DRAFT APPROACH PAPER

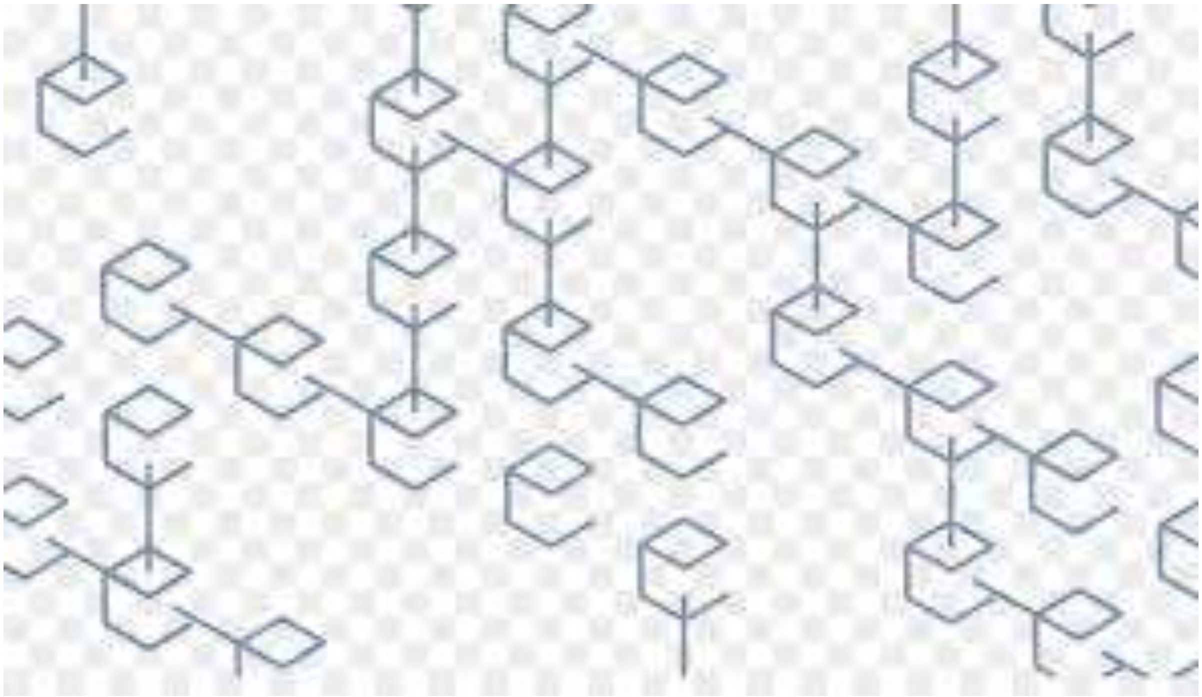


Image from: Sutardja Center, Univ. of California Berkeley

NATIONAL STRATEGY ON BLOCKCHAIN

December 30, 2019

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

National Institute for Smart Government
Architecting e-Government

TABLE OF CONTENTS

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 inabaility 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 Internt 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 apparoach 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.

1. Value Proposition of Blockchain Technologies

While real-world large scale blockchain technology based systems are still non-exstent, 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 through reduction in transactional costs. Cost reducation will be by modifying the existing processes by removing intermediaries or by lowering the administrative costs of safe record keeping and efficient transaction reconciliation. This is likely to shift the flow of value by reducing lost revenues and generating new revenues for businesses adopting blockchain-based systems. for blockchain-service providers. A recent report by Mackinsey 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 front runners in capturing the value. Financial services' core functions of verifying and transferring financial information and assets very closely align with blockchain's core transformative impact. Major current pain points, particularly in cross-border payments and trade finance, can be solved by blockchain-based solutions, which reduce the number of necessary intermediaries and are geographically agnostic. Further savings can be realized in capital markets post-trade settlement and in regulatory reporting. These value opportunities are reflected in the fact that approximately 90 percent of major Australian, European, and North American banks are already experimenting or investing in blockchain.

As with banks, governments' key record-keeping and verifying functions can be enabled by blockchain infrastructure to achieve large administrative savings. Public data is often siloed as well as opaque among

[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

government agencies and across businesses, citizens, and watchdogs. In dealing with data from birth certificates to taxes, blockchain-based records and smart contracts can simplify interactions with citizens while increasing data security. Many public-sector applications, such as blockchain-based identity records, would serve as key enabling solutions and standards for the wider economy. More than 25 governments are actively running blockchain pilots supported by start-ups.

Within healthcare, blockchain could be the key to unlocking the value of data availability and exchange across providers, patients, insurers, and researchers. Blockchain-based healthcare records can not only facilitate increased administrative efficiency, but also give researchers access to the historical, non–patient-identifiable data sets crucial for advancements in medical research. Smart contracts could give patients more controlover their data and even the ability to commercialize data access. For example, patients could charge pharmaceutical companies to access or use their data in drug research. Blockchain is also being combined with IoT sensors to ensure the integrity of the cold chain (logistics of storage and distribution at low temperatures) for drugs, blood, and organs.

Over time, the value of blockchain will shift from driving cost reduction to enabling entirely new business models and revenue streams. One of the most promising and transformative use cases is the creation of a distributed, secure digital identity—for both consumer identity and the commercial know-your-customer process—and the services associated with it. However, the new business models this would create are a longer-term possibility due to current feasibility constraints.

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, it's 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.

Blockchain's value proposition also hinges on the fact that it delivers consensus, provenance, immutability and finality to participants in a business network. Any useful blockchain use case will deliver one or more of these benefits.

- Consensus: Frequently within a business network, it's advantageous for a set of organizations to have the same view of a set of data that may be updated or changed by individual parties. For example, any use case or industry that relies on shared reference data — such as bank routing codes, employment records, title insurance and others — will benefit from this property of blockchain.
- Provenance: All transactions on a blockchain are tied to one another through an append-only process called hash chaining. Each transaction is tied to ones that came before it, resulting in a tamperproof audit trail that allows participants to know where an asset was first logged on the blockchain and how its ownership has changed throughout its lifecycle. Industries like

manufacturing, transportation and supply chain that need to track how often and through how many parties an asset changes hands, as well as ones that incur significant costs due to recalls, can benefit from blockchain’s provenance capability.

- Immutability: As described above, each block is linked to the previous one. This means that no participant can credibly claim that an earlier transaction changed or did not occur. Any industry with audits and regulatory compliance will derive its principal benefit from blockchain’s immutability since it creates an indelible record of all transactions, including seek and find access for auditors and regulators.
- Finality: Transactions and asset ownership on a blockchain are executed immediately upon the fulfillment of specified contractual conditions. In the global trade industry, for example, banks and corporations benefit from blockchain’s finality to make transactions nearly instantaneous, compared to the time and the cost associated with physically signing documents, currency fluctuations and more. Organizations can also leverage IoT devices in this scenario to help sellers draw down a buyer’s letter of credit at specified points during shipment. If an erroneous transaction is sent, reversing it would require an equal transaction in the opposite direction, with both transactions being visible. When assessing the need for finality, one needs to consider whether parties would benefit from the ability to create instantaneous and tamper-proof transactions.

What makes this technology special is not the above mentioned four characteristics, but also the promise of removing the need for trusted third party by transferring the trust from entity to underlying technology.Traditional data-centric business models often depend on one central authority vested with decision-making power and control over all data stored in a given database. As a result, other parties must simply accept, without tangible proof, that the information shared is complete, credible, and accurate, and that the central authority has not used their data for its own benefit.

While variations exist, most blockchain systems allow transactions to be executed and ownership to be shared in a peer-to-peer relationship, with multiple identical copies of the data stored in separate nodes of the network, and with the owners of the data and digital assets strictly controlling permissions for who can access what. The technology’s consensus mechanism ensures that these copies cannot be retroactively altered and authenticates the digital assets underlying each transaction. In this way, blockchain does away with a central authority and serves as a single source of truth, enabling parties to read and write (by mutual agreement of honest nodes through distributed consensus) to a common database or data repository that all participants can trust.

The transformative implications of these features are far-reaching. Blockchain technology has the potential to displace intermediaries, such as banks, brokers, and notaries, whose business models are predicated largely on providing independent third-party verification. By enabling greater transparency across the network, blockchain could also disintermediate market arbitragers, price-reporting agencies, benchmark providers, and others whose businesses create value by capitalizing on information asymmetry.

Blockchain’s structure and capabilities support end-to-end automation and easy data sharing across companies, and greatly reduce manual reconciliation efforts. In addition, anywhere, anytime access to complete transaction histories can significantly improve regulatory and audit compliance, decreasing the associated costs and boosting response times. Finally, blockchain technology enables “smart” contracts, with which contractual obligations can be enforced through predefined software code that requires no human interaction.

The four primary sources of value that blockchain systems can deliver for organizations including businesses are:

- **New Business Models.** Blockchain-supported innovation can help businesses create new revenue streams. In the energy sector, for instance, blockchain platforms can help individuals and entities trade excess energy stores autonomously and in near real time over the grid. Blockchain innovation can also allow product companies to move up the technology stack and expand their portfolios with higher-value service offerings, such as track and trace or analytics services based on data captured by blockchain.

- **Operational Efficiency.** Blockchain enables process automation and the removal of unnecessary intermediaries to help organizations improve productivity and performance. It also supports audit and regulatory compliance, generating significant time and cost savings. The use of smart contracts, for instance, can automate routine business functions, such as invoice generation and reconciliation, customs clearance, and property title transfer.
- **Risk Mitigation.** Companies can use blockchain-related applications to improve tracing and authentication across the supply chain. Better provenance and transparency throughout the supply and distribution chain, for example, could reduce counterfeiting and associated health and safety issues from fraudulent parts, thus mitigating financial and reputational damage.

- **Social Impact.** Blockchain platforms can be used to support a wide variety of initiatives, including voting and election management and ethical sourcing. The Democratic Republic of Congo, for instance, is using blockchain capabilities to build a new e-government platform that will help the country manage its natural resources and social welfare programs. Estonia is pioneering the use of blockchain for securing citizen information and is planning to adopt the technology to support other public welfare initiatives, such as those relating to personal ID and health records.

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.

2. Overview of Blockchain Technology

Before, we described the fondational 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 trsuted third party.

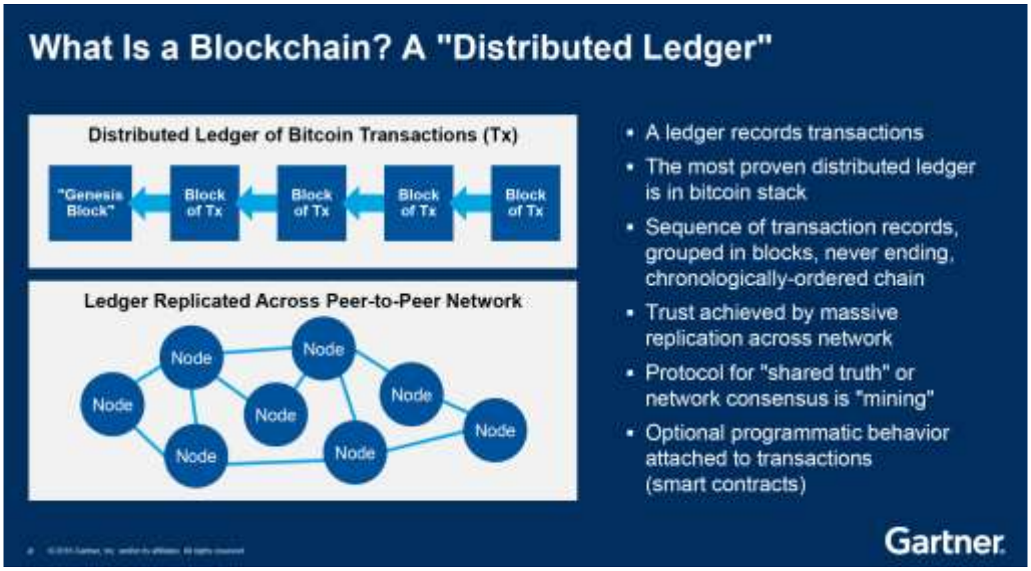
Historical perspective before Bitcoin: The growth of digtal technologies together with developmets of communication technologies in leading to laying of the foundations of the World Wide Web in 80s also provided impeteus to academicians as well as technology entreprenurers to experiment with creation of digital currency. Experts from diverse fields such as computer science and mathematics worked on different aspects of the foundational pilaars even before the advent of digtal 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 crypto-graphically 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 platform for radically decentralized applications to maintain records of ownership of assets and allow for transfer of assets as well as updation of records using peer-to-peer distributed consensus mechanism with out 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 exhanges 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 trsuted third parties as the 'trust' is created by the unique features of the technology and not by an organization or entity.



What Is a Blockchain? A "Distributed Ledger"

- A ledger records transactions
- The most proven distributed ledger is in bitcoin stack
- Sequence of transaction records, grouped in blocks, never ending, chronologically-ordered chain
- Trust achieved by massive replication across network
- Protocol for "shared truth" or network consensus is "mining"
- Optional programmatic behavior attached to transactions (smart contracts)

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 keeing and authenticity of records in ensured by the technology rather by a trusted third party. This can also be thought as a database encompassing a physical chain of fixed length blocks that 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 transations 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, it means that each transaction added to a new block is validated and then inserted into the block. The interaction and broadcast are verified by a distributed network and once validated a new block is created and when a block is completed, it is added to the end of existing block.

Once the first two pillars ensure a technology based system of ledger of ownersip 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'.

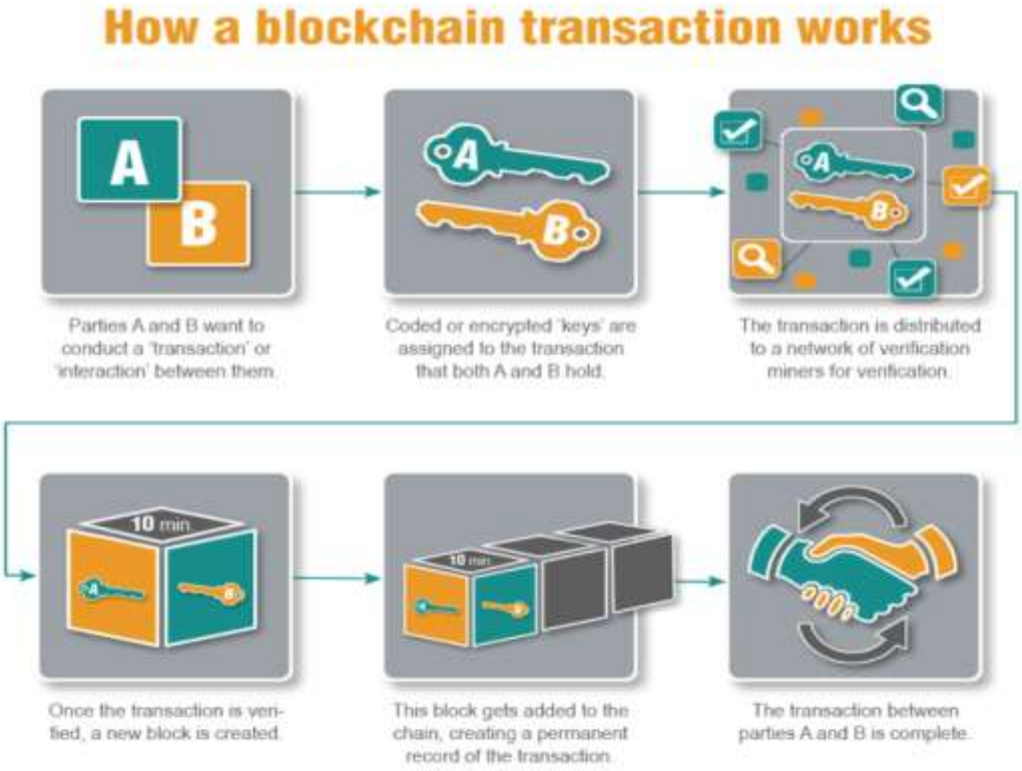

How a blockchain transaction works
A
B
Parties A and B want to conduct a 'transaction' or 'interaction' between them.
A
B
Coded or encrypted 'keys' are assigned to the transaction that both A and B hold.
A
B
The transaction is distributed to a network of verification miners for verification.
10 min
A
B
Once the transaction is verified, a new block is created.
10 min
This block gets added to the chain, creating a permanent record of the transaction.
The transaction between parties A and B is complete.

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.

