

DRAFT APPROACH PAPER-

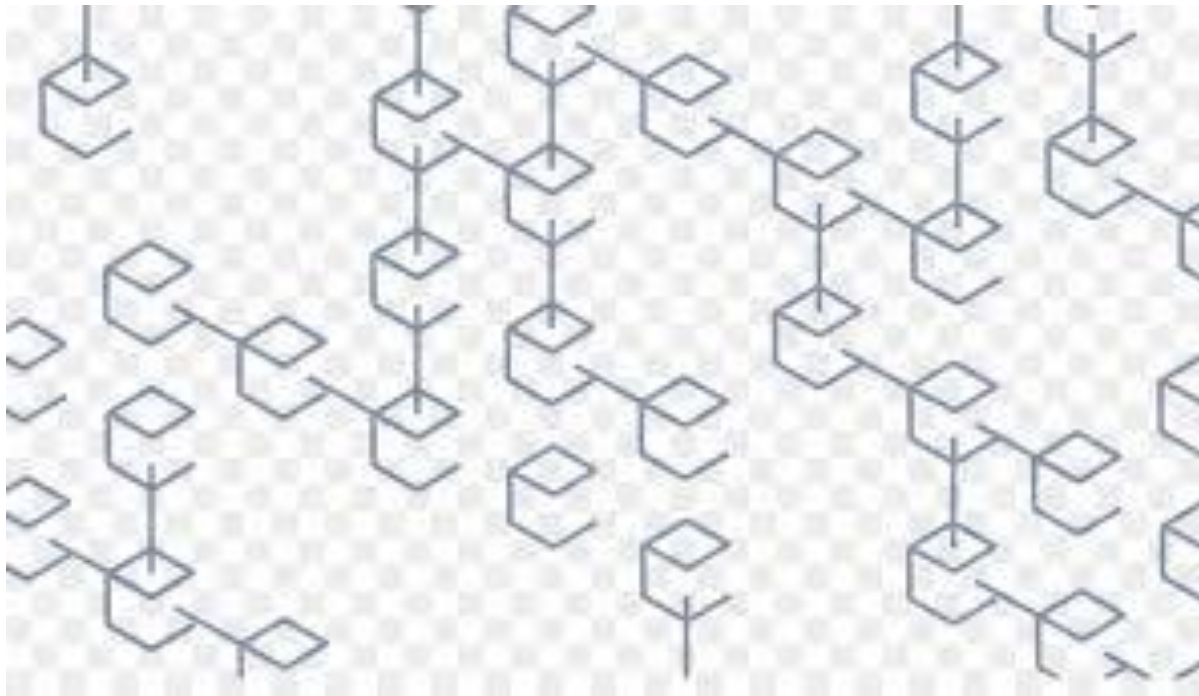


Image from: Sutardja Center, Univ. of California Berkeley

NATIONAL STRATEGY FOR BLOCKCHAIN

December 2019

NISG Team

Academic Advisor
Prof. Shivendu, S.
Univ. of South Florida, Tampa, Florida



National Institute for Smart Government

Architecting e-Government

TABLE OF CONTENTS

1. Introduction: What is New?	2
2. Value Proposition of Blockchain Technologies	Error! Bookmark not defined.
3. Overview of Blockchain Technology	6
4. Applications of Smart Contracts	16
4.1. Blockchain in Financial Applications	22
4.2. Digital Identity Management	23
4.3. Blockchain in Supply Chain applications	24
4.4. Blockchain in Manufacturing	25
4.5. Educational certificates & Student / Employee credentials	26
4.6. Blockchain in Healthcare	27
4.7. Blockchain in Telecommunications	27
4.8. Blockchain in Government	27
4.9. Shared Data Services	27
4.10. Decentralized Marketplaces	28
4.11. Other use cases	28
5. Challenges in Adoption of Blockchain Technology	29
6. Societal Impact of Blockchain Technology	33
7. Role of Government	34
8. Principles to Guide National Strategy	37
9. Going Forward: Think Networks, Think Global	40

1. Introduction: What is New?

Since the advent of Univac-1, manufactured by Remington Rand using 5,200 vacuum tubes, weighing around 14,000 Kgs and priced at \$ 1 million each, as the first commercial computer that attracted widespread public attention; computing technologies including hardware, software, and communication networks, have increasingly been the key drivers of economic growth and societal changes. Together with these technological developments, academics, business leaders and policymakers have been shaping the practice of managing organizations including governments.

The core technological layers of the Internet technologies, that is TCP/IP protocols, which allow computers to communicate with each other were invented in the 70s, but it was only in the late 80s the commercial applications of such technologies started to get popular, first as email applications, and later as e-commerce and digital publishing, which led to businesses around many-to-many communications networks such as in social networks. These technologies are often referred to as foundational technologies because their profound impact on societies as well as businesses is realized over a long period of time and across various sectors, unlike disruptive technologies that significantly impact a particular sector in a very short period of time. Though the foundational internet technologies have led to sea changes in the world in almost all aspects of life in the last three decades, organizations have largely remained hierarchical, isolated, and vertically integrated. The reason is that the existing internet technologies are orders of magnitude more efficient in moving ‘information’ or data across various participants or nodes in a network, but have significant limitations in transferring value across the network. The inability of internet technologies to transfer ‘value’ across nodes in a network lies in the fact that not only the authentication and verification of ‘ownership’ of value requires trusted third parties but these parties are also required for safe custody of the ledgers of records of ownership.

For example, when we email a textual document, or video or photograph or audio file to someone, we are sending a copy of the original and the recipient can copy and change it. Though we can transfer ‘information’ in the document to another person, we still need a ‘trusted third party’ to provide verification and authentication services. In the current business networks including government services operating on the backbone of internet technologies, we can transfer ‘information’ very efficiently, we still need intermediaries such as banks, technology companies, and governments to establish trust and maintain integrity to enable value exchange across participants. In other words, internet technologies facilitate stakeholders to create ‘internet of information exchange,’ but not that of ‘internet of value exchange.’ Moreover, though organizations and all stakeholders are connected to each other through the Internet, their databases are firewalled because they need to safeguard the custody of ledgers and that results in slowing down of transactions, leading to inefficiencies as well as costs.

What would happen if there were a set of technologies, which allowed participants to create ‘internet of value’ wherein participants could store and exchange value without the need for traditional intermediaries or without the verification and authentication services of a trusted third party? What would be the impact of a technology that operates on top of the ‘internet of information exchange’ to create an ‘internet of value exchange’ wherein the trust is coded in the technology in such a way that need for safe custody as well as authentication and verification by a trusted no more exists?

At the core level, this is what blockchain technology based systems offer. In the ‘internet of value’ created by blockchain technologies, value is stored in a global tamper-proof public record book and not in a file

stored somewhere in a firewalled storage system, and the new transactions including transfer of assets or value are authenticated, verified and approved leveraging a large peer-to-peer network through distributed consensus protocols rather than by a central authority.

In other words, blockchain technologies are a set of technologies that enable to keep tamper-proof record of transactions defining asset or value ownership efficiently through appropriate data structures, allow peer-to-peer participants to update the records when asset or value transfer takes place using foolproof mechanism through distributed consensus protocols, and create business value through smart contracts which are coded in software and are executed when objective conditions set in the code are met. This allows for the value to be transferred from one owner to another owner (ownership transfer) between decentralized peer-to-peer machines or nodes without the need for any central authority for authentication and verification. This feature also allows for autonomus systems to be built on top of Internet of Things (IoT) technologies.

Since these technologies work in networks, they need coordination, facilitation and appropriate legal as well as the regulatory framework. In order to achieve this, Governments all around the world are working on developing comprehensive national blockchain strategies including mission and vision statements and have been working proactively with industry and academia partners to facilitate integration of the technology with existing economic ecosystem and architecture by taking steps to reduce or remove regulatory hurdles, enable creation of skilled human capital, bolster research and innovation, and promote conducive policy frameworks.

This paper outlines a broad contours of approach to formulating a national blockchain strategy for India which is directed towards and is informed by the following Vision and Mission:

Vision Statement: India will be one of the leading countries in the world in innovation, education, commercialization, and adoption of blockchain technology in private and public sectors by 2025.

Mission Statement: Mission of National Strategy on Blockchain is to provide a set of policy frameworks and incentives in consultation with stakeholders to proactively facilitate integration of the blockchain technology with exiting economic ecosystem by implementing appropriate legal as well as regulatory architecture, creating incentive structure for academia and industry to promote research and teaching, and formulating policies leading to rapid innovation, adoption and growth of blockchain technology applications in public sector including government as well as private sector.

The approach paper is organized as follows. Before providing an overview of the blockchain technology as well as its foundationa pillars, we first discuss the value proposition of this technology and motivate potential sectors in the economic networks wherein this technology may be value enhancing. Thereafter, we describe various application domains which are potential candidates for the early adoption of blockchain technology, challenges in adoption of blockchain technology by public sector including government and private sector and the potential for societal impact if the adoption barriers are either lowered or removed altogether. This lays the ground for delineating the role of government and also need for a strategy at the national level. Thereafter, we lay out, based on policy developments in other countries as well as on academic work relating to blockchain, the guiding principles for national strategy and conclude by describing next proposed next steps.

In the end, the goal of this approach paper is to get the ball rolling by outlining a framework and contours of national strategy leading to wider discussion, consultation, knowledge sharing which in turn will lead to a more robust formulation of national strategy on blockchain.

2. Value Proposition of Blockchain Technologies

While real-world large scale blockchain technology based systems are still non-existent, blockchain was in full glare as a priority topic at World Economic Forum, Davos in 2018 as well as in 2019. A reputed business survey estimates that around 10 percent of global GDP will be stored and exchanged on blockchain by 2027.¹ Another metric that reflects global interest in this technology is that in past two years alone there have been more than half a million new publications on and 3.7 million Google search results for blockchain. Funding for blockchain-centric start-ups has been consistently growing and was estimated to be around \$1 billion in 2017.² Leading technology firms including IBM have also been investing in blockchain: IBM has more than 1,000 staff and \$200 million invested in the blockchain-powered Internet of Things (IoT).³

Blockchain technologies have disruptive potential but at the core level, these are foundational technologies which are likely to lead to new business models. The initial value proposition is likely to be operational efficiencies due to reduction in transactional costs. Modification of the existing processes by removing intermediaries or by lowering the administrative costs of safe record keeping will lead to cost reduction and efficient transaction reconciliation. This is likely to shift the flow of value by reducing lost revenues and will provide opportunities for new revenue sources for those businesses which adopt blockchain-based systems. A recent report by McKinsey Digital estimates that approximately 70 percent of the value in short term would be through cost reduction, followed by revenue generation.⁴

Given the nature of these technologies, certain business sectors core functional requirements make them more amenable to blockchain solutions. It is very likely that financial services, government, and healthcare sectors will be the front runners in capturing the value. Core functions of financial services are about verifying and transferring financial assets. This aligns well with blockchain technologies core value proposition. Inefficiencies in cross-border payments and trade finance, can be addressed by systems based on blockchain. This may also lead to reduction in the number of intermediaries. Blockchain based systems may also lead to value creation in capital markets by having efficient and fast trade settlements as well as savings in regulatory compliance. Due to these potential opportunities of value creation approximately 90 percent of major multinational banks are experimenting in development of blockchain-based systems.

Blockchain based systems can also enable governments' key record-keeping and verifying functions. This is likely to lead to large administrative cost savings. Public data which is often not shared seamlessly among government agencies as well as across businesses entities, regulators and citizens. This includes data relating to birth certificates to property ownership, and taxes. Blockchain-based systems together with smart

¹ *Deep shift: Technology tipping points and societal impact*, World Economic Forum, September 2015, weforum.org.

² "Blockchain startups absorbed 5X more capital via ICOs than equity financings in 2017," CB Insights, January 2018, cbinsights.com.

