सत्यमेव जयते

NITI Aayog

BLOCKCHAIN: THE INDIA STRATEGY

Towards Enabling Ease of Business, Ease of Living, and Ease of Governance

Part 1

January 2020

This page has been intentionally left blank

Acknowledgments

In writing **Blockchain: The India Strategy**, Arnab Kumar, Tanay Mahindru, Punit Shukla and Aalekh Sharan have made valuable contributions.

The support of several of our partners and contributors are also thankfully acknowledged. A list of all partners and contributors is appended at the end of this Strategy document

Anna Roy
Senior Advisor
NITI Aayog

Contents

Foreword

'Blockchain' has emerged to become a potentially transformative force in multiple aspects of government and private sector operations. Its potential has been recognized globally, with a variety of international organizations and technology companies highlighting the benefits of its application in reducing costs of operation and compliance, as well as in improving efficiencies.

While the technical underpinnings of the technology can be intimidating to a large section of policy and decision makers – simply and functionally, blockchain can enable ease of collaboration for enterprises and the ease of living for our citizens by bringing in transparency across government and private sector interfaces.

Despite the fact that the technology is still in a nascent stage of its development and adoption as it continues to evolve, it is important for stakeholders such as policy makers, regulators, industry and citizens to understand the functional definition of the entire suite of blockchain or distributed ledger technologies along with legal and regulatory issues and other implementation prerequisites. Equally important is the fact that this technology may not be universally more efficient and thus specific use cases need to be identified where it adds value and those where it does not.

This discussion paper, the first part of the strategy titled "Blockchain: The India Strategy –Towards Enabling Ease of Business, Ease of Living and Ease of Governance", aims to address these needs. The paper first analyses the value of blockchain in facilitating trust in government and private sector interactions, followed by considerations when evaluating a blockchain use case for implementation, possible challenges and lessons from NITI Aayog's experiences in blockchain implementation showcases potential use cases that the ecosystem may consider.

The paper is a culmination of multiple consultations over the last two years together with NITI Aayog's own experiences in implementing blockchain systems in a variety of contexts. It is meant to serve as an essential 'pre-read' to implementing a blockchain system in India and help guide broader thinking in the area.

Dr. Rajiv Kumar

Vice Chairman, NITI Aayog

Introduction

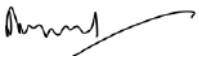
Blockchain technology has the potential to revolutionize interactions between governments, businesses and citizens in a manner that was unfathomable just a decade ago. Though very often grouped with technologies such as artificial intelligence (AI) or IoT (Internet of Things), the technology is unique in its foundational nature. Unlike other technologies, which have the potential to deliver completely new services to citizens and other stakeholders alike, blockchain has the potential to revamp currently existing processes to unlock new sources of efficiency and value.

Governance in India faces unique challenges given the scale, diversity and complexity of processes involved for delivery of varied public services. Blockchain offers unique possibilities of addressing issues relating to improving governance. In business, by allowing 'self-regulation', India can considerably move towards improving the 'Ease of Doing Business' by allowing entities to interact through a trusted medium with a reduced dependency on cumbersome regulatory oversight and compliance. By empowering citizens through features of transparency, decentralization and accountability, blockchain would help in improving ease of living.

The Strategy document is being presented in two parts where independent but connected pieces are aimed to help convey a more cohesive message. NITI Aayog has been at the forefront of promoting adoption of frontier technologies through demonstration of their efficacy. In this first part of the 'Blockchain: The India Strategy', various learnings from pilot initiatives and consultations undertaken over the last two years have been highlighted. Despite the hype around the technology, there is limited appreciation on its potential for governance. This edition of the Strategy document attempts to demystify and improve the understanding of amenability of blockchain to specific use cases. This is a fast evolving space and the Strategy aims to present a more functional view of blockchain and not delve in the technical aspects. A simple framework is also presented to help decision makers identify use cases that would benefit from the usage of the technology. This is supplemented by 'deep dives' of the initiatives undertaken by NITI Aayog in collaboration with a host of government and technology partners. The paper attempts to highlight the specific challenges faced during their implementation in an effort to help future initiatives achieve success, and ends with additional potential use cases that governments and businesses may explore towards 'Enabling Ease of Business, Ease of Governance, and Ease of Living'. Significant work is already being undertaken by a number of other nations, state government, government agencies and businesses, but this paper does not report them, and focuses on NITI Aayog's own experiences in the area.

Part 2 of the Strategy would elaborate on the recommendations in greater detail.

I hope this document would help start a dialogue on this very important subject and help various government instrumentalities to explore how this technology is effectively leveraged for the betterment of society.



Amitabh Kant

CEO, NITI Aayog

Blockchain: The New Trust Paradigm

Trust systems reimagined

The need for 'trust'

Milton Friedman publicized "I, Pencil" – an essay by Leonard Read that demonstrates the power of markets to drive collaboration. In the essay, written as an autobiography of a pencil, attention is drawn to the extremely complex and large-scale human collaboration needed to manufacture even something as simple as a pencil.

The pencil lists its constituents – including cedar, graphite, lacquer, ferrule, etc. and describes the interactions required to manufacture these through different processes across different components, from the complex machines that extract graphite to the sweeper in the factory and the lighthouse keeper granting entry into the port. The book draws attention to the fact that there is no mastermind directing this coordination. The '*invisible hand of the market*', with price signals being its only weapon, is able to incentivize collaboration amongst the various entities involved in the market thinking selfishly of maximizing their own respective gains.

Though the parable is instructive, in practice disagreements could potentially occur at each step – whether each entity got what they bargained for and whether promises were kept with respect to the mode and manner of value exchange. These disagreements can take a number of different forms and can cause delays or inefficiencies in the market, often leading to losses for the participants.

Such disputes are traditionally addressed by introducing trust in the system through a network of intermediaries to ensure that the entities adhere to the commonly understood '*rules of the game'*. We thus observe that the market never needed a mastermind, it needed an impartial and trusted facilitator – a mediator with the power to enforce rules. Banks, regulatory bodies, and even governments perform this role. Enforcement is typically through an ex-ante regulation – the state would employ a bureaucracy to ensure that laws and rules were being adhered to and would have the power to recognize, investigate, and punish transgressions. As the Noble laureate Friedman stated, contract enforcement as one of the three primary functions of a government is mostly implemented through mechanisms of deterrence and penalty. Consequently, these mechanisms have their own challenges that also introduce inefficiencies due to several factors including lack of transparency, rent seeking and apathy by the constituents etc.

Blockchains represent another form of intermediaries – code as a trusted intermediary. By encoding the rules of the game as computer programs and by allowing different entities with differing interests to collaborate on an immutable ledger, blockchains lead to a system that seamlessly adheres to the rule and fulfils the promise of not allowing transactions that did not comply to the agreed conditions. This aspect of blockchain technology is the harbinger of its true promise – seamless transactions

that promote ease of doing business as well as ease of living for citizens via disintermediation and the reduction of ad-hoc bureaucracy.

Transactions today are facilitated by 'trust systems' and intermediaries

Removed from the context of finance, a 'transaction' is commonly defined as "the act of carrying out or conducting a deal or exchange to a conclusion or settlement". Today, an individual 'transacts' with multiple entities every day, either offline or online, and in a variety of forms. Transactions could take the form of small purchases from a roadside vendor or a deal between two very large organizations. Immaterial of the size or nature, however, a common underlying feature of transactions is that they require the parties involved to trust each other, or adhere to a system that enables this trust to be executed.

These 'trust systems' can take a variety of forms, depending on the nature of transactions being executed, to create checks and balances to ensure that parties involved fulfil their responsibilities and recourse in the case of disagreements is available. In the assignment of a job to a vendor for a construction project, for example, trust is encoded in contracts enforceable by law. 'Escrow accounts' can be seen as another instrument to create trust. In the execution of outcome driven project financing, for example, escrow accounts are used to store project implementation funds pending completion of the project as per previously ascertained goals or objectives.

Economic structures, as we know them today, have evolved to create these systems of trust. Banks are perhaps the most well-known of these systems, existing largely to facilitate creation of trust while transacting in money. Regulatory bodies and certain government agencies exist almost exclusively to establish enforceable guidelines or regulations to create trusted environments for stakeholders to transact. In essence, the need for trust in execution of these processes necessitated the need to create 'centralized authorities' to oversee their procedures and enforce them.

These 'trust systems' have become increasingly complex

With development and growth, the complexity of these systems has increased, making them more susceptible to inefficiencies.

India, specifically, has not fared well in indicators to measure the efficiency of processes to ensure trust. In the 'Ease of Doing Business' rankings, released annually by the World Bank, while India has registered phenomenal progress and has gained 79 positions since 2015 to be ranked 63rd in the 2020 edition, it continues to perform abysmally low in indicators such as 'enforcing contracts' (ranks 163 out of 190 countries), 'property registration' (154 out of 190 countries) and 'starting a business (136 out of 190 countries)[1]. Of note is also India's poor performance in 'trading across borders' (68 out of 190 countries) which includes parameters such as 'cost of compliance' to export.

[1] World Bank Ease of Doing Business Ranking 2020

Apart from the increase in complexity, centralised authorities introduce risks and disadvantages of their own, since they themselves need to be trusted and compensated for their services. In India, the perceived level of corruption in public 'trust systems' is especially poor, with a position of 78 out of 180 countries in the 'Corruption Perception Index' released by the Transparency International[2].

The Government of India has taken several initiatives to improve both the ease of doing business and ease of living by streamlining and simplifying processes, primarily by leveraging technology as well as proactively rationalizing various regulatory and other requirements. However, there is still a case for further improvement. Blockchain presents the potential for achieving the vision of Hon'ble Prime Minister of less government and more governance.

Enter blockchain – a new paradigm of trust

In 2008, a technical white paper was released to describe the design of a new '*Peer to peer electronic cash system*' called Bitcoin. The paper argues that the traditional trust based payment models, with the possibility of reversals, lead to high transaction costs and increase the level of intermediation required by a 'trusted third party' (in this case, a bank). The high transaction costs, in turn, prohibit the digital execution of small value transactions[3].

The paper proposed that instead of trust being introduced to transactions through 'trust systems' or 'trusted third parties', it could be introduced to transactions cryptographically. This would ensure a shared order of transactions through computations without the need of parties knowing each other. Through a peer to peer distributed network that time stamped transactions, participants would be able to execute transactions without the need for a trusted third party as intermediary, thus eliminating inefficiencies caused by the more traditional system. While the shape and form the technology takes has evolved since its introduction, certain features remain consistent, as does blockchain's goal to facilitate trusted electronic transactions more efficiently.

Though some of the foundational technologies that made up 'blockchains' had been developed as early as 1995, it is the paper on the Bitcoin that is most credited for the advent of the new technology. Technical description of blockchain technology may be found in **Appendix 1**. The following section aims to describe the technology briefly, before describing the variety of forms it can take, and its core value proposition.

What is blockchain?

Blockchains can broadly be defined as a new type of network infrastructure (a way to organize how information and value moves around on the internet) that create 'trust' in networks by introducing distributed verifiability, auditability, and consensus.

[2] World Bank Ease of Doing Business Ranking 2019

[3] Bitcoin: A peer to peer electronic cash system, Satoshi Nakamoto, 2008

Blockchains create trust by acting as a shared database, distributed across vast peer-to-peer networks that have no single point of failure and no single source of truth, implying that no individual entity can own a blockchain network, and no single entity can modify the data stored on it unilaterally without the consensus of its peers.

New data can be added to a blockchain only through agreement between the various nodes of the network, a mechanism known as distributed consensus. Each node of the network keeps its own copy of blockchain's data and keeps the other nodes honest – if one node changes its local copy, the other nodes reject it.

Blockchains record information on a timestamped chain that extends forward infinitely. New data is added to the end, and once added, it is permanent. Older data can neither be removed nor modified because a snapshot of it is captured in the blocks of data that come after it.

Table 1**: **What is blockchain?

A **Database**	A list of records / transactions, like a ledger, that keeps growing as more entries are added;
Which is **Distributed**	Copies of the entire database are stored on multiple computers on a network, syncing within minutes / seconds;
adjustably **Transparent**	Records stored in the database may be made visible to relevant stakeholders without risk of alteration;
highly **Secure**	Malicious actors (hackers) can no longer just attack one computer and change any records;
and **Immutable**	The mathematical algorithms make it impossible to change / delete any data once recorded and accepted.

Blockchains leverage techniques from a field of mathematics and computer science, known as cryptography, to sign every transaction (e.g. the transfer of assets from one person to another) with a unique digital signature belonging to the user who initiated the transaction. These signatures are held privately but are verifiable publicly. This means that if a user with identity A sends an asset to identity B, anybody can verify that the asset was sent by A, but cannot use A's signature for their own transactions. This cryptographic system creates accountability while preventing identity fraud: if you send assets or update information on a blockchain, you later cannot claim otherwise or shift the responsibility for the action.

Blockchains also enable the creation of 'smart contracts', defined as self-executing contracts with the terms of the agreement between the buyer and seller directly written into lines of code. The code and the agreements exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

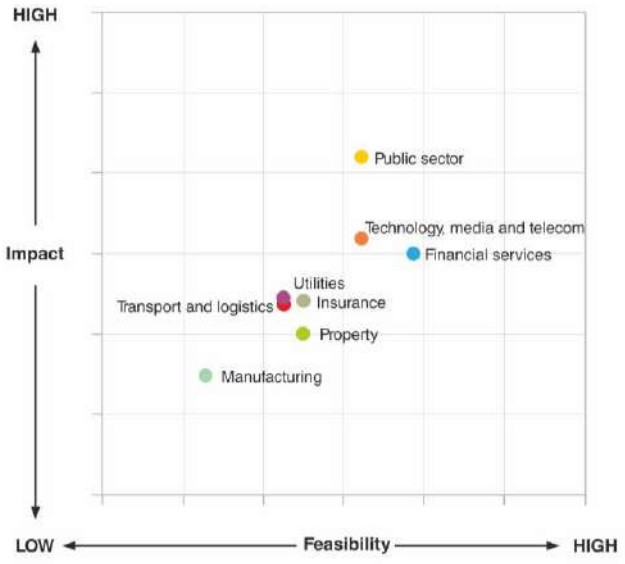
Unlike present day networks that depend on trusted intermediaries for security and trust, blockchains thus create trust organically through the underlying technology of distributed networks. They allow users to exchange digitized assets directly, in a way that is incorruptible (data cannot be changed once added) and transparent (all transactions are logged onto the timestamped ledger, with the identity of the person who committed the transaction).

What is the market value proposition of blockchain?

Blockchain is seen as a technology with the potential to transform almost all industries and economies. It is estimated that blockchain could generate USD3 trillion per year in business value by 2030[4]. The World Economic Forum (WEF) anticipates that 10% of the global GDP will be stored on blockchain by 2025 and lists blockchain as one of 7 technologies that are anticipated to revolutionize various aspects of our lives.

While blockchain is still a nascent technology that has seen adoption at a limited scale, its strategic value in the short term towards streamlining processes, reducing inefficiency, cost optimization etc. cannot be negated. Major savings can be achieved in resource conservation by reducing intermediaries as well as administrative effort of record keeping and transaction reconciliation. This can shift the flow of value by capturing lost revenues and creating new revenues for blockchain-service providers. As per a report by McKinsey, potential value created would differ from sector to sector, with the public sector perhaps best positioned to take advantage from the perspective of potential impact and feasibility to application.

