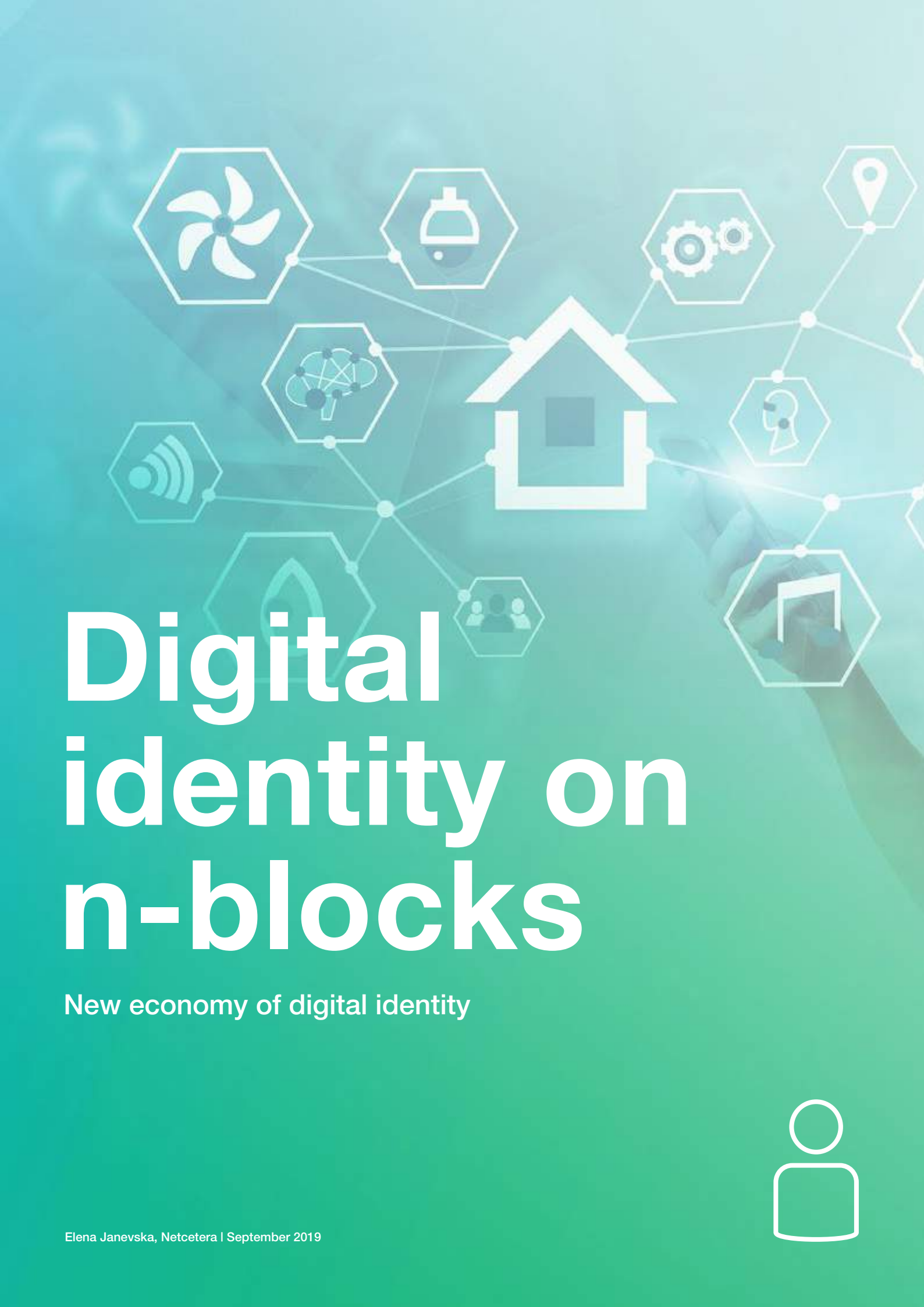


# Digital identity on n-blocks

## New economy of digital identity

Elena Janevska, Netcetera | September 2019

# Preface

Identity is an integral part of every transaction that involves two or more parties. This leads to identity management systems being the core component of every service we use.

Existing identity management systems are cumbersome and contain manual processes. New architecture and innovative technologies could benefit such systems by making them faster and more efficient. Besides, manual processes lead to identities becoming more and more fractured and redundant each time a new service provider or authority is formed. There is no doubt, we have to change the way we manage identities today. As the number of digital services and transactions grow, it will be increasingly important to ensure that transactions take place in a secure and trusted environment where each individual can be digitally identified and authenticated.

