Blockchain and Digital Identity: the path to Self Sovereign Identity

www.pwc.com/it

pwc

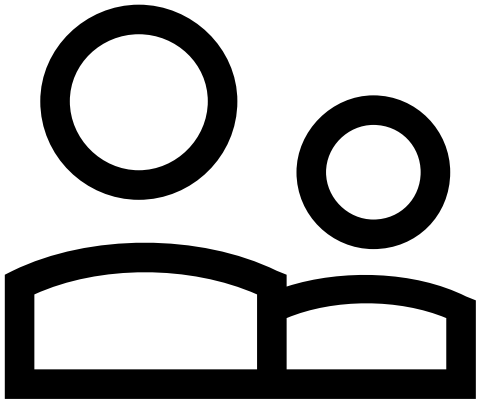
1 What is a Digital Identity?

What is a Digital Identity?

...2019 is showing to be **the year** of **digital identity** and **digital certificates** fever.

People are starting to realize **technology is ready** to give a digital identity to people everywhere in the world.

...**think of a world** where you don't need to queue up to have a piece of paper released by the municipality of your city, but you simply scan a QR with your smartphone to show him a **trustworthy digital credential**.



The technology is **here**, **fast**, **cheap** and ready to make this **a reality today.**

What is a Digital Identity? (continued)

...a **well known problem** in the cyberspace has always been knowing **who we are interacting with**...

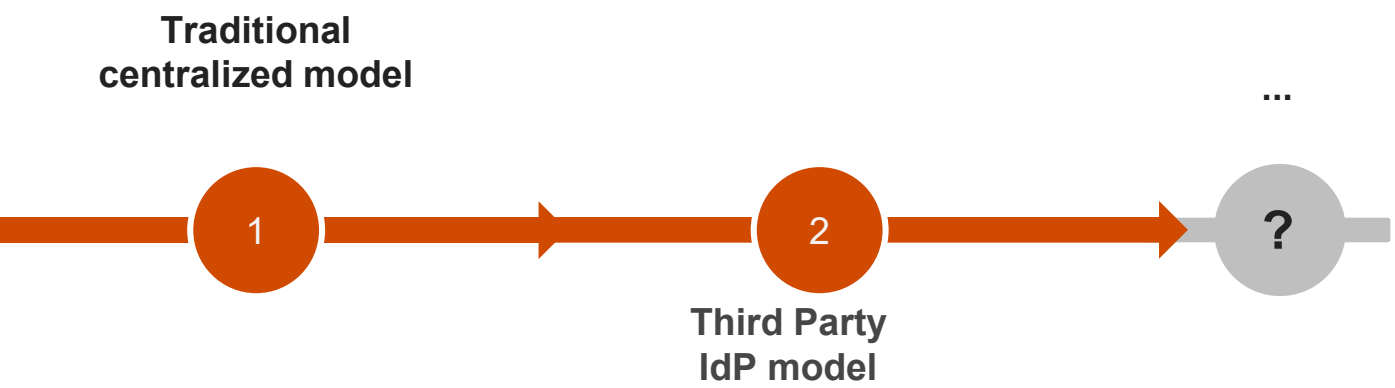
- An **identity** is defined as a "*set of attributes related to an entity*" *[ISO/IEC 24760-1]*
- A digital identity is an **information** used by **computer systems** in order to **identify** a defined subject.