³ "IBM invests to lead global Internet of Things market—shows accelerated client adoption," IBM, October 2016, ibm.com.

⁴ Blockchain Beyond the Hype: What is the strategic business value? July 2018; <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>

contracts can simplify interfaces between government agencies and citizens and also increase data security. Blockchain-based identity management systems can serve as key enabler for public service delivery systems leading to wider gains to economy.

Healthcare industry is another area where blockchain could be the key to unlocking the value of data by promoting data exchange across providers, patients, insurers, and researchers. Introduction of blockchain systems in health records will facilitate improved administrative efficiency and also give access to researchers to the historical data without revealing the identity of the patients. This is likely to be helpful advancements in medical research. On the other hand, patients may have more control over their data by introduction of smart contracts.

Much has been written about ability of blockchain technologies to increase privacy, enhance trust and remove friction within a business network. But blockchain's core value proposition rests on two key elements:

- **Verified origin of data:** While Blockchain does NOT guarantee data veracity, it does make it clear who put what data onto the ledger and when. Moreover, once the data has been put in a ledger or block, it can not be changed by any node in the network though a new updated record can be put in another block where old as well as new record are linked. In other words, once a record is created, its entire evolution is immutably recorded and given the current state of a record, one can trace the entire history of that record
- **Trusted processes (or workflows):** Blockchain creates the ability to track each step in a workflow, so that permissioned parties can understand and track how data flows through the process.

Furthermore, blockchain technology has extensive applications in following domains:

- KYC, Identity & Access Management,
- Verifiable claims of ownership of certificates ranging from academic to asset ownership and variety of other certificates,
- Voting in a variety of situations for political and business-related elections.
- Auditable track and trace record in the supply chains, transfer of ownership & invoice financing,
- Registry of things like Land registries, medical records, birth and death certificates
- Financial applications like Cross border & inter-bank money transfers, insurance claim settlement, commercial paper issuances, loan account management and the like.
- IoT security and smart contract settlements
- Cross enterprise collaboration in finance, supply chain, agriculture, energy trading, healthcare domains and the like and many more.

3. Overview of Blockchain Technology

Before, we described the foundational pillars of blockchain technology, we first provide a brief historical perspective to developments in the domain of digital currency till the advent of Bitcoin, as the first viable use case of blockchain systems which can create peer-to-peer value transfer network without the need for a trusted third party.

Historical perspective before Bitcoin: The growth of digital technologies together with developments of communication technologies in leading to laying of the foundations of the World Wide Web in 80s also provided impetus to academicians as well as technology entrepreneurs to experiment with creation of digital currency. Experts from diverse fields such as computer science and mathematics worked on different aspects of the foundational pillars even before the advent of digital technologies. Early scientific research by William Feller's probability theory (1957), followed by Haber and Stornetta's demonstration on how to stamp a digital document (1991) are precursors to viability of digital cash.

Renowned mathematician David Chaum in the 1980s published a research paper on cryptography in electronic payment systems, which eventually led to E-cash where one can store money in a digital format that can be spent at any shop where cash is accepted which is also cryptographically signed by a bank. In 1998, Wei Dai proposed B-Money, a technically anonymous distributed peer to peer network which takes care of ledger of transactions collectively and updates on different nodes of computers.

What is it in Layman Terms? A blockchain is a specific type of data structure which we can use to transfer value or assets across nodes or participants where the ownership rights are recorded in cryptographically stored and linked blocks which contain records of ownership of assets among the participants that can remain anonymous. Blockchains are open, distributed ledger that can record transactions between two parties efficiently and in a verifiable in a permanent way. To sum it up, it is a radically decentralized peer-to-peer technology to maintain asset ownership records and to allow for transfer of assets including updation of records using peer-to-peer distributed consensus mechanism. This removes the need for either safe keeping of records or authentication and verification by a trusted third party. A simple high-level view of blockchain system is shown in Figure 1.

A synonymous term that we hear when explaining or describing block chain is also Distributed Ledger or Distributed Ledger Technology (DLT). What this means in a generalized form is not only "Information sharing" but also a mechanism to update that information by the participants, even when there is no trust between them, as long as there is consensus between them. A Ledger is an authoritative record of important data or significant event. For example, this event could be a monetary transaction or valuable data like Medical Records, Government ID or a shipping record of supply chain logistics.

Before, we describe the foundational pillars to blockchain technology based systems, it is important to note that this technology allows for peer-to-peer exchanges and updation of ledgers without any trust created by a trusted third party. For example, in the current systems, transfer of any property by node A to node B in an economic networks requires not only a trusted third party like government to verify and authenticate the ownership from a repository of records which have been in safe custody of the government, it also requires a trusted third party like bank to verify that the promised sale consideration has been transferred or will be transferred by B to A, and after the transfer of property is effected, trusted government agencies are required to update the records with new ownership of property. Though these trusted third parties do provide economic value, the participants also bear the cost of using their services. Blockchain technology removes the role of trusted third parties as the 'trust' is created by the unique features of the technology and not by an organization or entity.

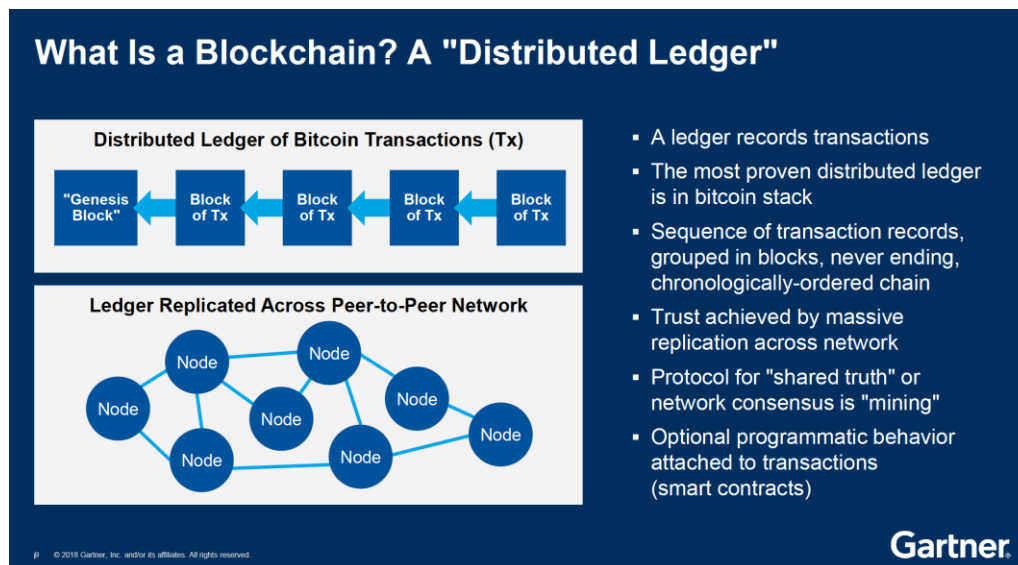


Figure 1: Blockchain/Distributed Ledger

Components of data structures in blockchain systems

A blockchain based business or economic system has three key pillars or components: data structures, distributed consensus mechanism and smart contracts.

Data structure layer ensures that data is stored, maintained and constantly updated in such a way that the safe keeping and authenticity of records is ensured by the technology rather than by a trusted third party. This can also be thought of as a database which comprises of a chain of fixed length blocks where each block can include 1 to N transactions.

Distributed consensus protocol or mechanism layer ensures that transfer of value or assets across nodes and updation of ownership records in the network can take place through peer-to-peer consensus mechanisms which ensures that only honest transactions are validated and recorded. This ensures that in a network consisting of non-trusting nodes, the value transfer and updating of ownership records can take place without the verification and authentication services of the trusted entities. In other words, each transaction that is added to a new block is first validated through a consensus mechanism, and then inserted into the block. The interaction and broadcast are verified by a distributed network and once validated a new block is created. When a validated new block is complete, it is added to the end of the existing block.

Once the first two pillars ensure a technology based system of ledger of ownership of asset or value and it honest updation without a trusted third party, then one can think of the third pillar, that is, Smartcontracts which allow the value transfer to effected by certain objective and verifiable conditions are met without the need for a ‘trusted third party’, and we have the ‘internet of value exchange’.

How a blockchain transaction works

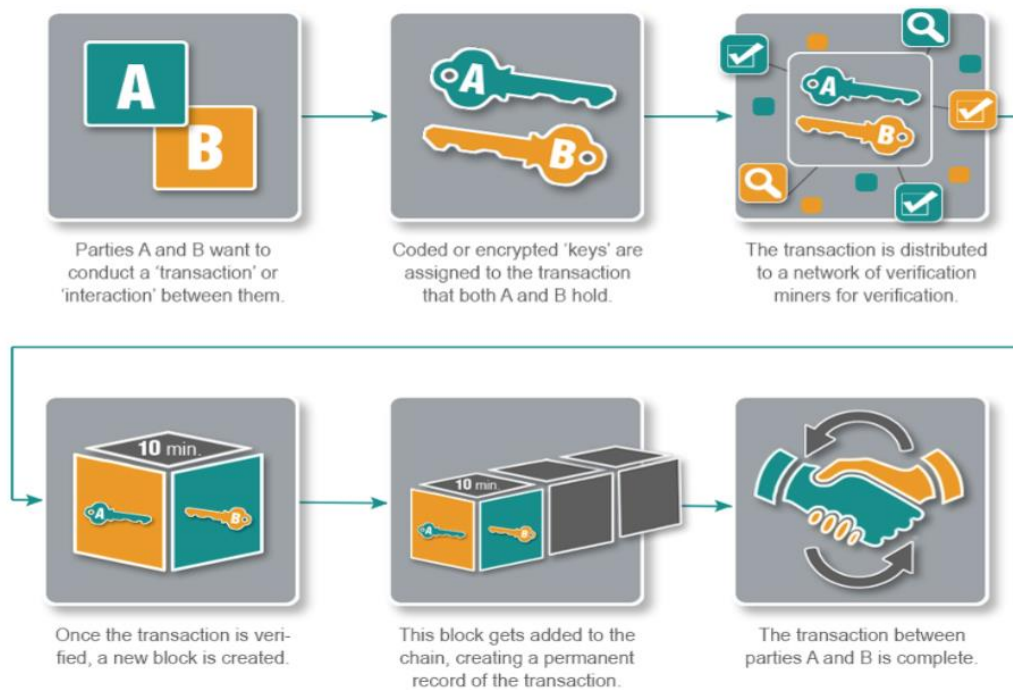


Figure 2: Transaction Flow in Public blockchain

In other words, blockchain systems build upon the ‘internet of information exchange’ to create an utility for ‘internet of exchange of value.’ Figure 2 provides and high level overview of how value transfer takes place in blockchain systems across nodes.

Let us say A and B are two entities that wish to conduct an interaction or transaction. First, cryptographic keys are assigned to each interaction.. The basic blockchain processing is performed in following steps:

- 1: Take new transactions and organize them into blocks. These transactions are undeletable.
- 2: Varification of every single transaction in the block cryptographically.
- 3: Then add this new block to the after the last block of existing immutable block chain.

Understanding the mechanics of blockchain: The blocks once recorded are resistant to modifications or any changes. In other words, this means that the data put in a block cannot be altered retroactively. Thus the use of a peer-to-peer (p2p) network and distributed timestamping server together with distributed consensus allows a public block chain database to be managed autonomously without any central authority.