The role of digital identity systems is equally important for both the public and private sectors. In order to interact with customers and provide services, many companies have to verify and authenticate the identities of their users at various stages of the customer lifecycle.

This paper explores the challenges of digital identity and the potential of the blockchain technology to solve those challenges. The first part of the paper defines digital identity attributes and describes the lifecycle as well as the roles of public and private sector players. The second part hereof reviews the history and evolution of the digital identity and demonstrates that decentralized identity is the next step in the identity evolution. Furthermore, the paper illustrates a solution of decentralized identity ecosystem using n-blocks. And finally, it lists the benefits that the new digital identity economy will bring.

## Contents

# Challenges and Opportunities

A reliable digital identity system that allows businesses to operate in a newly efficient and safe way is one of the main enablers of the future economic growth. The issue we face today is that the digital economy still depends on physical records needed to establish person's identity. Private companies as well as governments and regulators recognize this shortage in the services they provide. Therefore, they are extensively searching for solutions that will enable customers and citizens to identify themselves in the most secure way. Together they all share a common interest in promoting digital identity and authentication.

As pointed out above, existing identity management systems are clearly inadequate because they are still largely dependent on the physical world. Attempts to bridge the difference in nature between digital services and physical reality create inefficiencies and frictions. This difference is significantly lowering the level of automation and innovation these services can bring. Moreover, as transactions are growing in volume and complexity, the need for a digital identity solution becomes urgent. All stakeholders of these transactions are willing to change. On the one hand, businesses want to solve the identity problem, as it is a critical pain point for innovations, while customers expect seamless service delivery with a single identity they will own and control. On the other hand, regulators demand stricter compliance and better insight into transactions.

**"The capacity to prove your identity is a fundamental component of the economic, financial and social development. We are at a point where innovation is driving and identity's traditional ways cannot be ignored anymore."**

So, who will drive the innovation? Even though identity looks like a national concern, a global identity controlled by government authority is not a plausible option in the short term. To achieve complex solutions, businesses need to start acting locally and to collaborate with each other and the government.

This implies that both public and private organizations should tie solutions together and form a strong and integrated identity system. It has to be a convenient, effective and trustworthy solution that is able to handle enormous volume of transactions.  Most importantly, the system should let the users own, control and share their identity information.

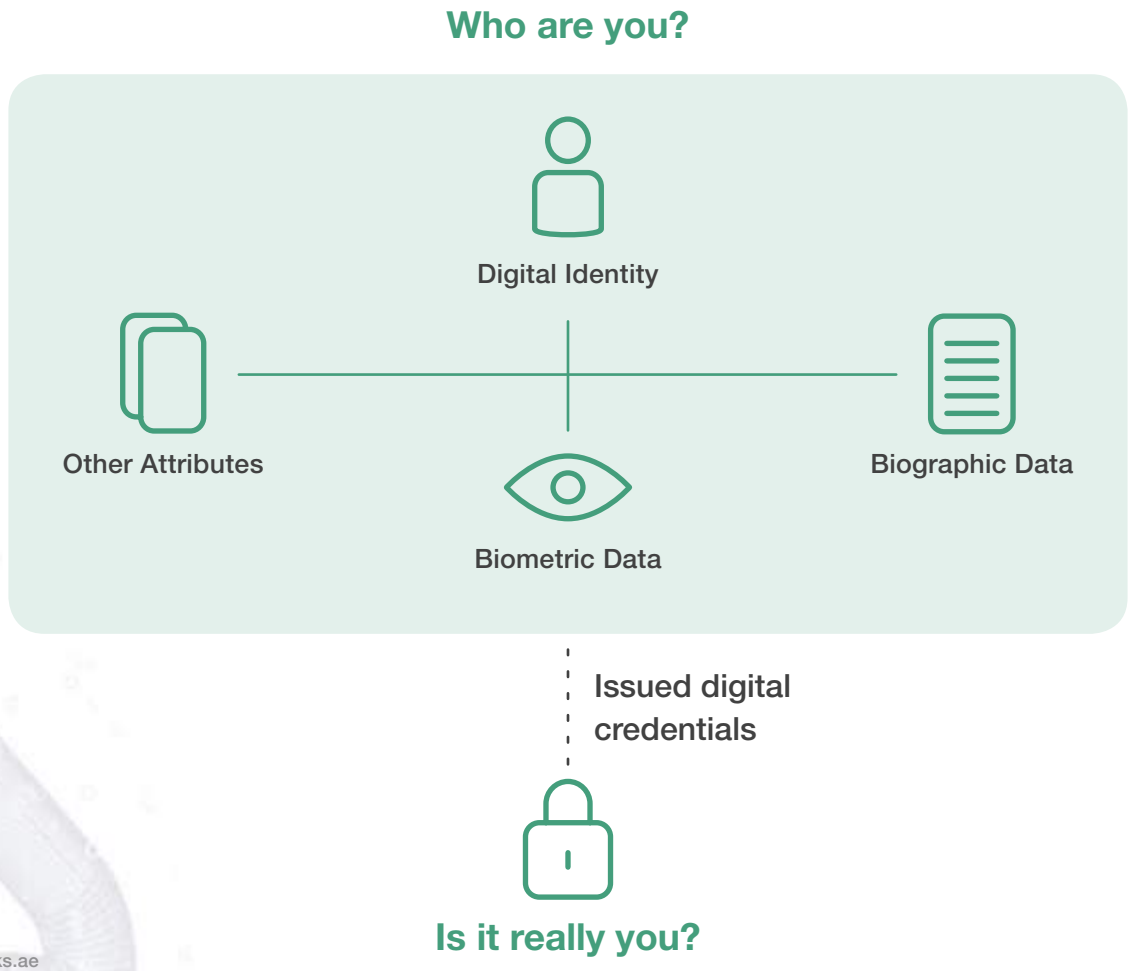
# Is it really you?