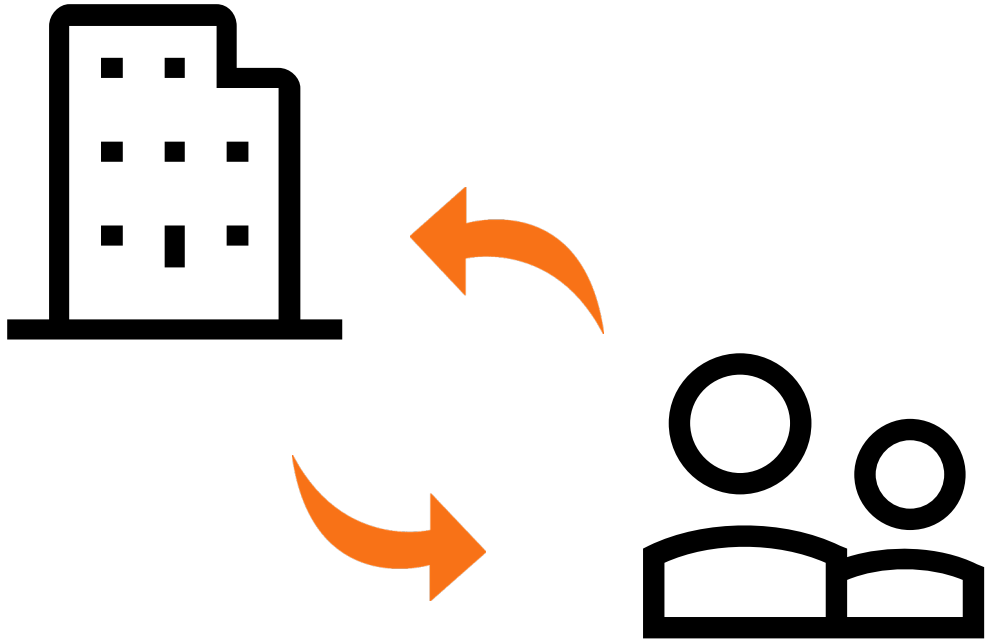
Nowadays, a digital identity **defines us all**, our **attributes**, our **credentials**, our **interests**, and even more...

What is a Digital Identity? (continued)

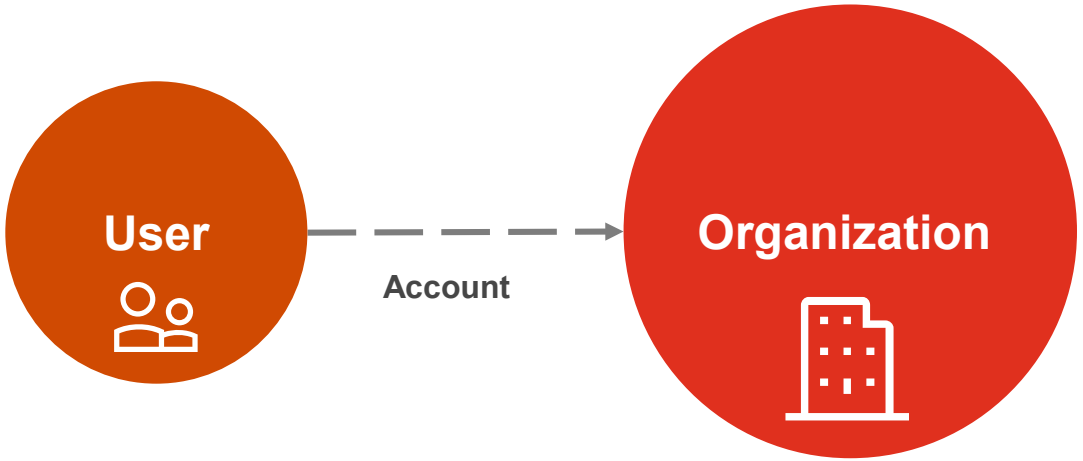
Digital Identity has **always been treated** from the point of view of the **organization** managing it and **not** from the perspective of the **user**, who **actually** is the **owner** of the **identity**.

During the course of history, from the advent of the Internet, there have been **two** main **models** for digital identity management.





