Aadhaar 2.0: Blockchain Technology in UIDAI

Overview:

With the advent of Digital India, there has been an impetus towards enabling digital service delivery of government, private and public services to citizens. Aadhaar (UIDAI) based Authentication, eKYC, and eSign have enabled the service providers to onboard users in a seamless manner. All these systems require a mechanism for obtaining and preserving user consent to operate effectively and securely. It also needs a Hyper fundamental solution for UIDAI as it has world's largest biometric database(i.e 1.28 Billions). The concern for Aadhaar 2.0 would be incorporating Decentralized Artificial Intelligence Technology. The ground step would be to merge the Blockchain technology to the exiting Aadhaar system.

Guiding principles for the sharing of user data across different services with user consent have been previously outlined in two key policy documents: namely, the "***Policy on Open Application Programming Interfaces (APIs) for the Government of India***" published by the *Ministry of Electronics and Information Technology (MeitY)* ,and the "***National Data Sharing and Accessibility Policy (NDSAP) - 2012***" by *the Department of Science & Technology.* The IT Act also requires that any entity sharing user data that is sensitive in nature must collect user consent from the user prior to such sharing. There is a requirement for a comprehensive technology framework to enable effective and secure implementation of the aforementioned policies with respect to user consent management.

The technology framework outlined in this document is designed to be open, secure, user-centric, and application-agnostic. Using this framework, data consumers (like Govt departments, employers, lenders, etc.) can access data of users from providers (like Govt departments, banks, etc.) using electronic consent, rather than requiring users to share credentials like passwords or to sign paper documents.

To intrude the vulnerability of the data and making the system more seamlessly secure, robust and make the public services more accesable in contributing the growth of the nation.

CONTENTS

BLOCKCHAIN TECHNOLOGY | **AADHAAR** | GOVT. OF INDIA

1. What is Blockchain Technology and How is it can/may relate to UIDAI ?
2. How does blockchain work ?
3. How is blockchain used in UIDAI?
4. Why should blockchain technology be trusted ?
5. What makes blockchain technology so robust ?
6. What is the difference between blockchain and Bitcoin ?
7. Who controls blockchain ?
8. Blockchain-based crypto money frauds are common. So how can a state trust and use blockchain to protect the private data of its citizens?
9. Can you provide any examples of blockchain technology actually being useful in protecting important the data of some state or important company ?
10. What happens if a blockchain company goes bankrupt, how is data protection assured then?
11. How does blockchain technology contribute to the well-being of a layman ?
12. How quickly can the misuse of data be detected using blockchain technology ?
13. What are the services that are accessible with blockchain incorporation ?
14. List of the emerging outcome and future-proof.
15. Government of India’s existing opinions/views/actions.

1. What is Blockchain Technology and How is it can/may relate to UIDAI ?

The blockchain is a mathematically ensured cyber security technology for rapid and immutable identity cation of Modifications in digital data and intelligent devices. Blockchain technology makes it possible to discover any and all changes made to digital data, no matter how small, no matter by whom, immediately and with zero error. Blockchain has only become a hot topic in recent years. The simplified approach of calling this technology would be “hash-linked time-stamping”.

Since UIDAI launched in 2009, It has 1.23 Billion (world’s largest biometic database) users data and by linking up this technology on the backend the incorporation would be more benefited to the National user in order to protect national data, e-services, and smart devices both in the public and private sector.

2. How does blockchain work ?

One way to look at the blockchain technology is to view it as a “Digital Transaction linked-list” that covers all the data and smart devices that need to be protected from corruption and misuse.

- Every change in data can be instantly detected based on traces left in the pattern of the “Digital Transaction linked-list” that covers the data
- Blocks of “Digital Transaction linked-list” are connected to each other and make up a chain that is distributed millions of computers all over the world, which makes it impossible to change data so that nobody knows –the chain instantly reacts all changes that mismatch the mathematical code in the chain

This way millions of lives and resources are saved, while the potential manipulation of sensitive data (such as health data, intelligence information, legislation-related records, etc.) or smart devices (such as military machinery, hospital equipment, intelligent cars etc.) is prevented or instantly detected.

3. How is blockchain used in Aadhaar 2.0?

Aadhar 2.0 would be more benefited by the data registries, such as the national health, judicial, legislative, security and commercial code systems, with plans to extend its use to other spheres such as personalized medicine, cyber-security, and data embassies.

"I would call it Aadhaar Version 2.0. Aadhaar has to be re-architectured to become a solidly reliable part of the digital governance ecosystem."
- Rajeev Chandrasekhar, MP, an UIDAI critic.

The technology behind this digital infrastructure would be incredibly impressive. The Public Key Infrastructure (PKI) and eID system are based on advanced encryption technology. Data will be decentralized and encrypted, yet never duplicated and always shared securely. We should address these design flaws. Make sure that privacy is an important issue that is addressed, that your data is never misused.

