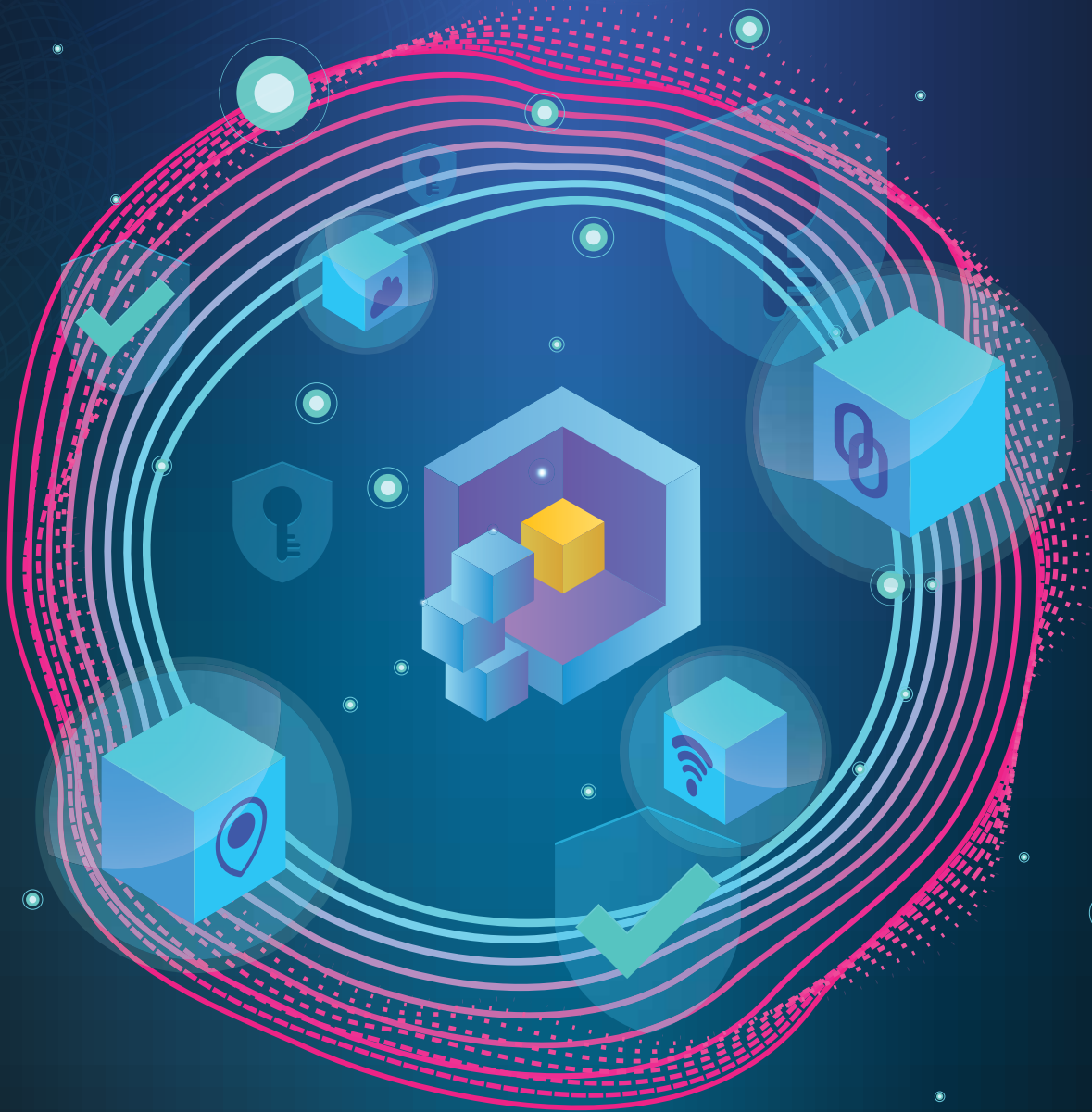




सत्यमेव जयते

BLOCKCHAIN FOR GOVERNMENT

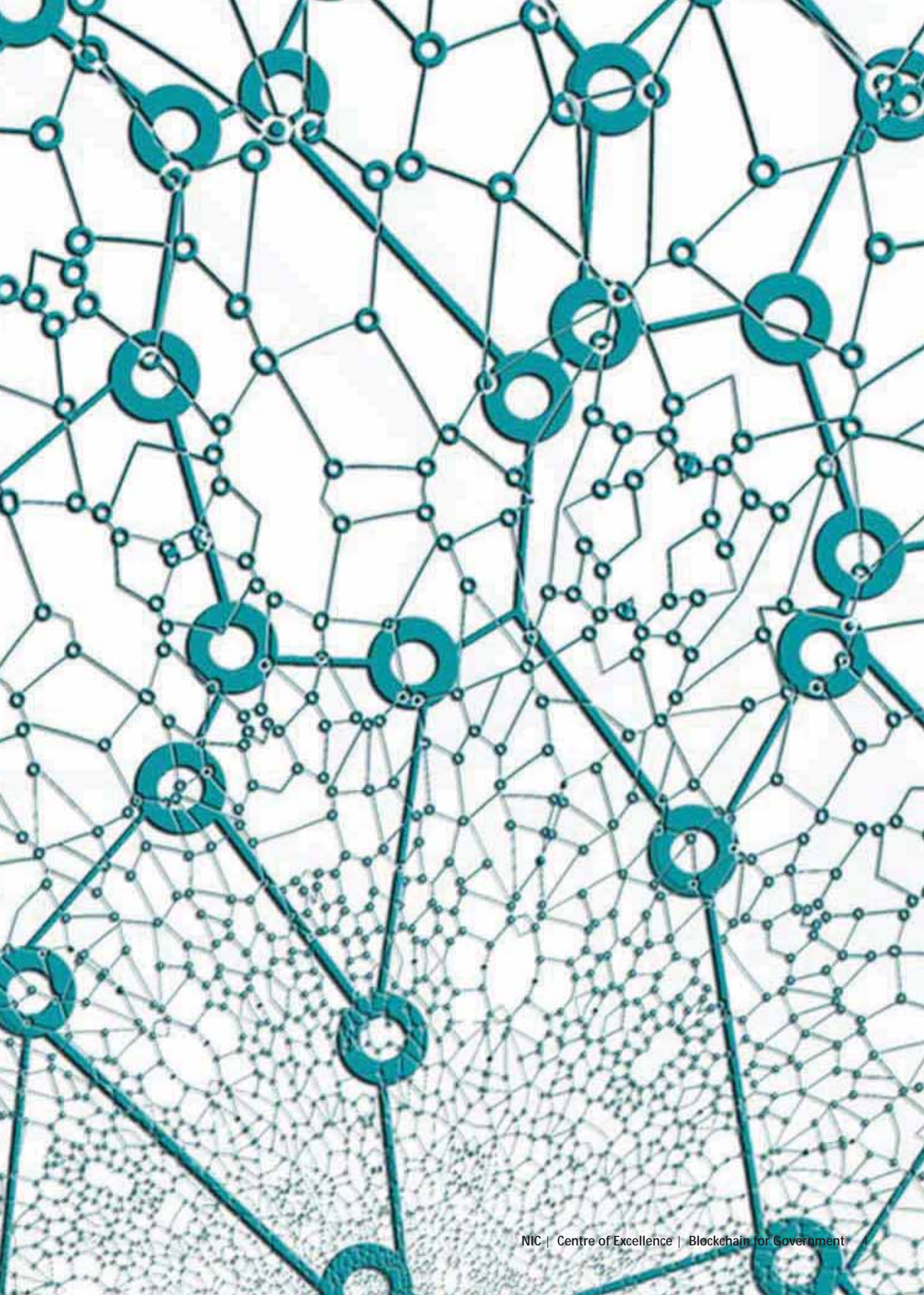


NIC एनआईसी
National
Informatics
Centre

January 2020

Table of Contents

1. BACKGROUND	15
2. WHAT IS BLOCKCHAIN ?	17
3. BLOCKCHAIN USE CASES IN GOVERNMENT	23
3.1. Blood Bank Management System	23
3.2. Public Distribution System	27
3.3. e-Justice System	30
3.4. Urban Property Management System – e-Aasthi	33
3.5. Land Records	36
3.6. State Excise Supply Chain	39
3.7. Aushada- Online Supply Chain Management System for Drugs	42
3.8. Certificate Verification System	45
4. CENTRE OF EXCELLENCE IN BLOCKCHAIN TECHNOLOGY	49



रविशंकर प्रसाद
RAVI SHANKAR PRASAD



मंत्री
विधि एवं न्याय, संचार
एवं
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी
भारत सरकार
MINISTER OF
LAW & JUSTICE, COMMUNICATIONS
AND
ELECTRONICS & INFORMATION, TECHNOLOGY
GOVERNMENT OF INDIA

MESSAGE

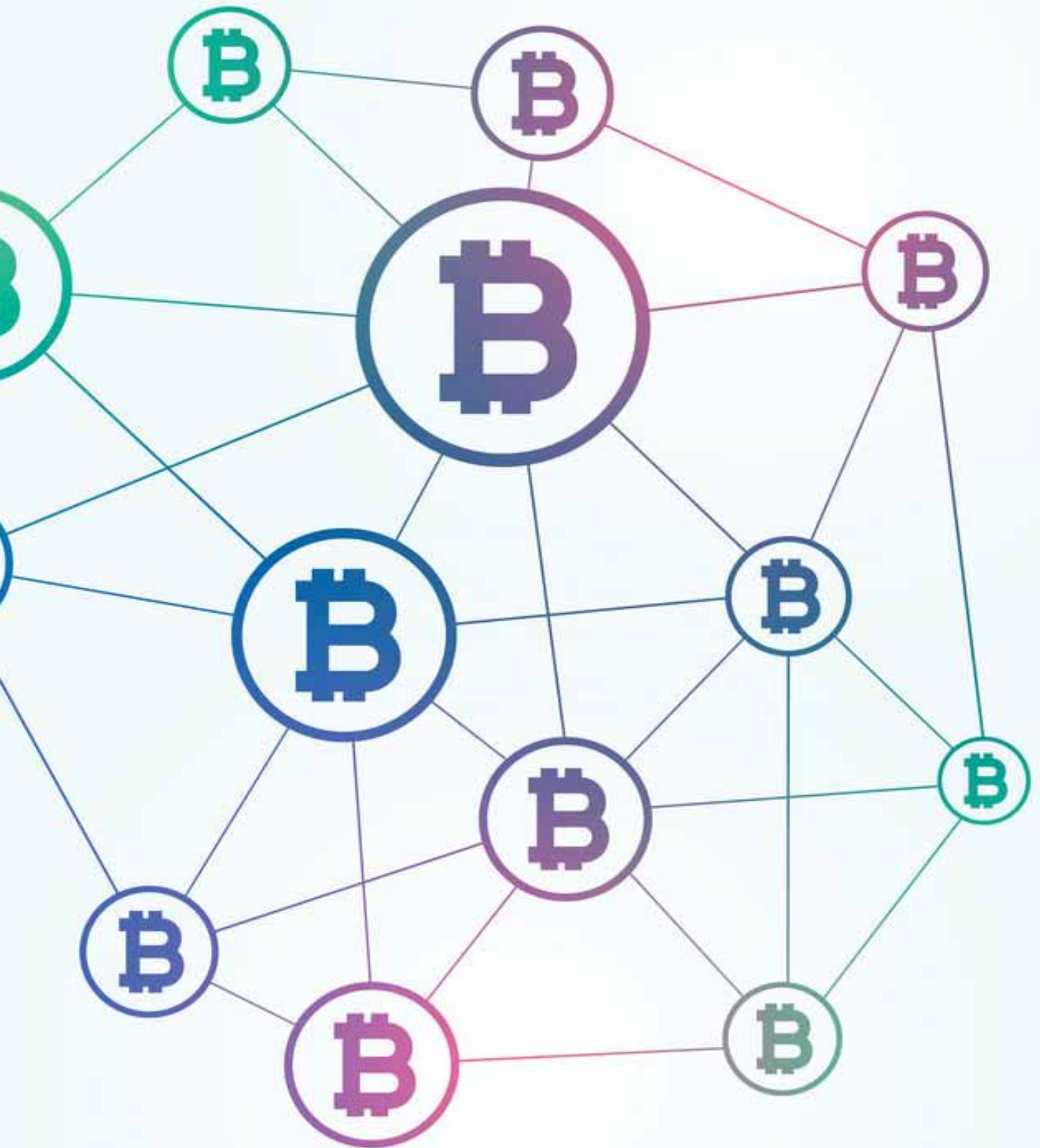
Digital India, a flagship programme of the Government of India, was initiated in 2015 with the vision to transform India into a digitally empowered society and knowledge economy. Digital India aims to leverage innovative technologies that are affordable and developmental to create inclusive growth and empowerment of citizens.

Blockchain as an emerging technology is poised to revolutionise how we perform transactions digitally. This distributed ledger technology allows storage of information securely across multiple systems to enable peer-to-peer transactions in a trustworthy manner.

It gives me immense pleasure to note that National Informatics Centre (NIC) has setup a Centre of Excellence (CoE) in Blockchain Technology' in Bengaluru to facilitate and promote adoption of this technology. The CoE of Blockchain shall be responsible for enabling an ecosystem of Blockchain technology within the country. It will facilitate in building the required capacity for adoption of Blockchain, along with testing viability of the use cases through development of Proof of Concepts. NIC through this CoE, also aims to provide Blockchain as a Service (BaaS) to help Government build, host and use their own Blockchain applications while NIC shall manage the necessary tasks to keep the infrastructure agile.

I convey my best wishes to all the concerned and wish them great success in their endeavour.

(Ravi Shankar Prasad)



संजय धोत्रे
SANJAY DHOTRE



D.O./ MoS (E&IT) 1208/2024

राज्य मंत्री
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी, संचार एवं
मानव संसाधन विकास मंत्रालय
भारत सरकार
Minister of State
Electronics & Information Technology,
Communications and
Human Resource Development
Government of India

MESSAGE

Government of India initiated the Digital India programme with the intention of bringing technology to the door step of the common man. It is also intended to make the most sought services of Government faceless, paperless and contact less. In this endeavour the Government has partnered with technology industry.

While providing service at the doorstep, one should not only ensure timely delivery of service but also the authenticity of information provided. But providing such services involves role of various stakeholders who would verify the information and authenticate/modify the same. There are huge data sets in Government which are being used and updated by various agencies. Ensuring consistency of data and tracking the modifications is a challenge especially when the data is highly volatile.

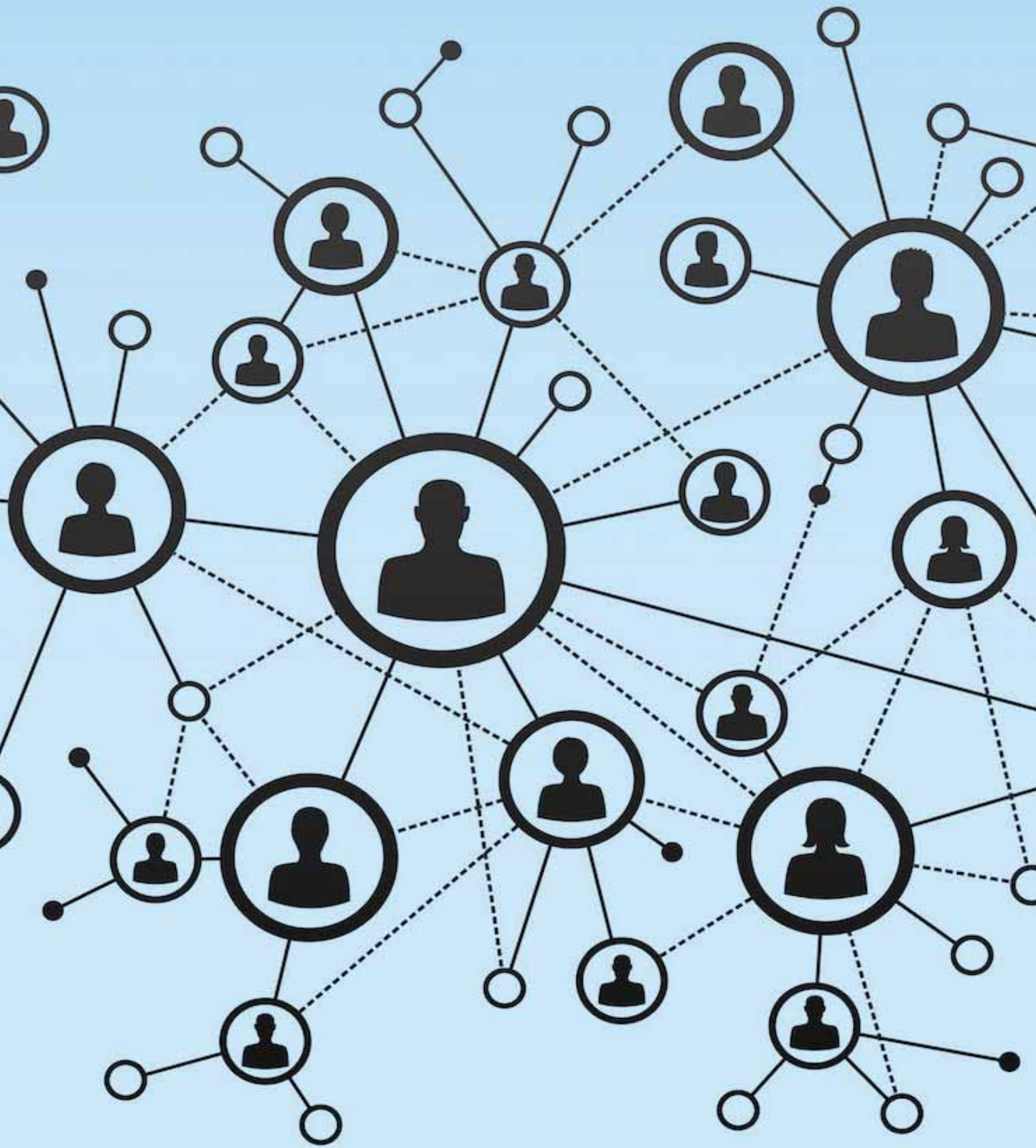
Blockchain technology would provide solution for maintaining such huge data sets and help in ensuring consistency. Government of India has been promoting such technological initiatives.