Model 1: Traditional Centralized Model

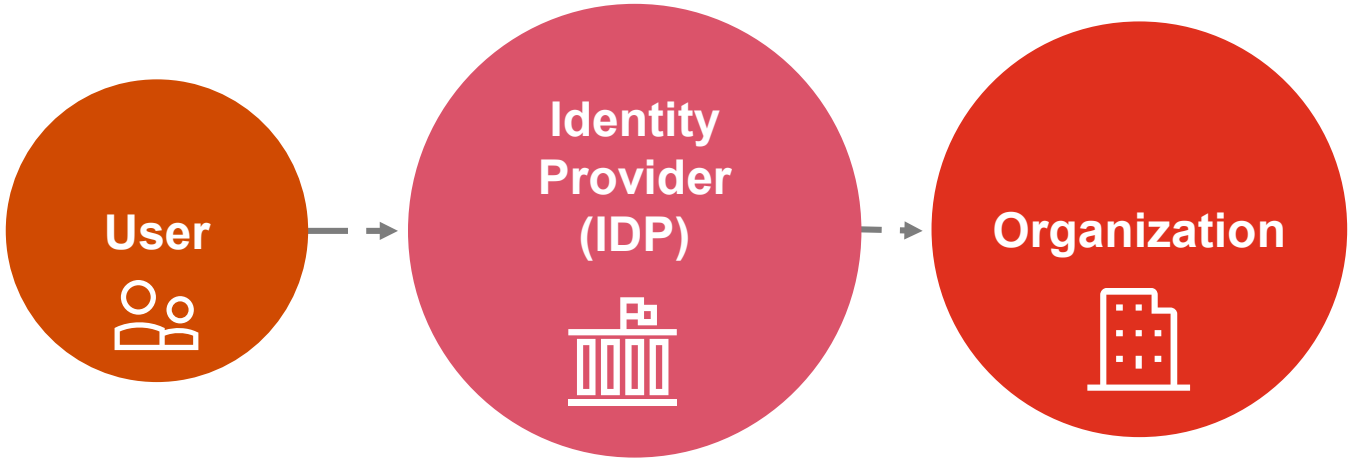


Traditional, "**centralized**" identity is the **simplest** of the models: an organization issues to users (or allows to create) a **digital credential** (account) that users can use to **access** its service.

In this model, trust between you and the organization is typically established through the use of **shared secrets**, username and a password. Sometimes shared secrets are augmented with additional factors such as physical tokens or biometrics.

At least some users' personal data is stored within the organization's "**database**", and it happens for every organization, app, or website you log into. As a result, this model requires you to **create** and manage **separate credentials** for **each relationship**.

Model 2: Third-Party IDP



In the **Third-Party IDP** model there is a new third-party that acts as an **Identity Provider** (**IDP**) between user and the organization (or **Service Provider**) that the user is trying to access. The **IDP** issues the digital credential, providing a "*single sign-on*" experience with the IDP which can then be seamlessly used elsewhere, **reducing the number of separate credentials** needed to be maintained.

1° Step
User
Gets digital identity from IDP

2° Step
IDP
Releases credentials for user

3° Step
User
Logs into an organization with the credentials obtained

4° Step
ORG
«Communicates» with IDP to authenticate user

5° Step
IDP
Verify credentials and authenticate user

6° Step
ORG
Receives IDP answer and user is logged into the organization

In this model, communication between the Identity Provider is made through **common protocols**, such as **SAML** or **OAuth**. **Data** is still **centralized** in the **Identity Provider**. A common example of such model can be Facebook, Connect, or SPID.

...but there are some downsides (Model 1)

Unfortunately, the **centralized approach** to digital identity have several **downsides** to be considered...

Cybersecurity

Data kept in a centralized way is subject to hacks (e.g. the Equifax breach)

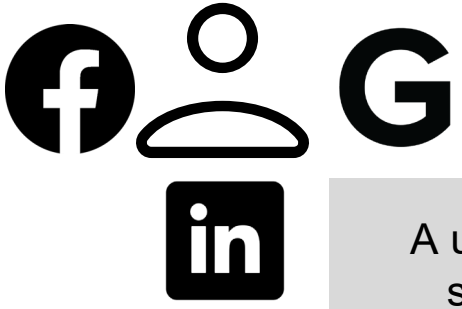
No control

User do not have control on their identities and easily lose track of their identities

High costs

The centralized model implies high costs for organizations, which must have large infrastructures in place

Moreover, the centralized model for digital identity has created the phenomenon of «**multiple identities**»



A user must keep multiple digital identities for each service he interacts with, for example LinkedIn, Facebook, Google, …

…but there are some downsides (Model 2)

Also in the **IDP approach** to digital identity there are several **cons** to be considered such as:

…the **costs!**

As outlined before in the explanation of the IDP Model, everytime a user wants to use a service, the Service Provider must «communicate» with the Identity Provider, in order to authenticate the user.

This requires the Identity Provider to have a **scalable** and **large infrastructure**, ready to «answer» all the **requests** from the Service Providers. This translates in high costs for maintaining data centers needed for this job.

Moreover, the Identity Provider is not able to generate revenue! **Who is going to pay for Authentication Services** when there are solutions such as **Google ID** that do **the same job for free**?

