AINA

AI and Analytics

Volume 3.0 Edition 2021-2022

Public Policy
Metaverse
Blockchain

Astronomy
Jurisdiction
Language Model

Digital Identity

Application of blockchain in public data

Aritra Sengupta
Deepanjan Saha

India is the largest democracy in the world with the second largest population (Source: World Bank Data, 2022). When it comes to governance, organized digital demographic data is one of the essential components of the modern era of data-driven technologies. Even though the government has initiated several steps to digitalize data, recent incidents of COVID had pointed out the necessity of further robust measures. For example, data related to migratory workers during lockdown, the number of citizens who needed social relief, and data on daily infection and death counts were unorganized initially. In our day-to-day life, we have to bear the nuisance of carrying multiple id-cards for various functionalities. For example PAN for financial identity, Aadhaar card for personal identity, driving license, PPO book for pension holders, health insurance card, and so on. Due to the multitude of information points for a single citizen, it is operationally challenging for the government to monitor or track all those points (the id-cards). At the same time, it is difficult for citizens to maintain such a long list of id-proofs.

Another challenge is data manipulation. Since the different governing bodies work separately, there is no in-place real-time data transfer mechanism among them. As a result, manipulating the personal data in any of these identity documents is an easy task. Several instances of duplicate id-card, fake id-cards, id-card of non-existent persons, etc. emerge frequently. This is a real threat to national security as data manipulation makes it difficult to identify unauthorized citizens.

So can we aggregate all such fragmented data sources from where all necessary information will be embedded and can be retrieved easily? Is there any benefit to that? Is there any potential risk associated? Is it even a feasible idea to implement?

Before we address those questions, one major concern arises about data security. A single point of truth may also become a single point of data breach. Some examples from the past may shed some light on the problems of single-point failure of data security.

Data breach of Bangladesh Central Bank (2016):
A cyber-attack on Bangladesh Central Bank caused an estimated loss of $81 million. Allegedly a hacker group operating from North Korea, named "Lazerus", had launched 35 fraudulent transfers from the bank. On further investigation, it was found that the hacker group exploited the weak data protection of the banking server. A malware was launched on one of the computers when an employee opened a spam email. The entire system was breached from a single node.

Ransomware attack on Colonial Pipeline, US (2021)
A cyber-attack on the Colonial Pipeline, which carries jet fuel and gasoline across the US, had stopped the entire fuel supply. A malware was installed by a hacker group by exploiting a weak password protection system. An undisclosed amount of ransom was demanded which the US government had to pay to the hacker group to regain control over the system.

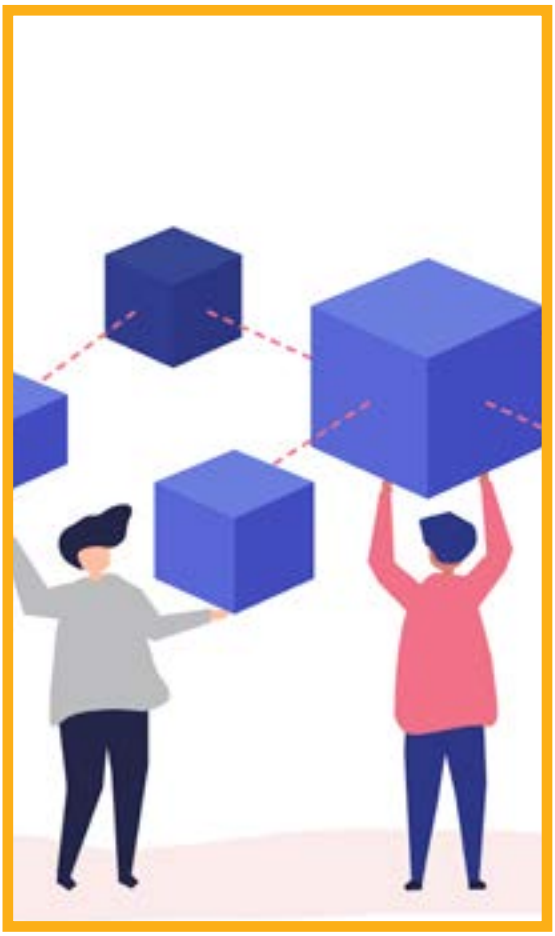
Cyber attack on Maharashtra Electricity Grid (2021):
The electricity grid was hacked using the vulnerabilities of the physical grid network and the power supply was disrupted for a long time. The breach raised questions about the security of India's Critical Infrastructure (CI) amidst growing threat of cyber attacks. The single-point failure of the power grid raised an alarm about cross-border digital warfare.