Figure 1: *Economic Potential of blockchain by industry sectors*



Source:
McKinsey

[4] https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain

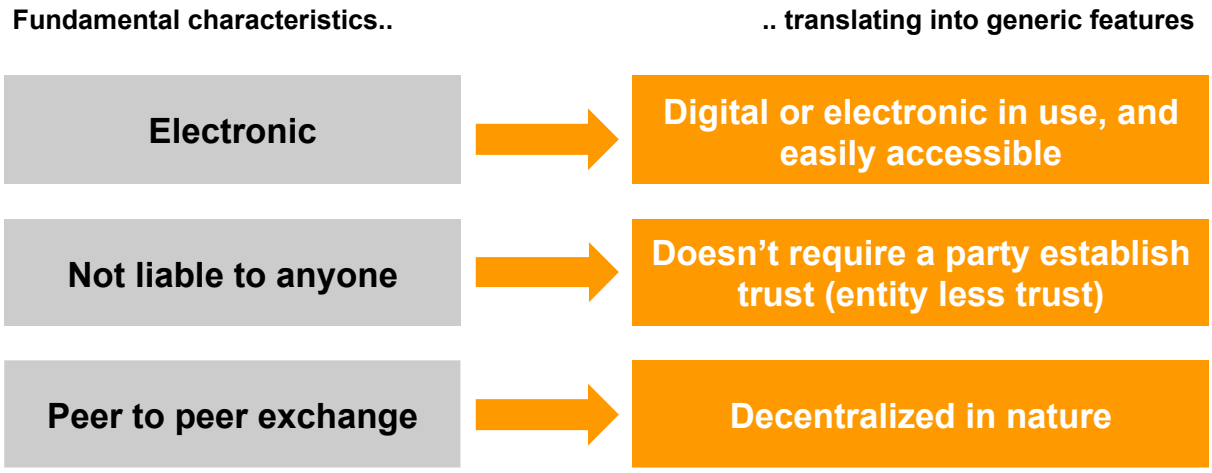
Value proposition of 'decentralised' and "entity-less trust' systems

A 2015 report on cryptocurrencies published by the Committee on Payments and Market Infrastructure set up by Bank for International Settlements (BIS) characterized cryptocurrencies through their three fundamental features:

- They are *electronic*;
- They are *not liability of anyone;*
- They allow *peer-to-peer exchange*

Although this definition is made from a cryptocurrency perspective, the fundamental features are quite representative of the truly unique nature of blockchain or Distributed Ledger Technology (DLT) based systems. Zooming out of the cryptocurrency lens, we can see how these fundamental characteristics translate into generic features:

Figure 2: *Features of blockchains*



Source: NITI Aayog

These generic features, on the right hand side, are paradigm changing features in the way our socio-political economy has functioned through the human civilizational period. How '*electronic*' modes of information, goods and services exchange have transformed the global economy and society is well understood. However, the next two features are novel and can change the way our existing economy functions. The next two sections discuss these two fundamental features.

Decentralised + entity-less trust Systems – why are they important and who should pay attention?

The current discourse on peer-to-peer exchange systems has been dominated by the use case of Bitcoin, a cryptocurrency, and other altcoins[5] and their potential use by malicious actors. This has resulted in a narrative putting them in negative light. However, an absolute analysis of systems which

[5] Altcoins are alternative cryptocurrencies launched after the initial success of Bitcoin. Despite being based on a common theory, Altcoins differ themselves from Bitcoin with a range of procedural variations, including different proof-of-work algorithms, different means by which users can sacrifice energy to mine blocks, and application enhancements to increase user anonymity (Source: Investopedia)

allow peer-to-peer exchange illustrates the usefulness of decentralised systems and how they have been used by governments. The most basic form of currency transaction is the use of cash – a peer-to-peer to exchange system, albeit not electronic. Every sale of goods and services happening at a mom-and-pop store is effectively a peer-to-peer exchange of value. World Wide Web enabled decentralised mechanisms of exchanging information and value at a global scale. All of these systems are well recognised by governments and regulators. There are umpteen areas of exchange where decentralised systems are the most value-creating mechanisms of that exchange. Blockchain and other DLTs enable the building of decentralised systems, thus creating tremendous economic and social value. Governments looking at engendering new areas of economic activity should look at decentralised systems and network effects of DLT based peer-to-peer transactions.

It is also important to understand that the mechanism of decentralization or peer-to-peer exchange is a spectrum and not a binary concept. It also has to be understood separately from government regulation – *networks completely regulated by governments can be decentralised and feature peer-to-peer exchange and, totally centralised systems can also be unregulated and operate beyond the bounds of law*. Decentralised networks do not necessarily mean they aren't regulated. This is where the notion of extent of decentralization comes into play. In DLT terms, this notion is largely defined in two categories – permissioned systems and permission-less systems (detailed definitions given in **Appendix 1**).

This new design of system where an entity is not responsible and accountable for building trust throws unprecedented challenges. The existing mechanism of contract enforcement is based on this primary fixation of accountability and responsibility to an entity. For example, two parties intending to execute an economic transaction enter into a contract with the belief that state will perform the contract enforcing function. However, this loss of accountability for establishing trust does not let existing legal and regulatory tools to function properly – which are primarily based on fixation of this accountability.

Governments should pay special attention to decentralised networks where peer-to-peer transactions can create more socio-economic value. Sectors of governmental intermediation where a state entity is involved just for ledger maintenance or collecting state dues but is not adding value to the transaction can be relooked to assess how government's role can be redefined in those sectors. For instance, land and property transactions are essentially a peer-to-peer transaction happening between a buyer and a seller. However, the State becomes a party to the transaction because the existing necessity of an intermediary to maintain records of ownership and ensure state dues are paid. With the development of DLT, it may not be necessary for the government to maintain records anymore. A peer-to-peer network with government as one of the players in the network can be a great way to revolutionize the land transactions market. The network will maintain the records of transactions (government need not deploy resources to maintain that ledger) and government being a player can also collect state dues based on the information in the shared transaction ledger.

In the same manner, wherever entities are playing the role of maintaining a shared information ledger but not really adding any specific value to the transaction, it may make sense in exploring if that activity can be done in a decentralised manner. A peer-to-peer exchange mechanism expedites transactions and removes unnecessary friction, a DLT enabled peer-to-peer exchange mechanism adds network and trust effects to such a system to effectively improve ease of doing business and ease of governance.

Objectives of the Strategy Paper

Blockchain is a frontier technology that continues to evolve. In order to ensure that India remains ahead of the learning curve, it is important to understand the opportunities it presents, steps to leverage its full potential and such necessary steps that are required to help develop the requisite ecosystem.

This Strategy document is targeted at all stakeholders such as government, enterprise leaders and citizens, with the aim to demystify the concepts surrounding this technology, identify areas where it can be utilized for more transparent and open models of cooperation between entities and recommend the next steps towards achieving this goal. The different types of blockchain technology not only have different technical but also legal and regulatory prerequisites for their effective implementation. It is also incumbent upon stakeholders to understand in which cases the technology adds value and in which cases it does not. Furthermore, it is important to recognize the economic value that this phenomenon can create and the new business models that can emerge. By creating an enabling ecosystem for the research, development and skilling of talent for the industry, India can hope to be well positioned to take global leadership in this space. Simultaneously, the central government and states need to work together to accelerate the adoption of blockchain technology in a way that creates opportunities for leveraging this technology for government as well as businesses for creating more seamless B2C and G2C interfaces. With a little foresight, this can be done in a manner that ensures interoperability between different blockchain databases and legacy infrastructural databases, while allowing different agencies and private organizations flexibility in implementation.

This strategy aims to be an essential pre-read for the above mentioned stakeholders in order to create a concerted national plan of action towards this technology by Team India (Union government in partnership with States).

The Strategy Paper is being released in two parts. Part 1 introduces the concept of blockchain to a and establishes how blockchain can redefine ‘trust’ in transactions towards ‘Enabling Ease of Business, Ease of Living and Ease of Governance’. It also identifies potential blockchain use cases and the lessons from NITI Aayog’s pilots in the area. Part 2, to be released soon, will cover specific recommendations that can enable the growth of a blockchain ecosystem in India.

The Blockchain Necessity Framework

Beyond the hype: blockchain is not a panacea for all problems

The blockchain frenzy

Blockchain has been positioned as a revolutionary new technology, the much needed '*silver bullet'* that can address all business and governance processes. While the promise and potential of blockchain is undoubtedly transformative, what hasn't helped this technology, that is still in nascence of its evolution, has been the massive hype and the irrational exuberance promulgated by a bevy of '*Blockchain Evangelists'.* With survey results such as "*more than 80% of business executives say their organisations are actively involved with blockchain*" (without explaining what this *involvement* entails and what has been the success so far), it isn't difficult to fathom why so many institutions, government agencies and businesses across the globe have pursued blockchain pilots and proof-of-concept (POC) projects, often with an unclear picture of what the scope or the success of such projects would look like.

"*Do you even blockchain bro*" seemed to be the mantra in the last few years. The immaturity of technology, combined with lack of a series of success stories beyond the Bitcoin / altcoin frenzy, may have led to a certain degree of disillusionment and '*buyer fatigue'*. Indeed, as the studies by McKinsey and Gartner point out, a vast majority of blockchain pilots and PoCs are still stuck in pioneering / exploratory mode or are being shut down. Key reasons for this pilot purgatory are understood to be unstructured experimentation without strategic evaluation, lack of problem-solution mapping, overly ambitious scope, tendency to 'force fit' the solution to the process, and a misunderstanding of what and how blockchain could help with the business process. Research by Gartner suggests that 93% of blockchain projects in supply chain will suffer from fatigue by 2023 due to lack of strong use cases[6]. What is thus imperative is the need for a structured decision making process, embedded with sound business rationale and understanding of process lifecycle of the problem being pursued. Blockchain as a technology is a means to end, and not an end in itself. Blockchain can be leveraged to develop new solutions to re-engineer processes i.e. create new operating and business models, and not necessarily be seen as a novel approach to build new solutions (e.g. democratise quality cancer diagnosis across India through advanced AI radiomics solutions). While strong enthusiasm for exploring blockchain for improving business capabilities is much needed, learnings from these several pilots and PoCs pursued so far should be factored in.

The Big Question: is there valid problem with clear business case?

As established in the previous chapter, blockchain solutions can enable reductions in transaction complexity and cost, as well as improvements in transparency and fraud controls. The foremost question to be answered therefore, before exploring a blockchain project, is whether there is a

[6] https://www.gartner.com/en/newsroom/press-releases/2019-05-07-gartner-predicts-90--of-blockchain-based-supply-chain

problem or pain point that needs to be addressed, in addition to a business rationale for pursuing the investment. As with any foundational technology, the strategic value of blockchain can only be realised if commercially viable solutions are deployed at scale. A McKinsey study of more than 90 blockchain use cases[7] suggests that the initial impact will be achieved through operational efficiencies. Cost can be rationalized for existing processes by reducing intermediaries or the administrative effort of record keeping and transaction reconciliation. Revenue generation and capital relief are second order benefits, and thus developing new business models and revenue streams will eventually follow, but not in immediate term.

NITI Aayog has pursued PoCs in four areas in an attempt to assess the potential of blockchain technology in delivering improved efficiency and better understand possible hurdles in implementation. These are:

1. 'Track and trace' of drugs in the pharmaceutical supply chain
2. Claim verification and approval in the disbursement of fertilizer subsidy
3. Verification of university certificates
4. Transfer of land records

For the fertilizer subsidy pilot undertaken by NITI Aayog (see **Box 1**), the problem / pain point was reducing the turnaround time for reimbursement of subsidies payments and freight claims. The existing workflow was saddled with inefficiencies, including multiple systems of record, limited visibility for inventory stocks and low trust in the data generated for subsidy and freight claims. There clearly was a valid problem, deeply embedded in business rationale.

The features of blockchain make it favorable in processes requiring decentralized access, auditability, security, disintermediation, and programmability. While alternatives such as distributed databases, or centralized databases with distributed API access may also solve specific issues in processes at a lower cost, blockchain has the potential to solve these problems simultaneously.

Several frameworks have been proposed in the recent past to evaluate the applicability of blockchain based solution. Based on our analysis, the framework suggested by WEF was found to be most intuitive. This paper proposes a framework to evaluate the efficacy of using blockchain for use cases, and is an adaptation of the WEF model, with modifications based on the learnings from the studies and initiatives pursued at NITI Aayog.

***Table 2:* Potential business features of blockchain solutions**

Improving profitability and quality	• Automation using smart contracts / algorithms • Traceability of all historical transactions • Speed and efficiency of transactions by eliminating intermediaries • Enhanced security by encryption of data at the stage of dissemination • Prevents tampering as any tampering may leave behind trail

[7] McKinsey Blockchain beyond the hype: What is the strategic business value?

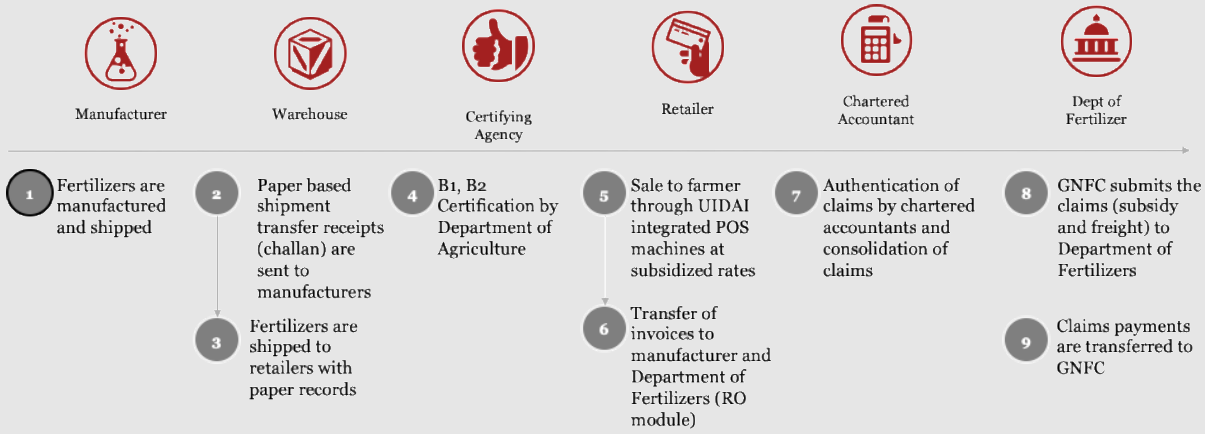
Increasing transparency	• Distributed ledger • Provides a comprehensive picture: all stakeholders see the same information to which they have access • Availability of multiple copies of the shared data
Reinventing products and processes	• Transparent and predefined rules which facilitates creation of new products / processes through a decentralized model • Tokenization / Digital Assets which are physical objects with a unique digital representation that enable digital ownership, management and transfer

Box 1: GNFC Fertilizer Subsidy Pilot (*setting the context*)

In India, fertilisers are provided to the farmers at subsidized rates, as decided by the Department of Fertilisers (DoF). The subsidy is paid to the manufacturer of the fertilizer post the sale of the product. Fertilizer subsidy is the second largest component of India's subsidy program and the total outgo expected in Budget 2019 – 20 was Rs. 79,996 crores.

Gujarat Narmada Valley Fertilisers & Chemicals (GNFC) is one of the largest fertilizer manufacturing companies in India, with products sold all across the country. Owing to its scale and pan-India presence, GNFC operates over a large and complex supply chain.

