Swaniti Initiative

Improving Public Service Delivery through Blockchain Technology

Applying blockchain technology to achieve data security and simplify Direct Benefit Transfers

1. Introduction

NITI Aayog's task of collecting and aggregating data to quantify Sustainable Development Goals (SDGs) and to provide policy inputs for pertinent issues can be integrated through **blockchain technology**. This integration has the potential to create an ecosystem that will not just provide meaningful results for technology enhancement but will also provide a framework for measuring impact of government policies. While most of the SDGs are dependent on individual as well as institutional data, a separate system can be planned and provided to both the stakeholders to measure SDGs. Blockchain technology will ensure that these data points are not used commercially but only for fulfilling developmental goals. Blockchain is essentially a *distributed*, rather than an integrated ledger system that will eventually enjoin information on monitoring frameworks, which can be utilized for specific pre-decided policy goals and purposes exclusively. This selective usability along with its relative incorruptibility adds to its appeal.

A major predicament in using information for public service delivery is the potential threat to citizens' privacy arising from possible misuse of data being collected. Blockchain technology promises a framework where the data amassed will only be used for a specific purpose set out in the planning phase for a particular policy impactor implementation monitoring. Apart from implementation cost, one possible drawback arises from the fact that the technology is designed as a ledger and hence does not allow for the data to be amended or eliminated once it has gone into the system. Hence there needs to be a sufficiently strong framework for collecting the information so that it does not require future edits.

As such, if blockchain technology is implemented without adequate planning, it can lead to heavy investment without commensurate results. The fact that the system requires highly skilled manpower to set up the automation and strict legalities to govern a space the has hitherto been a domain of tech-evangelizing innovator elites, means that considerable thought and capital has to be devoted in order to reap concomitant benefits. It also needs to be noted here that those in the judicial and executive arms of government may necessarily not be aware of the nitty-gritties of this technology, which makes it all the more imperative to bring about rational regulation in this space swiftly. For this purpose, stakeholders including citizen representatives and tech entrepreneurs need to be brought on board.

Blockchain technology emerged in the wake of the global economic crisis. The World Economic Forum defines blockchain technology (distributed ledger technology) as "*a technological protocol that enables data to be exchanged directly between different contracting parties within a network without the need for intermediaries*." The network participants interact with encrypted identities (anonymously); each transaction is then added to an immutable transaction chain and distributed to all network nodes. As evidenced below, this technology, owing to its potential to curb the middleman economy, presents an enormous prospect to revolutionize industries, business models and public service delivery systems across all sectors.

Definitions aside, the associated aspects of tech-adoption such as stability and robustness need thorough vetting. The real potential blockchain holds is in the plain technology-driven fashion whereby the requisite **trust** and security platform can be developed in order to facilitate efficient business functioning. For many organisations, this trust element is crucial, leading them to favour the exploration of blockchain as a viable solution to data- heavy problems that they meander in. The trust in the blockchain comes from the fact that interactions happen **peer-to-peer**, resulting in validation of each entry at the level of every block, all in a **timestamp server**. Therefore, data recorded is transactional, resulting in the maintenance of records of *what* was disbursed *when*, rather than who received what, available for all the nodes on the network of computers with no consolidated version of the entire database regarded as true and final. This kind of anonymity and decentralised ownership over data provides reprieve for concerns regarding privacy.

The current high energy manual investment and verification (mining) of new transactions due to proof of work usage means blockchain is reaching its limits in terms of **scalability**. Such technological challenges could be overcome in future through higher server and broadband capacities[1]. One of the successful applications of blockchain is smart contract. A smart contract is an agreement between two parties that is stored in the blockchain. Such an agreement may be concluded between two people i.e. peer to peer, person to organisation or person to machine. Yet another, and more popular application is that of the bitcoin. Bitcoin is a cryptocurrency which can be earned through mining and trading in supercomputer servers where blocks are mined and hashed in order to retrieve them at a later stage easily. The steps involved in the process of blockchain can be illustrated using bitcoin as an example.