Setting up of a 'Centre of Excellence in Blockchain Technology' by National Informatics Centre at Bengaluru is a step in that direction. It is an added advantage for the Government that in many important applications, NIC's services have been used. Thus the domain knowledge acquired would come in handy for preparing and evaluating the PoCs before deciding to move the apt use cases to production. Departments could leverage on the services and the infrastructure to develop and deploy applications in the NIC data centres.

I would like to convey my best wishes to all the concerned and wish them great success in their endeavour..

(Shri Sanjay Dhotre)







सत्यमेव जयते

अजय साहनी, आई.ए.एस.
AJAY SAWHNEY, I.A.S.

सचिव
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Secretary
Ministry of Electronics &
Information Technology (MeitY)
Government of India



MESSAGE


Technological advances in the last decade have changed the way we conduct business and simplified our lives by providing on-the-go services thereby enhancing productivity and providing better user experience. The Government Departments in India have spent the last decade in digitizing their processes and enhancing their service delivery.

Yet, a citizen still needs to wait for Government functionaries to verify and approve their request for a service. We must endeavour to build systems that augment their current paperless-faceless-cashless nature to 'paperless-faceless-cashless-intermediary less'. This would be a great leap forward in enhancing service delivery to the citizens and promoting digital inclusion as well as digital trust.

Blockchain technology would provide the necessary impetus to move from demand-based process of service delivery to an eligibility-based system. Immutability of data in the Blockchain and the transparency it provides, would make it possible to provide the necessary trust required to automatically initiate service delivery by executing the smart contracts stored in the Blockchain through a consensus process.

The Ministry of Information Technology, Government of India plans to bring out a National Blockchain Strategy to ensure that a conducive environment is provided for the Government, academia, corporate and start-ups to collaborate on this emerging technology and accelerate its implementation. Capacity building, Research and Development and setting up of incubation centres would be other agenda to facilitate quick adoption of Blockchain technology.

The 'Centre of Excellence (CoE) in Blockchain technology', being set up in Bengaluru, will facilitate the technology enthusiasts to build capacity on Blockchain, implement Blockchain applications and use its infrastructure to host ProofofConcepts. It is envisaged that the CoE would help to bring a revolutionary change in the life of citizens by changing the way e-Governance services are delivered. I am sure that this white paper would act as a reference document for all the Government departments and aid them in accelerating their Blockchain journey.


(Ajay Sawhney)

Place: New Delhi
Dated: 16th January, 2019



डॉ. नीता वर्मा

महानिदेशक

Dr. Neeta Verma

Director General



सत्यमेव जयते

भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
राष्ट्रीय सूचना-विज्ञान केन्द्र
Government of India
Ministry of Electronics & Information Technology
National Informatics Centre



MESSAGE

With the advent of fourth industrial revolution, emerging technologies such as Internet of things (IoT), data analytics, machine learning, robotic process automation, artificial intelligence and blockchain have taken the center stage. These emerging technologies have the potential to change the way we live, work and relate to one another. In recent years, blockchain technology has continuously evolved and is beginning to be deployed in real life applications.

To promote blockchain and its application in the public sector, National Informatics Centre has embarked on its journey by setting up a Centre of Excellence (CoE) in Blockchain Technology at NIC Bengaluru. The CoE has developed blockchain based Proof of Concepts (PoCs) for select government use cases to understand potential benefits provided by this emerging technology. As an initial effort, the CoE has prepared this whitepaper titled 'Blockchain for Government' for highlighting potential use cases of blockchain technology in different sectors of development. As the use of blockchain progresses, we anticipate its new and previously unforeseen applications for the government leading to enhanced transparency, traceability and trust in e-governance systems.

The Centre of Excellence will facilitate the Government departments in building proof of concepts for use of blockchain technology in different dimensions of governance leading to large scale deployment of some such applications. With NIC providing a robust and an agile infrastructure, the CoE shall also provide Blockchain as a service (BaaS) for efficient hosting of Blockchain network.

With the objective of learning and exploring the endless opportunities that blockchain technology has to offer, I am certain that this whitepaper will be of considerable use to readers be it scholars, government professionals, technology enthusiasts and other related stakeholders.

(Dr. Neeta Verma)



Executive Summary

The emergence of Blockchain technology holds promise for the government to foster trust and greater transparency in service delivery. This technology promises to provide tamper-proof storage of key transactions thereby eliminating 'intermediaries of trust'.

In addition to understanding the technology, determination of the right applications of the technology are a critical factor to accelerate its adoption. As in case of mature systems, advocates of government Blockchain solutions must provide strong evidence that such investments will save money and improve service delivery.

Being an emerging technology, the Blockchain ecosystem is quickly evolving to narrow down on key Blockchain based use cases. This whitepaper presents a few realistic use cases for adoption of Blockchain and discusses the benefit provided by adoption of this technology.

The possibilities of Blockchain are limitless; asset management platform, voting systems, tax collection, digital identity etc. may all be revolutionized by this technology. Therefore, it is imperative that such new ideas are tested thoroughly, via specialized Blockchain setups, prior to large scale adoption. Therefore, NIC has set up a Centre of Excellence in Blockchain at Bangalore in India.

NIC envisages to promote the use of Blockchain technologies, facilitate the rapid adaptation and on-boarding of Blockchain based solutions, foster stronger collaboration between the government, academia and private sectors to ensure that the latest technological standards are made available in a safe and trusted manner. Setting up Centre of Excellence (CoE) in Blockchain Technology is an attempt in this direction. The CoE will be instrumental in increasing the adoption of this technology by consulting the Government departments on potential use cases, offering Blockchain as a service for hosting of the application and building capacity within Government. It will also become a channel to engage companies and governments in Blockchain research.

The Blockchain Centre of Excellence will operate as a coordinated, interoperable Blockchain ecosystem around the nation, allowing all partners to benefit from shared learning, experiences and resources.

Nagesh Shastri
Deputy Director General - NIC



1. BACKGROUND

The last decade saw the proliferation of centralised computer system which led to easy deployment of the applications, faster implementation of enhancements, enablement of uniform security policy and its implementation. The advances in communication network, last-mile connectivity, storage capacities etc. have facilitated the adoption of centralised applications. The mobile technology also leveraged this architecture to provide ubiquitous access to services. While this approach provided a plethora of advantages, challenges such as single point of failure, creation of information silos, data-tampering, digital exchange of assets etc. are yet to be addressed. A few of examples of such challenges have been illustrated below:

Information Silos – Digital initiatives in the early 21st century have led to creation of department wise information silos. Such IT systems have no or limited connectivity thereby inhibiting provision of efficient service delivery to the citizen. For example, there is little uniformity in the way centralized databases of all land records are maintained across various departments such as revenue department, registration department etc.

While efforts have been made to eliminate such information silos through integration, the primary objective of these integrations was to obtain the data from the issuing authority to reduce the time for verification and also reduce the work load of the functionaries at the different levels in the Government. In order to facilitate this efficiently, there is a need to provide trust to the functionaries that the data presented to them electronically is indeed not tampered.

Single Point of Failure – Since all critical information of current IT systems is maintained in a centralized manner, they are prone to single point of failure. Such systems are prone to attacks/issues such as compromised database administrators (DBA), unavailability of the system, tampering of existing information etc.

Need for Data Integrity – Several departments that provide benefits to citizens such as scholarships, social security pensions, subsidies etc. verify the authenticity of the claim by the citizens with respect to caste, income, domicile and other selection criteria. They no longer insist on scanned copies / attested copies of certificates but take only the certificate numbers to perform the verification. Under these circumstances, it is extremely important for the document issuing authority to ensure that the documents are tamperproof to instill the trust in the consumers of data.

Facilitate Exchange of Digital Assets – Internet revolutionized the way we exchange information between peers. But in order to facilitate exchange of assets like currency, we establish trust through a number of intermediaries that exist for aggregating and validating information. Centralized systems have not been able to provide a ‘trustable’ system for managing transactions of such assets due to issues such as ‘double spend problems’.

Hailed as one of the most disruptive technologies in decades, Blockchain technology heralds a paradigm shift to manage data without the need of “trusted” intermediate entities.

The objective of this white paper is to list out the use cases of Blockchain in the Government sector and unleash the potential for its implementation in various applications to ensure integrity of data and bring down the cost and time in providing service delivery.





2. WHAT IS BLOCKCHAIN ?

Blockchain is a digital, decentralised (distributed) ledger that keeps a record of all transactions that take place across a peer-to-peer network. It is an interlinked and continuously expanding list of records stored securely across a number of interconnected systems. This makes Blockchain technology **resilient** since the network has **no single point of vulnerability**². This network effect also leads to real-time synchronization of data across all participants thereby deeming such a system a single source of truth for all transactions happening over the network.

Client applications of related businesses can read or append transaction records to the Blockchain. Transaction records submitted to any node are validated and committed to the ledger database on all the nodes of Blockchain network. Committed transactions are immutable because each transaction is linked with its previous block by means of cryptographic hash functions and digital signature values. Consensus algorithms ensure that the submitted transactions are transferred to all nodes and committed on all Blockchain nodes consistently.

As illustrated in Figure 1, Blockchain ecosystem consists of Blockchain client, consensus protocol, Blockchain data structure, Blockchain metadata, Blockchain node, Blockchain network, smart contracts (chaincodes), oracles, public/private key management systems and certificate authorities. In addition, decentralized storage systems, Blockchain security tools, Blockchain audit and analytics frameworks, Blockchain explorers, Blockchain data models, Blockchain interoperability solutions etc. may also be included as part the Blockchain ecosystem. A few of these have been explained below:

Blockchain client is an application that creates transaction message in a prescribed format and submits it to a Blockchain protocol that validates the content and the format and broadcasts the relevant information to the Blockchain node. Blockchain client can communicate / interact with a Blockchain node through an SDK, API, and / or through Smart Contract. Clients / Decentralized Apps can authenticate to a Blockchain Network through Certificate Authorities, Accounts in the Ledger, Time Stamps, Various Tokens etc.

It may be any existing application, which posts transaction message to Blockchain node. Clients are restricted using Public Key Infrastructure (PKI) technology at Blockchain node level.

Blockchain node is a server node that runs Blockchain services, interfaces, clients, web applications etc. responsible for receiving the transaction input. It then computes its state, generates block header, block metadata and block data in addition to broadcasting the block proposal and its state to other Blockchain nodes. As per the design, the node participates in consensus process to commit the block of transaction data to ledger database.

Blockchain network is a distributed network of linked nodes used to read and write transactions into ledger database. Traditional systems are centralized where all data and decision-making is concentrated on a single node or cluster of nodes. In decentralized systems, the data and decision-making are spread out among a large number of nodes.

² <https://digitalindia.gov.in/content/vision-and-vision-areas>

These nodes maintain copies of the shared database and decide between themselves which data is to be committed to the database using consensus mechanism. Decentralized networks can be an interconnection of centralized or hub-and-spoke type networks. A distributed network is a special case of decentralized system where every single node in the network maintains the shared database and participates in consensus to determine which data is to be committed to the database.

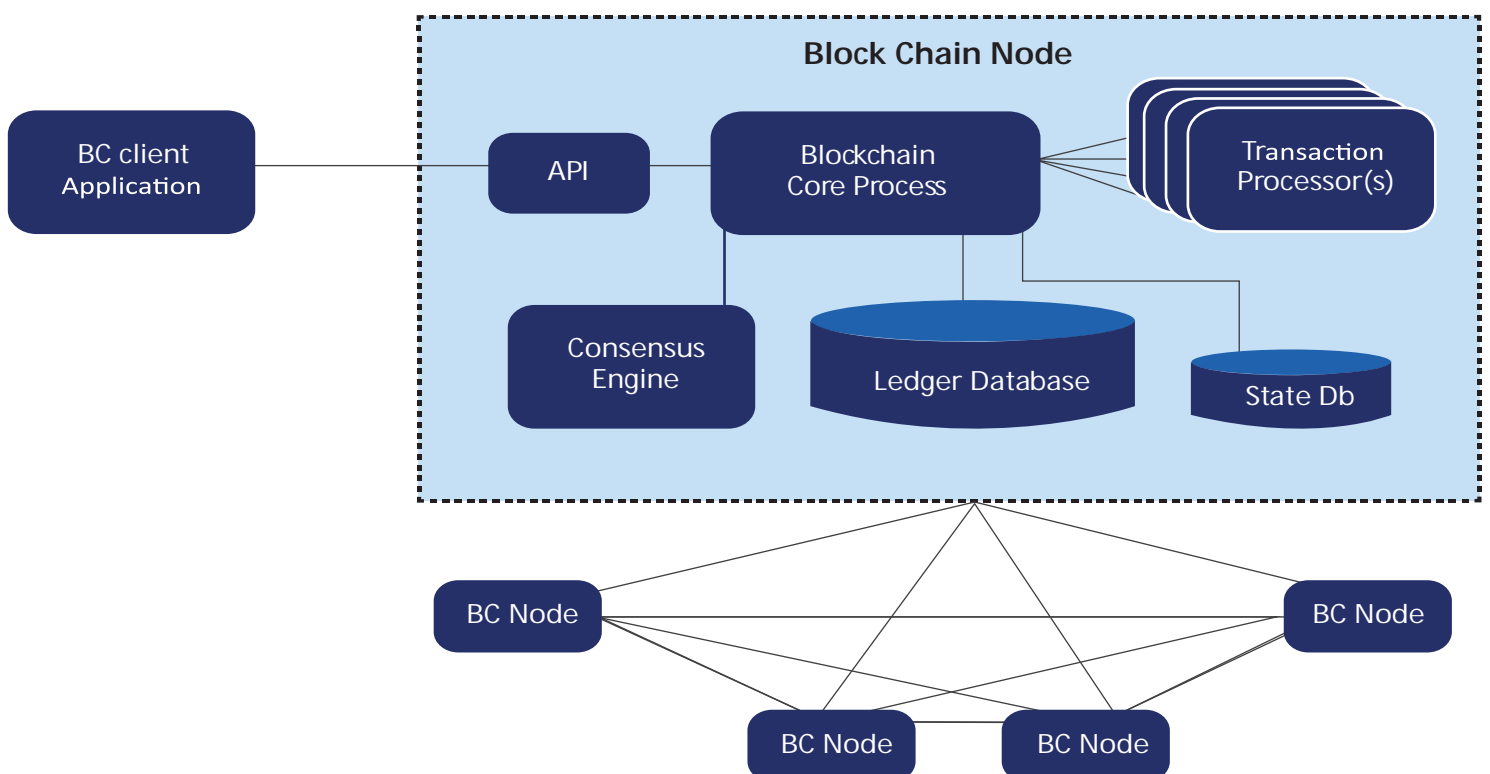
Transaction is a unit of business data. Block is a set of transactions, transaction metadata, timestamps bundled with signatures and hash value of previous block. Genesis block is the first block of chain created during installation and configuration.

Ledger/ Chain Database is a key-value database for a chain of serialized blocks. One block may contain one or more transactions. Key value database is a specific implementation done in the Hyperledger Fabric distributed ledger platform.

State Database is a key-value database for storing transaction state and links of its related transactions. Each Blockchain platform implements their own data structure and data model for the state database. **Transaction Processor/ Chain Code/ Smart Contract / Persistent Queries** run on Blockchain nodes for processing the transaction data and maintaining the status in ledger database. During the process, it can call or execute other business process tasks transparently before committing the transaction. Business rules are coded and executed through these Transaction Processor/ Chain Code/ Smart Contract / Persistent Queries before a transaction is committed.

Consensus Algorithm / Consensus Protocols Consensus Algorithms are a foundational property of distributed computing systems. Consensus algorithms enable distributed computing systems to communicate and compute information within the network in a fault tolerant manner. In a nutshell, it is a computational process used to achieve agreement on a single value among distributed systems. Such algorithms are generally designed to achieve stability, scalability and reliability in a network involving multiple nodes.