Figure 3: *GNFC existing business flow*



Source: PwC

GNFC claims the subsidy from DoF through the following process:

(a) *Subsidy claims*: The difference between the cost of production and the subsidized sales price of the fertilizer is claimed by GNFC based on the sales record of the product to the farmers. The sales record is accumulated using the invoices created by the retailers in the Point of Sales (PoS) machines. The invoice generated is stored on GNFC's servers (which currently uses an SAP based system) and is also replicated in real-time on DoF's Integrated Fertilizer Management System (iFMS) system. To claim the subsidy, invoices are consolidated by GNFC from iFMS system every week, authorized by statutory auditor and then submitted to DoF.

(b) *Freight claims*: Freight claims are for the cost incurred during transportation of the fertilizers. Freight claims are generated by accumulating the received quantity by warehouses. On receipt of fertilizer stock at the warehouse, a zero claim subsidy is generated and submitted to iFMS. The freight claim is consolidated and sent to DoF on a monthly basis.

Due to the presence of several redundant processes and inefficiencies (including paper based legacy systems), involvement of multiple agencies, need for explicit consolidation and lack of well-defined audit trail, the subsidy received by GNFC takes 3 to 4 months – a substantial working capital cost. The pain point being faced by GNFC was the linking of the final retail sales invoice with the challan generated when the shipment leaves GNFC's factory. An additional requirement was to maintain a unified system of record for the inventories with all supply chain actors downstream of GNFC.

NITI Aayog, in partnership with PwC and Intel, embarked on a pilot to optimise the fertilizer subsidy supply chain using a blockchain based solution. The goal of the pilot was to streamline the fertilizer subsidy supply chain by demonstrating a transparent and tamper-proof ledger for the track and trace of fertilizer movement across the value chain and reduce the turnaround time for subsidy activation by integrating the various transaction records such as challans, invoices and claims.

The blockchain use Case selection framework

1. *The need to reduce intermediaries*: The foremost requirement for a blockchain based solution to be appropriate is the need for reducing intermediaries (entities / brokers / processes) etc. If it is cheaper, faster and more efficient to collaborate directly with counterparties e.g. forward transactions between trusted parties in financial markets, blockchain solutions are not suited. In case of the GNFC pilot, there was a clear rationale for reducing intermediaries:
    i. Process intermediaries: (a) multiple system of records viz. SAP, iFMS and e-way systems; (b) authorization intermediaries: authorization by chartered accountants before claims are generated and auditing by Department of Agriculture on quantity and quality of product
    ii. Process flow intermediaries: (a) warehouses and (b) retailers

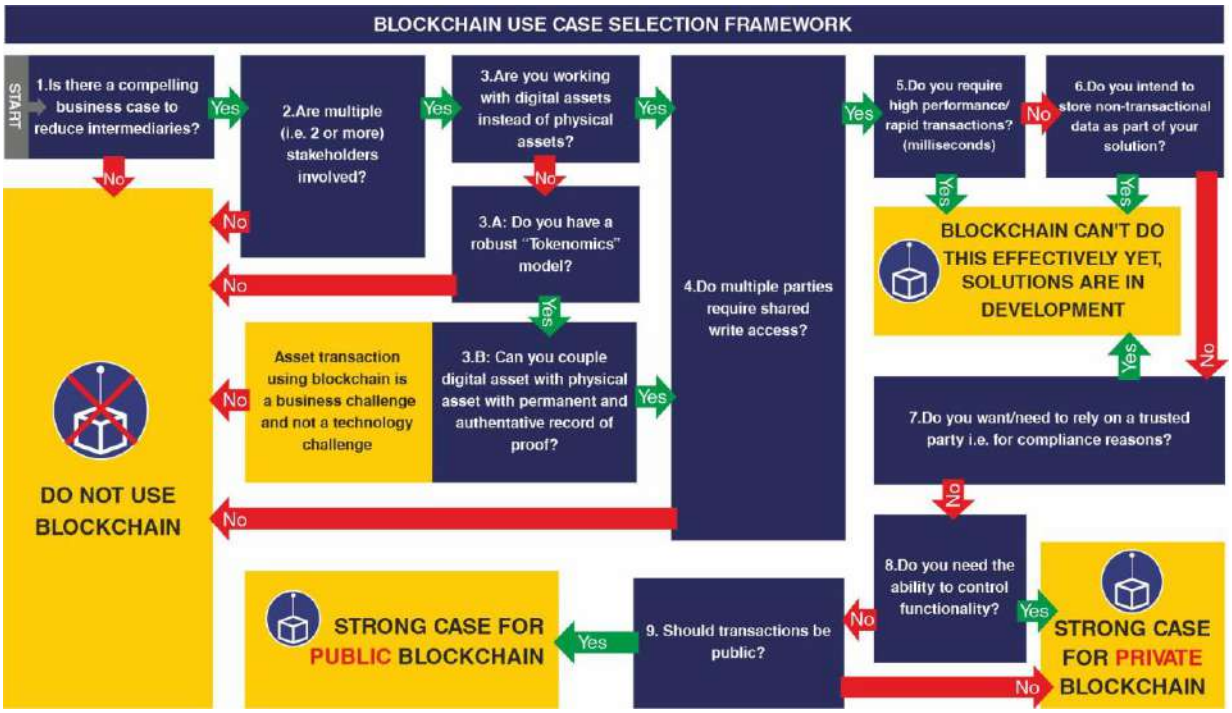
    It is worth noting that blockchain solutions will not necessarily lead to disintermediation i.e. removal of intermediaries but reduction of intermediaries. The majority of viable use cases for blockchain will be permissioned ones, not public blockchains. "*Public blockchains, like Bitcoin, have no central authority and are regarded as enablers of total disruptive disintermediation*. *Permissioned blockchains are hosted on private computing networks, with controlled access and editing rights i.e. there are still central authorities with admin rights*[8]."

[8] Asset Finance International

However, once allowed on the permissioned network, the parties can execute peer-to-peer transactions without the need of a central authority

2. *Multi-stakeholder environment*: The power of blockchain solutions is to act as source of trust, transparency and auditability, and hence are suited for process flows with multiple entities like the GNFC pilot.
3. *Digitally native assets*: For blockchain solutions to be successfully applied, there is need for assets that can be successfully represented in a digital format. *"If an asset has a physical representation that can change form, then it is difficult to effectively manage that asset on a blockchain. An example of this is tracking and tracing farm produce on blockchain – if a company wishes to track and trace wheat across the entire supply chain as it becomes bread, it is difficult to use blockchain to manage its transition from wheat, to flour, to bread.*[9]" In the GNFC example, while fertilisers are physical assets, the digital representation is achieved through challans and sales invoices.

Figure 4: *Framework for blockchain use case evaluation*



Source:
NITI Aayog

4. *Permanent and authoritative proof of record*: The need for creating a permanent trusted digital record for the asset can't be emphasized enough. One of the key features of blockchain is the immutability i.e. irreversible representation of the state of an object. If consensus can't be reached on the state of the object / transaction through trusted sources i.e. disputed land records, a block representation of that object / transaction is not feasible.

[9] WEF

In the GNFC pilot, the permanent record of the product is ascertained by the confirmation of shipment by warehouse and further authorization by the certifying agency.

5. *Share write access*: If multiple parties do not need to update the records, a central repository with multiple real-time read-only instances make more sense than a blockchain based solution. In the GNFC example, multiple entities viz. manufacturer, warehouse, PoS machines at retailer, chartered accountants and DoF need to update the records.
6. *Low transaction volume*: Despite the recent technological advances, blockchain technology still has limited processing power, which makes it difficult to perform large number of transactions simultaneously. To put in context, the most commonly used blockchain platform, Ethereum is striving to reach 3,000 transactions per second from the current level of a few hundred transactions per second. Compare this to a real time payments system e.g. Visa which is capable of processing more than 50,000 transactions per second. While permissioned blockchains can handle more volume than public blockchains, the limitations of processing time still remain. The GNFC example requires a fair amount of sales data to be captured, but is not volume intensive.
7. *Non-transactional data:* Blockchain shouldn't be seen as an alternative to databases and shouldn't be used for storing private / proprietary information. It is best suited for transaction records. In the GNFC example, the data stored on blockchain was the movement of fertilisers and the related claims only. Information like chemical composition etc. which are not pertinent to the transaction being targeted for streamlining using blockchain are not stored.
8. *Reliance on trusted third parties:* If a process flow has specific requirements on the use of intermediaries / trusted partners / regulators, then it may be complicated to deploy blockchain. In such cases, it may become necessary to include regulators etc. in the project and deliver means by which the regulators can ensure compliance with laws. In the GNFC example, there indeed is a need for certifying authority to audit the quantity and quality. The quality audit can't be done automatically, and hence the scaled-up version of pilot intends to have the certifying agency as a node in the supply chain. The B1 (quantity) certification was automated using blockchain in the pilot.
9. *Controlling functionality:* If the ability to change the functionality on a blockchain (e.g., node distribution, permissioning, engagement rules, etc.) without having a detailed discussion across the large open-source forums for blockchain is desirable, then a permissioned blockchain is more suitable.

Blockchain: the India imperative

India has a unique strategy for the Government to take the lead in creating public digital infrastructure and allowing private sector innovation to leverage it for further development. Over the past decade, India has successfully created foundational digital infrastructure envisaged to enable private sector applications running on top of it – just as government builds the roads and sewage

infrastructure in a city and private enterprise constructs buildings. We have created a uniquely Indian model of digital foundational infrastructure such as Aadhaar, UPI, e-Sign and Digilocker along with digitally enabled tax governance networks like GSTN or digitally enabled health coverage such as Pradhan Mantri Jan Arogya Yojana(PM-JAY).

Table 3: ***India's Digital Foundational Infrastructures***

Aadhaar	• World's largest identity database with more than 1.2bn biometric identities • More than 25 million authentications per day
Unified Payments Interface (UPI)	• World's most sophisticated digital payments system • 1.3bn transactions processed in December 2019
Goods and Services Tax Network (GSTN)	• More than 400 million returns filed • More than 800 million invoices uploaded
PM-JAY	• World's largest healthcare initiative with ~500 million beneficiaries covered • ~119 million e-cards issued so far, ~8 million hospital admissions

From an India use case perspective, blockchain solutions are both appropriately suited for addressing several challenges and will also benefit from the infrastructure created already.

Benefits of blockchain used in Indian enterprise would include better contract management and procurement, greater accountability and quality control across supply chains and decentralization of authority in decision making. For example, blockchain can radically transform agricultural sector in India by revamping the utility of eNAM by creating an audit trail of all farmer produce and removing the mistrust between farmers and arhatiyas (mandi intermediaries). Blockchain applications can be used to explore certification of the provenance of organic produce, thus increasing marketability to foreign markets. Section 4 of this paper outlines several India specific use cases that NITI Aayog has pursued and is exploring.

From an implementation perspective, a blockchain based technology stack would require integration with an identity platform and possibly an incentive mechanism / platform. India, with proven success of Aadhaar and UPI, thus has an inherent advantage in pursuing commercial scale blockchain solutions, while other nations struggle to find a good proxy for identity and need to ensure sanctity of crypto assets. In the GNFC example earlier, the identity layer was already built in (to be integrated in scale-up version) through Aadhar enabled PoS machines at the retailers.

Fertilizer subsidy supply chain pilot (*continued*)

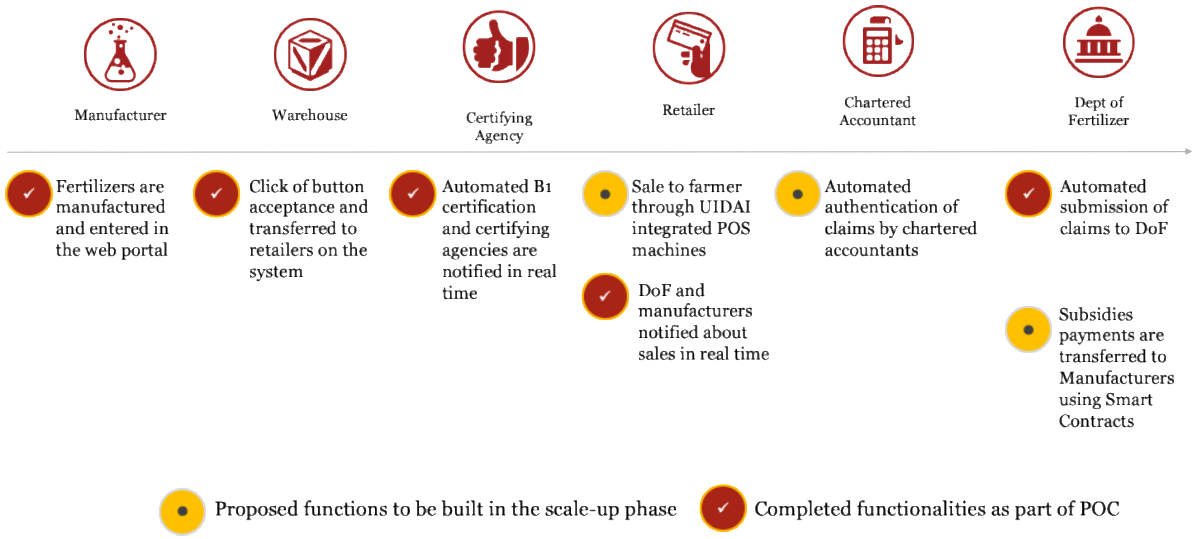
The key challenges faced in the GNFC fertilizer subsidy supply chain pilot were: (a) process inefficiencies, (b) limited visibility of stocks and inventory, (c) inability to track loss / pilferage, (d) multiple data entry points and (e) isolated claims data and generation process.

The pilot addressed these challenges by (a) creating immutable data shared with all stakeholders, (b) linking invoice to production and end-to-end visibility across the supply chain, (c) ensuring settlements and reconciliation were generated based on digital trust and (d) enabling real time claims and stock management across supply chain.

The pilot project enabled the following benefits:

1. Productivity increase: enabled shipment acknowledgements to manufacturer in minutes.
2. Near real time B1 certification as against few weeks being taken earlier: quantity of the shipped goods is tracked on blockchain and count is reported immediately.
3. Zero paper trails - shift from manual to digital: removal of existing paper based communication methods to single digital system.
4. Few hundred keyboard presses to just few clicks: integration with Enterprise Resource Planning (ERP) software enable pre-filled forms and reduction of inputs from users.

Figure 5: GNFC *blockchain based business flow*



Source: PwC

Table 4: ***Potential Benefits of Blockchain across Fertilizer Subsidy Value Chain***

Stakeholder	Current State	Future State
Manufacturer	• Has limited visibility and control into the system data and processes. • No insight into lost/spilled goods. • Dependency on paper trail.	→ Complete provenance trail of every asset. → Visibility into process flow and claim data via POS integrations. → Losses reported in real time via IoT sensors. → Real-time shipment acknowledgements.

Warehouse	• No visibility of incoming shipments. • Real-time stock and sales data aren't available. • Slow and isolated processes.	→ Complete provenance trail of every asset. → Visibility into process flow and claim data via POS integrations. → Losses reported in real time via IoT sensors. → Real-time shipment acknowledgements.
Retailer	• Fertilizer quality isn't guaranteed. • No visibility of incoming shipments. • Fertilizer losses along the way.	→ Fertilizer quality can be traced back to manufacturing source and B2 certificate. → IoT devices can help identify pilferage sources.
Government Agencies	• Auditing inventory and sales data is complex. • Isolated process structures and inconsistent siloed data.	→ Holistic data view for each participant. → Consensus and immutability ensure data is valid and can be trusted. → Minimises need for accounting and auditing.

