# Blockchain Technology and its Industry Adoption

**March 2021**

IAMAI
Internet And Mobile Association Of India

EY
Building a better working world

# Contents



# 01 Introduction

# Introduction

One of the reasons for the enthusiasm around blockchain[1] technology[2] is the impact that it can have on currencies, record keeping, sharing of information, contracting and creating individual identities. This technology has been brought about by progress in the fields of cryptography, computing, economics and law. While some argue that blockchain technology is as transformational as capitalism[3] and could change the way governments function;[4] others speculate that this technology may end with a whimper rather than a big bang.[5] These are still early days and one cannot be certain whether blockchains will live up to the expectation, but the technology does have its advantages.

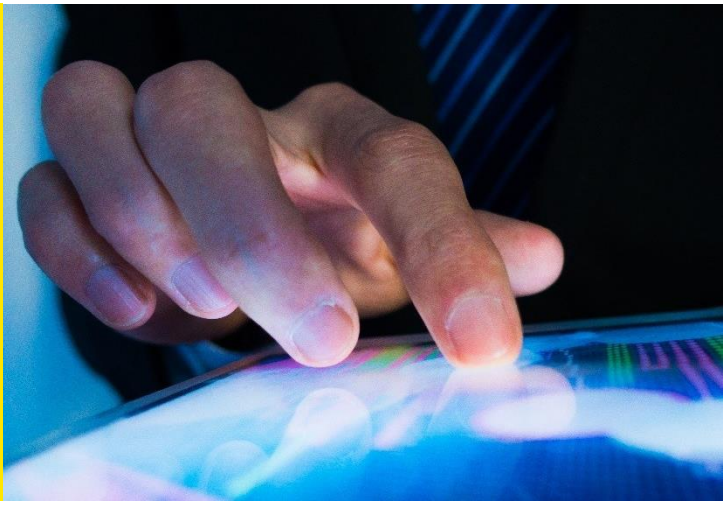
Before describing what a blockchain is, how it functions, the different types of blockchains, their features, and their evolution, it is important to first discuss how the world functions without blockchain technology. Presently, intermediaries mediate between the different entities and institutions wishing to enter into a transaction by providing the necessary trust to the involved parties. One could think of banks, credit card companies, or e-commerce platforms as intermediaries that resolve the issue of lack of trust between two transacting parties—buyers and sellers. These entities act as counterparty to each side, maintain a centralized database/ledger of all the transactions, facilitate sharing of information, and validate their identity. They act as the channel through which transacting parties go through to transact with an unknown entity/ individual and in return charge fees for this service provided by them.

Blockchain, theoretically, removes the need for such intermediaries as validators of trust and identity and support transactions between two entities without a third-party intermediary. Since trust is most essential in financial transactions, participants can exercise much more control[6] over the transaction and do not have to rely on such intermediaries.

## Please note

In January 2021, Ministry of Electronics and Information Technology has released draft National Strategy on Blockchain. Please refer the same in the low link.

https://www.meity.gov.in/writereaddata/files/NationalStrategyBCT_%20Jan2021_final.pdf



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

[2] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

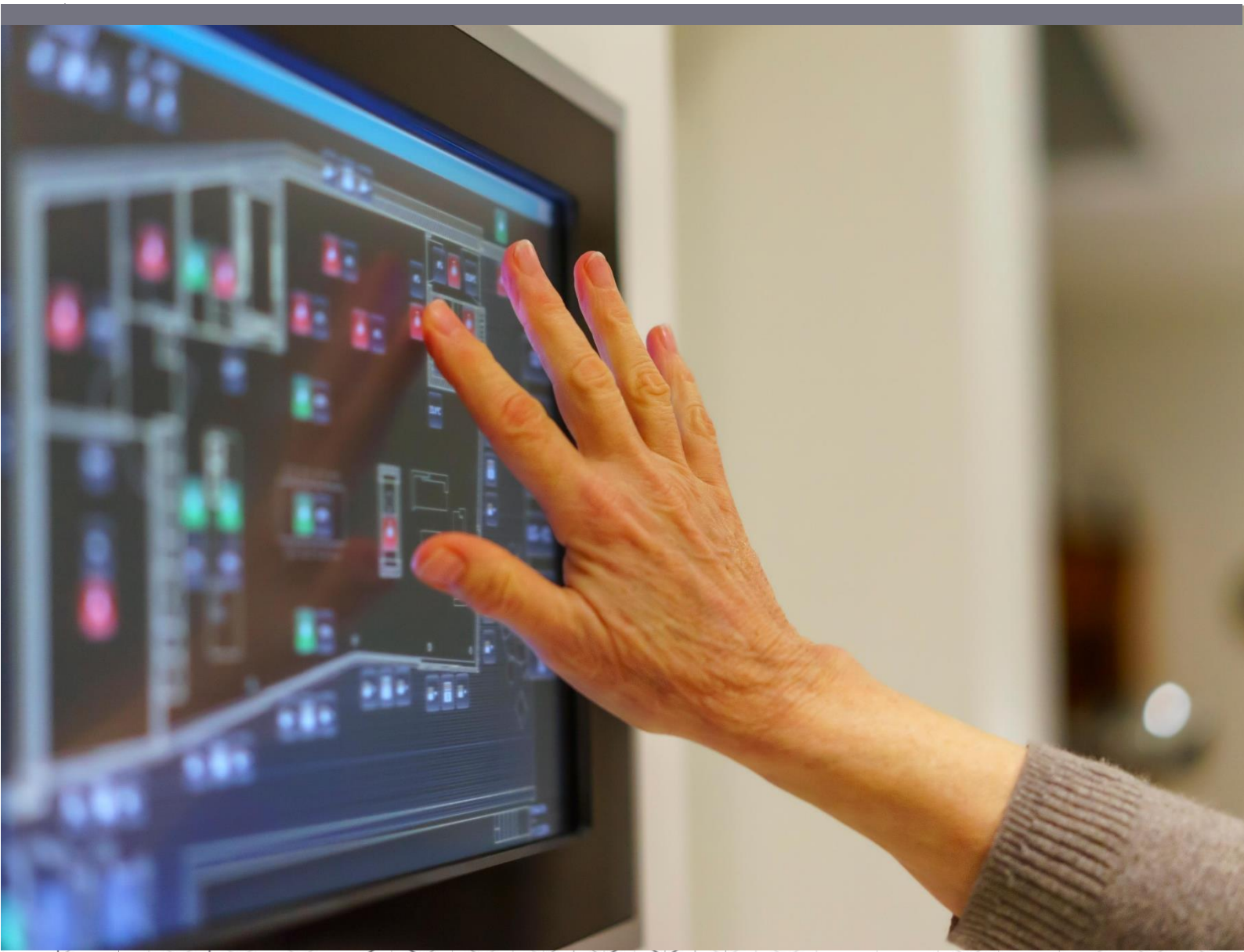
[3] Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain. Available at SSRN 2744751.

[4] https://medium.com/@glenweyl/a-radicalxchange-between-vitalik-buterin-and-glen-weyl-328d8ad088cf

[5] https://www.bloomberg.com/features/bitcoin-bulls-bears/. Most of the criticisms are centered around the Bitcoin- the most popular blockchain application