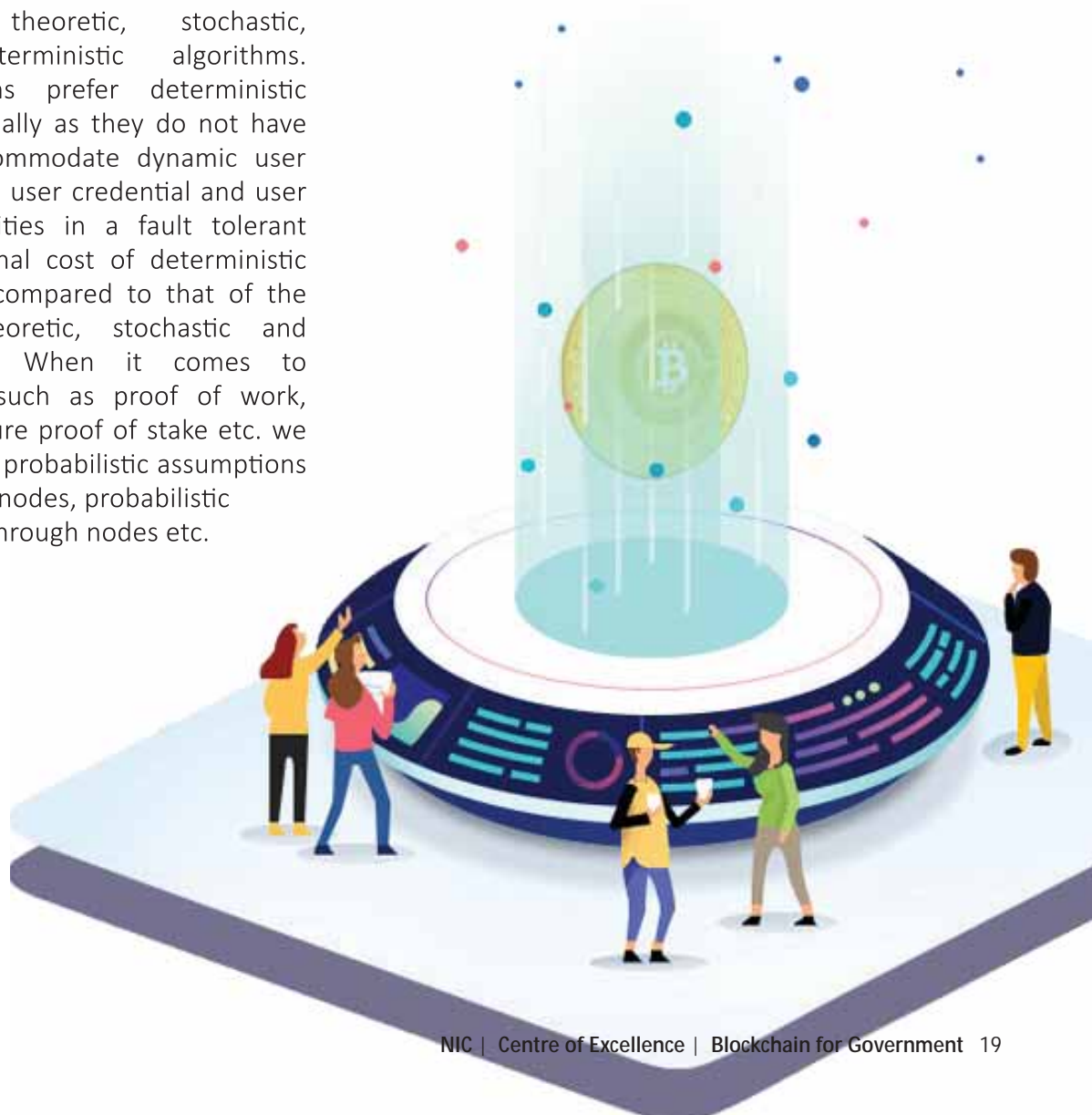
Figure 1 – Blockchain ecosystem



Blockchain networks can be categorized into Public, Private and Consortium as described in the table below:

Model	Description
Public Blockchain	<p>A public Blockchain operates in a decentralised open environment where there are no restrictions on the number of people joining the network (as peers or validators).</p> <p>Bitcoin and Ethereum are examples of public Blockchain.</p>
Private Blockchain	<p>A private Blockchain is a network with a single controlling entity, who has the power to determine who the participating entities in the network would be and their rights to append information to the ledger.</p>
Consortium Blockchain	<p>A consortium Blockchain operates in an environment where the rights to control who participates and what can be transcribed to the ledger is determined by a collection of known entities.</p>

Consensus algorithms can be classified into probabilistic, game theoretic, stochastic, randomized and deterministic algorithms. Permissioned Blockchains prefer deterministic consensus algorithms usually as they do not have the requirement to accommodate dynamic user onboarding, user security, user credential and user state management activities in a fault tolerant manner. The computational cost of deterministic algorithms is quite less compared to that of the probabilistic, game theoretic, stochastic and randomized algorithms. When it comes to probabilistic algorithms such as proof of work, delayed proof of work, pure proof of stake etc. we can see the application of probabilistic assumptions on the honest majority of nodes, probabilistic distribution of messages through nodes etc.





Prevalent Consensus Protocols

Proof of Work (PoW) – Earlier versions of Blockchain system such as Bitcoin, Ethereum, Litecoin, etc. used Proof of Work (PoW) for consensus process. Every validator node or participatory node is given a mining task, and a node that completes the mining task is selected for proposing a new block. Mining task is to find or calculate a certain pattern value of hash value by adding a random number called “nonce” to current hash. Node that participates in mining process requires heavy computing resources.

Proof of Stake (PoS) – In PoS the participant nodes are given block producing privileges based on their stake in the overall value distribution. Proof of Stake represents a class of consensus algorithms in which validators vote on the next block, and weight of the vote depends up on the size of its stake.

Proof of Authority (PoA): PoA is similar to Proof of Stake, where the stake and weight of vote depends on participant identity.

Practical Byzantine Fault Tolerance (PBFT) – PBFT is a state machine replication algorithm that tolerates Byzantine faults. The algorithm offers both liveness and safety provided at most $(n-1)/3$ out of a total of n replicas are simultaneous faulty.

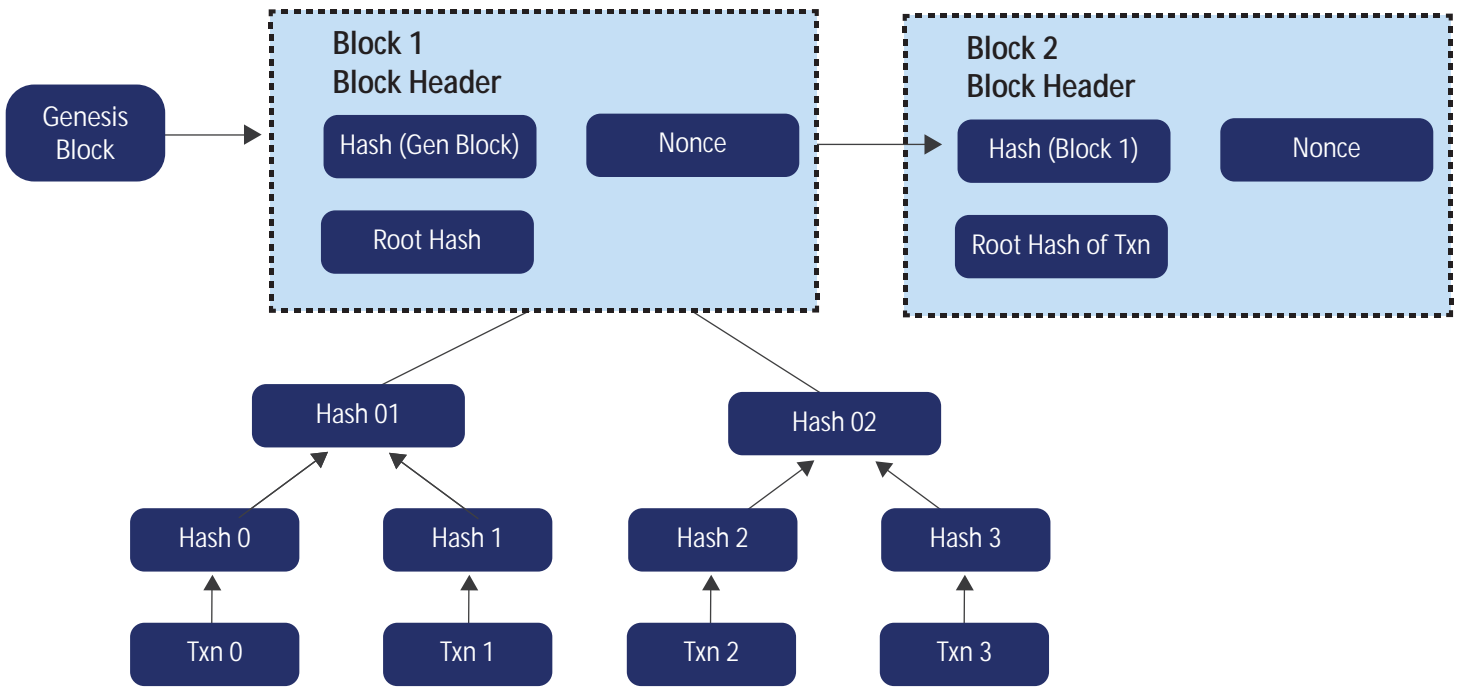
Proof of Elapsed Time (PoET) – in PoET, every node in the consensus process selects random time and keeps decreasing. The node that reaches zero first is selected as leader.

Few other prevalent consensus protocols include Delegated Proof of Stake, Delayed Proof of Work, Asynchronous Byzantine Fault Tolerance, Tangle etc.

We can see the application of randomness in algorithms such as proof of elapsed time Consensus algorithms such as delegated proof of stake are the combination of game theoretic models and economic models.

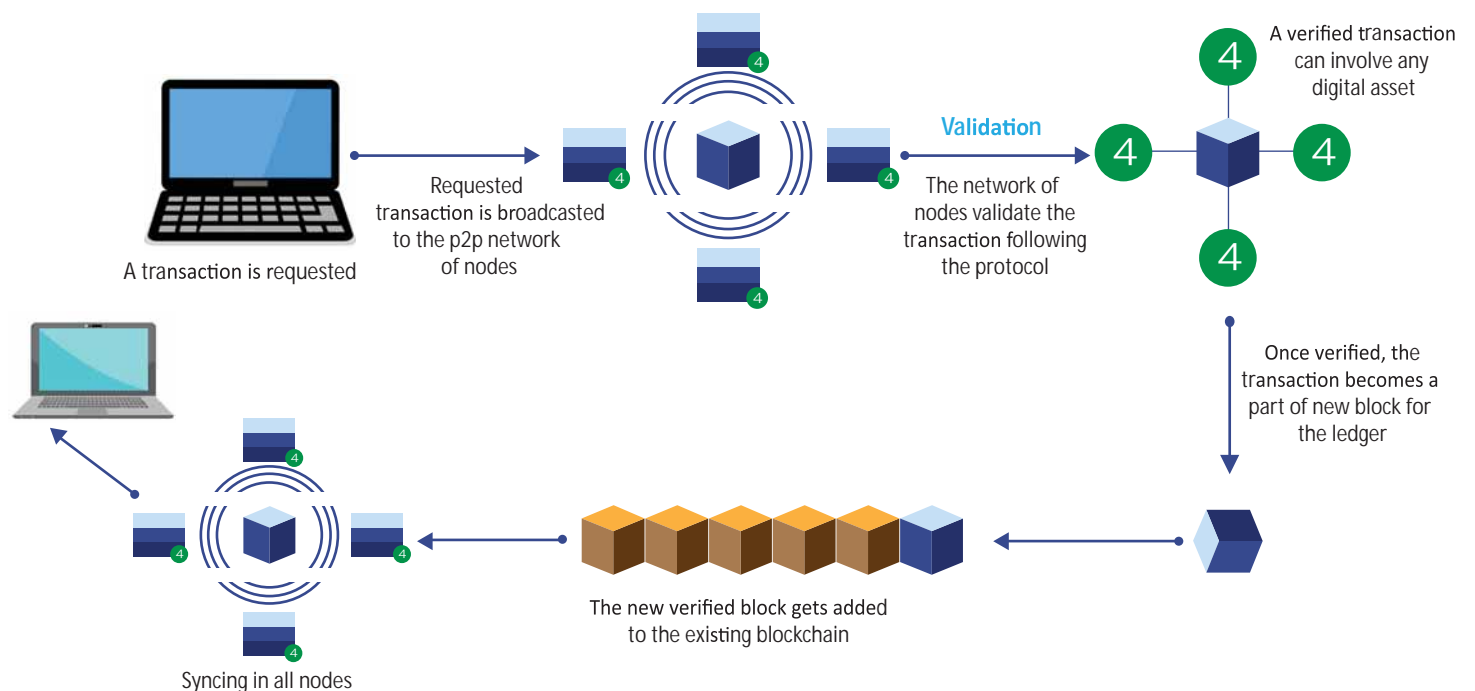
Merkle Tree is a tree data structure (as shown in Figure 2) in which leaf node holds hashes of every transaction and intermediate node holds hash calculated from immediate child nodes. In Blockchain, a block consists of one or more transactions and its respective tree of hashes. In a distributed system, this tree is used to maintain data consistency among all participating nodes.

Figure 2 – Blockchain transactions hashed in Merkle Tree



The below diagram illustrates a Blockchain network and process of consensus to commit a transaction into the Blockchain ledger.

Figure 3 – Blockchain network and process of consensus





3. BLOCKCHAIN USE CASES IN GOVERNMENT

The Government, both at central and state level, caters to a plethora of citizen and business centric services. While Blockchain finds its usability in almost all fields, there are certain use cases which are best-suited and derive maximum value from the inherent features of Blockchain. Some of these use cases are identity management, workflow management, supply chain management, verification etc. Many of these use cases have been successfully implemented on pilot basis and some are envisaged to be piloted in the near future. A few such cases are highlighted below:

- Blood Bank Management System
- Public Distribution System
- e-Judiciary
- Urban Property Management System – e-Aasthi
- Land Record Management System
- State Excise Supply Chain-e-Abgari
- Online Supply Chain Management System for Drugs Certificates verification system – Aushada

Each of these use cases is described in detail in the subsequent section, highlighting the challenges in current system and the value addition brought in by the Blockchain solution.

3.1. BLOOD BANK MANAGEMENT SYSTEM

Safe supply of blood and blood components is essential to enable a wide range of critical care procedures to be carried out in hospitals. Any transfusion of contaminated blood may lead to severe health complications for the blood recipient.

The Blood Bank Management System (BBMS) is developed to facilitate workflow management at blood banks. A blood bank carries multiple critical tasks such as donor record management, test result management, component management, crossmatching, blood issue, billing and inventory management. BBMS is a solution to manage all of the above-mentioned activities.

In India, established supplies are limited and donors usually donate blood only when family or friends require transfusion. Many donors donate blood as an act of charity, some donors are professionals, and in some cases there are incentives other than money such as paid time-off from work. According to a recent survey conducted by World Health Organization, 52.42% of all blood donated in India is through voluntary blood donation camps.



The figure was 45% in 2002. This shows that nearly 47.58% of all blood donated is either from paid donors or from family members.

Blood drawn from a donor, is tested, processed and stored for future transfusions. Donation may be done of blood as a whole, or only specific components such as platelets. Blood banks often participate in the collection process, as well as the post-blood-collection procedures.

Potential donors are evaluated for all conditions which might pose a threat either to the receiver or the donor. The screening process includes the following activities:

- Testing for diseases that can be transmitted by blood transfusion (E.g. HIV and viral hepatitis)
- Understanding donor’s medical history and performing a short physical examination to ensure the donation is not hazardous to his or her health
- Ensuring adequate time-gap between subsequent donations (It differs based on the component donated and the laws of the country where the donation takes place. In general, male donors must wait 3 months and female donors must wait 4 months before they can donate again)

Once the donor is found to be eligible for blood donation, the process of blood collection is initiated. All the activities involved in the end-to-end process, starting from blood collection to blood transfusion, are depicted in the process flow below:

Figure 4 – From Donor to Patient



Challenges

1. Transfusion of unsafe blood caused by human errors

Every unit of donated blood should ideally go through a thorough testing phase, where unsafe blood is identified and eliminated from the cycle. However, sometimes, due to human errors, unsafe blood can also penetrate this test and eventually be transmitted to a patient. When this problem goes undetected, consequences could be fatal.

2. Ineffective management of supply and demand

Another challenge in blood cycle management is effective mapping of demand and supply. On one hand 30% of the patients don’t get the components which they need, on the other hand 10-12% of the components go wasted due to expiry. This is a serious loss, as blood is a precious resource and the lack of it can cause several fatalities.

3. Unavailability of donor’s medical history

The medical history of the donor is crucial to ensure that the blood can be safely transfused. But, in most of the cases, it is not available in the donor database. In some cases, professional donors may intentionally or unintentionally hide certain details as well. Blood donors found reactive during their previous donation at a particular blood bank, end up donating again at multiple other blood donation camps. Also, many quarantined donors end up donating blood, which could lead to terrible consequences.

4. Lack of transparency and traceability

Donors hesitate to participate in the donation of blood due to the lack of trust and transparency in the system on how their donation is used. The patients and hospitals rely on the blood banks to ensure the quality of blood as it is not possible for them to conclusively trace the source of the blood and its be sure of its safety.

5. High operational costs due to excessive human intervention

Recruiting and retaining professionals is a challenge due to high attrition rate. While the Blood Bank Management System will address these challenges to some extent, the system is highly dependent on the stakeholders in maintaining up-to-date data, and there is no way of verifying the authenticity of data shared by stakeholders in the blood supply chain.



Proposed Blockchain Solution

In order to adequately address all these challenges and maintain a tamper-proof repository of blood, a Blockchain solution called 'Blood-chain system' is proposed. Blood-chain facilitates integration with the blood bank application to record transactions in the chain including donor registration, sample collection, testing, storage, blood requisition and transfusion. At each stage in the life cycle, certain details get added to the chain. To achieve this, different stakeholders in the chain should verify the quality of blood from the Blockchain ledger, while the network inherently provides the required trust factor.

Personal Identity Information & test results would be stored in an encrypted form and would be made available only to authorised users and not disclosed inadvertently. In the proposed system, there would be advance Blockchain privacy features like Zero Knowledge Proofs³ that can generate proofs of health for personal identity information and test results without disclosing any of the confidential data fields.

The proposed system connects all the key stakeholders involved in blood supply management – donor, test centre, blood bank and hospital. An overview of the envisaged Blockchain network is depicted in the Figure 5.

Each of the major steps shown in figure above are described as follows:

Donor Registration – Every donor would be registered on the system post which his/her details such as Name, Address, Age etc. are stored on the ledger. Donor privacy and confidentiality is ensured using techniques such as zero knowledge proofs and smart contract obfuscation techniques⁴.

Sample collection – At the time of sample collection, desired pre-conditions can be verified by requisitioning data from the Blockchain. This could include details such as the last time the donor donated blood, result of the sample tested earlier etc.

As part of subsequent phases, it is also proposed to integrate with e-Hospital system which would facilitate in fetching the medical history of the prospective donor. This information would help in determining the eligibility of the donor.

Testing – The authenticity of the sample can be verified by comparing the sample details with the previous details stored on the ledger. This could be automated using verifiable log data structures-based implementation of smart contracts in the Blockchain. The test results are also stored in the ledger to ensure traceability.

Blood bank – To ensure that no untested / unsafe blood is received, blood bank personnel are required to verify test results before storing the blood. The bag will be affixed with a QR code generated by the system, for clear identification.

Hospitals / Patient – A mobile application / web application will be designed to help the patient ascertain details of the test result, blood quality, expiry date etc. By scanning the barcode in the blood bag, the system can retrieve the details and facilitate the patient / care taker in decision making.

The requisition for blood from the blood bank and its usage for the patient should be recorded by the hospital on the ledger. This system will also be programmed to ensure that multiple requests for the same patient are not encouraged.