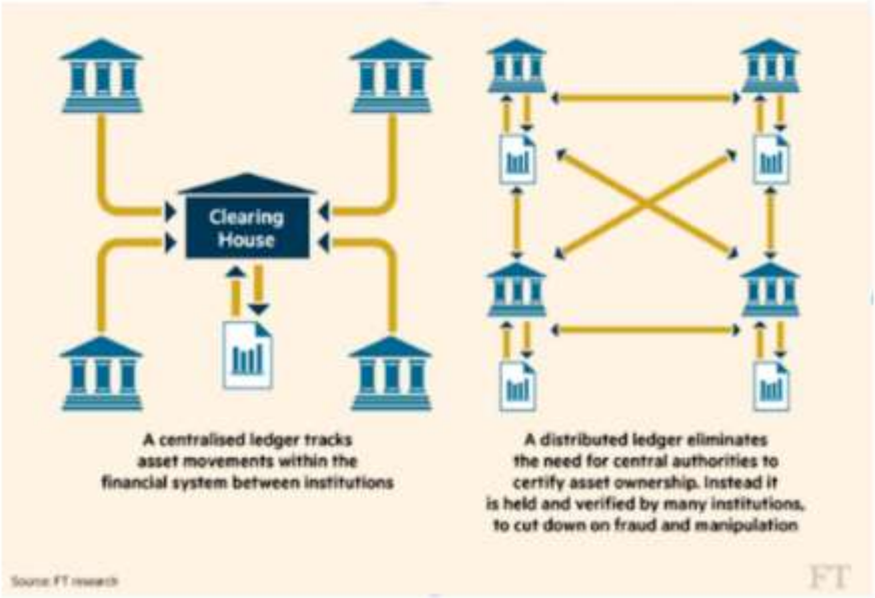
Let us say A and B are two entities that wish to conduct an interaction or transaction. Cryptographic keys are assigned to the interaction that both A and B Hold. So basic blockchain processing consists off the following steps

1: Add new and undeletable transactions and organize them into blocks.

2: Verify each transaction in the block. This is done cryptographically.

3: Append the new block to the end of the existing immutable block chain.

Understanding the mechanics of blockchain: The blocks once recorded are designed to be resistant to modifications which means that the data in a block cannot be altered retroactively. Through the use of a peer-to-peer (p2p) network and distributed timestamping server, a public block chain database is managed autonomously.



A centralised ledger tracks asset movements within the financial system between institutions

A distributed ledger eliminates the need for central authorities to certify asset ownership. Instead it is held and verified by many institutions, to cut down on fraud and manipulation

Source: FT research

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 consenus: 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 transcation 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.

In simpler terms, consensus is a dynamic way of reaching agreement in a group. While voting just settles for a majority rule without any thought for the feelings and well-being of the minority, a consensus on the other hand makes sure that an agreement is reached which could benefit the entire group as a whole. A method by which consensus decision-making is achieved in a distributed peer-to-peer network is called “distributed consensus mechanism”. The objectives of such a mechanism are:

- **Agreement Seeking**: A consensus mechanism should bring about as much agreement from the group as possible.
- **Collaborative**: All the participants should aim to work together to achieve a result that puts the best interest of the group first.
- **Cooperative**: All the participants shouldn’t put their own interests first and work as a team more than individuals.
- **Egalitarian**: A group trying to achieve consensus should be as egalitarian as possible. What this basically means that each and every vote has equal weight. One person’s vote can’t be more important than another’s.
- **Inclusive**: As many people as possible should be involved in the consensus process. It shouldn’t be like normal voting where people don’t really feel like voting because they believe that their vote won’t have any weight in the long run.
- **Participatory**: The consensus mechanism should be such that everyone should actively participate in the overall process.

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 he 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 anaccount(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 a 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 federate byzantine agreement protocol.
- **Other consensus protocols driven by other economic consideration**: There are many other consenus protocols which have the potential to be used in blockchain systems but have not yet attracted enough attraction from industy. 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. Therfore, 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 basic characteristics of blockchain technology which is also shared by smart contracts is transparency. As previously stated, smart contracts are filled with terms and conditions in absolute detail which are also checked by the parties involved in the agreement.

  This eliminates the chance of dispute and issues at the later stages as the terms and conditions are thoroughly checked and put into place only when all the participants agree to those. This trait of smart contracts allows the involved parties to ensure transparency during transactions.

  Moreover, need for precision in contract detailing keeps all the information open with everyone which ultimately resolves anything related to miscommunication issue. Therefore, with the aid of smart contracts, efficiency lost in communication gaps can be restored.

- **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 an explicitly detailed form. It requires to holds all the terms and conditions in it before it is finally put to work. Any condition that’s left out of the contract might result in an error while execution, therefore while creating smart contracts, all the conditions are put in the detailed form.

Due to this, the smart contract becomes a comprehensive agreement which when gets executed automatically, gets almost everything done. In the case of manual contracts, there are chances of errors as the person who is responsible for making a contract might miss one condition or the other. Moreover, there’s no way of even tracking it until the error is made. Therefore, smart contracts are a better alternative when it comes to achieving accuracy and precision.

- **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.

The potential of smart contracts cannot be limited. They can be used for small regular agreements as well as contracts for governments and enterprises too. They allow traders and buyers to track their purchase back in the supply chain which increases trust. While third-parties like lawyers, government bodies etc. make a hole in our pockets in the form of fees for making agreements; smart contracts save this money by eliminating the need for such intermediaries. When it comes to using smart contracts, all we need to do is check the code before the execution, everything after that will be done in an electronic way. Smart contracts provide us with an opportunity to make our routine transactions and processes more streamlined and automated.

The base of smart contracts are interfaces, business rules, and data. With evolving technology, smart contracts will also need to be updated for eliminating any compatibility issues with operating systems and perform their directed functions correctly. While smart contracts are still in their developing phase, they might face certain vulnerability attacks. In order to make smart contracts a part of our day to day life, both, cybersecurity practices as well as the platforms to create smart contracts need to be updated from time to time.

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.r3vev.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.

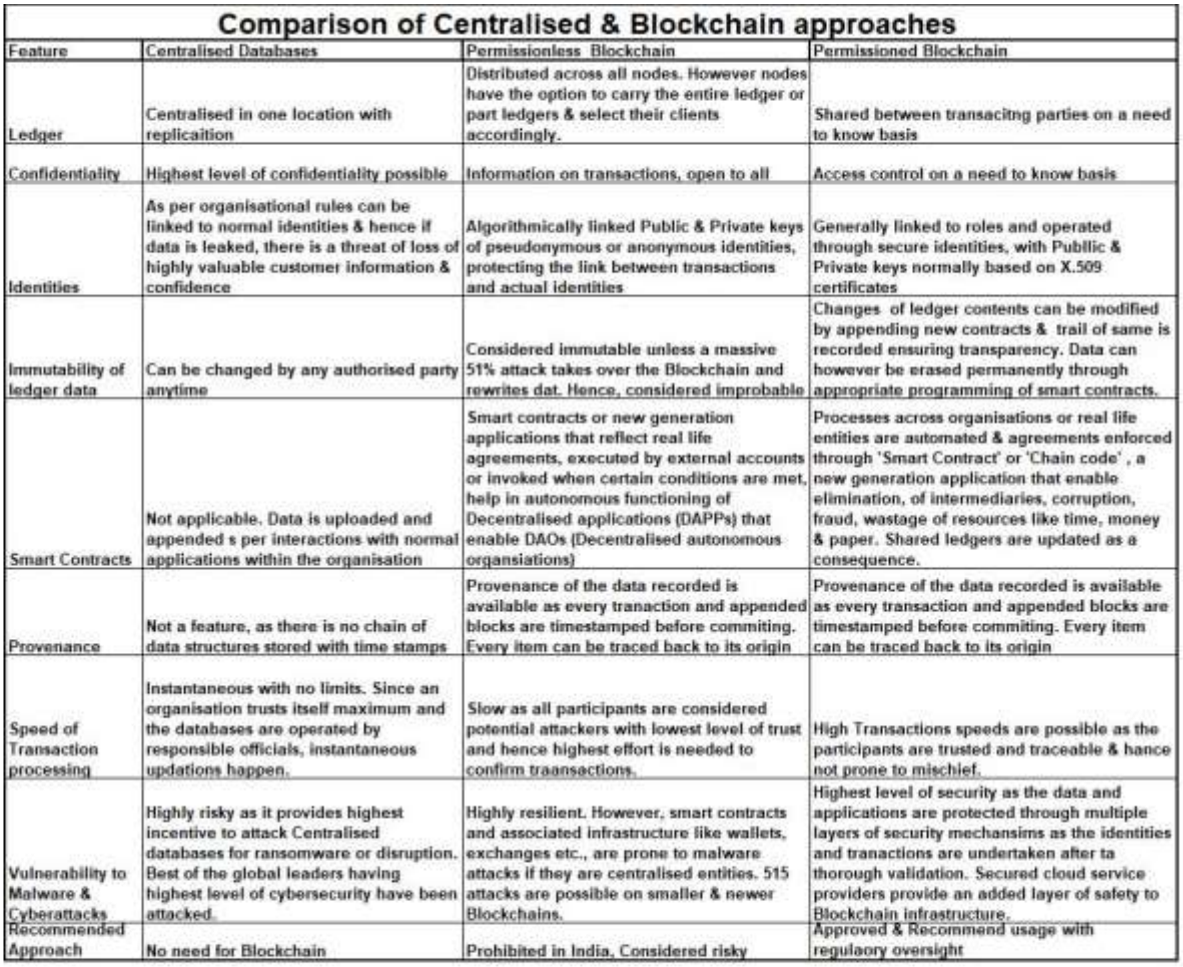
Key characteristics of Blockchain:

• **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 permissoned 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 prblems.

- **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: Comparision of traditional and blockchain based systems

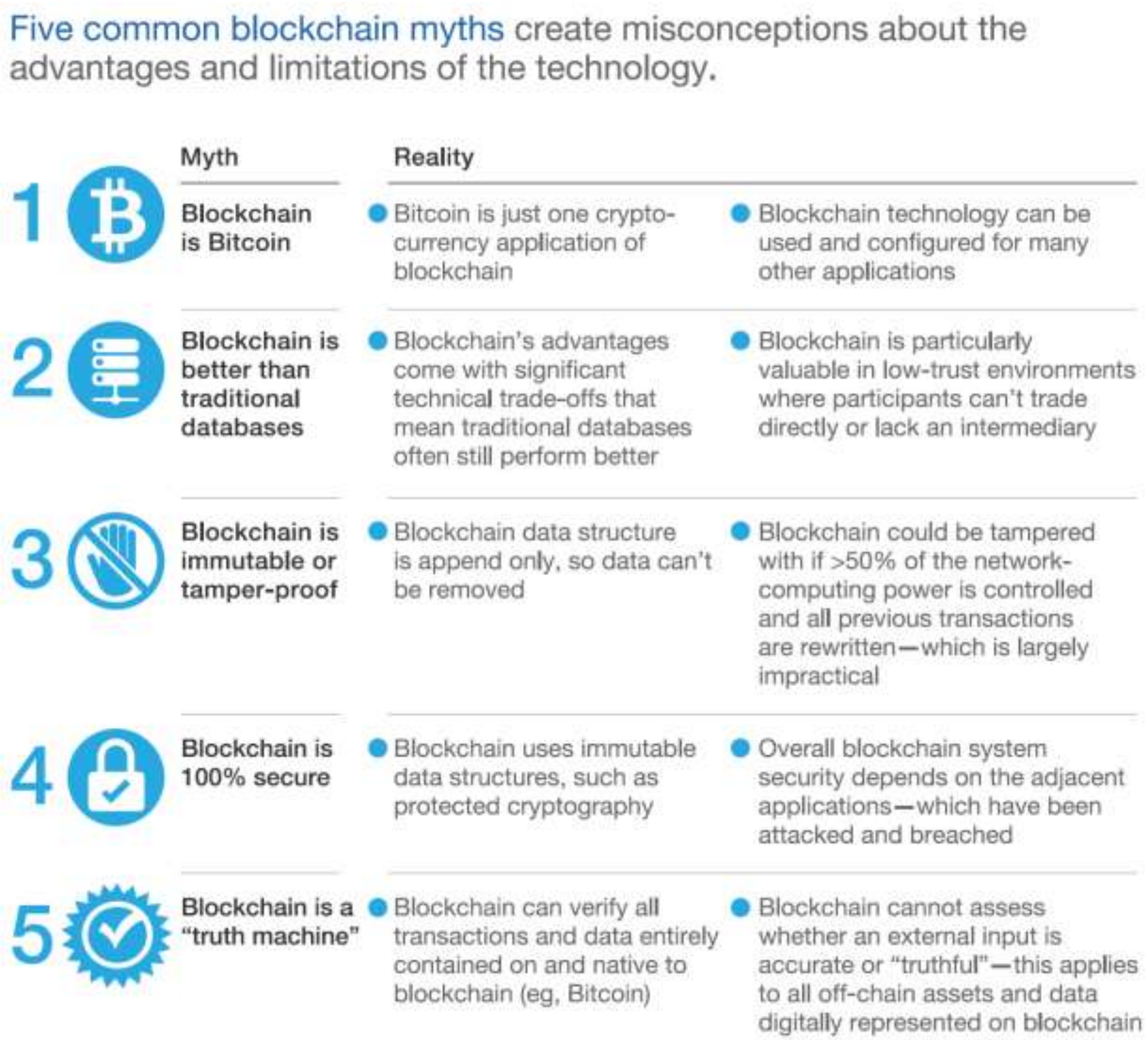


Comparison of Centralised & Blockchain approaches

Feature	Centralised Databases	Permissionless Blockchain	Permissioned Blockchain
Ledger	Centralised in one location with replicaition	Distributed across all nodes. However nodes have the option to carry the entire ledger or part ledgers & select their clients accordingly.	Shared between transacitng 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 Publlic & 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 organsiations)	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 commiting. 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 commiting. 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 tranactions 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

So what is blockchain technology? Cutting out all the hype around blockchain, bitcoin, cryptocurrecy, Blockchain is a distributed ledger, or database, shared across a public or private computing network. Each computer node in the network holds a copy of the ledger, so there is no single point of failure. Every piece of information is mathematically hashed and added as a new “block” to the chain of historical records. Various consensus protocols are used to validate a new block with other participants before it can be added to the chain. This prevents fraud or double spending without requiring a central authority. The ledger can also be programmed with “smart contracts,” a set of conditions recorded on the blockchain, so that transactions automatically trigger when the conditions are met.

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



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

	Myth	Reality	
1	**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**	● Blockchain's advantages come with significant technical trade-offs that mean traditional databases often still perform better	● Blockchain is particularly valuable in low-trust environments where participants can't trade directly or lack an intermediary
3	**Blockchain is immutable or tamper-proof**	● Blockchain data structure is append only, so data can't be removed	● Blockchain could be tampered with if >50% of the network-computing power is controlled and all previous transactions are rewritten—which is largely impractical
4	**Blockchain is 100% secure**	● Blockchain uses immutable data structures, such as protected cryptography	● Overall blockchain system security depends on the adjacent applications—which have been attacked and breached
5	**Blockchain is a "truth machine"**	● Blockchain can verify all transactions and data entirely contained on and native to blockchain (eg, Bitcoin)	● Blockchain cannot assess whether an external input is accurate or "truthful"—this applies to all off-chain assets and data digitally represented on blockchain

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

[5] McKinsey Digital, Blockchain beyond the hype: What is the strategic business value?, June 2018, Exhbit 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

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

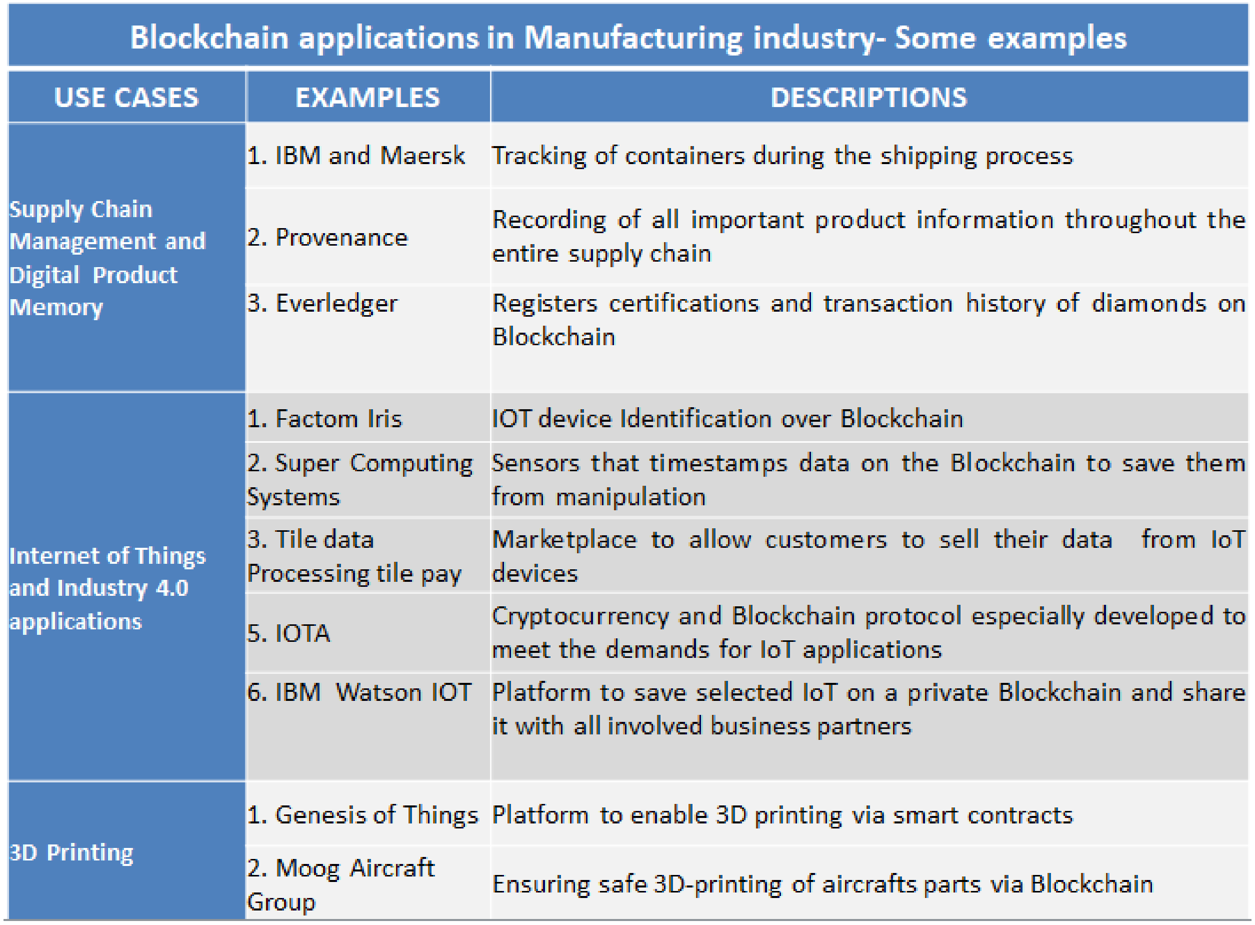
A lot of activity in Blockchain technology is centered on financial applications, asset tracking, and supply chain. The application of a framework to identify various aspects in the manufacturing sector gives us an idea of the segments that are amenable to the application of Blockchain technology. As 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 them 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 Karnakaka &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 to new borns.