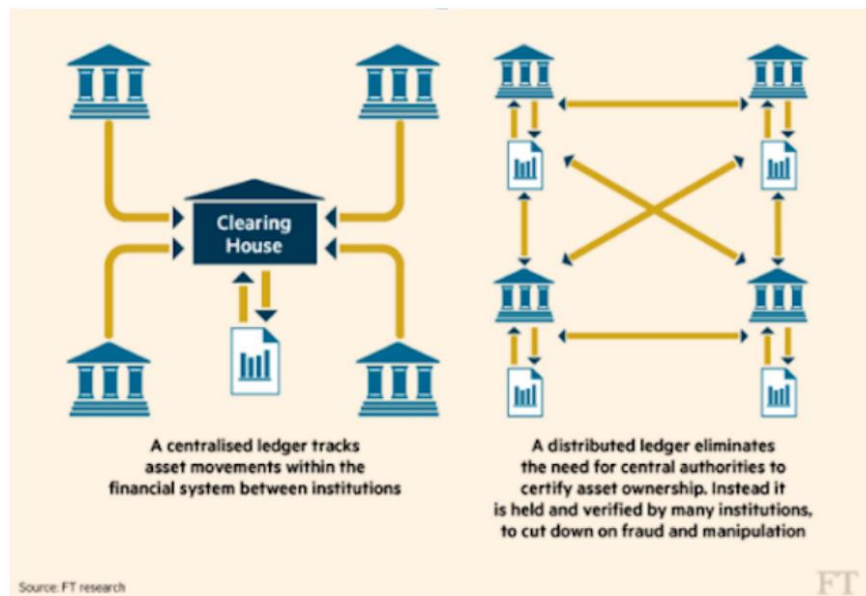


Figure 3: Decentralized versus Centralized Data Stores

Let's take a look at the public blockchain as an analogy. It is both a database and a software that envelopes it. As a software, it is like a BitTorrent, a program that allows you upload and download files directly with others also running the BitTorrent software. So instead of uploading the file to file sharing Service, such as dropbox and then sending the link to your peer to download the file, you just upload the file directly to your peer's computer. Figure 3 illustrates the key configurational differences between a centralized and decentralized data storage.

The public block chain is also a peer-to-peer program with one very important difference, not only does it move files (data) from peer-to-peer (p2p) within a network, it also ensures that all the participants have same exact data. It enforces the following principle, if the data changes on one machine, it changes on all machines. In addition, the public block chains like Bitcoin and Ethereum, new data is appended on to the old which means data is only written, never deleted.

A public block chain is not stored in one central computer, nor is it managed by any central entity, instead it is distributed and maintained by multiple computers or nodes. This is how the term **blockchain** was coined as the new data is added in batches or blocks and appended to an existing block. The public blockchain has no central authority to manage usernames and passwords instead it uses cryptography. In generic way, each user is able to generate a locker address (ID) and a private keycode that allows them to unlock the locker (ID). The primary keycode is unique to the user who generated address (ID). Now everyone in the blockchain can see the data tagged with the address (ID), however no one is allowed to modify it. It can be modified by the person who can prove that he is the owner via the private key.

It is this property of blockchain that the valuable data is recorded as a permanent, immutable, tamperproof uncensored record. The value that the block chain technology brings is “trust in an un-trustable environment”. This trust is established throughout the Distributed Ledger and larger the network the greater the trust.

Distributed consensus: Mechanism for validation of value transfer without trusted third party

A blockchain is a decentralized peer-to-peer system with no central authority figure. While this creates a system that is devoid of control from a single source, it still creates a major problem. And its not clear as How are any decisions made? And how does anything get done? In a normal centralized organization, all the decisions are taken by the leadership team but this isn’t possible in a blockchain system because a blockchain has no “leader”. For the blockchain to make decisions, they need to come to a consensus using “**consensus mechanisms**”.

Before we discuss some of the consensus mechanisms used in cryptocurrencies and in some Blockchain implementations such as Hyperledger, we first describe the underlying mechanism through which consensus works in peer-to-peer blockchain networks. In a blockchain system, there are generally many publishing nodes competing at the same time to publish the next block which updates the transaction ledger. These competing nodes are generally mutually distrusting users (more so in permissionless blockchain systems) who know each other only by their public addresses and have joined the network without any screening process. In this setting, it is natural for nodes to be motivated by their self-centered gain rather than for well-being of the other nodes or the network itself. In such a situation, why and how would consensus emerge in this type of network? Furthermore, who and how resolves conflicts when conflicts arise among nodes about updating the transactions or the publishing a block at approximately the same time? In blockchain systems, the role or use of consensus models is to enable a set of mutually distrusting and self-centered users or nodes to work together to achieve a common goal.

When a node joins a blockchain network, it agrees to the initial state of the system which is recorded in the genesis block which is the only pre-configured block in the system and is the first block that is published. Thereafter, every block is added to the blockchain after the genesis block in a chronological manner through an initially agreed-upon consensus mechanism or protocol, wherein each added block must be valid and thus can be validated independently by each blockchain network node. By combining the initial state (genesis block) and the ability of nodes to verify every block since then, nodes independently agree on the current state of the blockchain. In practice, all this is coded in software and the nodes do not need to be aware of these details. This leads to the key feature of blockchain systems wherein there is no need to have a trusted third party for updation of records to provide the current state of the system—every user within the system can verify the system’s integrity.

While in permissionless blockchain networks, the consensus protocols must work even in the presence of malicious nodes and non-trusting nodes where some nodes might try to disrupt or take over the blockchain, in permissioned blockchain networks, there may exist some level of trust between publishing nodes. In this case, there may not be the need for a resource intensive distributed consensus protocols. Generally, as the level of trust in the network increases, the need for resource usage as a measure of generating trust decreases, but so does the presence of trusted-third party. For some permissioned blockchain systems, the

consensus protocols are not limited to ensuring validity and authenticity of the blocks but includes the systems of checks and validations from the proposal for adding some transactions a block to its final inclusion on a block.

There are a large number of distributed consensus protocols that have been proposed by the academicians as well as blockchain/cryptocurrencies practitioners. At a high level, the consensus protocols can be classified in four groups:

- **Computational power driven consensus protocols: Proof-of-Work:** The core idea behind computational power driven consensus protocols is that the nodes that propose to publish a new block (add a new block to the blockchain) need to solve a computationally challenging puzzle and those who are able to solve that puzzle first get the opportunity to publish or add the block. Bitcoin and Ethereum employ proof-of-work distributed consensus protocols
- **Stake in the system driven consensus protocols: Proof-of-Stake:** The security of proof-of-work systems directly depends on the amount of computational work expended. The growing hash rate in the Bitcoin network, for example, makes attacks on the network costly. This security comes with significant economic cost: It is estimated that—in 2013—the amount of energy allocated towards bitcoin mining (in terms of electricity cost for the operation of CPUs and cooling systems) equaled that of the country Ireland. In light of the cost associated with proof-of-work consensus, proposals have been brought forth for a consensus mechanism centered around a different economic set. Proof-of-stake systems distribute state transition rights, among others, according to existing balances held by an account (the “stake” in the system). Delegated Proof-of-Stake is a modification of the base protocol where the nodes are allowed to delegate their stakes to another node and it can lead to further reduction in resources in reaching consensus. Ethereum Casper uses Proof-of-Stake consensus protocol.
- **Inter-Network relationship driven consensus protocols: Byzantine Agreement:** Another method for establishing consensus in a distributed setting is Byzantine Agreement. Byzantine Agreement comprises a class of systems that try to solve the Byzantine General’s Problem, first described by Lamport, Shostak, and Pease, in which consensus has to be established in the face of arbitrary failures of participants. These “Byzantine” failures can include malicious actors making incorrect statements, as well as statements being lost, e.g. due to technical problems. Two prominent methods for establishing Byzantine Agreement are Practical Byzantine Fault Tolerance (PBFT), and Paxos. Ripple uses probabilistic voting mechanisms and Stellar consensus protocol uses federated byzantine agreement protocol.
- **Other consensus protocols driven by other economic consideration:** There are many other consensus protocols which have the potential to be used in blockchain systems but have not yet attracted enough attraction from industry. These are proof-of-activity protocols, proof-of-burn protocols, proof-of-capacity protocols, proof-of stake velocity protocols, and proof-of-bandwidth protocols.

Business Value Layer: Smart Contracts

First coined by Nick Szabo, a cryptographer and digital money evangelist, the phrase ‘Smart contract’ has come to represent the new generation of applications that run on Blockchains as a part of decentralized application. Smart contracts embed the mutually accepted business logic of the transactions undertaken by

transacting parties and are stored on all the nodes that are a party to the transactions. The smart contracts are triggered based on certain events that are programmed into the contract to undertake certain actions and effect value transfers. They are cryptographically secured to ensure that the authenticity of the transacting parties and also address the confidentiality associated with the information stored and exchanged as per access controls that are coded into the program.

Smart contracts are an essential component of automation that enables digital identities on the Blockchains to conduct varied transactions and undertake coordinated value transfers once certain conditions are met. While the term ‘Smart contract’ is widely used, it is termed differently in different blockchain systems. For example, in widely used enterprise applications in Hyperledger Fabric, smartcontracts are written in ‘Chaincode’ that codifies and embeds the business logic in enterprise Blockchain systems.

Smart contracts are the layer that has the most economic value in business as well as governmental applications of the blockchain technology. This layer leads to not only reduction of the transaction costs significantly, but also leads to minimize contractual disputes and litigations. The feature of Turing-completeness allows the creation of customized smart contracts, which inturn makes it possible to develop applications in different industries such as e-commerce, financial services, asset management and real-estate.

So what is a smart contract and what makes it smart? A smart contract contains a computer code that converts a set of rules or terms and conditions for execution of a business trasction agreed upon by two or more parties that are involved in value exchange, into a computer executable program. This program executes on the top of a blockchain where the value transfer is recorded without the authentication and verification of the trusted third party when the transaction is executed conditional upon well defined condtions coded in the program. In other words, if a set of pre-defined rules are met, the smart contract executes itself to produce the output which is recorded on blockchain. Therefore, this small program or piece of code allows decentralized automation by facilitating, verifying, and enforcing the conditions of an underlying agreement. Smart contracts are key to creation of ‘network of value exchange’ without a trusted third party. The computer code running on the top of blockchain allows exchange of value including any asset in a decentralized yet fully secure and transparent manner, thus eliminating the need for a third party or middleman, without any chance of contractual dispute.

In the current state of technology, getting a court-registered document as a proof, one would first need to go to a lawyer or notary, pay them for their services and then wait till they authenticate the document. However, with blockchain technology the scenario changes completely. When this process is exected with smart contract, one would simply get the document by only making the payment for the asset that is recorded in the document and not for services of any third party such as a lawyer. Therefore, smart contracts not only define the rules around any agreement but they are also automatically execute those rules, transfer value and update the asset ownership records.

In other words, Smart contracts are automatically executable lines of code that are stored on a blockchain which contain predetermined rules. When these rules are met, these code executes and provides the output. In the simplest form, smart contracts are programs that run according to the format that they’ve been set up by their creator. Smart contracts are most beneficial in business collaborations in which they are used to agree upon the decided terms set up by the consent of both the parties. This reduces the risk of fraud and as there is no third-party involved, the costs are reduced too. In summary, smart contracts are computer code that has the properties of self-verification, self-execution and are tamper proof as they are recorded on blockchain.

In order to understand how a smart contract works, let's take an example where you wish to sell a property of your own. The process of selling properties demands a lot of paperwork as well as communication with multiple parties. Other than the communication complexity, it also involves the risk of frauds. In the current times, most of the people who want to deal in properties make their way ahead through real-estate agents. These agents are responsible for dealing with the paperwork and markets. They act as intermediaries in the overall process and work on negotiations and overseeing deal.

In such cases, you can't rely on the person that you're dealing with therefore, the agencies provide escrow services which transfer the funds from one party to the other. When the deal is finalized, you will have to pay both, the agent and the escrow service their commission in terms of the decided percentages. This leads to an extra loss of money and more risk on the seller's end. Enter Smart Contracts. Using smart contracts in such situations can result in more effectiveness by reducing the burden. Smart contracts are designed to work on condition-based principle (if this then that), which will resolve the ownership issue by transferring it to the buyer only when the monetary, as well as other conditions, are agreed upon. Moreover, when it comes to escrow services, smart contracts can replace those too.

