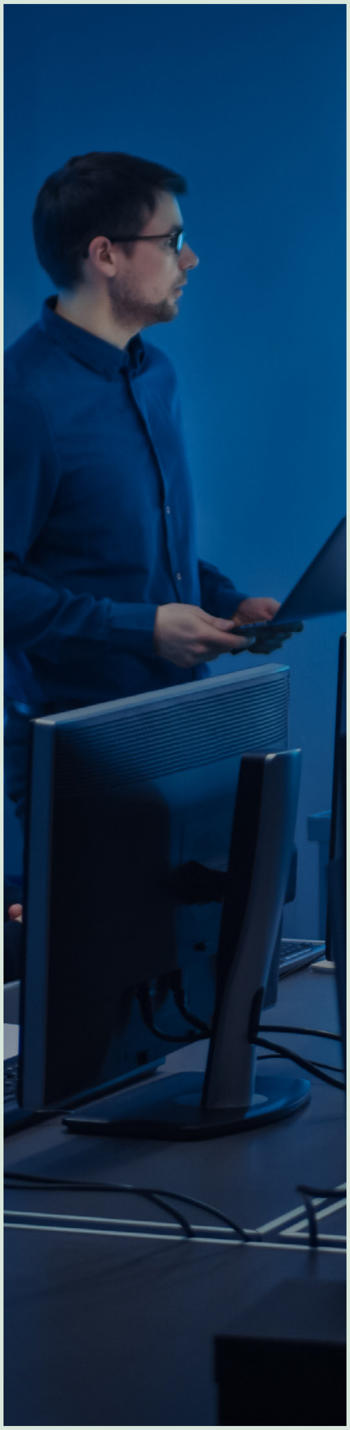
WHITE PAPER



IMPROVING GOVERNANCE THROUGH DIGITAL IDENTITIES WITH BLOCKCHAIN, LEVERAGING BLOCKCHAIN HYPERLEDGER INDY TECHNOLOGY

Abstract

This paper explains the potential application of Blockchain Digital Identity technology for state and local government use in providing citizen-centric services like License issuance, identity issuance, healthcare services and how to bridge the existing service gap.

Infosys®
Navigate your next

Today Citizens across the globe have high expectations of their governments to deliver services in a manner that is not only efficient but also transparent, accurate, speedy, and brings personalized essence to it. Citizens expect the use of mobile phones, digital technologies, social connections while interacting with the public sector because they are experiencing the same with commercial sector organizations.

Government agencies generally work in silos and are responsible for storing and maintaining huge amounts of data. Due to reasons like data security and privacy, these systems are not always integrated and have limited data sharing capabilities. Majorly these government departments depend on manual record management and authentication mechanism which is not only error-prone but also creates information silos thus resulting in consumer displeasure and trust loss.

Blockchain – Digital Identity, holds immense potential to disrupt the way these citizen-centric services are delivered by the government. Technology can solve many of the challenges which citizens face while applying for Government services. Blockchain can build confidence among citizens in government facilities/services and increase the pace with which these are delivered. For governments, it can act as a powerful means to manage registries, certificates/permits, identities, licenses, and supply chains.

What is the Gap?

Despite being cumbersome, paper credentials such as licenses have been around for centuries. In the digital age, distributed ledger technology (DLT) framework with verifiable credentials can be a key differentiator and bridge the trust and experience gap between citizens and public organizations. Take the case of a driving license. This distinctive paper is issued by a government department after an individual proves their identity and age via a birth certificate as well as their skills in operating a vehicle. A driver's license can also be used as proof of identity, proof of age, proof of address to avail other important services such as passport verification, bank accounts, university admission, hotel bookings, and more. In most cases, the citizen repeatedly proves their credentials to the respective department by submitting the driver's license. This is then verified by examining the authority issuing the license, whether the data is valid, and checking that the citizen is in fact the same person. These types of exchanges between citizens and government departments or public officer have been well accepted by society. With digital becoming the mainstay for a connected world, even utility companies are looking for ways to deliver mobile-first experiences for citizens.

Public Departments work in silos because of legacy systems and do not support cross-departmental integration. There are also certain privacy rules to consider. For instance, to avoid data theft and data misuse, departments may severely limit data sharing. From a service standpoint, however, citizens are left with multiple non-intuitive touchpoints when interacting with public departments. They are forced to re-register themselves at each department separately, usually re-submitting the same documents of proof for authentication to every government agency. The manual and time-consuming nature of these processes leads to acute discontent. Some of the common complaints are service delays, loss of documentation, manual errors, etc., arising from sorting through large piles of documents, authenticating ID proofs, and inaccurate or incomplete information.

