law. This may be achieved by proactively engaging the blockchain stakeholders (miners, developers, users, etc.) at an early stage while the technology is still being developed, making these stakeholders aware about the likely concerns of competition law that may arise and how competition authorities deal with them. This discussion paper is an endeavour in this direction.

This advocacy effort is likely to encourage blockchain stakeholders to take necessary steps to avoid certain conduct which may be potentially anti-competitive. For instance, if the concern related to the exchange of competition sensitive data among competitors is explained to the developers of blockchain applications, then they may adopt appropriate measures to remain compliant to the competition law. The solution adopted may include avoiding storing such information on a blockchain.

With strong advocacy and if feasible, through regulatory sandboxes, it may be possible to code and integrate competition law requirements into blockchain applications, which would benefit both the blockchain's stakeholders and promote the level of competition in India.

[87] Schrepel, T. (2018). Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.*SSRN Electronic Journal.* [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576

Box 5: Issues for further deliberation (Part 2)

5. Would agreements between different players in the blockchain ecosystem (especially where clear horizontal or vertical linkages are absent) be covered under Section 3 of the Act?
6. Would anonymity/opacity and decentralisation create hurdles for CCI to regulate the market activity, and if so, how can CCI overcome them?
7. How can CCI leverage its co-operation agreements with competition authorities outside India to address competition issues related to blockchain applications?

6.2 Blockchains and anti-competitive agreements

Section 3 of the Act prohibits enterprises, persons, or association of enterprises (or persons) from entering into anti-competitive agreements related to production, supply, distribution, storage, sale (or price), and trade in goods or provision of services. Specifically, the Act restricts a firm (or association of firms) from colluding with other firms (or association of firms) at the same or different levels of the production chain.

This sub-section discusses the potential examples of anti-competitive agreements (based on current available information relating to blockchains) and how they may be addressed within the purview of the existing law.

6.2.1 Horizontal agreements (Section 3(3) of the Act)

In the case of competitors (firms engaged in the same economic activity), anti-competitive agreements often take the form of collusion (cartelisation or bid rigging).

Various efficiency reasons may exist for competitors being a part of the same blockchain application (such as the creation of a new market or improving the current processes).

However,in certain cases, blockchain applications can also alter the gains and challenges associated with maintaining a collusive agreement.

For a collusive agreement between competitors to be successful, the firms that are a part of such an agreement should be able to:

- Interact with each other and arrive at a mutually agreeable coordination strategy.
- Monitor each other's conduct to ensure adherence to the agreement.
- Punish a firm in case of deviation from the agreement in such a way that the penalty supersedethe benefit from cheating on the collusive agreement.

Exchange of information

One of the benefits of blockchain is the ability of creating trust through a repository of verified immutable records. Blockchain applications facilitate sharing of a large amount of information, thereby increasing transparency. Transparency of information generally is expected to intensify competition.However, in some cases, it is possible that there may be visibility of information belonging to competitors, who are part of the blockchain. In a blockchain application, unless adequate measures are adopted, the transactional information in the ledger can be easily viewed by the blockchain participants (visibility effect). However, the same information may not be accessible to entities outside the blockchain (opacity effect) due to restricted access (in case of a permissioned consortium blockchain) or encrypted data with pseudonyms (in case of a permission-less public blockchain). Adequate safeguards should be put in place to ensure that this feature does not enable competitors to arrive at an agreement and monitor each other's conduct.

However, it is important to consider whether there is any difference that blockchain applications create for information exchange vis-à-vis other existing systems (such as physical or digital exchange of information). One difference may be that through a blockchain information can be exchanged on a near real-time basis. Additionally, there may be greater trust in the authenticity of the data stored in a blockchain than other systems, due to the secure and immutable nature of blockchains.

Self-enforcing smart contracts

As mentioned previously, with the advent of 5G, IoT and AI, smart contracts would play an important role in the world of technology and commerce by creating new products and services. However, smart contracts in a few cases could be used to enforce and maintain collusive agreements without the need for extensive information exchange. One way to do this would be for competitors to use smart contracts to self-enforce collusion using code and pricing algorithms in line with the collusive agreement[88].

Further, smart contracts could be misused to self-execute punishment on a co-conspirator who deviates from the terms of the collusive agreement. For instance, a smart contract may be used to create a fund with contributions from each firm. When one of the firms deviates from the agreed price or output levels by lowering their price or increasing their output, a smart contract may result in automatic forfeiture of the amount and its distribution among the other firms[89]. If the loss to the deviator from the forfeiture of funds exceeds the benefit from deviation, the smart contract could act as a deterrence to deviation and thereby facilitate collusion.