[6] https://taylorpearson.me/fat-thin/

# 02 Background



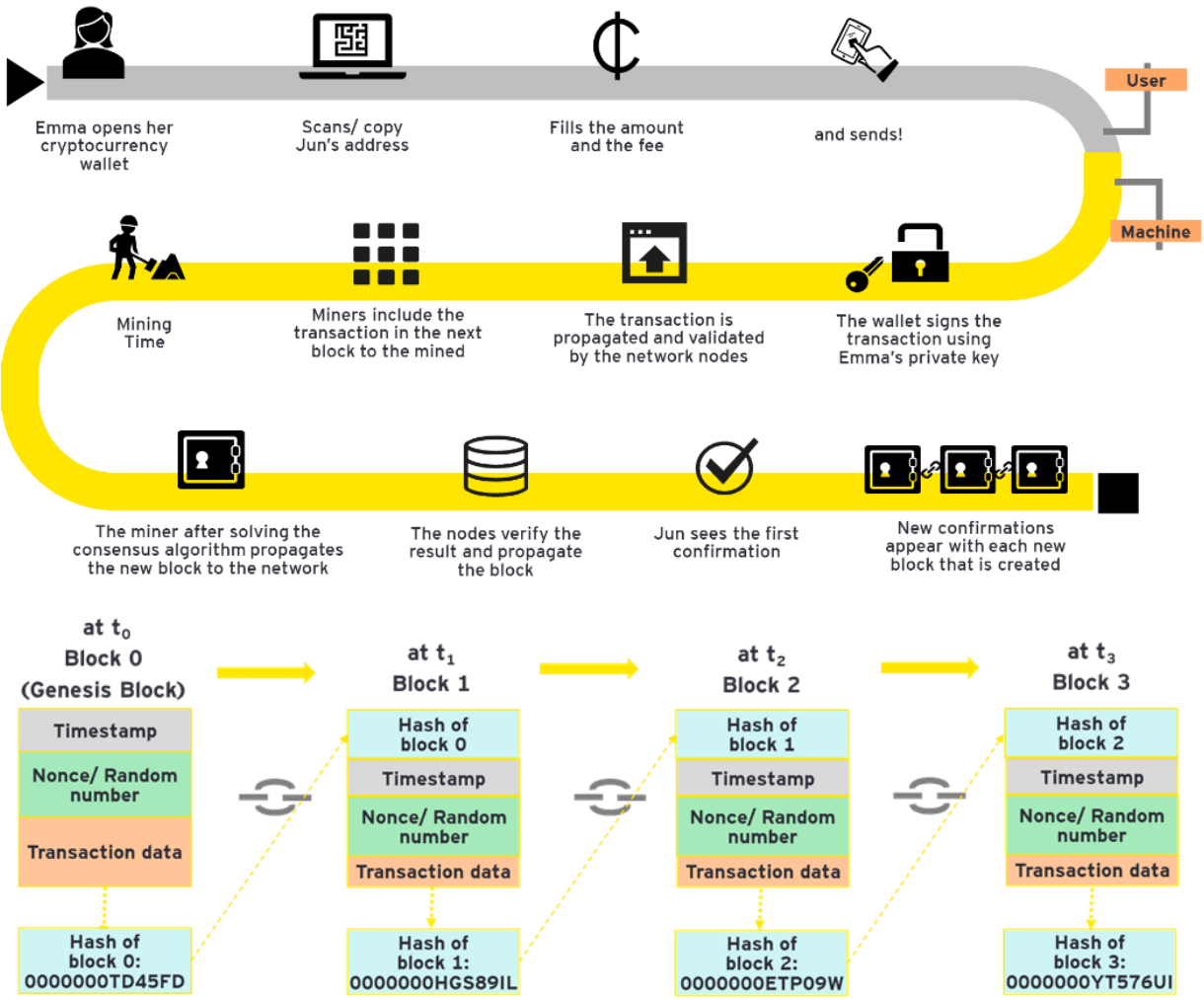
# Background

## 2.1 What is a blockchain?

Blockchain has been heralded as the next stage in the evolution of the Internet. If the current Internet is a network for the exchange of information then the Internet with blockchains can be thought of as a means for the exchange of value.[7]

In simple terms, a blockchain is a chain[8] consisting of information on various blocks (transactions) strung together sequentially. This chain maintains a record (or ledger) of the transactions taking place between the different users of the blockchain with each node[9] (computer connected to the network). This creates a ledger that is decentralized, distributed, immutable and secure, without the need for a centralized intermediary.

**Figure 1: Under the hood of a blockchain**




*Source: https://www.bambora.com/en/ca/blog/bitcoin-explained/*

[7] Currently, walled gardens have to be created on top of the internet layer for creating verifiable online identity and exchange of value

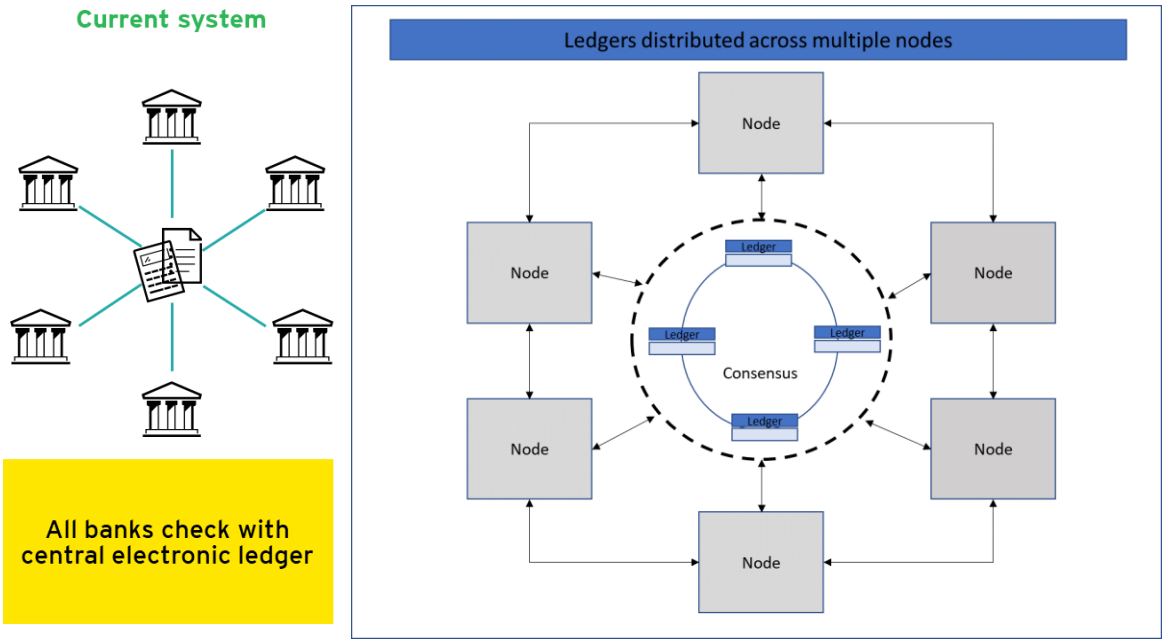
[8] It is a software construct in the realm of bits. See Box 1 for further details

[9] Individual/entity/computing machine on a network

**To illustrate how a blockchain[10] works, we consider the case of Bitcoin:**

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 transaction signatures get pooled together in a repository.
2. In the case of a centralized database, a neutral intermediary verifies these transactions and updates the database with the record of new transactions and the balances of different nodes. However, in blockchains such as Bitcoin, the process of ledger updating is done in a decentralized fashion. All the nodes on the blockchain network have a copy of the ledger available with them at a given point in time. A subset of nodes on the blockchain– miners/validators– run the validation process called mining.

**Figure 2: Difference between Centralized System and Blockchain**




*Source: Financial Times*

3. The process of updating the ledger/database is run at regular intervals of time. The validators select the pool of transactions they want to include in the next block. Following pieces are required for running the updating process: -
   a. Hash function. It is a mathematical algorithm that takes input data and outputs a string (hash) of a pre-specified length. This function is very sensitive to the input message and even a minor change in the input message can completely change the output hash. It is next to impossible to guess the input from the output. This feature acts as the key security mechanism in blockchains.
   b. Hash of the previous block.
   c. Signatures of the various transactions to be validated.
   d. A random number generator for Nonce.[11]
4. No node has prior knowledge of the exact hash value which the hash function will output. However, certain attributes such as the length of the prefix 0s of the hash output are known to all the nodes. In the case of Bitcoin, for instance, through a brute computation[12] process, different miners compete to produce an output hash-- with the desired 0s length by changing the Nonce repeatedly. There is an inbuilt incentive mechanism

[10] The algorithm is for public permissionless application like Bitcoin. The other types of blockchain mechanisms have similar and simpler algorithms

[11] Jargon for a random number

[12] This is the Proof of Work (PoW) consensus mechanism. Other consensus mechanisms like Proof of Stake (PoS) are similar but are not inefficient in terms of computation and energy spent to achieve consensus. See Box 1 for further details.

to encourage this computation, and energy-intensive process –miners collect a transaction fee[13] from the nodes whose transactions get committed to the block.

5. The miner who discovers the desired hash first broadcasts the necessary information required to check the veracity of the hash first. Once the other nodes agree on the value of the hash calculated by the miner, a consensus has been reached. Then as the other nodes have verified the hash output, a new block is created, and it is linked to the previous block on the blockchain. Once committed, it is almost impossible to change the content of blockchain. This process is called committing a block on the blockchain.
6. The process from step 3 is repeated again for mining the next block with a new set of transactions from the repository.

As this process illustrates, a blockchain can be defined as a decentralized, distributed, immutable, secure database[14] technology.

**Decentralized**

The process of adding a new block to the database/ledger is governed by a consensus protocol[15](See Box 1) 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 decentralized 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. This creates redundancy in the network and provides security against record falsification. Specifically, any attempt to corrupt the network (by a hacker for instance) will have to alter the data stored on the majority of the nodes in the network.

**Immutable**

Once an entry has been added to a blockchain, it is nearly impossible to edit, update, or delete it. This makes a blockchain an almost permanent and unalterable record of the history of transactions.

**Trustless**

The process of adding a block to the database involves cryptography (a mathematical algorithm to encode information for security purposes) and economic mechanisms which do not require trusting the other nodes involved on the network. This is the emergent property of maintaining a distributed and decentralized database along with the consensus mechanism involved. Not requiring trusting the other nodes involved creates an opportunity to transact and interact without worrying about the risk of fraud and cheating.

### 2.1.1 Main consensus mechanisms in permission-less and permissioned blockchains

Blockchain applications may use various consensus algorithms to authenticate the inclusion of a new block into the blockchain ledger. Permission-less algorithms need more rigorous processes as they are open to a commit by anyone on the blockchain. The two most popular mechanisms currently in use are: -

- **Proof of work:** The legitimacy of a 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, computer hardware and storage space required. Section 2 explains this mechanism in detail. The challenge with this mechanism that it is seen as energy inefficient and not easily scalable because of the large time periods required to solve the hash functions. Both Bitcoin and Ethereum use this consensus mechanism.
- **Proof of stake:** In the beginning, any node wanting to be the validators can stake its assets (currency token of the platform) as collateral for being considered and appointed the validator. There are two main mechanisms for choosing validators and achieving consensus: -
- Chain-based proof of stake, the algorithm randomly selects a validator during each time slot and assigns that validator the right to create a single block. This block must build on a previous block (normally the block at the end of the previously longest chain), and so that over time most blocks converge into a single constantly growing chain. **Example: Peercoin, Ethereum Casper**

[13] In case of Bitcoin, the miner/validator/supernode/miner gets a newly minted bitcoin as well

[14] Database is a systematic collection of data, usually stored in a computer for future retrieval and manipulation.