The issue of citizenship should be addressed at least in version 2.0. If you can't identify between a citizen and a non-citizen, then what is the use of Aadhaar?

4. Why should blockchain technology be trusted ?

No data is ever stored on a Blockchain - instead, blockchain works like a speed camera that detects who has violated the law, when and how. Due to the fact that data, protected by blockchain technology, is covered with the "Digital Transaction linked-list", every change in the data can be detected because it leaves a trace in the pattern.

It's an Open Decentralized Encrypted Database, any misconducted, misuse or any ill-usage activity by the intruder would be traced and recorded.

5. What makes blockchain technology so robust ?

Mainstream Potential of this technology is its scalability. This means that even large amounts of data can be covered with "Digital Transaction linked-list" since the parts of the linked-list (blocks) are connected to each other using a mathematically very able code that connects the blocks into a chain, which cannot be changed without leaving a trace behind.

6. What is the difference between blockchain and Bitcoin ?

"*Blockchain*" and "*Bitcoin*" are two separate terms and should not be confused. While blockchain is a technological concept, Bitcoin is one of the use cases for a particular type of a blockchain technology. Bitcoin was launched as a type of unregulated digital currency. The value of the digital currency may vary (increase or decrease), whereas the value of the data covered with "Digital Transaction linked-list" does not change and this very fact makes the data even more valuable.

7. Who controls blockchain ?

The chain of blocks of "Digital Transaction linked-list" (aka block-chain) reaches a great number of computers all over the world, and can therefore be controlled and verified by great number of parties. The blockchain is, after all, just an internet-hosted network which stores information as a shared/open database.

That means the information isn't stored in a single location and no centralized version exists for a hacker to corrupt, making it safe to use. Some blockchain vendors - like Guardtime, a company behind the KSI blockchain- have gone even beyond that, and publish the blockchain also in the physical media, like the Financial Times newspaper. If someone would want to manipulate the KSI blockchain without anyone noticing, they would not only have to deal with the "Digital Transaction linked-list" in the electronic domain but also replace tens of thousands of copies of newspapers in the world's libraries. It is clear that no-one - not even Guardtime itself - is able to do that, and therefore the data on the blockchain can be considered immutable.

As a result, while it today takes on average about 7months to discover the breach or misuse of an organization's data, the blockchain helps to discover such threats instantly.

8. Blockchain-based crypto money frauds are common. So how can a state trust and use blockchain to protect the private data of its citizens?

When dealing with any sensitive data, it is obvious that this data should not be kept on the blockchain - after all, blockchain relies on a large number of eyes to keep it secure! Instead, in order to secure sensitive data, what's kept on the blockchain are the “hash values” - essentially digital fingerprints of the original data. Just like your own fingerprints uniquely represent you, but don’t tell anything about your race, eye color or thoughts, the same applies to digital fingerprints - while uniquely representing the original data, it is impossible to know anything about the data itself based on the “hash values”.Therefore - it does not matter if anyone gets their hands on the blockchain - there is absolutely no original data there to be compromised!

9. Can you provide any examples of blockchain technology actually being useful in protecting important the data of some state or important company ?

- Millions of lives and resources are saved as the potential manipulation of defense data or smart war machines is prevented using blockchain technology.
- In order to keep health information completely secure and at the same time accessible to authorized individuals, the electronic ID-card system used by the Estonian e-Health Record uses blockchain technology to ensure data integrity and mitigate internal threats to the data. In this way every occurrence of data use and misuse is detectable and major damages to a person’s health can be prevented (such as the wrong medicine or the wrong dose).
- The Estonian KSI Blockchain technology protects Estonian e-services such as the e-Health Record, e-Prescription database, e-Law and e-Court systems,e-Police data, e-Banking, e-Business Register and e-Land Registry.

The same KSI Blockchain technology is used by the NATO Cooperative Cyber Defence Centre of Excellence, European Union IT Agency, US defense department and also by Lockheed Martin, Ericsson and others.

10. What happens if a blockchain company goes bankrupt, how is data protection assured then?

The company itself can NEVER see the actual data that is protected, it only provides the "Digital Transaction linked-list" solution that can ensure its integrity and mitigate internal threats. So nothing happens when a blockchain company disappears, all the data protected will remain very able for its integrity for forever based on the shared blockchain, and if applicable for a particular blockchain technology, also based on the physical publication of the blockchain in the world's newspapers.

11. How does blockchain technology contribute to the well-being of a layman ?

Blockchain technology helps to ensure that data concerning the person is not misused.
For example:

- Blockchain technology helps detect who looks at a person's digital health data and changes it and when;
- Blockchain technology helps to see when information about a company in the e-Business Register was changed and why;
- Blockchain technology helps to detect who changed data about real estate in the e-Land register or statements documented in the e-Court system as well as when and how;
- Blockchain technology helps to ensure that no one has manipulated smart devices such as intelligent transportation or smart war machines that could become life-threatening.