Envisaged Benefits

The advantages of Blockchain would be:

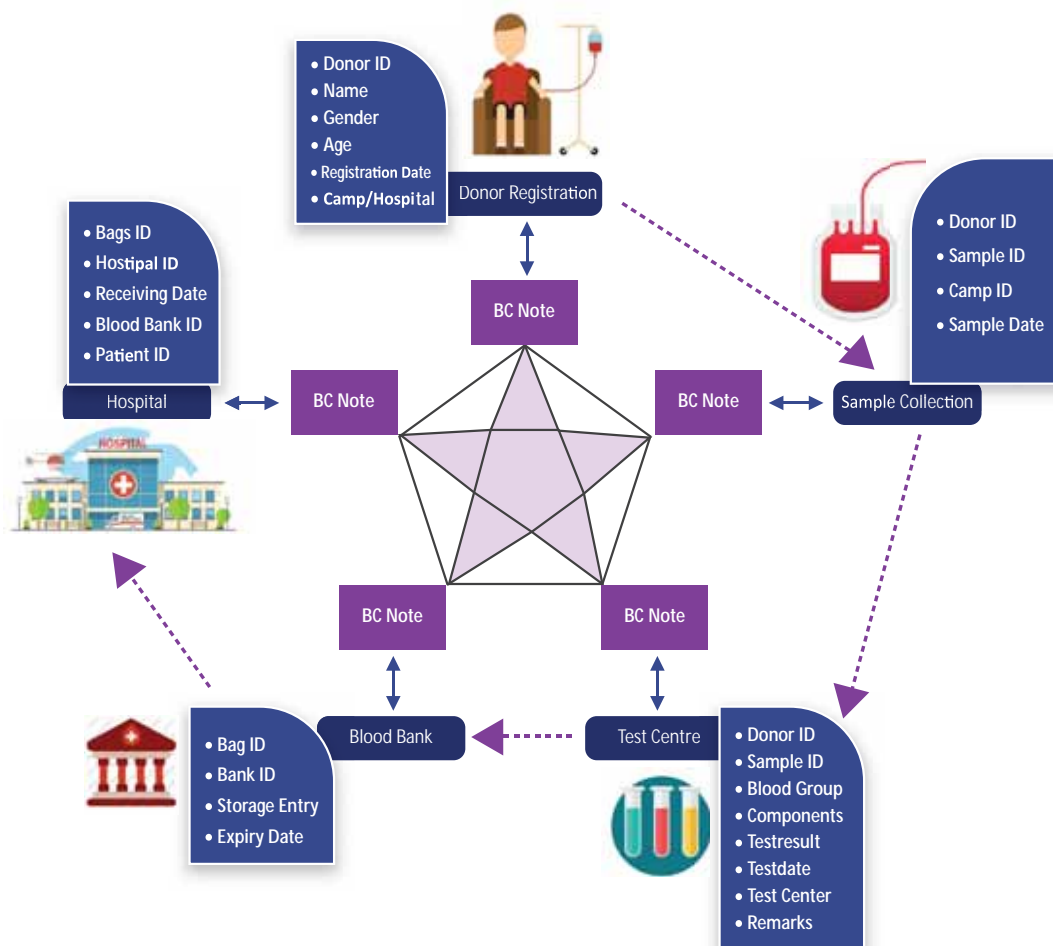
Quality and availability of blood is visible to all stakeholders

The system will also facilitate them to get the availability of blood and its components. The mobile / web application should onboard the right set of stakeholders and users as participants in the Blockchain network.

³ Zero Knowledge Proof is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

⁴ Smart Contract Obfuscation – <https://blog.ethereum.org/2016/01/15/privacy-on-the-Blockchain/>, <https://medium.com/talo-protocol/how-to-secure-sensitive-data-on-an-ethereum-smart-contract-77f21c2b49f5>

Figure 5 – Blood chain: Ensuring safe blood to the patient



Donor history can be tracked and verified

Using a unique identification of the donor, blood bank / donation camp organizers can view the medical history and blood donation history of the donor.

Traceability of blood from donor to recipient

Using Blockchain, it would be possible to trace and track the lifecycle every unit of blood. Lifecycle of the blood bag contains the physical and digital data from the lifecycle of patient data collection, blood collection and blood data analysis.

The system is fool-proof as it is entered into Blockchain only after it is validated by smart contracts. This ensures data integrity and immutability across the value chain.

Elimination of blood wastage due to mismanagement

The portal is provisioned to trigger periodic alerts in case a certain blood sample is close to expire. The ledger would also be useful in mapping supply and demand as real-time information regarding blood availability can be viewed by hospitals and patients online.

3.2. PUBLIC DISTRIBUTION SYSTEM

Public Distribution System (PDS) evolved as a system for distribution of food grains at affordable prices. The government provides subsidized food grains to almost two-thirds of the total population which is below poverty line. Farmer cultivates food grains which is then procured by the government through millers and procurement centers.

The following steps are involved in food grain distribution:

Step 1 – Millers register themselves with the Government

Step 2 – Registered millers collect food grains from the farmers. A farmer gets paid under Minimum Support Price (MSP) fixed by the Government for the quantity supplied to the miller / procurement center

Step 3 – These millers then hull the grains to be deposited with the Government.

Step 4 – These grains are moved to state godowns or warehouses. Millers get paid for processing these commodities and transporting them to the nearest state godowns.

Step 5 – Grains are then distributed to Fair-Price Shops (FPS), schools, colleges, charitable institutions for distribution to beneficiaries

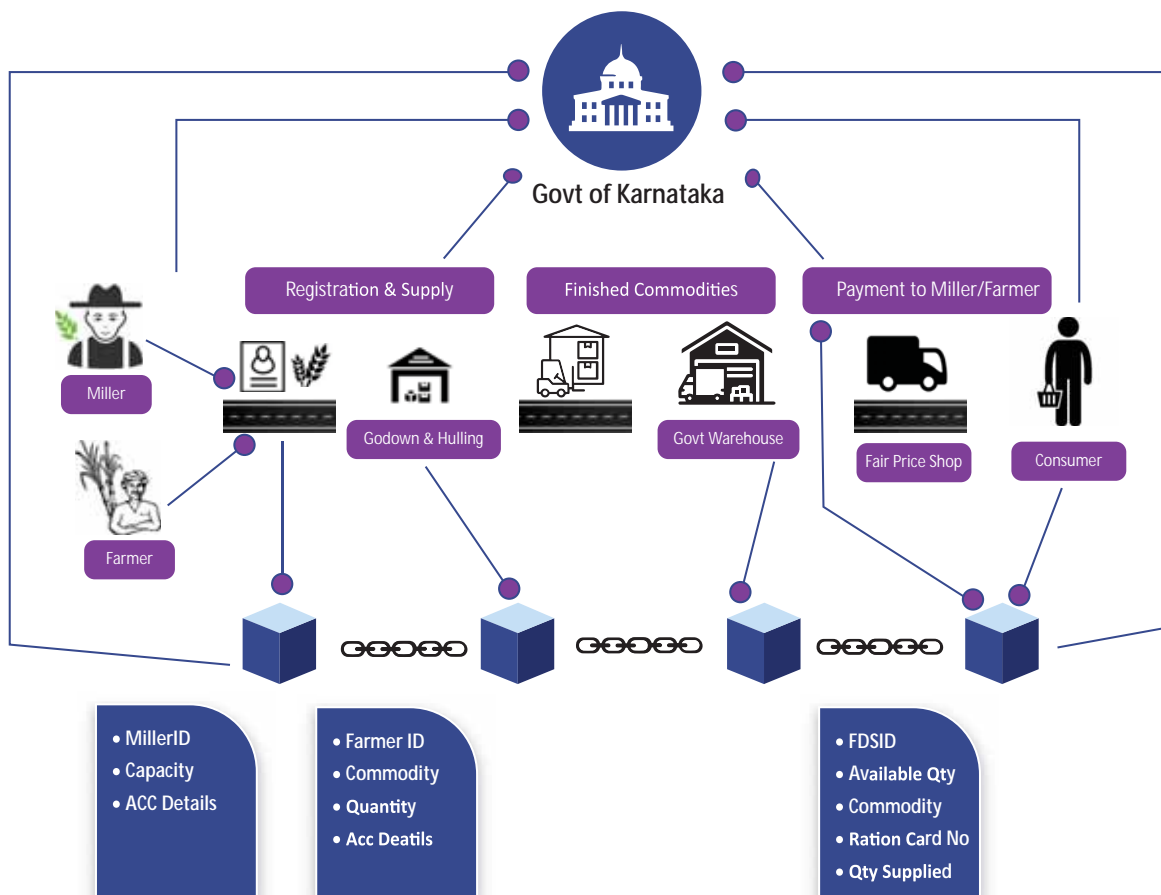
Challenges

PDS is a complex system and has a unique set of challenges. Some of the major challenges are listed below:

1. Unpredictable supply

Production of food grains is a seasonal activity and the quantity of produce is relatively uncertain due to various natural factors such as unfavourable weather, water availability, crop diseases etc. Meeting demand adequately with this kind of unpredictable supply is a major challenge.

Figure 6 – Food Chain: Ensuring timely payment to the farmer, miller & tracking supply



2. Wastage due to logistic issues

A large portion of grains are lost due to issues during storage and transportation. High pilferage is also caused due to delay in collecting grains from warehouses.

3. Administrative obstacles

Some of the administrative inefficiencies and loopholes that affect PDS system are as follows:

- Inability to obtain ration cards
- Irregular opening of the FPS
- Frequent stock-out situations
- Distribution of inferior quality of food grains
- Non-awareness of their entitlement
- Circulation of ghost cards
- Non-existence of grievance-redressal channel

Proposed System

The objective of using Blockchain technology in PDS is to track food grains and record all key data throughout the supply chain. The important data stored would include price, MSP, quantity delivered at each stage etc.

A fool-proof end-to-end PDS system will enable quick payments to the farmer for the supply of the commodity to miller, payments to the miller for hulling and transporting the grains. The implementation will also facilitate the identification of key data points such as leakages, the availability of stock in different godowns along with the time stamping based date of receipt in the store. This will enable effective utilization of grains and reduction of wastage due to rotting. There is a need to uniquely identify the bags of grains in the entire supply chain using the QR code or the RFID tags and the quantity and quality of grains as a transaction metadata. Unless this is done, it would not be possible to provide effective solution to address the challenges faced by the PDS.

The supply chain application presently being used by the Government will be integrated with the Blockchain system developed for the PDS. At appropriate levels in the supply chain, relevant data will be stored in the chain. Business logic implemented through smart contracts will facilitate different agencies to streamline and secure payments to farmers and millers. It will also help in tracking and tracing the movement of stocks through the supply chain. It will also facilitate the identification of inefficiencies and inaccuracies in the supply chain quickly.

The different stake holders in the PDS chain are the millers, the farmers, the warehouses, the beneficiaries and Government. At each stage, it is proposed that the new Blockchain enabled system will store the following details:

Miller / Procurement centre

The miller will register with the Food and Civil Supplies Corporation / identified agencies. On approval by the officer, a miller ID will be generated and the details of the mill such as the mill name, storage, hulling capacity and the details of the PBG/EMD – namely, Date of the PBG/EMD, the validity and amount will be stored on the Blockchain ledger.

Farmer

Farmers register with the miller and then supply commodity during procurement period. When the commodity is collected in the mill, the present storage available and the quantity supplied by the same farmer for the same procurement period is retrieved from the ledger to ensure that there is sufficient storage and whether the farmer is eligible to supply the quantity he intends to supply. Blockchain will enable the PDS consortium to capture the collective information about the farmer registration process through various smart contracts. These checks will be part of the validation process in Blockchain. The weigh scale data is proposed to be digitally captured and stored in the ledger along with the farmer registration details.



Whenever, the miller sends commodities to the storage facility, the available storage capacity in the mill will be automatically updated by smart contracts. This will be implemented by collecting commodity information in the Blockchain ledger with digital and physical details of the commodity and amending the storage capacity of the mill through a collective decision making by executing relevant consensus algorithm.

Storage facility

The miller will hull the commodity and then send the same to the designated storage facility. At each storage facility, the current stock will get updated when the stock is taken in. When the commodity is picked by the FPS, the changes in the status of stock will be updated appropriately.

Definition of contract

For every procurement season, the details as required for payment to the farmer, miller etc. need to be captured. The MSP for the commodities, the procurement period and other variable parameters should be coded in the smart contracts.

Payment

On the last date of the procurement period, the smart contract as defined in the Blockchain will get executed and generate payment-slip for all the farmers, millers etc. and transfer the money to their bank accounts respectively. There are various approaches to scheduling smart contracts using hash time lock contracts⁵, hash time lock agreements⁶ etc. Automatic alerts can be sent to the officials regarding the quantity of grains that are lying in the godowns beyond a certain period.

Benefits

Prompt payment to Farmers and Millers

Use of Blockchain can reduce the delay in payment to the farmers based on procurement done by the miller. On receipt of the commodity by miller, it would be possible to trigger the generation of bill and initiate payment through Direct Benefit Transfer (DBT) system. Similarly, payment to the miller can also be initiated on receipt of commodity at the warehouse. Since the procurement season is defined for each commodity, payment can start immediately without waiting for the other activities to be completed in the supply chain.

Tracking stock at different locations

The tracking of the bags of grains can be done accurately as the data cannot be tampered. The officials will get a holistic view of the available stock, demand and take decision to procure from Food Corporation of India to cater to the need of all the beneficiaries accordingly. Based on the availability of goods and the demand, the system can provide inputs for effective utilization. The transport of food grains from surplus locations to deficit locations can also be done through this centralized system.

Identification of pilferages

Since data pertaining to the quantity of commodities moved from one location to the other is maintained in an immutable form, it would be possible to easily detect leakages. Alerts can be triggered to inform the relevant stakeholders about leakages, if any.

Hyperledger sawtooth framework is used to implement the PoC.

⁵Hash time lock contracts are a class of payments that uses hash locks and time locks that mandates timely acknowledgements

⁶Hash time lock agreements are a generalization of hash time lock contracts that can be implemented over any type of ledgers.

3.3. e-JUSTICE SYSTEM

Indian democracy is held up by three pillars – the executive, the legislature and the judiciary. These pillars are complementary to one another. As per the Constitution of India, the judiciary is the most independent out of the three and is given a wide range of powers so that it is capable of offering free and fair justice. The 3095 court complexes with 6702 establishments in the district and Tehsils of India provide facility to the aggrieved citizens to knock the door of justice. However, several external factors come as hindrances to speedy disposal of cases.

The Indian Judicial system comprises of the Supreme Court, High Courts, District and Tehsil courts. The Indian Judiciary has been one of the early adopters of ICT. The e-Courts system has facilitated all the courts in India to record case details, facilitate easy creation of documents such as summons, maintain a ledger of the certified copy requests and a ledger for judicial deposits made by the party. The judgments are digitally signed and stored in a repository. The use of ICT in the registries of these courts has provided transparency by providing the cause list, case status, judgments etc. online.

The Judiciary depends heavily on documents from different pillars of the Criminal Justice System namely the Prisons, Police and Forensic labs.

Filing, proceeding and closing of cases involves multiple stakeholders. While civil cases can be filed by advocates in the respective courts, the criminal cases are initiated with the police registering a FIR which is then sent to the court.

Receipt of FIR is acknowledged and if necessary, proceedings could be initiated. The police then prepare the charge sheet and submits the same to court. The proceedings take place in Court. Notices, summons are issued to the concerned party through the police. Bail orders / conviction orders are sent to the Prisons.

Thus, there is a need for exchange of data between the different pillars of the criminal justice system. The need for trust between these systems and availability of immutable data is what makes the Blockchain technology an enabler for speedy disposal of cases.

Challenges

1. High Turn-Around Time (TAT)

There is an inherent delay in the posting of the cases after filing as the scrutiny of cases is time consuming and requires multiple iterations.

2. Maintenance of multiple physical records

The maintenance of several registers for managing the judicial deposits is a humungous task.

3. Lack of a tamper-proof mechanism for data and document exchange among stakeholders

A huge number of documentation and information is exchanged between the Judiciary, Police and Prisons. Since, the content of these documents have great significance, it is also prone to tampering. There is a need for certified copies of some of these documents to be obtained from the court. This is not only time consuming but also leads to the overall execution of a case.

4. Disconnected systems

Presence of disparate systems results in delay. Integration of data from all the pillars of the criminal justice system would provide data at a single location for analysis. However, there is no common and trusted location for sharing of the documents that are essential for enabling the agencies to take decisions.

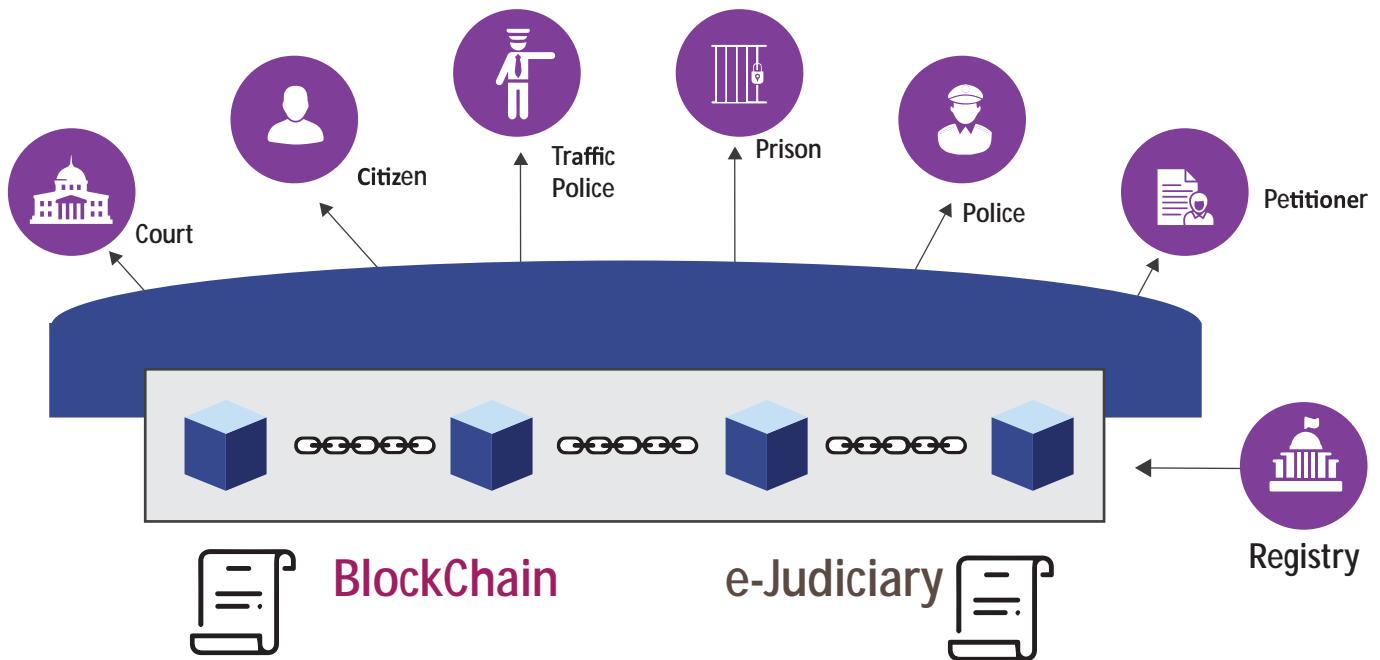
Proposed System

It is possible to implement Blockchain for various activities in the e-Judiciary. Blockchain technology can be used under the following scenarios for the Judiciary.