Box 2: The Gartner Blockchain Spectrum

Gartner, the research and advisory firm, defines five elements of a true blockchain: distribution, encryption, immutability, tokenization and decentralization. That blockchain participants are located physically apart and are connected on a network is defined as distribution, and decentralization emphasizes that no single entity controls all the nodes or dictates the rules.

Gartner further proposes a framework for explaining the evolution and maturity of blockchain solutions, based on these five elements. The framework, Gartner Blockchain Spectrum, has three phases:

Phase 1: Blockchain-inspired solutions

"*This phase began in 2012 and will last through the early 2020s. These solutions include only three of the five elements: Distribution, encryption and immutability. Often these offerings are experimental and not fully implemented, and they focus on creating greater efficiency by streamlining existing processes.*"

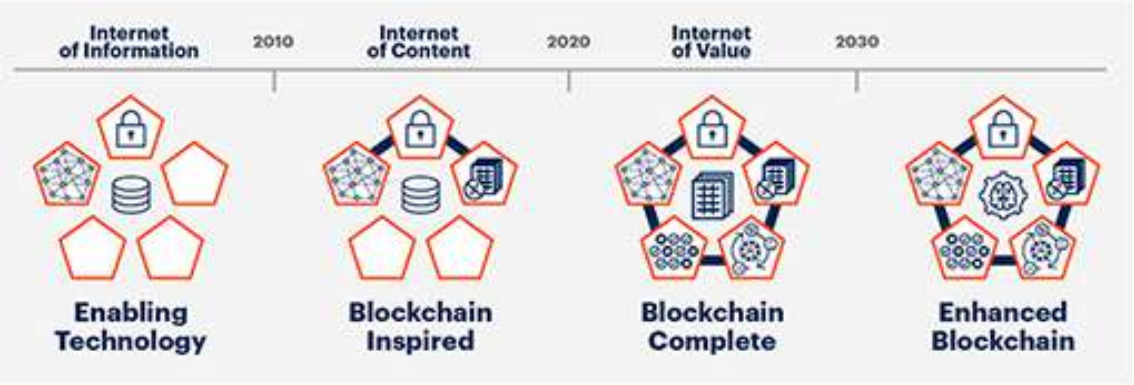
Phase 2: Blockchain-complete solutions

"Solutions in this phase include all five elements, with the intent of delivering on the full value proposition of blockchain. Currently, only startups are focused on this level of maturity, though Gartner expects these solutions to gain momentum in the market around 2023."

Phase 3: Enhanced-blockchain solutions

"The third phase of blockchain will combine blockchain-complete solutions with complementary technologies such as artificial intelligence (AI), the Internet of Things (IoT) and decentralized self-sovereign identity (SSI) solutions."

Figure 6: *Gartner Blockchain Spectrum*



Source: Gartner

Challenges in Blockchain Implementation

Learnings from projects pursued by NITI Aayog

Any transformative technology, in its initial stages of development, as it moves out of research / development phase to first few applications to large scale deployment, faces several challenges. Part of the problem is that such technologies are initially intended to solve a specific set of problems. Bitcoin, which has led to the popularity of decentralized trust systems and has powered the blockchain revolution, was intended to develop a peer-to-peer electronic cash system which could solve for double spending problem without being dependent on trusted intermediaries viz. banks. As Bitcoin started gaining prominence, the potential of underlying blockchain technology started getting traction. However, some of the early design features that made Bitcoin popular, primarily limited supply and pseudonymity, have become potential challenges in wide scale implementation of blockchain.

The evolution years of blockchain technology can be compared to that of the World Wide Web. Although detailed by Tim Berners-Lee of CERN in his paper "Information Management: A Proposal" as early as 1989, the Web struggled to gain prominence till we had intuitive interface in the form of Mosaic browser in 1993 and advent of Java Virtual Machine in 1995 which made it easier to deploy large scale Web applications. Off the blocks came the likes of Yahoo, Amazon and Google, and the internet has approximately 150 million users by end of 1998 (contrast that to 26 publicly accessible sites in 1992 and 16 million users in 1995). Blockchain in 2019 is what World Wide Web was in 1995, although rapid technology advancement has ensured that several underlying technological humps have been scaled.

The success of the initial use cases will set the tone of adoption of blockchain beyond the current experimentation phase. Selecting the right use cases for blockchain implementation, as highlighted earlier, thus becomes the biggest challenge for ensuring that, in times to come, the disruptive potential of this technology would indeed get an opportunity to play out.

Analysis of NITI Aayog's pilots has led to the led to realization of a number of lessons in implementation of blockchain, specifically in the Indian context. These factors are envisaged to be key to the success of a blockchain pilots and initiatives in both public and private sector settings.

Garbage In, Garbage Out: significant amount of work needed to ensure data is 'dispute free'

Blockchain's '*immutable'* nature necessitates the need to create a single source of truth before a process is put on blockchain. In order to maintain the sanctity of the blockchain network, and preventing retrospective changes to blocks, the business data at the time of blockchain implementation has to be the single-source of truth.

This was most evidently clear in the creation of a prototype for the management of land transactions by NITI Aayog. The entity governing the recordkeeping of land records has to make sure that all instances of land records are dispute free. Clear land titling has been a contentious issue globally, and more so in India, leading to a lack of large scale initiatives globally, despite this being an intuitive use case for blockchain implementation.

The efforts of the Union Territory of Chandigarh are commendable in this regard. While Chandigarh has the advantage of being a city that has existed for only 66 years and most land parcels may have exchanged hands may be 2 to 3 times, the work done to ensure that every piece of land has a unique ID and is mapped for ownership (including change of ownerships) had made it an ideal candidate for NITI Aayog to pursue a PoC project for land records using blockchain. The Government of Telangana has taken similar strides.

Processes may require changes to be made blockchain amenable, a shared view of success potential needs to be defined

As highlighted in the blockchain assessment framework, blockchains require that the asset being tracked be represented digitally. This requirement for a viable blockchain use case often require changes in the traditional process before blockchain can be deployed, which may cause the involved stakeholders to be reluctant to participate.

For example, in the NITI Aayog pilot for usage of blockchain for 'track and trace' of pharmaceutical drugs, drug packaging required a three tiered 'QR code' or 'barcode' for the tracking of drugs as it moved through the supply chain. Since this was not a requirement for domestic trade of drugs, stakeholders in the pilot were required to attach barcodes 'stickers' on drug packaging manually. In addition, stakeholders were required to scan the barcodes at each stage of transfer – an action previously not required in the supply chain. To obviate this challenge, it must be made clear to stakeholders the potential of cost savings due to blockchain in the long run.

Integration with legacy systems needs to be at the forefront of technical design choices

As blockchain implementations move from sandboxed pilot experiments to larger adoptions, integration with existing and usually complex legacy systems will be a real challenge for large corporations. It is no wonder that most of the use cases so far have been limited to specific parts of businesses, as corporations figure out their blockchain strategy. Even public blockchain based use cases have struggled to integrate information coming from external systems (called Oracles) in a trusted manner. However, given the predominance of such legacy systems (such as national IDs, payment systems, supply chain information, weather etc.) in current economy, it is important for blockchain systems to develop capability to integrate with legacy systems

In the implementation of blockchain for 'track and trace' of pharmaceutical drugs, for example, existing ERP or SCM (Supply Chain Management) needed to be integrated with the blockchain platform for a unified view of drugs as they moved through the supply chain. During the pilot, the

technology partner used a number of 'enterprise application adapters' part of an 'integration cloud' for the smooth ingestion of data into the blockchain. For the ingestion of data from IoT devices, as well, a software middle layer was created so that only significant events were passed on to the blockchain platform, given the inability of certain blockchain platforms to handle low latency inputs.

Legal and regulatory modifications are key to enable deployment of blockchain at scale in the private and public sectors

Blockchain deployment reduces the need for 'traditional intermediaries', instead recognizing the blockchain platform as a trusted entity to enable transactions. Historically, in the absence of trusted digital means of executing transactions, checks and balances have been developed in the form of certifications or physical verification/presence attestation. During a process for transfer of land, for example, registration of sales deeds at the registrar requires the physical presence of witnesses to ensure that transactions are not fraudulent. Blockchains, however, offer a means of carrying out these processes in a manner that would eliminate the need for cumbersome processes.

Allowing witnesses to verify transactions, electronically on blockchain, for example, would eliminate the need for physical presence and ease the process while maintaining means of establishing that transactions are not fraudulent. Among others, modification or easing of existing regulations to examine the potential benefits of blockchain, either through 'sandboxes' or otherwise.

Using technology to regulate: RegTech

Under the common law system, the traditional contract is said to be executed when there is a meeting of minds between two clearly identifiable parties for consideration, i.e. exchange of something of value. The contract may be either oral (unless explicitly forbidden by any law) or written. The written contract has evolved into including digital contracts, i.e. contracts written by humans on electronic medium and digitally signed by the respective parties.

Blockchain technology has allowed for framing and deployment of 'smart contracts' at scale. Smart contracts are a manifestation of representing traditional contractual terms in lines of code- a series of if-then functions. Transactions or data recorded on the distributed ledger can trigger clauses in smart contract which can control real life assets such as real estate, insurance claims, etc. The self-executing and self-enforcing nature of smart contracts entails that the parties have no role to play and whatever result the smart contract achieves has to be considered to be the ideal one, regardless of its absurdity and practicality.

Smart contracts pose their own set of legal challenges, such as:

i. Can smart contracts be afforded legal recognition?

ii. Can they be enforced in the same manner as traditional contracts?

iii. Can smart contract be executed between two (or more) parties, the identities of whom may not (or cannot) be known to each other?

iv. Given the hyper-literal nature of smart contracts, can human interpretation be permitted to prevent absurd results?

v. In case of breaches/hack, who is to be held liable?

While it is yet to be seen how legal regimes evolve to accommodate smart contracts, it is clear that computer codes cannot constitute the whole of the understanding reached between two parties. As contracts are as much as social tools as legal instruments, machine codes cannot accommodate for tacit agreements or implied understandings between two parties. One recommendation which can be readily implemented is to devise a hybrid contractual model, where the smart contract clauses are supplemented by readily available and legible traditional contractual documents. In case of conflict between the two, precedence should be given to the traditional contractual document, as it will more readily reflect the intention of the parties. At the same time, it is important to discern which interfaces are operations are amenable to be on loaded on smart contracts and with which parties.

Apart from the challenges directly observed in the implementation of blockchain to specific use cases, a number of exogenous challenges are also highlighted below:

1. ***Suitability of atomic vs. non-atomic transactions***: The initial implementation of blockchain solutions indicate that it is more amenable to atomic transactions i.e. transactions that have a finite life, as compared to non-atomic transactions which may have large / infinite life e.g. land records. It comes as no surprise that supply chain has been the most preferred sector for blockchain solutions, securing origination and final dissemination of an asset say a shipping container or pharmaceuticals. Similarly, clearing and settlement exercises, with a finite life, have found Blockchain solutions to be attractive. Non-atomic transactions on the other hand require 100% clean antecedents as a starting point, and hence require a lot more legwork for them to be amenable to blockchain solutions.
2. ***Initial cost of implementation***: As discussed earlier, most of the initial blockchain implementations will be in the form of private or permissioned blockchain networks. The initial infrastructure cost of such a system, which unlike in a public blockchain could have been crowdsourced, has to be borne by the business itself. The high cost of computing and development has to come from the institution itself, and so will be the ongoing maintenance requirement. Quantifying this cost element and putting in place a clear system for defraying the same both for the pilot as well as scale up version would need to be done upfront.
3. ***Human resource constraints***: Any emerging technology, in its early years of adoption, requires evangelists / champions across business functions, especially at the top. In addition, technical expertise is needed to ensure implementation. The requisite numbers for both are in short supply at present in India. Lack of regulatory uncertainties is further discouraging people from venturing in this sector.
4. ***Nascent developer community:*** Even by the most aggressive estimates, the number of qualified blockchain developers globally wouldn't be greater than 10,000. Contrast this to the number of Java developers, well north of 10mn across the globe. The good news though

is that underlying blockchain programs are not very dissimilar to the popular programming languages such as Java and Python, and existing programming community can be upskilled to blockchain programming. Large blockchain companies, the likes of Consensys, have also understood that talent needs to be invested in and have started programs to build developer communities.

Box 3: Blockchain Implementation for Land Records – laws may need to be amended for large scale implementation

Realization of the full benefits of blockchain technology in land transactions would see the technology used not only for storage of information pertaining to land ownership, but act as a platform for payment of stamp duty, registration of title deeds, payment for utilities, and more. Land transactions in India are governed by multiple central and state-specific legislations. Interestingly, the Information Technology Act, a central legislation, does not afford legal sanctity to instruments (contracts) effectuating a change in title of immovable property (for example, land). Moreover, the Registration Act, dealing with registration of instruments including for property transactions, requires the physical presence of the parties and witnesses before the registration process. Other state specific legislations have made land transactions in India a daunting and extremely slow process. Some examples are stated below:

Obligation to give duly stamped documents when amount greater than Rs. 20 is received (if so demanded by the other party), Indian Stamp Act, 1889

The original act requires that the receipt to be stamped and given in physical form. While some states have made a provision for online payment of stamp duty, however the concerned party still has to physically go to designated centres for printing of the stamp paper.

Persons to present documents for registration, Registration Act, 1908

The original law requires a person and his/her representative to be present at the registrar's office for the purposes of registration. This law would need to be amended for a full scale blockchain implementation to remove the mandatory presence of a person since the entire process would be conducted digitally.

Key to the legislative and regulatory enterprise surrounding blockchain is the need for using clear and simple language to enable lawmakers and practitioners to grapple with, and starting assuming control over, the constantly evolving blockchain ecosystem. The choice of language will go a long way in ensuring that the end users make informed decisions and reduce the power imbalance, given the legal and technical risks surround blockchain applications. Adopting standardized terminologies for blockchain concepts will help demystify the technological enigma that blockchain is made out to be, which can build political will to bring about the regulatory changes required for adoption of blockchain at scale.

Blockchain Use Cases

Case studies from NITI Aayog's vault

1 Land Records: Creating a new system to manage land record transfer and ownership

Context

As an asset, land has intrinsic value dependent on its location and corresponding demand and limited supply. It is, in fact, one of the critical factors of production. Access to land has wide ranging economic, social, cultural, livelihood and industrial implications[10].

India's land ownership and transfer system, however, has largely been inherited from the British administration. Land ownership is primarily established through a registered sale deed. This document is not a government guaranteed title to the property, but only a record of the transfer of property – and hence subject to challenge.

During the course of the pilot, NITI Aayog found that administration has to sometimes go back to several years of documents, including manual records, to find any ownership claims on a piece of property. Such a process is inefficient and causes time delays as departments, at times, work in silos, and the data across departments is not updated efficiently. Not only that, there is always a realistic chance that the records are lost due to fire or natural calamities. Some departments also have a policy of weeding out old documents from time to time. Hence, discrepancies and disputes pertaining to land records and ownership compromise a large corpus of matters pending before various judicial and administrative forums.

The process for transfer of land was also found to be extremely complex, with a number of steps requiring seemingly redundant visits to government offices responsible for oversight of the process.