12. How quickly can the misuse of data be detected using blockchain technology?

According to the research by FireEye, one of the leading cyber security vendors in the world today, it currently takes organizations on average of about 7 months to detect breaches and manipulations of electronic data. With blockchain solution like the one Estonia is using, these breaches and manipulations can be detected immediately.

13. What are the services that are accessible with blockchain incorporation ?

- **e-Governance** is a strategic choice for Digital India to improve the competitiveness of the state and increase the well-being of its people, while implementing hassle free governance. Citizens can select e-solutions from among a range of public services at a time and place convenient to them, Many public services are now available to citizens as e-services. In most cases there is no need to physically attend the agency providing the service. The efficiency of e-Government is most clearly expressed in terms of the working time ordinary people and officials save, which would otherwise be spent on bureaucracy and document handling.
- **e-Tax** Modern e-solutions have made setting up and running a business in India quick and easy. e-solutions for business, such as electronic tax claims, have pared bureaucracy down to a bare minimum and facilitated an environment where business is extremely convenient.
- **Digital ID** Nearly every one of India's 1.23 Billion biometic citizens has an ID card, which is much more than simply a legal photo ID. Technically, it is a mandatory national card with a chip that carries embedded files, and using 2048-bit public key encryption, it can function as definitive proof of ID in an electronic environment.
- **Public Safety** The introduction of IT could helped to strengthen public order in INDIA and assist in the case of accidents. The use of IT tools in the security services (e-Police, rescue board, emergency centre) could halved the number of deaths by accident. The other issues like theif, crimes, could be addressed.
- **e-Health** Blockchain technology solves many of the problems that data governance professionals have been trying to solve for years.Patients own their health data and hospitals can made this available online. The data generated by hospitals and doctors can been digitized, and blockchain technology can be used for assuring the integrity of stored electronic medical records as well as system access logs. e-Health solutions can allow India to offer more efficient preventative measures, increasing the awareness of patients and also saving billions of euros.
- **Interoperability services** e-Land Register, Population Registry, Moblity Regresity, e-busineess regestry and many paperless federail work can be incorporated.

Ambitious future

- **New Digital Nation:** e-Residency is building a new digital nation for citizens of the world where no one is held back from their entrepreneurial potential because of where they live or where they choose to travel. This has enormous potential for unlocking global growth by democratising access to entrepreneurship and e-commerce.
- **Cyber Security:** Increased cybercrime and politically motivated attacks on electronic services mean cyber security is more important than ever for both the private and the public sector. This comended preparedness to handle cyber crises has significantly increased over the past decade. The country has created intrusion detection and protection systems, practised cooperation with both public and private institutions, significantly contributed to the awareness of users, and is participating in intensive international cooperation.
- **Intellgent Transporation:** An innovation leader in IT with electronic identity cards, i-Voting and e-Residency. We can work upon an important step when the government made it legal to test self-driving vehicles on all national and local roads. The self-driving technology helps improve road safety and road use efficiency. Apart from the various modes of transpoarion could be more secured and inturder dectable.
- **Smart Policy Framework:** Blockchain is still relatively new technology so entrepreneurs and their customers are often either faced with the uncertainty of operating in legal grey areas or are being constrained by existing legislation. Far from hampering the development of blockchain technology, a smart policy framework could both encourage entrepreneurial activity and provide greater consumer protections. For example, we have the technology to monitor who is accessing our data, conduct e-voting or digitally sign documents, but those things are useless without the policy framework to ensure improper access of our data is punished, e-votes are counted and digitally signed agreements are legally binding.
- Clearer policy frameworks around blockchain are now on the way globally too, including regulations that will require stronger KYC (know your customer) procedures to reduce risk and protect the public interest from challenges like money laundering. Unfortunately, this could also increase costs for blockchain startups or limit their products and services to certain markets.