If firms use smart contracts to engage in collusive conduct, then they would be acting in contravention of the Act.

Reduced uncertainty about the market

In general, market uncertainty and volatility reduce chances of a stable cartel, since the participants of the cartel cannot differentiate between market volatility and competitors' behaviour causing such volatility in their own performance. However, when most players participate in a blockchain application, the resulting transparency in market information may reduce such uncertainty. For example, if each participant has information about the total number of transactions taking place on the blockchain application, it may provide an accurate and real-time indication of market conditions to the participants of a collusive agreement. This may allow them to differentiate between the instances of poor market conditions and deviation from the cartel agreement.

To conclude, it would be incorrect to assume that blockchain applications always facilitate collusion. But such a possibility may exist when competition-sensitive information is shared among competitors. Competition-sensitive information includes information about current and/or future price, discounts, profitability, cost, production, or information on future strategy and investment plans. Generally, sharing of data not related to price, cost or output and historic or aggregated data, do not raise concerns with respect to competition law. However, blockchains record transaction data, which may include competition sensitive data on quantity and price. Further, since new blocks are added to a blockchain without significant delay, the data is also not historic (and is shared frequently).

Concerns are less likely in the case of blockchain applications that include only the information that must be communicated to achieve their defined objectives and exclude other competition sensitive information which can be used for unlawful information exchange. For instance, in a blockchain application whose focus is to record land ownership, the only data that should be ideally recorded and shared should be the sale of land from A to B and not its price. Thus, in line with best practices associated with data protection, it is recommended to restrict data sharing to only that data which is relevant for the purpose at hand and is not competition sensitive. Governance rules of some blockchains, such as Corda, are designed such that when a transaction takes place, only the minimal and required amount of information is recorded in the blockchain.

Thus, just like industry associations, blockchains also need to avoid certain conduct. Specifically, a blockchain should undertake all necessary measures to ensure that competition sensitive data is not shared among competitors.

Box 6: Issues for further deliberation (Part 3)

8. What would be the economic rationale for competitors in a market participating in the same blockchain?
9. Could blockchain technology, particularly smart contracts, be used to maintain collusion, for example, setting up a system of side payments to competitors?
10. Should all nodes of a blockchain be held equally liable in the case of a collusion, even if they do not exchange information or act on competition sensitive information shared through the blockchain?

6.2.2 Vertical agreements (Section 3(4)of the Act)

Anti-competitive agreements between firms engaged in different stages of the value chain could take the form of tying-in agreements, exclusive supply/distribution agreements, refusal to deal agreements, and agreements aimed at resale price maintenance as per the Section 3(4) of the Act.

Following are some possible types of vertical agreements:

- A blockchain's governance prohibiting access for an entity using a competing blockchain application/wallet/exchange.

[88] Lianos, I. (2018, September). Blockchain Competition - Gaining Competitive Advantage in the Digital Economy: Competition Law Implications. Research Paper Series: 8/2018. Centre for Law, Economics and Society, UCL.

[89] For this threat of punishment to be credible, the loss due to the punishment should outweigh the benefit that a firm would make by deviating from the collusive agreement.

- An agreement between a blockchain platform and developer of blockchain applications running on the platform prohibiting/restricting the developer from dealing with any other competing platform.
- An agreement by a mining hardware provider tying the sale of its product to a miner by using a specific wallet.
- An agreement between a blockchain and its nodes/wallet/exchange that requires the latter to use only the blockchain application in question (thereby prohibiting the latter from participating in any other competing blockchain application).
- Smart contracts that self-enforce tie-in, exclusive supply/distribution, refusal to deal, or minimum resale price maintenance between entities at different levels of the value chain.

In some cases, the above vertical agreements could adversely affect the competition. Whether a vertical agreement is anti-competitive or not, is assessed on a case-by-case basis by balancing the anti-competitive impact against justifications for the vertical arrangement.