Transaction	A transaction involves two contracting parties exchanging a given digitally **recordable asset** such as data, contracts or money between them.
Verification	The **transaction** is either executed immediately or transcribed in the protocol and added to the outstanding transactions.
Structure	Each newly verified block receives a numerical code for identification, known as a **hash**, which also contains a reference to the preceding block.
Validation	Each block must be validated before being added to the Blockchain. Blocks in the bitcoin blockchain are validated according to the "proof of work" concept.
Blockchain Mining	The 'proof of work' solution is found by making changes to one variable until the network accepts the solution. This is carried out by **miners**.
The Chain	After being **validated** successfully, the block is added to the chain at each node.
Integrated Protection	The security mechanism makes it impossible for nodes in the network to alter blocks that have already been validated.

[1] https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-blockchain-revolution.pdf , accessed as on 22.11. 2017

2. Scope of Transforming the Public Sector through Blockchain Technology: International Overview

Recent blockchain's benefits—of security, privacy, and speed—are relevant to public sector organizations, and the technology's potential states the need of its usage in government by administrative leaders. Undeniably, experiments through blockchain in the public sector are picking up the pace globally. The ability to record transactions on distributed ledgers offers new approaches for governments to improve transparency, prevent fraud and establish trust. The Deloitte report on Blockchain has classified blockchain's usage in public administration as "high on financial impact and mid-to-high-level on transformational impact."

Blockchain technology has the ability to simplify arrangement and management of trusted information for an easier access to government agencies. Additionally, it has the ability to use critical public-sector data while maintaining the security of this information. As already mentioned, a blockchain is an encoded digital ledger that is stored on multiple computers in a public or private network comprising data records, or "blocks." Once these blocks are collected in a chain, they cannot be changed or deleted by a single actor; instead, they are verified and managed using automation and shared governance protocols.

According to a recent survey conducted by IBM and the Economic Intelligence Unit, government interest in blockchain is high as[2]:

- 9 in 10 Government organisations planning to invest in blockchain for use in financial transaction management, assets management, contract management and regulatory compliance by 2018.
- 7 in 10 Government executives predicting blockchain to significantly disrupt the arena of contract management.
- 14 percent of government organisations expecting to have blockchain in production and at scale in 2017.

In last three years, agencies in more than a dozen countries—including Canada, the United Kingdom, Brazil, Estonia, China, and India—are running pilots, tests, and trials examining both the architecture's broad utility as a basis for government service provision and procurement, as well as developing individual blockchain-based applications for internal use. These applications, often unique to the particular circumstances of a country, state, or municipality, are in development around the world across an expanding range of use cases and asset classes. The technology is being utilised for purposes as varied as record maintaining in healthcare and banking, e-voting, registration and transfer of titles, and most significantly, personal details of individuals.

Core Characteristics	
Shared Data	Need for a structured repository of information
Multiple Parties	More than one entity writes or reads the database. Access may be permissionless ("public"), permissioned ("consortium"), or private
Low Trust	Less than complete trust between the entities (readers, writers, nodes, witness, etc.) in the ecosystem
Auditability	Transactions are immutable- once written; they cannot be modified or deleted. Participants have digital identity on every transaction

[2] https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855, accessed as on 15.11.2017

Value-add Characteristics	
Disinter-mediation	No Central gatekeeper to verify transactions; cost of intermediary may be reduced.
Transaction Interaction	Smart contract code runs on the ledger for interaction, dependency, or "settlement" between transactions from different entities
Auditability	Transactions are immutable- once written; they cannot be modified or deleted. Participants have digital identity on every transaction