Blockchain Startup Ecosystem in India

SOMISH is a technology and product development company based out of India since 2006 with expertise in building automation systems using cutting-edge technologies. For over 10 years, they have continuously served top-line customers with their ability to re-engineer, design, develop and implement automation systems.
They are now advocating and building the blockchain based solution in India and rest of the world. Their team is providing blockchain solutions and has a clear understanding of key tenets behind Blockchain Technology, having worked on a wide variety of blockchain use-cases like:

- P2P Insurance
- Aviation Maintenance Log
- Subsidy Distribution
- Crisis Fund Distribution
- Bill Discounting
- Tokenized Fund Transfer

2. EzyRemit: As the name suggests, they are working on easy remittances built on top of the blockchain. They are an innovative company trying to solve some of the long-standing issues of fintech, banking, and payments through their flagship blockchain-based products. Some of their products such as EzyRemit and EzyHedge are also available for demos.

3. Signzy:Signzy aims to couple artificial intelligence with the blockchain to make secure, compliant and user-friendly products.Their flagship Signzy API enables:

- Improved user experience with multi-device support.
- Faster onboarding using real-time APIs.
- Enhanced security and compliance.

They have three main products:

1. **RealKYC** – Bank-grade digital KYC in real-time
2. **Digital Contracts** – Secured digital contracts enabled by Aadhaar and Biometrics
3. **ARI** – Algorithmic Risk Intelligence

4. Primechain: Primechain is a young Indian startup that aims at "building blockchains for a better world".

They provide blockchain solutions to industries such as banking, capital markets, government, healthcare & pharmaceuticals, insurance, manufacturing, aviation, shipping & logistics, telecommunications, and defense & military. They have quite a few blockchain-powered products:Primechain CONTRACT

- Primechain API
- Primechain LOAN
- Primechain Charge Registry
- Primechain KYC
- Primechain MONEY

They have also formed a community of banks called BankChain.

5. PSI PHI Blockchain Labs: This startup is building next-gen solutions for the digital economy based on distributed ledger technologies because they believe that the blockchain is going to revolutionize digital economy.

They mainly work in three key industries:

1. Supply Chain
2. Telecom
3. Healthcare

Their core products are: CRYPTO LOCKER – Store and share documents on blockchain using a set of APIs and DIGI RAIL – Multi-party shared database to optimize supply chain data flow

6. Darwin Labs: Darwin Labs is building applications for the blockchain, virtual reality, artificial intelligence, and other technologies which will help mankind evolve.

To accelerate this process, they run a blockchain startup incubator for Southeast Asia called Satoshi Studio.

They are also working on blockchain-enabled smart contracts across various industries such as healthcare, banking, trade finance, insurance, etc. under their flagship initiative Blocksmiths.

7. KrypC: KrypC makes it possible for various businesses to implement blockchain tech while providing a platform for these businesses to quickly do so.

They have developed a proprietary framework for developers, clients, and IT companies to implement blockchain tech effectively in less time and with less cost.

They follow a three-step strategy to do this:

- *STEP 1 Drag and Drop*

Define your innovation in the KrypC platform by simply dragging and dropping various elements of your innovative business models.

- *STEP 2 Quick API Integration*

Connect your business applications through the KrypC API framework.

- STEP 3 Unlock

Let your business team experience and adapt their innovative business models.

8. Sofocole Technologies: Sofocole is a service-based company that provides blockchain solutions to its clients across the globe.
They provide consultation on wallets, exchanges, private blockchains, and smart contracts products.

Some of their products which are already on the market are:

- SofoCap – Supply chain financing solution
- SofoChain – Product supply chain solution
- SofoInsure – Autonomous claim processing solution

9. Zebi: Zebi specializes in providing blockchain based solutions to governments and enterprises to leverage, protect their high value & sensitive data.
The company is founded, mentored and managed by Oxford, MIT, Stanford, and IIT veterans. And aims to solve the problem of Big data in India.

10. Smartchainers: Led by an experienced team of technocrats, Smartchainers is a pioneer in providing enterprise blockchain applications on a PoA based fork of ethereum blockchain and is serving a number of organisations in India and overseas. The company has completed unique blockchain PoCs for real estate applications in Middle east and also for employee expense management for a Korean client.

11. Astra Quark: One of the few Indian organisations to implement a Production grade blockchain application for India‘s leading battery manufacturers for end to end procurement management processes in tool tracking, Astra Quark, a Chennai based enterprise blockchain focused organization is exploring blockchain use cases across a variety of domains for clients based in Dubai and USA.

Educational initiatives in India for Blockchain:

In India, all the leading Institutes of National importance like IITs and IISc have started offering elective courses in Blockchain technology under the aegis of their Computer Science Department. There has been an exploding demand from the students to pursue Blockchain technology related courses. Demand for post graduate specialization and PhD programs is also on the rise.

AICTE Model curriculum of India for Undergraduate courses in emerging areas, for the year 2019-2020 contains detailed description of the courses that can be offered by the Indian Universities as a part of the curriculum. These technologies are:

1.Artificial Intelligence (AI)

2. Internet of Things (IoT)

3. Block Chain

4. Robotics

5. Quantum Computing

6. Data Sciences

7. Cyber Security

8. 3D Printing and Design

9. Virtual Reality (VR/AR)

It is important to note that Blockchain has been identified as an area of importance by the Indian Government and also MieTY, India's apex governing body for Information Technology. This timely joint initiative of All India Council for Technical Education (AICTE) and National Institute of Technical Teachers Training and Research (NITTTR), Chandigarh, is expected to bring translational skills among the students of under-graduate programmes to meet the expectations of the industry.

A number of Universities and IIITs are offering online Post Graduate programs in Blockchain Technology & Management. Some of the leading institutions offering 6-11 month online programs for working professionals are, Amity University, IIIT Bangalore & IIIT Hyderabad while IIITM-K (Trivandrum) offers a comprehensive full time program for Blockchain professionals.

Global Country Level Initiatives

ESTONIA

At a time when most of the world is cautious about cryptocurrencies, Estonia has already fully embraced it. At least the technological part of it. Now let’s look how.

In 2016, the Estonian government was looking for new and innovative ways to secure the health records for its 1.3 million residents. It turned to blockchain. There are many more examples of blockchain being used in the public and private sector in Estonia. If you have a great interest in starting a new cryptocurrency or to raise funds for your next world-changing idea, then look no further than the famous e-Residency program.

The team behind e-Residency, which is backed by the Estonian government, has been hard at work looking for opportunities to ensure the legitimacy of cryptocurrencies and ICOs (initial coin offerings), which have had their fair share of scammers exploiting them.

The head of public relations at e-Residency tells us that they know people in the administration who are working to make Estonia a very crypto-friendly jurisdiction for trusted ICOs.

Although the team behind e-Residency has been working on a few different cryptocurrency ideas none of them are ready for prime time now. One of the most promising ideas involves the trusted ICOs. Right now, there are a lot of scam artists who start an ICO just to steal people’s hard-earned money and run off with it. Trusted ICOs means that the people behind the initial coin offerings have been fully vetted by the Estonian government and hold e-Residency status, which means their backgrounds have been checked by the Police and Border Guard Board. This gives a sense of security to potential investors that the people running the ICO have no known ties to terrorism, money-laundering and other illegal activities.

DUBAI

Dubai is getting ready for a change — digitizing paper records, which can potentially help do away with alterations, thereby protecting the integrity of data storage in the government. All these documents will now be safely transacted using Blockchain. Dubai wants to live up to the name “City of the Future” by investing massively in this project and the team at SDO (Smart Dubai Office) is certain of finishing the project well before time. Some of more than 20 use cases recognized for this project have already started land registry transactions. The Dubai Government has roped in IBM and Consensys to provide their services and partnered with them as technology partners to further their objectives defined in the Smart Dubai initiatives.

The big development came in the form of a retail payment application (DubaiPay) which became blockchain-enabled in a collective effort between the SDO and Dubai’s Department of Finance (DoF). DubaiPay’s platform is supporting 40 government and non-government agencies and has collected over $35 million in the last year. The new arrangement would permit the platform to settle & register the transactions in real-time. The initial stage of this real-time processing scheme is being led by two of the government departments, namely Dubai Electricity and Water Authority (DEWA) & the Knowledge and Human Development Authority (KHDA), which processed over 5 million deals on the decentralized ledger.

Dubai Tourism has also announced a remodeling of their current system by introducing a Blockchain based virtual marketplace. Another development is that Dubai's Roads and Transport Authority's announcement about a vehicle administration system to be released in 2020. The largest bank in Dubai had also launched a Blockchain based plan to counter cheque fraud. Also, the Prime Minister of UAE launched the UAE Blockchain Strategy 2021 that stands on four pillars based on the resident's happiness, government efficiency, advanced legislation and global entrepreneurship. All these sectors and the Smart Dubai initiative has received international recognition and acclaim for its determined Blockchain endeavor, which continues to take great strides towards the adoption of developing technologies.

EUROPEAN UNION (EU):

EU started off with Distributed Ledger Economy (DLT), but after months of monitoring and observing its challenges, it made a turn into the blockchain industry. European Commission (EC) launched the EU Blockchain Observatory and Forum, aimed to support European cross-border engagement with the technology and its multiple stakeholders and to unite the economy around blockchain. Since its official launch, the newly established organization — supported by European Parliament — has released three thematic reports: the first one in July, dubbed "Blockchain Innovation in Europe"; the second one in October, "Blockchain and the GDPR"; and the third one in December, "Blockchain for Government and Public Services."

The second major step was taken in April when 22 countries — 21 EU member states and Norway — signed a Declaration that created a European Blockchain Partnership (EBP). During 2018, five more European countries joined the EBP: Greece and Romania in May, Denmark and Cyprus in June, and Italy — the last member to join — in September. The partnership's focus is on cybersecurity, privacy, energy efficiency and interoperability, all in full compliance with EU law.

DLT has also been implemented in the financial sector. It has proven to improve transparency and reduce transaction costs and other hidden costs by better management of data. Also, the processes have been streamlined. The local regulatory authorities and the EC are set to monitor trends and are also encouraged to do the research and experimentation that major financial institutions have undertaken in the exploration of the capabilities of the DLT.

CHINA:

The regulators in China have continued the clampdown on cryptocurrencies in the country, but still China is bumping up its adoption of the Blockchain Technology. In 2017, the Chinese government took several high-profile regulatory measures to protect investors and reduce financial risk, including announcing that initial coin offerings are illegal, restricting the primary business of cryptocurrency trading platforms, and discouraging cryptocurrency mining. Bitcoin trading in the Chinese currency, renminbi (RMB), fell to less than 1 percent of the world's total, from a peak of more than 90 percent, according to the People's Bank of China (PBoC). China's actions halted cryptocurrency speculation and prevented widespread fraud and manipulation, sparing many Chinese investors from the extreme volatility and tremendous losses sustained throughout 2018.

Hong Kong's Securities and Futures Commission (SFC) issued a warning to investors that tokens issued via ICO may be classified as securities, and that the Commission is "concerned about an increase in the use of ICOs to raise funds in Hong Kong and elsewhere". In a public notice in September 2017, the SFC urged investors “to be mindful of potential scams as well as the investment risks involved in ICOs. As ICOs operate online and may not have a presence in Hong Kong, investors may be exposed to heightened risks of fraud.”

Global Initiatives by Firms in Blockchain Domain

DELLOITE:

Though blockchain hasn’t reached its full potential, executives continue to see the technology as a connecting platform that can enable many business processes. The respondent report that overall corporate block- chain investment is growing across most sectors as new, practical applications has started to gain traction.

Deloitte conducted this survey between February 8 and March 4, 2019, primarily as a research vehicle to gain greater insights into the overall attitudes and investments in blockchain as a technology. The release of the survey highlights in this article reflects those opinions and perceptions around blockchain and the potential impact of the technology in the future. The information shared provides summaries of a subset of the overall data and insights collected.

The survey polled a sample of 1,386 senior executives in a dozen countries (Brazil, Canada, China, Germany, Hong Kong, Israel, Luxembourg, Singapore, Switzerland, United Arab Emirates, United Kingdom, and the United States) at companies with US$500 million or more in annual revenue for US respondents and at companies with US$100 million or more in annual revenue for respondents outside of the United States. Respondents had at least a broad understanding of blockchain and were familiar with and able to comment on their organizations’ investment plans.

Most people first heard of blockchain through its connection to bitcoin, which inextricably linked the technology to cryptocurrency. Enthusiasts promoted it as a driver of a new distributed economy in which users of token-based currencies would cut traditional banks and brokers out of peer- to-peer and B2C transactions. As such, blockchain advocates were slow to show how it could be used to disrupt and revolutionize other business sectors.

Years later, to the frustration of speculators, cryptocurrency adoption remains a slow-moving revolution. But this slowdown has boosted block- chain’s adoption elsewhere, as other use cases have emerged and begun to drive innovation. In short, as organizations look at blockchain more critically, it is becoming more well-rounded and, potentially, useful to a wider group of users. There also exists a wide range of applications that don’t require the use of a coin, including management of loyalty points, digitizing physical assets, and creating virtual wallets for finance management and reconciliation.

Now let us discuss what would the key issues be in this implementation:

1. Emerging disruptors:

Where enterprise organizations seek ways to integrate blockchain into their existing business models—or, more accurately, how to transform existing processes and systems to work with blockchain emerging disruptors built their businesses around blockchain from the start. This makes them potentially more fluid and agile than competitors and less constrained by similar challenges that inhibit adoption among their more established competition.

We're seeing signs of these abilities as organizations enter the second phase of disruption, in which most are no longer strictly focused on blockchain but are, instead, reinventing existing business models to create dynamic, blockchain-enabled solutions to reduce friction across organizations and industries.

For this year's survey, Deloitte targeted a small sample of emerging disruptors to gauge their attitudes and practices. Given their exclusive focus on blockchain solutions, it is unsurprising that they are more advanced in their deployment of blockchain than are enterprise organizations, and in developing and implementing new solutions to leverage blockchain's potential in new ways.

What is interesting, however, is that the survey results show nuance. For example, when asked for blockchain's most significant advantage over existing systems, respondents from enterprise organizations showed relative parity among several advantages, including new business models and value chains (23%), greater security/lower risk (23%), and greater speed compared to existing systems (17%). In contrast, emerging disruptors were more focused on new business models and value chains, which 42 percent cited as the most significant advantage.

An interesting difference between emerging disruptors and enterprise organizations is their attitudes toward security offered by blockchain. Enterprise organizations overwhelmingly (around 71%) believe that blockchain provides greater security than conventional IT solutions, while only 48% of emerging disruptors feel the same. While we cannot fully explain these differing viewpoints, it is still a noteworthy difference that merits further consideration.

Some key National and Corporate developments:

1. **China:**

In China, the government recently established key strategic technology priorities in its 13th five-year plan for IT. A white paper published by the Ministry of Industry and Information Technology cited blockchain as a key driver of economic development. The paper further suggested that the "real economy" was an area in which blockchain could find long-term applications—for example, product traceability and copyright protection. Fintech was also noted as a technology that government regulators were developing along with blockchain solutions to carry out public functions. Survey respondents overwhelmingly agreed with this assessment, with 73% suggesting blockchain is a top-five critical priority in China, a figure substantially higher than most other countries in our sample. And because China essentially bans cryptocurrencies, private blockchains and to some extent, permissioned blockchains could remain vital, especially given the size of Chinese industrials and their typically large numbers of subsidiaries.

Some 34% of respondents "strongly" believe in the disruptive potential of blockchain, more than most countries in our sample. This is important, given China's place in the global economy and the leadership role it has assumed in the Asia-Pacific region.

2. **Israel:**

There is substantial blockchain activity within Israeli organizations, focused largely on digital assets, cryptocurrencies. Israel stands as a strong leader in entrepreneurial activity and R&D in areas such as cyber, cryptography, and intelligence, which, in turn, seems to create a natural affinity for blockchain. Toward that end, some see Israel as a hotbed of blockchain activity. Crypto activities might currently outnumber corporate blockchain efforts, but a shift may be looming. Israeli blockchain startups are pursuing projects in such other areas as DNA data storage, diamond registration, cybersecurity, and international shipping.