# What is digital identity?

An identity is made up of different pieces of information that are referred to as attributes. The more attributes there are, the stronger the identity is. Bearing that in mind, we can define digital identity as a collection of individual attributes that describe an entity in order to determine transactions in which that entity can participate.

A person's digital identity is usually composed of biographic data (ex. social number, name, date of birth and gender) and biometric data (ex. fingerprints and iris patterns). This is the way the unique attribute set of an identity is determined. Then, the identity is amplified with additional attributes that are more broadly related to other services. Once all these data elements are collected and verified, they can be used to identify a person by answering the question "who are you?" However, to answer the question "is it really you" when someone is using the identity, we need to issue secure digital credentials.

The attributes and authentication methods used in a digital identity may vary from one context to another depending on the type of the identity system.



# Digital identity lifecycle

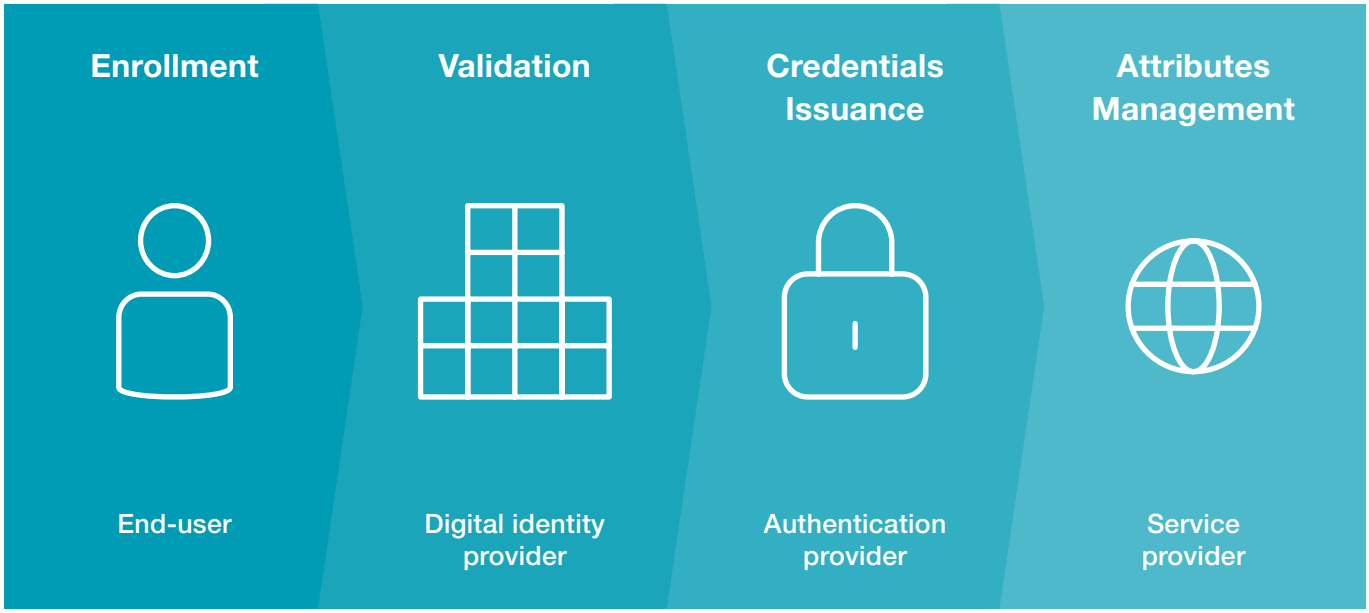
Digital identities are created and used within the lifecycle that includes the following stages:

- Registration or enrollment of the user
- Adding of the unique identity attribute set
- Validation of the user's identity
- Issuance of the digital credentials
- On demand, authentication of the user
- Managing and updating attributes by service providers

**The primary end-users are individuals whose identity is stored in the system. They can be citizens, employees or clients. On the other side, government bodies, private firms and departments are the primary providers of digital identity and the attributes. They also take care of providing the authentication, and the services. The system can be open to other users as key stakeholders that are responsible for regulation, standard setting and trust building."**

After issuing the identity, identity providers still stay engaged in the ongoing management and maintenance of the data elements of the system. They can update attributes, revoke or terminate identities.

**Digital identity lifecycle management consists of the following stages.**



## 1. Enrollment (registration)

The identity management process begins with enrollment of the user that requests an identity in the system. It is a process of capturing and recording key identity attributes from a person that claims their identity. The initial request should include basic biographical data. Depending on the identity system, biometrics can be added at this stage, or later at the validation stage. The identity provider can also do the enrollment on behalf of the user. As far as identity proof is concerned, this is the process with the highest security level. In this case, the user is present with their ID card and biometrics, while the identity operator issues new identity. The unique attribute set that is gathered at this stage builds the options for utility and interoperability with other domestic and international identity systems.

## 2. Validation (of  the identity)

Once the person has claimed an identity at the enrollment stage, this identity is then validated by verifying the attributes presented against the known data. The identity claimed should exist and be reachable as well as unique and linked to existing national identity databases. The identity can also be compared to different population registries, tax records etc. The identity provider should have an opportunity to validate and confirm the identity. This is the way the future status of the identity is set in the system.

In the case described above, organizations create a customer identity based on regulations known as Know Your Customer (KYC). These organizations are usually banks or mobile operators at the time of account opening for their customers. It is imperative for them to be certain the identity is real. Due to the KYC, these identity accounts have become source credentials that other companies would trust and prefer for identity verification.

## 3. Credentials issuance

Once registered, the identity should go through the issuance of credentials before the person can use it. For an ID to be considered digital, the credentials are supposed to be electronic (i.e. store and communicate data electronically). The types of electronic credentials include:

- Smart card
- 2D Bar code card
- Mobile Identity
- ID in the cloud

## 4. Attributes Management

Many organizations and departments that are part of the system can add and update attributes related to the identity. New service providers may join the system and leverage the potential of the digital identity records.

Throughout the lifecycle, digital identity providers manage and arrange the identity. For example, users may need to update the address, marital status, profession, etc. In addition, identity providers may need to revoke the identity, which involves invalidating the digital identity for either fraud or security reasons, or terminating it.

# Roles in the digital identity ecosystem

There are various stakeholders involved in the processes of the digital identity lifecycle. The stakeholders may play different roles throughout the lifecycle.

## Digital identity providers

Digital identity providers register and validate the identity of the entities by referring to their unique identity data. They are responsible for validating identity attributes as well as issuing digital credentials and additional documentation related to the identity. Therefore, when referring to digital identity providers we also imply digital identity verifiers. In some context of implementation, they can still be separate roles and organizations. For example, an operator from a private company can enroll a new user and send a verification request to another operator from a governmental institution that can confirm the user's identity attributes.

> **Governments are actually encouraging companies to enter the market as Identity Providers. When these companies build their users network and become a trustful provider, many people will easily get and verify accounts avoiding slow and manual government paper processes."**

## Digital authentication providers

These actors verify the attributes or identity of the entity in order to determine its right to access a service in the system. They can be a separate company that issues digital credentials on a smart card or on a mobile app. Such a role may overlap with the digital identity provider role or the service provider role.

## Service (attributes) providers

Entities that provide services directly to end-users are called service providers. They may render public services like e-Government or private services. In a digital identity ecosystem, service providers can themselves be identity and authentication providers. For instance, one department or a firm can be a digital identity issuer and other departments can be different service providers. They can also be referred to as attribute providers, since they add up new attributes in the same identity container of the user.