[15] Computer algorithm where all the nodes decide whether to add a new row to the database or not after verification

- In Byzantine Fault Tolerance (BFT)[16]-style proof of stake, validators are randomly assigned the right to propose blocks, but agreeing on which block is final is done through a multi-round process where every validator sends a "vote" for some specific block during each round, and at the end of the process all (honest and online) validators permanently agree on whether or not any given block is part of the chain. **Example: Hedera**

| | Proof of Work | Proof of Stake |
|---|---|---|
| **Participants** | Called Miners, open to everyone on the network | Called forgers, the validator is chosen based on the amount of stake given as a collateral |
| **Requirements** | Requires burning an external resource (mining hardware, power) | Requires high stake in the cryptocurrency |
| **Validation Process** | All miners compete with each other to solve a cryptographic puzzle to validate the transaction | Set validators participate in a consensus algorithm to vote on the next block to be forged |
| **Energy Cost** | Higher | Lower |
| **Mining Power** | With more computing power | With more stake in cryptocurrency |
| **Mining Process Centralization** | Higher | Lower |
| **Reward** | Cryptocurrency + Transaction fees | Transaction fees |
| **Censorship Resistance** | Higher | Lower |
| **Ease of implementation** | Easy | Difficult |
| **Safety** | Lower | Higher |

The permissioned blockchain applications can use relatively simpler consensus algorithms. Easy scalability and implementation have made private permissioned blockchains popular for the public permission-less Blockchain applications. Coming together of a group of entities and the private nature of the blockchain application requires the pre-existence of trust between them. Therefore, consensus algorithms are simpler in this case.

Other consensus mechanisms 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. **Example: 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). **Example: MultiChain**
- **Proof of elapsed time**: A secure hardware time source sends generates random wait times 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. **Example: Hyperledger Sawtooth**

[16]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: GeeksforGeeks. (2019). *practical Byzantine Fault Tolerance(pBFT) - GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/ [Accessed 30 Aug. 2019]

## 2.2 Main types of blockchains

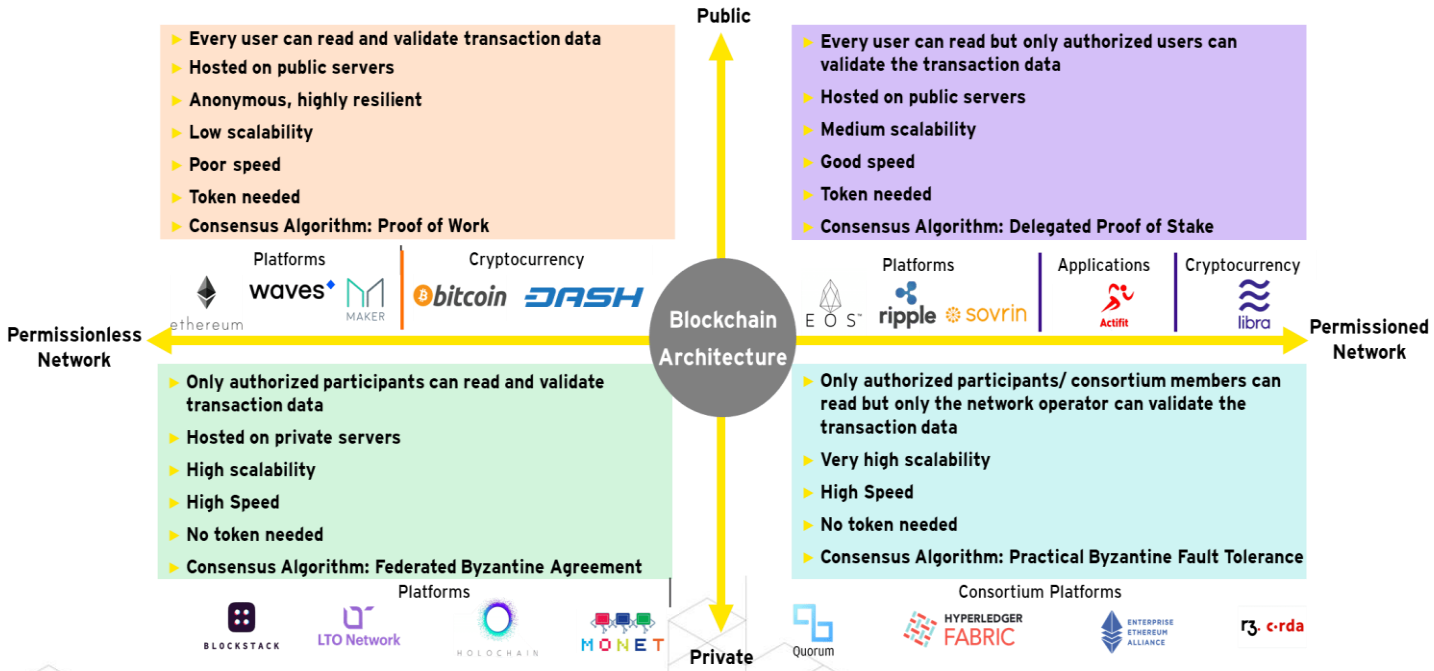
There are two main dimensions in which blockchains can be segregated. These two dimensions are:

i. Who has the access to read the information stored on the blockchain? Anyone can access the information on the public blockchain. If only an individual entity or a consortium of entities can access the information on the blockchain, then is classified as a private blockchain.

ii. Who has the access to write (submit transactions)/ validate (mine) blocks on the blockchain? If anyone in the public can submit and validate transactions, the blockchain is referred to as a permission-less blockchain. On the other hand, if it is authorization is required to submit and validate transactions, the blockchain is referred to as a permissioned blockchain.

Therefore, there are 4 principal categories of blockchains—public permissioned, public permission-less, private permissioned and private permission-less. Their usage depends on the needs of the participants and the use case. Figure 3 below shows the different aspects related to these 4 types of blockchains. Figure YY also provides the names of blockchain applications based on these 4 types.

**Figure 3: Comparison of four types of blockchains**




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

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

**Blockchain-as-a-Service**

Blockchain-as-a-Service, or BaaS, is a managed blockchain platform allowing buyers to build blockchain applications and digital services on a distributed network while the vendor supplies infrastructure and blockchain building tools.

BaaS helps organizations develop and host blockchain apps and smart contracts in a blockchain ecosystem that is managed and administered by cloud-based BaaS service providers.

Blockchain-as-a-Service has been effective in providing the service efficiently and at a reduced cost with the transparency that the business needs. For organizations pairing cloud services with BaaS could be enormously valuable. The personalized flexibility of BaaS technology allows businesses to combat pain points by tailoring integrations. Whether it is acting as a smart contracts platform for a real estate company or a payment processing service for a retailer, BaaS is making waves across a variety of industries.

**The key BaaS service providers are;**

- IBM Blockchain Platform
- Oracle Blockchain Cloud
- EY Blockchain Cloud
- Kaleido
- Azure Blockchain Service of Microsoft
- Hyperledger Fabric
- Factom Harmony
- Dragonchain
- Amazon Managed Blockchain
- NexLedger
- Corda
- Rubix
- HPE Mission-Critical DLT
- Magic FinServ
- Crypto APIs
- ISG Blockchain Now
- Alibaba Cloud Blockchain as a Service (BaaS)
- Mitosis Technologies
- MultiBaas
- Hyland Credentials
- akaChain
- VMware Blockchain
- Aurachain
- ECOS

**Source :** https://www.trustradius.com/blockchain-as-a-service-baas

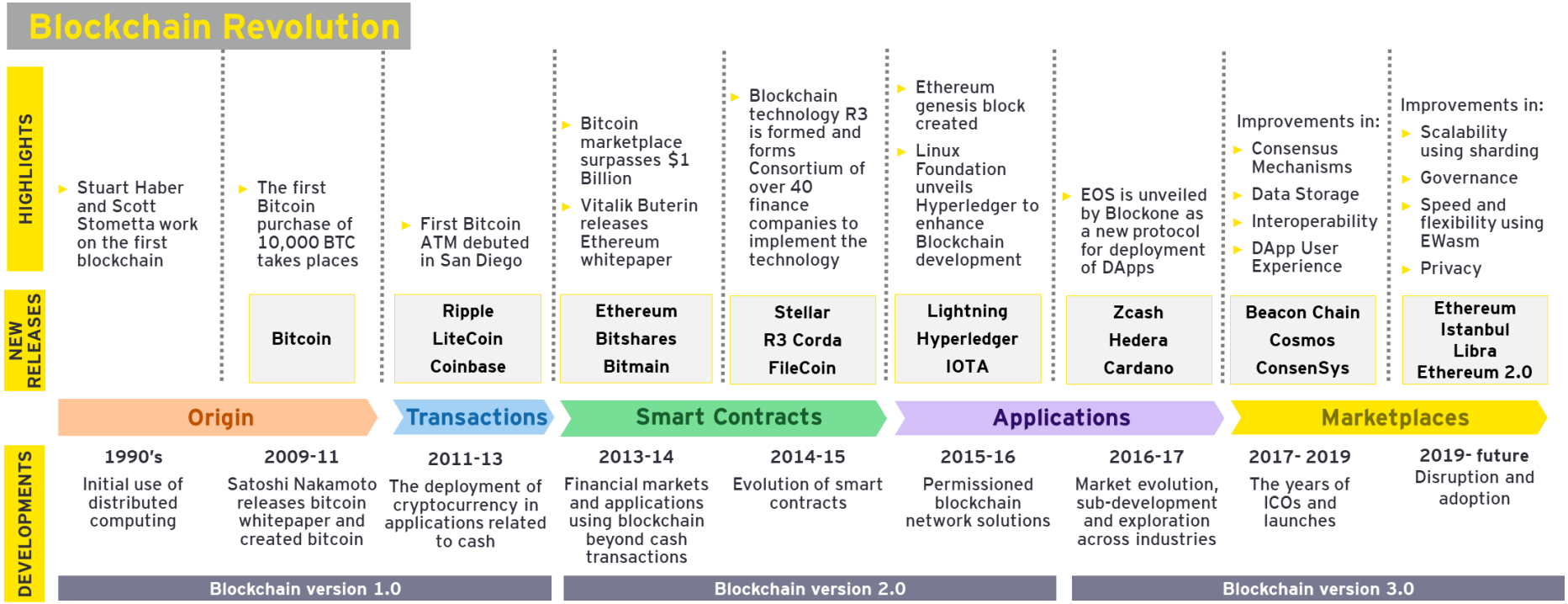
**https://builtin.com/blockchain/blockchain-as-a-service-companies**