Mentioned below are examples of how government around the world are taking the first steps in adopting distributed ledger technology with various blockchain initiatives and pilot projects:

a. The United Kingdom- Blockchain-as-a-Service (BaaS), Welfare Payments

The UK Government's Digital Marketplace has made BaaS available for purchase. With this services at hand, government agencies are free to experiment, build and deploy digital services based on distributed ledger technology. The Department for Work and Pensions in 2016, began a trial to use blockchain technology. Claimants can use a mobile app to receive and spend benefits payments, and with their consent, transactions are recorded on a distributed ledger to support their financial management. UK government's chief scientific adviser Sir Mark Walport has highlighted in a report how blockchain can help in areas such as reducing benefit fraud, protecting critical infrastructure and registering assets.

b. Estonia – Blockchain Identity Management, E- Voting and Electronic Health Records (EHRs)

Currently, Estonia is one of the leading nations in the adoption of blockchain technology. The nation has issued cryptographically secure digital ID card powered by blockchain infrastructure on the back end for its citizens and e-residents, allowing access to various public services. The citizens can verify the integrity of the records held on them in government databases on the blockchain platform. In 2017, NASDAQ, a stock market technology provider, successfully completed a trial in Estonia that enables company shareholders to use a blockchain voting system.

Estonia is also approving blockchain technology to secure the country's 1 million health records. Every update and access to healthcare records is registered on the blockchain, preventing medical fraud and making it impossible for hackers to hide their trail. It also provides real-time alerts to attacks, enabling the government to respond to incidents immediately before large-scale damages occur.

Blockchain-based Electronic Health Records (EHRs)

Numerous industries are examining the potential application of digital contracts. For example, healthcare companies such as Novartis and Pfizer have recognised the added value offered by these contracts. In particular, tests are being conducted on the use of Blockchain –based electronic medical records (EMRs). Personal health records can be stored and managed via the Blockchain in an EMR system. Personal health records are coded as digital assets and stored securely in the Blockchain under a pseudonym (e.g. digital address and not a coded name). Users can allow doctors and other parties to view their medical records as required with their private key. The records might contain information from a fitness tracker, vaccination status, prescriptions, previous treatments, doctors' recommendations and proof of insurance. This anonymised health data will open up new sources of income for ethical and targeted drug development for pharmaceutical companies.

c. Singapore – Blockchain Interbank Payments

The Monetary Authority of Singapore (MAS) has successfully completed a proof-of-concept pilot to explore the use of blockchain for interbank payments. Partnering with a consortium of financial institutions, blockchain infrastructure was used to produce a digital currency issued by MAS and methods were tested to connect bank systems through distributed ledger technology. The technology will simplify the payment process, reduce time taken for transactions, enhance transparency and system resilience as well as reduce the cost of long term record keeping. MAS is looking at this project as the first step in leveraging blockchain to verify and reconcile trade finance invoices, verify the performance of contracts, keep an audit trail and deter money laundering.

d. Dubai – Global Blockchain Council

A Global Blockchain Council has been set up in Dubai to explore current and future application of blockchain technology. The Council currently launched seven blockchain proofs-of-concept trails, covering health records, diamond trade, title transfer, business registration, digital wills, tourism engagement and shipping. IBM has partnered with the Dubai government to try blockchain for trade and logistics solutions. The solution transmits shipment data, allowing key stakeholders to receive real-time information about the state of goods and the status of the shipment, and replaces paper-based contracts with smart contracts.