Both money and the right of possession of the property can be stored in a distributed system which can be viewed by the involved parties in real-time. Since the money transfer will be witnessed by all the network participants, the chances of fraud are eliminated. Moreover, there's no chance of an intermediary to be involved as the trust between parties is not an issue anymore. All the functions performed by the estate agent can be coded into the smart contract, thus, saving a considerable amount of money on both, buyer and seller end.

By applying smart contracts in our day to day life, we can make phenomenal changes as they offer multiple advantages over the traditional contracts. Smart contracts are more convenient and faster which make those acceptable for people to streamline their workflows.

They provide you with the right blend of security and ease of application as and when you need to exchange anything of value be it property, money or shared.

Eliminating the need for intermediaries make smart contracts even more attractive to apply in our lives. The usage of smart contracts is likely to gear up with the advancement of technology. Let us look at the benefits offered by smart contracts:

- **Transparency**

One of the core characteristics of smart contracts is transparency. Smart contracts describe all the terms and conditions in absolute detail and these are also checked by the parties agreeing to the contract.

- **Time-efficient**

In order to go ahead with any process involving documentation, it usually takes more than at least a couple of days. The delay in processes is due to a lot of intermediaries and unnecessary steps along the way. On the other hand, smart contracts are run through the aid of the internet as they are nothing but pieces of software code.

Therefore, the speed of completing transactions through smart codes is way too fast. Smart contracts can save hours or even days as compared to any traditional business process. Moreover, the time delay due to manual involvement is also eliminated.

- **Precision**

A smart contract is coded in such a way that it holds all the terms and conditions of exchange of assets or completion of a transaction. Leaving out any condition in the smart contract may result in an error in execution.

- **Safety and Efficiency**

Smart contracts with automated coding features are the safest options when it comes to data encrypted technology in the current times. Since they match the highest safety standards, the level of protection involved in them allows them to be secure to use for critical processes.

Moreover, since the smart contracts are so accurate and secure, their level of efficiency is way too high which generates more value in transactions.

- **Data Storage**

Smart contracts are accurate and precise to the minutest level of the agreement. All the details of any transaction are stored on the contract and anyone among the involved parties can access it at any given time. Moreover, these transactions are stored on the blockchain in the form of future records. This is particularly helpful in terms of any dispute regarding the contract terms in the future.

- **Savings**

Using smart contracts in place of traditional agreements can result in a lot of savings. First and foremost, as smart contracts only involve parties that are the part of the agreement; the need for middlemen is eliminated and the money involved in that is also saved.

All the lawyers, witnesses, and intermediaries have no role when smart contracts are used. Moreover, as stated earlier, smart contracts also save money as paper-based documents are not involved in any processes.

- **Trust**

The properties of transparency and security make smart contract trustworthy in businesses. They obliterate any probability of manipulation as well as manual errors and establish confidence in their execution. Upon agreement on all the conditions, the contract automatically executes itself.

Another unique feature of these contracts may be their capability to significantly lessen the requirement of litigation and courts. Self-executing Smart Contracts allow parties to commit and bind by the conditions and rules written inside.

- **Paperless**

As smart contracts are computer coded documents, the use of paper in the entire processes is eradicated. On one hand, this saves the cost while on the other, this is useful for companies globally as it helps them to save their bit of paper usage in terms of contracts and promotes their contribution towards the society.

Applications of Smart Contracts

Be it a new job or buying any new product, contractual agreements come into play as a proof for such things. However, the complex process of traditional paperwork and contracts involve high costs, third parties and chances of manual errors in such processes.

With digitization and technology moving ahead, we can make these processes more reliable and cost-effective with the help of smart contracts. The concept is to avoid any intermediaries and third-party systems and make the systems more effective and efficient. Smart contracts can be applied in different industries and sectors. Let's have a look at some of them below:

- **Insurance**

Lack of automation in insurance administration, claim processing can take a long time ranging from weeks to months. This becomes an issue for both the customers as well as the insurance companies as the customers are trapped in time constraints for their money. On the other hand, the companies have to face issues like unwanted administrative costs, dissatisfied customers, and inefficiency.

By using Smart contracts in such processes can result in simplifying and streamlining the processes by automatically triggering payment for a claim when certain conditions are met as per the client and company's agreement. For example, in case of loss due to a natural disaster, smart contracts can be executed in a timely manner and people can claim their money and use them in time of need. Any specific details like the extent of loss due to damage can be kept on a blockchain and the amount of compensation can be decided accordingly.

- **Internet of Things**

The IoT technology is being utilized to connect everyday devices to the internet in order to improve the interconnectivity of the systems in with the help of sensors. These devices can be connected to the blockchain system to keep a track of all the products and processes in the loop. For example, in a general scenario, you might receive a wrong order while shopping something online but with the combination of Blockchain and IoT, the product and its location can be tracked on every step of the way including the warehouse, transport, shipping to your doorstep. A fully-automated system will ensure that the right product gets delivered to the right person.

The sensors involved in the system create their own nodes on blockchain and with the help of smart contracts, the location and possession of the respective product can be traced. A smart contract keeps the location status updated all along the way till the product gets delivered. This helps in ensuring the correctness of the product from the initial shipment to delivery.

- **Mortgage Loans**

Mortgage agreements are complex as many details are included in them such as income of the mortgagee, credit score as well as outgoings. In order to go ahead with mortgage loans, it is extremely necessary to carry out the checks on these details. This process often goes in the hands of intermediaries and third parties which makes it lengthy and troublesome for the lender as well as the loan applier.

Using smart contracts in this situation is beneficial due to multiple reasons. The most important being the elimination of the middlemen to avoid any lengthy process and confusion. Moreover, all the details can be stored in one location which is accessible by both parties at all times.

- **Employment Contracts**

Employment contracts are another area where smart contracts are needed. If either of the party i.e. the employer or the employee fails to meet the set expectations, the terms of the agreement can be compromised. This leads to a lack of trust which is solved by smart contracts. By using a single smart contract for both the parties, the terms, and conditions can be made clear which would help improve fairness. These records could be anything such as salary amount, job responsibilities etc. Once these transactions are recorded on smart contracts, they can be looked into in case of any conflict. This will improve the employee-employer relationship.

Moreover, smart contracts can be utilized to make wage payment processing easier so that the desired employee receives the agreed amount in a specific time period. Also, in the case of temporary labor where the employer, employee and an agency is involved, smart contracts can be used to introduce transparency. This will prevent the agencies from interfering with the contract term of the employee once he/she is hired by the company. Any changes in terms can be detected with the aid of smart contracts.

- **Securing Copyrighted Content**

In the digital world of today, content is not limited to just words. It could be anything from a written document to a video to an audio clip. When a piece of content is released commercially, the owner of the content receives a royalty fee theoretically. However, the process of creation involves multiple parties and thus, all of them are liable for payments or royalty. In practical implication, this is not ensured as there is no defined way of clearing the confusion over entitlement. Smart contracts can resolve this by ensuring the royalties to the desired contributor by recording the ownership on a blockchain.

- **Supply Chain**

Supply chain management involves the flow of goods and products from the initial stage to the final stage. Being a major part of many industries, proper functioning of a supply chain is crucial for businesses. Supply chain management is not a one person job to do and thus, there are different entities involved in it. Smart contracts in the supply chain can record ownership rights while the products are transferred through the supply chain. Everyone in the network can track the location of the product at any given time.

The final product can be checked at each stage throughout the delivery process until it reaches the end customer. If an item is lost in the process, smart contracts can be used to detect its location. Also, if any stakeholder fails to meet the contract terms, it would be transparent for the whole system to see. Smart contracts bring transparency to the overall supply chain system.

Smart contracts have certain advantages for many industry sectors such as, reducing overhead costs, providing transparency, and saving time. While they are more reliable, secure, efficient and trustworthy as compared to paper contracts, care needs to be taken to avoid the risks of code corruption and as businesses move forward and accept digital processes, risk awareness is integral too.

Types of Blockchain: Apart from the public blockchain described above, there are different categories or types of blockchain that have emerged as companies started to use the technology for the purposes of data storage, identity, agreements, property rights etc.

- **Public blockchain** – Public blockchains are open networks that allow anyone to participate in the network, hence the name ‘public’. Such a network depends upon the number of participants for its

success, and hence encourages more and more public participation through an incentivization mechanism. The best example of a public blockchain is Bitcoin where participants in the network (miners) are rewarded with BTC tokens and anyone can join as a node to transfer (including to buy, sell or hold), or to mine, or to just be an observant node.

- **Private blockchain** – Limited within an organization to be able to access and update. Fully private blockchain is a block chain where write permissions are kept centralized to one organization. Read Permissions public on restricted to an arbitrarily extent. Application or used of a private blockchain includes database management and internal auditing.
- **Consortium blockchain** – It is used in collaboration with other. A consortium blockchain is a distributed ledger where consensus process is controlled by preselected set of nodes. For example, R3 (www.r3dev.com) a consortium of financial institutions dedicated to developing blockchain technologies for financial sector where each member operates as a node. The right to read the blockchain may be public or restricted to the participants.

Table 1 describes the key differences between traditional centralized database driven systems, permissioned blockchain systems and permissionless blockchain systems. In summary, the key characteristics of blockchain systems are as follows.

Key characteristics of Blockchain:

- **Distributed Ledger:** In blockchain systems all data is stored in each node of the network, in other words, in distributed ledger, which is maintained and updated by nodes in the network instead of being stored in a single computer with restricted access and the updation rights are permissioned by a central authority.
- **Cryptographically connected blocks:** The data security and immutability is ensured by connecting blocks through the hashing algorithm (Example SHA256) of the previous block being stored in the current block along with the data. Using merkel trees to connect and stores blocks along with digital signatures and use of private and public key to create identities allows for confirmation of unique ownership of assets and prevents double-spend problems.
- **Decentralized Validation Process:** Transactions are approved and authorized by a tested democratic process known as distributed consensus mechanism which ensure that only transactions approved by the honest nodes are added to the new block. This ensures Trust between Transacting Parties without Intermediaries.






Table 1: Comparison of traditional and blockchain based systems

Comparison of Centralised & Blockchain approaches			
Feature	Centralised Databases	Permissionless Blockchain	Permissioned Blockchain
Ledger	Centralised in one location with replication	Distributed across all nodes. However nodes have the option to carry the entire ledger or part ledgers & select their clients accordingly.	Shared between transacting parties on a need to know basis
Confidentiality	Highest level of confidentiality possible	Information on transactions, open to all	Access control on a need to know basis
Identities	As per organisational rules can be linked to normal identities & hence if data is leaked, there is a threat of loss of highly valuable customer information & confidence	Algorithmically linked Public & Private keys of pseudonymous or anonymous identities, protecting the link between transactions and actual identities	Generally linked to roles and operated through secure identities, with Public & Private keys normally based on X.509 certificates
Immutability of ledger data	Can be changed by any authorised party anytime	Considered immutable unless a massive 51% attack takes over the Blockchain and rewrites dat. Hence, considered improbable	Changes of ledger contents can be modified by appending new contracts & trail of same is recorded ensuring transparency. Data can however be erased permanently through appropriate programming of smart contracts.
Smart Contracts	Not applicable. Data is uploaded and appended s per interactions with normal applications within the organisation	Smart contracts or new generation applications that reflect real life agreements, executed by external accounts or invoked when certain conditions are met, help in autonomous functioning of Decentralised applications (DAPPs) that enable DAOs (Decentralised autonomous organisations)	Processes across organisations or real life entities are automated & agreements enforced through 'Smart Contract' or 'Chain code' , a new generation application that enable elimination, of intermediaries, corruption, fraud, wastage of resources like time, money & paper. Shared ledgers are updated as a consequence.
Provenance	Not a feature, as there is no chain of data structures stored with time stamps	Provenance of the data recorded is available as every tranaction and appended blocks are timestamped before committing. Every item can be traced back to its origin	Provenance of the data recorded is available as every transaction and appended blocks are timestamped before committing. Every item can be traced back to its origin
Speed of Transaction processing	Instantaneous with no limits. Since an organisation trusts itself maximum and the databases are operated by responsible officials, instantaneous updations happen.	Slow as all participants are considered potential attackers with lowest level of trust and hence highest effort is needed to confirm traansactions.	High Transactions speeds are possible as the participants are trusted and traceable & hance not prone to mischief.
Vulnerability to Malware & Cyberattacks	Highly risky as it provides highest incentive to attack Centralised databases for ransomware or disruption. Best of the global leaders having highest level of cybersecurity have been attacked.	Highly resilient. However, smart contracts and associated infrastructure like wallets, exchanges etc., are prone to malware attacks if they are centralised entities. 515 attacks are possible on smaller & newer Blockchains.	Highest level of security as the data and applications are protected through multiple layers of security mechansims as the identities and transactions are undertaken after ta thorough validation. Secured cloud service providers provide an added layer of safety to Blockchain infrastructure.
Recommended Approach	No need for Blockchain	Prohibited in India, Considered risky	Approved & Recommend usage with regulaory oversight

Before, we describe business applications of blockchain technology, the following table reproduced from a report from Mackinsey Digital highlights the key myths and reality about various aspects of blockchain technology.⁵

⁵ McKinsey Digital, Blockchain beyond the hype: What is the strategic business value?, June 2018, Exhibit 1. https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Blockchain%20beyond%20the%20hype%20What%20is%20the%20strategic%20business%20value/SVGZ_Blockchain-beyond-the-hype_ex1.ashx

Five common blockchain myths create misconceptions about the advantages and limitations of the technology.