## 2.3 History of blockchains

As blockchain applications are growing stakeholders are realizing lacunas in the blockchain architecture. Developers have been focusing on building the required tools and platforms. The parallels between the development of blockchains and the internet are very similar. The internet layer by itself was not end-user centric and required the building of web browsers, website hosting platforms and services, search engines, application development tools so that other developers could develop services like social networks, ride-hailing applications, and video platforms. A similar dynamic is at play with blockchains . Developers have been working on the very basic plumbing of blockchain technologies which can help in the creation of new application and services.

Figure 4 highlights the structural developments of blockchains over time. Blockchain version 1.0 was of Bitcoin and the basic tools around it. Most of the applications were centred around financial applications of Bitcoin and helping user transact in Bitcoin. This changed with the advent of Blockchain version 2.0, which saw the emergence of Ethereum andsmart contracts , building the tools which the developers themselves needed to build consumer-focused applications. It also saw proto-app developments as a proof-of-concept which only served the purpose of identifying gaps in the tools required to do further developments of apps that can compete with centralized walled gardens on the Internet. Blockchain 2.0 also saw the development of private blockchain tools such as Hyperledger. Blockchain version 3.0 is trying to solve the problem of scalability, identity and creating tools for the developers. It is also seeing changes at the base level with Ethereum's decision to move from PoW to PoS.

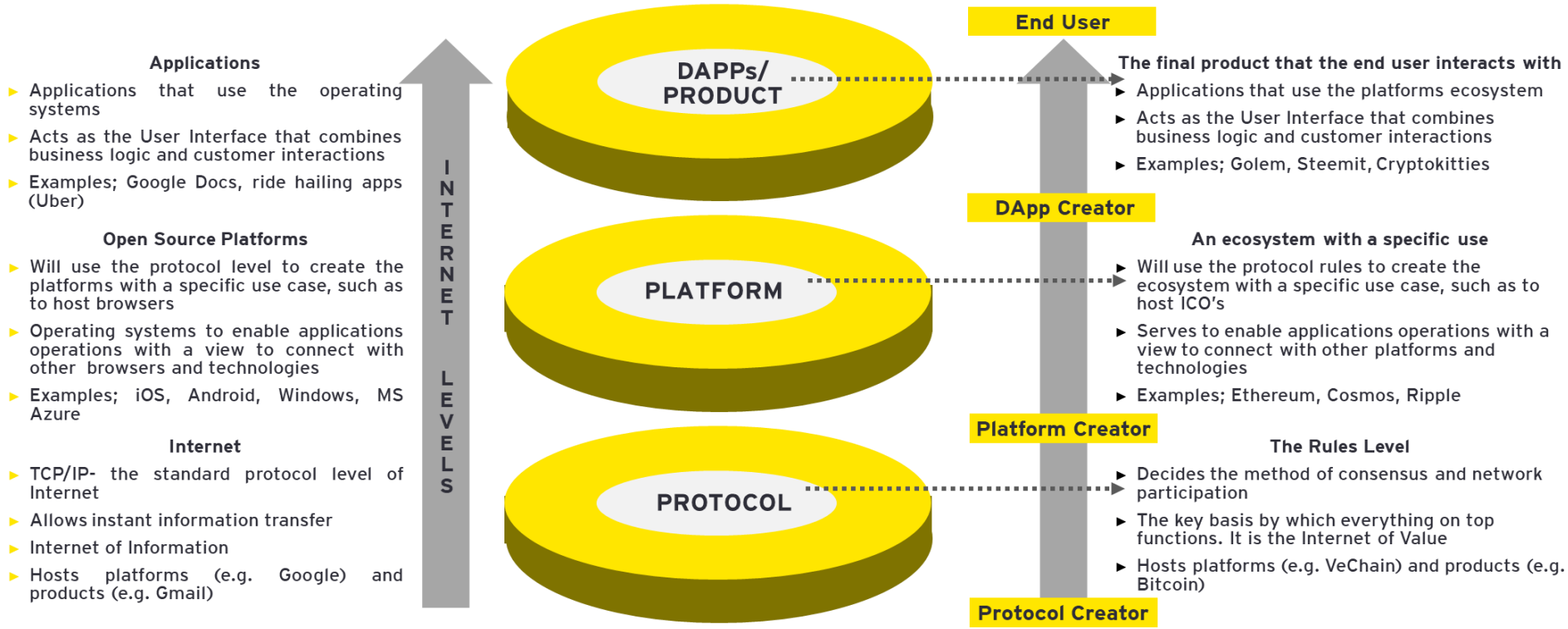
**Figure 4: Blockchain structural developments**




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

Figure 5 below shows the structural evolution in the blockchain technology space. The structural evolution in blockchain can be viewed on three levels. Level 0 as the base layer of blockchain technology akin to the Internet and the web. Level 1 as the platforms and tools which need to be developed to leverage the full power of blockchains. Ethereum being the primary example of this level. Level 2 as the customer-facing decentralized applications (DApps) and smart contracts. Figure 5 highlights the details further with comparison to the Internet.

Figure 5: Blockchain structural evolution



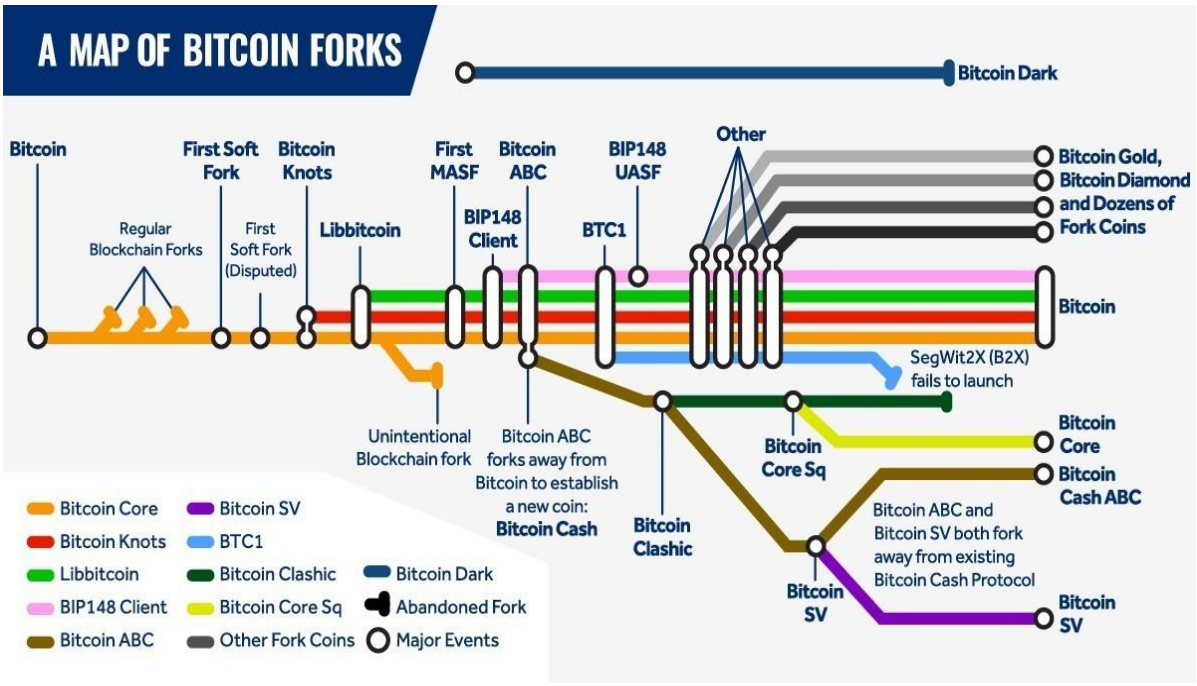

*Source: Snapper (2018). Protocols Platforms and DApps - blockchain layers explained - OriginTrail community. [online] OriginTrail community*

## 2.4 Features that enhance the concept of blockchain

### Forking

One of the features of blockchain is that all transactions are with the governance provisions, developed at the time of commencement. Thus, one of the questions is, Do blockchains have the flexibility to adapt to changing circumstances? Forking enables this change. Blockchain forking is similar to an operating system update for a computing device. Blockchains governance is decentralized and all the nodes have an equal stake in the functioning of the network. The different nodes on the blockchain need to run on the same protocol and algorithm to function well and maintain a canonical version of the blockchain ledger. Therefore, forking has to be achieved with a consensus or democratically the different group of nodes can decide to go ahead with a software upgrade or not go ahead with the forking. This can spawn the different versions of the blockchain running independently from each other. The image below shows the history of Bitcoin forks over the years.