While analysis is undertaken on a case-by-case basis, generally the vertical anti-competitive agreements have a higher probability in the case of permissioned consortium blockchains than permission-less public blockchains. If a public permission-less blockchain, already in operation, is to engage in a vertical restraint such as a refusal to deal with an entity, there is a need to modify its rules, which would require the nodes to be in consensus with each other[90]. Further, any such change in a public permission-less blockchain's protocol would imply that it is no longer "permission-less" and "public". Whereas, in a permissioned consortium blockchain nodes can change their governance rules to engage in such conduct (by not permitting an entity from reading the information on the blockchain or/and restricting them from proposing new transactions or/and forbidding them from verifying transactions)[91].

Similarly, in a public blockchain, since the data is public, there is no incentive for the blockchain application to impose an exclusive dealing condition for the publishing of blocks. Further, once the block is published in a public blockchain, the node also has no incentive to publish it in another public blockchain given the costs involved. However, in a permissioned blockchain, dealing exclusively may be appealing to a blockchain application if it wishes to be the only source for data on a transaction (being the sole source of a data may increase the attractiveness of the blockchain)[92].

Blockchain technology could lead to several market efficiencies and create pro-competitive effects. For example, use of blockchain technology by a manufacturer to manage the procurement of inputs could allow him to consider a greater set of suppliers due to enhanced trust created by the blockchain system. This could result in greater competition benefiting the consumers. Some blockchain technology innovation may only be possible over permissioned blockchain with reasonable and justified restrictions in who could access the application. To conclude, there are various efficiency reasons due to which firms may prefer a permissioned blockchain over permission-less and public ones and these reasons are factored in while conducting a competition assessment.

6.3 Abuse of dominance (Section 4 of the Act)

In addition to anti-competitive agreements, the Act prohibits an enterprise from abusing its dominant position in a relevant market. Competition assessment related to abuse of dominance involves analysis of:

- Market power (or dominance) of the entity under investigation
- The impact a dominant entity's actions may have on the competition.

6.3.1 Assessment of market power

The first step while investigating an allegation of abuse of dominance (or analysis of a proposed combination) is the determination of the relevant product and geographic markets followed by an analysis of market power (dominance) in the delineated relevant market. Market power assessment is crucial as it enables filtering out the cases where the entity being investigated is a small player and its conduct is unlikely to harm competition in the market.

Relevant product market

The key principle used to define the relevant market is the demand substitutability of the product/service. As per the Act the "relevant product market" means a market comprising all those products or services which are regarded as interchangeable or substitutable by the consumer, by reason of characteristics of the products and services, their prices and intended use. Section 19 (6) and Section 19(7) of the Act provides guidance for the assessment of the relevant geographic market and relevant product market, respectively. All close substitutes to the product/service in question are considered while assessing the relevant product market. While assessing the substitutability, a commonly used test is 'small but significant and non-transitory increase in price' (SSNIP) test. This test starts with taking the narrowest possible relevant market and assessing whether the SSNIP in this hypothetical market would be profitable or whether consumers will switch to other products. In case of latter, the market definition is expanded to include the substitute product to which

[90] Ibid
[91] Schrepel, T. (2018). Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.*SSRN Electronic Journal.* [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576
[92] Ibid

consumers switch to, and the SSNIP test is undertaken again. Thus, the SSNIP test provides a useful framework to assess demand substitutability of different competing alternatives.[93]

In the case of blockchain applications, there are various possible ways in which the relevant market may be defined. The following are some of the possibilities[94]:

- *Each blockchain application as a market (since its ledger would be distinct)*: Such a market definition may be appropriate only when there are no close substitutes to the blockchain application, either in terms of other blockchain applications, non-blockchain technologies or offline substitutes. This is likely to happen in case blockchain applications are leveraged to create new markets that do not currently exist.
- *Blockchains with similar applications as a single market*: Blockchains providing similar applications may be defined as a relevant product market when there are no substitute non-blockchain applications. This is likely to be the case with blockchain applications that create relatively new but similar types of products or services.
- *Relevant market consisting of similar blockchain applications and non-blockchain applications*: The relevant product market can be defined to include similar blockchain applications as well as other similar digital/non-digital substitutes (if any) when they are all close substitutes[95]. This is comparable with online sales and offline sales from brick and mortar stores being considered as part of the same relevant market.

The delineation of a relevant market in case of a blockchain application depends on how the blockchain technology develops in the future and on facts of the case (focusing specifically on the presence/absence of close substitutes to the blockchain application at hand).

Relevant geographic market

As per the Act, "relevant geographic market" means a market comprising the area in which the conditions of competition for the supply of goods or provisions of services or demand of goods and services are distinctly homogenous and can be distinguished from the conditions prevailing in the neighbouring areas. Section 19 (6) of the Act lists down the factors that should be taken into consideration while determining the relevant geographic market.

