


**TAL  
TECH**

 [blockchain.taltech.ee](https://blockchain.taltech.ee)

# **DIGITAL IDENTITIES ON THE BLOCKCHAIN**

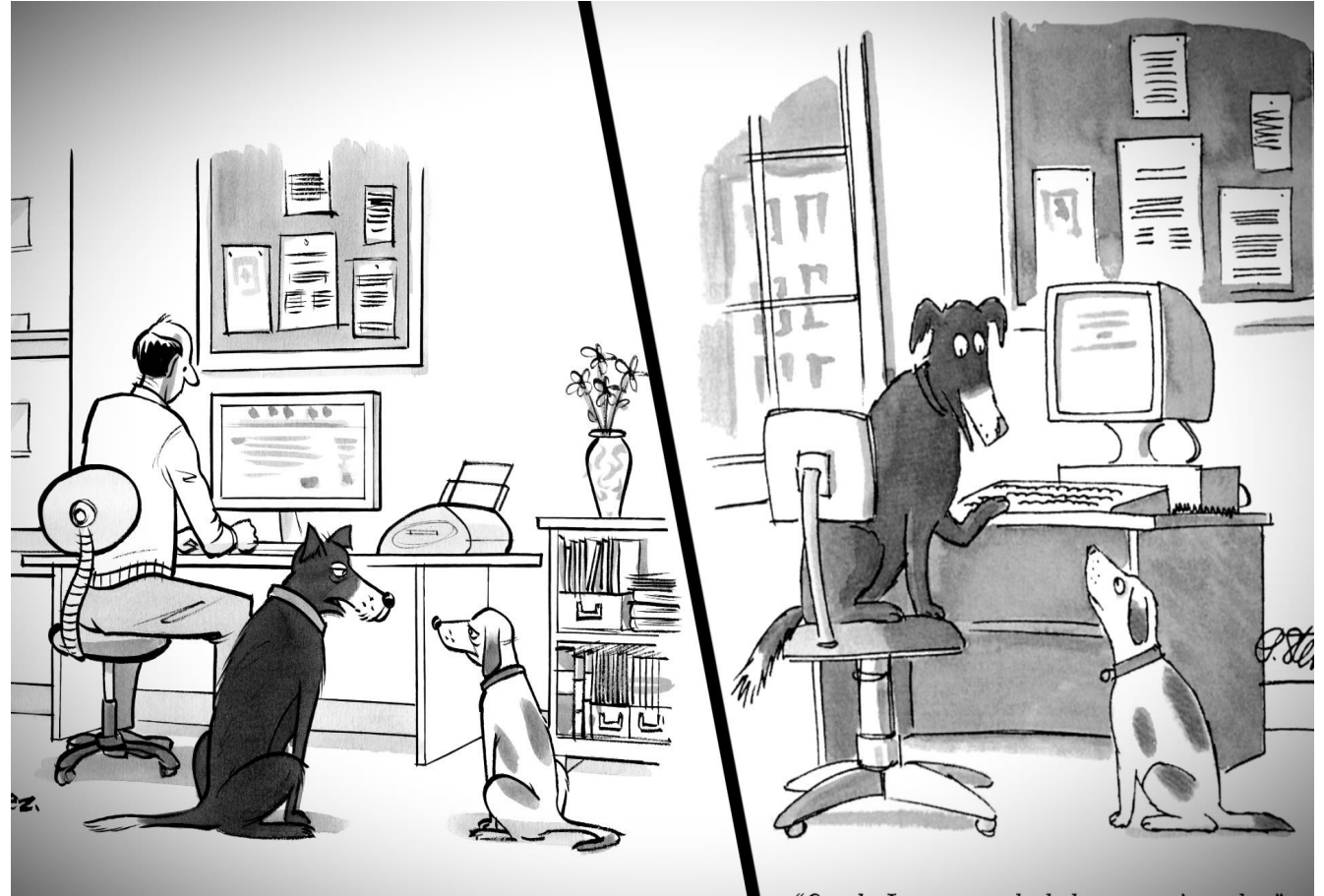
04.07.2021

# AGENDA

- Introduction
- Basic Concepts
- Evolution of digital identities
- Centeralized vs. decenteralized identity solutions
- Blockchain-based digital identity
- Decentralized Identifiers (DIDs)

## MOTIVATION

- A mutt on a computer commenting to a fellow hound, "On the Internet, nobody knows you're a dog."
- Steiner's cartoon perfectly captured the absurdity of those early days of the internet and how difficult it was to distinguish true identities.
- By 2020, "Internet dogs" will be actively armed. A large percentage of attacks use identity as their primary attack vector.



Source: Peter Steiner - The New Yorker  
(1993)

## WHAT IS DIGITAL IDENTITY

- Any personal information found online that can be traced back to the real you
- The notions and properties associated with digital identity are listed below.
  - identifier: a set of attributes allows an application domain to associate a previously declared identity with a known digital entity.
  - Uniqueness: A unique identifier, used in an application domain, ensures a one-to-one connection to an entity within that domain.
  - Authentication: one confirms the digital identity by stating their identifier and the digital proof of identity (Credential).
  - Anonymity: a characteristic of information that cannot be used to identify an individual.
  - Unlinkability: impossibility to connect separate messages, URLs, actions, or identifiers to a single person or group of people.