Judicial Deposits

Under certain circumstances, a party is ordered to deposit money with the court. The registry then puts the money in fixed deposits in banks. At various stages during case hearing, the court might also order that a portion of the judicial deposit be given to the other party. The Registry maintains these ledgers. There are instances when the deposits are not claimed by parties due to various reasons. These transactions on judicial deposits can be immutably stored in the Blockchain ledger. It could also facilitate automatic initiation of refund process.

Figure 7 – e-Justice Blockchain: Speeding up Justice delivery system



Transfer of FIR, Charge-sheet & traffic challan data from Police Department

The FIR and charge-sheet issued by Police need to be presented at court within a stipulated time. The details of FIR are captured in case information system in courts and then registered as a case. Sometimes, even though the charge sheet is not filed, the hearings can be made based on the FIR itself. The charge sheet is submitted by the police to the prosecution after validating the admissibility and then it is handed over to the court. The Court then acknowledges the receipt and the charge sheet is admitted.

Instead, the police / traffic police department software can store the hash of the FIR, charge-sheet, traffic offence details & fine amount in the Blockchain. This will facilitate the following

- I. Certified copies of the FIR / charge sheet document are also requested by the citizens. While the document is retrieved from the document management system, its hash can be compared with that stored in the Blockchain. This will enable the system to check the authenticity of the document before issuance of hard copies through counters or facilitate other agencies to download the soft copy.

- II. The Court can refer to the FIR metadata from Blockchain for further processing without waiting for the hard copy of FIR.

- III. The fine on traffic violation can also be retrieved by the traffic court to dispose these cases quickly.

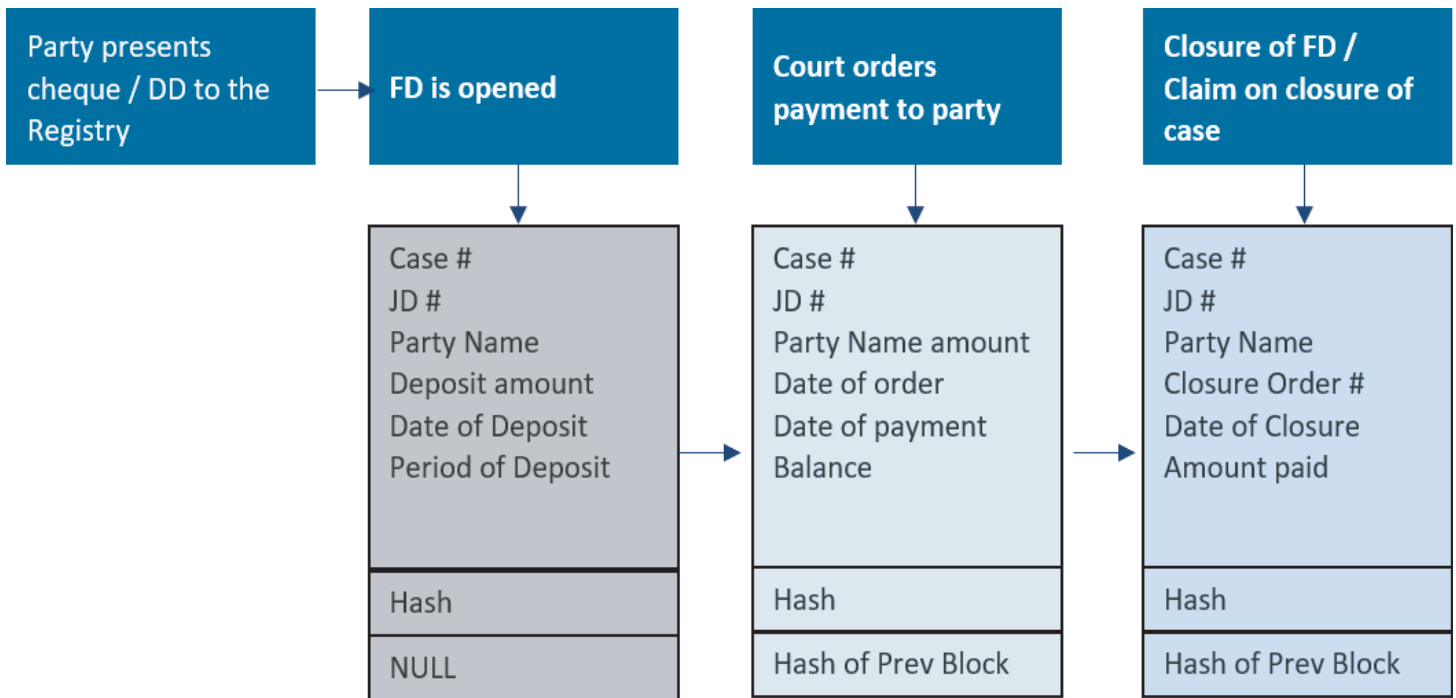
Publishing the notices and summons to the parties served by the Police

The time and effort needed to issue summons and notices to parties can be greatly reduced by ensuring that the registry stores the hash of these documents in the Blockchain. This would also enable the police staff to download the documents from the document store after verifying the authenticity of these by comparing the hash with that in the Blockchain.

Issue of bail orders by the Court

Bail orders issued by the court is one of those documents which require to be presented in prisons at the shortest possible time. Enabling the bail orders to be stored in Blockchain will facilitate in-time retrieval of the bail order document. The immutability of these documents ensures that the authorities at the prison and the parties involved can trust the digital document.

Figure 8 – Judicial Deposit Ledger



Use of land records & registration data

The land records & registration system would store the details of land, its ownership, transaction data on the Blockchain which can be used by the Judiciary during the different stages in the case proceedings to check for transaction details and ownership of the land or property.

Benefits

Implementing Blockchain in Judiciary & other pillars of Criminal Justice System will provide the following benefits:

Tracking of Judicial deposits

Maintenance of the Judicial deposit registers will ensure that no tampering occurs and also automate certain business tasks which would have otherwise be dependent on human discretion.

Real-time document storage and transfer

Since the documents that are available in document management systems can be verified for its integrity using the hash of the document in the Blockchain, the need for certified copies of these will be reduced to a great extent as the participating agencies can directly download the soft copy of the documents after verification on Blockchain.

Substantial reduction in Turn Around Time (TAT)

Reduction in time taken for the movement of the documents between these pillars can improve the efficiency of the systems.

The aggrieved parties will also be able to rely on the data available in the document store using verification process enabled through Blockchain; thereby reducing dependency on lawyers.

Verification of facts from documents issued by other departments such as land records, property registration etc. will help in quicker disposals.

3.4. URBAN PROPERTY MANAGEMENT SYSTEM – e-AASTHI

In India, with the introduction of digital property records system in the last two decades, several States have digitized property records and have enabled all transactions to be performed on digital platform only. Several States have also integrated registration system with property records system to facilitate seamless exchange of information. This is extremely useful, especially in enabling automatic initiation of mutation for transfer of ownership.

e-Aasthi is a workflow-based Urban Property Management System application implemented to provide citizen-centric services in the State of Karnataka. e-Aasthi has till-date facilitated the registration of more than 5 lakh property records and has issued about 6-lakh documents. e-Aasthi is an exemplar of e-Governance system that has brought transparency in the process of creating digitally signed property records. The system has increased the responsibility and accountability on the part of Bill Collectors and Revenue Officials of the Urban Local Bodies (ULB).

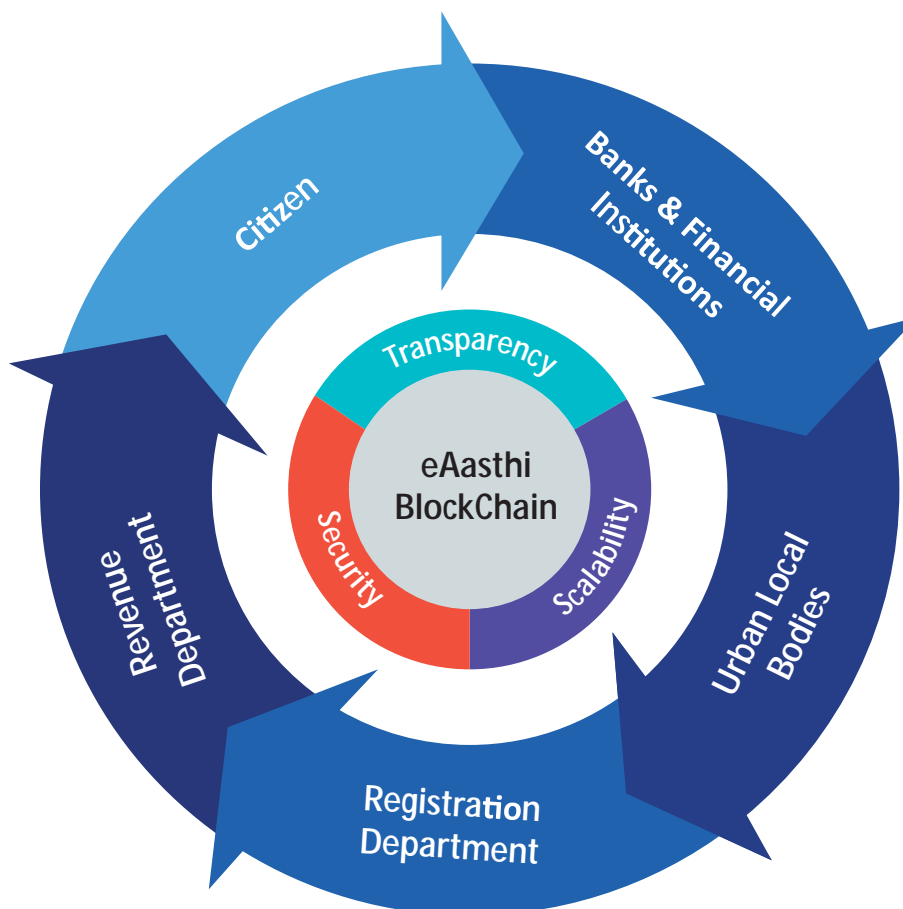
By adopting state-of-the art technology, the revenue officials of the ULBs enter data in the field itself during field visit. All the property records created in e-AASTHI are digitally signed.

In the management of the urban property records, the contributors for maintaining the data of ownership, rights and liabilities are many. These include the Revenue department, the urban local bodies, financial institutions, town planning departments etc.

Challenges

In spite of availability of electronic data, there has been no great reduction in the number of property related court cases filed in the various courts of the country. Instances of data manipulation, production of fake document are some of the causes leading to a rise in the number of property disputes. These frauds cause great hardship to the citizens who rely on the developers and hence, are not able to take an informed decision.

Figure 9 – Stakeholders in the e-Aasthi system: Enabling ease of service delivery





Proposed System

The urban property management system requires verification of facts at every stage in the process of transfer of ownership, approval for formation of residential layouts, liabilities of the owner, obtaining loans from financial institutions etc.

It is proposed to enable e-Aasthi system & the software put to use in the Revenue Department, Urban local bodies, town planning department, financial institutions to integrate with Blockchain to maintain their ledgers. The on-boarding of these departments to Blockchain will be a pre-requisite for harnessing the benefits of this technology. The existing applications in these departments will have to store the data in Blockchain ledger and refer to details to provide an effective solution to the problems being faced by the common man. The rules for updating the attributes related to the owner or property can be defined and recorded in the Blockchain. The Blockchain system would then be able to trigger activity based on events in any of the applications through smart contracts.

The key stakeholders of this proposed system would be as follows:

Urban Local Bodies

Management of property records under their jurisdiction including textual data such as property ID, owner details, bio-metrics, extent of built-up area, the type of construction and GIS data. This information needs to be stored in the Blockchain in an encrypted fashion.

Citizen

The citizen being a major stakeholder should have access to check his/her property details. Purchasers can verify ownership, liabilities and other details before property transaction.

Revenue Department

As the boundary of urban area is extending into surrounding rural areas, there is a need for several agricultural lands to be converted for non-agricultural purpose. Such conversion orders need to be stored securely and provide access to other stakeholders to take correct decisions.

Registration department

Registration department is provided with all information about a property at the time of registration and should not be allowed to perform any transaction in the absence of the rightful owner identified by bio-metrics. In the event of death of the owner, transfer of ownership should be based on documentary proof provided by way of certificates such as legal heir / surviving family members etc. issued by the competent authority. Land conversion orders should also be verified from the Blockchain ledger before registration. The financial transaction details such as payment of stamp duty and registration fees should also be stored on the ledger.

Town and Country Planning

Approval for building license and updation of property records can be done easily because of availability of authentic documents on the ledger.

Banks and Financial Institutions

Financial institutions would have access to authentic data which would help them clearly distinguish between legal and illegal properties. This would expedite their due-diligence process before sanctioning the loan.

The details of loan and the release of the property etc. would also be recorded on the ledger which would help prospective buyers and other stake holders, make learned decisions.

Utilities department

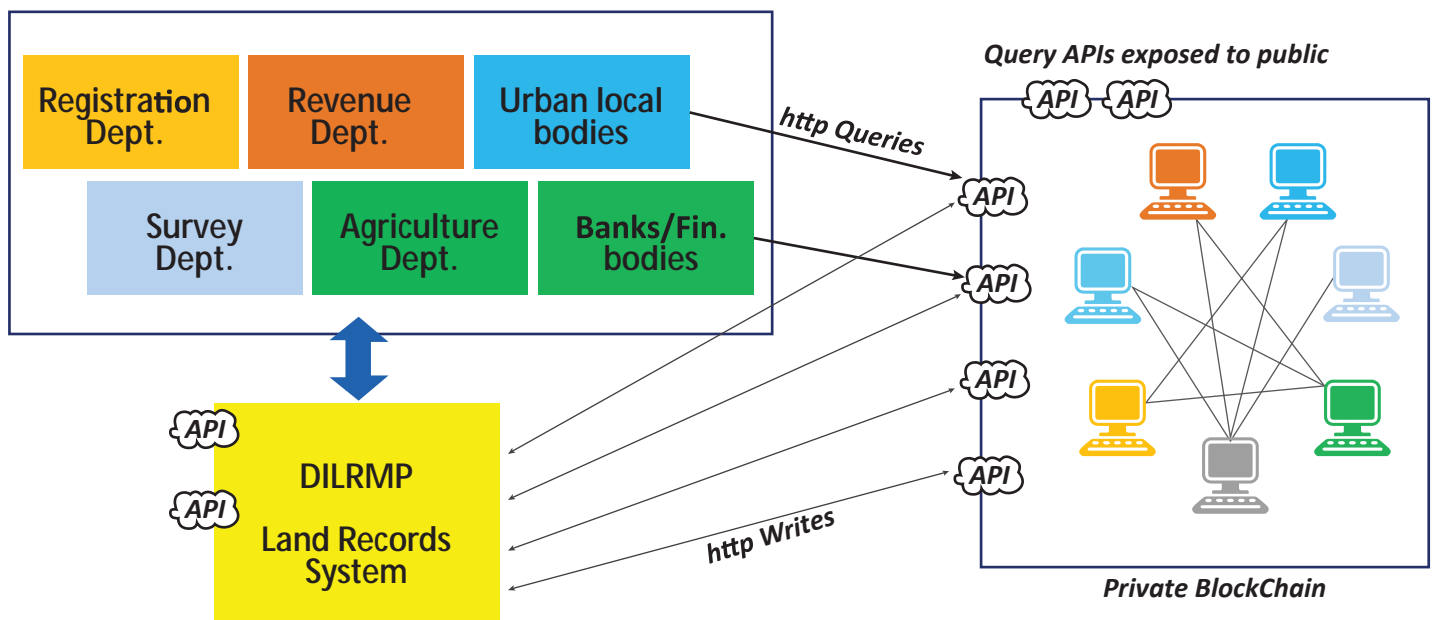
The authorities that provide license / permission for providing daily amenities such as water supply, electricity etc. will be able to complete the verification quickly and provide service in the shortest possible time.

Benefits

Advantages of implementing Blockchain with e-Aasthi are as follows:

- Immutable property records and immutable financial transactions to establish the rightful owner
- Tracking of property ownership history transfer facilitated by provenance of property ownership, partition of plots and simultaneous updation of maps and land records
- In the case of mortgaging property, banks and housing finance companies can validate the information before sanctioning loan

Figure 10 – Securing the Land title in Blockchain



3.5. LAND RECORDS

In India, the ownership of a property is proved through presumptive land titling Record of Rights (RoR)-chain of documents that provide evidence of the transaction history from person to person over the years all the way to the current state.

Registration is only recognized as an agreement between two parties for transfer of property. An important constraint is that any one of these intermediate transactions is liable to be challenged as the office of sub-registrar (SRO) is only undertaking deed registration under the central registration act 1908 and does not verify the ownership of land. This ambiguity is one of the reasons for property disputes and fraudulent transactions.

Land records is under the jurisdiction of state laws. The Revenue department/ Revenue & Panchayat Raj department is the custodian of the land records. They are authorized to maintain land record details. The various other transactions related to change of ownership through sale, loan, mortgage, release of mortgage, crop updation initiated by other departments are approved by the revenue department officials and the Record of Rights (RoR) document gets updated accordingly.

The Land record management system deployed in the various states facilitate the mutation of land. The change in ownership of land, the cultivators, the crop grown, the source of irrigation, rights and liabilities are some of the key data fields that are stored and maintained. The RoR document is required for farmers to obtain benefit from the Government in the form of subsidy for seeds, fertilizers and for other purposes like securing loan, for sale etc.

The Registration departments in the country use a software independent of the land records system. The complete document pertaining to the property to be registered is uploaded along with meta data by the citizen. It undergoes approval process and at final stage, biometrics of the parties involved (executant and claimant) is taken. Then the sale deed document is printed, signature is obtained from executant and claimant and uploaded again into the system for future issuance of certified copy.