2

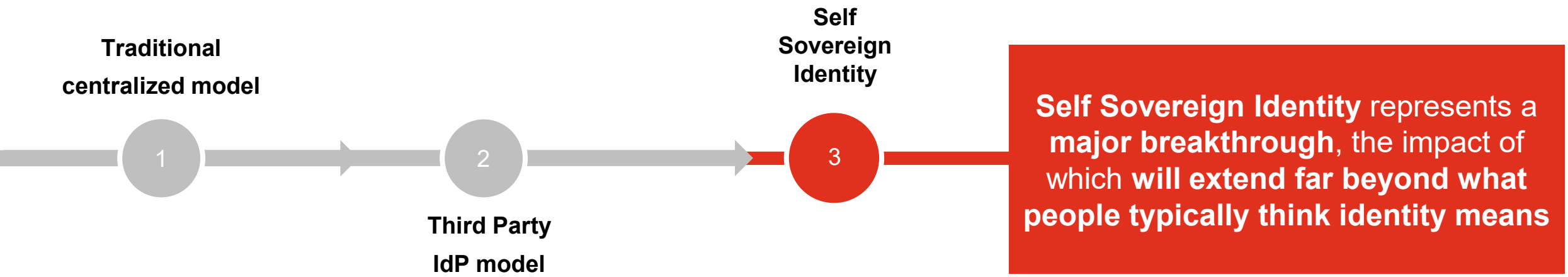
The next step:

Self Sovereign Identity

The step to the new model: Self Sovereign Identity

As we have seen, **digital identity suffers** from different downsides, which make life **harder** for **users** and **organizations**.

A new approach to digital identity comes with the concept of Self Sovereign Identity, which aims at an giving back to the user **full control on its identity**.

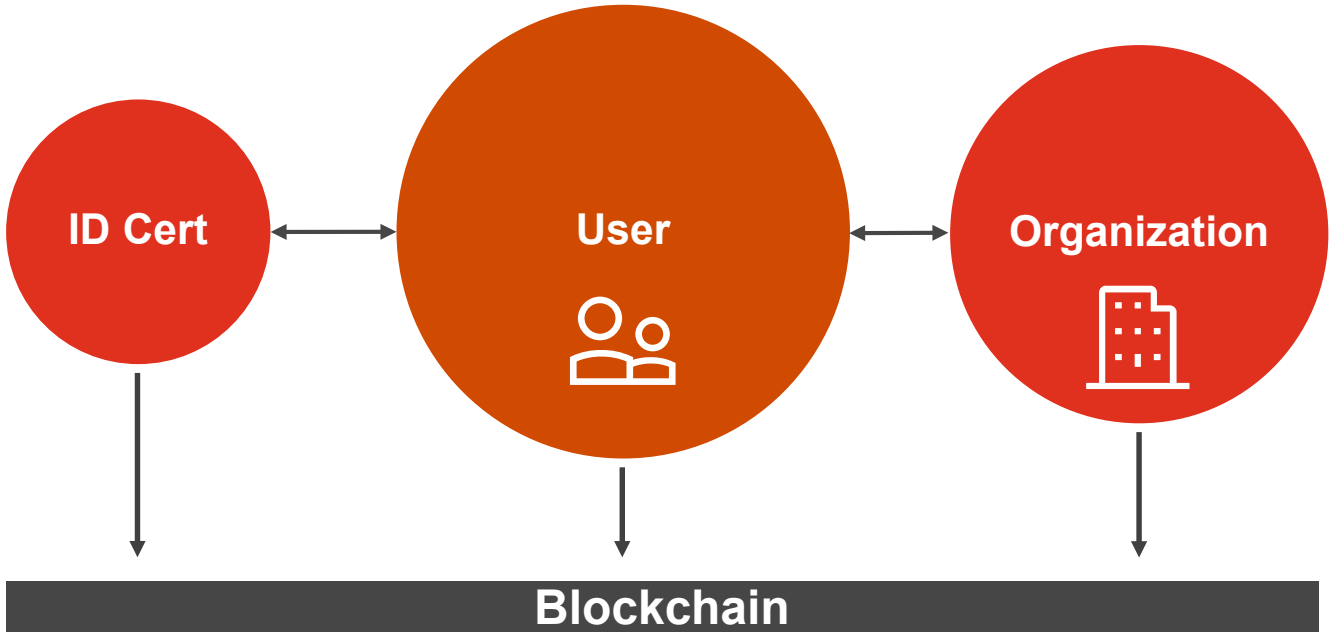


“

Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity

Cristopher Allen, Blockchain and cryptography pioneer, co-author of the TLS Security Standard.