In the case of blockchains, pseudonymous nature and the ability of the same application to transcendent geographies could add to the complexity of defining the relevant geographic market.

In cases where the identity of the participants of the blockchain and their geographical location is unknown, delineation of the geographical boundaries of the relevant market could become challenging, Pseudonymous nature of the nodes participating in a public, permission-less blockchain can complicate the definition of a relevant geographic market. The relevant geographic market may be relatively less complex to delineate where the identities and locations of the participating nodes are known. While a blockchain application may originate in a particular geography, its application may transcend to other jurisdictions including international jurisdictions. Ultimately, the definition of the relevant geographic market would depend on the specific facts of the case.

Market power

Market power may be assessed on a case-by-case basis based on various possible indicators. One of the key indicators of market power is the market share of a firm. In cases where the relevant product market comprises only blockchain applications, factors such as number of users (or active users), number of recorded transactions, number of blocks, revenue or a combination of these may be relied on to assess the dominance (in addition to any other relevant factors). In instances where the relevant market comprises blockchain applications and non-blockchain based applications, market share could be assessed based on the number of users, number of transactions, revenues, or a combination, thereof.

Another factor that is considered while assessing market power is the presence/absence of barriers to entry. If barriers to entry are low, then market power may be limited. In such a market, an incumbent blockchain application with a high market share may be unable to unilaterally increase its price. Higher price in such a market would imply higher profitability for the incumbent, which would incentivise new players to enter the market. Thus, the resulting competition among the incumbent and the new entrants would drive down the price charged. Conversely, a blockchain application with high barriers of entry could indicate high market power.

A new entry in case of a blockchain can also take the form of forking. The possibility that a forked blockchain may also contain the historical data could increase the effective competition resulting from such entry.

Additionally, while assessing the dominance of blockchain applications, the presence (or absence) of network effects may also be relevant. Network effects refer to a phenomenon wherein an increase in the number of users/participants of a good/service, increases the

[93] Application of the SSNIP test in technology markets where prices are zero can be sometimes challenging. In such cases, it may be advisable to make suitable modifications to the test.

[94] Schrepel, T. (2018). *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.* SSRN Electronic Journal. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576

[95] Ibid.

network's value for the users. It is a well-known fact that network effects in digital markets can result in a firm achieving market strength in the long run. Similar network effects are likely to exist in the case of blockchain applications as well, especially in cases where applications are set up as two-sided marketplaces.

Dominance within a blockchain

Dominance can also emerge within a blockchain when a participant achieves a position of power. This may be observed when entities having an existing dominant position exert their market power in the functioning of a blockchain application. For instance, a large existing entity may sponsor/develop a blockchain application such that its design, governance and terms of participation draw support from the entity.

An example of dominance within a blockchain could be a mining pool that has achieved market power through which the said pool can unilaterally determine which blocks to verify and which should be omitted. While such dominance and its abuse has not yet been observed, the experience from Bitcoin mining shows that there is a possibility of dominance to exist. When Bitcoin was first introduced, a desktop computer was used for mining. However, over the years as Bitcoin became popular and its value rose, the hardware used for mining become complex (from a computer processing unit (CPU) to graphic processing units (GPUs) to field-programmable gate array (FPGA) devices to application specific integrated circuits (ASICs))[96]. China-based Bitmain Technologies which designs ASIC chips and sell mining hardware controlled over 74% of the global market in 2018[97].

Further, the advancements in the hardware used for mining made it difficult for individual miners to be successful. As a result, mining pools (the group of miners who combine their computation power and share the profits in line with each miner contribution) and mining farms (large mining facilities) gained popularity[98]. Thus, competition among miners also reduced. Instead of individual miners competing with each other, miners started collaborating and establishing mining pools and farms. The six largest mining pools in the world, namely, BTC.com, Antpool, ViaBTC, Slushpool, F2pool, and BTC.top, together control over two-third of the total hashing power[99]. Interestingly, Bitmain Technologies fully owns and operates Antpool and BTC.com and is the main investor in ViaBTC. Together, these three mining pools accounted for around 48% of the bitcoin hash rate distribution in September 2018[100].