Challenges

Some of the major challenges faced in this system include the following:

1. Increase in fraudulent transactions and land disputes

History shows that duplicate registration documents are generated by tampering original documents and the properties are being sold on the basis of the tampered documents. Also, one property is being sold to multiple purchasers. This is possible as the current system does not share real-time data with other key stakeholders.

2. Lack of a single-source-of-truth for land ownership

Determination of current ownership of a land requires tracking a long history of transactions. Moreover, different departments have different versions of land ownership details stored in their database.

3. Time consuming and cumbersome processes

A lot of paper work is required for any land related transaction such as selling land, dividing land, obtaining loan from banks using land as collateral security etc.

4. High Turn-Around-Time (TAT) for service delivery

Citizen has to wait for days, weeks or months to avail a service related to land due to the involvement of multiple departments and lack of seamless information flow between them.

5. Possibility of data tampering due to lack of tamper-proof system

There is a need to ensure that the data in the land records system, registration system etc. are not susceptible to alteration as each of these departments rely totally on the integrity of the other to initiate transactions. Hence there is a need for trust to use a common source of data to perform approvals for different activities so as to avoid the problem.

Proposed System

Land is one of the most valuable assets in the world and hence, land records require high accuracy and security and should be immutably stored. Key data fields such as ownership details, area, rights and liabilities on a parcel of land along the existing history and encumbrance should be stored on the Blockchain ledger after approval by Revenue functionaries in the State. The approved data will be digitally signed and stored. This will form the base record for any mutation in the future. The certificate details issued by the Revenue Department will be stored on the Blockchain ledger and can be used by the other agencies like the bank for real-time verification process during a land transaction.

The transactions related to change of ownership through sale, loan, mortgage, release of mortgage, crop updation is initiated by other departments. The required due-diligence before performance of these tasks can be done by accessing the Blockchain ledger which would contain 360-degree view of all information regarding the land parcel. After the approval of transaction in the respective database, the transaction details are again pushed into the Blockchain ledger.

Specifically, the registration department will fetch details w.r.t a survey number from the Blockchain and ensure that the ownership of the land parcel indeed rests with the prospective seller before initiating a sale. After obtaining the signature of the purchaser (claimant) and seller(executant) in the sale deed, the document should be stored in a document management system with the hash in to Blockchain Network to create a block. Once the block is created it cannot be edited or tampered. Likewise, the chain of blocks is created every time.

The banks would complete loan approval process by using the details of the RoR and the solvency certificate issued by the Tehsildar. Through the implementation of smart contracts, certain events can be auto triggered. For instance:

Specifically, the registration department will fetch details w.r.t a survey number from the Blockchain and ensure that the ownership of the land parcel indeed rests with the prospective seller before initiating a sale. After obtaining the signature of the purchaser (claimant) and seller(executant) in the sale deed, the document should be stored in a document management system with the hash in to Blockchain Network to create a block. Once the block is created it cannot be edited or tampered. Likewise, the chain of blocks is created every time.

The banks would complete loan approval process by using the details of the RoR and the solvency certificate issued by the Tehsildar. Through the implementation of smart contracts, certain events can be auto triggered. For instance:

- Registration of the land can automatically initiate mutation request in the land record
- Loan sanction by the bank can update the rights and liabilities
- Crop details updation can trigger the updation of cultivators and crop details in RTC

Smart contracts can also facilitate the payment of subsidy to farmers on failure of crops. In cases when the entitlement is only for certain types of farmers, the eligibility can be ascertained from the Blockchain. The services provided by the Agriculture / Horticulture departments such as subsidy towards farmer equipment / sprinkler system / drip irrigation etc. can also be recorded in the block chain.

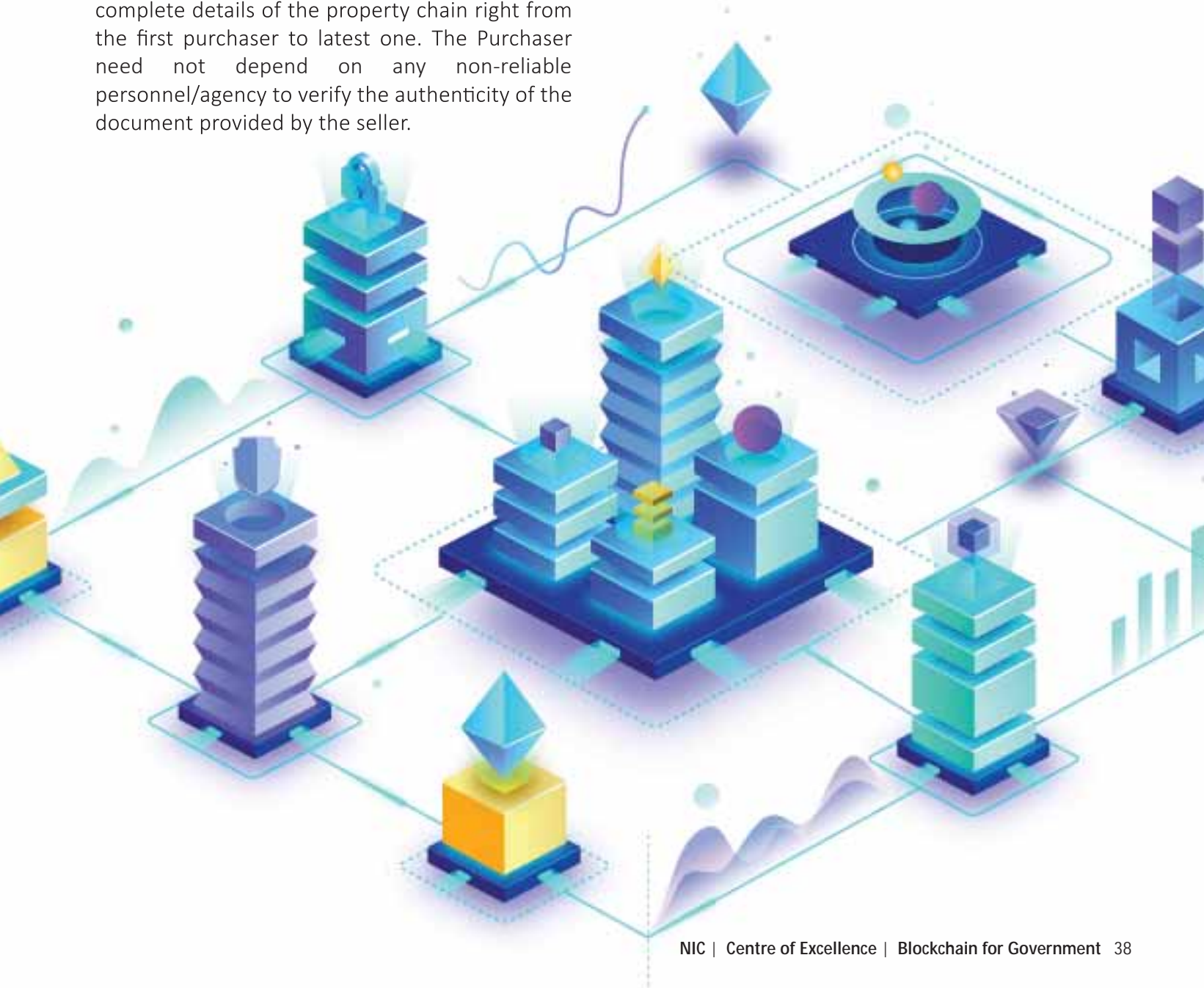
Benefits

The following would be the benefits obtained by implementation of Blockchain in land record management:

- The availability of data in a central location that can be accessed by all departments which would enable faster disposal of requests for subsidy, mutation etc.
- There would be no need for trusted authority like notaries to provide attested copies of documents
- Citizens would be assured that their land ownership cannot be changed by spurious persons

- Loan processing and approval will be easy and quick. The updation of the details related to liability in the Record of Rights can be done by the financial institutions as soon as the farmer repays the loan. This will facilitate the farmer to avail other benefits.
- The facilities provided to the farmer from different departments such as Horticulture, Agriculture, Animal Husbandry etc. can be tracked to ensure that the same benefit is not availed from multiple departments illegally. This would also help in ensuring that only eligible candidates receive the benefits.
- Blockchain data of the property registration will be made available in the work flow system of the Registration software as well as to the public for verification through APIs. This will provide the complete details of the property chain right from the first purchaser to latest one. The Purchaser need not depend on any non-reliable personnel/agency to verify the authenticity of the document provided by the seller.

- Using Blockchain, the registration department will be able to verify the integrity of the document in their document repository which can be used not only by themselves, but also by other agencies.
- The availability of document chain will eliminate registration based on bogus documents. The number of land related cases filed in the different courts of the country will reduce drastically and thus reduce the pendency in the courts



3.6. STATE EXCISE SUPPLY CHAIN

State excise duty contributes almost 20 percent to most of the State exchequers. To augment the excise revenue, it is needed to ensure that all Beverage Alcohol, Medicinal Alcohol, Industrial Alcohol & Life Saving Narcotics Drugs available in states are sourced and sold through legal channels. This would help in eradicating manufacture, distribution, supply & sale of illicitly distilled /counterfeit / non-duty paid intoxicants to arrest revenue leakage points and safeguard public health.

Most excise supply chain systems are centralized systems that include the following functionalities:

- Capture of production data
- Provision of shopping cart facility
- Generation of transport pass & invoice during supply
- Maintenance of inventory on real time basis
- Integration with Bank Payment Gateway
- Maintenance of Payment Wallet

Involvement of third parties include Banks, Police, Excise Authority, all of whom process and verify transactions as they pass between buyers and sellers before authorizing the transfer of value, whether Packaged Liquor or Invoice Amount or Service like NOC/Pass.

Stages in the supply chain include:

- Packaged Liquor Manufactory/Bottling Plants (both Country Liquor & Foreign Liquor) produce bottled liquor, affixes 2D QR Coded Hologram Labels on bottle tops, put the bottles in a case, affix case level QR Codes, store in adjunct bonded warehouse.
- Traders/Distributors place requisition for procurement of packaged liquor from Manufactory/Bottling Plants. De-bonding of requisitioned quantity of packaged liquor is done through payment of appropriate excise duty. QR Coded labels of requisitioned packaged liquor cases are scanned using Hand Held Terminals (HHT) while uploading into carrier vehicle. Transport Pass & Invoice are generated based on scanned data. Debit & Credit operations in digital inventories of manufactory & distributor are made.
- Traders/Distributors receive physical stock using HHT on arrival of vehicle at their premises.

- Retailers (Liquor Off/On Shops) put online requisition for procurement of packaged liquor from Distributors and pay online to the
- Distributor. Subsequently, QR Coded labels of requisitioned packaged liquor cases are scanned using HHT while uploading into carrier vehicle meant for supply to retailers. Transport pass & invoice are generated based on scanned data. Debit & credit operations in digital inventories of distributor & retailer are made.

Challenges

The following are the major challenges in the current system:

1. Revenue leakage

Excise revenue is lost out because of a significant increase in sales of fake labels—poor quality blends that are packaged as popular premium alcohol brands. It has become increasingly lucrative to sell counterfeit labels because of a sharp rise in excise duty. Sales of non-duty paid fake bottle products are now accounting for as much as 10-12% of overall excise revenue, which is a significant loss to the exchequer.

2. Lack of a fool-proof tracking system

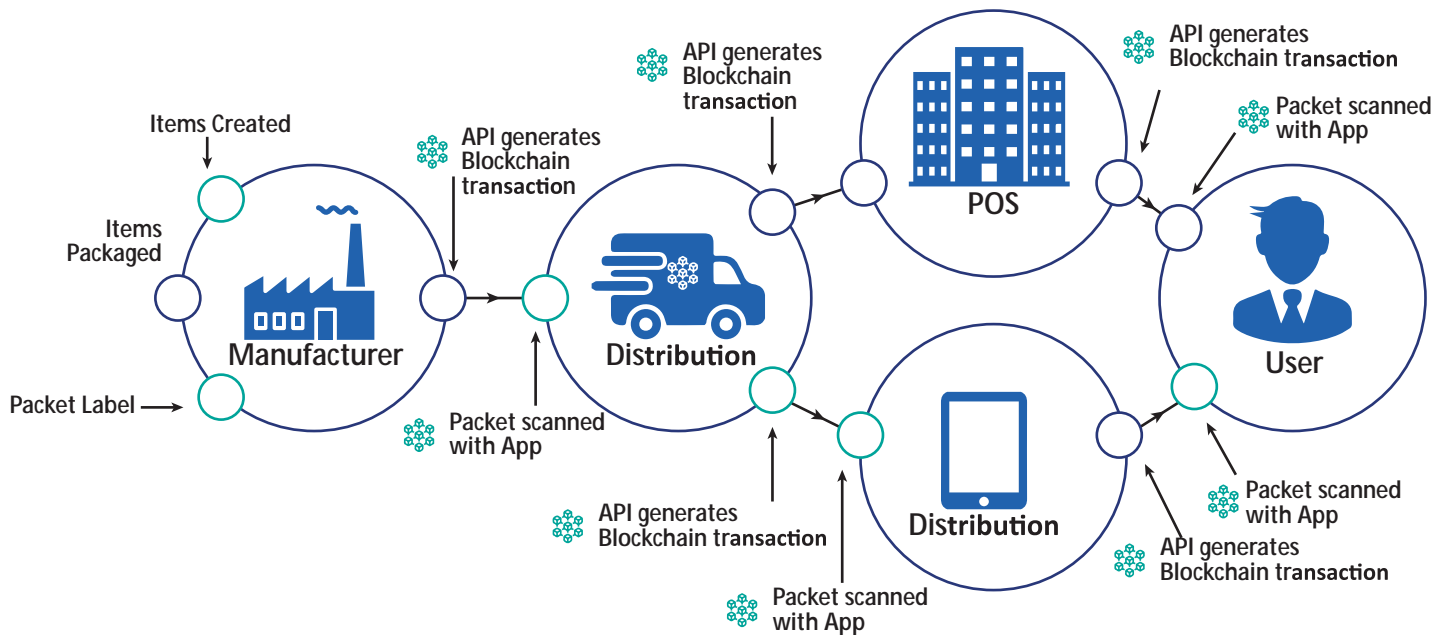
It is difficult to ensure authenticity of Packaged Liquor that is required for arresting revenue leakage & safeguard Public Health. Even if there is a Central repository that stores all the information about the supply chain of packaged liquor from manufactory till retail outlets, it is difficult to establish trust among all the entities involved. The fundamental issue is that central repository does not have the ability to provide decentralized trust, immutability and tamper evidence.

3. Information silos

Stakeholders cannot maintain an appropriate overview of their supply chain networks within state excise supply chain as data is fragmented into various silos with very little data interoperability. The stakeholders e.g. Government, packaged liquor manufactories, warehouses, retail outlets & consumers have no incentive to share data. This makes it harder to ensure integrity of packaged liquor as they flow through the supply chain.

Figure 11 – Excise supply chain on Blockchain

Use Case of Blockchain based State Excise Supply Chain



Fighting contamination, reducing counterfeiting, and maintaining an efficient supply chain are some other challenges faced by the system.

Proposed System

In proposed environment of State Excise Supply Chain Management System enabled by Blockchain technology, transactions will become peer-to-peer with little need for intermediaries.

At every stage in the movement of goods, the details of the movement along with the necessary permission details reproduced in the movement documents would be stored in the Blockchain ledger. Specifically, the lot number, the date of receipt, quantity etc. can be recorded. The process of verification of details of goods received can be verified with data in the Blockchain. QR codes affixed to the bottles received would be compared to that stored as a transaction at the previous level in the supply chain and can be verified. This would facilitate the detection of any tampering of the documents and also the entry of spurious liquor.

At the packaged Liquor Manufacturer/Bottling Plants Bottle IDs, the case IDs that are sent to the adjunct Bonded Warehouse for storage has to be recorded. When distributors put requisition for procurement of Packaged Liquor from Manufactory/Bottling Plants, the details of the payment of appropriate excise duty is stored in the ledger. During the scanning of the QR Coded labels while uploading into carrier vehicle, the transport pass & invoice are generated. The transport pass & invoice details along with the item wise IDs will be stored in the Blockchain. As part of the smart contract execution, debit & credit operations in Blockchain will be automatically initiated and reconciled.

Traders/Distributors receive physical stock using HHT on arrival of vehicle at their premises. The verification of the supplied stock can be ensured by comparing it with the data entered by the distributor and will give the necessary confidence to the distributor about the authenticity.

When retailers (Liquor Off/On Shops) apply for procurement of packaged liquor from distributors the data of the invoice, IDs of the cases etc. will be stored as in the stage when distributors put in requisition from manufactory.

Benefits

Efficient collaboration between all participants

Use of Blockchain should help to cut acquisition, management, documentation and compliance costs. With the ever-changing rules, the compliance would be simpler. There would be lesser disputes as the contracts can be effectively implemented.

Improved customer satisfaction

By simplifying the use and increasing transparency, it will also help to improve customer satisfaction. Authenticity of the package of alcohol can be verified by the consumer who would also be able to obtain all the details from the manufacturer to the retail store.

Process of reconciliation is simplified

There would not be any need for each of the stakeholders to perform verification of financial transactions manually, and every entity will be able to verify the same from the ledger. It would also reduce the risk of human errors.