Model 3: Self Sovereign Identity



Users and organizations can present **digitally signed claims** related to them, which have been **signed** by a new role in the system: the **Identity Certifier**. The verification process of the signed claims is automatic and with **no intermediary needed**

The **Self Sovereign** model allows the creation of a system in which **identity** and its **related claims** (so anything «linkable» to an identity, such as a diploma) are **totally given back to the user**. There is **no central authority** needed in order for the system to work.

Each of these is a **claim** of the user.

Self Sovereign identity: an overview

Self Sovereign Identity envisions the user as **central actor** controlling everything related to its identity in a «digital wallet» that contains **verifiable claims** related to him, like its curriculum, passport, bachelor degree certificate… Just like in a «normal» wallet!

Each verifiable claim (such as a diploma in this case) related to the user is **digitally signed** and can **cryptographically prove** to any **verifier**:

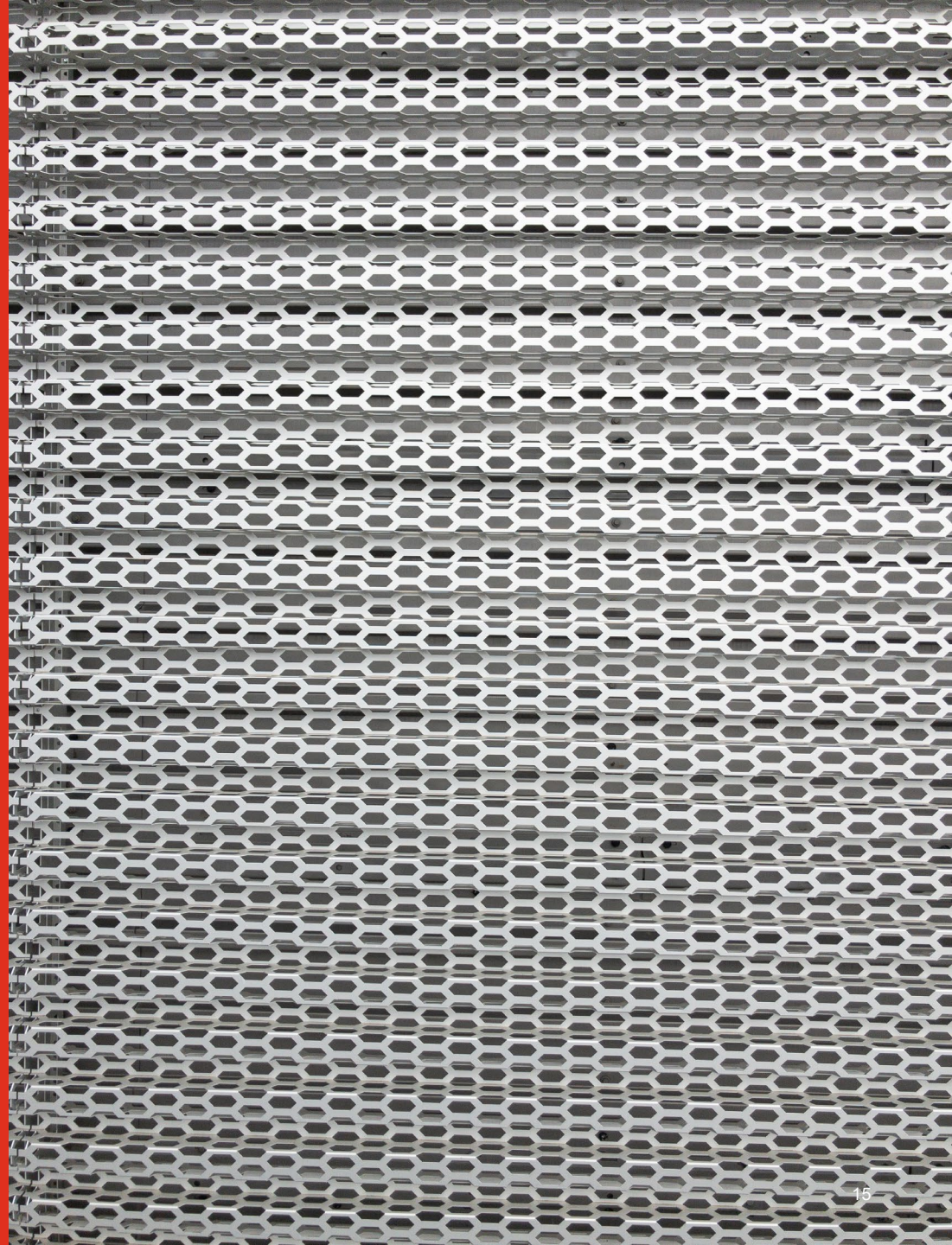
- **Who** is the issuer (e.g. the University issuing the Diploma);
- **To whom** it was issued (e.g. the user);
- Whether it has been **altered** since it was issued;
- Its **validity**.