Some service providers may outsource identity verification and authentication to identity providers. They are referred to as relying parties. Those firms seek to verify the end-user and are usually charged for this service by identity providers.

## Regulatory agencies

There are organizations that regulate, control and audit digital identity data. These actors require adequate level of access to the system to ensure that digital identity and authentication providers follow legal standards in managing identities and using personal data.

## End-users

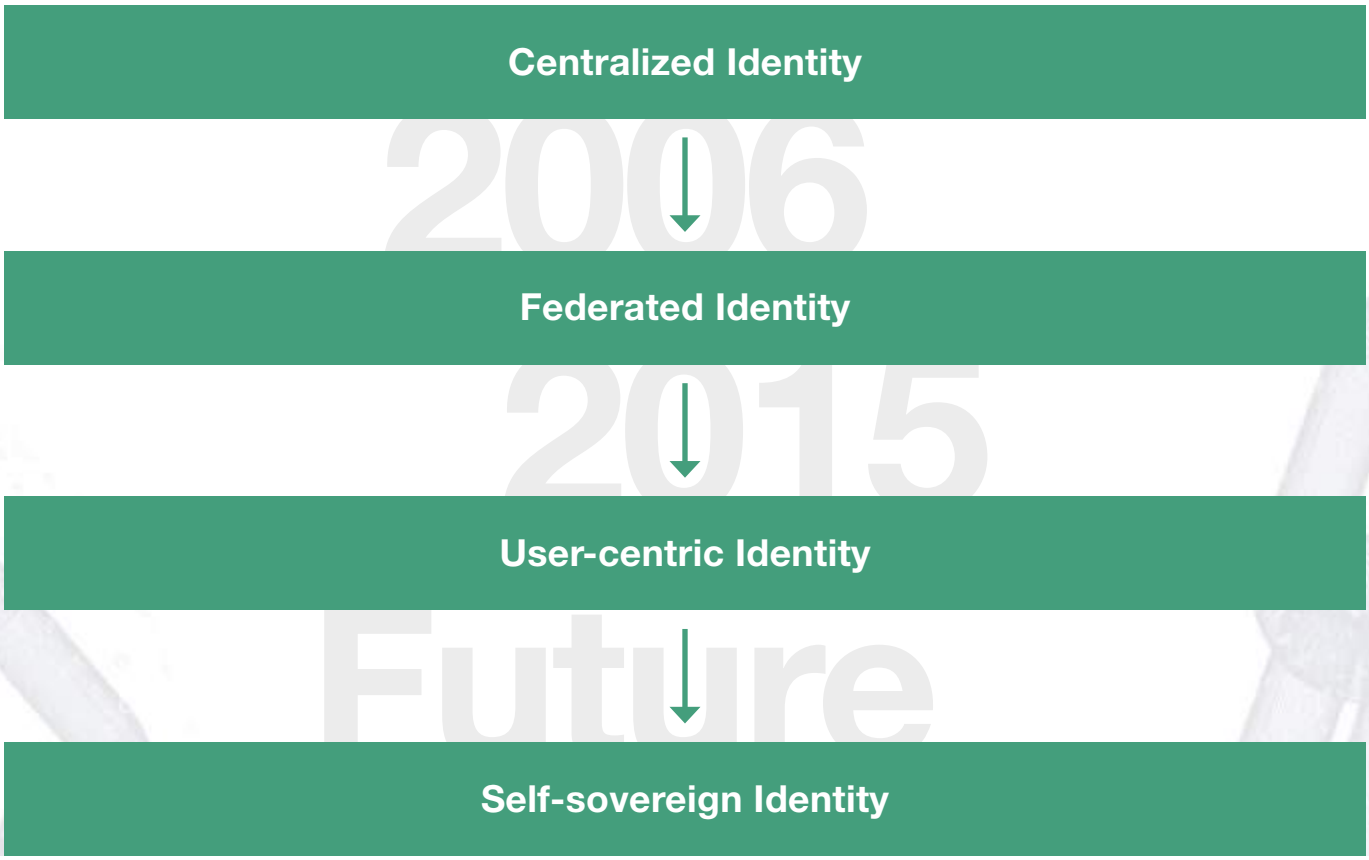
End-users are individual citizens and clients whose identities are represented in the digital identity system. They enroll and use the credentials they receive to access the services of a given company of the ecosystem.