Ability to take informed and timely decision

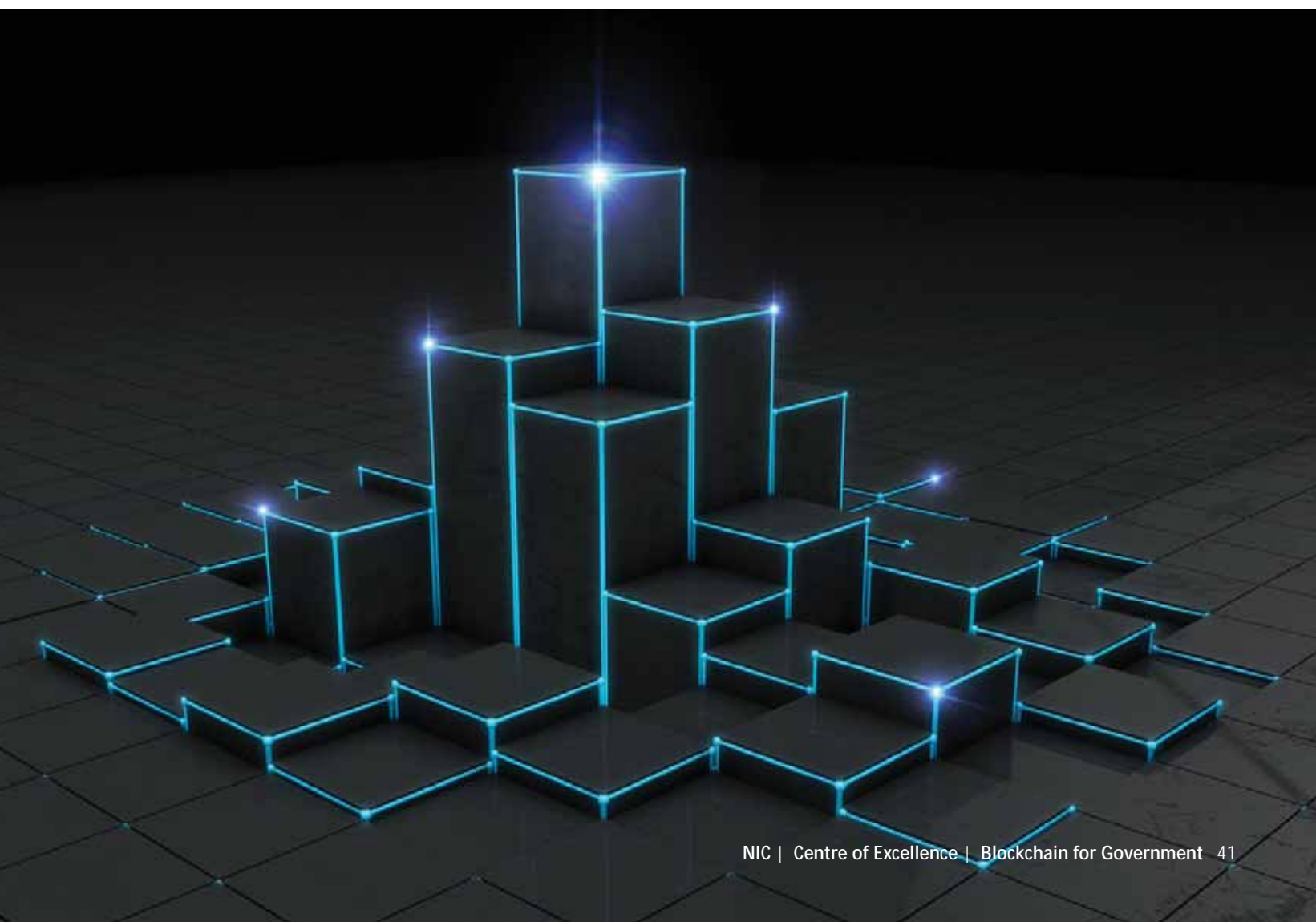
Blockchain would ensure continuous availability and accessibility to verify the data associated with Packaged Liquor Supply Chain. In case of any fraud, it would be possible to easily identify the complete lot and its location and the same can be withdrawn in the shortest possible time.

Automated reconciliation and payment

A Blockchain based system shall allow for automatic triggering of payments and replenishing orders. The facility for cascading purchase orders, invoices, receipts etc. for automatic verification shall also be provided.

Recalling of specific cases / lot

If a complaint is received regarding the quality / safety of a particular bottle of liquor, then it is recorded in the system. The smart contract can identify the source of the supply and block further movement of the commodity till the issues are resolved.



3.7. AUSHADA - ONLINE SUPPLY CHAIN MANAGEMENT SYSTEM FOR DRUGS

Government of Karnataka, with the help of Government of India [NRHM], procures and supplies free drugs for the patients across the state to facilitate treatment on time without any shortage of drugs. Around 2,911 hospitals are covered under this scheme and every year more than 300 crores worth of Drug is procured and supplied to these hospitals through 26 Warehouses.

The main objective of implementing Aushada Software is to automate the Supply chain management system at Karnataka State Drugs Logistics and Warehousing Society (KSDLWS). All 26 District Drug Warehouses and 2,911 Health institutions across Karnataka State are expected to be users of this system

Key objectives of the system are to:

- To monitor current stock position of all 2,911 Health Institutions located at different levels in the district.
- To control expiry of drugs and maintain the minimum stock of essential drugs at all health institutions.
- To record the result of the lab tests and enable issue of only Standard Drugs and freeze those that are not of standard.

To achieve these objectives, the process of procurement and supply involves the following steps:

- Collection of annual requirements from 2,911 Hospitals which amounts to INR ~300 crores per year
- Submission of consolidated requirement to the State Therapeutic Committee
- Placement of Purchase Order with Delivery Schedule for 700 to 800 drugs with 400 suppliers
- Receipt of the Drugs at the Warehouses from the Suppliers
- Inspection of the Quality of the drugs

- Monthly Requirement by the Hospitals sent to warehouse
- Approval of Monthly Requirement by the Warehouses
- Receipt of the physical stock at the Hospitals
- Issue to the Sub Store

Challenges

Key challenges of the system include:

- Possibility of tampering of crucial data like expiry of drugs, Quality of Drugs etc.
- Possibility of counterfeit drugs in the supply chain
- Lack of visibility of adherence to precautions during transportation of drugs

Proposed System

Drug Supply Blockchain system is proposed to integrate with the existing online Supply Chain Management System to record the transactions in a Blockchain based system at all stages of the supply chain. As illustrated in the Figure 12, all key transactions at hospital, during procurement, at warehouse and at sub-store shall be recorded on a Blockchain based ledger thereby providing unprecedented transparency and traceability across the system.

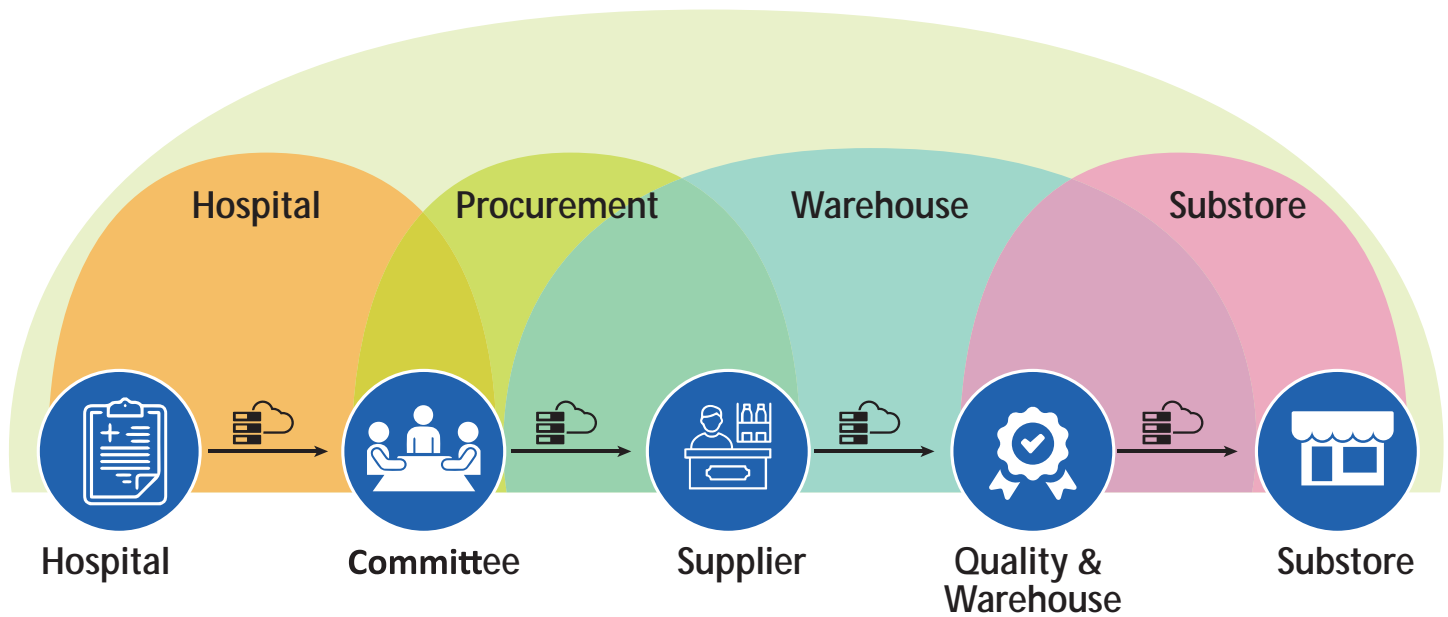
A few of the transactions that are recorded on the Blockchain based system are:

Procurement and Schedule – Purchase Order is prepared for every supplier. The purchase order has the drug wise and warehouse wise quantity to be supplied with the time schedule. The schedule is published so that the supplier makes arrangement to supply the drugs to the concerned warehouse.

The details of Notification of Award [NOA] Number, PO Number, Supplier, Drug Name, PO Date, Rate, Warehouse, Quantity are stored in the Blockchain ledger.

Figure 12 – Drug Chain: Ensuring availability of drugs to the Patients on time.

Blockchain-Drugs Logistics



Warehouse Inward – Warehouse pharmacist receives drugs against the purchase order along with batch details. The physical receipt of drugs is verified against the quantity mentioned in the invoice.

The pre-conditions before receiving the same can be ascertained by requesting the details of suppliers and the drugs to be supplied for the concerned warehouse from the Blockchain ledger.

The details of PO Number, Supplier, Drug Name, Warehouse, Receipt Date, Invoice No., Invoice Date, Rate, Batch No., Mfg. Date, Exp. Date, Batch Qty are stored in the Blockchain ledger.

Payment to the supplier can be initiated automatically at this stage, via a pre-installed smart contract.

Quality Check – The quality check is done for every batch of drug by selecting the samples from 3 randomly selected warehouses. All these warehouses send the drug to the QC section.

The QC Section in the Head Quarters selects one sample out of the 3 warehouses from where the drugs are sent for testing. One of these is sent for testing to labs by generating a QC Code. The selected batch is available for outward to the Hospitals. If any of the drugs is identified as "Not of Standard Quality", the batch is frozen across the warehouses and the Hospitals so that the further issuance is stopped.

Drug Name, Batch No., Warehouse, Qty Lifted, QC Code, Result will be stored in the Blockchain ledger. If the batch is "Not of standard quantity" an intimation is sent to Commissioner for approval. Batch of drugs are frozen and automated alerts are sent to all concerned stakeholders.

Monthly Indent by Hospitals – A monthly indent is raised by the hospital to the mapped warehouse. The pharmacist request is approved by the in-charge of the hospital. The warehouse approves the indent with or without change in the quantity requested by the hospitals based on the stock available at the warehouse. The drugs approved by the warehouse are transported to the hospitals. The indent is raised when the quantity reaches the minimum stock level.

Indent No., Warehouse, Month, Year, Drug, Qty Required are stored on the Blockchain ledger.

Institute Indent No., Warehouse, Institute, Batch No., Mfg. Date, Exp Date, Qty, Supplier, Rate, Drug, Outward No., Outward Date are stored on the Blockchain ledger.

Receipt and Issue by Hospitals – Hospital take inward of drugs sent by the warehouse. The hospital main store issues the drugs to the Sub Store on daily/weekly basis.

Inward No., Inward Date, Warehouse Outward No., Institute, Warehouse, Indent No., Drug, Batch No., Mfg. Date, Exp Date, Rate, Qty, Outward No., Supplier are stored in the Blockchain ledger so that only authentic batches are received by the Hospitals.

Issue No., Institute, Drug, Batch No., Manufacturing Date, Exp Date, Qty, Issued to, Issue Date are stored in the Blockchain ledger.

Patient can check the manufacturer, expiry details and standard of the batch of drug before consumption.

The objective of using Blockchain Technology in Online Supply Chain Management System is to ensure transparency and traceability of drugs across the supply chain. This also ensures eradication of any counterfeit drugs across the supply chain. To achieve this, entities in the supply chain should verify the quality / expiry of drugs from the Blockchain ledger which stores this information in a seamless and tamper-proof manner. The batch details could also be verified by the warehouses to ensure that invalid batches are excluded. This system will also facilitate in providing details of stock levels across warehouses and hospitals.

Benefits

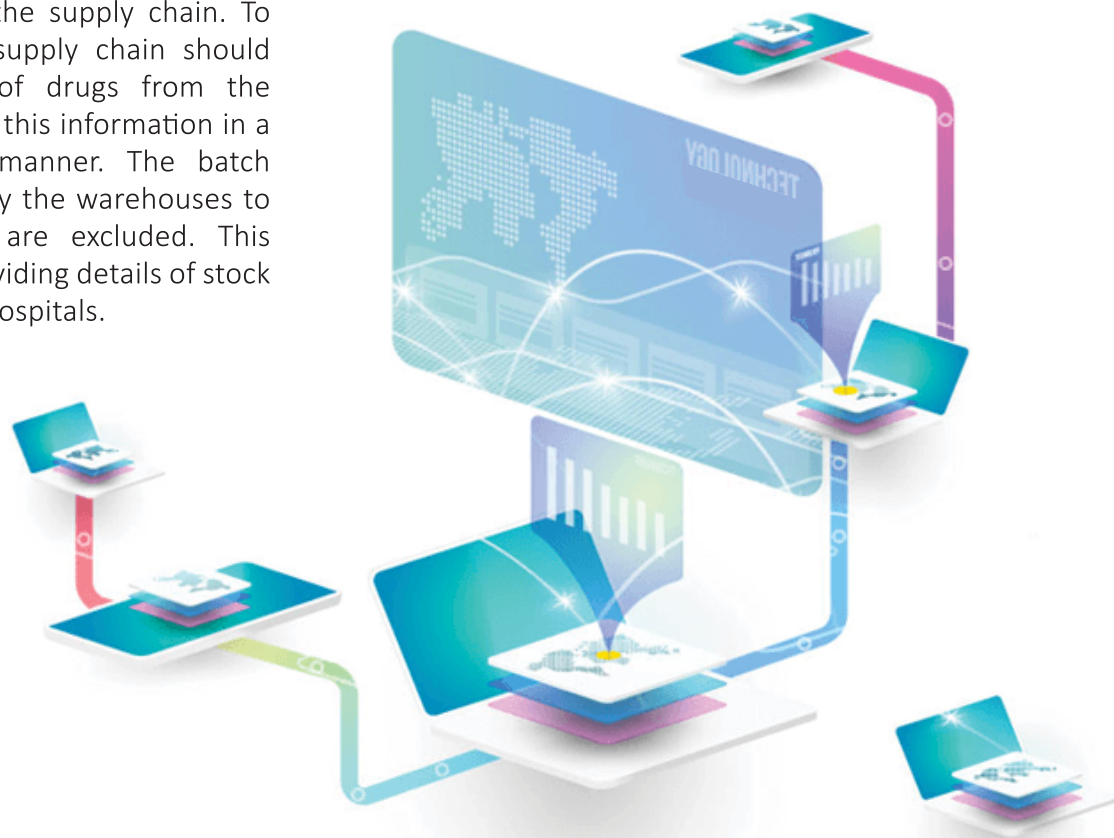
Smart Contract based automatic payment – The process of payment can be automated using smart contracts. As soon as quality of a shipment is checked and an approval is given on the shipment, a smart contract can be initiated to facilitate a payment. This will reduce the delays in payment and help in increased participation of stakeholders.

Enhanced Traceability – Using Blockchain, the drugs can be traced across the supply chain in a real-time and transparent manner. This will help in improved inventory management, easy recall of low-quality products etc.

Elimination of counterfeits through provenance – Any interested party in the supply chain would be able to identify the origin of the drug. This would help eliminate counterfeit drugs.

Inherent trust that only approved drugs reach end consumers – Only drugs which have undergone a thorough quality check would reach the hospitals.

Move to Push based inventory – If real time view of inventory of all medical supplies is available, a push-based inventory model can be implemented where drugs are replenished when a minimum stock level is reached.



3.8. CERTIFICATE VERIFICATION SYSTEM

As an infant is born and goes through the phases of education, employment and retirement, he / she is required to produce several documents to get admission in school, college, university, employer, government etc. Documents such as birth certificate, education certificates, income certificates, caste certificates etc. are required frequently by a citizen for purposes such as admission to educational institutions, concessions, scholarships, availing reservation quota based on social status etc.

Challenges

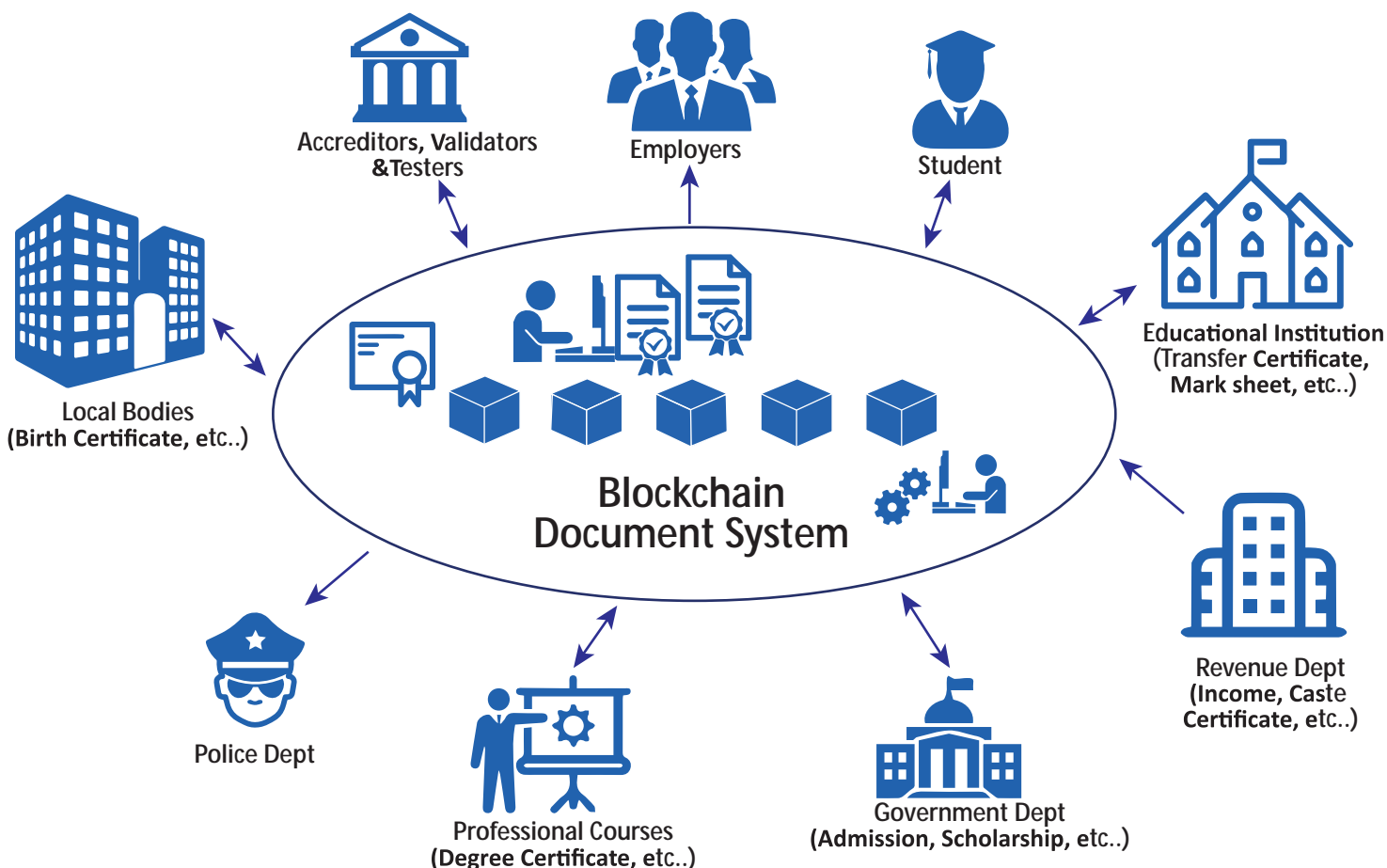
A lot of effort and time of a citizen is spent in obtaining these certificates. Multiple visits are required at times to obtain such documents. A few of such documents even have a validity period thereby making it a periodic task for a citizen.