3. **Singapore**:

In light to China’s de facto ban, Singapore is positioning itself to promote cryptocurrency. Indeed, the government has been highly supportive of free public blockchain platforms. In fact, the Monetary Authority of Singapore has adopted a pro- blockchain stance with favorable tax treatments and public funding for blockchain development. The government, too, appears to be moving beyond its traditional regulatory role by announcing its understanding and acceptance of the importance of blockchain to the financial future. As such, the Monetary Authority recently called blockchain technology “fundamental” to economic development in Singapore. Coupled with the country’s high level of that indigenous talent, entrepreneurial spirit, and fintech development, blockchain is expected to maintain an upward adoption trajectory in Singapore.

It is thus unsurprising that Singaporean executives report a uniformly greater belief in the potential of blockchain than respondents from many other countries. Respondents from Singapore also tend to be more aggressive than their global counterparts in hiring for blockchain-related positions—and more patient in waiting for the technology to provide measurable results.

This Blockchain story is beginning a new chapter at the global level, one in which the questions executives are asking are tougher, more granular, more grounded, and more pragmatic. They are questions that show an emerging awareness that the technology seems ready for prime time. It works. Now executives must figure out how to make the technology work for them i.e. how to leverage innovation created by emerging disruptors and how to align within the ecosystem.

Our survey seems to make clear this evolving landscape of pragmatism and maturation—more varied use cases and applications than last year, across a greater variety of sectors. Respondents show a more balanced view of expectations and concerns than last year, pointing to an increasingly practical sensibility. And indeed, what appears to be happening every day in the real world also appears to confirm what our survey is telling us. A day hardly seems to pass in which we do not read about new blockchain use cases or new ways to tokenize assets. Certainly, blockchain remains a subject of debate. But the tone and terms of the debate themselves seem to be shifting, reflecting more developed use cases and strategic visions of the future. Even people may be viewing blockchain with a new sense of possibility.

Of course, nobody can accurately predict the future, and we too will refrain from predicting a precise timeline on blockchain’s greater adoption. Yet the trajectory for blockchain in 2019 and going forward appears to point in a clearly upward direction. And that journey is the story of growth and potential that disruptive technologies characteristically take, offering adopters tangible strategic advantage in ways that few thought imaginable before.

IBM

Demand:

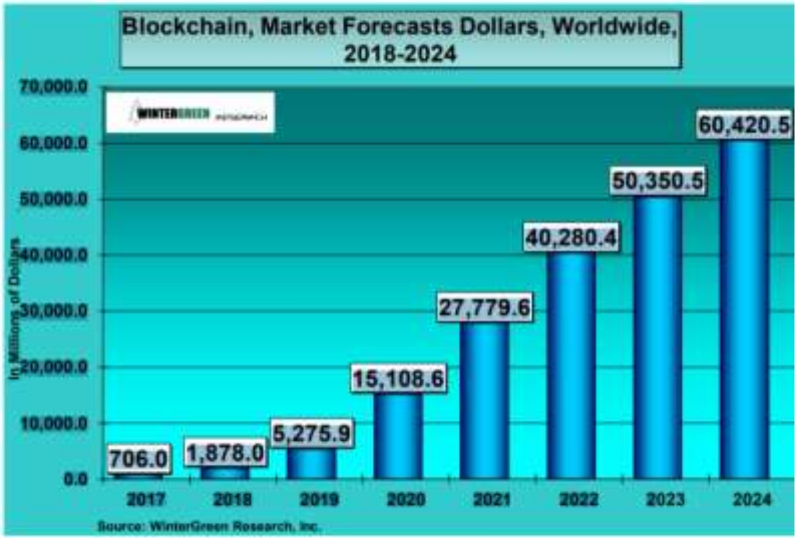
Demand for blockchain technology is growing among the largest users of IBM cloud capacity. IBM 60 cloud data centers see blockchain growing to be one of the top applications in use. IBM blockchain digital ledger market is growing rapidly, a much-needed event for big blue. Microsoft enterprise customers are making the transition to cloud services and blockchain on Azure. Blockchain Cloud Service helps customers extend existing applications like enterprise-resource management systems. SAP SE said clients in industries like manufacturing and supply chain were testing its cloud service. And on Nov. 20 2018, Microsoft expanded its partnership with consortium R3 to make it easier for financial institutions to deploy blockchains in its Azure cloud. Big Blue, meanwhile, has been one of key companies behind the Hyperledger consortium, a nonprofit open-source project that aims to create efficient standards for commercial use of blockchain technology.

Blockchain and AI:

Artificial intelligence (AI). BT powered by AI is the most advanced IT development taking place in the blockchain and cryptocurrency market. AI provides several features to manage decentralized monetary systems. AI algorithms can be used to predict the value of bitcoins, which can help bitcoin traders to manage bitcoin transactions. It will also help the customers to have easy access to comparative information and will allow investors to be better informed before making decisions about their financial plans. This, in turn, will augment growth in the global BT market during the forecast period.

Blockchain Market Forecasts:

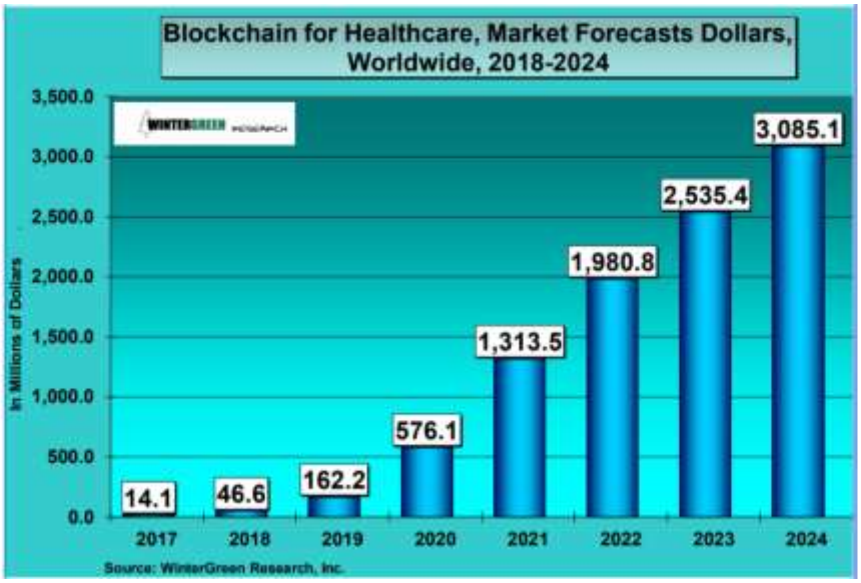
The digital ledger market for blockchain products and services is anticipated to reach $60.7 billion in 2024, up from $708 million in 2017. IBM and Microsoft are driving blockchain as their clients are making the transition to cloud services. Accenture has measurable market share as well. Private investments into blockchain companies topped $4.5 billion in 2017. This is 8 times more than the same period in 2016. There are 15.2 million users. That is 0.2% of the global population. A new law paves the way for Bitcoin to be more frequently used in daily transactions. The impact of blockchain technology goes well beyond Bitcoin, it promises to re-make the banking and finance and insurance industries. It promises to create digital currency for all transactions. Blockchain brings together shared ledgers with smart contracts to allow the secure transfer of any asset. Physical assets like a shipping container, financial assets like a bond, and digital assets like music can be transported across any business network. Blockchain does for trusted transactions what the Internet did for information.



Source: WinterGreen Research, Inc.

Blockchain for Healthcare:

The Center for Disease Control and the General Services Administration are experimenting with pilot blockchain projects from IBM. Experts from the Centers for Disease Control and Prevention (CDC), Aetna, and the Altarum Institute see blockchain as an essential technology for healthcare technology. Blockchain for healthcare markets at $14 million in 2017 are anticipated to reach $3.1 billion by 2024.



Source: WinterGreen Research, Inc.

And publicly, the Trump Administration has doubled down on its commitment to adopting blockchain technology in government operations, two senior White House officials said in September 2017.

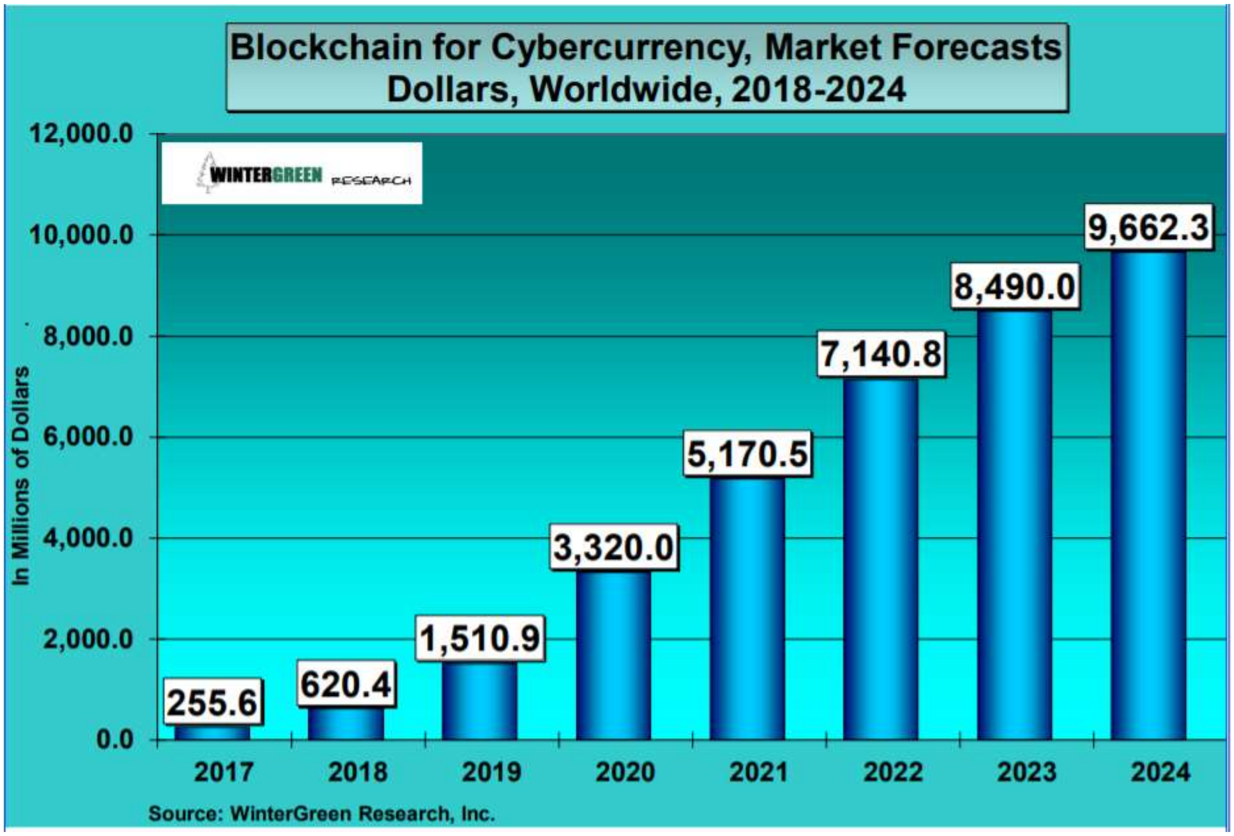
Framing IBM's broad strategic thrust around cognitive computing, Rometty told her audience, "Analytics, cloud, mobile—those are all very important to be a part of the digital society and economy. But when everyone's digital, then what? I always think of digital as foundational; I believe it is disruptive… It is the dawn of a new era. Think of digital business and business intelligence put together, and that will give you cognitive," she said. Very importantly, she said, "It's data that's visible and invisible." In fact, she said, in terms of the digital data available worldwide, the volume of that data is hard to comprehend, as it is now estimated to fill 150 exabytes, or "3 million times all the written books in the world. This year, the volume of digital data will reach one zettabyte, or the equivalent of 30 million times all the data in all the books in the world." And yet, she quickly added, 80 percent of data is unstructured, and in healthcare, that means data in such stores as doctors' notes, patient monitoring machines, wearables, and sound forms.

Rometty also announced the formation of a new initiative inside IBM. "We've been widely recognized for the Corporate Services Corps, modeled after the Peace Corps. Thousands of IBMers have helped with communities. Now we're going to focus that program on helping to increase access to care around the world. That could be water, transportation, food safety, and the like. But every team will have a new teammate, Watson. We've had two pilots for this already," she explained. "We've done a U.K. pilot, in one borough, on obesity and early mortality. And Watson has ingested all the field notes with all the caregivers and in fact has designed fitness solutions for many. We've also been working with the African

Health Placements group in Johannesburg. They hire people who give care in the last mile. We are working on an app to get care to people faster.” In the end, Rometty said, the ongoing Watson initiative has a very future-oriented and strategic purpose. “Healthcare has the opportunity to dramatically change,” she said. “And we understand something about dramatic change. But we also understand something about the promise of change. This industry has very talented people, very committed to change. That’s why we’ve invested in this as one of our moonshots. This will drive this industry to value and outcomes-based. It will allow collectively the ability to tackle some of the greatest challenges our world has seen in healthcare. And it will generate a new generation of talent. So, we’ve taken a different approach. It is about an open ecosystem. It’s standards-based, regulatorily compliant, and open to all."

Blockchain for Cybercurrency and legal industry:

R3 has traction in the cybercurrency markets as a blockchain technology. Ethereum smart contracts have great potential to increase efficiency in the legal industry. These self-enforcing contracts ensure that only once specific terms are met will the contract follow through with its instructions. A smart contract will always run exactly as written, so great care must be taken when creating one. Blockchain for cybercurrency at $255 million in 2017 are expected to reach $9.7 billion in 2024.



Source: WinterGreen Research, Inc.

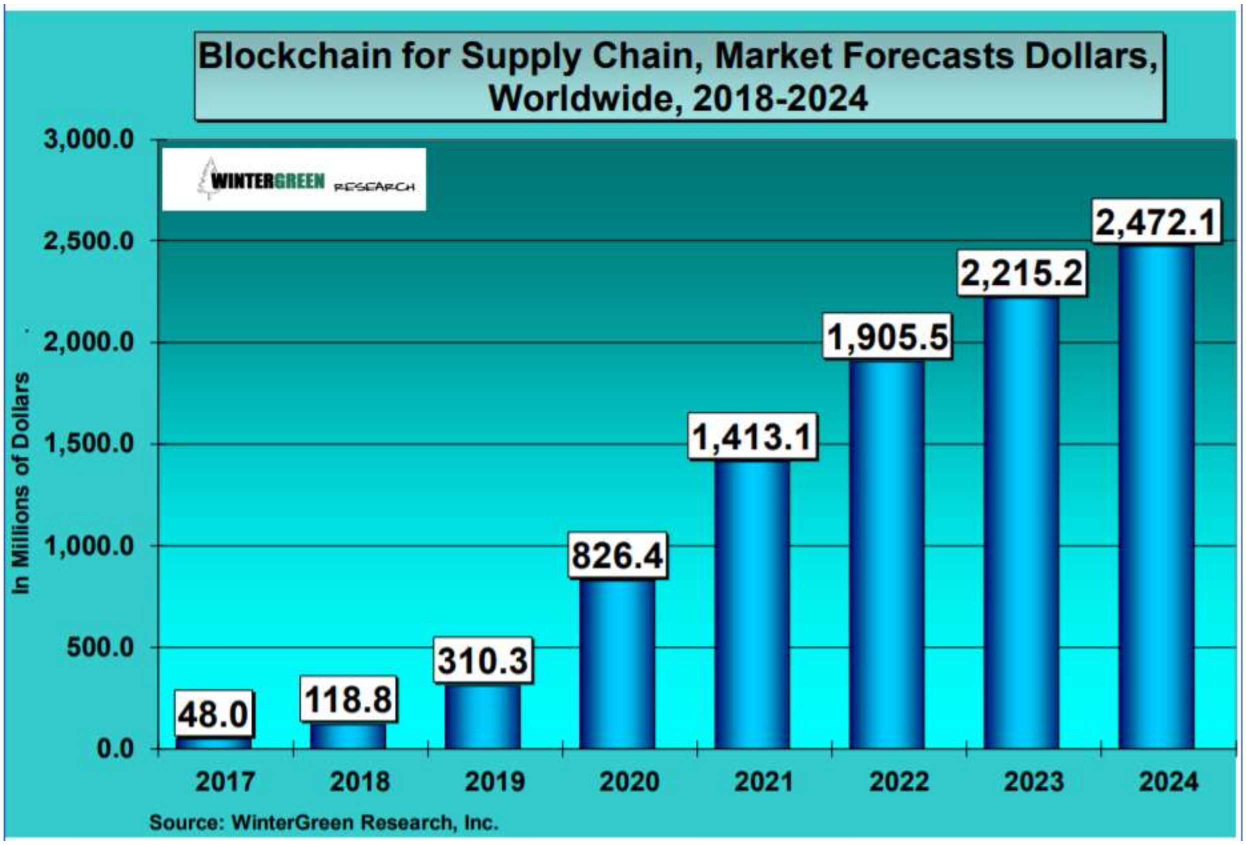
Law firms are part of this cybercurrency blockchain market. Due to their immutable and autonomous nature, smart contracts provide an alluring alternative to traditional legal contracts, and law firms are taking notice. In August of 2017, ten law firms and four legal institutions joined the Ethereum Enterprise Alliance. Among these is Hogan Lovells, the 14th largest law firm by revenue in the United States. This is a big deal, as it signifies Ethereum’s adoption by major law firms, and with it, the adoption of smart contracts. However, legal interest in smart contracts goes beyond the EEA. Frost Brown Todd (FBT), a

500+ attorney law firm based in the US, has taken the initiative to understand the implications of smart contracts in the legal field. In May of 2017, FBT announced their completion of a prototype smart contract to be used in software escrow agreements. Attorney Josh Rosenblatt, head of FBT's Blockchain team was able to get first-hand experience with smart contracts. He stated that: "For a lot of people in the industry, until you get your hands dirty, it's hard to understand what the advantages and disadvantages really are." While smart contracts are certainly a viable option for law firms, it's unlikely that attorneys will be working alone to create them. Attorneys generally don't have the technical skill set needed to do so. Smart contracts are written in computer code, so third party smart contract specialists would likely be pulled in by law firms to collaborate with attorneys. This means that while smart contracts may ultimately replace traditional contracts, they demand a new set of skills to do so. This may slow adoption of smart contracts in the legal industry. The immutability of smart contracts is a double-edged sword. When written correctly, it ensures a contract is successfully carried through regardless of the circumstances. When done poorly, it can open up the contract to exploitation.