Current issues in land transactions

a) Establishing ownership over land: Ownership to land can come through inheritance, gift, purchase, and relinquishment. In India, property ownership is primarily documented through a registered sale deed in case of a purchase of a land property. Other documents which establish ownership include property tax receipts, survey documents, etc. However, while entering into a transaction, the onus is on the purchaser to verify the credentials and ownership status of the seller. As the sale deed is a mere record of transfer of property, and is not a government guaranteed title to property, it can always be subject to challenge.
b) Poor maintenance of land records: Government authorities such as Registrars, Patwaris and Revenue Offices maintain records of property ownership and transfer, especially those of land. Official land surveys conducted by the State have been extremely irregular, for

[10] PRS India, Land Records and Titles in India (http://www.prsindia.org/uploads/media/Analytical%20Report/Land%20Records%20and%20Titles%20in%20India.pdf)

instance, last land survey in Telangana (erstwhile Andhra Pradesh) was done during Nizam's regime in 1932-36. Prior to transfer of a property, the purchaser often has to seem through a pile of documents, which are mostly manual and are sometimes in a dilapidated or illegible condition, to verify the nature of title to the property that the seller has. Such a process is inefficient and causes time delays as the concerned departments work in silos, and the data across them is not updated efficiently. Not only that, there is always a realistic chance that the records are lost due to fire or natural calamities, or even due to deliberate acts by corrupt officials for the benefit or detriment of one or the other party.

c) High amount of litigation: Discrepancies and disputes pertaining to land records and ownership comprise a large corpus of matters pending before various judicial and administrative forums. Land related disputes, such as those related to validity of land titles and records, account for two-thirds of all pending court cases in the country[11]; and which take on average about 20 years to be resolved.[12]

d) Asynchronicity of information: Registers held by different agencies (e.g. Estate Office and Sub-registrar office) are updated at different times in the land transfer process – leading to a lack of clarity in ownerships status and cumbersome tasks for the citizen.

NITI Aayog's approach to blockchain in land records

On completing the survey of the 'as is' process in the Union Territory of Chandigarh, NITI Aayog and its technology partner created a process flow in order to identify sections of the process for which specific blockchain features may be utilized. While some of these features may have been realizable through pure 'digitization' of processes by improved usage of existing IT systems, features of blockchain such as its decentralized nature and ability to execute 'smart contracts' were found to be critical in simplifying the process tremendously.

A 'prototype' was developed to showcase the abilities of a revamped system build on top of a blockchain. This system allowed for necessary stakeholders to be brought on board with adjustable read/write accessibility, citizens to manage their land transfer (including uploading of necessary documents, payments) through a single user friendly portal, and ability to view current status of their transaction through events immutably stored on the blockchain.

[11] "India- Land Policies for growth and poverty reduction", Agriculture and Rural Development Sector Unit, India Country Management Unit, South Asia Region, World Bank,

[12] "Strengthening Arbitration and its Enforcement in India – Resolve in India", NITI Aayog,

Figure 7: *A snapshot of blockchain system for land records*

Source:
ConsenSys

Benefits of a blockchain enabled system

The blockchain enabled system created immutable records for land ownership, which are then digitized and stored permanently on the system, with the ability to track any change in ownership of these titles. Any new transaction (such as further sale or mutation of title) gets recorded on the blockchain immutably while remaining available to other stakeholders (utilities, insurance, etc.).

Highly recommended and adopted in many countries, the Torrens system of land registry is based on three fundamental principles:

- Mirror principle: the land records register reflects (mirrors) accurately the details of all registered land assets
- Curtain principle: the recorded facts about the asset are sufficient; do not require an ownership trail of documents
- Indemnity principle: the state provides for compensation in case of error made by the state

A blockchain based land registry system ensures the first two principles by design. The inherent design of the distributed record of land assets and its transactions automatically implement the mirror and curtain principle. The third principle of indemnity is implemented by the State once the record system has gained a critical confidence on the data and transaction integrity.

The other potential benefits of 'scaling up' the developed prototype was perceived to be as:

- Ensuring certainty about ownership of property which can pave the way for a system of 'conclusive titling'
- Reduction in litigation associated with land transfer as the title records are clearly and immutably recorded

- Stimulate land purchase transactions and investment by companies – create a seamless marketplace for land transactions thus unlocking economic value and liquidity
- Overall system transparency through real-time audit capabilities, and digitally-signed and time stamped records

With the characteristic requirements of maintaining clear ownership records, transaction history and allowing transaction between multiple parties, blockchain technology serves as the best way to implement the land records system as it inherently offers these benefits. A blockchain based land titling and transaction system will track purchases and sales of land titles, mortgages and rentals, as well as notary services on top-of-stack land registry and verification platform for financial institutions.[13]

This platform will capture transactions, verify the data and work with financial institutions to update current registries, enable smart transactions and distribute private keys for clients - to allow an automated and trusted property transactions between all parties.

Partners (Nodes) Identified to hold access to the private information on blockchain, were identified through the pilot to potentially be the following: Title Holder of the property, Purchaser of property, Government registrar, Government revenue office, Land survey office, Real Estate Regulatory Authority (RERA), Financial Institutions, Financial Regulatory Authority (for monitoring purposes), Real Estate Companies or Appraisers, and Insurance Providers.

2 Pharmaceutical drugs supply chain: 'self-regulation' of the sector through blockchain enabled trust

Context

The issue of counterfeit drugs is a global concern, with every country currently tackling its menace. It is an increasing worldwide dilemma with a profound impact on lower income countries (LIC) and lower middle-income countries. As per the recent WHO estimates, an estimated 1 in 10 medicinal products circulating in low- and middle-income countries is either substandard or falsified. In India, fake medicines are a major concern with approximately 3% of drugs being substandard or counterfeit, as per National Drug survey 2014-2016, conducted by National Institute of Biologics, Ministry of Health & Family Welfare.

With this growing threat of spurious drugs entering the supply chain, especially reaching the hands of customers, it was recognized that there is an imperative need of greater visibility and traceability into the origin of medicines and how they have been handled throughout their journey in the supply chain.

13 Chromaway, Blockchain Land Registry System 2017

Current process and challenges faced

In most cases, research and interviews conducted during the initial stages of the initiative found that drugs coming directly from the manufacturer's facility are trustworthy and that the risk of entry of fake drugs arises when the products are handed off between the various stages and layers of the complex supply chain (i.e. wholesalers, distributors, or sub-distributors). At each transfer point from the factory to the patient, drugs can be stolen, adulterated, and replaced. The result of such malpractice leads to financial loss to the drug makers, and more importantly, significant risk to patient safety.

It was noted that National Informatics Centre has designed and implemented a new system named Drug Authentication and Verification Application (DAVA), based on the GS1 standards, for drug tracking and traceability. The system is based on the use of Global Trade Item Numbers (GTINs) and serial numbers provided by manufacturers for identification of various hierarchy levels for product packaging. The aim is to improve India's image as a world leader in production of safe pharmaceutical products by providing real-time visibility of drugs produced and exported out of India. The entire DAVA system will be rolled out in phases and will include 2000 manufacturers, beginning with the participation of large and medium manufacturers, followed by small-scale manufacturers. Barcoding at the primary level will be optional, however, barcode labeling and marking at the secondary and tertiary level will be compulsory.

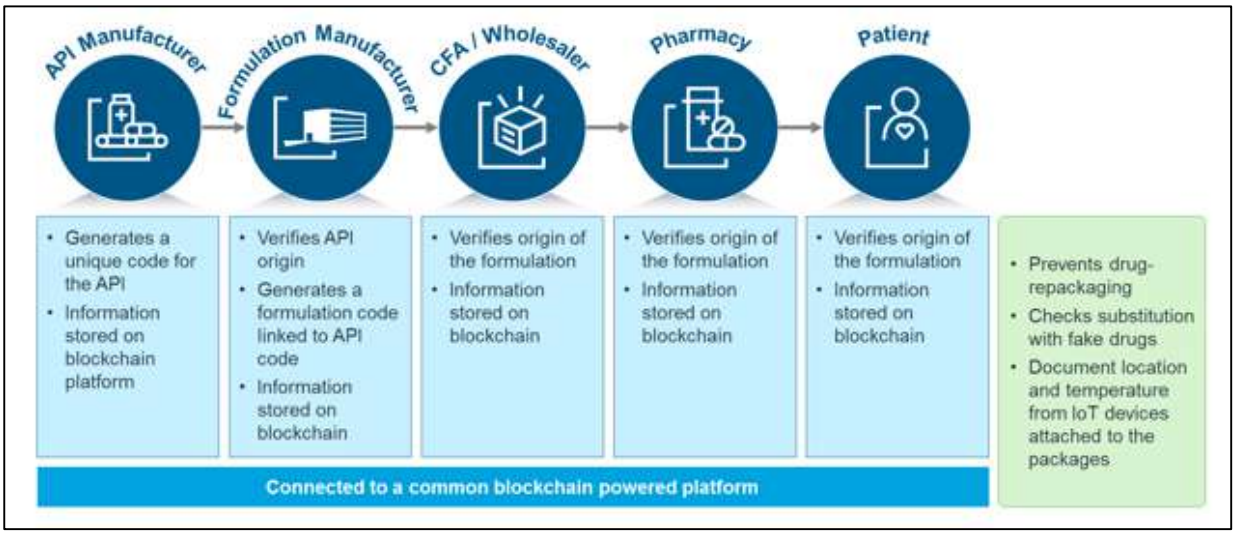
While DAVA provides for information about products at the manufacturer level which can be verified by other stakeholders, however, it was found that it may not encompass the full functionality that blockchain can. For example, it does not ensure visibility of each transaction to all stakeholders that is of immense importance in a multi-stakeholder, multi-location and multi-product scenario. Further, it is not able to track and trace the product throughout the supply chain and ensure temperature compliance. With emerging technologies such as blockchain and Internet of Things (IoT), these can now be achieved.

Leveraging blockchain technology for a unified data system

NITI Aayog organized this initiative with a host of partners in the healthcare and technology domain. In this sense, the pilot was unlike the other pilots conducted in that the process was not entirely 'captive' to a single institution and required large scale collaboration for its execution. The partners onboarded ranged from drug manufacturers, to transporters and logistics providers, and drug retailers.

The pilot required the integration of a number of a number of independent IT systems for the transmission of information on the receipt and transfer of goods, and a concerted effort was made to ensure that manual entry of information was restricted.

Figure 8: *The ideal case blockchain implementation*

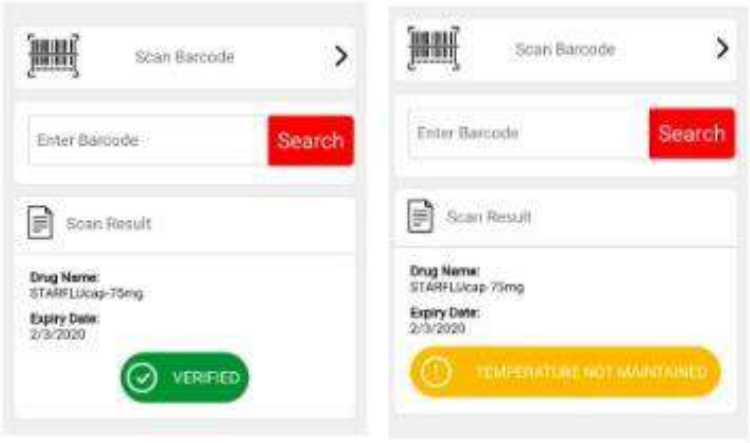


Source: IQVIA

As the pharmaceutical drug moved through the supply chain, each transaction was pushed by internal systems in an automated manner and registered as well as time-stamped using the ledger to ensure security and safety of the product. Due to decentralization, encryption methods and immutable record keeping, a large amount of associated data can be shown to the stakeholders without compromising the data security. Further, even manufacturing inputs, like active pharmaceutical ingredients and excipients were tracked and linked to the final pharmaceutical products. Additionally, the blockchain documented critical details like location and temperature from IoT devices attached to the packages, making the journey visible to all stakeholders, thereby limiting the possibility of record tampering.

The scope of the project enabled track and trace beyond traditional methods by allowing users to verify that prescribed conditions for the transportation of drugs was not breached (through IoT sensors) and status was made available to stakeholders through a mobile application. Specially created bar codes were sourced from the international standards body, GS1, to enable tracking.

Figure 9: *Snapshot of mobile application for blockchain solution*



Source: Oracle

Benefits of blockchain technology observed

It was found that blockchain technology has the potential to improve transparency, efficiency and reliability of transactions in a heavily regulated pharmaceutical industry. Using blockchain, manufacturers and other supply chain participants can gain real-time data access and greater visibility throughout the supply chain, starting from the point of manufacture (raw material/API suppliers' product codes) to the point of sale (pharmacy stores dispensing prescription/OTC medicines to patients). Most importantly, however, consumers will have the ability to verify the provenance of the drugs at the point of purchase. Major benefits are highlighted below:

- End-to-end traceability of pharmaceutical drugs: Provide streamlined visibility of the movement of drugs or medicines at each stage/stakeholder in the value chain. This improved traceability facilitates the optimization of drug flow and an efficient inventory management system, leading to considerable improvement in planning of stocks.
- Transparency to enhance accountability: The shipping of drugs throughout the supply chain can be traced at each point of ownership. Also, it is possible to trace the actors or stakeholders involved in the chain of shipment. If any problem arises during the supply of drugs or medicines, blockchain can enable to identify the last stakeholder by which the product passed through.

  Blockchains also allow the identification of exact locations of medicines at each point of transaction and allow for 'batch reminders' to be sent out efficiently to ensure safety of patient's health.

The introduction of blockchain technology in the supply chain will enable pharma companies to reduce dependence on intermediaries, ensure transparency in stock movement, control quality, and improve overall reputation of the industry. The government can play a lead role in enabling a common public infrastructure built on top of an underlying blockchain system. This would also greatly benefit various government schemes in the health sector.

3 SuperCert: anti-fraud identity intelligence blockchain solution for educational certificates

Context

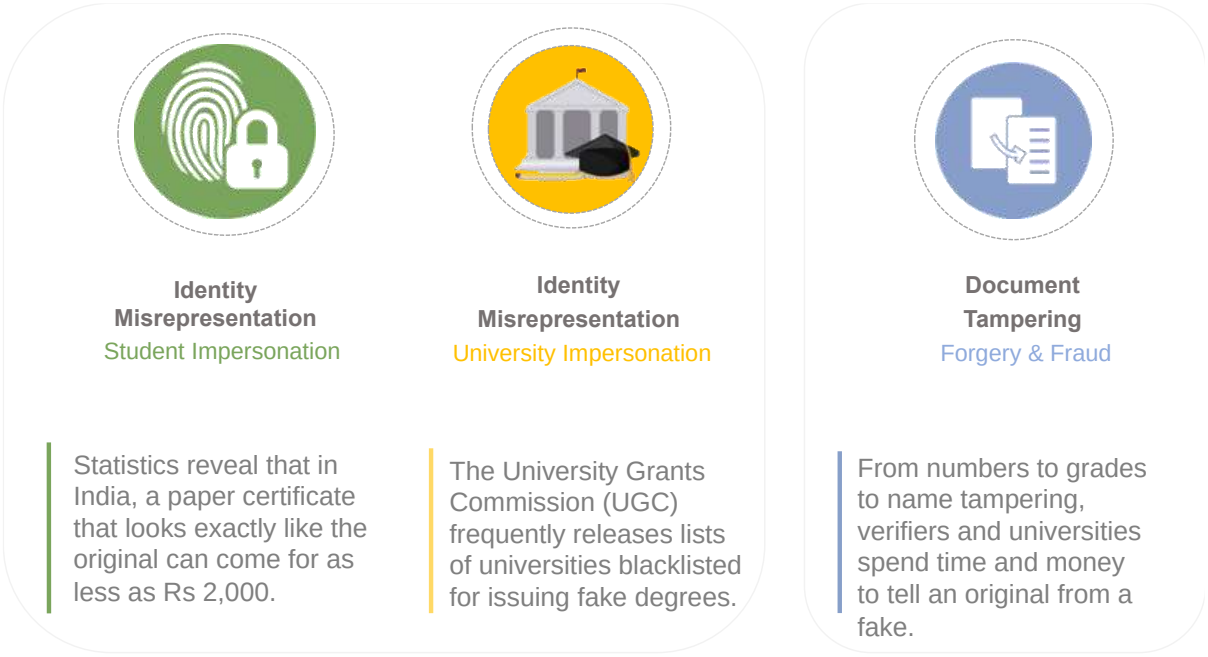
'Certificates' are a means of verifying the credentials of individuals across domains and geographies. A paper-based certification is fallible to manipulation and susceptible to fraud. According to a report by First Advantage, a background screening company, there are more than 7,500 organisations that provide fake employment and educational certificates. There are usually two problems at play: degrees from fake universities and fake degrees from real universities.