14. List of the emerging outcome and future-proof.

- **Smart contracts :** Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met.
- **The sharing economy:** By enabling peer-to-peer payments, the blockchain opens the door to direct interaction between parties — a truly decentralized sharing economy results.
- **Crowd-funding:** Blockchains take this interest to the next level, potentially creating crowd-sourced venture capital funds.
- **Governance:** By making the results fully transparent and publically accessible, distributed database technology could bring full transparency to elections or any other kind of poll taking.
- **Supply chain auditing:** Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with blockchain-based timestamping of a date and location — on ethical diamonds, for instance — that corresponds to a product number.
- **File storage:** Decentralizing file storage on the internet brings clear benefits. Distributing data throughout the network protects files from getting hacked or lost.
- **Prediction markets:** Prediction markets that payout according to event outcomes are already active. Blockchains are a "wisdom of the crowd" technology that will no doubt find other applications in the years to come.
- **Protection of Intellectual Property:** Smart contracts can protect copyright and automate the sale of creative works online, eliminating the risk of file copying and redistribution.
- **Internet of Things (loT):** Smart contracts make the automation of remote systems management possible. A combination of software, sensors, and the network facilitates an exchange of data between objects and mechanisms.
- **Neighbourhood Microgrids:** Blockchain technology enables the buying and selling of the renewable energy generated by neighborhood microgrids.
- **Identity management:** Distributed ledgers offer enhanced methods for proving who you are, along with the possibility to digitize personal documents. Having a secure identity will also be important for online interactions — for instance, in the sharing economy.
- **AML and KYC:** Anti-money laundering (AML) and know your customer (KYC) practices have a strong potential for being adapted to the blockchain. Currently, financial institutions must perform a labor-intensive multi-step process for each new customer. KYC costs could be reduced through cross-institution client verification, and at the same time increase monitoring and analysis effectiveness.

- **Data management:** In the future, users will have the ability to manage and sell the data their online activity generates. Because it can be easily distributed in small fractional amounts, Bitcoin — or something like it.
- **Land title registration:** AsPublicly-accessible ledgers, blockchains can make all kinds of record-keeping more efficient. Property titles are a case in point. They tend to be susceptible to fraud, as well as costly and labor-intensive to administer.
- **Stock trading** When executed peer-to-peer, trade confirmations become almost instantaneous. This means intermediaries — such as the clearing house, auditors, and custodians — get removed from the process.

15. Government of India's existing opinions/views/actions.

In the Right to Privacy judgment, Justice Chandrachud gives an exhaustive account of the complications of data protection in the digital age. While some of these issues are brought about by characteristics that are inherent to the nature of information, others concern the nature of user experience on the internet. With regard to information, he states that information is nonrivalrous which means that multiple individuals can use it or access it at the same time. Further, he points out that a lot of the data that is available is inconspicuous, which makes it hard to identify when privacy has indeed been invaded. Moreover, he states that it is "recombinant" which means that information can be resynthesized to create more information. Additionally, he points out that individuals, through the course of their online activities, volunteer more information about themselves than they may be aware of.The judgment concludes that data protection regulation, then, must do three key things.

First, it must safeguard matters where there is a "reasonable expectation of privacy" such as personal medical reports. Second, it must go beyond the personal privacy and also protect individual autonomy. Third, it must also ensure that there is no discrimination in terms of race, political leanings, faith, mental or physical health, or sexual preference when data is collected.

What can be gleaned from these conditions is that an individual's personal data must be taken with his consent and that this must be done in a way that is transparent. The Government has responded to this challenge with a proposal for a comprehensive data protection bill, a draft of which slated to be ready sometime in December.

As it currently stands, Aadhar does not adequately safeguard personal information and therefore fails to meet the conditions set down in the Right to Privacy judgment. A report by the Indian Institute of Technology, Delhi revealed that the current Aadhar system is open to attack both from external as well as internal sources as it stores information on a centralized database. If the database is compromised in any way, either by an internal leak or an external hack, the information on it can be used for authentication. The report also argues that biometric information is not a great security measure as it can easily be extracted from the public domain such as a fingerprint which can be lifted from anything someone touches. Linking Aadhar to bank accounts, PAN numbers, and phones, then, exposes an individual's entire existence to a substantial amount of risk.

A blockchain-based Aadhar would help the database match the data protection stipulations outlined in the Right to Privacy judgment. It would allow for information to be collected and held transparently, with the consent of the individual whose information it is. Additionally, it would virtually do away with the concerns about storing biometric data in a centralized database. A blockchain based Aadhar identity system, then, would allow the Government to meet its purported goals for the Aadhar without compromising the security of individual's information. Though a blockchain-based Aadhar has been suggested before, concerns about operationalizing a scheme of this magnitude have not been adequately brought out.

First, given the immense cost and scale of the Aadhar project, would it be economically feasible to change Aadhar's technical architecture this late in the game? Second, as blockchains are a complex and energy-intensive technology to deploy, does UIDAI have the bandwidth for a system like this? Third, there may be issues with technology compatibility, and it might be altogether impossible to integrate blockchains with the current Aadhar database. Fourth, it might be difficult to onboard individuals and get them to trust the technology, given the unfortunate publicity blockchains has received for its connections with the nefarious Silk Road network. Fifth, in the case of private blockchains, where all the nodes know one another, there lies a significant risk of nodal collusion.

These are questions that must be answered before looking seriously to blockchains to solve the issues with Aadhar. However, with this in mind, it is also imperative for the Government to go beyond the bill of legislative acts if it wants to bolster confidence in the Aadhar program and realise its vision of a truly digital India.