Carefully laying out clauses and edge cases can take a long time, as great care must be used when programming a smart contract. Until a standard format for legal smart contracts is laid out, these contracts may not make a routine appearance in the legal industry. Smart contracts can streamline and enforce legal contracts, but they aren't going to be replacing attorneys. In fact, smart contracts need attorneys to help lay out their terms and conditions. It's more likely that smart contracts will bring developers and attorneys together to collaborate and provide progressive solutions for the legal industry.

Blockchain for Supply Chain:

Blockchain is a decentralized ledger that can be used to streamline processes while keeping them secure. In supply chains instead of each business in the chain (manufacturer, shipper, buyer) all using their own paperwork for tracking and invoicing, the blockchain allows everyone to see each step in an open, secure ledger. IBM has a lead in blockchain technology. IBM has been developing blockchain to implement distributed databases. These are positioned to implement IoT and supply chain applications, going way beyond crypto-currencies. IBM has put the technology into production for its own supply chain. IBM has positioned to bring blockchain adoption to financial institutions, which have recognized the technology's benefits but have been cautiously slow to adopt it. Banks are accepting the blockchain cloud platform from IBM. IBM has been selected by a consortium of seven large European banks to build and host Digital Trade Chain, a trade finance platform based on blockchain, designed to simplify and facilitate domestic and cross-border trade for small and medium enterprises. IBM has implemented enterprise blockchain to help quickly bring a highly scalable system into production IBM has a collaboration with 10 food suppliers, including brands Nestlé, Tyson Foods, Unilever, Walmart, and Kroger, to track food products from farm to grocery store shelves in the interest of efficiency and food safety. This market becomes a $2.5 billion market by 2024.



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 lead to enormous interest in cryptocurrecies, which in turn lead to it interest among entrepreneurs and developers towards the applicability of the technology beyond cryptocurrencies.

Currently,technology giants 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 take 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 currecy 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 very discussed in terms its ability to support this new type of currency or so called cryptocurrecy 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 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 decdes 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

A major challenge of blockchain networks is related to the technical scalability of the network which can put a strain on the adoption process, especially for public blockchains. In contrast, legacy transaction networks are known for their ability to process thousands of transactions per second. Visa, for example, is capable of processing more than 2000 transactions per second. In contrast, the two largest blockchain networks, Bitcoin and Ethereum fall short when it comes to transaction speeds. The Bitcoin blockchain can process three to seven transactions per second, and Ethereum can handle approximately 20 transactions in a second. Compared to their centralized counterparts, this gap in performance deems the technology as non-viable for large scale adoption.

A potential solution for the scalability issue consists of adding a second layer to the main blockchain network in order to facilitate faster transactions. Also known as second-layer scalability solutions or off-chain solutions. These solutions consist of secondary protocols built on top of the main blockchain where transactions are ‘off-loaded’ from the main blockchain to save space and reduce network congestion.

For example, the Lightning Network is a second-layer scaling solution for Bitcoin. It incorporates smart contract layer on top of the Bitcoin blockchain, which in turn facilitates creation of private, off-chain pathways that allows instantaneous transactions. The key idea behind the Lightning Network is that it lightens the computing load of the main blockchain by moving the transactions off the main chain to a secondary chain. Since the transactions inside payment channels are between two parties, the transactions need not be broadcasted to the public blockchain network. The transactions are broadcasted to the main blockchain only when the parties decide to close the channel. The advantage of this approach is that transactions are executed within this side-channel are instant, requiring minimal computing.

Plasma is another off-chain scaling solution. Devised for the Ethereum blockchain, it makes use of ‘child chains’ that stem from the original blockchain (also referred to as the parent blockchain). Each child chain functions as a separate blockchain that processes its own transactions while relying on the security measures deployed on the parent blockchain. Each child chain operates independently and runs parallel to each other, which boosts the speed and efficiency of the system. Furthermore, each child chain can have its own set of rules and qualities. This means that child chains can be designed to process only a specific category of transactions.

Scalability is less of an issue for private blockchains since the nodes in the network are purposely designed to process transactions in an environment of trusted parties, which makes sense business-wise.

Lack of interoperability

Blockchain has now become a rapidly expanding industry with a large number of players, platforms, approaches and usecases/solutions. With so many different networks and approaches, the blockchain space is in a state of confusion with no clear approach and a lack of standards do not allow different networks to communicate with each other. Currently, most of the blockchains present in the market work in silos, incapable of sending or pulling information from another blockchain. While the lack of interoperability allows blockchain coders and developers freedom and space for experimentation, it makes the task of IT departments very hard because the platforms cannot communicate without external software that allows the platforms to communicate. A recent report highlights that on GitHub, over 6,500 projects are leveraging a variety of blockchain platforms with different protocols, coding languages, consensus mechanisms, and privacy measures. Standardization is required to help enterprises collaborate on application development, validate proofs of concept, and share blockchain solutions as well as making it easier to integrate with existing systems.

As time passed, various projects have emerged that offer interoperability among different blockchain networks, such as Ark, which uses the SmartBridges architecture to address this dilemma. Ark claims to provide universal interoperability, and cross-blockchain communication and transfers. Another similar project is Cosmos, which uses the Interblockchain Communication (IBC) protocol to enable blockchain economies to operate outside silos, and transfer files between 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.

Blockchain technology creates the most business value for organizations/companies when they work together on areas of shared pain or shared opportunity – particularly problems that are intrinsic to each industry sector. The current approaches involve different organizations developing their own Blockchain models and applications to run on top of their existing architecture. In every industry sector, several Blockchains are being developed by different organizations as per different standards. This defeats the purpose of distributed ledgers, fails to harness network effects and can be less efficient than current approaches.

The Blockchain technology is emblematic of a shift from the traditional ways of doing things – even for industries that have already seen the significant transformation from digital technologies. It places trust and authority in a decentralized network rather than in a powerful central institution. And for most, this loss of control can be deeply unsettling since there is no avenue for legal recourse in case the application or system based on this technology is compromised.

Lack of frameworks to estimate lifetime costs and measure benefits

The speed and effectiveness with which Blockchain networks can execute peer-to-peer transactions come at a high aggregate cost, which is greater for some types of Blockchain than others. This inefficiency arises because each node performs the same tasks as every other node on its own copy of the data in an attempt to be the first to find a solution. For the Bitcoin network, for example, which uses a proof-of-work approach in lieu of trusting participants in the network, the total running costs associated with validating and sharing transactions on the public ledger are estimated to be as much as $600 million a year and rising. This total does not include the capital costs associated with acquiring specialist mining hardware.

A limited knowledge available on use cases and success stories also pose a challenge for selecting the right use case & appropriate approach to implementing the solution as this involves an investment of permanent nature.

Regulation and governance

Government regulations struggle to keep up with advances in technology, especially in the Indian context. Some technologies like the permissionless Bitcoin Blockchain bypass regulation completely to tackle inefficiencies in conventional intermediated payment networks. One of the other challenges of the Blockchain approach, which was also one of its original motivations, is that it reduces oversight.

While cryptocurrencies like Bitcoin offer pseudonymity (Bitcoin transactions are tied to ‘wallets’ rather than to individuals), many potential applications of the blockchain require smart transactions and contracts to be indisputably linked to known identities, and thus raise important questions about privacy and the security of the data stored and accessible on the shared ledger.

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.

In most cases, when an organization decides to integrate its legacy system with a blockchain, it has to completely restructure its previous system, or devise a way to successfully integrate the two technologies. The problem is that due to the lack of skilled developers, organizations do not have access to the necessary talent pool to engage in this process. Reliance on an external party can alleviate this problem, but most solutions present on the market require the organization to invest a significant amount of time and resources to complete the transition. Also, the high incidences of data loss and breach are sufficient to discourage most companies from transitioning to blockchain.

Recently, new solutions emerged which enable legacy systems to connect to a blockchain backend. One such solution is Modex Blockchain Database, a product designed to help people without a background in tech, access the benefits of blockchain technology and remove the dangers posed by the loss of sensitive data.

Modex BCDB is a new take on blockchain technology which removes the need to invest resources in blockchain training and facilitates fast adoption of the technology in businesses. The solution proposed by Modex is a middleware that fuses a blockchain with a database to create a structure that is easy to use and understand by developers with no prior knowledge in blockchain development. As a result, any developer who knows to work with a database system can operate with this solution, without needing to change their programming style or learn blockchain. Modex BCDB is able to transform with minimal changes any type of database into a decentralized database which holds the same valuable characteristics inherent to blockchain technology: transparency, increased security, data immutability, and integrity.

Every enterprise is reserved and unwilling to make changes to its database, and for good reason, as data loss or data corruption constitute major risks. Modex BCDB doesn’t work by deleting the existing database, or data entries. The database is maintained intact throughout the process, data integrity is ensured by calculating the metadata of the records and storing it on the blockchain.

Data Portability

As with other record keeping systems, once data is logged in one system, transferring that data to a new system may be problematic. This issue impacts many blockchain applications. Once a user chooses to use one blockchain, they are unable to remove their previous records of transactions and transfer them to a new system as those transactions are part of the blockchain and any alteration to the chain would result in users being unable to generate legitimate hash values for new blocks. The existence of that data is permanent on the blockchain.

Additionally, if a user seeks to copy their data from one blockchain to another, there are no standards for data construction from one blockchain to the next, so all the elements of data from one blockchain may not be imbedded in another, nor will how they process public-private keys or hash values. The lack of standards in blockchain technologies extends beyond how data is stored to how public-private keys are generated, how hash values are generated, and how data is broadcast across peers. The lack of standards effectively means that once a user chooses one blockchain for their use, they may be unable to transfer to another blockchain. While they may be able to recreate their current allotment of resources on a new chain and conduct transactions from that point, their history will be encapsulated on the previous chain.

Ill-Defined Requirements

As with adopting any technology, adopters must examine the business, legal, and technical aspects of adopting blockchain. Because blockchain is in the early stages of its development and adoption, users are likely to face a set of questions that do not have clear answers. What is the business case for the technology? Do customers demand attributes that the new technology provides? Will employees benefit from the use of the technology? What are the legal implications for using the new technology? Will adhering to compliance regimes be easier or more difficult? Will data held in the new technology be accessible to auditors for review? Will it inhibit regulated transparency? Finally, what particular technology will be adopted? What are the attributes to that technology (e.g., using one hashing algorithm instead of another)? How will it affect current business or management practices, and how might it adapt over time?

User Collusion and Control

Groups of users on the blockchain may combine computing resources and collude to mine blocks. In some blockchain implementations this is allowed and encouraged. However, it does present a situation where groups of users may wield unintended influence over which transactions make it into a block, and the blocks that are posted. Additionally, a user, or group of users (the attacker) with sufficient computational power may be able to recreate the blockchain, thereby altering previous transactions and broadcasting to blockchain users that the attacker’s chain is valid. As it would be the longest chain, other users may automatically accept it, even though it was illegitimate. This is called the 51% attack. While it is computationally difficult to carry out against established blockchains, it may allow an opportunity for nefarious users to corrupt a new blockchain platform, which has a shorter ledger, thereby ensconcing the attackers as controllers of block creation.

User Savviness and Safety

Another issue that affects other technologies, and one that applies to blockchain, is the level of comfort and knowledge a user must have with the technology in order to properly and safely use it. For instance, many drivers do not know how a car works but can still safely drive a car. Or, many users do not know how computers and networking work, but can still type out and send an email. Safe and efficient lay-user participation is possible because certain design and implementation decisions were made by government (e.g., seatbelt requirements and the need for a driver’s license) and engineers (e.g., simple user interfaces) that enable users to use those technologies. As blockchain technology is developed, adopted, and used, similar design requirements or standards may be necessary to ensure proper use and safe adoption of the technology. As with any new technology, users may also need to be aware of its pitfalls and tradeoffs before adopting it. For instance, stories have circulated that users who own Bitcoin have lost access to their private keys, thereby prohibiting the use of that asset in the future—they effectively lost the asset and, without a central authority, have no recourse to restore that asset.

Legal Challenges in Adoption in India

The RBI has imposed a prohibition on dealing in Virtual Currencies[6] and issued a circular to stop crypto-currency 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 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 compataible 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.

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

[7] https://www.w3.org/2016/04/blockchain-workshop/report

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

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.

Harnessing Blockchain for societal impact[8]

The following eight case studies represent not only what blockchain can do today, but what it promises to accomplish in the future. Each example demonstrates how blockchain has helped to overcome challenges of accountability, security, or efficiency within a specific social sector.

<u>Aid Provision: Building Blocks (UN World Food Program)</u>

This blockchain application addresses the challenges of participation of individuals without bank accounts or government identity documents in financial systems. Currently, organizations like the UN World Food

[8] newamerica.org/bretton-woods-ii/blockchain-trust-accelerator/reports/blueprint-blockchain-and-socialinnovation/

Programme (WFP) coordinate with more than 30 other relief organizations and international financial institutions to deliver aid. Traditional systems not only incur significant banking fees, but also delay transaction resolution between cooperating partners, banks, and the WFP. As numbers of displaced persons increase and cash transfers become a predominant form of aid disbursement, intermediary banking services create inefficiencies and absorb resources.

The Building Blocks program of UNDP is built on the Ethereum blockchain, due to its need for high scalability. Money transfers are represented with digital tokens, which are exchanged for food and supplies. WFP reconciles payments with vendors monthly, bypassing escrow and bank charges while preserving payment security. The initial pilot in Jordanian refugee camps serves over 100,000 people, while significantly reducing bank transfer fees and increasing responsiveness and time-efficiency when acting on beneficiary needs.

Refugee families receive tokens in their digital wallet every month, which can be credited to participating markets in exchange for goods and services. Each family's identity is verified by the existing UNHCR case number via iris scanners (biometric identity) at each vendor. WFP transfers payment directly to the vendor. In this system, cash never enters the blockchain, but represents wealth transfers that are reconciled each week.

By creating a transparent, tamper-proof record of provisions purchased by refugees, blockchain allows relief agencies to directly reconcile payments to each other and to suppliers, reducing redundant activity in auditing payments. Furthermore, the security of blockchain technology removes the need for banks to facilitate transactions and for refugees to carry cash or bank cards, lowering associated costs and potential theft.

The initial pilot underutilized the blockchain's capacity to integrate data from multiple sources, since WFP was the sole party processing information. Once additional parties—such as markets, banks, and other UN agencies—are added, Building Blocks will encounter new governance challenges as more entities access and write to the blockchain.

The potential to secure human rights and improve access to resources extends beyond refugee populations. UNICEF is exploring blockchain applications to crowdsource aid funding, reduce operational expenses, and make field staff more effective. Other examples of organizations working to leverage blockchain to safeguard human rights include a partnership between BTA, Coca-Cola, and the U.S. State Department to combat forced labor in global supply chains which utilize migrant workers. The De Beers Group has announced a project to weed out blood diamonds from supply chains. Everledger is a start-up company building blockchain-based solutions in markets where provenance matters, such as diamonds, art, and wine—proving a consumer appetite for transparency and ethical trade.

Land Records: Republic of Georgia

Land is a principal source of wealth and economic mobility, and land registries grant owners legal authority to leverage property. Ambiguous ownership, corruption, and cumbersome transaction processes increase instances of fraud, erode trust in institutions, and stifle economic mobility. In Georgia, years of corruption enabled by a fragmented registry system crippled trust in a new digital public registry system implemented as a result of government reforms following the 2003 Rose Revolution.

The Republic of Georgia's National Agency of Public Registry (NAPR) partnered with Bitfury in April of 2016 to create a blockchain solution that allows NAPR to verify proof of ownership, while enabling citizens to verify the legitimacy of their documents without exposing confidential information. Citizens now have a transparent and auditable method of ensuring that land registry records remain legitimate.