# Levels of assurance

When an entity authenticates itself and uses the identity attributes, the degree of confidence depends on the degree of security assurance provided in the system's implementation. The way in which the information is stored and processed for authorizing the entity that they claim to be is referred to as the level of assurance (LOA). Levels of assurance depend on the strength of the identification and authentication processes. They are critical to access control and reducing identity theft. The higher the LOA is, the lower is the risk that service providers will face a compromised credential during a transaction.

| **Low LOA:** Accept risk | **Substantial LOA:** Reduce risk | **High LOA:** Avoid risk |
|---|---|---|
| **Secure Authentication:**<br>• Closed networks<br>• SMS<br>• Passwords and security codes | **Strong Authentication:**<br>• SIM Applet<br>• Smartphone App<br>• Token OTP | **Very strong Authentication:**<br>• SIM Applet with PKI<br>• Smartphone App with PKI<br>• Biometrics |
| **Identity registration:**<br>• Presentation of ID | **Identity registration:**<br>• Verification of ID | **Identity registration:**<br>• In person verification of ID |

# Identity evolution




Identity management systems are still evolving. It started with internal and closed identity management two decades ago where the same party acted as an identity provider and a relying party that used the data. It was a starting point that led to centralized identity being the first stage of the evolution. The government is still the identity provider but now it is starting to open and transfer user attributes to relying parties. For example, it shares a citizen registry with institutions that manage voting, taxes, statistics, and so forth. The goal of this centralized identity system is to enable creation of the identity that operates for the benefit of the user rather than for the sole benefit of the service provider. Slowly the user is starting to take control over its identity, or at least to preview its use. However, these systems still have the problem of security, since the user has to rely on the issuer of its identity and the centralized system administration.

Subsequently, federated identity systems are the ones where identity provider engages a number of third parties to authenticate users to relying parties. Similar to the centralized identity, the government owns the data; some private brokers issue digital identities as a service to subscribers.



Finally, what distributed identity systems achieve is connecting many identity providers to many relying parties. This type of a system provides users with consolidated identity that serves as a common authentication mechanism to multiple services. Generally, these systems rely on common operating standards rather than on a governing body. The authority is distributed among many trusted actors. This is the so-called “self-sovereign identity” which is the next level of the identity evolution. Having adopted the distributed ledger technology, the individual would not need to rely on a centralized authority to get, transfer, share or secure their data. This is where the blockchain as a technology becomes relevant.

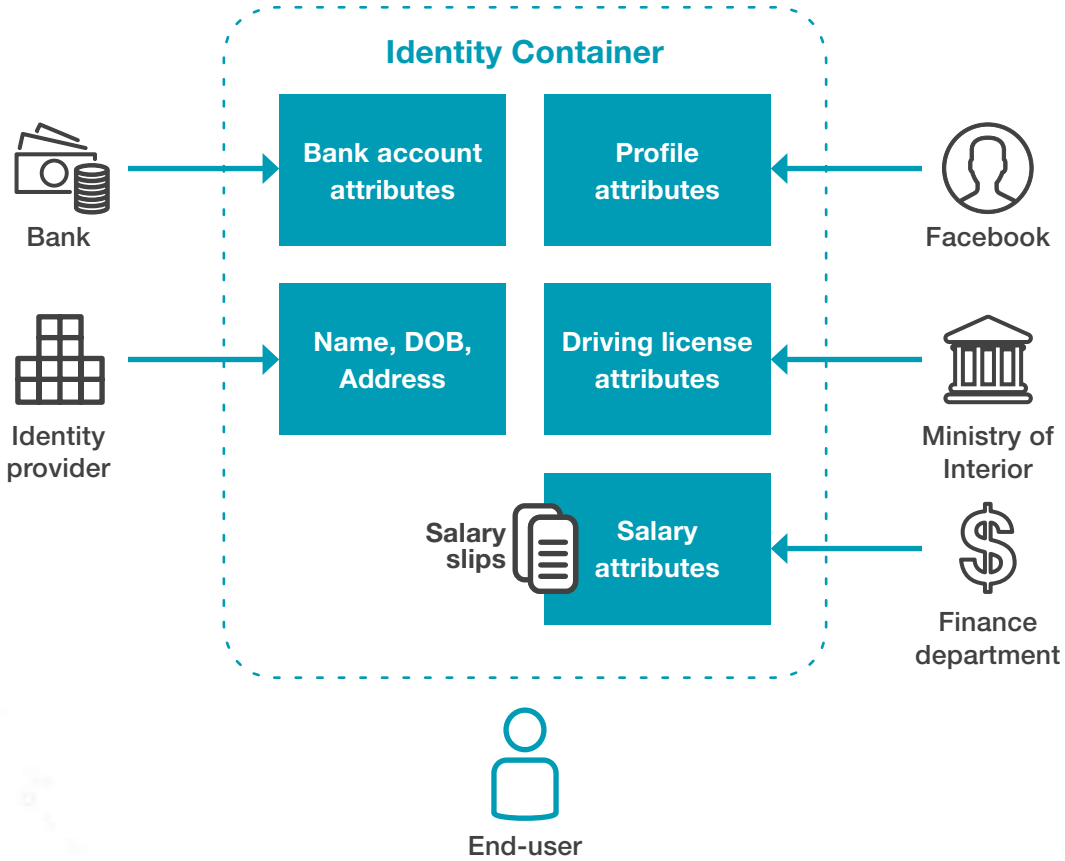
## Trends driving the need for decentralized digital identity systems

