IMPACT OF BLOCKCHAIN ON DIGITAL IDENTITY

BUILDING TRUST IN THE CYBERWORLD

Background

The fourth industrial revolution or Industry 4.0 has the world gearing up for intelligent and autonomous systems driven by data and Machine Learning. As technology becomes more intertwined with cyber-physical systems, data privacy and digital identity in the cyber world has gained paramount importance. In this digital age, when consumers are increasingly embracing the Internet to perform online transactions—both for buying goods and services as well for banking—and across multiple devices, the concept of “Digital Identity” comes to the forefront. The International Telecommunications Union defines Digital Identity as “a digital representation of the information known about a specific individual, group or organization”. Digital identity consists of all of the individual’s personal data that is available online. It can be all encompassing — not just an e-mail or physical address, but also pictures, bank account information,
shopping preferences and also physical identity information. This identity is not uniform, and can vary across platforms like banking systems, telecom and social media platforms, including Facebook and LinkedIn, among others.

Digital identity is a convergence of offline and online identities, where the latter refer to those stored or used by computer systems and embedded software (IoT). A digital identity can be assigned to an individual, a legal entity or companies and even assets.

Across the world, many organizations and nations have rung alarm bells on identity theft and are reiterating the importance of protecting “digital identity”.

The objective of this paper is to discuss the importance of digital identity, as well as to explore how blockchain can help protect this sensitive information.

**Why is Digital Identity important?**

A crucial aspect of online financial transactions, Digital Identity ensures accuracy while expediting

**Digital Identity Management Aims**

To standardize and streamline citizen services provided by nations. Hence, a strong digital identity platform can help deliver multiple services, touching our lives in various ways.

**Blockchain Solutions are Increasingly being Explored**, given their inherent characteristics of engendering trust and transparency and user control all key factors for digital identity management.
the customer on-boarding process and preventing Anti Money Laundering (AML) and fraudulent activities. Digital identity Management aims to standardize and streamline citizen services provided by nations. Hence, a strong digital identity platform can help deliver multiple services, touching our lives in various ways as depicted in the graphic (Figure 2).

An important area where digital identity is being leveraged to truly bring about social transformation and economic upliftment of communities is in the delivery of citizen welfare measures and some examples include:

• The National Digital Identity (NDI) system, a part of the Smart Nation initiative in Singapore, which when completed is expected to help citizens with access to e-government services more securely.

• In India, more than 1 billion Indians today have an Aadhaar ID, a digital identity that is getting linked to all the social schemes and has transformed the way subsidies are being paid out to economically weaker sections of society.

• Smart cards were issued as early as 2014 in Nigeria, enhancing security and public services in the country.

• Kenya followed suit with a digital ID that has also reduced social crimes.

The responsible use of digital identity is not only about authentication, but also its capture in a tamper-proof form that can be securely transmitted and used by multiple systems on a need basis.

**Regulatory Angle to Identity Protection**

General Data Protection Regulation (GDPR), an EU wide mandate that went operational on May 25, 2018, aims to strengthen protection measures impacting EU citizens’ personal data and privacy, and lays down rules covering aspects such as processing of and restricting the free movement of personal data. It also addresses considerations related to export of personal data outside the EU. A whole set of data subject rights including the “Right to be forgotten” are in the gamut of this regulation. Needless to say, any breach of data privacy will be treated severely with large penalties. Data authentication, encryption and pseudonymization are all part of its ramparts, thus reiterating the importance of protection of Identity information.

Similarly in the USA, the California Consumer Privacy Act, A.B. 375 provides residents with equivalent provisions for data privacy and identity protection.

In South Africa, the Protection of Personal Information Act (PoPI), covers the data protection rights of subjects and puts forth conditions for its usage once collected from customers. It also impacts the technical, process and operational aspects related to access of personal data and identity information.

Data privacy and the need for digital identity protection is therefore resonating with law makers in multiple continents.

**Digital Identity Management – Leveraging the power of blockchain**

Starting from plain vanilla guidelines of security such as using a complex password to deploying cutting-edge technologies such as Biometrics, Machine Learning and Robotic Process Automation, multiple methods are being evaluated for digital identity protection.

Effective though they are, when applied on a Centralized Digital Identity Management system, these solutions prove costly and sometimes not as effective. One of the main drawbacks of such a centralized system is that the control of data remains with one entity. Tampering with and the loss of data is easy, with identification taking time. Estimates peg identification of data breaches to seven months. And, this is where blockchain solutions are increasingly being explored, given their inherent characteristics of engendering trust and transparency and user control, all key factors for digital identity management. The 5 pillars of a blockchain based solution for digital identity are:

• **Trust** - In blockchain-based systems, the metadata used for communications is maintained in the distributed ledger. The authenticity of the data is verified through multiple nodes, through a consensus mechanism. This decentralization is useful in the context of Digital Identities, especially when National Identifiers are used across multiple agencies.