Citizens register their property through a digital interface, which creates a timestamped hash of the property certificate and uploads the hash to the public Bitcoin blockchain. Timestamping the hash on the Bitcoin blockchain tamper-proofs the documentation and enables its owner to prove that the certificate was authorized by NAPR and any subsequent records disputing their ownership are invalid. A fraudulent record results in a different hash than that registered on the public blockchain, proving the edited record invalid.

By creating transparent and verifiable registry systems, governments can restore confidence in property titling and foster investment and newamerica.org/bretton-woods-ii/blockchain-trust-accelerator/reports/blueprint-blockchain-and-socialinnovation/ 37 economic growth. The decentralized blockchain network reduces the risk of fraud by constantly verifying and reconciling transactions against unique land ownership records. The transparency and resiliency of a publicly accessible blockchain reduces the risk of corruption and restores public confidence in the system.

The Republic of Georgia land management bureaus underwent significant institutional reform beginning in 2004, and already held land registries in a digital format. Nascent bureaucracies like in Honduras, on the other hand, may have incomplete or analog records that are not ready for blockchain implementation. Additionally, encoding records onto a blockchain assumes confidence in the existing registry. Countries must ensure that land registries have not been manipulated before adding them to the blockchain, or else risk codifying injustice into a new registry.

Other countries are pursuing land registries to reduce transaction costs and secure land capital for economic growth. The Swedish Lantmariet is piloting a solution to accelerate real estate transaction speeds from 3-6 months to 10 days. The Dubai Land Department has begun recording property transactions via blockchain, enabling global investors to verify property data and ensure the accuracy, credibility, and transparency of investment transactions. The University of British Columbia partnered with blockchain land registry company Ubitquity to pilot a solution for the Real Estate Registry Office of Brazil to reduce fraud and human error in the recording of land ownership. Land registry solutions are projected to benefit developing countries with lower levels of institutional trust, where a projected interest rate reduction of 0.1 percent "would create USD $14B per year in added value worldwide," opening up new sources of capital for millions of landowners.

Supply Chains: Walmart

While retail food stores safely provide fresh produce to their consumers the vast majority of the time, food contamination poses severe dangers to consumers, retailers, and farmers. Tracking the sources of food products through the supply chain is notoriously difficult and time consuming. Paper-based systems are susceptible to human error, and digital data systems are often siloed and unable to trace the full journey of a product from farm to store. When food contamination is discovered, stores must implement sweeping recalls despite only a small fraction of products being affected, costing millions of dollars in wasted food and labor, and posing significant danger to the public.

Walmart leveraged IBM’s Food Trust technology, a private blockchain built on Hyperledger that can traces food production in retailer supply chains. Food Trust stores data on a traditional database and exports a record of changes to the blockchain, which ensures data privacy of supply chain partners, maintains high scalability, and aligns with existing industry standards. Initial pilots in Spring 2017 reduced trace time from days or weeks to seconds, encouraging Walmart to implement Food Trust as a requirement for all suppliers of fresh produce by September 2019.

Workers within the supply chain upload food processing data to the blockchain via a standard naming convention so goods can be consistently tracked across suppliers. Between each exchange of ownership, the blockchain confirms the origin, path, destination, and entry date of the product. Authorized users can then verify food provenance to determine the scope of the problem, determine contamination origins, and conduct more precise recall measures from affected retailers, creating transparency and accountability that doesn’t exist in the original system.

Blockchain provides a tamper-resistant and decentralized way to trace a food item from its origin to its point of sale at a store. By requiring food producers and logistics workers to input transportation data onto the blockchain as a product travels through the system, retailers can transparently and accurately trace dangerous food items directly to their source, reducing the risk of foodborne illness and passing on savings to consumers.

IBM Food Trust is a private and permissioned blockchain that restricts visibility of data to authorized users. While this enables transparency within the distributor’s network, it excludes other important entities such as regulatory agencies and research institutions from accessing data, limiting accountability to the public and depriving public-interest organizations from capitalizing on data. Inclusive permissions can enable third party read-access to the food supply chain while restricting write-access to authorized distributors, which would more fully employed the benefits of blockchain openness and provide impactful data to organizations operating in the public interest. Additionally, tracking non-digital assets increases the probability of errors and requires external structures to encourage correct data entry into a blockchain.

Despite its reliance on human input, Walmart leveraged a blockchain system that considered the needs of users, scaled carefully after early pilot success, and worked alongside redundant system for added security. Blockchain has diverse applications beyond food supply chains. The World Wildlife Fund launched a pilot to improve traceability of fishing practices in the Pacific Islands and help mitigate illegal and unregulated fishing. Maersk built a blockchain to more efficiently fulfill shipping orders, reducing wasted cargo space and diminishing marine shipping traffic in the long-run. These are a few examples of how blockchain can securely track assets and increase efficiencies within supply chains.

Energy Management: LO3 Energy and Brooklyn Microgrid

Newly affordable sources of renewable energy enable households to produce and consume power locally, creating a more efficient energy grid. However, the current centralized model of energy distribution is inefficient and restrictive. Establishing a decentralized model of energy infrastructure is crucial as energy demand evolves and fossil fuels exacerbate climate concerns.

LO3 Energy created a local energy marketplace which enables solar panel owners (“prosumers”) to buy and sell energy locally over existing electrical infrastructure. The Brooklyn Microgrid uses its blockchain based marketplace to connect various solar sites to customers, who can buy and sell local power while preserving the utility provider maintenance of the electrical grid. This solution promotes a sustainable clean energy model, increases electrical grid efficiency and resiliency, and drives down costs for consumers.

Participants access the local energy marketplace through the Brooklyn Microgrid mobile app. In the app, people can choose to buy local solar energy, renewable energy produced outside of the Brooklyn, New York area, and/or grid energy. Prosumers sell their excess solar energy onto the marketplace for consumers to bid on. Local solar energy is “won” by consumers via an auction. Prosumers can sell their excess energy on the marketplace once they have installed a Brooklyn Microgrid smart meter system, which gathers and records energy data for use within the energy markets. The marketplace is scalable to communities all over the world via Exergy, an open-source platform and token system for managing and permissioning access to energy data. As a foundational protocol, Exergy enables digital applications, such as the Brooklyn Microgrid marketplace, to be deployed almost anywhere.

Blockchain provides a decentralized infrastructure, a secure method of recording transactions, and a transparent interface. Smart contracts built into the blockchain enable the marketplace auction mechanism. The distributed functionality will allow for millions of users and devices—with different incentives—to participate in the market over time.

Brooklyn Microgrid is aiming to change the way electricity is bought and sold. Although this innovative approach is in alignment with New York’s energy policy “Reforming the Energy Vision,” it requires a revision of the existing regulatory framework. Currently, this model functions on a small scale, but may receive industry pushback as it scales. Additionally, the pace of expansion will be limited by the installation speed of and excess supply from local solar panels. Therefore, owners feel the network effect benefits until a critical mass of additional participants are established.

LO3 Energy and other organizations continue to test how blockchain technology can democratize access to sustainable energy. LO3 Energy also partners with Centrica to test a similar peer-to-peer energy exchange market in Cornwall, England. The energy needs of the twenty-first century require innovative ways of producing and effectively allocating power to the world’s population. Blockchain technology offers a secure and decentralized structure to ensure that new infrastructure is equipped to handle this need.

Financial Inclusion: AgUnity

Smallholder farmers in developing countries greatly benefit from cooperatives in which they can collectively bargain for better prices for their goods, share equipment, and circulate best practices. However, restricted access to information and corruption within cooperatives erode trust in the system, disrupt transactions, and create financial losses.

AgUnity provides smartphones to farmers that are pre-loaded with the app, ensuring that farmers use compatible hardware for the program and utilize secure devices when accessing the AgUnity blockchain. Built on the Multichain blockchain platform, the app can operate offline in rural areas until an internet connection is reestablished. The pictographic interface is customizable, enabling different crop types and cultural nuances to integrate into the platform. Initial pilots in Kenya and Papua New Guinea demonstrated a 300 percent increase in income for farmers equipped with AgUnity devices.

Farmers log on to record crop-processing transactions and sales. The transactions are visible to all other members, ensuring transacting parties follow through on agreements. Each farmer is assigned a digital wallet which stores receipts, which are then converted to cash upon arrival at the cooperative. AgUnity also provides encrypted messaging services for farmers to collaborate on harvest planning and equipment sharing.

Blockchain creates a permanent record of transactions, enabling farmers to be confident that agreements with cooperative representatives will not be changed without their consent. Furthermore, the record is auditable by other members of the cooperative, providing transparency and accountability to farmers who are concerned that crop brokers might renege on their commitments.

Despite the efforts to instill trust in the cooperative system, AgUnity centrally controls transaction records, identity data, and programming on participating devices. This requires farmers to trust AgUnity as a mediator and limits expansion. Additionally, farmers are not paid independently of financial institutions and must exchange digital credits for cash (although integration with digital cash platforms like M-Pesa are forthcoming). Lastly, there is no independent validator of transactions and farmers still rely on off-chain enforcement if a cooperative defaults on an agreement.

AgUnity continues to expand its financial inclusion offerings, including digital wallet capabilities and securitized loans. Other blockchain companies are addressing gaps in financial services in developing countries. BitPesa is a mobile payment system that lowers transaction costs and manages risk, bringing stability to communities and fostering economic mobility. WorldRemit provides blockchain-driven remittance services that are nearinstant, secure, and direct, encouraging financial exchange and providing stability to beneficiaries. Building financial tools for marginalized populations is a critical component of achieving global development goals, and blockchain will be central to successful financial inclusion.

Voting: West Virginia

Overseas military members and their families have few choices when it comes to voting in U.S. elections. Currently they must either mail in their ballot, fax or email it to a county clerk's office, all of which have proven to be cumbersome (and often impossible) for uniformed service members in remote areas of the world. But military members have no guarantee that their vote will reach their clerks in time, be counted, or remain private and secure throughout the process. These factors reduce the ability, willingness, and motivation of service members and overseas voters to participate in the democratic process.

The Office of the Secretary of State of West Virginia, in partnership with Voatz, Tusk Montgomery Philanthropies, and the Blockchain Trust Accelerator piloted a mobile voting application powered by blockchain in the 2018 Primary and General elections in accordance with state and federal regulations for absentee ballots. The initial pilot was limited to West Virginia UOCAVA (the Uniformed and Overseas Citizens Absentee Voting Act) eligible voters registered in Harrison and Monongalia Counties for the Primary election, then scaled up to 24 counties in the General election.

The first vote in a U.S. federal election cast through a blockchain-based solution was cast on March 24, 2018—the day absentee voting opened in the 2018 West Virginia primaries. The first vote cast in a general election was hashed to blockchain on September 21, 2018. In the Primary election, 13 votes were cast through the solution. In the General election, 144 votes from voters in 31 different countries were cast out of 160 voters who applied to use the technology.

Eligible voters complete and submit the Federal Post Card Application (FPCA) to their county clerk. Once the FPCA is received and the voter's information is confirmed, voters are prompted to download the Voatz app, verify their identity and eligibility using biometric security measures, and then complete the voting process securely and privately through their smartphones or tablets.

Blockchain enables voters to submit their election ballots through a distributed, cryptographic ledger that has no single point of failure and cannot be edited. Furthermore, votes remain auditable by election committee officials without providing personally identifiable information about a voter, providing the same anonymity that poll voters are guaranteed.

While the blockchain mobile voting process is a significant improvement to existing systems for overseas voters, a number of concerns remain. Mobile voting requires voters to have smartphones or tablets, and despite the security measures that blockchain offers once data is recorded, unsafe internet connections and/or unsupported devices may impact the ability of a voter to submit a ballot successfully. The application utilizes sophisticated malware detection software, which will disable the application and prevent a ballot from being accessed if the device is deemed insecure. In that case, alternative methods of absentee voting remain available to those whose devices are insecure, and to those who do not own or cannot operate a smartphone. However, like all technology, security must be constantly monitored and updated as nefarious actors adapt and look for ways around the current protections.

Blockchain has the potential to transform the way citizens interact with their government and restore trust in the institution of voting. The city of Zug, Switzerland recently leveraged a blockchain-powered mobile voting platform by Luxoft for its municipal elections. The Republican Party of Utah partnered with Smartmatic to offer its party members the ability to vote from anywhere in the world for the 2016 Republican Presidential Caucus. As the technology matures and more election officials and the general public increase their understanding of the system, blockchain-powered voting will provide citizens with a responsive, effective, and trusted method by which to engage with their government.

Social Investment: Neighborly and City of Berkeley Blockchain Initiative

Municipal bonds have long been a key source of funding for public projects. By connecting investors with local governments issuing bonds, they fund civic investments like schools, libraries, and parks. However, complex regulations and a scattered bond landscape create barriers for willing investors, preventing communities from accessing capital when needed. Furthermore, investors encounter challenges when tracking the impact of their investment, leading to accountability issues that dissuade investment within communities.

Elected officials with the City of Berkeley partnered with Neighborly and the UC Berkeley Blockchain Lab to explore building a platform that would facilitate investment opportunities between residents and the city for as low as $10. By broadening the range of investors and investment opportunities, City of Berkeley officials seek to empower residents to invest in projects that are significant to them, expanding the types of projects that could be funded with municipal bond financing given current federal, state and local regulations.

Investors will buy tokenized municipal bonds, denominated in U.S. dollars, that will enable the city to allocate resources more broadly and quickly, but also to create new initiatives such as food vouchers for the homeless. Since local investors will have better access via the blockchain enabled financial tools, it could be increasingly easy for investors to indicate a project they would like to fund, discover how their funds will contribute to the project, and review investment characteristics.

Blockchain technology can bypass middlemen and decrease transaction costs, enabling small investors and municipalities to easily form mutually beneficial partnerships. Decentralization enables companies like Neighborly to store financial information accurately and cheaply, while an auditable trail provides "Know Your Customer" audit compliance. Finally, blockchain tracks all financial movements to prove that investments have been spent as intended.

This pilot is in its infancy and few details have been published about the mechanics of the blockchain solution. However, blockchain would enable varying degrees of data viewability, instilling transparency and accountability for regulators and investors. While blockchain makes the transaction process between issuers and investors easier, more accessible, more efficient, and more transparent, project selection will be contingent on the local governments issuing the bonds.

The efficiency and transparency challenges in procurement, fundraising, and social investment are well-suited for blockchain intervention. AidCoin built a fundraising platform that tracks contributions through blockchain to lower fees and offer clarity into how funds are being allocated. St. Mungo's, a charity based in London that provides services to the homeless population, uses a blockchain transparency tool called Alice to track contributions in real-time and reallocate funds as new priorities arise, giving more power to donors to choose how their contributions are utilized. Blockchain offers the security and accountability that communities and charities seek to revitalize trust and galvanize social good investments.

Environmental Sustainability: Plastic Bank

Every year, approximately 8 million tons of plastic enter the oceans, adding to the over 4 trillion pounds of plastic currently destroying marine ecosystems, endangering food supplies, and degrading living conditions for millions of coastal communities. Over 80 percent of waste is generated by populations with insufficient waste management systems. Garbage can provide income for millions of marginalized people living in polluted areas through recycling redemption programs. However, cash transfers invite crime in underdeveloped societies and currency localization inhibits organizations from growing to meaningfully impact the enormous accumulation of plastic on the planet.

Plastic Bank partnered with Cognition Foundry and IBM to create a mobile app to track the amount of recyclables submitted to local drop off depots in participating areas. Local populations download the app onto their smartphone and collect plastic in their neighborhoods. Collectors earn digital tokens by weight that they can either redeem for currency or spend at participating stores, Wi-Fi hotspots, and phone charging stations. The plastic is then exported to factories processing sustainably-sourced plastics.

The growing ubiquity of internet-enabled smartphones allows blockchain to provide financial services to previously inaccessible populations. Failure-resilient, secure transactions offer a reliable and safe method of earning and spending income. Rather than constructing a centralized network, blockchain enables decentralized ecosystems in which local plastic collectors can directly connect with manufacturers without any intermediaries managing the relationship.

Despite the wide adoption of smartphones and significant gains in internet connectivity, Social Plastic still relies on internet connectivity to provide financial services to its clients. While they do not need connectivity while collecting plastic, transactions that occur outside of covered areas will not benefit from immediate transaction resolution. Also, income for collectors is contingent upon companies paying above-market prices for recycled plastic. The success of this model relies on sustained demand for ecologically responsible products.

Other organizations are leveraging the power of blockchain technology to repair and protect the environment. Sustainability International's Clean Up Niger Delta project pays community members via digital currency for completing clean up assignments, then documents it on the blockchain. In another project, IBM partnered with Chinese Energy-Blockchain Labs to build a carbon asset management system on Hyperledger, reducing the cost of participating in carbon credit exchanges and helping businesses emit less carbon into the environment. Blockchain technology enables small groups to create economically viable environmental cleanups around the globe by storing verifiable information about pollution trends and repairing the environment through decentralized collaboration.

Combating Fake News: Democracy Notary

Factual proof forms the foundation of all evaluation and decisionmaking, from journalism to policymaking and voter choice. Forgeries undermine the public's ability to make sound judgements or to trust facts when they are presented. Increasing sophistication of photo-editing software, lower barriers to access, and larger networks to proliferate forgeries have eased the circulation of misinformation. Convincing forgeries of photos, videos, documents and voice recordings post severe threats to privacy, national security, and democracy.