In the unfortunate event of losing any proof of identity or registry, agencies that rely heavily on paper-based models make it additionally cumbersome for citizens who will then have to repeat the entire process of submission, authentication, etc., for a simple ID re-issuance.

With data theft becoming a looming concern, public departments bear huge costs to manage and process data, store documents, and adhere to regulations. As each organization follows similar practices, the cumulative costs – and man hours spent – are substantial.

The lack of transparency within the public sector is another factor that bothers citizens. When an application is submitted to obtain a specific service or license, details such as the status of the application, escalation matrix, estimated completion date (ECD), etc., should be made available to the applicants. In most cases, citizens are not provided with this information, leading to lack of trust due to low transparency, accuracy, accessibility, efficiency, and personalization.

An often-asked question is: Why cannot the agencies share data to provision these government services?

Complications related to the legitimacy of ID proofs, inaccurate, incomplete information, and verification lead to a range of concerns like delayed service, loss of papers, manual errors. which are regularly being faced by these departments.

When assessing these difficulties, it is important to recognize that the pace of digitalization need not be uniform across central and state governments within the same country. Technologically advanced state governments may aggressively adopt digital platforms while others continue to use manual processes to store data and provision services. Misalignment in the overall digital and data sharing strategy creates frustration among citizens for cross-border services such as transferring one's vehicle registration, renewal of driver's license, and address change in one's passport.

The time and cost associated with data management, document processing, enforcing regulatory compliances borne by public organizations is huge, and all the organizations are doing it to avoid theft and misuse of data. So, cumulative time and Cost would be massive.

To establish trust among citizens, governmental departments, and agencies, these gaps must be bridged. Blockchain digital identity systems provide the right means for local and state governments towards this objective.

What is Digital Identity?

Typically, a digital Identity is digital information that represents a person, an organization, or a device. For the purpose of this paper, 'digital ID' refers to identity information pertaining to citizens of a country.

In today's Digital world "owning" Digital Identity is of vast concern. But still, our identities are owned by the government, since those documents which prove our identity are controlled and owned by the government. And government only has the right to revoke/retain these identity documents.

Blockchain digital identity technology establishes a 'Self-Sovereign Identity' (SSI) that shifts ownership of digital IDs from governments to users. SSI provides the approach of digital credentials for citizens to control and own their digital identities and personal data. There is a shift of ownership from governments to users using blockchain technology.

How Infosys Solutions bridges the Gap?

Paper credentials/licenses though cumbersome have worked for thousands of years. Distributed Ledger Technology framework with verifiable credentials can be a differentiator and eventually bridge the trust gap and experience gap that is ever widening between citizens and public organizations.

A distinctive paper license like a Driving License is issued by government department, after citizen proves who he is via a birth certificate and that he is eligible to drive. This paper license is then used by the citizen at several other places like passport offices, bank account openings, universities, Hotels, and restaurants, to avail various services. When this is done, citizen is proving its license/credential to these departments. These departments verify this paper license by checking the authority which has issued this paper, is the data valid and not tempered, and whether the citizen is in-fact the person who is in that paper. This transaction is between the citizen and that department.

This exchange was well accepted by society till it became digital. The world has become digital, and mobile apps are there for every utility. But still, government services are predominantly paper-centric. This needs to change, and **Infosys Blockchain Digital Identity Solution** can bring that change. The solution is integrated with Distributed Ledger technology (DLT), so all the features and benefits of DLT are attached along with Digital Identity benefits.

How the solution works?