1 	Myth	Reality	
	Blockchain is Bitcoin	● Bitcoin is just one crypto-currency application of blockchain	● Blockchain technology can be used and configured for many other applications
	2 	Blockchain is better than traditional databases	<div data-bbox="576 535 950 682">● Blockchain's advantages come with significant technical trade-offs that mean traditional databases often still perform better</div> <div data-bbox="966 535 1388 682">● Blockchain is particularly valuable in low-trust environments where participants can't trade directly or lack an intermediary</div>
	3 	Blockchain is immutable or tamper-proof	<div data-bbox="576 724 950 829">● Blockchain data structure is append only, so data can't be removed</div> <div data-bbox="966 724 1388 913">● Blockchain could be tampered with if >50% of the network-computing power is controlled and all previous transactions are rewritten—which is largely impractical</div>
	4 	Blockchain is 100% secure	<div data-bbox="576 955 950 1060">● Blockchain uses immutable data structures, such as protected cryptography</div> <div data-bbox="966 955 1388 1081">● Overall blockchain system security depends on the adjacent applications—which have been attacked and breached</div>
	5 	Blockchain is a "truth machine"	<div data-bbox="576 1123 950 1249">● Blockchain can verify all transactions and data entirely contained on and native to blockchain (eg, Bitcoin)</div> <div data-bbox="966 1123 1388 1281">● Blockchain cannot assess whether an external input is accurate or "truthful"—this applies to all off-chain assets and data digitally represented on blockchain</div>

4.0 Application Domains

Blockchain can replace trusted intermediaries and also in some cases help efficiently increase their transparency, security, or reliability of their performance. Through the decentralized approach, smart contract triggered real-time & automatic execution of transactions that enforce contractual obligations, offering an immutable ledger of assets that track the changes in ownership, Blockchain facilitates a new paradigm of transparency and automation at scale. Many a time, there is often a grey area between the suitability of a situation for a Permissioned Blockchain application that offers an alternative to a normal database application. Simply converting applications to run on a Blockchain instead of traditional databases would not necessarily add value, and in fact, would likely be inefficient and costly.

The myriad of applications that Blockchain facilitates are described below. This list is only illustrative and not exhaustive.

4.1. Blockchain in Financial Applications

Individual transactions and cross border payments for large transactions can be effected through a private Blockchain where counterparty banks are members, drastically reducing costs and improving efficiencies. Globally, several banks are forming consortia to take advantage of Blockchain technology for efficient cross-border money transfers. Ripple Labs and R3 Corda have led these consortia globally, and SBI-led consortium, among Indian banks, is exploring its use case actively. In India, organizations like Bajaj Electricals with the help of YES Bank, and Mahindra and Mahindra group, through its group company Mahindra Finance, are exploring trade financing through Blockchain technology.

For Blockchain to have a wider impact in the finance domain, it is important that a large number of parties transacting with each other come on board on a common Blockchain platform. This is still a long way off, and several organizations are still working on their proof of concepts. Some of the prominent applications of Blockchain are detailed as follows:

1. **Cross-border remittance:** Cross-border remittance is often a time-consuming process as it involves multiple countries, banks and regulatory and non-regulatory agencies. This results in delays and a lot of documentation & high transaction charges across the various parties. A Blockchain connecting interested parties as nodes on either side of the border, and also regulatory agencies as participants, can speed up the process significantly. However, the financial organization serving as the intermediary has to be in tune with the regulatory environment to avoid any legal issues.

The solution offers the following benefits:

- Details of the customer transferring the money, and the one receiving money can be cryptographically encoded to ensure their details are confidential and known only to relevant parties on a must/ already know basis
- Instantaneous transfer of money through smart contract operation
- Reduced transaction fees by cutting down on irrelevant intermediaries

In the recent past, there have been a number of such initiatives led by JP Morgan, Facebook lead consortium, R3 Corda have been announced in the names of JPM Coin, LIBRA, Corda Settler, etc., to facilitate a speedy and ultra-low-cost transfer of money among participating banks & entities of their Blockchain consortiums.

2. **Bill discounting:**

Invoice discounting is often undertaken by medium and small-scale industries dealing with large creditworthy organizations. The process involves a lot of documentation and time-consuming procedures. Here, Blockchain can offer a solution by offering trust through a smart contract, and by cutting down a number of mediators between parties.

The solution involves a regulatory node having oversight to ensure transaction sanctity without intruding into the confidentiality of transactions.

3. **Insurance:**

The following are some use cases emerging in the insurance domain.

- Automated comprehensive background and authenticity verification of all things insured

- Automated claim handling and settlement
- Elimination of insurance fraud due to transparent recording and immutable data sets on the Blockchain that removes the propensity to defraud insurance companies with inflated and multiple claims
- Automated insurance settlement through smart contracts that get triggered on impacting events.

The Government of Singapore has implemented Blockchain-based medical insurance for a segment of its population on a pilot basis. An Ethereum based private Blockchain is implemented to connect health insurance providers, hospitals and banks. When a patient in a given risk category signs up for an insurance plan, the details are recorded on the Blockchain.

In case a patient undergoes a procedure and needs to avail insurance, the smart contract gets triggered and the money is transferred from the insurance company to the hospital within 24 hours to clear the bills. This has substantially eased the pain point of patients who are often unsure about the settlement of claims.

4. **Trade finance on Blockchain:**

Companies seek credit from banks and finance companies for

- Working capital
- Manufacturing costs
- Temporary spurts in the demand

For this, they have to provide extensive documentation to banks, leading to high costs, and also payments to intermediaries to facilitate documentation, relationships, contacts, and other logistical issues.

With the help of Blockchain, companies can directly transact with banks securely, with limited paperwork in a high-trust environment.

The use of Blockchain technology helps in the following aspects:

- Reduction in transaction costs due to the elimination of middlemen.
- Trust through the system as all transactions are recorded on a distributed ledger with established identities and are time stamped.
- Transparency and elimination of duplicity or mistakes in invoices as all records are managed through a streamlined process and verified formats that are encoded into the system.
- All parties can operate in a safe and efficient environment, devoid of human dependency.

4.2. **Digital Identity Management**

In recent times, there has been a renewed interest in the identity problem, both online and offline. On one side, there has been a higher concern for the privacy of communications due to extensive governmental surveillance programs and by the rise of social networks. On the other side, the on-going migration crisis has brought challenges for both humanitarian and security agencies trying to identify migrants where previous data is either lacking or it cannot be trusted. (Source: Provable)

Creating a unified digital identity on a Blockchain platform is one of the biggest applications being experimented across the globe. Identities recorded on a Blockchain enable the member to access their benefits or entitlements in an authentic and secure manner not only eliminating a lot of intermediaries

engaging in the identification process, but also ensuring that the right benefits are reaching the right person entitled to them.

An Indian state has successfully experimented with a benefit distribution program of offering targeted benefits to students. This has substantially reduced the menace of fake, wrong and unaccounted claims availed in the name of non-existing parties through forged identities.

World Food Programme's aid disbursements to Syrian refugees: The World Food Programme created a private Blockchain fork of Ethereum with the help of engineering firm Parity and is transferring aid to Syrian refugees directly.

World Food Programme earlier provided vouchers as an aid to refugees, which they used to encash in retail outlets and supermarkets against their purchases. This amounted to huge leakages on account of wrong voucher submissions, bank charges, and time delays.

With the help of Blockchain, refugees are provided accounts on the Blockchain, identified by the scanned images of their irises. Upon purchasing any item at a supermarket, the refugees are identified by iris scanners and the due amount is charged to the World Food Programme.

This has saved the WFP over 98 percent in the bank and other financial charges, and now, it plans to spread the same to refugees across regions for a variety of services.

KYC/AML services undertaken by the financial organization to qualify their customers, clients and merchants can be automated and standardized through a Blockchain application improving the convenience of the transacting parties in a number of ways. The citizens with KYC and identity recorded and tracked through a Blockchain can get an idea of the places where his identity has been accessed, which further can be enabled by his/her access.

4.3. Blockchain in Supply Chain applications

The supply chain industry consists of several non-trusting parties interacting with each other, exchanging a humongous amount of information through documents. The application of Blockchain to the supply chain industry promises a huge benefit in terms of streamlining of operations, speedy and efficient processes, and elimination of time, effort- and money-consuming paperwork.

Blockchain can enable direct interaction among various parties in a supply chain, establishing program-driven trust and eliminating intermediaries. One example could be the tracking of refrigerated goods by recording the temperature across the value chain with the help of IoT devices. Further, the movement of goods from the manufacturer to the end consumer, along with the various parameters associated with the goods, can be tracked on a live basis with IoT sensors and devices tagged to the goods. This will further help in the elimination of fake products as their ownership can be traced.

In the pharmaceutical industry, it would be possible to track the movement of a medicine strip across the value chain - from the manufacturer to the last distribution point - proving the source, and differentiating it from a fake.

Similarly, in agriculture, produce can be tracked from farm to fork, and IoT technology can be used to monitor storage conditions like temperature to ensure it is not spoilt along the way.

IBM & Maersk led consortium Travelens, Walmart Led consortium Food Trust and Samsung & port of Rotterdam consortium Deliver have made substantial progress in the recent past to create a cross border, multi-party blockchain systems in the Supply Chain and Logistics domain.

4.4. Blockchain in Manufacturing

A lot of activity in Blockchain technology is centered on financial applications, asset tracking, and supply chain. The application of a framework to identify various aspects in the manufacturing sector gives us an idea of the segments that are amenable to the application of Blockchain technology. As per an assessment, at least four out of six aspects governing the relationship between the parties must be met, as given in the Table 3.

An overview of the use cases across various segments of manufacturing, along with the current use cases, as sighted in the mentioned paper by Philip Sanders are given in the Table 3. The activities that may see strong benefits from Blockchain technology are mostly in the proof of concept stage, and their real economic impact can be felt in three to five years.

The activities that may see strong benefits from Blockchain technology are mostly in the proof of concept stage, and their real economic impact can be felt in three to five years.

The activities that may see strong benefits from Blockchain technology are mostly in the proof of concept stage, and their real economic impact can be felt in three to five years.