Figure 6: A map of Bitcoin Forks




Forks that are incompatible with older versions of the protocols and algorithms are called **"hard forks."** Hard forks typically change consensus rules (i.e. block size, mining algorithm, consensus protocol) in a way that makes previous versions of the blockchain incompatible. However, some forks *are* compatible with older versions of the blockchain. **"Soft forks"** are updates that still work with older versions.

### Smart Contracts

A smart contract is an analogous version of contracts in the physical world and financial contracts traded digitally which are intermediated by third-party platforms. It is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Platforms like Ethereum provide setting up of programming logic for executing transactions between nodes depending on the state of the network or state of the world.

With the advent of 5G, Internet of Things (IoT) and Artificial Intelligence (AI), smart contracts will play an important role in the world of technology and commerce. Already, most of the trading on stock exchanges is algorithmic trading where AI algorithms decide to buy and sell securities. Theoretically, a decentralized blockchain solution using smart contracts can obviate the need for stock exchanges going forward.

### Tokens and initial coin offerings (ICOs)

For financial transactions to be consummated on a blockchain, a medium of exchange is required. Blockchain tokens are analogous to loyalty points, flying miles, credit card points or other units of account and medium of exchanges used by a select group of individuals between themselves or with a small set of organizations. They have some features of a currency but do not have the universal usage and fungibility as the currencies usually have.

Crypto tokens are a special kind of virtual currency tokens that reside on their blockchains and represent an asset or utility. Such crypto tokens often serve as transaction units on the blockchains that are created using standard templates like that of the Ethereum network that allows a user to create their tokens. Such blockchains work on the concept of smart contracts or decentralized applications, where the programmable, self-executing code is used to process and manage the various transactions occurring on the blockchain. Tokens can also be created to create equity and debt instruments as well.

ICO refers to the creation and sale of digital tokens. In an ICO, a project creates a certain amount of a digital token and sells it to the public, usually in exchange for other cryptocurrencies such as bitcoin or ether. The public could be interested in the tokens on offer for either or both of the following reasons:

1) The token has an inherent benefit – it grants the holder access to a service, a say in an outcome or a share in the project's earnings.

2) The benefit will be in increasing demand, which will push up the market price of the token.

Tokens, especially those of successful sales, are usually listed on exchanges, where initial buyers can sell their holdings and new buyers can come in at any time.

As a type of digital crowdfunding, token sales enable start-ups not only to raise funds without giving up equity but also to bootstrap the project's adoption by incentivizing its use by token holders. Buyers can benefit from both the access to the service that the token confers and from its success through appreciation of the token's price. These gains can be realized at any time (usually) by selling the tokens on an exchange. Buyers can show their increasing enthusiasm for the idea by purchasing more tokens in the market.

**Decentralized Autonomous Organization (DAO)**

The existence of firms and companies is seen as an old puzzle[17] in economic theory. Economic theory studies voluntary transactions between atomistic agents. Firms and companies, however, do not function on this principle. Since it can be very difficult to manage contracts between individuals for completing the work efficiently, a decentralized autonomous organization (DAO) helps. DAO is primarily a business or organization whose decisions are made electronically by a written computer code or through the vote of its members. In essence, it is a system of hard-coded rules that define which actions an organization will take.

However, with the advent of digital technologies, the internet and blockchain, smart contracts and ICOs, many people believe that firms can be organized in a different fashion where rather than having a hierarchical centralized structure these technologies can be used to reduce frictions and run the firm in a decentralized fashion. The idea of the Decentralized Autonomous Organization is born out of this philosophy and background.

## 2.5 Application of blockchains

Blockchain technology frees up a key constraining dimension —the need for trust— required for executing transactions. The potential use cases of blockchains for storing and distributing information securely has resulted in it being heralded as the next big disruptive technology. Enthusiasts believe that the possibilities for blockchain is abundant and the technology may even disrupt established digital economy platforms. Some commentators refer to blockchain as the "new internet"[18] --comparable today to what the Internet was three decades ago.

Bitcoin, the first and possibly the best-known application of blockchain, can be characterized as follows:

- It is a decentralized network of nodes that own and wish to transact in the digital cryptocurrency;
- It is a ledger that sequentially records the ownership of bitcoins with each node;
- It is an immutable record of all past ownership and transactions of bitcoins; and,
- Each node on the network has a unique identity.

Other applications of blockchain are also built around each or a combination of these attributes which help establish a high level of trust between entities. Blockchains have the highest potential in markets where trust, transparency and a high level of decentralized information is required. The power of tokenization - 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 blockchains beyond cryptocurrencies.

**According to a study by NASSCOM and Avasant on blockchains:**

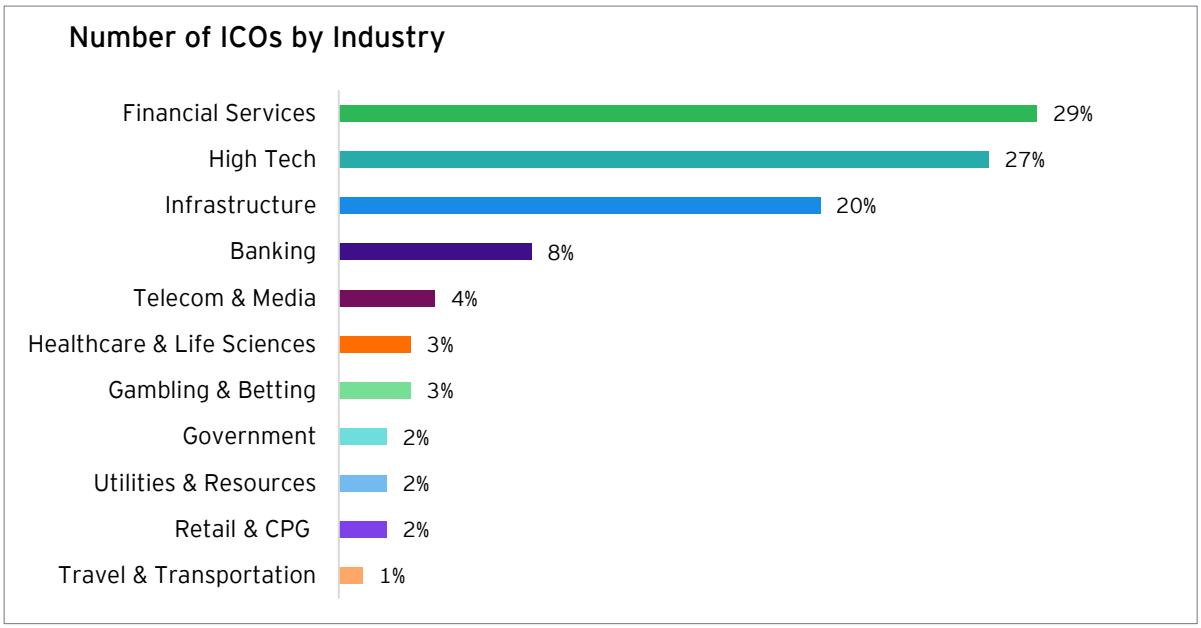
- 50 countries have embarked on initiatives to integrate blockchains in their economies;

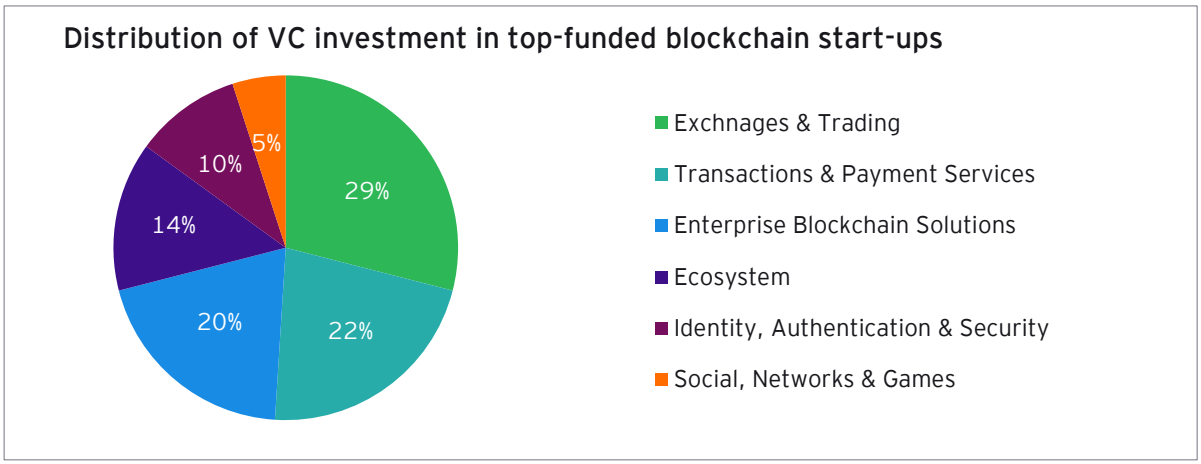
[17] Ronald Coase and Oliver Williamson- Two Nobel laureates

[18] Cretin, A. It's 2018 — Blockchain is on its way to Become the New Internet (5 January 2018). The Medium < https://medium.com/@andrewcretin/its-2018-blockchain-is-on-it-s-way-to-become-the-new-internet-7055ed6851ec>

- Global blockchain investments through venture capital and initial coin offerings were 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 a pilot stage; and,
- Blockchain technologies are evolving - some of the areas of focus are interoperability between platforms, cost-effective and faster transaction.[19]

As illustrated by the below figures, blockchain investment in terms of initial coin offering (ICOs) and venture capital investment has been well distributed across major industries and solutions.