The University Grants Commission (UGC) has been acting on several of these complaints, and frequently blacklists universities and organisations, however scrupulous agencies keep mushrooming up.

The problem has a tangible cost – companies spending significant amount of money to verify the credentials of prospective employees; cumbersome and time consuming process for students planning to pursue further studies both in India or abroad.

To address the problem, several institutes have moved to digital methods of certifications. However, the current system of digital certification, digital signatures and certificates rely on a set of trusted third parties. This process is also susceptible to fraud and malicious attacks – as seen in the 2018 case of CEO of CA Trustico mailing the private keys of 23,000 certificates, forcing the Root CA to invalidate the certificates.

Figure 10: *Fraud in educational certificates*



Source: Bitgram

Current challenges

Existing solutions of educational certificates verification thus have the following challenges:

i. Centralised i.e. completely dependent on certificate issuing authority

ii. Manual i.e. verification is usually done through emails, phone calls or web forms

iii. Time consuming – could take weeks or months

iv. Easy to breach and tamper

There is thus the need for a decentralised trust system that is verifiable and tamper-proof, is automatic, real-time and is fraud-proof.

Leveraging blockchain for educational certificates

NITI Aayog, in partnership with the Indian School of Business (ISB) and Bitgram, attempted to address the challenges in educational certificates through a blockchain based solution. The approach, SuperCert, has a permissioned blockchain architecture that involved decentralization, intelligent identity encryption and identity interlinking for issuance of educational certificates. The process involved:

i. Creation of student identity – Superidentity. A unique blockchain representation of the identity is provided, along with a set of public and private keys.

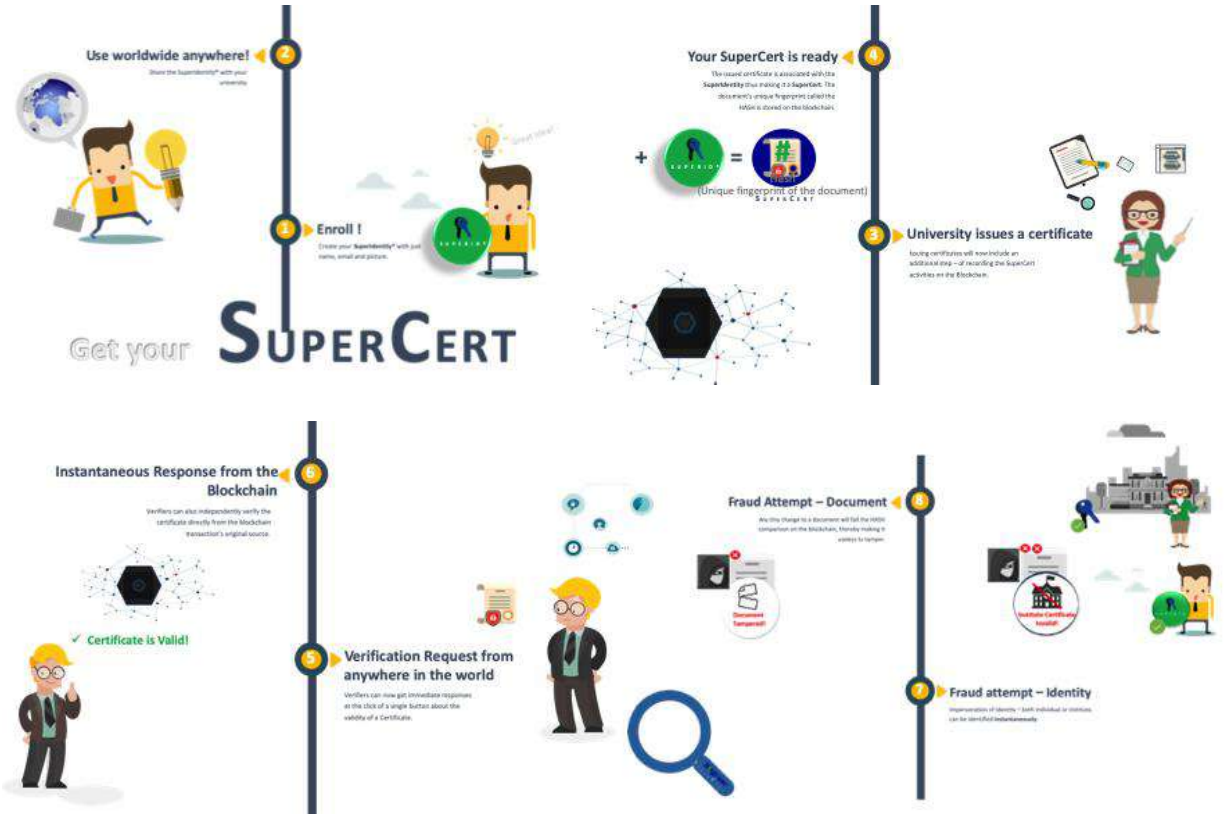
ii. Issuance of certificate by university, together with Superidentity of the student.

iii. SuperCert i.e. creation of a block of student certificate – hashed version of the certificate on the blockchain

iv. Verification of the certificate using the public key of the student and the public key of the university. The solutions have features for both online and offline verification.

The immutability feature of blockchain ensures that tampering of certificate is not feasible – both the content of the certificate and the identity of the certificate holder.

Figure 11: *Process flow for blockchain based educational certificate solution*



Source:
Bitgram

The key features of SuperCert include:

i. Data privacy: data stays with the entities that own them.

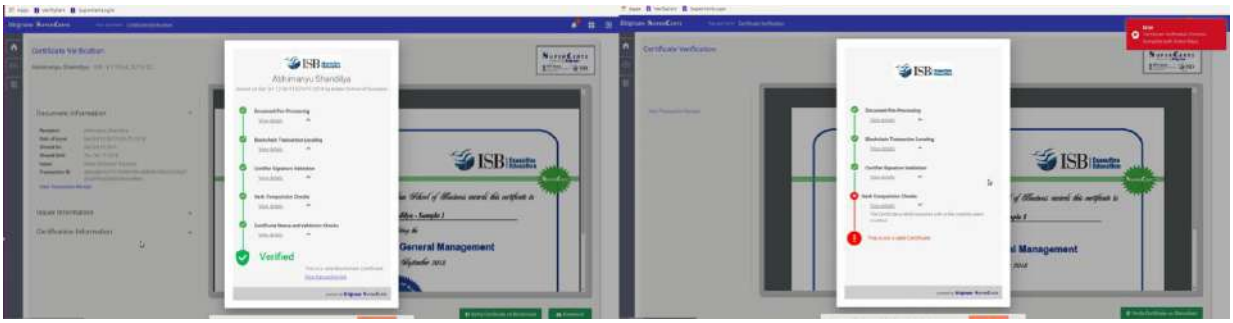
ii. Real-time, automated verification from anywhere in the world.

iii. Tamper and fraud resistant

iv. Permanence: the certificates will survive beyond organisations – removes dependence on the issuing authority for future verifications.

v. Scalable to national and global level.

Figure 12: *Verification process for SuperCert*



Source:
Bitgram

The production version of SuperCert is ready and has been tested, and is expected to be deployed in pilot mode for one of the courses offered by ISB in next few weeks.

Other use cases explored by NITI Aayog

Immunization Supply Chain: Building A New Immunization Infrastructure for India - Unified and Enhanced by Blockchain

Context

Immunization has shown to be one of the most cost-effective interventions for controlling infant mortality, with a measurable impact on both life expectancy as well as economic outcomes at the community and national level. Thanks to strong government support, India has and continues to make progress in immunizing the nation's population by expanding the basket of available vaccines (introducing 5 new vaccines IPV, adult JE, Rota, PCV, MR in past 3 years) and taking these vaccines to the last-mile through programs like Universal Immunization Program (UIP), which is the largest in the world by number of vaccines administered, size of geography covered, and number of beneficiaries.

However, India also accounts for over large percentage of global child mortality, caused in great part by mortality due to preventable diseases such as measles, rubella, hepatitis, pneumonia, diarrhoea, malaria and others. As per a study conducted by the University of Michigan, only 18% of India's children receive the whole dose course for diphtheria, pertussis and tetanus, while only 33% of the children get a second dose of measles vaccine by the recommended age of 10 months[14].

Current process of vaccination and record keeping

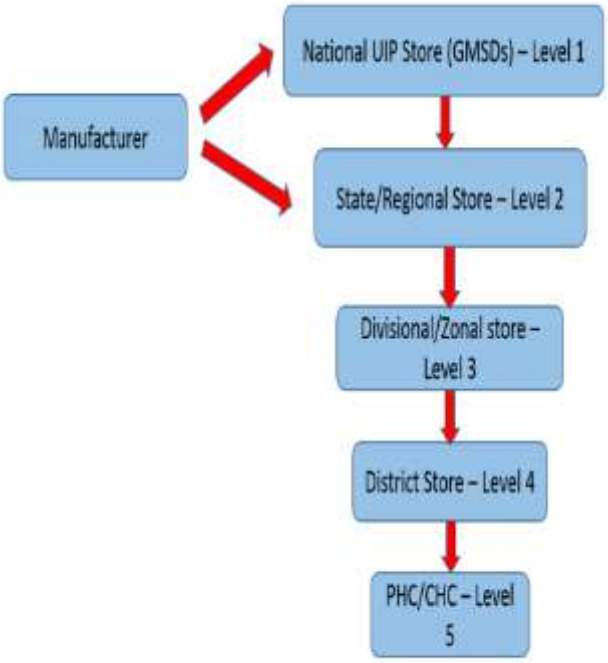
Every baby born at a hospital is given an immunization card which is to be maintained and presented by patents before the immunization centres every time the child is given a vaccine dose. If the card is lost however there is no other record for immunization events. This problem is magnified for population residing in urban slums and rural areas.

As per the National Immunization Schedule issued by the MoHFW (Ministry of Health and Family Welfare), for most of the Vaccine Preventable Diseases (VPDs), a child has to be immunized anywhere between 24 hours, since birth, to 24 months. In this timeframe the child has to get multiple immunization shots for the concerned disease at regular intervals.

India has built a vast cold chain infrastructure consisting of as many as 27,000 cold chain points, yet many vaccines may lose their potency and efficacy by the time they reach the last-mile due to unreliable handling and inefficient real-time tracking mechanisms. The flowchart below represents the current vaccine logistics system in the country:

[14] University of Michigan, Vaccination Timeliness in Children Under India's Universal Immunization Program, 2016

Figure 13: *Current vaccine logistics system*



Source:
NITI Aayog

Current challenges

Implementing an immunization program over a population as large, as widespread, and as diverse as India's requires the following features, the lack of some of which may be challenges to blockchain implementation:

i. Accurate, reliable, and real-time data: Constant monitoring is required on the state of vaccine coverage and consumption at multiple levels in order to facilitate planning for what / how many vaccines are needed where, and to allow for evaluation of program success.
ii. Vaccine supply chain (cold-chain): Vaccines can only save lives if they remain cool. Cold chain is a system to ensure that the vaccine is stored and transported at the recommended temperature from the point of manufacture to the point of use.
iii. A network of health workers and an incentive system to motivate them and hold them accountable: These health workers include those working within cold-chain facilities, those in last-mile delivery centers, and those in immunization centers that play a role in reporting outcomes so that the information can be bubbled up the value chain and analyzed by administrators.
iv. Data incompleteness and tardiness: Health workers in the field and at health clinics forget to enter patient data (e.g. Aadhaar numbers) when vaccinating individuals, or they enter it incorrectly and with delays. The same is true for cold-chain workers.
v. Fragmented data and lack of interoperability across databases: There is no way to reconcile immunization coverage data (from the supply chain) with immunization utilization data (from

the health clinics), as the two are written onto different systems. Inventory data and transactions involving motion of vaccine vials from place to place are recorded on the electronic Vaccine Intelligence Network (eVIN) system. Utilization data recorded by health workers is written onto systems like MCTS (Mother and Child Tracking System) and HMIS (Health Management Information System). These systems are not interoperable.

vi. Data inconsistencies and corruption: The two aforementioned facts result in an abundance of discrepancies between data collected and stored in different places and lack of methods for resolving them. Some discrepancies are accidental, some are purposeful (dishonest reporting, mis-direction / pilfering of vaccine vials).

Leveraging blockchain technology for a unified data system

The application of blockchain technology to the immunization system could potentially help realize the following benefits:

1. Cold Chain Management: As blockchain implemented solution will allow the concerned stakeholder to know who wants what type of vaccine, where, and when. This will improve managerial efficiency as there would be less human-level intervention at different points, while giving much lesser and more experienced number of users across each state the power to make decisions. At the heart of the technology would lie a means to add a QR code to each vaccine container, and an internet connected device that would enable broadcast of its GPS location and real time temperature. This information would consistently be added to the blockchain. Moreover, blockchain would also facilitate tracking of returned vaccines and make physical stock registers redundant; as well as vaccine forecasting and procurement management

   It is pertinent to note that Ministry of Health and Family Welfare has launched an electronic Vaccine Intelligence Network (eVIN) that digitizes vaccine stocks and monitors its temperate. Integration of blockchain technology with this project could help us reap exponential benefits.

2. Ensuring timely vaccination: By putting in place a blockchain powered digital registration infrastructure, health officials and workers can digitally register the incidence of birth of a child anywhere-including, for instance, when a child is brought to an immunization center. Immunization centers can especially play a central role regarding children who are delivered at home or unregistered private hospitals/clinics, but who are brought to the centers for vaccination. By letting health facilities be the nodal point for birth registrations, and digitally integrating it with the National Immunization Schedule, health officials can be alerted about children in need of their first or subsequent vaccine doses, rationalize procurement and distribution of vaccines; while at the same time providing the government with robust statistics on vaccine coverage.

Blockchain can also be integrated with two of MOHFW's projects - Health Management Information System (HIMS) and Mother and Child Tracking System; the latter's main goal to be to ensure that all pregnant women are given the right healthcare and all the children receive their full immunization schedules.