Table 3: Blockchain applications in manufacturing

Blockchain applications in Manufacturing industry- Some examples		
USE CASES	EXAMPLES	DESCRIPTIONS
Supply Chain Management and Digital Product Memory	1. IBM and Maersk	Tracking of containers during the shipping process
	2. Provenance	Recording of all important product information throughout the entire supply chain
	3. Everledger	Registers certifications and transaction history of diamonds on Blockchain
Internet of Things and Industry 4.0 applications	1. Factom Iris	IOT device Identification over Blockchain
	2. Super Computing Systems	Sensors that timestamps data on the Blockchain to save them from manipulation
	3. Tile data Processing tile pay	Marketplace to allow customers to sell their data from IoT devices
	5. IOTA	Cryptocurrency and Blockchain protocol especially developed to meet the demands for IoT applications
	6. IBM Watson IOT	Platform to save selected IoT on a private Blockchain and share it with all involved business partners
3D Printing	1. Genesis of Things	Platform to enable 3D printing via smart contracts
	2. Moog Aircraft Group	Ensuring safe 3D-printing of aircrafts parts via Blockchain

4.5. Educational certificates & Student / Employee credentials

Blockchain has extensive applications in the education sector. Every year, millions of certificates are issued by various institutions to students across the world, which are used as credentials for various purposes. It is imperative to have a fool-proof process to confirm the authenticity and originality of these documents. Blockchain now offers a platform for organizations to confirm the authenticity of these documents electronically. For this, organizations who give out the certificates record them in a Blockchain. Any party looking to confirm the authenticity of a certificate can verify the same by comparing it with the original. For this, the property of ‘Hashing’, which generates a unique hash for a unique digital document, is used, and hashes of the original and presented documents in conjunction with the digital signature are compared, and the originality ascertained if the hashes are identical.

Apart from this, teachers and students can discover each other and offer peer-to-peer training and educational services as well.

Background verification and identity management can also be integrated into the Blockchain platform for educational resources and interactions.

4.6. Blockchain in Healthcare

Blockchain can enable patients to store their electronic medical records in a confidential, safe and secure manner across their lifetime. This enables doctors to have verifiable, tamper-evident medical records with the entire history of diagnostic tests to offer the right prescription. A patient can use his mobile device to access information, and also provide permission to a healthcare provider to access the health data

Blockchain also enables trustworthy Clinical Trial management process by reliably recording the patient consents an activity which is often looked at suspiciously.

4.7. Blockchain in Telecommunications

Blockchain has a great role to play in ensuring compliance of the telecom players to the government regulations that demand them to respect the privacy of their users. Activities like Unsolicited Commercial communications are best monitored with the help of Blockchain and many telecom companies in India are working along with TRAI to arrest this menace with the help of Blockchain technology.

4.8. Blockchain in Government

Digital identities, maintaining digital certificates of citizens from birth to death and that of different types of asset ownership, electronic voting, educational certificates of students for all academic purposes, monitoring welfare programs, tracking procurement of all key products and services across Government departments, protecting patents, copyrights and trademarks, confidential access and tracking of health records of all citizens, cybersecurity of critical infrastructure are some of the key applications of Blockchain technology, being explored by Governments across the world.

Various states in India are in the process of experimenting with Blockchain applications across a variety of use cases.

Tracking the ownership of Land records, issuing Motor vehicle licenses using a Blockchain platform, tracking the utilisation of Benefit distribution program using a Blockchain, maintaining registries of Birth certificates, Death certificates, Marriage certificates, Municipal authority approvals and permissions, Police clearance certificates to citizens for various purposes are some of the use cases being explored and proof of concepts being undertaken by some of the Indian states. An urgent need is felt by the Indian Government to come out with a guiding policy document bringing clarity enabling full-fledged applications being implemented in a coordinated fashion across the country.

4.9. Shared Data Services

Many organizations with conflicting interests benefit from a single repository of data. Users can access their own analysis and decision making. For example, the sensor-generated data from various sensor locations and farms can be utilized by multiple companies who can then create their own layers of applications and dashboards depending on their need. Similarly, details of erratic customers or fraudsters can be shared across multiple service organizations to pre-empt them from becoming victims. Blockchain facilitates the sharing of critical & valuable data on a peer to peer basis, among a consortium of partners in a trusted manner while maintaining the necessary confidentiality through access controls and digital signatures.

4.10. Decentralized Marketplaces

The rise of the social media and e-commerce industries has led to the internet behemoths that have now become notorious in abusing their economic power boosted by the ownership of data belonging to trusted users. Data breaches, malware attacks, and wilful actions have dented the trust of the consumers in such entities and Blockchain offers a credible alternative where a consortium of Permissioned Blockchain system can offer Trust as a Service to guarantee quality & origin of goods and transaction guarantee to the buyers and sellers on the platform. Indian Government is experimenting with a Blockchain-based e-marketplace for Coffee growers to help integrate the farmers with markets in a transparent manner and lead to the realization of a fair price for the coffee producer.

4.11. Other use cases

There are numerous other use cases like

- a) Monetizing intellectual property, arts, music and movie rights to targeted clients
- b) Tracking product warranties
- c) Tracking Industrial Waste & Emissions (at State & National level or even at International Level)
- d) Notarised document management
- e) E-Procurement process management
- f) Loyalty management
- g) Mobile Phone Roaming fraud tracking
- h) Commercial paper & Bonds issuance
- i) Clearing & settlement

and many more that are being explored that facilitate unknown and mutually distrusting parties to confidently trade with each other.

Blockchain Initiatives in India

The following are the Blockchain applications being implemented in India currently:

A) Land records - APCRDA is implementing DLT for recording Land registration. This is being implemented by ZEBI, a Hyderabad based company.

B) University certificate- Zebi is also implementing Blockchain based certificate management for 35 Universities/ Colleges in Karnataka & AP.

C) Unsolicited Commercial Communication tracking: Tech Mahindra along with Microsoft & IBM has implemented a DLT solution for registering customer preferences and tracking customer complaints about the UCC. All the telecom companies and TRAI along with approved Third party service providers and approved Tele-marketers are sharing the data of the preferences recorded & violations as per complaints by customers. Any cellular service provider unable to block such UCC calls will be heavily fined.

D) Some of the states have started coming up with tender notices for Blockchain based Land records management system.

E) Trade finance and Letter of Credit applications have started growing.

HSBC India and ING Bank Brussels have successfully executed a blockchain enabled, live trade finance transaction jointly with Reliance Industries and Tricon Energy on a R3 Corda powered platform.

The blockchain enabled Letter of Credit transaction facilitated shipment between Reliance Industries and Tricon Energy. Industry first integration between an electronic Bill of Lading provider and a

blockchain-based trade finance platform enabled the transfer of title.

F) Bankchain by SBI led consortium is exploring Blockchain for a variety of use cases like shared KYC / AML, syndication of loans / consortium lending, trade finance, asset registry & asset re-hypothecation, secure documents, cross border payments etc.. This is however under a lot of experimentation and has not stabilised.

G) Telengana Government is exploring Blockchain for Motor Vehicle Department applications to track the vehicle lifecycle from manufacturing to end of warranty period & is evaluating some PoCs.

H) West Bengal has implemented Blockchain based issuance of Birth certificates to new borns.

5. Challenges in Adoption of Blockchain Technology

Since the advent of Bitcoin in 2009, blockchain has become an essential part of the discourse of the technology-centric community including entrepreneurs. It is often referred as the ‘biggest disruptive force’ after the World Wide Web and the Internet. In its initial phase, Bitcoin which was built on the top of blockchain technology was a pathbreaking innovation, as it was the first technology that succeeded in creating digital money which can store and transfer value just like any other fiat currency. This led to enormous interest in cryptocurrencies, which in turn led to interest among entrepreneurs and developers towards the applicability of the technology beyond cryptocurrencies.

Currently, technology giants such as IBM, Microsoft, Facebook and Amazon are actively working on myriad blockchain platforms, use cases and pilots. Many Proof-of Concept prototypes have demonstrated that blockchain based systems do increase efficiency and lower transactions costs in key industries such as healthcare, data storage, supply chain, logistics, fintech, cybersecurity, and government services.

Given the active interest in blockchain, and involvement of technology giants, it may appear puzzling that blockchain technology has still not been adopted for any large scale business or government services applications. In other words, the adoption of this technology has been very slow given the promise, interest and the technology being around for a decade or so. As explained earlier, some of the disappointment may be due to mischaracterization of this technology as ‘disruptive’. This is indeed a foundational technology, which takes longer time to scale up, but once scaled up and mature, they transform almost all sectors and business systems.

The initial widespread interest in blockchain was based on its ability to support a digital peer-to-peer currency (unlike fiat currency issued and fully controlled by a central authority) by ensuring trust between actors from all over the globe who do not know or trust each other. For almost a decade, the blockchain technologies were very discussed in terms of its ability to support this new type of currency or so called cryptocurrency leading to an explosion in the Initial Coin Offering (ICO) events. But by the end of 2018,

the interest in ICOs waned due to numerous unscrupulous practices and many quick get rich scams, the trust significantly decreased around anything surrounding ICOs. In a way, this was good for the development of blockchain technology as many financial speculators left the domain but technologists and entrepreneurs who understood that cryptocurrencies are only one application of the technology, continued to work towards new use cases that bring tangible business value.

Furthermore, it is important to understand that blockchain technologies are built on the top of the internet technologies. The Internet technologies took almost two decades before successful e-commerce and content publishing business applications started to emerge at scale and took another two decades to transform and impact each and every business sector as well as government services all across the world. Even if a technology seems to hold the potential to stimulate an increase in productivity and overall quality of life, it first goes through the trial and error phase where enterprises, emerging disruptors, and governments identify and address implementation challenges. Blockchain technologies are in that phase, and identification of implementation challenges is key to formulation of an effective strategy. Below, we describe some of the key challenges in adoption of this technology.

Scalability

Technical scalability of the network is a major challenge of blockchain networks. This can make adoption of such systems in large scale applications very hard.

Lack of interoperability

Various Blockchains have evolved in last many years due to a rapidly expanding industry. A large number of platforms, players and approaches to developing such systems including usecases/solutions have emerged. This has led to some confusion in this space, There is no clear agreed upon approach. Furthermore, there are no standards which allow different networks to talk to with each other.

Lack of awareness and support

A major challenge in the implementation and use of Blockchain technology is a lack of awareness of the technology, especially in sectors besides banking where there is widespread lack of understanding of how the technology functions. It is imperative therefore to determine which organization will act as the thought leader for the country at large and at the industry level.

Lack of frameworks to estimate lifetime costs and measure benefits

The speed at which blockchain networks execute peer-to-peer transactions has cost implications. This also impacts the usefulness and effectiveness of these systems. In the absence of standard frameworks to estimate the lifetime costs and benefits of business use if these applications is very hard. Given that business make capital investment based on a standard cost-benefit analysis, lack of such frameworks for blockchain systems makes it very hard for the senior leadership in firms to make a large investment in adoption of such applications.

Regulation and governance

Government regulations struggle to keep up with advances in technology. Some permissionless blockchain systems like bitcoin bypass regulation. Since one of the promise of blockchain systems is to reduce or even remove the need for central authority, regulators tend to have distrust in this technology..

Integration with legacy systems

Difficulty in integration with a variety of back end systems of various organizations that are part of the Blockchain system. This is because Blockchain connects a number of organizations as an inter-enterprise platform working with organizations with disparate internal systems at varying stages of the lifecycle. Since Blockchain is a newly evolving technology, the various platforms that are in the market keep coming out with frequent upgrades. This poses a challenge for Blockchain implementing organizations, who are already plagued with limited knowledge of the subject to keep the option of adaptability of their applications being developed to future upgrades.

Data Portability

The blockchain systems are such that once data is put into one blockchain, transferring that data to a new blockchain system can be very difficult. This issue has implications for adoption of this technology because firms do not want to be locked-in with one set of technologies or platform with very high switching costs.