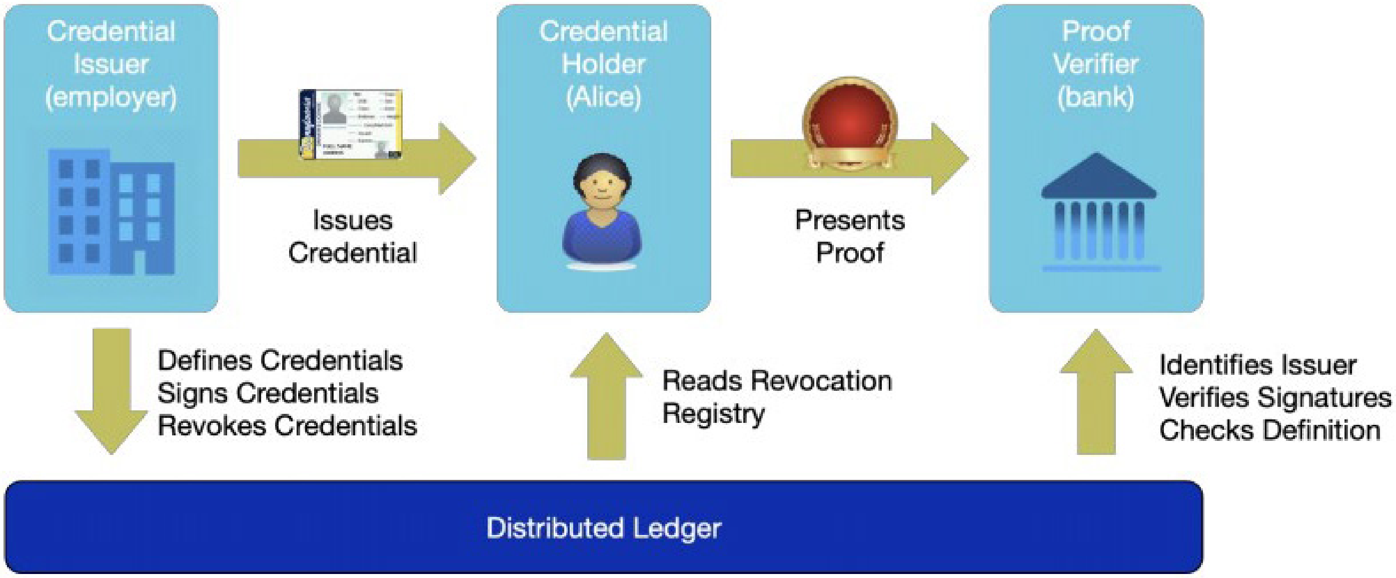


Figure 1 - Blockchain Digital Identity Mechanism

Image credit: https://sovrin.org/

- A public authority decides about user eligibility and issues one verifiable credential to support this.
- The user holds this credential in its (digital) wallet—**it never goes on the distributed ledger!**
- At later point, a verifier (any other organization) asks user to prove its identity and share requisite credentials.
- Once the user shares its identity specific information with the verifier, through a verifiable presentation, this acts analogous to paper-based license verification process.
- **In addition:** This helps to establish another aspect that the issued credentials are legitimate and not cancelled.

It is important to note that these verifiable credentials and presentations are not simple documents that anyone can create. They are cryptographically constructed and must fulfil the following four attributes:

- Who is the issuing authority for the credential?
- Who is the owner of this credential?
- The information is un-altered
- The credential is legitimate and not cancelled/nullified/revoked.

What are the challenges we foresee in implementing this model?

Though there is a need and an appetite for digital Identity solutions, still there are some challenges that may impact the viability of this solution for citizens.

The very notion of Digital identity challenges one of the most foundational aspects of our society, the ownership of our identities which was previously handled by governments would now be owned and managed by citizens themselves.