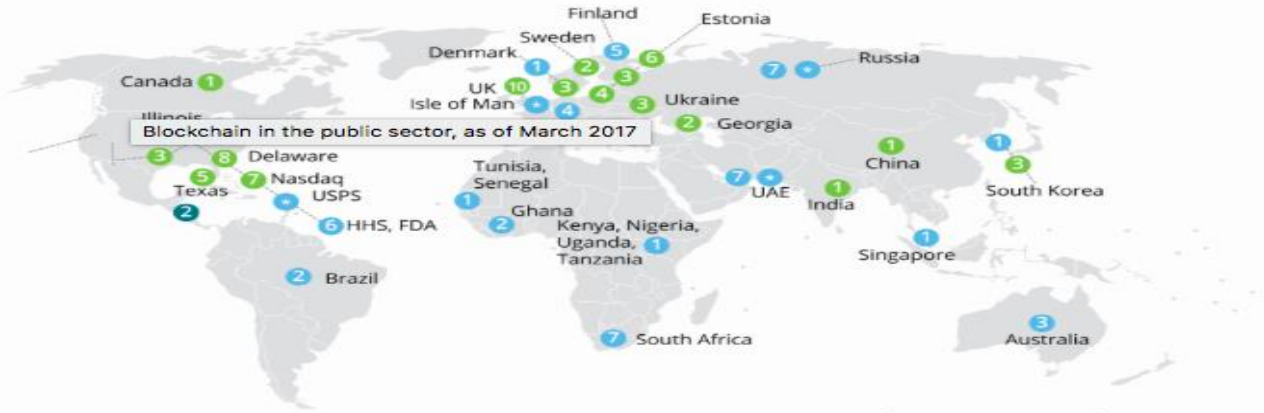
e. Delaware, USA – Smart Blockchain Contracts, Public Archives

In 2016, Delaware became the first US state to embrace distributed ledger technology. Blockchain technology was used to store contracts and other corporate data on a distributed ledger, allowing companies and agencies to store their documents in more than one location. This will keep them more secure and allow automated access by constituents, shareholders and employees. The Delaware Public Archives will be among the first to use the distributed technology to archive and encrypt government archives. The use of blockchain means the documents can be replicated in multiple locations, providing better disaster recovery and saving the cost of off-site physical storage.

Governments and public sector actors are increasingly realising that with the advent of this technology, which is reducing dependence on the existing intermediary institutions and their accompanying layers and costs, blockchain has the potential to eliminate significant resource burden. With a system that is mostly dependent on intermediary entities and/or institutions, Indian Government can dig deep to explore the advantages of this technology. Accelerating transactions and simultaneously lowering their costs, it can help eliminate layers of redundancy, ease regulatory compliance burdens, introduce recordkeeping efficiency and generally smoothen government operation across sectors. Harnessing those advantages and applying them toward public institutions' mission goals provides an opportunity for realizing both agency-specific and whole-of-government benefits that can foster more efficient and

Figure 1. Blockchain in the public sector, as of March 2017

Blockchain experiments in the public sector are accelerating globally, with a concentration in the US and Europe



Top 10 most active public sector use cases*

1. Digital currency/payments
2. Land registration
3. Voting (elections)
4. Identity management
5. Supply chain traceability
6. Health care
7. Voting (proxy)
8. Corporate registration
9. Taxation
10. Entitlements management

* Measured by observing the number of public sector blockchain experiments planned, in progress, or stalled globally

Color coding key
- In progress
- Planned
- Announced

Source: Deloitte analysis in conjunction with the Fletcher School at Tufts University.

Deloitte University Press | dupress.deloitte.com

effective mission delivery in these challenging times.

3. Applying Blockchain Technologies to improve Public Services Delivery: Scope in India

The Indian government has pursued the task of assigning unique identification numbers to each citizen over the past few years in order to develop a centralized database containing granular information about each enrolee down to the level of biometric data. This 12-digit combination called the Aadhaar Number is to act as a digital artefact that will summon this information for multifaceted uses as envisioned by the government. One such use that has been extensively deployed is in Direct Benefit Transfers of subsidies and doles by the Central Government. But the move has attracted many controversies including the fact that such a massive database is also prone to breach, which will have drastic consequences for the security of private citizens. Blockchain tech has potential solutions to both issues- that of achieving transparency in DBT transactions and in protecting sensitive data concerning every citizen of India above the age of five.