Ill-Defined Requirements

Firms adopting blockchain technology need to examine the business, legal, and technical aspects of adoption. Given the early stage of adoption of this technology, there are many questions and concerns users may have for which there are no clear answers. Furthermore, due to lack of frameworks, users face challenges in defining the requirements for the blockchain based system.

User Collusion and Control

Blockchain systems are based on distributed consensus. A large set of users may combine their computing power to collude leading to wrong transactions getting recorded on the blockchain.

User Savviness and Safety

The level of comfort and knowledge that users have about this technology also has implications in its adoption. Many users do not know how this technology works and hype created over the last many years does not help in users' comfort with the technology.

Legal Challenges in Adoption in India

The RBI has imposed a prohibition on dealing in Virtual Currencies⁶ and issued a circular to stop cryptocurrency transactions in India. However, there is a lack of clarity on whether activities involving tokenization also come under the circular's purview. Nonrepudiation requirements in banking regulation

⁶ <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11243>

that require in-person verification for several activities defeat the purpose of implementing a blockchain based technological solution.

The 1st Schedule of the Information Technology Act, 2000 provides that nothing in the Act will apply to any transactions involving immovable property, wills, and negotiable instruments. Since digital signatures are an innate feature of the blockchain apparatus, this provision precludes the applicability of the technology to these activities. Thus, may prevent the end-to-end carriage of real-estate transactions on blockchain enabled technologies.

Privacy as envisaged under Section 43A of the IT Act currently does not provide adequate safeguards for blockchain. The ‘Right to be Forgotten’, a common feature of data protection legislation such as the Draft Personal Data Protection Bill, 2018 is at odds with the fundamental structure of blockchains as data cannot (read should not) be deleted from them.

Localisation: Since public blockchains automatically store data redundancies across all nodes on a network, the technology may hit a hurdle with localization requirements, even if they are restricted to solely critical personal data as is purportedly being mulled over by the Ministry of Electronics and Information Technology (MEITY). Data portability, another requirement in the Draft Personal Data Protection Bill, may also present a challenge as it is presently unclear how this operation can be carried out on a blockchain.

The Draft Personal Data Protection Bill 2018 also allows citizens to modify and amend their personal data. This will serve as a point of friction with blockchain technology that does not allow for the amendment of any data once uploaded. Presently, the law does not account for the security standards used by Blockchain technology nor does it encompass any provisions that ringfence the digital economy from the cyber-security threats presented by blockchains.

Decentralised Autonomous Organisation: “A DAO is a virtual autonomous organization, in which the functions of the organization exist in software, and the laws governing the organization’s functions are set into smart contracts that become automatically enforceable if a set of defined conditions are met. As a result, the DAO becomes a company that runs by itself, without a centralized governing body.”⁷ This framework is not compatible with company law, because it does not fit neatly into the definition of partnership or a company. DAOs also lack fixed jurisdiction so applicability of law is a question of concern and also have lack of clarity on the membership/organisational structure.

There is also lack of clarity on whether ‘digital contracts’ executed on blockchain are recognisable and enforceable by law. There is also a question of what remedies are owed to an aggrieved party if the code underpinning the digital contract is hacked. Ambiguity exists as to whether tokens issued on a blockchain can be categorized as “securities” under the Securities Contract (Regulation) Act, 1956.

Lack of blockchain talent

⁷ <https://www.w3.org/2016/04/blockchain-workshop/report>

Whenever a groundbreaking technology emerges, the developer community needs time and resources to accommodate the new demand. Blockchain is currently still in its infancy, as a result, there is an acute shortage of developers proficient in this technology. The fact that educational institutions have just recently begun to introduce blockchain-related courses, will alleviate the market demand but the results will become palpable only after students will finish their training.

A research conducted by Glassdoor indicates that the demand for blockchain-related jobs has increased by 200% between 2017 and 2018. Having a sufficient pool of qualified developers is a top industry concern. The gap in market demand and current availability of skilled developers is reflected by the higher than average salaries a company is willing to pay to a blockchain professional.

Energy consumption

The majority of blockchains present in the market consume a high amount of energy. This is because Proof of Work, the consensus mechanism used to validate transactions and ensure trust in the network is purposely designed to be difficult and inefficient. This mechanism requires high amounts of computation power to solve a complex mathematical problem to verify and process transactions and to secure the network. The amount of energy consumed by computers that compete to solve the mathematical puzzle has reached an all-time high. Add to this the energy needed to cool down the computers, and the costs increase exponentially.

Concerning this issue, the World Economic Forum published in 2017 a white paper where it states that “Estimates liken the bitcoin network’s energy consumption to the power used by nearly 700 average American homes at the low end of the spectrum and to the energy consumed by the island of Cyprus at the high end. That’s more than 4.409 billion kilowatt-hours, a Godzilla-sized carbon footprint, and it’s by design. It’s what secures the network and keeps nodes honest.”

The large amount of energy required to maintain and run a blockchain network acts as a deterrent to companies that are seeking more viable alternatives. To overcome this issue, many blockchain proponents are developing more efficient consensus algorithms, that are less energy taxing. Furthermore, from a business perspective, private blockchains are more suitable to serve company interests, as they provide restricted access, an additional layer of privacy to protect trade secrets, and are more energy-efficient.

To conclude, blockchain seems to have embarked on an ascending trend. Countries are manifesting real interest in the applicability of the technology in enterprise use cases which signals the fact that blockchain is steadily reaching maturing. The acknowledgment of blockchain’s potential to act as an innovative new paradigm, across multiple industry segments and businesses may soon trigger mass adoption. Although there are still multiple challenges that need to be addressed before witnessing large scale use, the increase in trust and eagerness to tap into the benefits of blockchain means that the technology is on the right track.

6. Societal Impact of Blockchain Technology

Blockchain allows mutually unknown parties to communicate, coordinate, collaborate and cooperate with each other for achieving common goals. By eliminating non-value adding middle parties and wasteful

processes it increases transparency, productivity, security and trust for the citizens and society at large. It has been a well-known fact that societies with high levels of trust have the lowest levels of costs and high levels of productivity and happiness due to convenience and pleasant experiences.

Activities recorded on the Blockchain offer permanent, indelible and tamper-evident records forever. Thus, Blockchain acts as a significant deterrent to those who wish to commit malpractices and also undertake fraudulent activities. This will keep a check to fake products, fake certificates, fake licenses, fake identities, fake scheme beneficiaries, fake drugs, fake claims, insincere commitments and many more avoidable traits and pollutants of our day to day lifestyle. This increases purity & honesty across all our interactions thus substantially improving the quality of life adding to the society's Happiness Quotient.

By automating many activities, facilitating trusted human to machine and machine to machine transactions, Blockchain adds to the convenience and productivity substantially. The sharing economy characterized by many people sharing a given resource at the same time, fractional ownership of assets thus minimizing the idle times and also reducing the stress of unproductive & idle assets that can be substantially boosted with Blockchain.

Voting and consensus are part and parcel of our day to day life in many ways. By facilitating accurate Identity management, authorization and authentication of the votes cast in a confidential manner, Blockchain can help in substantially crashing the cost of conducting elections at the same time, facilitating instant and live results. The unlocking of the resources that were denied to the legitimate producers of goods and services or the beneficiaries of schemes and aids, can lead to a dramatic improvement in the productivity of enterprises and Governments.

Blockchain facilitates auditing and compliance in an easy manner. This helps in releasing a huge amount of resources spent in policing activities, the window dressing of records, Tax administration & compliance and the corresponding infrastructure needed to put such activities in check leading to all-round prosperity.

7. Role of Government

The birth of the Blockchain technology in the form of bitcoin was rooted in the anti-establishment & anti-regulatory approaches it seemed to symbolize. Further, blockchain deals with only digital versions of the physical beings or their assets which is not only abstract to perceive but also cuts across the countries without any boundaries.

Hence it is natural that the existing legal & regulatory regimes see it not only as a threat to their sway over their assets but also as something that can cause their citizens to be victims of unregulated and unaccountable fraud.

This suspicion has caused enormous debates and delays in coming to terms with the benefits of the underlying technology that is now beginning to be understood.

Blockchain deals with digital identities and tracks them through their lifecycle, The digital identities could be things, people, assets, documents, products, intangible assets or ownership rights and the like.

While the activities of the citizens need to be tracked and monitored to make them accountable, the value transfer across the participants should be legitimate and not violate the various laws of the land.

There are three core themes that define the role of government in mainstreaming of blockchain technology:

- **Leadership and vision from government:** Currently there is a need for greater vision and leadership across government regarding the development of technology for a digital-blockchain economy, and India's role in this future economy . Industry leaders believe this technology will be core to the future of the economy as a whole, just as the Internet has become . This foundational economic impact may range from supply-chain logistics management, to finance and insurance, to identity, to government services, and more.
- **Close collaboration between Industry and government:** The technology industry needs to collaborate closely with all levels of government, and clearly communicate the value proposition of blockchain technology and its potential role in the future economy – to address current hype about blockchain technology that can result in misinformation for lawmakers, regulators, lawmakers, and citizens alike . Furthermore, industry needs to demonstrate real production examples of blockchain technology deployment across various segments of the economy, such as supply chain management.
- **Increased research and test-bed deployments:** More resources need to be allocated toward this nascent yet rapidly evolving technology, much in the way the US government funded research into the Internet in the 1970s and 1980s . It was this support from government, combined with a shared vision for a U.S. leadership role in initial Internet communications technology, that allowed the Internet to flourish with broad adoption and become the foundation of the digital economy today. US reaped enormous benefits because of technology breakthroughs through funded research. Any government including that of India needs to take the leadership in funding high-risk research in this nascent technology.

Regulator and Rule maker -

Hence it is imperative that there must be a regulatory oversight on all the identities that are created as digital replicas of the citizens of the country and be made subject to the laws of the land. There should be a regulatory clarity on what is perceived right and what is perceived against the law. This will enable the citizens to confidently undertake transactions to fully leverage the power of Blockchain technology.

It is important that KYC & AML regulations should be made applicable to all the citizens and businesses taking part in legitimate transactions and the Government should offer the same legal protection against any deceptive or fraudulent behaviors that are discovered over these platforms.

The consensus mechanisms undertaken by the Blockchains have the power to transfer value as per the executable smart contracts. This opens up the possibility of a section of participants colluding to manipulate the consensus and shortchanging minority participants. The government should enact regulations to ensure technology neutrality and also appropriate safeguards to ensure that the fraudulently and unfair practices of consensus management are checked.

Encouraging and ensuring interoperability and technology neutrality will result in consumer protection and freedom of choice like in the case of Telecom interoperability to prevent misuse of platforms by the founding partners.

Blockchain ledgers store a lot of value and engage in their transfer across real-life entities. This could potentially trigger a lot of taxable transactions and hence a clarity is required by the users as well as the regulators as to how we can subject them to the fair and practical tax regime.

For this, it is important for all the officials in the Government and Public sector undertakings to be fully conversant with the benefits of technology, its potential, and limitations.

Major User -

It is well understood that Blockchain has the potential to let the Government maintain & issue many types of registries, records, and certificates in a speedy and transparent manner. Further many citizens targeted beneficial schemes and procurement decisions awarding contracts, need to be managed in utmost transparency for maximum productivity of valuable resources contributed by the citizens in the form of taxes and savings.

Hence Government should look at leveraging the Blockchain technology as a user across all the potential areas of application, ranging from issuing Blockchain-based identities to all citizens to monitoring the last rupee spent by it with utter transparency and accountability.

Facilitator -

This will enable the Government to leverage the talent and give an opportunity for a number of entrepreneurs and professionals boosting the career opportunity within the country. This will further propel the country to be a leader in Blockchain technology that can offer its expertise and experience as a global backyard of application development and management of the Blockchain systems across the world.

Maximiser of Social Welfare –

Leveraging Blockchain Technology will enable the government to ensure that the targeted benefits to all sections are reaching in an optimal manner boosting their productivity and plugging leakages. This can enable the Government to increase such allocations to benefit larger sections of its deserving citizens.