Identifying disinformation is only one piece of the puzzle. In partnership with the Design 4 Democracy Coalition, Emercoin, and the Blockchain Trust Accelerator piloted the Democracy Notary platform, which secures official copies of public statements to prove that content is original and legitimate. Its first use case was in relation to the 2018 Macedonian referendum. Built on Emercoin's permissioned blockchain, it permits trusted civil society organizations to upload content and provides the public with read access to compare disseminated reports with verified blockchain entries.

Democracy Notary immutably encodes key documents into a blockchain that can serve as a "truth-check" when manipulated or falsified documents are used as a weapon of disinformation during high-stakes events such as elections. The Design 4 Democracy Coalition aims to eventually give permissions to trusted civil society organizations to post to the Democracy Notary, which converts documents, reports, and other original media of public interest into unique hashes and posts them on the blockchain where it becomes mathematically impossible for data placed in the system to be altered or destroyed. Blockchain, therefore, can demonstrate the integrity of information and make it possible to debunk forgeries and manipulation.

Blockchain technology uses algorithms to assign hashes to uniquely identify data files. Any changes to an original file will result in an obviously different hash, and therefore be easily recognizable as a different file than the original. Blockchains are accessible globally, enabling individuals around the world to easily record hashes of original content and enable others to verify copies of information by comparing their hashes to the catalogued hash of the original.

While the Democracy Notary platform was designed to help citizens find accurate sources of information for elections, challenges remained in driving user adoption. The team sought to embed the technical complexities of the platform behind the user interface to simplify the user experience. Despite its difficulty, creating user-centric interfaces is critical to creating value for end users and for broader adoption of a new technology. Moreover, Democracy Notary experienced challenges in educating the public about its service in the weeks leading up to the election. Platforms that combat fake news should be coupled with sustained public education campaigns to inform concerned citizens of secure, reliable news alternatives.

Blockchain enables immutable timestamping of content, creating a niche for content verification and notary services to make forging information more difficult. Blocksign enables users to sign legal documents and timestamp digital signatures on the blockchain to prove that a document was validated at a certain time without trusted intermediaries. Blocknotary extends these services to any type of media, and offers a video interview process for remote verification of identity. While questions of originating ownership and court eligibility demonstrate off-chain challenges to digital notary services, they offer a significant tool to combat fraud and forgery in public documentation.

In today’s world, widespread uncertainty cultivates fear and suspicion; disillusionment prevails between communities, their governments, and the institutions that uphold societal values. The cooperation which builds successful human enterprise is founded upon trust, but that trust is eroding at an alarming rate. Leaders must analyze the problems they face and their potential solutions. Blockchain technology will not always prove an optimal approach. However, the degree of accountability, security, and efficiency that blockchain lends to recordkeeping systems merits serious consideration by government agencies, nonprofits and businesses attempting to rebuild trust between themselves and the communities they serve.

Blockchain is still in its infancy, and technologists, policymakers, and academics will continue to discover new dynamics of the technology. These will affect both potential and established blockchain deployments. Those considering blockchain systems as well as those who have already adopted them should remain abreast of ongoing developments in the space. In order to achieve full societal potential of blockchain, further research is required to address following challenges.

Digitizing off-chain assets and analog data

Blockchain requires integration with digital data sources, posing challenges to groups limited to analog data. If high-bandwidth connectivity and accurate digitized records remain largely restricted to developed countries, the potential impact of blockchain tech will be significantly limited. As blockchain technology gains traction, limited internet connectivity in certain regions of the world will exacerbate the existing digital divide and may lead to greater global inequality. Accurately converting physical data to digital form will be expensive and time consuming, both in terms of input processes and data accuracy. The latter is especially important considering the difficulty of altering data on the chain. Regardless of potential difficulty, these hurdles must be addressed for blockchain to achieve its full potential as an open, democratic technology.

Refining effective identity solutions

Blockchain solutions require an integrated identity management platform to authenticate users and maintain accountability. The lack of an effective blockchain identity solution creates gaps of anonymity which can be exploited to threaten the integrity of blockchain tech. The development of a secure proof-of-identity on blockchain will facilitate the effective linkage of on- and off-chain activity, potentially transforming the lives of 1.1 billion people worldwide without recorded identity. By providing a verifiable identity, many of the services governments and nonprofits are currently unable to provide, such as aid distribution, land titling, and financial services, will become manageable. Simplifying blockchain governance: Blockchains are rigid by design. The creation of an effective and secure identity solution may also help to simplify protocol changes while minimally impacting the technology's tamper-resistance and security. Despite the technology's inherent inflexibility, the blockchain ecosystem is evolving rapidly. Anticipating bugs and errors within governance models and developing methodologies to improve existing protocols and coursecorrect as mistakes arise is vital to system sustainability.

Instituting blockchain-specific laws and regulations

Regulators must balance the entrepreneurial opportunities of blockchain tech with the imperative to protect human participants. To date, most regulation has centered on cryptocurrencies themselves—not their underpinning infrastructure. While tokens and the blockchains on which they're traded merit consideration, regulation of the base technology can be applied to far more use cases. Particularly important will be to manage how on-chain data impacts the off-chain world; information sharing information, digital signatures, and smart contracts all require a framework upon which to interact with existing legal systems. Doing so will provide much-needed clarity for developers and improve interactions between blockchains and legacy processes.

Developing blockchain ethics

Blockchain technology may involve certain trade-offs, such as efficiency versus security, accountability versus privacy, or permanence versus flexibility. Though many may be tempted to address these questions exclusively through the lens of code and mathematics, these problems —and their potential solutions— stem from cultural norms in future contexts we cannot anticipate. As traditional ethicists construct a code of moral standards and considerations for technologists and policymakers, social values can be better upheld within interactive blockchain ecosystems.

Combatting disinformation through blockchain

Today it seems more vital than ever to re-instill trust in the digital information which comprises and informs current events. Blockchain-verified timestamps and geolocation can combat disinformation in the news and on the web. Blockchain can serve as a supply-chain record for facts, helping citizens to distinguish genuine content from fake news. As these capabilities are further developed and disseminated, they will help to return integrity, clarity, and trust to public information landscapes.

Exploring the intersection of frontier technologies

To address social impact and governance challenges, innovators must consider potential synergies between blockchain and other emerging technologies (such as Artificial Intelligence, Internet of Things, and quantum computing). Tech companies are already considering how these technologies will interact. Social sector innovators should do the same.

Incorporating differential privacy into blockchain solutions

Despite the significant value that collecting and synthesizing large amounts of public data can contribute to effective policy making and service provisions, privacy concerns have become a primary consideration as more personal data is captured by companies and governments. Even though many groups anonymize datasets in an attempt to protect individuals, identities remain vulnerable to discovery through certain coding tricks. Blockchain could exacerbate this problem by offering increased opportunities for data synthesis and access to accurate public data. Coalitions of data scientists, game theorists, privacy experts, and policymakers should consider using methods which prevent the isolation of specific individuals from datasets while maintaining those datasets' openness and completeness.

Cultivating future talent for blockchain solutions

Like computer science a generation ago, blockchain technology is only thoroughly understood by a few programmers and tech firms. There is consensus in the blockchain community that there's a need for more programmers proficient in building blockchain solutions. As the field grows, emerging programming talent should ideally reflect the diversity of a global user base. Blockchain resides at the nexus of several disciplines: cryptography, game theory, tokenomics, network theory. Crosssector blockchain projects, startup-in-residence programs, academia, hackathons, and traditional accelerators will continue to attract new leaders to the discipline as the tech matures.

By facilitating transparency and verity, blockchain technology can create opportunities for collaboration that were previously rendered impossible by boundaries, both digital and physical, and mistrust. The technology's benefits promise to be vast. It will provide the opportunity to facilitate the inclusion of billions left behind by economic progress. Blockchains may also allow for greater coordination among impact organizations, reducing redundant and ineffective spending and increasing the visibility of those having the biggest impact. Greater efficiency and transparency in governance will increase institutional trust and accountability while empowering individuals to make informed, independent decisions about their own data. Digitized records and interoperable government services will equip governments for the twentyfirst century.

Blockchains are not a panacea. As such, the decision to implement them should not be a foregone conclusion. But, in one capacity or another, blockchain will likely play a meaningful role in restoring trust in global civil, governmental, and charitable institutions. More importantly, it will facilitate innovations which improve people's lives. Someday, this technology's benefits will be taken for granted; it will become as mundane and indispensable as scanners and spreadsheets.

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 andleadership across government regarding the development of technology for a digital-block-chain 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 man-agement, 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.

This report highlights the set of challenges and questions for policymakers and regulators including who gets regulated, who is responsible for compliance with those regulations and which activities related to the technology should be regulated. Before, getting deeper into those challenges and questions, there are two important core foundations.

First, it is important to recognize that new technologies are unique in their ability to solve challenges where and when we least expect them. When policymakers think about how to address these challenges, they must recognize the need to maintain flexibility as new challenges arise and that the new technology provides myriad ways in which to solve them. Second, what follows is by no means an exhaustive list of challenges and, therefore, of policy responses. This list merely reflects some of the top priorities.

Safety and Stability of the Ledger

The foremost concern with blockchains is that the new ledger is safe and accessible. This means that users must be able to rely on the accuracy of the information in the distributed ledger and can, therefore, use it reliably to engage in transactions. A similar critical aspect is that users can easily and cheaply access the information whenever necessary.

For example, in order to be reliable, a blockchain based payment system would need to ensure that the ledger itself is accurate, the communication infrastructure is stable and the ledger can be accessed easily so that transactions can be conducted at any time, with only short delays, and in a wide range of situations. It is often hard to assess in its early stages whether a blockchain application offers such features. While sophisticated users will be able to do so, it is far less clear whether the broad public can do so as well.

A prime example that comes to mind is the Mount Gox Exchange where many bitcoin users lost their coin holdings due to a safekeeping loophole. Even more problematic would be incidents where newly created ledgers get compromised due to a design flaw. One leading example is the Ethereum platform that has been recently compromised so that a significant part of its currency could be stolen. Such experiences can lead to a quick loss of confidence in the new technology and problems in the early adoption stages.

Hence, over time, some standards will likely have to be developed to protect consumers from unsafe implementation. This requires a continuous dialogue among regulators, developers and users during the creation of applications. But it also needs a certain degree of monitoring to ensure basic cybersecurity and stability protocols are being followed.

Another concern is the legal certainty of transactions based on the distributed ledger. For users to have trust in the ledger, they must be confident that its information can be used in legal disputes. At the moment, to our knowledge it is not clear how to treat ledger discrepancies or how to change a ledger in response to legal decisions about its entries. This is a particular problem for unrestricted ledgers. One of the design principles in such ledgers often is that everyone has direct access to the ledger, but can remain anonymous. This makes participants potentially unaccountable for their actions. Of course, with restricted ledgers that are permission based, all the nodes can easily be identified and held accountable for their actions. Consequently, in many applications related to financial markets, such ledgers hold a distinctive advantage.

Another particular concern is that any change in the ledger needs to be coordinated and accepted across the network nodes. It is currently not clear how a blockchain would handle mistakes in transactions that have been undone retrospectively in the ledger. Standard blockchain applications like bitcoin, for example, are irreversible and do not have a mechanism that would allow past transactions or records to be adjusted. Similarly, any well-functioning payment system needs to provide a mechanism to undo transactions if requested by the original counterparties.Without a central settlement engine, it is not clear how such a change could be reflected quickly in the ledger.

Anonymity and Regulatory Entry

The very design of a distributed ledger where nodes remain anonymous implies that no party can be readily identified that would be responsible for implementing or complying with regulations. Indeed, the members of a truly distributed system that actively maintains the ledger are often hard to identify and possibly shift constantly over time.

One particular concern is that members could avoid regulation by shifting their activity across borders to escape the reach of any particular regulator. The implication then is a focus on activitybased regulation. Here, rules focus on the activity rather than the institution carrying it out, thus bypassing the need to identify constantly changing "institutions." Activity-based regulation, however, often suffers from regulatory arbitrage. Once an activity has been singled out to be regulated, a network can fairly quickly shift to a slightly altered activity, thereby avoiding such regulation. One can see that this puts enormous strain on current regulatory bodies to keep up with a fast-evolving technology.

Accenture is looking to patent an editable blockchain (Accenture 2016). However, it is not clear how a blockchain that can go back and make amendments will fit in the larger regulatory scheme and assist in resolving legal disputes. All LVTS (Large Value Transfer Systems) payments are final and irrevocable. Any adjustment can be done only through a reversing transaction. It is not clear how that would work under a blockchain-payments system. Such concerns seem to be mute in consensus ledgers that simply agree upon and update the state of records without maintaining a continuous record of transaction histories. Such ledgers are often permission based and have only a few participants with direct access.

In principle, it is possible to trace participants and transactions in distributed ledgers. This is part of the reason why bitcoin – although heralded as granting anonymity – is not seen as a concern for law enforcement. Recent developments, however, such as Zcash claim to have achieved full anonymity rather than what some experts describe as "pseudo-anonymity."

A principle-based approach to regulation has worked in the past to contain such problems in the area of payments and settlements. However, one needs to recognize that such success was tied to having intermediaries in charge of critical infrastructure. With a blockchain-based payment system, however, there might not be a direct counterpart for regulators to monitor to ensure that principles are being followed.

Blockchain applications within financial markets are likely to be permission-based networks with only a limited number of participants. This facilitates regulation and supervision in the sense that it might be possible to still hold institutions accountable for their trades and actions. In this context, however, two different challenges arise. First, participants in financial markets need to stay anonymous as far as their trading strategies are concerned. Hence, distributed ledgers will have to be designed to respect such anonymity among members, but still have to ensure transparency for regulators. This points to a more sophisticated ledger where different entities have different rights to access information. Some new efforts have been undertaken where regulators hold special private/ public keys to have unique access to specific information stored in a ledger.

Second, even in permission-based chains, one has to update the ledger with information that parties might want to keep private from other members. While this seems to inhibit confirming and updating transactions within the ledger with regular protocols, new methods are being designed based on so-called “zero-knowledge proofs” to make distributed ledgers a possibility for trading in financial markets. Once again, regulators and clearing and settlement agents, including a central bank, would need to have access to the information even within an environment where the network members have no access to this information.

Coordination and Network Dynamics

Distributed ledgers are network based and, hence, their viability relies on being accepted among a sufficiently large number of users. In other words, blockchain technology involves network externalities where the benefits of an application increase with the number of participants. Adopting a new blockchain application thus suffers from the requirement that one needs to gain a critical mass of participants to reap the benefits of the technology. The adoption of any new ledger will take time. For example, if a new blockchain-based payment system is to be successful, one needs to ensure that there are sufficiently many potential payees and payers for any individual person or business to accept payments made through this technology. Similarly, too many competing applications that are not compatible may cause a barrier to adopting any payments solution based on this technology.

Hence, one needs to have some degree of coordination when introducing a blockchain alternative or a new application of this technology. Furthermore, the immediate gains from the technology might not be large enough initially for a single private entity to introduce a new application that is beneficial in the long run for itself and an efficient solution for the economy. This implies that existing record-keeping systems will not necessarily be transformed into newer blockchain-based ones, even if it would be efficient to do so. While this does not suggest direct involvement of government, it points to a role for leading industry participants and government to act. Indeed, after the 2008 financial crisis, regulatory efforts such as the Dodd-Frank Act and the introduction of ESMA (European Security Markets Authority) in the European Union make such transparency a cornerstone of financial regulation and supervision.

Government of India could also spearhead efforts to achieve sufficient standardization that allows one to operate a new blockchain-based payments technology nationally and possibly integrate it into cross-border payment applications.

Unfortunately, it is also conceivable that some of the technological change is being driven by rent-seeking and not by efficiency considerations. Rent-seeking behaviour seems especially likely to materialize in the case of financial markets, where blockchain technology offers a tremendous opportunity to reshape market infrastructure. For many intermediaries, there is an imminent risk of being made redundant by the principal users of the infrastructure itself.

At the same time, blockchain technology offers the most benefit in permission-based ledgers with only few direct participants. Consequently, intermediaries at every layer of the trading and post-trading landscape are bound to exploit new market opportunities. In this scenario, if traditional intermediaries are simply replaced by other ones that branch into different areas of financial markets, then efficiency gains and perhaps, more importantly, cost cutting for end users will not necessarily be realized with existing rents simply redistributed.

Therefore, policymakers should be wary of blockchain applications that are designed to purely cut out intermediaries for the sake of recapturing rents rather than to realize efficiency gains that ultimately benefit consumers. Now, there can be positive economic externalities that emerge from a redistribution of rents that do not completely get passed down to end users. However, policymakers need to be aware of how large and truly positive those redistribution externalities are to ensure that regulation and the spread of this technology are appropriate, given incentives to maintain or obtain rents.

Public, Private or Administered Networks Coordination problems and network considerations raise the question of whether distributed ledgers can be arranged in a purely decentralized fashion for critical infrastructure. As discussed earlier, most applications are likely to be driven by new or existing businesses. Thus, it seems reasonable to expect that future blockchain applications will rarely be fully public networks where every user has unrestricted access to the ledger. Consequently, private networks that retain the distributed nature of the ledger, but restrict the right to update and modify it, are thus the most likely outcome.

Of course, traditional intermediaries -- for example, banks and settlement providers in payment systems -- would still play a central role within the blockchain. How users can access and use the ledger then become important design principles. This points once again to private-public partnerships where public involvement guarantees fair access for payment providers and safety for users, while designated parties maintain and update the ledger. Such solutions have the potential to most efficiently use parts of the blockchain idea such as cryptographic communication and the distributed nature of the ledger.