Aadhaar enrolment as a process and as a policy has been criticized in some quarters for the perceived lack of security of data collected. It is here that the concept of blockchain can prove to be immensely beneficial. Since it is conceived as a ledger system, blockchain can be an excellent technology design for storing copious amounts of data, anonymized by category. Therefore, the data will be stored in a randomized fashion, not as discrete units, which prevents easy manipulation of the system by vested interests. The Aadhaar ID, when conceived as a cryptographic combination, will act as a key to bringing these seemingly unconnected blocks that pertain to the particular ID together. The blocks of information thus stored will be disjointed and converged by categories, but not by a person's details in the database server. This will pave way for a robust system that may be virtually incorruptible, while simultaneously enabling data collection for the purposes of governance.

The Aadhaar data thus collected, can be deployed for several public service delivery purposes; the government's current efforts in using this data to target public service delivery to those who need it is a case in point. This is presently achieved by triangulating Aadhaar data with perceived income levels validated by the biometric information of the person availing of the service. However, this system still suffers from the issues that plagued its predecessor: while the beneficiaries are being verified, there is no mechanism to ensure that the service have been actually transferred to the needy. Additionally, the services intended for specific beneficiaries are still not being delivered to them in the most optimum manner. Customizing the system to enable tailor-made benefits to be delivered to the intended recipients is a possibility that can be explored in detail using blockchain technology.

The blocks of information collected in a blockchain scheme can be leveraged to assemble disaggregate data into distinct Aadhaar IDs where information pertaining to an individual can be accessed, thus creating a database of Aadhaar IDs that

require specific welfare benefits. While this exercise will seem counterproductive to the aim of the blockchain, appropriate guidelines and restricted utilization of this potential can prove to be immensely constructive. Extending such an endeavour, the system can be built to ascertain if the intended beneficiaries have indeed availed of the facility, or not. Thus, specific personas can be built on the basis of the kind of services provided to them, and this programme, in a limited format, can be extended to other public utilities such as higher education and healthcare. At the very least, this application yields an exhaustive and detailed database, helping to frame appropriate policy as the context demands.

Implementation of Information and Communication Technology (ICT) -enabled healthcare system has been a part of the developmental discourse for a long time. The National Knowledge Commission, through its Report of Working Group on Health Information Network of March 2010, recommended a comprehensive set of measures to be undertaken for implementation of the EHR/EMR system. The report proposed to identification of technology and network infrastructure for integration, and definition of standards for data sharing, protection of data. The report also proposed the creation of a National Health Information Authority (NHIA) as a standardization and regulatory body for ICT in healthcare. Similarly, the High Level Expert Group Report on Universal Health Coverage for India recommended "the adoption of system-wide Electronic Medical Records; which is critical for the health IT network to track and monitor diseases, expenditures and performance to deliver both favourable health and financial outcomes".

Use of Blockchain technology in such a framework would enable faster adoption of an ICT-enabled hospital management system with in-built resilience and integrity of data storage.

So far, the interoperability of medical data among institutions has followed three models:

- **Push**- a payload of medical information is automatically made available to providers, usually by means of encrypted transmissions between sender and receiver. This method is highly secure but at the same time, it requires substantial investment in building the infrastructure surrounding its use and also in the development of a web of legally enforceable obligations for all parties to a transmission. Further, there is no surety of the integrity of the data being transmitted since it does not require a secure and accurate data storage system or a verifiable audit trail on the part of the sender as a prerequisite.
- **Pull**- allows providers access to community-wide, longitudinal patient records. This suffers from the same issues that plague the push system such as the lack of verifiable audit trail, high infrastructure costs, etc.
- **View**- allows any provider to view required data within the system of another provider. This model, yet again, suffers from a lack of standardised approaches to security and integrity.