*Source: NASSCOM Avasant India Blockchain Report, 2019*

While there are several use cases of blockchains, most will tend to fall under the following categories.

**Increasing efficiency through decentralization and disintermediation**

One of the features of a blockchain is the ability to verify transactions collectively and not having to rely on a central entity for verifying and consummating transactions. As a result, peer to peer transactions without the use of an intermediary can be undertaken. In several markets, for instance, trading of securities or payment systems, an intermediary is required for a variety of reasons such as to take counterparty risk, maintain ledgers, update and share information and other services incidental to those marketplaces. Some of these markets are potentially at risk of disruption by blockchain-based applications.

An application of blockchain that is gaining increasing attention given its decentralized nature is smart contracts (which can be used to exchange tokenized products and services). Essentially, a smart contract is a

[19] NASSCOM Avasant India (March 2019). Blockchain Report 2019

programmable code that is executed on a blockchain (when certain predefined terms and conditions are met) to enforce an agreement between two or more parties.[20] They are based on the "if, then" logic – 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. For instance, the French insurance company, AXA, used blockchain technology to introduce a flight delay insurance service, Fizzy, that processes claims using a smart contract.[21] Once a customer has recorded his flight, selected his cover, and paid his premium, a smart contract is created in the form of a code.[22] From public sources, the smart contract information about flight delays and automatically pays out to a consumer in case his/her flight is delayed. [23]

Smart contracts can be used in various sectors including 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).[24] The advantages of such a smart contract are that there is no need for manual intervention (such as raising a claim request or processing it saving time and cost for both parties. As an example, in clearance and settlement systems, blockchains will allow near real-time transactions between the two parties directly, thereby reducing cost and time.

In existing markets, where transaction costs are high and a large number of intermediaries are required to consummate transactions, or where the exchange of information or transaction involves significant time delays, blockchains can save transaction costs and transaction time.

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

In markets or in business processes where verification of the identity of an individual or verification of the origin of products is critical, blockchain can be effective as it can create an immutable database that can be used to trace the authenticity of a product or verify the identity of an individual. Usage of blockchain ensures that the information once recorded cannot be amended and is therefore verifiable quickly and at a low cost.

This particular application may be used by firms across industries to increase the efficiency and transparency of their supply chains – i.e., from tracing the procurement of raw material to manufacturing and warehousing, to delivery and payment.

For instance, an Italian food and wine producer, developed a proof of concept for a blockchain wherein customers 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 the single bottle through a smart label. Blockchain applications in addition to enabling users to trace the distribution of the product can also and overcome the issue of counterfeiting (with strong potential in the pharmaceutical sector to verify the authenticity of medicines).

Similar blockchain-based solutions can also be used to facilitate international trade and improve customs processes. For instance, Maersk and IBM introduced a blockchain solution for containerized shipping developed by them, TradeLens.[25] The blockchain essentially integrates trade data from industry partners onto a common, secure business network, and then provides real-time, secure access to end-to-end supply chain information to all actors involved in a global shipping transaction.[26]

**Creating trust through a repository of verified immutable records**

Blockchains also have a strong use case where individuals wish to exercise greater control over their data or when maintenance of verified records is extremely important. Blockchains can contribute significantly in creating a registry of verified records for a variety of purposes, be it education, work experience, health or land titles.[27]

For instance, a blockchain for land registry, which can be viewed by all stakeholders – buyers, sellers, agents, and banks, has been successfully tested by the Swedish Lantmäteriet.[28] The registry contains bills of sale/purchase and the contracts, identity documents and signatures of the parties, and ownership

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

[21] https://www.axa.ch/en/unternehmenskunden/blog/start-ups-and-innovation/blockchain-insurance-switzerland.html

[22] https://www.axa.ch/en/unternehmenskunden/blog/start-ups-and-innovation/blockchain-insurance-switzerland.html

[23] https://www.axa.ch/en/unternehmenskunden/blog/start-ups-and-innovation/blockchain-insurance-switzerland.html

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

[25] https://docs.tradelens.com/learn/tradelens_overview/

[26] https://docs.tradelens.com/learn/tradelens_overview/

[27] 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).

[28] Srivas, M.K., Yeboah, T. The Disruptive Blockchain: Types, Platforms and Applications. 5th Texila World Conference for Scholars (TWCS), 2018 on Transformation: The Creative Potential of Interdisciplinary & Multidisciplinary Knowledge Exchange

information.[29] Similarly, there is scope for blockchain that can be used by potential recruiters to verify a candidate's information about educational history or employment record.

The healthcare sector can also benefit from the security and accuracy of records in a blockchain. Clinical and medical data, such as vaccination and medication records, patient data, genetic histories, insurance policies, and clinical trial results can easily be stored and shared across relevant parties through a blockchain. An example is the blockchain-based personal healthcare record operating system (phrOS) developed by and Taipei Medical University Hospital and Digital Treasury Corporation (DTCO).[30] The blockchain ensures that medical data is collected and stored, protects the medical data from being hacked. At the same time, it facilitates the seamless sharing of information across hospitals for treatment and hassle-free online insurance claims by individuals.[31]

### Public services

Blockchain's ability to provide security and transparency makes it very attractive for the government, be it for digital record keeping, facilitating cross-departmental coordination, or provision of public services or aid. An example is the public blockchains developed for the City of Vienna to validate and secure the city's Open Government Data (OGD).[32] The OGD includes data such as public transport routes, train schedules and surrounding communities' voting results.

Blockchains could also simplify the government's taxation process. For instance, under the Australian tax law, if a person contributes more than their annual limit to their superannuation fund, they and their fund need to complete various paper-based forms to be sent to the Australian Tax Office (ATO) for the over-contributed funds to be released. Once the ATO has the required forms, it will authorize the "release" of the over-contributed funds to be paid to the person. This "release authority" process requires several manual forms that need to be reconciled and matched with payment instructions as well as input from multiple parties including a person, a financial institution, and the tax authority. Given this business problem, a large Australian financial institution built a blockchain prototype for tax reporting and payment ecosystem (in close consultation with the ATO).

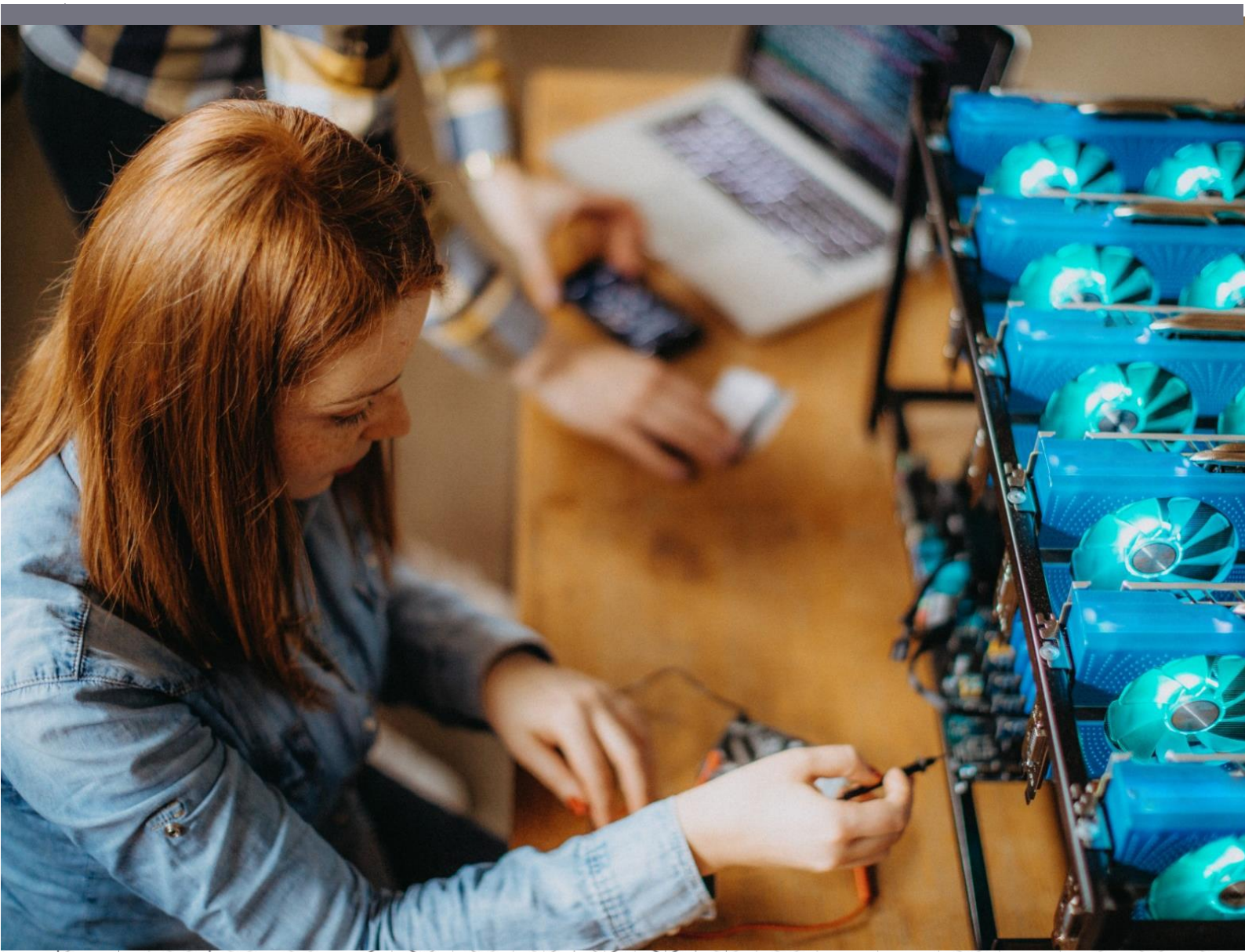
[29] Srivas, M.K., Yeboah, T. The Disruptive Blockchain: Types, Platforms and Applications. 5th Texila World Conference for Scholars (TWCS), 2018 on Transformation: The Creative Potential of Interdisciplinary & Multidisciplinary Knowledge Exchange