An example of a blockchain antitrust case

Allegation of collusion before the US District Court for the Southern District of Florida (United American Corp v Bitmain Inc)

- United American Corp offers various blockchain solutions, which rely on the cryptocurrency and Bitcoin cash. In November 2018, when Bitcoin Cash was scheduled for a routine protocols upgrade, there was a disagreement between the protocol developers on the new rules, resulting in a split between the two groups into different forks: Bitcoin ABC and Bitcoin SV. The two forks fought with each other to gather support from the miners for their respective fork, leading to the combined value of the forks dropping below that of Bitcoin cash before it forked. Eventually, Bitcoin ABC gained larger miner buy-in and thus retained the name and ticker of Bitcoin cash.
- United American Corp filed an anti-trust complaint against various investors, mining pools, crypto-exchanges and protocol developers for allegedly colluding to gather maximum support for their Bitcoin ABC fork over Bitcoin SV form. As a result, the market conditions for mining Bitcoin cash were no longer normal, which adversely affected the performance of United American Corp's investments.

Given that the consensus mechanism is central to a blockchain application, abuse of dominance by a miner within a blockchain can have a potential adverse effect on the competition. Any abuse of dominance within or by a blockchain application would be a contravention of Section 4 of the Act.

Box 7: Issues for further deliberation (Part 4)

11. Under what conditions should blockchain applications and non-blockchain applications providing the same service be considered a part of the same relevant product market?
12. How should relevant geographic markets be delineated in the case of permission-less blockchains?
13. What factors can be considered to determine the dominance withina blockchain?
14. How would the possibility of forking of a blockchain affect the assessment of dominance?
15. Are network effects present in the case of blockchain applications?
16. What are the different possible barriers to entry from the perspective of a blockchain application?

[96]Supra note 89.
[97]Corporate capture of blockchain governance: The next big antitrust issue? (2019) (online) Available at: http://www.aei.org/publication/corporate-capture-of-blockchain-governance-the-next-big-antitrust-issue/
[98]Supra note 89.
[99] Ibid
[100] Corporate capture of blockchain governance: The next big antitrust issue? (2019) (online) Available at: http://www.aei.org/publication/corporate-capture-of-blockchain-governance-the-next-big-antitrust-issue/

17. Can entities such as developers, miners or users gain dominance in a blockchain? Are there specific conditions when such outcomes are more likely?
18. How can the risk of already dominant entities exerting their market power in development of a blockchain application, such as in terms of its design, governance rules, and terms of participation be mitigated?

6.3.2 Abusive conduct

It is possible that in the future, a blockchain application may gain market power and be in a position of dominance in the relevant market under consideration. Such dominance is not an issue according to competition law principles. However, any direct or indirect abuse of the dominant position is a contravention of Section 4 of the Act.

Refusal to provide access to a permissioned blockchain

One common form of exclusionary abuse of dominance is refusing access to a market. The key question that needs to be assessed in such cases is – when can the denial of access by a blockchain application raise competition concerns?

Access to blockchain applications may be restricted for a variety of economic and technical reasons. This restriction may raise competition issues if the blockchain itself is deemed to be an essential facility and if the refusal to access is unjustified. A traditional example of an essential facility is a bridge on a river that is the only way to access consumers on the other side. If it is controlled by a competitor which denies access to that bridge to other competitors, it may harm competition. However, infrastructure may be considered an essential facility only if it is not easily replicable and its access is essential for entities to operate and compete in the market. Further, a competition authority may also assess if such restrictions incentivise greater technological innovation and investment in blockchain applications which has a pro-competitive effect in the longer run. Regulatory interventions are warranted only when likely anti-competitive effects outweigh the pro-competitive effects.

A blockchain application could become an essential facility in case its historical data on the ledger needs to be accessed as an important input for a business operation. The French and German competition authorities recognise that data can be an essential facility. Their joint paper on Competition Law and Data, states, "*Refusal to access to data can be anticompetitive if the data are an "essential facility" to the activity of the undertaking asking for access*"[101]. Hypothetically, a blockchain application could be developed for recording regular data from IoT devices installed in cars. This data could be, used by insurance providers to determine the car insurance premium based on the risk profiles developed from the historical data. If a new insurance company is denied access to this hypothetical blockchain application, it is possible that it may not be able to compete effectively in the market (unless there is an alternate way – even if it is costly – for the new entrant to generate similar data). Thus, access to an incumbent's blockchain application may not be deemed "essential" just because the cost of entry is very high, rather only it may be so only if there is no other way for a new entrant to compete in the market.