3. Alerting parents: By way of digitising and having one central repository with details of immunization doses of every child, a consequent alert system can be designed which will automatically send SMSs to the concerned parents regarding reminders and progress of immunization, as well as where and when the next immunization schedule would be held. In addition, this, individuals recognised by the community as socially adept can be put in charge to disseminate awareness about immunization and details about the oncoming immunization drive.
4. Incentivising parents and health officials: The use of blockchains as a record-keeping mechanism opens up the door to innovations such as automatic benefits transfers to health workers and cold chain workers to reward them for data timeliness/completeness or to penalize them for the lack thereof. These transfers would be self-triggering, trustless, and efficient, leaving no room for corrupt institutions in the middle to misdirect funds meant for field workers, as is often the case in the developing world.

Unifying immunization data on a blockchain infrastructure would immediately improve real-time visibility of immunization vial transfers and delivery, while creating a foundation for future innovation e.g. the use of smart contracts for rewarding health workers.

Chit Funds: A blockchain based model to enhance trust and unlock value creation

Context

In a chit fund scheme, a group of individuals comes together for a pre-determined period and contributes to a common pool at regular intervals. Every month, until the end of the tenure of the scheme, the collected pool of money is loaned out internally through a bidding mechanism to the winner of the auction. This way, people who need funds are served by those who want to save, for an interest rate derived from bidding. In general, the rate of interest earned by a subscriber is more than the rate of interest offered by banking systems in time deposits and offers flexibility to borrowers from the chit fund mechanism at a competitive interest rate determined by the chit group dynamics.

Existing Process

Chit funds are run across the country through a range of mechanisms. Traditional chit funds have been run in hyperlocal markets where the group is formed by a foreman within his trusted circle where the trust is mutual and the risk is always social inhibitions. The foremen manage these lending fee (‘commission’).

These traditional chit fund businesses have been corporatized and is now currently run by private limited companies. The Supreme Court of India has classified chit funds as a special kind of contract, on which both the central government as well as state governments may frame laws. In 1982, the Government of India enacted the Chit Funds Act, 1982 to regulate the sector.

Legal Framework: Telangana Case Study

The Chit Funds Act, 1982 empowers state governments to whom this legislation applies, to frame rules to give effect to the provisions of this legislation in their respective states. In 2008, the government of Andhra Pradesh framed the Andhra Pradesh Chit Funds Rules, 2008. The government of Telangana, through its Registration & Stamps Department registration and stamp department has notified the Andhra Pradesh Chit Funds Rules, 2008 that govern the working of chit funds in Telangana.

As per the Chit Funds Act, 1982, there is a set process which is defined and which all chit fund companies have to abide by. In the existing chit fund process everything from applying for a previous sanction order ("PSO"), reporting, cash handling, accounting records, auction services, fees, taxes and many more things are handled manually. There is a huge potential to reimagine this space and make this as an opportunity for both the economy and businesses as well.

The Act prohibits commencement of chits without the sanction of the state government, followed by registration of the chit as per the procedure mandated by the state government under the Andhra Pradesh Chit Funds Rules, 2008.

Further, the Act and the Rules provide for the lapse of the sanction within a specified time period, publication or circulation of any invitation for subscription subject to the publication of details of the sanction obtained along with it and furnishing of security amount by the foreman.

In addition, commencement of any chit is subject to the issue of a certificate of commencement by the Registrar. The certificate of commencement is issued only after the foreman provides the necessary details about the fully subscribed tickets in the chit agreement to the Registrar.

The commencement, and subsequent operation of sanctioned and registered chit funds is contingent of maintenance of minimum capital adequacy requirements under the Act.

Leveraging blockchain technology

Chit funds as a financial instrument have many strengths and weaknesses (in operations and administration). Blockchain can be leveraged to address many of the challenges, which would reduce the information, interaction and innovation frictions (fees, cash movements, reporting, auditing and potential fraud from the parties including foreman and subscribers).

For Regulators, the following are few benefits the government registrar/regulator can derive by administering chits funds on our blockchain driven platform:

- Protect the interest of millions of subscribers in the state

- Seamless reporting and auditing
- e-KYC / Identity for all Subscribers
- Reduce information friction by using secure, permissioned access systems
- Easy to use interface both for regulator and foreman
- Grievance redressing will be easier
- Get more insights on the per capita debt on the system in near real time
- Payment gateway integrations for the necessary challan payments
- Collective knowledge about administering and monitoring
- A blockchain driven chit fund administration will protect the interest of both subscribers and the government.

For Foreman (Chit Fund Companies), it will enable the ease of doing business on processes, by facilitating events such as:

- Online application process for PSO, group commencement, etc.
- Reporting the monthly minutes online into the system.
- Enabling credit assessment, defaulters management kind of activities.
- Driving Audit and reporting compliances by means of smart contracts
- Enabling access to other auxiliary services based on the business demands.
- Renewed trust in the system will drive the business to a new level. Business model innovations become easy to implement and monitor.

Subscribers to chit funds can easily register to any Chit Fund company on the blockchain by validating the credentials of the company. Since the entire system will be on secured, permission based, blockchain, a few things he can expect by being on this network are:

- Complete transparency in the process and way of doing chit funds.
- End to end tracking mechanisms based on his permissions.
- Choose to opt in to share his information to valid entities only.
- Better service because of increased operational efficiencies.
- Auxiliary services from the network for his active participation in the chit funds.

The subscribers once on boarded into the system will have multitude of opportunities to participate in a chit which he wants to be part of. As the system matures, the subscriber will be at huge benefit.

The following section describes briefly other possible use cases of blockchain technology towards enabling Ease of Business, Ease of Governance and Ease of Living:

1. Insurance (Medical, Automotive, etc.)
2. EV Battery Swapping
3. Organic Farming
4. Energy management

Insurance (Medical, Automotive, etc.)

Context

Insurance is a sizable market where a surprisingly high fraction of funds is lost to fraud and inefficiency. Globally, premiums for life and non-life insurance plans sum to over $4 Trillion USD. In the United States, where 2016 premiums exceeded $1 trillion USD, the 'Coalition Against Insurance Fraud' estimates that over $80 billion were lost to fraud.

The Indian insurance market is over 84 billion USD in size as of 2017[15], and growing rapidly across all service lines driven by rising incomes, improving life expectancy, and new insurance products.

Current Problems

In spite of its size, growth, and importance, the market suffers from archaic systems and broken processes that are opportunistically exploited by all parties involved:

- Insurees make multiple claims across different insurers for a single loss
- Insurees withhold information from insurers that may affect their premiums
- Insurance brokers pocket premiums not meant for them
- Insurers request compensation for services never submitted or upcode services rendered into higher price tiers

The cause for the problems:

- Difficulty in stakeholder coordination: Multiple parties involved (consumers, brokers, insurers, reinsurers) with complex interactions, lack of interoperability across databases, and lack of socio-political will to collaborate (fear of free-riders and unequal benefits from the collaboration)
- Slow or manual processes: Even if (or after) the requisite data is shared across the parties, claims need to be settled and payments need to be made. This takes time as money changes hands using banking systems which are separate from the insurance information systems, and each party must manually update their system once funds are received.
- Strong financial incentive to exploit system vulnerabilities: There is a lack of systems to discover fraud in real-time and to hold parties accountable. We are talking about billions of dollars in insurance premiums.

Insurance systems need a reform. First, we need to digitize and securely share claims data and other associated data (health records for health insurance, automobile records for auto insurance, etc.) across stakeholders. Second, we need to codify business rules and automate claims processing, such that payments are automatically and quickly transferred when claims are verified.

[15] https://www.ibef.org/industry/insurance-presentation

How can blockchain help?

Blockchain solutions can help by enabling secure data sharing and claims processing:

- Shared view of truth: A blockchain system would allow same-time access to the shared truth on patient health (past and present), processing status of the current claim, the history of past claims, etc. This shared database should be permissioned, such that the various parties may only read or write fragments of data that pertain to them.
- Programmable transfers: In a 'smart contract' enabled solution - when the encoded conditions are met (e.g. a claim is validated), funds can instantly and frictionlessly be transferred from source (insurer) to destination (consumer). Insurance is a use case requiring financial exchange, and blockchains provide the unique ability to handle financial exchange on the same platform as the information system. This is in stark contrast to the current system where payments go through separate routes and information is updated on separate databases, and information asymmetries can arise. Blockchain smart contracts cannot be modified once published, and their fund transfers cannot be intercepted.

  When the encoded conditions are met (e.g. a claim is validated), funds can instantly and frictionlessly be transferred from source (insurer) to destination (consumer). Insurance is a use case requiring financial exchange, and blockchains provide the unique ability to handle financial exchange on the same platform as the information system. This is in stark contrast to the current system where payments go through separate routes and information is updated on separate databases, and information asymmetries can arise. Blockchain smart contracts cannot be modified once published, and their fund transfers cannot be intercepted.

- Transparency for relevant institutions: A blockchain would remove the need for unnecessary middlemen and force integrity and accountability upon those that may previously have been corrupt. The insurance process would benefit from a system in which no party owns the data yet multiple stakeholders can view and modify it – where all have same-time access to the shared truth on patient health (past and present), processing status of the current claim, the history of past claims, etc. This shared database should be permissioned, such that the various parties may only read or write fragments of data that pertain to them.

EV Battery Swapping

Context

The government has set a target that 30% of all vehicles be electrically driven by 2030. For this aim to be realised requires that strong incentives be created for the manufacture, sale, and usage of electric vehicles. In addition, it is expected that the increased usage of EVs will substantially increase the usage of batteries to power them.

Current Problems

There currently a number of challenges to increasing adoption of EVs in the country, largely due to the high cost of usage and low range of the vehicles. Though technology is improving, an issue of battery charging is particularly troubling. 'Charging station' infrastructure required to allow large scale proliferation of EVs is still limited, and affects choice in buying of vehicles. A proposed method to deal with this challenge is to bypass cumbersome charging stations and create battery sharing ecosystems - which would (very basically) allow users to swap batteries out on the exhaustion of charge. Though the proposed system may be easier to build than a network of charging stations, it posed challenges of its own:

- Costing usage of battery: Location aside - some features of batteries may directly affect their worth, such as the age of the battery and its historical treatment. Tracking of energy consumption is also cumbersome.
- Difficulty in energy source attribution: An aspect of EV usage sometimes overlooked is that they are largely environmentally viable only if the source of electricity is also driven by renewable energy. Attributing electricity sources is a difficult process, however.

How can blockchain help?

The storage of parameters describing each battery on blockchain, used together with IoT, emerges as a possible solution to the problems highlighted above.

- Immutable battery information storage: The blockchain may store information such as age of the battery and its previous treatment in an immutable fashion, thus removing the possibility of misrepresentation to increase price or lower cost of usage.
- Attribution of energy source: Usage of blockchain to store information on the sources of energy used to charge the battery may help inform choice to incentivize usage of sources of renewable energy.
- Programmable transfers: Exploiting the 'smart contract' feature of blockchain applications would allow for more efficient swapping of batteries at charging stations, since simple rules on costing can be applied on the basis of battery attributes and executed on exchange.

Organic Farming

Organic agricultural produce is defined as produce for which no chemical pesticides, fertilizers, etc. have been used for production. While India's overall agricultural exports have stagnated since 2015-16, export of organic foods has seen substantial increase, as consumers in developed markets such as UK, USA, and Canada have become more conscious of healthy diets. Export of organic foods has risen by almost 25 per cent between 2015-16 and 2016-17 from Rs 19.76 billion to Rs 24.78 billion at a time when overall farm exports grew by less than one percent from Rs 1,074.31 billion to just Rs 1,084.26 billion.[16]

[16] https://www.business-standard.com/article/economy-policy/organic-food-exports-surge-certification-remains-a-major-issue-118032800261_1.html

Though it is a very small portion of India's overall agriculture export basket (less than 3 percent), the potential for growth in this segment presents a large opportunity for Indian agriculture. There have been issues, however, that have affected growth.

Current problems

One of the significant issues in the area is that certifications are required from multiple parties for the products to be deemed 'organic'. Currently, there are two government sanctioned mechanisms for issuance of certification:

1. PGS Participatory Guarantee Systems (PGS): Farmers in a group inspect each other's land and vouch for its organic credentials. The inspection is carried out at the start of every sowing season and farmers visit each other almost weekly to provide counsel. If a farmer is found to be in violation, her produce is not sold through the group till she rectifies her mistake.
2. Third party certification: The farms is certified by authorized third party certifying agencies.

The database of India's organic products is very poor and traceability, which is key for export growth, remains weak, while third party certification as insisted by APEDA is very costly. In addition, major markets for export do not accepts PGS certification, and there is no mechanism to link certifications by third parties and PGS.

How can blockchain help?

The challenges presented here make this use case 'ripe' for application.

- **Establishing traceability:** Placing information regarding the lifecycle of crops on a blockchain will help improving trust in the self certification process and establishing traceability at the point of sale.
- **Disintermediation of multiple stakeholders:** As highlighted, the process of third party certification is often expensive, and in turn drives up cost of produce, making it harder for farmers to sell. Disintermediation through peer to peer certification mechanisms, or integration of third party certifiers into the PGS process would unlock large markets for produce and reduce cost of production.
- **Programmable transfers:** Much like in supply chain, tracking of products using IoT devices along their value chain can help increase efficiency in transfer of asset between stakeholders, and alert stakeholders immediately of issues.

Energy Trading

India currently faces a dual problem of poor access to energy, and high proportion of fossil fuel mix. As of 2016, only 86.8 percent of the Indian population has access to energy[17]. A recent report also highlights that the central grid (which powers most Indian households) is driven largely by fossil fuels, with this percentage predicted to remain above 50 percent in 2040.

[17] World Bank Group, https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=IN

Current Problems

Renewable energy driven microgrids have been suggested as a possible means of solving the dual issues of poor access and source mix. These would be particularly valuable in areas with no grid connectivity. As the central grid expands, these grids would benefit from the capability to interface with the central grid through mechanisms such as Power Purchase Agreements (PPAs) to help increase renewable energy mix, and allow conscious consumers to choose the energy of their preference.

In today's market, there are different authorities and intermediaries in the process where there is an entity responsible for registering assets, verifying whether they are renewable, measuring their production, and finally creating REC certificates. A lot of buyers are not dealing directly with specific generation assets rather they are going through brokers or intermediaries. There are different authorities that are responsible for reporting and verification and preventing things like double-counting and making sure that once you claim a credit that it is retired and no longer available to be traded or sold or claimed against.

How can blockchain help?

Blockchain may serve as a valuable platform to achieve the proposed targets due to the inherent features it would help deploy. Blockchain may enable a sustainable energy trading system by implementing smart PPAs (Purchase Power Agreements), smart microgrids, REC Certificates Issuance etc. Making energy resources into digital assets that can be traded on a blockchain could open new investing and trading opportunities allowing ease of entry to the new players and fostering innovations. It can also lead to a community-driven change that would solve the problem of last mile access.

Way Forward

Recommendations

The first part of the two-part Strategy document has focused on the application of blockchain to resolve business and governance process inefficiencies. The paper has also highlighted lessons from the pilots and PoCs that NITI Aayog has completed so far. Going forward, NITI Aayog is focused on scaling up some of these pilots, in addition to pursuing selective pilots and PoCs.