[30] Lu, N. Taipei Medical University Hospital and Digital Treasury Corporation Jointly Release "phrOS"- The First Healthcare Blockchain Platform Worldwide, Ip Seeds, https://medium.com/blog-ipseeds-net/taipei-medical-university-hospital-and-digital-treasury-corporation-jointly-release-phros-the-7e80cdfa87b9

[31] Lu, N. Taipei Medical University Hospital and Digital Treasury Corporation Jointly Release "phrOS"- The First Healthcare Blockchain Platform Worldwide, Ip Seeds, https://medium.com/blog-ipseeds-net/taipei-medical-university-hospital-and-digital-treasury-corporation-jointly-release-phros-the-7e80cdfa87b9

[32] https://www.ey.com/en_gl/news/2018/08/ey-and-city-of-vienna-collaborate-on-public-blockchain-networks

# 03 Blockchains in India



# Blockchains in India

In India, cryptocurrency has received a great deal of attention over the past several years culminating in a recent recommendation to ban cryptocurrency nationally. Since last year, banks in India have been barred by the Reserve Bank of India (RBI) from dealing with cryptocurrency firms and exchanges. Several petitions have been filed to overturn the RBI ban, and the matter is with the Indian Supreme Court. Further, the inter-ministerial committee set up by the Indian Government to determine the legality of cryptocurrencies and blockchain submitted its report to the Finance Ministry on 23 July 2019, recommending that private cryptocurrencies be banned completely in India.[33] The committee also formulated a draft law, the 'Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019', which mandates a fine and imprisonment of up to 10 years for offences.

The committee, however, said the government should keep an open mind on the potential introduction of an official cryptocurrency. The Committee also recognized the fact the there is a difference between cryptocurrency and its underlying technology i.e., Distributed Ledger Technology (DLT) or blockchains. The Committee in its report went on to identify a number of 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 to the banking and financial sector in India where it has identified blockchain as one of the 'Three Pillars' which will 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.

[33] https://www.livemint.com/industry/banking/government-panel-suggests-ban-on-private-cryptocurrencies-1563796292369.html

India has witnessed various start-ups that are using blockchain applications to resolve issues in a wide range of sectors.

## Technology

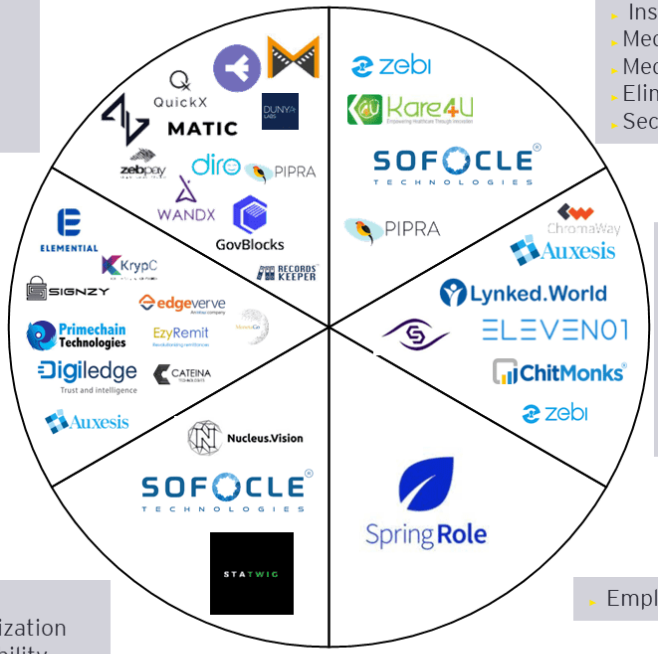
- Token trading
- Identity Verification
- Decentralized exchanges
- Loyalty programs
- IP management
- Micro-corporations management
- Micropayments
- Crime reporting
- Media IP protection
- Privacy control

## Healthcare

- Insurance and medical loan
- Medical record maintenance
- Medicine supply chain
- Elimination of fake drugs
- Secured healthcare data sharing

## BFSI

- Faster and cheaper remittances
- Authentication, verification and storage of electronic records
- Secure digital compliance
- Vendor management
- Efficient supply chain trade finance
- KYC norms
- Digital onboarding solutions




## Government

- Organ tracking for transplantation
- Rationing management
- Vehicle title management
- Sapling management and monitoring
- Chit fund operations administration
- Identity management
- Digital certificates management
- Land registry management
- Citizen electronic health record
- Agricultural supply chain

## Retail and CPG

- Brand engagement
- Privacy control
- Loyalty programs
- Anti-counterfeiting
- Food auditing
- Loyalty programs
- Procurement optimization
- Supply chain traceability
- Inventory control

## Human Resource Management

- Employment verification
- Candidate recruitment

*Source: NASSCOM Avasant India Blockchain Report, 2019*

Examples of the usage of blockchains in India are discussed in the following box.

## Box 3: Examples of blockchains 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:

- sofoPay, introduced by Sofocle Technologies, is a blockchain solution aimed at assisting enterprises by easing the complexities of procure to pay and reducing costs by eliminating manual processes. In a traditional procure to pay process, there are various manual steps involved from placing a purchase order to delivery and confirmation of goods received, and finally invoicing and payment. sofoPay, built on HyperLedger, uses smart contracts to digitize and streamline this process by automating payments made by businesses to vendors and partners. sofoPay thus created a network enabling trade partners to interact with each other in a transparent ecosystem without any restrictions or reservations. It has been designed to overcome the challenges faced by enterprises while managing payment against an invoice.
- Somish BlockchainLabs, developed GovBlocks, an open permission-less blockchain (decentralized applications/dapps) for governance which is based on Ethereum. One of the uses of GovBlocks is the data exchange framework, which has various benefits compared to traditional data exchange measures. Traditionally, when sharing its data with another entity, data owners bestow trust on the former (which may be breached). There is a lack of clarity and visibility related to the use of the said data, for which data privacy and protection laws are relied upon. Blockchain-based GovBlocks can help overcome some of these challenges by (a) sharing the same data (on a nearly real-time basis) with all stakeholders with proof of exchange, eliminating the need for centralized trust; (b) providing an on-chain approval mechanism for exchange of data between two entities; and, (c) ensuring data ownership by providing an immutable audit trail of data requests, exchange and edit approvals. GovBlocks' applications include citizen certification, land registry, health services, inter-department data exchange, and legal documents. Somish has also leveraged the protocol of GovBlocks to introduce a new permissioned solution for data sharing –Data Exchange Framework (DEF). DEF can be used to improve supply chain management, thereby saving employee time, improving data quality and operational efficiency.
- Coffee Board, in collaboration with Eka Plus' blockchain-based marketplace application (Eka Blockchain Marketplace), launched a pilot blockchain-based coffee e-marketplace to integrate Indian coffee growers with markets in a transparent manner and ensure fair price realization for the producers. While Indian coffee is highly valued globally and is sold at a premium, the small business size of producers and the presence of various intermediaries (among other factors) results in meagre earnings for the coffee growers. This blockchain application is likely to improve transparency in the trade of Indian coffee, maintain the traceability of Indian coffee from bean to cup so as the consumer tastes real Indian coffee, and ensure that the grower is paid fairly for the coffee produced. By directly connecting producers with the market and ensuring reliable traceability, this application is expected to reduce the number of layers between coffee producers and buyers and help farmers double their income. The blockchain can be used by coffee farmers, traders, coffee curers, exporters, roasters, importers and retailers and will include details about the coffee such as the place where it is grown, details of the crop, elevation, certificates (if any), etc.
- Zebi Data India Pvt Ltd.'s, Edu Chain, is a blockchain-based digital credential management solution that enables students and universities to store, retrieve, and verify the data online. Various universities, including IIT Basara, have adopted this solution due to its various benefits. This application of blockchain technology benefits students by storing their academic records securely, enables quicker verification of their records by employers and universities, and enables them to store their educational certificates in their wallets. Universities on the other hand are protected from fraudulent activities, their educational certificates' credibility increases and fee collection and payment can be tracked easily with an audit trail for each transaction.
- NITI Aayog, Oracle, Apollo Hospitals, and Strides Pharma Sciences piloted a blockchain-based real drug supply chain solution. The solution permanently registers a drug's record (serial number, labelling, scanning) through its movement from manufacturer to logistics, from stockist to hospital, or from pharmacy to consumer, leaving no scope for record tampering. Oracle's 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. It is expected that this solution will support governments and healthcare experts to quickly detect fake drugs and enable them to penalize wrong-doers with easy, proof-based data.