A vibrant capability building program is necessary for the country's talent to be abreast of new technologies. Hence Government should proactively encourage the academic institutions and universities to undertake professional educational programs and research that not only generates patentable solutions but also gives a boost to the understanding and practice of the technologies that offer a paradigm shift in reaching a higher orbit of profitable growth.

Another grey area that needs to be tackled is the issue of Data Privacy that needs to be balanced with that of the transparency that a Blockchain-based system offers. While it is important to safeguard the data privacy issues of the citizens, it is important that the Government is conscious of not stifling the innovation mindset that could get curbed due to over-regulation.

A healthy debate between the Government and industry in balancing the various risks and contradictions, while ensuring that the technology is fully leveraged without stifling innovation, is the need of the hour for a strong foundation for Blockchain technology in India.

8. Principles to Guide National Strategy

As an important input to the National Strategy document, it is important for us to evaluate the SWOT (Strengths, Weaknesses, Opportunities, and Threats) of the Blockchain technology and its current status in the Indian scenario. The same is presented in Table 4.

Table 4: SWOT Analysis for Blockchain Technology at National Level

Blockchain – Where does India Stand? A SWOT	
STRENGTHS	WEAKNESSES
Large Technology workforce that has been the Knowledge backbone of the world can quickly reskill for leadership	Lack of regulatory clarity stifling the plans of decision makers on investment programs to boost Blockchain adaption
Strong identity management system across the country in the form of UIDAI & Aadhar	Lack of Government support for Blockchain projects as a key user of the technology has delayed the takeoff
Strong IT consulting and implementation partners like NIST, NIC and e-Governance practices adopted.	Negligible investments in Blockchain by Private sector as there is a lack of understanding of the potential benefits & Government's stand.
Use cases across multiple domains for PoCs	Very few production level applications in country
Access to global technology leaders & platforms as potential technology partners and customers offers a captive opportunity	Investment climate not conducive to innovation as India's venture capital is mostly focussed on growth oriented projects and not for incubating curriculum
Ability to adopt integrated strategies across multiple disruptive technology domains	Very poor awareness among decision maker community in public & private sectors
OPPORTUNITIES	THREATS
Opportunity to be the Blockchain development backbone of the world by reskilling the developer population in advanced	Large pool of IOT devices susceptible to cyberattacks can derail the automation programs and Industry 4.0 plans
Potentially largest pool of IUI devices generating monetizable data as India sports one of the highest citizen base and telecom penetration.	Differences between different entities that are expected to collaborate may create roadblocks and deadlocks
Large opportunity for data monetisation by creating a market place for anonymised data through Blockchain can lead to unlocking of the value both in the country and across	The high potential of data triggered prosperity can lead to excessive attention of cyber attackers. Poor compliance on cybersecurity best practices can spur a collapse of connectivity
Increasing transparency in Banking system to eliminate NPA Burden. Transparent processes for procurement and loan process management can help in humongous savings	The Transparency threatened lobby that has been used to exploiting inefficiencies in weak systems can apply roadblocks to blockchain programs
Improving transparency in Benefit programs can enable the schemes to maximise positive impact on citizens	Improper connectivity of distant places and underdeveloped areas can restrict the benefits of technology depending on internet connectivity.
Crashing of expenses of elections and offer instantaneous election results	Lack of digitisation and legacy backlogs can create inertia to shift to advanced technologies.

Although blockchain is already being used to execute financial transactions, it is relatively nascent in other sectors of the economy. Because of its novelty, blockchain is being piloted by industry, but at this time does not appear to be a replacement for existing systems. Given these conditions, the technology does not contain the same level of adoption that previous technology had when facing potential legislative action.

However, in addition to examining legislative options concerning the technology's use, Government of India should provide oversight of other state governments and departments which are seeking to (1) use it for government business, and/or (2) regulate its use in the private sector.

For example, several state governments have formulated blockchain policies/strategy documents and are attempting to promote this technology to achieve efficiencies in the current functions of government. Some of these approaches involve ways to better manage identities, assets, data, and contracts. Additionally, many state governments are creating test beds for blockchain technology.

Notably, the involvement of premier academic institutions in the blockchain space has not been very proactive. Indian Institutes of Technologies and National Institutes of Technologies are only now starting to offer some courses on blockchain technology. There is an urgent need for greater involvement of these premier academic institutions in establishing standards and platforms for research and testing. There is need to create testbeds to examine blockchain applications and uses, providing various government departments first-hand experience with the technology as well as information concerning its limitations. This experience can better inform senior leadership in departments to determine if they seek to use the technology and it can also help them in their interactions with the private sector concerning the technology.

Historically, this option has been used when a technology is advanced and in relatively wide use, or is targeted at a specific industry or has a very specific application. When a technology has a broad application (e.g., information communication technologies) Government of India has historically opted to have several ministries oversee the technology, charging different ministries/agencies with overseeing the different applications of that technology.

The National Blockchain Strategy should be based on following four key principles:

1. Ensure technology neutrality: Government should allow for competing technologies and platform to emerge and to the extent possible not hard-wire its strategy for policies or programs to any specific technology. The Strategy as well as policy should be technology/platform agnostic. This will allow the emergence of best technological solutions without foreclosing future developments.
2. Ensure policy and regulatory framework at national level: The policy framework should be at the national level and states should be encouraged to experiment and promote development as well as adoption of blockchain technology within the national policy framework. This will remove policy uncertainty and promote private sector investment in development of technology. The regulatory framework should promote and protect innovation and experimentation rather than prevent usage and creation of new business models, products and services. Regulatory framework should focus on solving known problems and should not try to foreclose all future unknown problems. In other words, policy and regulation should be seen to reduce known risks and not future perceived risks. Regulation should not lead to preventing innovation. The regulatory framework should be flexible enough to protect various stakeholders without sacrificing development of new products and services. Moreover, the regulatory framework should allow for smart contracts as legal contracts and should promote data interoperability for blockchain applications.
3. Leadership in knowledge leads to leadership in technology: India's ability to attain global leadership role in blockchain technology is contingent on investment in research, human capital and supportive regulatory framework. Government should invest in research at premier universities and create appropriate funding framework for promising research projects.

4. Development of capacity in government: Given the preminence of government in indian economy, social sectors and education, it is critical that government functionaries, especially at the senior levels understand the building blocks of blockchain systems and its value proposition. Also, government should support blockchain adoption in various departments by experimenting with promising use cases.

The national blockchain strategy should promote innovation and facilitate adoption of Blockchain in a coordinated manner resulting in all-round prosperity that it promises. Government of India is undertaking a meticulous and calibrated methodology to study the repercussions of the usage of Blockchain technology in its entirety, examining the best use cases across the globe, consulting the thought leaders, business leaders, policymakers and technology implementation partners across the cross-sections of the polity. This will enable the country to forge ahead by taking advantage of the disruptive potential while balancing the risks.

Interest in blockchain technology continues to grow in both the public and private sectors. However, it is helpful to remember it is not a single technology, but a novel way of using existing technologies already to enable transactions. Those transactions can also occur through using a combination of commercial off-the-shelf technologies without using blockchain. But, because of the cryptography involved in blockchain implementations, those transactions can occur among parties that might not otherwise have an established means to carry out a trusted transaction or do not mutually trust each other.

As the public and private sectors consider blockchain use, awareness of both its advantages and limitations will better inform decisions concerning its adoption or avoidance.

Key Building Blocks of Blockchain Strategy

Encourage innovation and experimentation by private sector

The private sector was a leader in the US in developing the Internet in the 1990s and 2000s and Government should encourage the private sector to take the lead in innovation in this technology. Any regulatory overreach may be highly counterproductive at this stage of the evolution of blockchain ecosystems. Rather than regulating, the governments should encourage and support experimentation with use cases for the next generation of technological development.

Adopt a light touch regulatory approach at this initial stage

Regulation that is too restrictive or does not take into account the potential for future innovations will stymie the growth of this industry and scuttle government efforts to remain a leader in, and keep pace with, technological development. Government should involve

Policy and regulation should be clear before enforcement

Industry must have clearly articulated and binding statements from regulators regarding the application of law to blockchain-based applications and tokens before bringing enforcement actions. Public statements, whether through the press or formal speeches, are helpful but are not official statements of application by the agency. If an agency intends to enforce its laws in new and innovative ways, it must first notify industry stakeholders of its intent to do so and the way in which existing law applies.

Regulation and law should be based on functions performed, not the technology

Virtual currency and digital asset-related statutes and regulations should emphasize function. New rules and statutes should not be based on the type of technology itself but, rather, the use or activity involving the technology.

Government should not do regulatory patchwork

Government of India and various state governments should cooperate and coordinate in their policymaking efforts to prevent a patchwork of regulations and statutes related to similar functions. There is need for a framework at the national level to facilitate the coordination and to ensure that legal, regulatory and policy framework is consistent and is formulated after taking inputs from all stakeholders. There is need for a comprehensive, coordinated, pro-growth approach to developing blockchain technology in India.

Regulation or law should be clear, predictive and pro-innovation

Technology changes rapidly. As such, laws and regulations should be drafted with the intent to endure future iterations and not focus solely on one technology or application. For example, in the US the Electronic Signatures in Global and National Commerce Act (ESIGN Act) and state Uniform Electronic Transactions Acts (UETA) were written to validate electronic signatures and records and to be agnostic to the technology used. The same principles should be considered when developing future rules in India for blockchain technology.

Policy makers should have a comprehensive understanding of blockchain technology

Blockchain platforms can be complex. Government stakeholders must take the time to learn how it works, its strengths and weaknesses, and how those attributes can create new mechanisms for enabling the provision of products and services by governments and businesses, as well as enabling better access to consumers.

Establishment of an office/body to coordinate blockchain strategy

Given the multi-tiered and multi-stakeholder structure of regulation, a coordinated approach across departments and sectors is necessary to ensure streamlined regulation and growth of the industry. Not only would this office work to determine applications of blockchain that could cut costs for taxpayers, it could also provide a gateway for entrepreneurs to best understand the laws surrounding blockchain and virtual currencies. Such an office can better develop blockchain-based economic development and activity and coordinate the government's policies going forward.

9. Going Forward: Think Networks, Think Global

There has been a movement world over to leverage the benefit of blockchain technology while being cautious about the speculation has driven the crypto-asset economy. The nations world over are circumspect about the negative aspects of the unregulated crypto-economy, while being excited about the potential and prospects of the underlying blockchain technology to offer new business models and the highest level of transparency and better governance to citizens.

There is also a need to give encouragement to the innovation that is facilitated by the new paradigms of our generation and ensure that our country and citizens are ahead of the curve and immensely benefited by these trends.

There is a need to clearly differentiate between different types of blockchain systems, welcoming all such applications that fall in the ‘permissioned’ space and hence offer a total clarity on the administrators, validators and the people who conduct transactions by strictly following the laws of the land and the KYC/AML aspects of verifying identities.

To facilitate innovation, we can examine the concept of a Central Bank Digital INR (CBDR) administered through a National Permissioned Blockchain that can run decentralized applications written in Turing complete programming languages and offers Trust As a Service.

Permissioned blockchain applications can also account for regulatory oversight through participatory nodes by corresponding regulators and leverage the National Public Blockchain platform as a trust anchor.

We foresee a lot of decentralized applications and a number of permissioned enterprise blockchain applications built in the country in the future that can leverage the infrastructure of a National Blockchain Platform and also move towards secure tokenization of assets on the same.

A competent developer ecosystem, capability building strategy and well-involved industry leveraging the benefits of the technology for a paradigm shift in performance will attract a vibrant investor community. This then can facilitate all-round prosperity empowered by Trust and Transparency for a great future of our country.

We look forward to a healthy debate on the various issues discussed in this paper that can help India in evolving a comprehensive and forward-looking strategy & standards to help us leverage the power of Blockchain technology, while also plugging interoperably with the global eco-system.