• **Security** - Blockchain technology has been designed to maintain data in an encrypted and immutable manner, and secured through cryptography, thereby, keeping the ID protected and traceable. Moreover, blockchain based systems removes the vulnerability associated with password protection.
Impact of Blockchain on Digital Identity

• **Integrity** - The advantage of this kind of identity system over traditional ones is the ability to maintain each identity across all the nodes in the network. Though the data is distributed across peer-to-peer networks, it is continuously reconciled and kept up to date. Also, the blockchain network does not have a single point of failure, making it difficult for hackers to break the integrity of the data set.

• **Simplicity** - A blockchain framework simplifies the process for each stakeholder involved:
  - **Identity issuers**: Automation of the issuance of digital identity – reduces time and manual interventions.
  - **Identity verifiers**: Customer onboarding and data verification is simpler and cost effective.
  - **Identity Owners**: Blockchain moves away from centralized data management, giving users control over their identity. It is also possible for users to create their own identity data for social media/payment transactions. This is referred to as a “Self-Sovereign Digital Identity”.

• **Privacy** - Regulators across the world are clamoring for privacy of citizen’s personal and sensitive information. Blockchain encryption combined with the digital signature ensures “Privacy by Design” through pseudonymization. Affixing the digital signature to all transactions carried out by the user makes it foolproof as well.

Permissioned blockchain systems where government organizations maintain digital identities seamlessly are emerging as the platform of choice across countries. A few real life examples of how blockchain technology is being used for Digital Identity Management are:

• Since 2012, blockchain has been used in Estonia to maintain national data and services both in the public and private sector. Estonia maintains the multi-purpose digital ID card on blockchain and makes sure that every change in data is immediately detected based on audit trails left by the “digital defense dust” that covers it.

• The city of Zug in Switzerland is exploring a self-sovereign government issued identity on Ethereum, enabling access to a suite of e-government services in a convenient and secure manner. This eliminates the need of a user ID/password to access government services.

• “ID2020” is a global alliance across governments, public, private and non-government organizations to accelerate the process of assigning digital identity to those who are ‘invisible’ to the society. To address this goal, blockchain-based solutions and interoperability across multiple security, integrity, trust, and privacy pillars are introduced.

![Figure 3: Five Pillars of a Blockchain Based Digital Identity System](https://joom.ag/PgYa)
geographies and the reuse/integration/connectivity for existing frameworks is being worked out.

- A digital identity network being built on the Hyperledger fabric in Canada will facilitate citizens to privately maintain their digital identity credentials, and to only share information as needed to service providers based on the access to the service that they apply for.

- BanQu is a proprietary platform that captures a “Self-Sovereign digital identity”, allowing farmers to set up a unique digital profile and then help them connect with peers, aid organizations, governments, banks, and payment companies to help accumulate data from a variety of personal and financial transactions. The objective is to connect needy farmers with the global financial economy. This initiative has had early success in Asia.

The Road Ahead

Digital identity is associated with the socio-economic wellbeing of citizens, and slowly becoming essential to them getting the right to vote, open a bank account, and gain access to healthcare and education. A World Economic Forum published report in 2016 titled “A Blueprint for Digital Identity”, outlining the need for the creation of digital identity systems and associated benefits for stakeholders, also reiterates why blockchain is best suited for digital identity systems.

Having said this, it is also important to note that blockchain cannot be viewed as the panacea for digital identity issues. It does provide the framework and accompanying benefits; nevertheless, like every system it comes with its own pros and cons. One being the evolving nature of the technology itself, and two, the lack of standardization of data exchanges. Many institutions are invested in the technology and continuous efforts are on to make blockchain-based systems fool proof.

Leveraging the benefits of transparency and trust provided by blockchain frameworks, many organizations and nations are joining hands to ensure interoperability across their borders. Siloed personal identity systems are giving way to decentralized digital identity systems that are transcending borders. Therefore, National Digital Identities are expected to lead to “Global Identifiers” thereby helping combat cyber terrorism and money laundering.

While it goes without saying that no mechanism can be completely foolproof and devoid of vulnerabilities, continuous technical innovation and awareness can significantly help in bringing down the risk and help us move towards a safer world.

References

- https://e-estonia.com/solutions/e-identity/id-card/
- https://id2020.org/