On the other hand, it is equally difficult for the validating authorities such as educational institutes, Governments etc. who spend heavily on the verification of these documents. Since the volumes are large, there are possibilities of fake documents entering the system which could lead to ineligible candidates gaining benefit while depriving the deserving candidates.

As a specific case, the Karnataka Examination Authority which conducts the Common Entrance Examination for admission to professional colleges has a great challenge in verification of the documents submitted by the students of Karnataka and from other states. Various certificates such as X Standard marks card, caste, income, rural area certificate etc. are submitted by the student to claim reservation. Verification of the documents is a humungous task.

The welfare departments also spend significant time to verify the claims of the student while applying for school / college admission, scholarships, hostel admission etc.

Figure 13 – Certificate Blockchain: Ensuring security of documents



Proposed Solution

The issues pertaining to fake certificates can be eliminated by building a trusted environment for the validating authorities by enabling the issuers of the certificates to store the certificate details in a Blockchain based ledger in a tamper-proof manner.

In such a scenario, all the certificate details required by a student can be stored in an envisaged Blockchain system and validating authorities may log-in to the Blockchain ledger to verify the required documents.

The different departments / agencies which may become part of such a Blockchain network are –

Municipalities / Revenue Department– The birth certificate, caste, income, rural area certificates are issued by the revenue department and municipalities. These documents are very important to the citizens and several benefits are given by the other Government departments based on the availability of the documents.

Department of Education – Education certificate, transfer certificate, school completion certificates, marks cards issued by department of education may be stored on the Blockchain ledger and utilized by other organizations on the network.

Welfare departments – Departments of social / Tribal / Minorities / Backward classes welfare departments run hostels for poor students and also provide scholarship for poor / meritorious students. Based on the income, grades and caste, the Blockchain system can prepare a list of eligible students for awarding of scholarship / fee concessions without the need for manual verification of paper-based certificates.



Employers – The Government as an employer needs to verify the caste, income certificates along with educational certificates to provide employment based on reservation policy of the Government. Committees are constituted by the Government for the purpose of verification of the documents submitted as proof of claim by the applicant. It would be extremely easy for all agencies to verify the eligibility using the Blockchain based system.

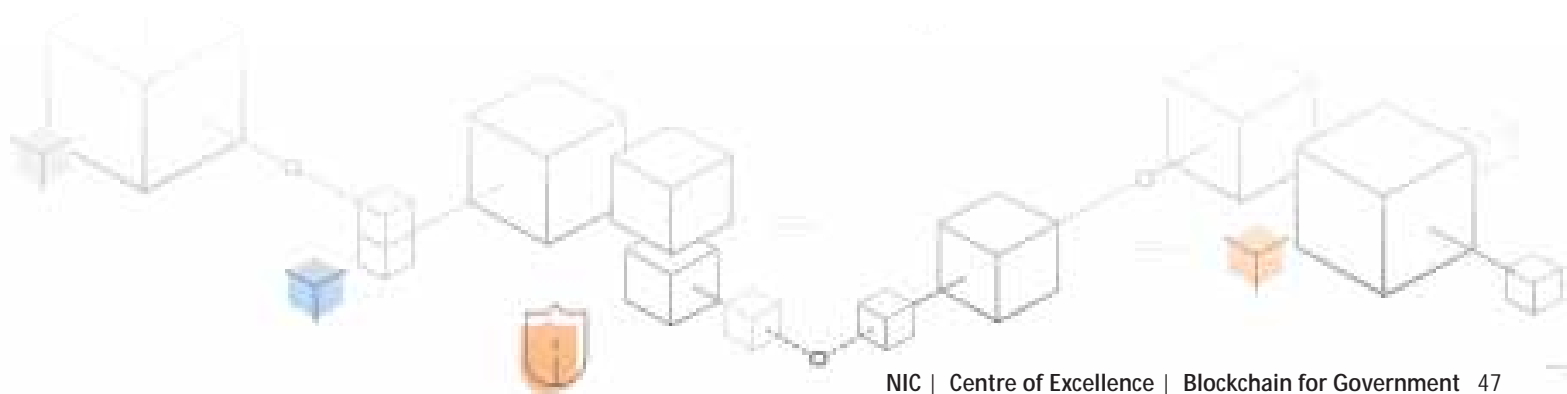
For the older certificates issued by the agencies, the student can upload the certificate meta data and the respective departmental systems can trigger a request to the issuing agency to notarize the certificate details. These notarized certificate details can then be stored in a Blockchain based system in a tamper-proof manner.

Any attempt to modify/tamper the document would fail due to inherent immutability provided by Blockchain based systems.

Benefits

A certificate verification system shall facilitate the student, Education institutions, Government and Non-Government agencies to access and share tamperproof record of certificate details.

This system will reduce the errors in manual verification of the document. The process of preparing the eligibility list would be simplified and automated due to the availability of all necessary data through a resilient, tamper-proof system. The establishment of the certificate chain will change the way the Government processes applications for admission, recruitment, scholarships, social security pensions and various other government initiatives. This system could pave the way for entitlement-based service delivery.





4. CENTRE OF EXCELLENCE IN BLOCKCHAIN TECHNOLOGY

Blockchain technology has drawn significant attention from the Government due to the pain areas that it promises to address. Several schemes of the Government require real-time verification of the documents / facts to ensure the eligibility of the application. This is currently an inefficient process. Although some of the departments use the electronic data available with other agencies to verify the applicant's claim electronically, the lack of confidence that the data has not been tampered has set the Government to look at alternatives such as Blockchain.

Although the decision makers in the Government are enthusiastic, the following challenges associated with this emerging technology are yet to be resolved:

1. Hosting of Blockchain proof of concepts (PoCs) / pilots require high infrastructure investment, thereby rendering such applications expensive for a Government department
2. Expertise required to build these solutions is not available with all the system integrators
3. The technology is still emerging and is constantly evolving
4. Government departments need support to identify the right Blockchain use cases due to low capacity building on this technology
5. Need for multi-stakeholder collaboration to form a network

Considering the above challenges there appears to be a need for an agency / center that the Government departments can partner with for consultancy, preparation of Blockchain design, provisioning of a platform for hosting PoCs/pilots and support in large scale roll-out of the PoCs. The CoE anticipates to provide these services to all Government departments.

CoE in Blockchain technology shall provide world class Blockchain services to Government by competent and knowledgeable consultants, a high-end laboratory housing different Blockchain frameworks for testing and evaluation of PoCs, and also an incubation center. It shall help the departments to:

1. Evaluate the maturity, feasibility and viability of Blockchain implementations for various departmental and inter-departmental use cases in Government
2. Identify the data sets that need to be stored in the Blockchain for use by other consuming departments
3. Identify the data sets that need to be provided with restricted access
4. Provide the consuming agencies an interface to fetch the data
5. To identify departmental workflow that could be streamlined and secured using Blockchain Technology
6. Provide a Blockchain as a service (BaaS) to Government departments
7. Best practices to manage Blockchain Infrastructure in a seamless manner

National Informatics Centre has been the pioneer in the area of eGovernance. With the vast domain knowledge with respect to various sectors and capability to use appropriate technologies to solve problems, NIC would be able to provide the necessary support for implementation of Blockchain Technology. The Centre of Excellence will be located in the Kendriya Sadan in Bangalore building. It houses a developer zone, a laboratory area and testing area. A video conference facility has also been established. The offerings of CoE on Blockchain technology would include:

a) Evangelising use of Blockchain technology in Government

The CoE will collaborate with industry, Government and Educational institutions to conduct workshops for Government departments and facilitate them to understand the use of Blockchain technology and its use in the areas of their work.

Specific problems of different verticals that can be solved using Blockchain would be identified and the CoE would work closely with the department to build and test the necessary Blockchain based applications.

b) Provide Blockchain platform as a service

The NIC Blockchain Platform would provide a managed, full stack Blockchain- as- a- service (BaaS) offering delivered in different environments including the NIC Cloud and on-premise. It would facilitate the Government departments to develop, operate and govern a Blockchain network with the performance and security necessary for eGovernance applications.

To start with, the CoE will coordinate with the departments and facilitate the setting up of the necessary network, develop and maintain the necessary APIs and SDKs for integrating the Line-of-Business applications with the Blockchain. Subsequently, the CoE will provide an interface for the departments to create a Blockchain network, define a node, instantiate a node, define workflow engines, define transaction validators, build smart contracts and facilitate user management.

The CoE will provide BaaS service for select platforms such as Hyperledger Sawtooth and Hyperledger Fabric initially. CoE will continuously evaluate other platforms for addition to their BaaS suite.

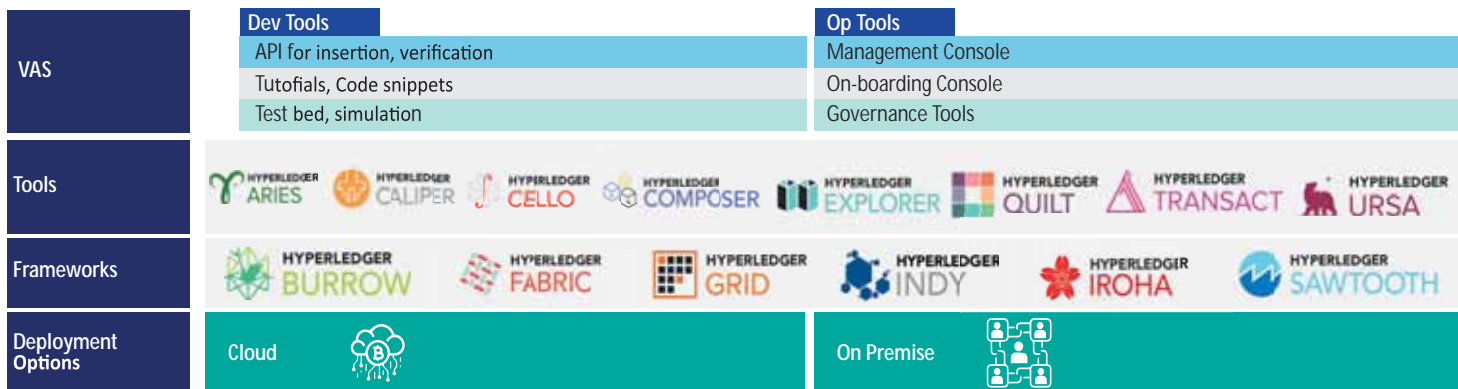
c) Consultancy services and development of PoCs

The National Informatics Centre has been providing consultancy services and also has been the architect for various flagship programmes of the Government. With good domain knowledge and ability to map the right technology for a business use-case, NIC has been instrumental in providing great user experience to different stakeholders. The CoE would collaborate with the Government departments to understand their requirements and partner with them to implement different schemes effectively. NIC shall endeavour to ensure that benefit of the technology reaches the target beneficiaries and enhance service delivery.

CoE has been working on the PoC for Blood bank, Excise chain, PDS, land records etc. At NIC, we believe that undertaking a proof of concept is a good way to test the technology and its applicability. CoE has used Hyperledger Sawtooth to build the PoC for the blood bank, Public Distribution System (PDS) and Excise supply chain. Hyperledger Fabric has been used for the NGDRS system.

Figure 14 – Blockchain-as-a-Service

Blockchain Platform



The Seminal Paper on Zero Knowledge Proof-- https://people.csail.mit.edu/silvio/Selected%20Scientific%20apers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf
 Verifiable Log Data Structures-- <https://github.com/google/trillian>, <https://github.com/google/trillian/blob/master/docs/papers/VerifiableDataStructures.pdf>

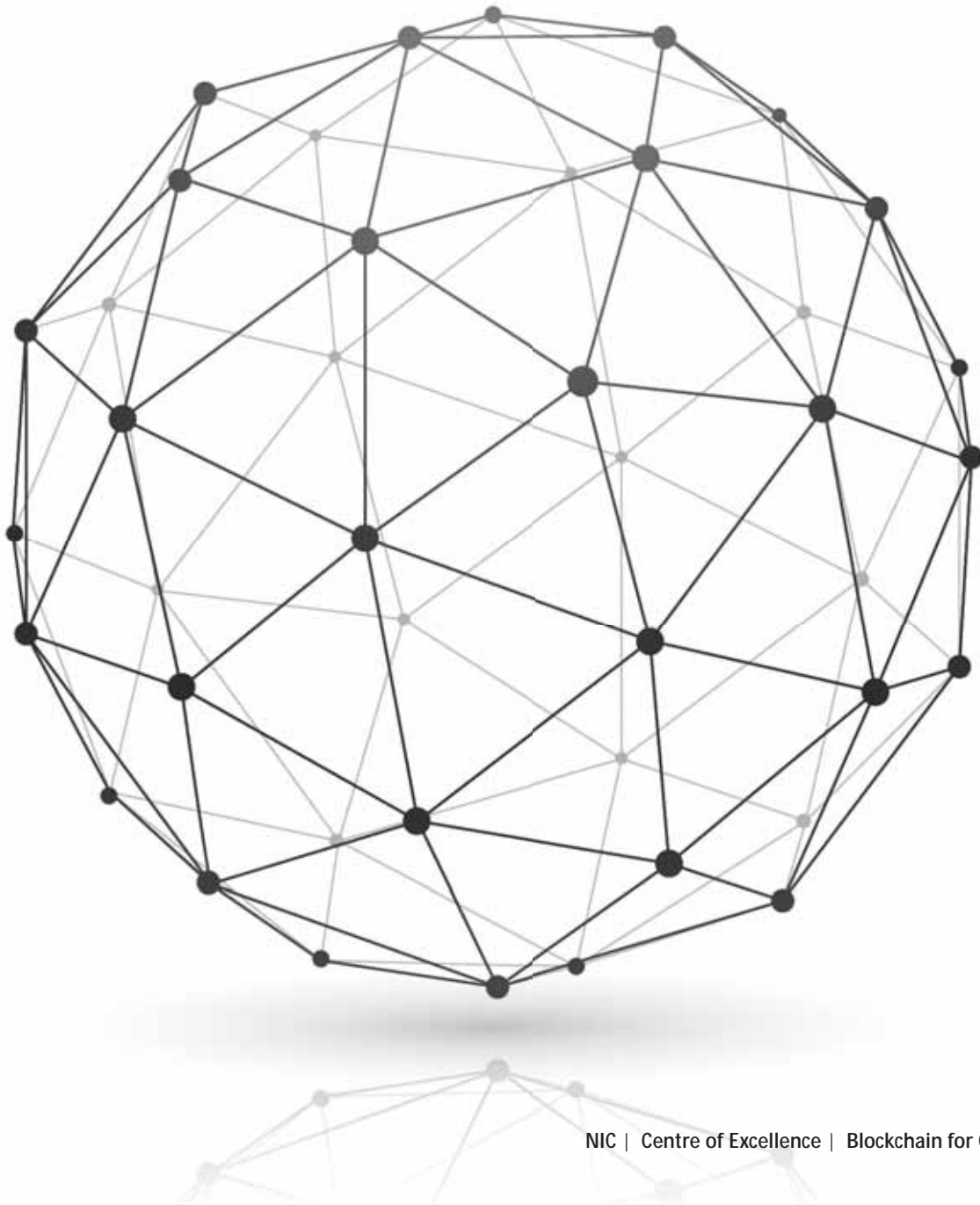
CoE shall endeavour to move these applications into production and develop more use cases over Blockchain.

d) Training on Blockchain Technology

Different levels of training shall be organized for technical officers of NIC by CoE. Regular technology upgrade sessions in coordination with the training division are proposed. The CoE also plans to collaborate with educational institutions and Technology providers to provide the best possible training programmes.

e) Large scale implementation

While a proof of concept is undertaken in a curtailed environment, there are multiple ramifications of taking a Blockchain use case to production. Key considerations such as privacy, efficient digital key management etc. require deliberations and identification of the right implementation strategy. CoE shall partner with Government departments to provide consultancy services for development of an enterprise scale Blockchain based system.



Contributors

B.Vinaya

State Informatics Officer
Karnataka

Mainak Mukhopadhyay

Sr. Technical Director
NIC- West Bengal

P. Sumanth

Scientist B
NIC- Karnataka

Jayanthi. S

Dy. Director General
NIC- Karnataka

Sreekumar

Sr. Technical Director
NIC- Karnataka

K. Pariselvan

Sr. Technical Director
NIC- Goa

T. Pechimuthu

Technical Director
NIC- Karnataka



Blockchain for Government
Centre of Excellence in Blockchain Technology

National Informatics Centre
4th Floor, F Wing, Kendriya Sadan, Koramangala, Bengaluru - 560034