Blockchain offers an alternative to all three and has the potential to enable secure medical record sharing and provide scalability and uniformity as well. With Blockchain, there is no problem with security, and standardised and verifiable audit trails since it provides an effective and universal set of cryptographic tools to create secure infrastructure. Such cryptographic tools can be used to create discrete blocks of data which are verified by all users in such ecosystem in order to provide:

- Integrity of data at point of sending
- Verifiable audit trail regarding use of such data and any alterations made thereto
- A standardised approach which works to reduce cost of adoption and scaling
- Enables the control of medical records by the individual rather than delegating them to service providers

- Standard forms for interactions that simplify legal obligations between providers and patients.

Consequently, it would be beneficial if India would make adoption and use of Blockchain an integral part of its efforts to develop an ICT enabled healthcare system.

The downside to relying on a peer-to-peer, distributed ledger such as a blockchain is that data, once ratified, cannot be rectified retroactively unless the entire network colludes on the alteration of the subsequent blocks. This makes it a stable mechanism, and is also its greatest advantage. Decentralised consensus thus achieved is the height of democratising ownership over data. All information in a blockchain is distributed, not duplicated, and every transaction is recorded. This feature can find widespread application: for instance, several intermediaries can be eliminated with the implementation of the blockchain. A PDS shopkeeper can, with the assistance of a friendly User Interface, directly receive payment from the government accounts for the quantities of subsidized food items given to the deserving beneficiaries, circumventing cash transfers to the beneficiaries' accounts, which in turn, may or may not be used to purchase food. The beneficiaries are verified by the same database that stores the particular information related to all individuals, which minimises issues related to data imprecisions. The same layout can be applied to maximising financial inclusion such as that aimed by the JAM (Jan-Dhan, Aadhaar, Mobile) Platform.

Large-scale investments such as that piloted by the MAS of Singapore in arraying blockchain for inter-bank transfers are great attempts which yield high dividends, if proven successful. The ICICI Bank was the first lender in India to employ blockchain-based solution innovated by fintech entrepreneur Ripple to facilitate inter-country fund transfers in 2016, by instantaneously transferring credit to their partner bank in Dubai, UAE. The YES Bank followed, by piloting a smart contract application for Bajaj Electricals and its vendors to facilitate easier fund disbursal and discounts. SBI has also proposed implementing of smart contracts to manage KYC over BankChain, a consortium conceived with 28 other member banks in India and abroad, for utilizing the various potentials of blockchain in banking. Most recently, Axis Bank also adopted the blockchain- based solution by Ripple to enable its corporate customers to receive payment from UK and Singapore. These are all instances of niche applications, and the adoption of blockchain to other streams of banking and financial services will take more testing and time.

Initiatives in the direction of implementing welfare schemes better directly tie to the United Nations SDGs, that focus on wholesome development of all in the fronts of malnutrition, healthcare access, housing facilities, drinking water and sanitation, and gender equality. This can be achieved with proper data utilisation trained at personalisation of needs, and can be uniquely applied to the Direct Benefit Transfers (DBTs) scheme that the government is currently pursuing in India. This is premised on the idea that direct cash transfers, instead of providing subsidies, will ensure better services to beneficiaries in a targeted manner. For instance, the SDG to make human settlements resilient, safe and sustainable globally taking cognisance of the environment and associated phenomena, will require pooling of multiple datasets that deal in infrastructure, public works, health records among others. This could be achieved easily via a blockchain integration system, thus yielding a tenable system that caters to a semantic accuracy required of a targeted PDS. Achieving SDGs can be approached in this manner for every goal with select databases put together to work the best solution.

In conclusion, it will be useful to adopt a holistic implementation model by ensuring linkages through Aadhaar to DBTs in a blockchain method, from the inception itself. This will ensure uniformity in approach to the issue and the solution. The existing applications of blockchain in banking and finance institutions in India are based on solutions employed internationally elsewhere, and this is a useful way to approach full integration of the systems. The fact remains that transactions in relatively small volumes in international exchanges of funds alone have been attempted in India so far, and with scaling up, come a number of problems which can be addressed with effective legislations.