Verifiable Claims issued in the Self Sovereign Identity context can be used **wherever they are trusted**. The digital identity in such context is **as strong** as the **claims** it "contains", **strong enough** for even high-trust industries such as **finance**, **healthcare**, and **government**.

“

“But what does blockchain allow here? […] It allows a very subtle, but crucial shift—you and I could actually own our own digital identity.”

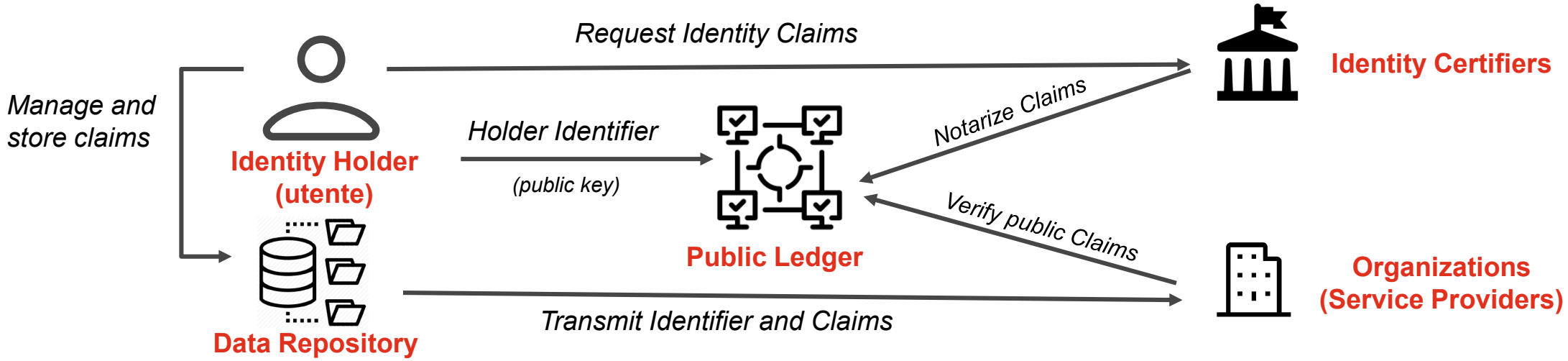
Darrel O’Donnell, CTO @CULedger



Self Sovereign Identity: how does it work?

Blockchain technology allows the Self Sovereign model to work. In this model, identity and the claims of a user are **directly** and **autonomously managed by the user**. This system allows to manage a **root-of-trust** without a central authority or a **single point of failure**.

From an **high-level perspective**, the **functioning** of the Self Sovereign Identity model is represented below:

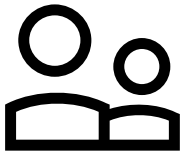


Self Sovereign Identity and the Blockchain

Thanks to **Blockchain technology**, it is possible to build a Self Sovereign Identity system. A Blockchain has **three main characteristics**:

It's a **Ledger**

A Blockchain is only one of the possible ways to store and share data among several participants.