The French and German competition authorities also recognise that the refusal to access data may be held to be anti-competitive only if it can be demonstrated that the data is "*truly unique and that there is no possibility for the competitor to obtain it to perform its services*"[102]. In such cases, the incumbent may be required to provide the new entrant with access to the blockchain application on fair, reasonable and non-discriminatory terms. However, while doing so, the investments made, and risks borne by the incumbent would be taken into consideration. If due regard is not given to the incumbent's investment and risk, it may discourage innovation and investment in R&D related to blockchain technology.

Further, refusal to provide access can also be indirect. For instance, consider a scenario wherein a group of competitors set-up and promote a blockchain application to which membership is open to all, but has a relatively high membership cost. The high cost may make it difficult for small competitors to compete in the market. The competition analysis would assess if this is a case of anti-competitive cost-raising strategy or a natural market outcome.

Thus, competition assessment in such cases focusses on assessing whether the refusal to provide access (directly or indirectly) was aimed at excluding a new entrant (or competitor) or whether there were other rational economic or technical justifications for the same. For instance, if the entity seeking access to the blockchain application does not have the necessary cyber security measures in place, then the restriction to access may be justified.

Refusal to provide access to industry standards

Denial of access in the case of blockchains could also emerge with respect to access to industry technical standards established for blockchains. The Organisation for Economic Cooperation and Development (OECD) recognised the "*need for a technical standard for interoperability to be defined by a standard setting organisation so that blockchains used by different firms can interact with one*

[101] Competition Law and Data. (2016). [online] Available at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf
[102] ibid

another"[103]. Much like businesses that rely on standard setting to ensure the compatibility and interoperability of their technologies, companies using similar blockchain applications may develop common technical standards[104].

It is believed that future standardisation in this area can boost their development and provide them with international standards, stimulating greater interoperability and enhanced innovation. In a survey of governments, industry, academia and consumer organisations undertaken by the International Standards Organisation (ISO), "*more than 88% of respondents indicate a role for standards in supporting the roll out of blockchain technology*"[105].

Globally, various initiatives are underway towards establishing common industry standards.

- In 2016, ISO formed ISO/TC/307, which is focused on the standardisation of blockchain and distributed ledger technologies[106]. The group has several focus areas including architecture and taxonomy, use cases, security and privacy, identity, smart contracts, governance and interoperability between blockchains.
- IEEE Standards Association (IEEE-SA), a globally recognised standards-setting body, has also been actively pursuing blockchain standardisation efforts through various activities in multiple industries and sectors, including the launch of the world's first virtual blockchain workshop.
- World Wide Web Consortium (W3C), which played a crucial role in the early days of the internet in standardising the functionality of web browsers, has a Blockchain Community Group which is working on a Web Ledger Protocol and have published a draft which covers "an extensible data model and syntax for expressing cryptographic ledgers and a protocol for reading and writing to ledgers[107]".

In the long run, as blockchains establish themselves, coordination among blockchain members to adopt common technical standards may be required to ensure interoperability and long-term benefits to the economy as a whole. This could play a vital role in ensuring competitiveness and encouraging innovation.

However, while setting standards, it is possible that a dominant firm includes its patented technology as a part of the standards, but it may then refuse to provide its competitors access to the technology. Unless reasonably justified, the firm's refusal to provide access to set standards on fair, reasonable, and non-discriminatory terms (FRAND) terms may be considered to be anti-competitive.

Other anti-competitive abuse of dominance

In addition to the refusal of access, a dominant position can be abused by undertaking other forms of anti-competitive conduct such as bundling, predation, discrimination and leveraging. As with any other allegation of abuse of dominance, a case-by-case analysis may be adopted in the case of blockchain applications as well. The alleged anti-competitive conduct may not always be aimed at restricting competition in the market, it may be introduced keeping other economic or technical objectives, such as security measures, in mind. Every case would be assessed in accordance with the relevant provisions of the Act and depending on the nature of allegation appropriate analysis would be undertaken.

The following are some other potential forms of anti-competitive abuse.

Inclusion of unjustified conditions

Anti-competitive conduct by a dominant entity can include unjustified and unrelated conditions for its primary contract. For instance, a dominant blockchain application may engage in anti-competitive conduct by bundling together access to its blockchain application withusing a specific digital wallet, so that the users of its application do not have the choice of using any other wallet service.