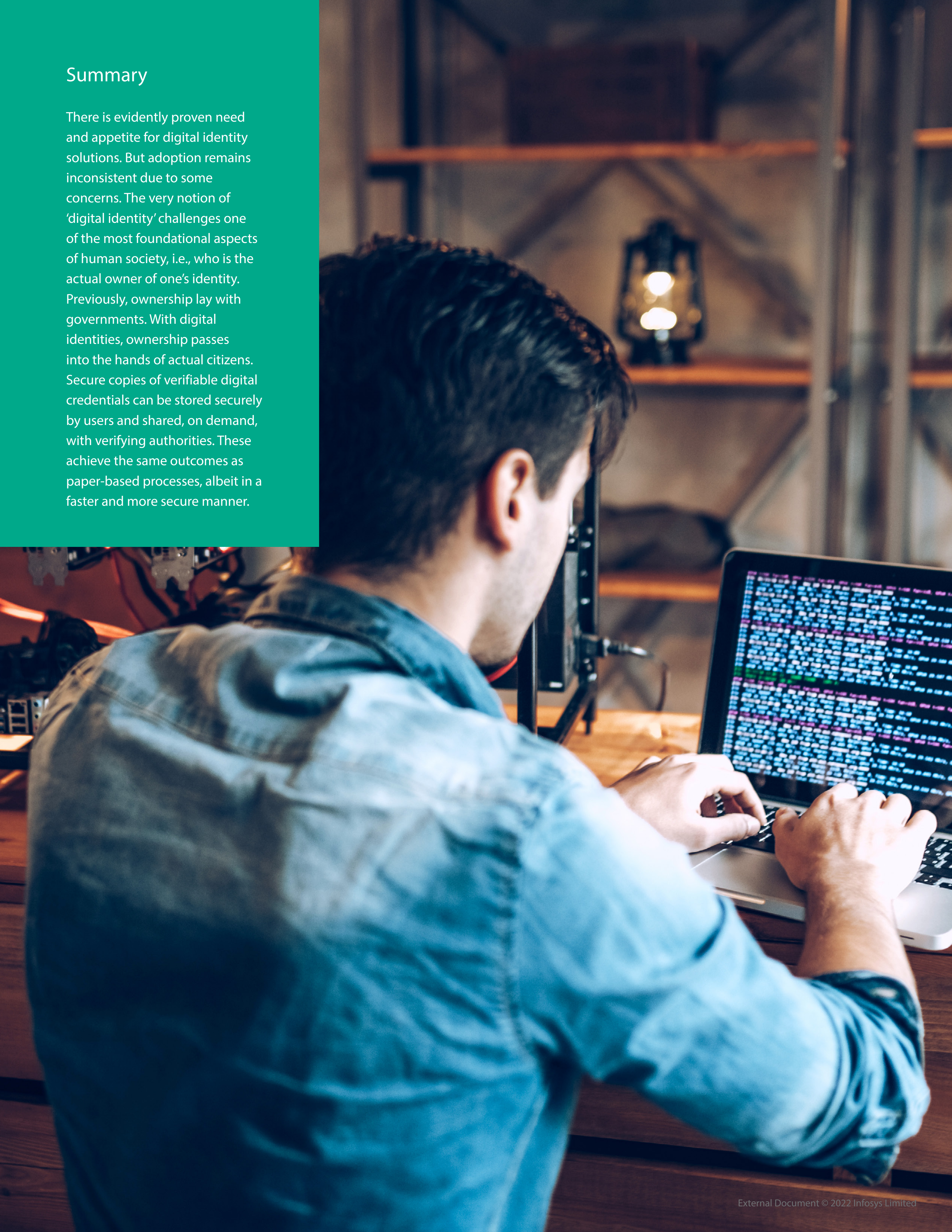
For a Digital Identity solution to work, it must be safe, secure, controllable, and portable.

It is critical to assure that personally identifiable information is kept secure. The user should be able to control access on their data and track their usage of the same.

Users should also be able to use their identity data whenever they want. Such solutions must also cater to legal regulations such as the EU-based Electronic Identification, Authentication, and Trust Services (eIDAS).

Summary

There is evidently proven need and appetite for digital identity solutions. But adoption remains inconsistent due to some concerns. The very notion of 'digital identity' challenges one of the most foundational aspects of human society, i.e., who is the actual owner of one's identity. Previously, ownership lay with governments. With digital identities, ownership passes into the hands of actual citizens. Secure copies of verifiable digital credentials can be stored securely by users and shared, on demand, with verifying authorities. These achieve the same outcomes as paper-based processes, albeit in a faster and more secure manner.



About the Author

Ashima

Principal Consultant, Infosys Blockchain

Ashima is responsible for development of Governance and Identity Solutions in Infosys Blockchain practice. She has 18 + years of IT experience covering Banking and Blockchain domain. She works closely with clients and development teams on Blockchain initiatives and enterprise integration for blockchain solutions.

References

https://www.hyperledger.org/blog/2021/04/21/why-distributed-ledger-technology-dlt-for-identity

https://www.fujitsu.com/global/imagesgig5/Blockchain-Digital-Identities-White-Paper.pdf

https://hexaware.com/wp-content/uploads/2019/10/Whitepaper_MCP.pdf

https://www.infosys.com/newsroom/press-releases/2021/launches-blockchain-network-riverside-california.html

For more information, contact askus@infosys.com

Infosys®
Navigate your next