… **Shared** …

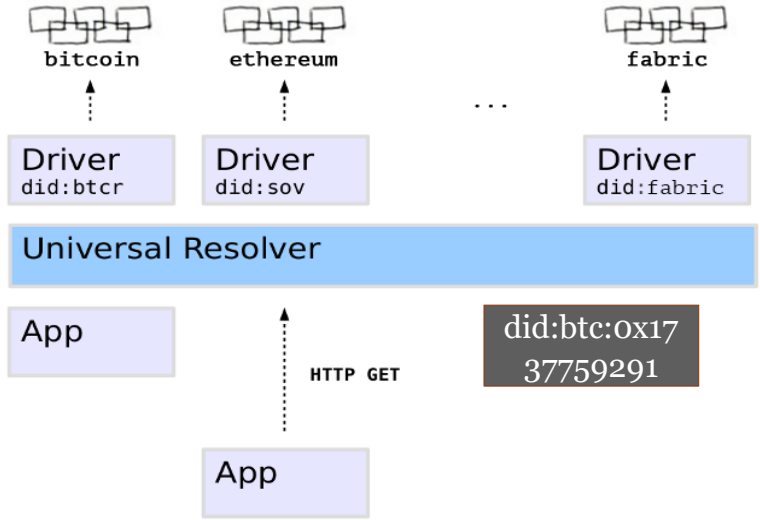
Each participant keeps a local copy of the whole ledger, containing the whole history of transactions.

… and **Democratic**.

Modifications to the Ledger and the protocol must be approved by all participants.

In the Self Sovereign Identity model, entities (people, businesses, devices) can be identified with a new approach: Decentralized Identifiers (DID)

- A DID allows to recover univocally a **DID Document**
- A DID Document contains the **Verifiable Claims** and it is stored on a **Blockchain** or a **centralized system**



What is so good about Self Sovereign Identity?

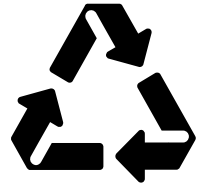
Self Sovereign Identity has a life-altering potential for **any person in the world**. There are **several pros** that can arise from the spread of the Self Sovereign model. There are many, but these are just some…

Business impacts

In the IDP and traditional models, an **Identity Provider** must **authenticate all its users**. In the SSI model, **authentication** is **processed** by **Service Providers**, which are able to scale their infrastructures the best way, **according to the number of their users.**

Privacy and GDPR

Identity Certifier that create Verifiable Claims does **not need to keep data** of its users anymore, simplifying data management. Moreover, **the user keeps its own data** and on the **Blockchain** are **stored** only **hashes** with no content.



Interoperability

Self Sovereign Identities of citizens can be **used for any type of service**, web or not, national or international, and it can enable **instantaneous KYC**. Service Providers **only need to have access to the Blockchain**.

3

PwC: Blockchain and Self Sovereign Identity

PwC and Self Sovereign Identity

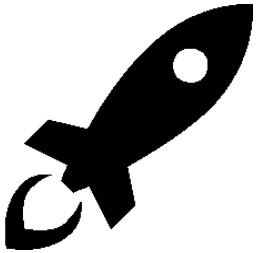
Along with the **continuous digitalization** occurring in the world, **technological** innovation has made the Self Sovereign concept possible, with the aim of a **user-centric approach to digital identity**…

PwC Italy, through its **Blockchain Competence Center**, is **currently experimenting** the Self Sovereign approach with **great interest** and hopes, by getting "**hands-on**" with Blockchain technology, with its **team of expert Blockchain and DLT developers and analysts**, in order to make Self Sovereign Identity real, touchable and usable by **anyone on earth**.

…the time for Self Sovereign Identity has come…

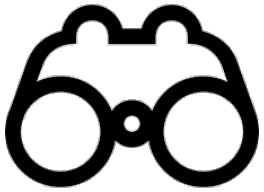
PwC Blockchain CC

PwC Advisory Italy Competence Center dedicated to Blockchain and DLT technology



- **Launched in January 2016**
- Experience on Blockchain since **2012**
- **Certified** Blockchain and DLT developers
- Great **knowledge** and **experience** on several international projects with different Blockchain and DLT technologies

- Developing a **Blockchain Value Proposition** for the **Italian market**
- Supporting the **Global PwC** activities
- Facilitating the creation of a **Blockchain ecosystem**
- **Monitoring** the **evolutional** Blockchain **Trends**



- Evaluate Use Cases **objectively**, overcoming the **Hype**
- Offer support on technologies studied through **research** and **experimentations**
- Working closely to clients in order to understand their real needs

Key contacts

Silvia Morera

+39 348 2403774

silvia.morera@pwc.com

Marco Monaco

+39 3425549439

marco.monaco@pwc.com

Roberto Lorini

+39 335 7164464

roberto.lorini@pwc.com

pwc.com/it