The Indian Computer Emergency Response Team (CERT-In) reported around 313,000 incidents related to cyber-security in 2019. From Air India to Domino Pizza, almost all major businesses faced data breach related issues in recent times.

There are many such examples across the world. The common pattern in all such events is a single-point failure of a network. It is evident that centralized systems are hackable. Even a centralized system with an over-expensive firewall is susceptible to failure from a single unsecured point (e.g. opening spam e-mail).

We have understood the issue with a centralized system. Now let us look at the decentralized system for possible solutions.

Hackers who hacked the 5500 mile long Colonial Pipeline demanded an undisclosed amount in ransom



The master database of centralized network can be directly accessed through end nodes. The decentralization ensures that data is replicated across multiple nodes, essentially eliminating the concept of master node.

Decentralize the data

A decentralized system is an interconnected information system where no single entity has the sole control or authority. From the point of view of information technology, it is a network of interconnected computers where the information is replicated across all nodes. Hence altering data at some nodes does not affect the integrity of the data as it is available to all other nodes. To manipulate information, all participant nodes have to be hacked simultaneously which is practically impossible. The Internet is a very common example of a decentralized information system.

2008 was a revolutionary time when a breakthrough technology in digital decentralized technology emerged called the blockchain. As we look for a secure data system blockchain appears to be a promising solution. The question is "what blockchain is and how it can solve our purpose?"

Blockchain – The Power of Peers

From a layman's perspective, Blockchain is a way of maintaining (storing and adding but not modifying) data securely. Security is ensured by maintaining multiple copies of the same data in the network. Every person in the network has the latest copy of the data. Updating existing data is extremely hard, only new data can be added and, that too, when a majority of the network (> 51%) provides consensus to it. The algorithm using which majority of nodes reach consensus is called Byzantine Fault Tolerance. So, even if few systems are breached, the peers will reach consensus to reject the modification.

The design and implementation of blockchain are built on many strong mathematical models. For example, decentralized systems need communication between nodes which is accomplished using Peer to peer (P2P) network. Also, Blockchain is claimed to be extremely secure. A block contains data along with the hash value (a unique alphanumeric key) of the previous block. A hash value is unique for the data inside the block. Since the blocks are linked together (thus the name blockchain) via hash values, the tiniest change in one block will change the hash of the block completely, and this will affect all the subsequent blocks. To tamper with data in a block, one has to re-compute hash values of current and all other subsequent blocks which is nearly impossible due to Proof of Work mechanism.

Also, when we are talking about decentralizing public data, identity protection is a fundamental requirement. Cryptography helps in maintaining the anonymity of the user's data by masking sensitive information. A combination of cryptography on top of blockchain prepares the ideal foundation for public data systems.

Before we think of implementing similar technology in India, we should investigate "Has any country in the World applied the technology in governance?" A Baltic country has an astonishing use case as follows:

Estonia – Way ahead in times

Estonia is located in Northern Europe which, in recent times, is known for being one of the most digitally advanced societies. It has internet coverage across the entire country. Even before bitcoin's first white paper was released in 2008, Estonia was already testing blockchain technology under the name 'hash-linked time-stamping'. But the most relevant use case is the digital identity program which addresses the multiple id-card issues.