| User behavior | Need for trust | Privacy concerns | Rise in technology | Cost reduction |
|---|---|---|---|---|
| Need for seamless and ubiquitous authentication<br><br>Preference to use one and single digital identity<br><br>Dissatisfaction with passwords and codes<br><br>Lowering rates of online transactions due to lack of trust | More complex and private transactions are taking part<br><br>Lack of trust to online businesses | If consumers feel their data is not protected, they will not transact online<br><br>In which way, where and by whom the information is used?<br><br>Increasing privacy awareness in the digital native population | Emerging technologies are improving ID management very effectively and quickly<br><br>Blockchain, Big data, Biometrics, Machine learning | Digital identity systems are cheaper to run than physical ones<br><br>Use of a digital identity is already validated by a trusted third party |

# Decentralized identity ecosystem based on n-blocks

n-blocks provides a decentralized digital identity ecosystem. It is aimed at creating enabling infrastructure that supports identity standards and allows third-party providers to develop products and services on top of the identity base. Organizations that form the n-blocks ecosystem should not necessarily be digital identity providers. Most of the organizations will just use the identity and authentication services in order to issue new attributes for the user.

An individual creates an identity container or an account that allows them to accept attributes or credentials from any number of organizations. The first attributes in the container are inherent and unique, describing the individual, but not their relations with external entities. With time, users can have accumulated attributes resulted from adding and updating records while using the system. Accumulated attributes are the result of commercial or operational transactions. Service providers issue another type of attributes that define the relationships between the individual and the entity. We refer to them as assigned attributes.




The example above shows inherent attributes i.e. the name, date of birth and address. The salary attributes are assigned attributes that define the relationship of the individual and the finance department. It could be represented as a document defining all contract salary attributes. When the finance department issues monthly salary slips, they become accumulated attributes of the user.

| Inherent attributes | Assigned attributes | Accumulated attributes |
| --- | --- | --- |
| Name, DOB, Address | Salary attributes | Salary slips |

**n-blocks enables individuals to fully own and manage their own identities, and realizes the idea of "self-sovereign" identity systems. When combined, the distributed ledger and encryption technology create immutable identity records that cannot be deleted by any government or firm.**

### Main features of the n-blocks decentralized identity ecosystem are:

- Operating with or without government credentials
- Enabling granular and secure sharing of attributes
- Individuals own and manage their identity
- Individuals can choose the information they prefer to keep private
- Individuals know when and why organizations looked through their data
- Apart from individuals, the identity may represent devices and assets

Digital identity based on n-blocks focuses on the highest LOA with very strong authentication. Each user in the ecosystem has public and private key pair stored securely and locally on the client's side. As a part of using the private key, n-blocks authentication app implements multifactor identification and can ask for biometric confirmation like fingerprint scanning.

# New economy of digital identity

Providing online identity assurance services will definitely lead to new market opportunities and will affect the current economic situation.

## Lower costs

Today the process of following KYC and onboarding a new user into the system, costs $15 to $20 [1]. A report shows that on yearly level, total costs of identity assurance processes in the UK exceed £3.3 billion [2]. Half of the cost is to the providers and half of it to the end users. Onboarding processes repeat each time the customer decides to use a new service that requires KYC. The duplication can be eliminated by using digital identities on n-blocks, which are verified once and used many times.

Service providers will no longer verify the identity of an individual or entity from scratch. Moreover, there will be no intermediary that takes fee for providing identity checks. Transaction fees will be very low. The costs for both creating and using identities will be reduced. The costs of using identities may be reduced by over 90% as processes that once required human activity are digitally automated.