In certain areas, the government would clearly need to take on a more active role in supplying a blockchain application. Any area that requires a very high degree of security should see the government taking a special role in updating and maintaining the ledger. One solution would be distributed networks where the government serves as the network’s centralized administrator. Of course, it is then unclear whether the ledger has to be operated as a blockchain per se. It seems most likely that only features such as public/private key security and distributed storage of the ledger would be essential in such administered networks.

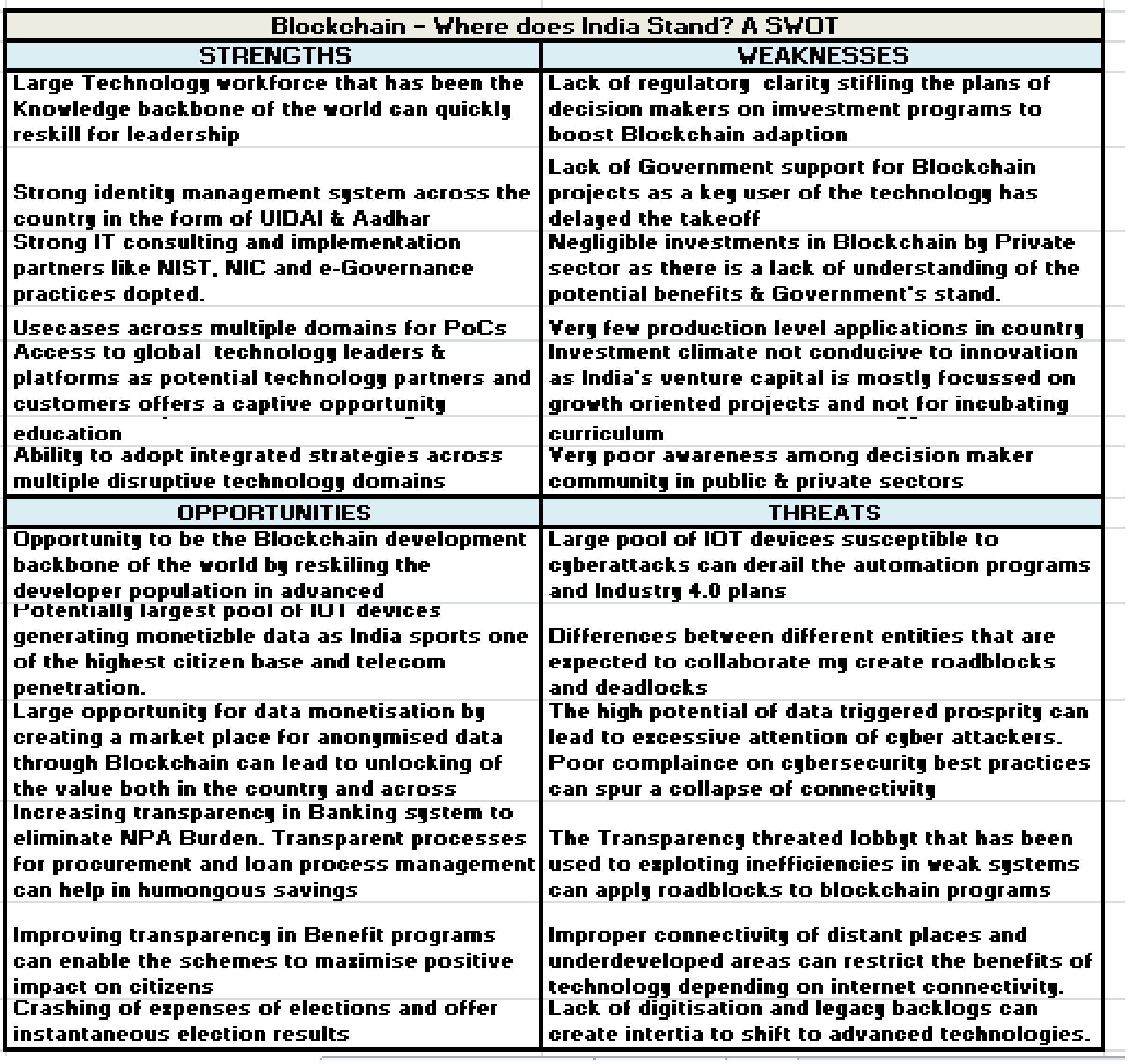
One example would be an integrated national or international system that allows people to access all kinds of online services, Internet sites and computer applications with a unique ID stored and maintained in a single, but distributed ledger. While the records might be distributed among many servers, the updating procedures would probably remain under centralized government control. Indeed, some recent developments like Jasper see a public sector involvement to integrate private efforts to design a new blockchain application.

Our goal has been to unveil the potential of blockchain technology and guide regulators in how to approach the challenges this technology entails. It will also be crucial to achieve safe and secure applications of this new technology without stifling innovation. In determining this balance, policymakers and regulators will have to decide whether to design rules and regulations along a principle-based methodology like was done with the Internet in the 1990s or whether to operate on a case-by-case basis. Given the uncertainty of how blockchain technology will evolve, it seems reasonable, however, to rely only on a relatively narrow set of guiding principles with a view that allows the technology to develop flexibly in different directions over time.The key challenge will be to define public involvement in blockchain applications. Many of its most promising uses lie in areas where critical infrastructure is concerned. Governments do not usually have the same expertise and incentives as private businesses to pursue new technologies. Hence, blockchains will test whether public-private partnerships can really implement frontier technology in a cost efficient and safe way.

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 imvestment 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 dopted.	Negligible investments in Blockchain by Private sector as there is a lack of understanding of the potential benefits & Government's stand.
Usecases 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
education	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 reskiling 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 IOT devices generating monetizble data as India sports one of the highest citizen base and telecom penetration.	Differences between different entities that are expected to collaborate my 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 prosprity can lead to excessive attention of cyber attackers. Poor complaince 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 threated lobbyt that has been used to exploting 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 intertia 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 governemnts have formulated blockchain policies/strategy documents and are attempting to promote this technology to achieve efficiencies in the current functions of government. Some of the these approaches involve ways to better manage identities, assets, data, and contracts. Additionally, many state governemnts are creating test beds for blockchain technology.

Notebly, the involvement of premier academic institutions in the the blockchain space has not been very proactive. Indian Institutes fo Technologies and National Insititutes 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 instutions 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 priciples:

1. <u>Ensure technology neutrality:</u> Governerment should allow for competing technologies and platform to emerge and to the extent possible not hard-wire its strategy for plocies 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. <u>Ensure policy and regulatory framework at national level:</u> 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 uncertainity and promote private sector investment in developmet of technology. The regulatory framework should promote and protect innovation and experimentation rater than prevent usage and creation of new business models, products and services. Regulatory framework should focus on solving known probelems and should not try to forcloase 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 shold promote data interoperatibility for blckchain applications.

3. Leadeship in knowlwdge leads to leadership in technology: India’s ability to attain global leadership role in blockchain technology is contingent on investment is research, human capital and supportive regulatory framework. Governement 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 Governemnt 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 envolve

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.

9.1 Promising Opportunities for Blockchain applications in India:

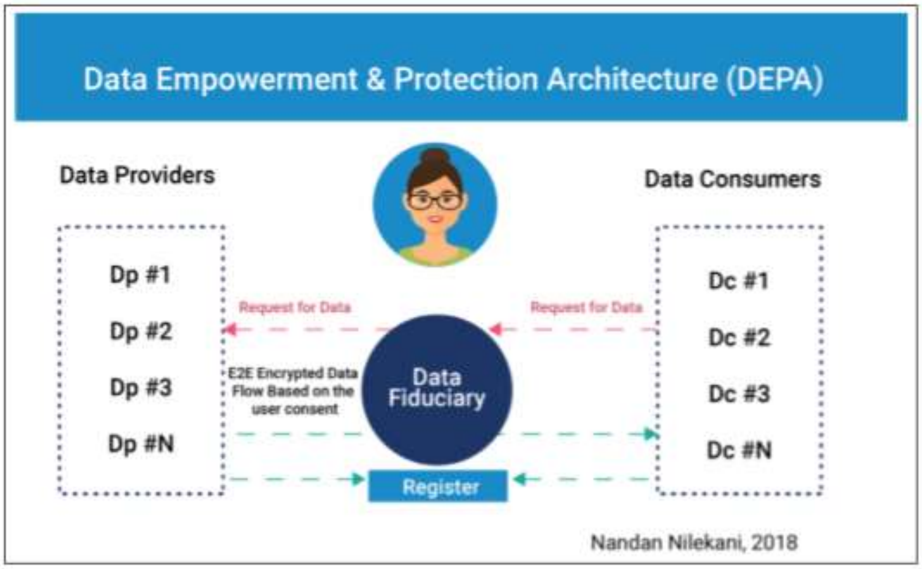
To facilitate innovation, we can examine the concept of a Central Bank Digital INR (CBDR) administered through a National Permissioned Blockchain that can run decentralized applications written in Turing complete programming languages and offers Trust As a Service.

Data explosion and the monetization opportunity:

India is a country with over 1.3 billion citizens, and a huge concentration of smartphones. With 1.21 billion mobile connections, 1.19 billion Aadhaar enrolments, 462 million Internet users, 582 million bank accounts and 375 million social media users, India is one of the largest generators of online data globally.

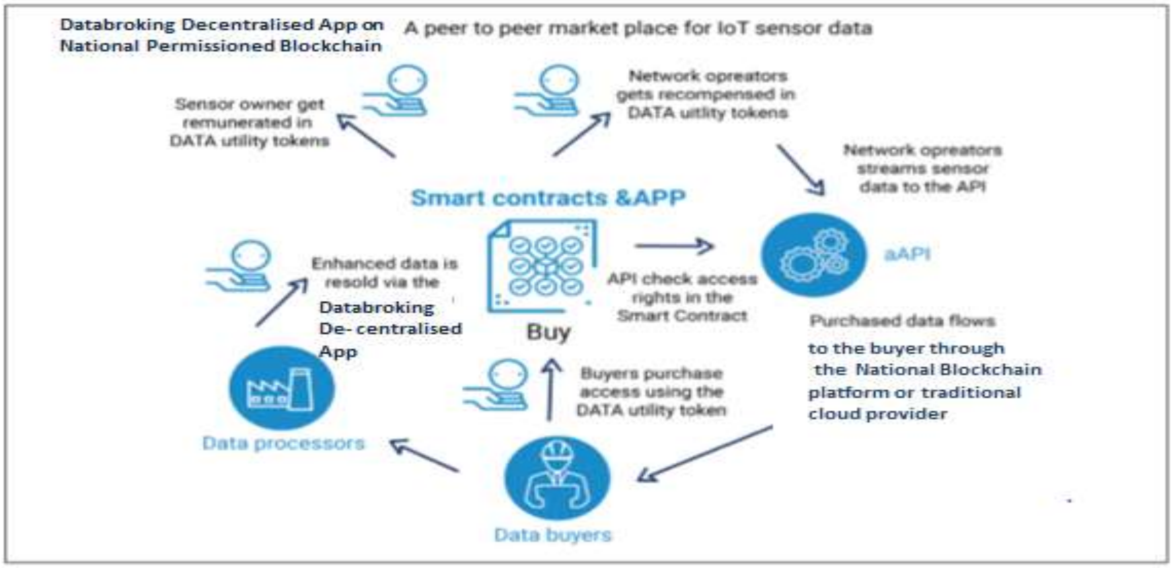
Monetising data being generated by its citizens and billions of Internet of Things (IoT) devices in the future in a secure and anonymised manner made possible by Blockchain, has the potential to catapult India to one of the richest countries in the world in future.

Apart from existing connections, the increase in the number of IoT devices will lead to a huge deluge of data. Unlocking the value of the data in the hands of citizens in a secure manner could give a big boost to citizens' disposable incomes. This implies an urgent need to set up a trusted and centralised data repository, and a mechanism to enable citizens and organisations to monetise the data in a secure and credible manner.



Currently, a lot of organisations like ecommerce companies, banks, NBFCs, telecom companies, employment exchanges etc., are sitting on a vast amount of data which they mine using advanced analytics to increase the life time value of their customers. To enable them to target a greater number of customers effectively, and increase their business, they need to exchange and procure data from other sources and organisations. This calls for a mechanism to exchange curated data among holders of the data across organisations and individuals. This can be made possible with Blockchain. For this, a normalising means for commercial exchange is needed, which can be made possible with a data token on a Blockchain system.

This will have implications for all sectors of the economy as a trusted data source at a nominal cost will be available for sectors like education, healthcare, telecom, NBFCs and banks. Interestingly, across the world, there are a number of companies leveraging Blockchain technologies to forge commercial interactions between data generating and data seeking organisations.


Databroking Decentralised App on National Permissioned Blockchain
A peer to peer market place for IoT sensor data
Sensor owner get remunerated in DATA utility tokens
Network opreators gets recompensed in DATA uitlity tokens
Network opreators streams sensor data to the API
Smart contracts &APP
Enhanced data is resold via the
Databroking De-centralised App
Buy
API check access rights in the Smart Contract
aAPI
Purchased data flows
to the buyer through the National Blockchain platform or traditional cloud provider
Buyers purchase access using the DATA utility token
Data processors
Data buyers

Central Bank Digital currency on a Permissioned Ledger:

As an alternative to Public Blockchains that operate with native cryptocurrency, like Ethereum, it is strongly recommended that Government of India along with RBI come out with a Central Bank Digital INR (CBDR) administered over a Public Permissioned Blockchain that processes transactions through a Turing Complete Virtual Machine allowing decentralised applications to run on its platform.

Central bank digital currency (CBDC), also called digital fiat currency or digital base money is the digital form of fiat money (a currency established as money by government regulation or law). Central bank digital currency is different from virtual currency and cryptocurrency, which are not issued by the state and lack the legal tender status declared by the government.

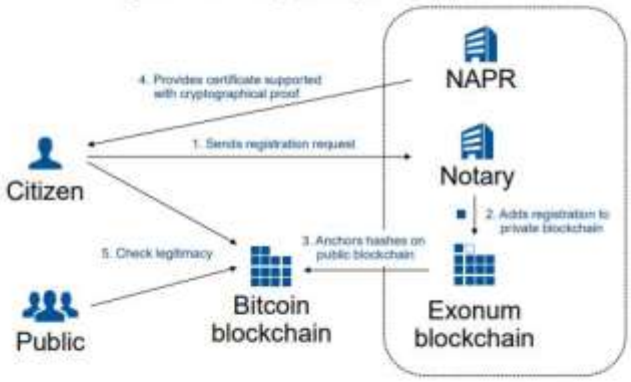
The advantage of offering CBDR is that it can allow the Indian Blockchain developers and entrepreneurs to create and run decentralised applications like in the case of the open source Permissionless Blockchains like Ethereum, EOS etc., while benefiting from regulatory oversight and corresponding protection.

A number of countries in the world are experimenting with the concept of CBDC and it is considered a transitory step to the ultimate eventuality of a fully digitalised currency with the added security measure offered by a Blockchain approach. It is also pertinent to note that António Guterres, Secretary-General, of the United Nations, Recommends Embracing Blockchain Technology. António Guterres, secretary-general of the United Nations (UN), stated recently that the organization must encourage and support the ongoing development of blockchain technology.

Globally many Blockchain applications employ a 'Hybrid' approach where a combination of private and public Blockchain systems is used to secure the integrity of the data stored. A case in point is the land registry application by the National Agency of Public Registry (NAPR) of the Republic of Georgia which uses Blockchain as shown in the figure below:

Instead of the Bitcoin Blockchain in the below example, we propose that similar applications can use to anchor their hashes on a Public Permissioned Blockchain created by Government of India and RBI that also are powered by a CBDR on the ledger.

Figure 3. Land tile registration process by NAPR


NAPR
4. Provides certificate supported with cryptographical proof
Citizen
1. Sends registration request
Notary
2. Adds registration to private blockchain
5. Check legitimacy
3. Anchors hashes on public blockchain
Public
Bitcoin blockchain
Exonum blockchain

Source: Blockchain for Digital Governments, An assessment of pioneering implementations. A report by JRC Science for Policy report by European Commission

9.2 National Blockchain Platform: The road ahead:

The National Permissioned Blockchain can offer 'Trust as a Service' to a variety of decentralised applications and any number of permissioned Blockchain applications as depicted in the above example.

An option for technical implementation of the National Public Blockchain could be a Quorum or a Private Ethereum version or Hasgraph with a Proof of Authority Consensus Mechanism, with the validator nodes being hosted by selected Government departments and Industry Associations. There can be many other options that need to be evaluated before a final decision is taken by the Government in this regard.

By undertaking these actions, Government of India can send a strong signal about its intention to leverage Blockchain technology and facilitate a vibrant industry and start-up ecosystem that caters to the demand of all industries - public and private. This will institutionalise Blockchain applications, while availing the Trust as a Service facility of the Public Permissioned Blockchain network under the aegis of various Indian regulators. The decentralised applications that can be created over this network can also facilitate India's participation in the Industry 4.0 revolution through scalable & secure automation. The monetary value of the data expected to be generated by IoT devices can be unlocked bringing prosperity to India and its citizens.

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.