The digital identity program of Estonia:

Estonia has successfully digitalized its identity-related documents. Internet connectivity across the country makes it easier to avail digital facilities. Under the concept of digital identity, there are various services available for the citizens:

Digital ID
The digital ID issued by the state to its citizens serves various purposes like banking-related proof of identity, health insurance ID, travel ID across the EU, digital signature, voter ID, to avail e-Prescription, etc. One single ID substitutes multiple IDs. between different departments becomes much more easier.

X-Road
It is a decentralized and secure information exchange system where the data can be shared easily between different organizations and information systems. Any member of the X-road system can access data. Hence information sharing between different departments becomes easier and a single document is sufficient for all such proof related purposes.

KSI Blockchain – Data protection:
Estonia has implemented blockchain technology to secure public data. Guardtime, a private company, has designed Keyless Signature Infrastructure (KSI) blockchain technology which is adopted by the government. The KSI system is so secure that it is even used by NATO. A tricky solution is implemented to add an extra layer of protection. They started publishing the blocks in the Financial Times newspaper. So, even if someone manages to modify the blockchain network, one also has to change all the previous hard copies of newspapers published across the nation to date. Healthcare Registry, Property Registry, Business Registry, Succession Registry, Digital Court System, and State Gazette are a few of the State registries which are now backed by the KSI blockchain.To address the data privacy problem in a decentralized network, the KSI blockchain only stores the hash value of the data and not the actual data.

So far, blockchain service in governance is successful in Estonia. It is estimated that digital signature saves 5 days of work per year due to fast approval. As per government reports, an estimated 1400 years of job hours are saved due to the implementation of blockchain-based digital identity.

Estonia is at present is one of the most digitally advanced country. The government is able to scale the technology for its citizens due to omnipresence of internet connectivity. The Estonia model provides an opportunity to study the use case of blockchain on a scalable size.

A second interesting application of blockchain has been adopted by another EU nation to solve an age-old problem. Let us explore Finland's example.

Finland's digital card to aid immigrants

Immigrants often take refuge without valid documentation. Also, information related to their birth, education, previous employment, etc. is seldom available. This makes it difficult for them to open a bank account, apply for government jobs or get admission to schools/universities. To help them on board, the government has to provide aid until they are financially stable. It was very difficult for the government to track how these aids were being spent by the immigrants. There were instances of aid misuse. In 2015, The Finnish Immigration Service Migri launched a pilot project in collaboration with a start-up MONI to provide a digital solution for aid services. The aids are provided through a prepaid Mastercard which is linked with their digital ID card. Ethereum-based blockchain technology is used to record all transactions through the card. Hence, the money trail can easily be followed. Since the system is protected by blockchain and backed by the government, it helps migrants to use it as valid identification proof and get jobs easily.

These examples indicate a potential future of blockchain in the public domain. Now let us answer how blockchain can be used in the Indian scenario.

The Indian Context – a practical use case

Data is abundant in India when we talk about nearly 1.38 billion people. But most of them are currently fragmented and unorganized. Hence, blockchain-based digital data network has many practical applications in the Indian ecosystem. The digitalization spree in India is at full pace for the last few years. With the 5G network appearing soon, we are in the best position to leap forward in digitalization. We can integrate several ID cards into a single one for the convenience of both government and users. Illegal immigration has been a challenge for Indian borders where fraudulent certificates are used to bypass security officials. Once a ledger-based identity system is used, it will be very difficult to forge the identity data. A significant amount of time in documentation and verification can be saved using technologies like X-Road where information will be seamlessly shared across various departments. Considering the amount of time being invested in multiple levels of verification in different government procedures like legislation, licensing, criminal record tracking, financial history, and others, efficient implementation can save us a lot of resources. These implementations will need an extremely secure network for which blockchain is a promising solution. People will trust the system if data protection is ensured. From the Estonia case study, it is evident that blockchain is trusted at the public level.

So far we have highlighted the opportunities and benefits of using a blockchain-based decentralized identity system. But to implement such a system in India, there is more than what meets the eye.