A case-by-case analysis may be required in case of such allegations, taking into consideration the application's basic features, objective and conduct as well as justifications for the conduct.

Predation

A dominant firm may also abuse its dominance by engaging in predation. There are two forms of predation:

[103] Directorate For Financial and Enterprise Affairs Competition Committee, OECD. (2018). Blockchain Technology and Competition Policy-Issues paper by the Secretariat. [online] Available at: https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf
[104] FinTech Weekly (2018). *Blockchain, Antitrust, and Standard Setting*. [online] Medium. Available at: https://medium.com/fintech-weekly-magazine/blockchain-antitrust-and-standard-setting-3c737c03c186
[105]Standards Australia. (2017). *Roadmap for Blockchain Standards.* [online] Available at: https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx
[106] ISO. (2019). *ISO/TC 307 - Blockchain and distributed ledger technologies*. [online] Available at: https://www.iso.org/committee/6266604.html
[107] Github.io. (2009). *The Web Ledger Protocol 1.0.* [online] Available at: https://w3c.github.io/web-ledger/

- **Predatory innovation**: A dominant firm may undertake innovation or technical changes not for the benefit of its consumers, but to eliminate the competition. Predation innovation can be implemented swiftly and at no cost either by directly denying access or by restricting their ability to read, submit or verify transactions[108].
- **Predatory pricing**: Another predation strategy that may be adopted by a dominant firm is to reduce transaction fee below cost so that the competitors exit from the market. Once the competitor(s) exit the market, the dominant firm will increase its price and earn high profits, enabling it to recoup the loss incurred by pricing below cost. For instance, a dominant blockchain may significantly reduce its transaction fee to eliminate a competing blockchain from the market and then increase the fee after the competitor exits.

Predatory conduct would be assessed in accordance with the relevant provisions of of the Act. The Act defines predatory price as *"the sale of goods or provision of services, at a. price which is below the cost, as may be determined by regulations, of production of the goods or provision of services, with a view to reduce competition or eliminate the competitors"*

Discrimination

Discrimination refers to the practice of imposing different conditions on similar transactions with distinct entities, resulting in the firm subject to unfavorable conditions being at a competitive disadvantage. One of the most common discriminatory practices is price discrimination, wherein different buyers pay different prices for purchasing a similar volume of the same product or service. In the case of blockchain applications, this could also take the form of the governance mechanism being designed such that it discriminates against its members in terms of the time taken to verify their transaction and/or adding them to the blockchain. This is less likely in a case of a blockchain where transactions are verified by POW consensus since miners compete with each other to verify transactions and earn the transaction fee (or token currency).

Allegations of discriminatory pricing would be assessed in accordance with the relevant provisions of the Act.

Leveraging

A dominant entity may adversely affect competition by leveraging its position of market power in one market to enter/strengthen its position in another market. Leveraging can take various forms. For instance, a dominant blockchain application may increase the transaction fee it charges and use the higher revenue to provide wallet service at a lower cost, thereby driving out competitors from the market.

A case-by-case analysis based on the features and conduct of the blockchain application may be undertaken while assessing allegations of such conduct.

Abuse of dominance is possible with both permissioned and permission-less blockchains. However, in the case of public permission-less blockchains, such conduct may be possible only if the governance rules are designed to facilitate such conduct. This might require coordination and consensus among the nodes. The ability to engage in such conduct in a blockchain application is thus dependent on the governance rules, including how easy it is to make changes to the governance[109]. Changes in governance may be made much more easily in a permissioned consortium blockchain vis-à-vis a permission-less public blockchain.

Blockchain antitrust case example

Anti-competitive leveraging complaint before the Australian Competition and Consumer Commission (ACCC)

- Australian Securities Exchange (ASX) recently announced its plan to adopt a blockchain ledger as a replacement for its clearing and settlement system. In the present system, there is a clear demarcation between ASX's role as the licensed market operator who makes the rules, roles and functions of other service providers such as share registries.
- However, it is alleged that the new system is not a simple and technical system upgrade, instead it will reconfigure the services provided by various market players such that ASX will undertake the roles and functions presently provided by the competing share registries.
- The allegation against ASX is that introducing a blockchain with the objective of extending its reach and taking over some of the functions currently provided by the share registries, will adversely affect competition in the market.