The second part of the Strategy, to be released in coming weeks, will focus on recommendations to establish India as a vibrant blockchain ecosystem. The suggested recommendations include:

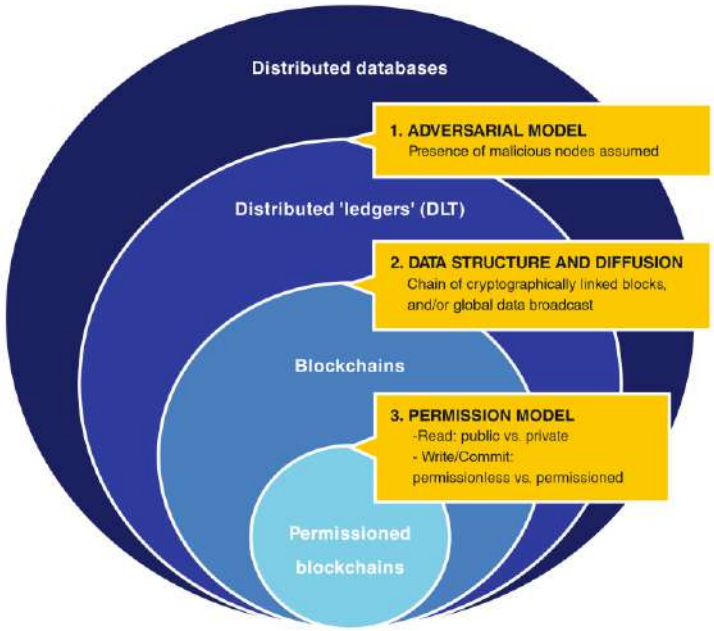
1. Regulatory and policy considerations for evolving a vibrant blockchain ecosystem
2. *IndiaChain*: creation of a national infrastructure for deployment of blockchain solutions with inbuilt fabric, identity platform and incentive platform.
3. *India as blockchain hub*: promotion of research and development in blockchain, in addition to focus on skilling of workforce and students
4. Procurement process for government agencies to adopt blockchain solutions
5. Pegged stable coin for Indian Rupee for seamless exchange for blockchain solutions. This may be in conjunction with the need for re-evaluating cryptocurrencies.
6. *Crypto currencies for India*: Does India need a cryptocurrency / ICO market? What could be the possible contours for facilitation of ICO market in India that assuages all the regulatory concerns?

Appendix I: Blockchain Explained

A techno-functional guide

Blockchain is part of a broader suite of technologies called Distributed Ledger Technologies (DLT). Though often used interchangeably, blockchain technology and distributed ledger technology distinguish themselves in their structures of data storage. Blockchain can be considered a subset of distributed ledger technology in which multiple transactions are stored in 'blocks' and cryptographically linked to the previous block by a 'chain'.

Figure 14: Distributed technologies



Source:
University of Cambridge

Blockchain technology, simply stated is the use of distributed databases to store information about transactions between parties. A defining feature of these databases is that they cannot be altered except without concurrence of a significant fraction of the custodians (and users) of the distributed database. The use of cryptographic functions ensures that transactions can be authenticated as originating from a particular identity and transactions completed without the need for any central authority.

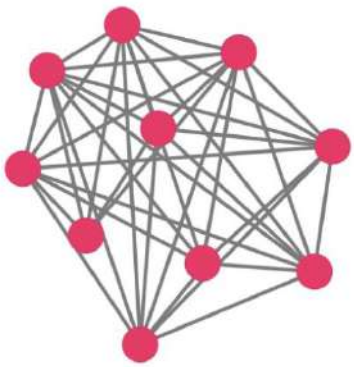
The first use of this technology that emerged in the public consciousness was by the Bitcoin phenomenon. For long the terms ‘blockchain’ and ‘bitcoin’ were used interchangeably without the realisation about the far-reaching impact of this new technology for new models of efficient and transparent governance, especially those involving multiple entities with differing incentives. It was only recently that the tremendous potential presented by this technology has emerged out of the shadows of the Bitcoin revolution and has developed an identity of its own. According to the World

Economic Forum, blockchain technologies are one of the 7 technological forces alongside AI, IoT, etc. with the potential to fundamentally change the way the global economy works.

Common Terms

Consensus Protocols	Computer algorithms that define the modality of how the blockchain based system defines what is the correct updated state of the database. The simplest version of this would be a simple majority amongst nodes.
Cryptography	Method of protecting information and communications through the use of codes so that only the recipient can read it. In computer science, cryptography refers to secure communication techniques based on algorithms which transforms confidential messages (like email, credit card transactions, web browsing) in ways that are hard to decipher by third parties.
Hashes	Mathematical functions that convert data of indeterminate length to a 'fingerprint' of a fixed length. It is astronomically unlikely for two different sets of data to have the same 'hash'.
Merkle Tree	Structure (also used in BitTorrent, Git, Bitcoin and Ethereum) that summarises data of all related transactions in a block by producing a digital fingerprint in the form of a hash (or a transaction ID) for each transaction and thereafter for every pair of transactions until only one unique ID/ hash is left (called the Root Hash/ Merkle Root). The structure is built from the bottom up from hashes/ Transaction IDs of individual transactions and tests whether a specific transaction is included in the block or not. It records transactions in a chronological order and can verify whether the record has been altered or tampered with, or whether the record has been branched or forked
Mining	Refers to the actions nodes take to authenticate transactions. Miners are economically incentivized to spend resources for maintaining the network by a reward of tokens which are generated by the distributed network.
Nodes	Entities a blockchain system that maintain a copy of the most updated state of the blockchain database and participate in the authentication of new changes. However, all nodes may not store a full copy of a blockchain or validate transactions.
Smart Contracts	Represent an if-else construct which enable blockchain based systems to autonomously record a transaction if certain pre-requisites are completed.
Token(s)	Essential components of most public blockchains. They are a unique asset class which not only denote ownership of the network (like shares of a company) but also form the basic unit of value exchange.

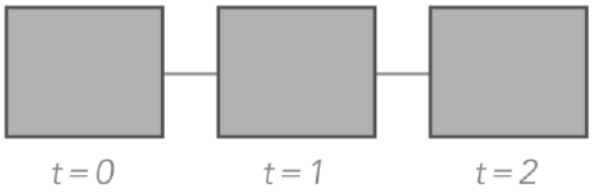
How does blockchain work – a simple explanation



Blockchains are a new type of network infrastructure (a new way to organize how information and value moves around on the internet) that create 'trust' in networks through introducing distributed verifiability, auditability, and consensus.

Blockchains act as a shared database, distributed across vast peer-to-peer networks that have no single point of failure and no single source of truth. No individual entity can own a blockchain network, and no single entity can modify the data stored on it unilaterally without consensus of peers. New data can be added to a blockchain only through agreement between the various nodes of the network, a mechanism known as distributed consensus. Each node of the network keeps its own copy of the blockchain's data and keeps the other nodes honest -- if one node changes its local copy, the other nodes reject it.

Blockchains record information on a timestamped chain that extends forward infinitely. New data is added to the end, and once added, it is permanent. Older data can neither be removed nor modified because a snapshot of it is captured in the blocks of data that come after it.



Blockchains leverage techniques from a field of mathematics and computer science known as cryptography to sign every transaction (e.g. the transfer of assets, like money, from one person to another) with a unique digital signature belonging to the user who initiated the transaction. These signatures are *held privately but are publicly verifiable*.

This means that if a user with identity A sends money to identity B, anybody can verify that the money was sent by A, but cannot use A's signature for their own transactions. This cryptographic system creates accountability while preventing identity fraud: if you send money or update

information on a blockchain, you cannot later claim that you did not or shift the responsibility for the action.

Unlike present day networks which depends on trusted intermediaries for security and trust, blockchains create trust organically through the underlying technology of distributed networks. They allow users to exchange digitized assets directly, in a way that is **incorruptible** (data cannot be changed once added) and **transparent** (all transactions are logged onto the timestamped ledger, with the identity of the person who committed the transaction).

As they effectively reduce the dependency on 'middlemen', blockchains can also **generate savings** by streamlining processes and reducing inefficiencies typically introduced to systems due to multiple layers of control. Gartner estimates that distributed ledgers and blockchains will create USD3.1 trillion in added business value by 2030, driven by fraud prevention, cost savings, and added transparency.

Core features of blockchain

1. *Recordkeeping on a time-stamped, fault-tolerant ledger*:
   At their core, all blockchains make it technically and economically infeasible to modify a record already added to the blockchain.

   Once added, the timestamp of the transaction, the metadata contained within the transaction, and the digital signature of the parties involved in the transaction are recorded on all nodes of the network. These data cannot be modified unless a majority of the nodes in the network collude (a situation that becomes increasingly unlikely and expensive as the network grows).

   Person A transferred 500 Rupees to Person B (timestamp t=1)

   Person B transferred property LAND_XYZ to Person C (timestamp t=2)

   Company ABC transferred domain XYZ.com to Company DEF (timestamp t=3)

   Blockchains inherently maintain an audit trail, and therefore are an ideal choice for recordkeeping of any digitizable asset – money, land, rare collectibles, domain names, etc.

2. *Smart Contracts for decentralized, corruption-proof, self-triggering applications*: So far, we have discussed blockchains as a global, peer-to-peer database, but they can also be extended to act as a global, peer-to-peer computer – one that runs code and applications published by developers in an incorruptible manner.
   Code that is executed on a blockchain network is known as a 'smart contract' for it acts as a legally binding document – once published, the code cannot be tampered or unpublished. More importantly, it can self-trigger blockchain transactions when encoded conditions are met, without allowing any room for corrupt parties to intervene.

   Take for example the following script (encoded as a smart contract):

When Person A Transfers Property XYZ to Organization B,

Transfer Rupees 1 crore from Org B's account to Person A's account

The above contract self-executes when transfers of property (represented as a digital asset on the blockchain) occur between a person and an organization, and auto-transfers funds from the new property owner to the former.

Because both code execution and funds transfer occur on the blockchain, a serverless/decentralized infrastructure, no third party may prevent the transaction or intervene to route funds to itself.

3. *Digitization of assets and new economic models*: A real-world asset can be represented digitally – be it tangible or non-tangible (gold vs. an IP copyright), fungible or non-fungible (money vs. collectible artwork), movable or non-movable (cars vs. land).
   Blockchains are a perfect platform for asset digitization as they allow any asset to be represented as a token that represents either full or partial ownership of the underlying economic resource. Blockchain tokens can be traded in a frictionless manner between parties (without intermediaries), creating liquidity even when the underlying asset is illiquid and opening the door for innovative economic models, e.g. automatic dividends to partial land owners using smart contracts, or automatic payments from asset consumers to asset providers.

   Unlike digital assets and tokens on traditional database systems, tokens implemented on blockchains are cryptographically secured – identity of the token's owner can be verified but not faked or modified. Transfers of these tokens on blockchain systems are incorruptible – double-spending is inherently impossible and middlemen cannot intercept transfers or steal funds.

What are the different types of blockchains?

Blockchain can be categorized into groups differently on the basis of a number of different underlying technological choices. The definition stated above, however, remains largely consistent; as does the potential of the technology to radically improve our existing processes. Some of the technological choices and corresponding groups of the technology have been highlighted below.

- Should transactions be public? Public blockchains and Private blockchains
- Achieving consensus for addition of new information? Different consensus protocols

Private blockchains systems

In a private blockchain system, every single node in the peer-to-peer network is a known entity and is invited to be part of the network and the system administrator is able to determine the read/write scope of each node on the network. E.g. think of a large company that builds a private blockchain for its manufacturing supply chain. Every member of the supply chain will be sanctioned to run a node in this network. Nobody else will be able to do so.

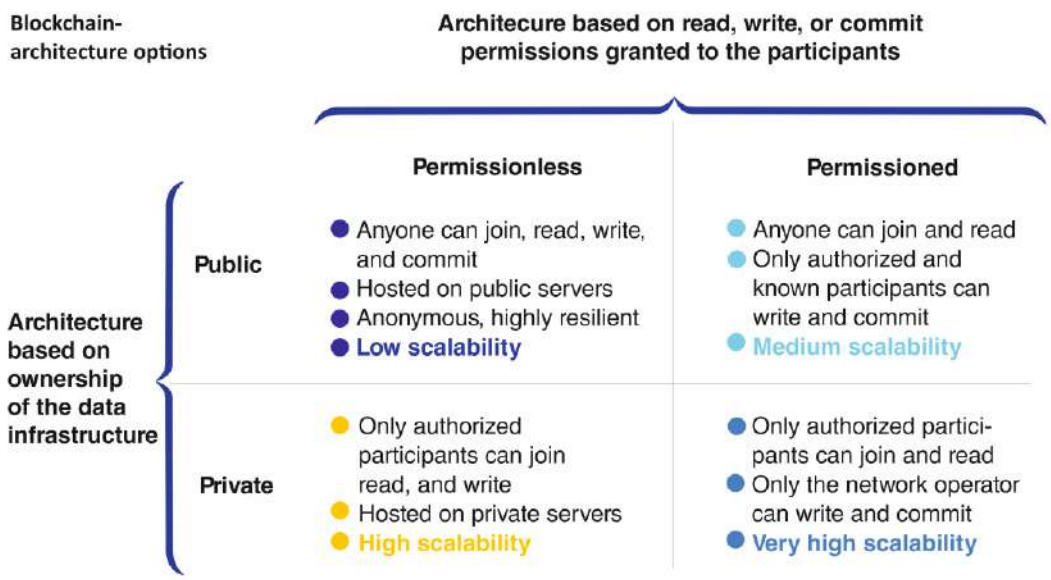
Thus, the parties involved can be considered to recognize (if not trust), requiring a more relaxed mechanism to establish consensus or make modifications to the database. Private blockchain systems like this are permissioned – they provide fine-grained access controls that allow the system administrator to determine the read/write scope of each node on the network.

Public blockchain systems

In a public blockchain system, anybody can join the peer to peer network without needing invitation. All nodes have the same permissions – all of them can read everything from the blockchain network and can submit transactions to the blockchain network.

Unlike private blockchains, where all nodes are assumed to be trustworthy, public blockchains are completely open and can have corrupt or colluding actors that, for example, try to overwrite/delete past transactions, or change a piece of data. To prevent dishonest behavior, public blockchain systems offer economic rewards for honest behavior and economic penalties for bad actors. The nature of how public blockchains scale require them to have a token economy – since it is highly likely that the most promising use cases will come from public blockchains due to a variety of factors, regulatory clarity will be required to enable this important type of blockchain in India.

Figure 15: *Types of blockchain*



Source: McKinsey

Acknowledgement

In its essence, blockchain is a largely collaborative technology – a property driven by its decentralized nature. This paper is no different and the material found here is a result of efforts by a large number and variety of partners. These partners have been listed below.

- For contributions to the overall paper and feedback at regular intervals: Anshul Bhagi and Sinchan Banerjee (Proffer), Nitin Sharma (Incrypt Blockchain), Kartikeya Asthana (ex-NITI Aayog), and Bhagwan Chowdhry (ISB);
- For execution and study of the pilot in land records: The Government of Chandigarh (IT Department), ConsenSys, Sudhir Vohra
- For execution and study of the pilot in pharmaceutical supply chain: Oracle Corporation, Apollo Hospitals, Strides Pharma Sciences, Efftronics, and GS1;
- For execution and study of the pilot in fertilizer subsidy disbursement: Gujarat Narmada Valley Fertilisers & Chemicals (GNFC), Intel, and PwC;
- For execution and study of the pilot in educational certificates: ISB and Bitgram
- Komal Modi, Archit Sinha, Ayush Sharma, and Viplove Bhargava for contribution as part of the ISB Experiential Learning Project.
- Chitmonks and Energy Web Foundation for sharing information on use cases