Data related to labour migration is mostly unstructured in India

The Challenge of scale

Internet connectivity:
Compared to Estonia (89%), only 43% of the Indian population have internet access. Even though India has the second highest number of internet users, the rural penetration is only 37% so far. To implement a model like Estonia, first, we need to have scalable internet accessibility in the coming years.

Technological literacy:
Citizens must be aware of the know-how of using digital ID technology. They have to trust the system. The transition from the present multiple ID cards to a single digital ID will need psychological acceptance from the mass. The digital payment system in India is well accepted which indicates the agility of the population for technology.

Backward compatibility:
The decentralization of public data will take time. Some will migrate to newer technology while others will still be in the transition phase. So all institutional bodies have to work with both kinds of identification documents for some time which may cause some level of discomfort. Hence, the transition has to be done rapidly.

Data Aggregation:
Data from various independent institutions have to be aggregated in a single network. Considering the variety, complexity, and size of such data, aggregation is a challenging task. Data from the ministry of health have to be integrated with data from the ministry of finance and so on.

Manpower requirement:
A large pool of skilled professionals with expertise in blockchain technology will be required in the drive to build a nationwide information network. The expertise is limited due to development in the technology.

These challenges are impeding us from adopting blockchain in public data. Owing to the size of the Indian population, adopting new technology at the mass level is always a complex task. But slow and steady improvements can build the necessary foundation. UPI is one of the most successful digitalization drives. There are several initiatives where blockchain technology is already implemented but at a relatively lower scale.

Blockchain in India's current digital ecosystem:

India is slowly adopting blockchain into its existing ecosystems. National Informatics Centre (NIC) is a government body under the Ministry of Electronics and Information Technology (MeitY). The Centre of Excellence for Blockchain Technology (CoE BCT) is a gateway for the development and testing of the projects undertaken by NIC. The various government department can develop and host apps or services built on top of blockchain using CoE BCT's blockchain as a service (BaaS). There are a few more initiatives as well:

Digital Education Certificate:
The process of academic document verification is time-consuming and laborious. Many organizations either outsource the work which adds cost. Also, forgery in qualification-related documents happens very frequently. To solve those issues, NIC provided a solution using BCT called Certificate Chain. Institutes can now directly upload certificates to the blockchain where they will be tampering-proof and available to all peer networks simultaneously. Karnataka Secondary Education Examination Board and Karnataka Pre-University Education Examination Board have participated in this program.

Similarly, the Central Board of Secondary Education (CBSE) has deployed a blockchain-based marksheet distribution system where the marksheets for grades X and XII of the academic year 2019, 2020, and 2021 are published in a blockchain network. Marksheets of previous batches are also being appended to the system.

Drugs Logistics in Karnataka:

The Government of Karnataka supplies 700 to 800 types of drugs, purchased from over 400 suppliers worth Rs.300 crores to 2911 hospitals across the state for free medication for needy people. They have integrated blockchain technology in the supply chain network to immutably record all transactions.

Many initiatives are being taken by NIC in the domain of the Public Distribution Systems, Land Records, Digidhan dashboard, and many more. All of these initiatives incorporate blockchain in some form or other. Even state governments have taken initiatives to integrate blockchain into their existing systems. For example, the Maharashtra government's Disaster Management Department, in partnership with start-up Print2Block, started issuing Covid-19 test certificates to citizens who tested negative. They have deployed a private blockchain to store these certificates.

The road ahead:

We have discussed the applicability of blockchain in public data. We have also seen the challenges to be overcome. As per the Office of Principal Scientific Advisor of the Government of India, "integrity of information" is the highest priority. It is undeniable that implementing the same in India is a challenging job. But different blockchain-based applications in public sectors are already in place. The path forward will be to find out the solutions for effectively scaling the technology. Higher coverage of high-speed internet, digital literacy among citizens, government backing for technology, industrial support in large-scale infrastructure development, and strategic investments are the key requirements for bringing up such a robust solution. But the benefits are superior to the costs. Learning from the experience of countries that have successfully implemented blockchain in public data, we can create our digital ecosystem in the near future.