Box 8: Issues for further deliberation (Part 5)

19. In a permissioned consortium blockchain what could be the economic/technical justifications for not allowing access to the blockchain? Would such justifications outweigh the potential anti-competitive effects of such refusal?
20. Under what conditions should blockchains be considered as an essential facility?
21. How can standardisation of blockchain technology affect competition and what measures can be taken to address anti-competitive conduct resulting from such standards?

[108] Ibid
[109] Ibid

22. What is the likelihood of bundling/predation/discrimination/leveraging by a dominant blockchain?

6.4 How can a blockchain facilitate the implementation of competition law?

One of the key features of a blockchain is that it is distributed, immutable and a secure ledger. This attribute may assist competition authorities towards enforcement of the competition law.

A major challenge usually faced by competition authorities while investigating allegations of anti-competitive conduct is the paucity of information and data to provide the necessary evidence. Often the data procured from the parties to conduct an investigation is not verifiable from a third-party source. However, in blockchain applications, the necessary information could be obtained by viewing the ledger of the blockchain application (which have been verified and cannot be altered). For instance, if there is an allegation that competing firms using a blockchain application have cartelised, then by accessing the transaction information on the blockchain, it is possible to analyze the data to determine whether there is economic evidence of collusion or not. Similarly, data from a blockchain application may also facilitate with an assessment of how a proposed combination of firms (merger, acquisition, or joint venture) is likely to influence the competition.

However, the ability to analyze data from a blockchain comes with certain challenges. In the case of public blockchains, some data could be encrypted and pseudonymous, while in the case of permissioned consortium blockchains, there exists a possibility to access the data on the blockchain.

Further, under the leniency programs, in the case of blockchains, the firm making the leniency application may be able to use the blockchain application itself to collect and provide extensive information to assist the competition authorities in their investigation. For instance, if a cartel among the firms in a blockchain application exists that shares competition-sensitive information amongst each other, one of the cartel members can file for leniency and support the competition authorities by providing the data available from the blockchain application.

Finally, blockchains may also improve competition law enforcement through the use of smart contracts, specifically, to ensure that a firm complies with the commitments it has proposed and which the competition authority has accepted. A smart contract can be introduced within the blockchain in which the firm participates to self-enforce adherence to the conditions of the commitment. For instance, if a firm commits that it will not raise its price by more than 10% in a year to ensure compliance, the competition authority can introduce a smart contract that permits the sale by the entity only if the price increase is not more than 10% of the price charged in the previous year. This might significantly save cost and effort that would have otherwise been incurred in monitoring the compliance to the commitment.

Box 9: Issues for further deliberation (Part 6)

23. How can the data from a public blockchain be used for competition investigations where it is encrypted or pseudonymous?
24. How can different governance mechanism of blockchain applications influence the effectiveness of the leniency program?
25. Would the use of smart contracts by competition authorities to monitor commitments improve enforcement?

7. Suggestions for stakeholders while assessing competition compliance

Based on the discussed in the previous sections, the following are some broad-level guidance for various stakeholders in a blockchain ecosystem (who, *inter alia*, include technology developers, blockchain platforms, wallets, miners, exchanges, mining hardware manufacturers and users):

- Blockchain stakeholders should be mindful of the provisions of the Act while participating in a blockchain.
- Blockchain applications should not be used to exchange competition-sensitive information among competitors. This includes recent data on prices, cost or output information of competitors.
- Blockchain or smart contracts should not be designed to enable enforcement of any collusive (including imposing punishment in case of deviation from collusive agreement) or anti-competitive conduct of any form.
- Stakeholders need to be mindful of the provisions related to Section 3(4) of the Act while creating any smart contract or blockchain application between parties that are part of a production chain, such that these do not result in or are likely to result in appreciable adverse effect on competition.
- Any enterprise operating or participating in a blockchain, which is in a position of dominance (as defined in Section 4 of the Act), should avoid potentially anti-competitive behaviour such as fixing unfair or discriminatory prices or conditions or provision of services, limiting or restricting production/development of goods or services or denial of market access of goods or services.
- While designing the governance mechanisms of a blockchain, consideration should be made for the possible changes in compliance relating to any requests or orders issued by CCI.

A more detailed guidance on the competition compliant conduct for enterprises (also applicable to blockchain stakeholders) is available in the Compliance Manual by CCI[110].

[110]CCI (2017, May). Compliance Manual for Enterprises. Available at: https://www.cci.gov.in/sites/default/files/manual_compliance/manual_booklet.pdf

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

EYIN1912-006

ED None