## Innovation and new offerings

The real opportunity of digital identity is in creating the landscape for many new offerings on the market. The identity attributes of the end-user will help identity providers and relying parties deliver new tailored products and services. Identity service providers can well position themselves at the market for verified attributes.

A second market is also emerging called Personal Information Management Services [3]. It helps individuals gather, manage and use their information. For this market to exist, they will be heavily dependent on verified attributes, especially identity attributes.

One of the reasons for many transactions to be undertaken manually is unwillingness of one or both parties to transact online. This applies mostly to the cases where digital identity is at stake and risky transactions like selling a property cannot be conducted completely online. When the risk and cost of these transactions is reduced enough, we can expect expansion of possibilities in new online transactions.

## Massive and faster transactions

Completing and closing transactions will be easier if digital identity is used. There will be much fewer barriers in the process. Identity checks will take place in a large number of transactions from different service providers. A new economy can be created by massive amount of low cost identity check transactions.

## Revenue growth

Having implemented digital identity, firms will have opportunities to offer Identity-as-a-service and get into this fast growing market.

Identity-as-a-service offers enterprises access to identity management services in the cloud. Identity providers manage and host the authentication infrastructure as well as the data and the access-management services. Enterprises that act as relying parties will leverage advanced identity capabilities without having to deal with complex digital infrastructures, policies and high security standards. Relying parties make it easier to complete transactions, while identity providers can process them for a fee.

Another revenue growth will arise from better knowledge of the customer. Digital identity data will provide many opportunities to institutions for improving existing products and offering new products.

## Privacy and security

Blockchain as distributed ledger is the only technical solution that can completely address the privacy and security concerns for implementing digital identity. Using n-blocks people will be able to own and control access to their identity information. They will know how and when their attributes were exposed. The encrypted attributes will be shared point-to-point in a dispersed and immutable network. Data will remain transparent as well as protected from damage or theft with cutting-edge authentication and security protocols.

## Improved compliance

Identity management practices change from industry to industry and they are not always open or accountable. Many integrators do not follow a standardized way in collecting minimum needed identity data. n-blocks provides transparent system with immutable history of all transactions needed for an audit. Looking at the latest state of n-blocks, regulators will have better access to trusted and up-to-date information.

# Conclusion

**There will not be a single global solution for digital identity in the near future. We have a principled basis for building and connecting identity networks between businesses and we should start applying it. Firms need to consider a bottom-up approach to digital identity. First, test and refine the system with a critical number of parties and then gradually develop it to include more users, relying parties, and identity providers.**

The system should implement highest LOA and always put the end-user in the center. It should be privacy enhancing, meaning the user's information is exposed only to the right entities under the right circumstances. Users are supposed to have control over their information and determine who holds and accesses it.

Even if we achieve a technically perfect solution, firms should work on its sustainability and business model. The system has to withstand shifting procedures and stakeholders. It should implement open standards that will allow scaling and development from the future.

**n-blocks has been developed by a Swiss software provider - Netcetera. Netcetera has been in the software industry since 1996 and delivered 2000 projects for mission critical systems in diverse industries and across different geographies. 500+ experts spread across 6 countries and 14 locations deliver elegant solutions to real needs.**

n-blocks by netcetera

Learn more about n-blocks solutions on **www.n-blocks.ae**,
and more about Netcetera on **www.netcetera.com.**

# References


1. “Civic whitepaper,” Civic Technologies, 2017.
2. A. Mitchell and J. Smith, “Economics of Identity,” The open identity exchange.
3. “Personal Information Management Services: An analysis of an emerging market,” www.ctrl-shift.co.uk.
4. B. Pon, “Private-Sector Digital Identity in Emerging Markets,” Caribou Digital.
5. “A blueprint for digital identity, Delloite”.
6. “Private Sector Economic Impact from Identification Systems,” World Bank Group.
7. B. Robinson-Morgan, “The value of digital identity to the financial service sector”.
8. “The value of our digital identity,” Liberty Global.
9. “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation,” World Bank Group.
10. “Technical Standards for Digital Identity,” World Bank Group.
11. R. J. McWaters, “A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity,” World Economic Forum.
12. “Digital Identity - On the Threshold of a Digital Identity Revolution,” World Economic Forum.
13. A. S. Domingo and Á. M. Enríquez, “Digital Identity: Current State of Affairs”.

Elena Janevska, Netcetera | September 2019