- 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, IndiaFirst Life Insurance, ICICI Prudential Life Insurance, Bharti AXA, Aegon Life, and Star Union Dai-ichi Life Insurance) developed a blockchain-based solution for information exchange between the firms. The solution, built on Corda (a platform developed by R3 and hosted by Microsoft's Azure infrastructure) is aimed at enabling insurers to overcome the risk of data breaches, fraud, and money laundering and improve their process efficiency, record-keeping and turnaround time. With the adoption of the blockchain, records will be available in near real-time, transparently and consistently and can be audited easily, thereby reducing operating costs for insurers by avoiding duplication of procedures and streamlining approvals.

Various other blockchain applications have been adopted in India. For instance, the National Stock Exchange (NSE) has used blockchain for its know your customer (KYC) and also undertook a pilot for e-voting using blockchain, and Axis Bank has collaborated with Ripple for faster and secure cross-border payment.

In July 2018, the Telecom Regulatory Authority of India (TRAI) passed the Telecom Commercial Communications Customer Preference Regulations, 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 communication; 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 3 years. The blockchain should also enable the interaction and exchange of information between relevant entities safely and securely. The regulation also talks about the possibility of setting up regulatory sandboxes for blockchain solutions.

## 3.1 Centralized databases vs blockchains

As discussed above, blockchains provide several benefits such as the creation of new markets; increasing the efficiency of existing markets by decreasing transaction costs and reducing processing times; streamlining business processes, etc. These benefits may be attributable to the difference in characteristics of a blockchain *vis-à-vis* a traditional centralized database.

**Table 1: Key differences between different kind of databases**

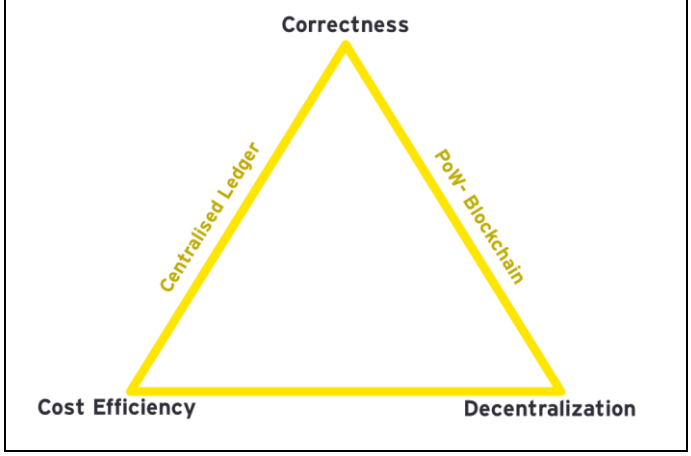
| | Traditional centralized database | Permissioned blockchain | Permission less blockchain |
|---|---|---|---|
| **Type of network** | Centralized | Semi-Centralized | Decentralized |
| **Cost of transaction** | High | Low | Low to High (depends on consensus mechanism) |
| **Speed of transactions** | High | High | Low to High (depends on consensus mechanism) |
| **Ease of implementation** | Can use the existing system | Requires wider network bandwidth | Requires wider network bandwidth |
| **Geographical dispersion*** | Single or select location | Can be Select also (depending on the location of nodes) | Can be distributed globally |
| **Control Dispersion*** | Low | High | Low |

| Table 1: Key differences between different kind of databases | | | |
|---|---|---|---|
| | Traditional centralized database | Permissioned blockchain | Permission less blockchain |
| **Architectural Dispersion*** | Low | Medium | High |
| **History of records and ownership** | Not available | Available | Available |
| **Consensus Mechanism** | None | BFT protocols depend on blockchain platform such as Raft Consensus, Istanbul(BFT), | PoW, PoS |
| **Token use or crypto use?** | Not required | Not required | Facilitates the application Meaning? |
| **Identity** | Known Identities | Known Identities | Anonymous |
| **Scalability/ ability to change** | High | High | Low |

While blockchain has its benefits over centralized databases, as is increasingly being realized, scalability is a big challenge with blockchain technology. The two biggest financial transaction applications of blockchain—Bitcoin and Ethereum—have far slower[34] transaction processing speeds than the centralized platforms. The failure to scale up the speed has also led to increased transaction charges[35] on the platforms which further constrains the usability. This also explains why most applications are permissioned blockchains until now.

Blockchain technology as it exists today suffers from a central trilemma, which could explain its slow growth to date. Being a decentralized distributed ledger technology, compared to a centralized database, a blockchain application have a trade-off between either achieving correctness or speed of consummating transactions (leading to cost efficiency). The Ethereum blockchain platform's future transition to proof of stake consensus from its original proof of work consensus is a step to solve the speed issue. However, if it will be successful in reducing the transaction charges will only be clear when it is implemented.

Figure ZZ: Public blockchain trilemma[36]




[34] https://en.wikipedia.org/wiki/Bitcoin_scalability_problem

[35] https://bitinfocharts.com/comparison/transactionfees-btc-eth.html. https://www.thestar.com/business/2019/08/19/ethereums-vitalik-buterin-on-reducing-cryptocurrencys-risks.html

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

## 3.2 Policy and regulatory compliances

As noted earlier, blockchain is an evolving technology and its applications are growing and gaining strength. Like with all new developments, the government is working on policy and regulatory needs that relating to Contracts, Jurisdictional, Data protection and privacy, Competition, Cybersecurity are the key areas that governments have addressed in the whitepaper published by MEITY for "National Strategy for Blockchain" in January 2021

https://www.meity.gov.in/writereaddata/files/NationalStrategyBCT_%20Jan2021_final.pdf

Blockchain technology presents is a distinct breed in and of itself that may be outside the paradigm of existing legal and regulatory frameworks this requires industry and government to work together to define policies and laws needed to govern Blockchains.

**Jurisdiction and anonymity**

Regulatory body and laws for Blockchain will help improve adoption, given the decentralized nature of Blockchain, there may not be any identifiable host or an operator and the nodes may be spread across a large geographic area with transactions occurring between nodes located in different jurisdictions. In the case of permission-less blockchains, network participants may be anonymous or pseudonymous i.e., their identities are not fully known. In such a scenario, regulatory body and policy will help to define ownership and associated liabilities for participants of the blockchain.

**Data privacy and protection laws**

Generally, blockchains offer greater data security compared to traditional systems. Blockchain can enable storage for any types of information/ documents that provide right to assets – legal documents, healthcare records, payment or identity information. Once this data is codified and entered into the ledger, copying or duplicating that information without the owner's explicit permission is impossible under current technology.

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 through access to the central data repository, which represents a single point of failure. In the case of a blockchain, a hacker would have to target at least the majority of the nodes on a blockchain.

New privacy and data protection frameworks as they get defined will address the blockchain needs:

Newer Data Privacy and localisation laws will address the underlying principles of blockchain

- Blockchain is decentralised and no one entity is responsible for ensuring that the data of an individual stays confidential.
- Blockchain data is immutable and not erasable
- Blockchain can run across multiple jurisdictions, cross-border transfers of data

## 3.3 The future of blockchains

As discussed above, there are economic benefits for India from the use of blockchain technology. Research and development on blockchains, including their different applications, their scaling up and future development are underway. Applications are being explored across sectors including automobile, insurance, healthcare, public services, and supply chain.

In general, it is expected that blockchain applications will compete with similar existing systems/ technologies. This is already being experienced to some extent in the financial sector. Initial application has been focussed on the financial sector including cryptocurrencies, digital payments, financial securities, and lending. For instance, in the market for providing cross-border payments, traditional banks may have to compete with blockchains such as Ripple[37] which enables users to make cross-border payments in various currencies. The competitive pressure exerted by Ripple on the traditional banking system is strengthened by the fact that the former's reliance on blockchain technology enables it to make payments faster, cheaper and transparent.

Blockchain technology is an important innovation that can cause fundamental disruption and promote competition across different sectors of the Indian economy. Given the nascent stage of its development, removal of regulatory uncertainty and addressing policies putting blockchain applications at a competitive disadvantage can go a long way in fostering the growth of this technology which has the potential to promote competition.

[37] https://www.ripple.com/ripplenet/

Ernst & Young LLP

**EY** | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, 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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata – 700016



EYIN2103-011
ED None



AK1



## About IAMAI

The Internet and Mobile Association of India [IAMAI] is a young and vibrant association with ambitions of representing the entire gamut of digital businesses in India. It was established in 2004 by leading online publishers in the country. In the last 16 years, the association has brought out and addressed several challenges facing the digital and online industry involving mobile content and services, online publishing, mobile advertising, online advertising, ecommerce and mobile and digital payments.

Sixteen years after its establishment, the association is still the only professional industry body representing the online industry in India. It is registered under the Societies Act and is a recognized charity in Maharashtra. With a membership of nearly 300 Indian and overseas companies, and with offices in Delhi, Mumbai, and Bengaluru, the association is well placed to work towards charting a growth path for the digital industry in India.