## WHAT IS DIGITAL IDENTITY

- Linkability: the opposite of linkability Tracing back to the identity of a cybercriminal is particularly useful.
- Pseudonymity: To protect their digital identity, individuals or organizations can use a pseudonym. Unlike anonymity, linkability is possible.
- Trust: An application domain can test transactions, digital identities, and authentication levels to assign trust levels. The trust here is attributed to the application domain, and not the other domains.
- Reputation: The quality of the relationship and service is determined by each digital identity rating and comparing with the other identities.

## IDENTIFICATION METHOD

- Name
- Social Security Number
- Photo
- Possession (ID, passport, keypair)
- Biometric
- Phone number
- Location
- Motion



## VALIDATION AND VERIFICATION AND AUTHENTICATION

- **Validation** is where an individual's information, such as name, address, telephone number, and email address are checked to see if they exist in the real world.
- It is important to note, that identity validation does not link that data to you as the individual interacting with the organisation.
- **Validation** provides less friction in the customer journey and is of particular use when onboarding customers for low risk products.
- In the validation step, companies are seeing if the data is real, in **verification step** a customer is tied directly to the information and verified as genuine by additional checks including official databases such as driver license files, electoral registers and the credit bureau.
- **Verification** has more friction than validation however this is good when more certainty is needed that the individual's data links, e.g. their address matches their name.

## VALIDATION AND VERIFICATION AND AUTHENTICATION

- **Authentication** is the process by which a customer's identity is qualified against something that only the user should have or know.
- This process can provide friction in the customer journey however developments in this area, like using biometrics, are improving the customer experience and providing greater certainty for businesses.

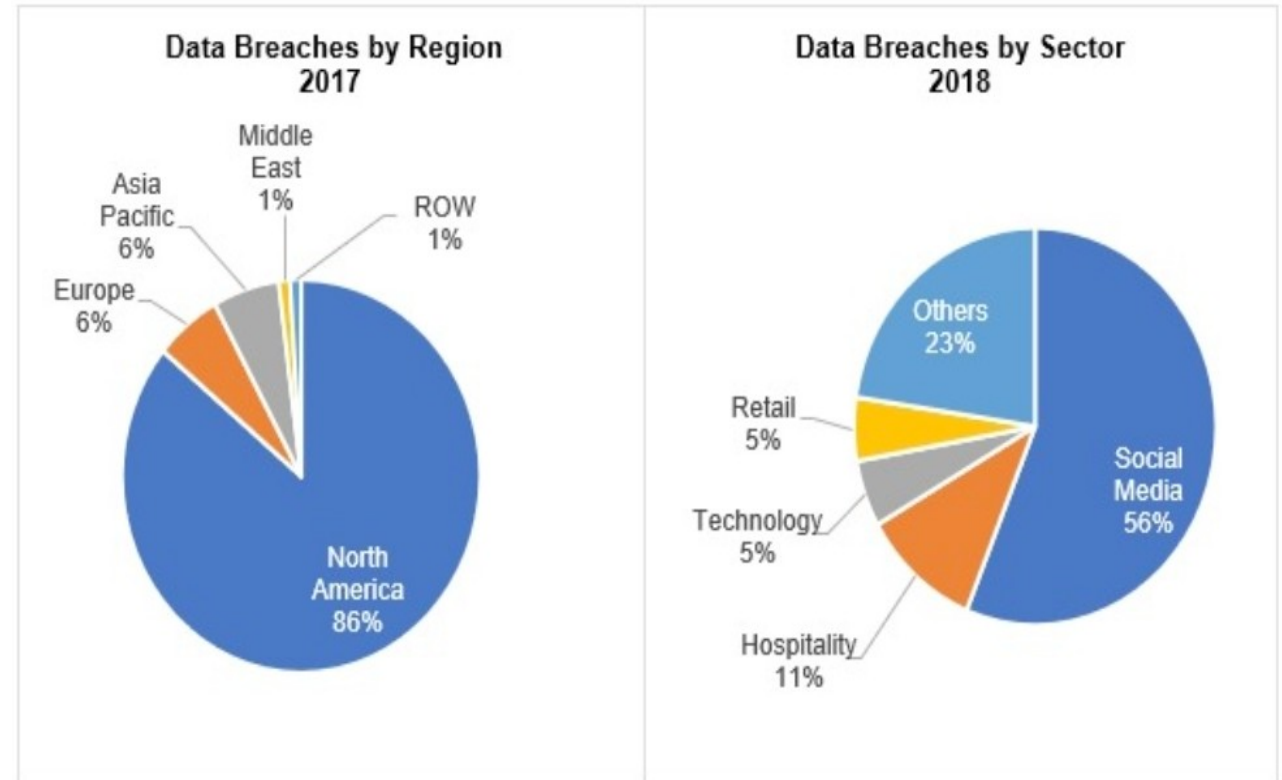


## VALIDATION AND VERIFICATION AND AUTHENTICATION

- **Authentication** is the process by which a customer's identity is qualified against something that only the user should have or know.
- This process can provide friction in the customer journey however developments in this area, like using biometrics, are improving the customer experience and providing greater certainty for businesses.

## DATA BREACHES-OVERVIEW

- Every year data breaches are reported across the world across all sectors.
- More than 86% of all data breaches occurred in North America, followed by Europe and Asia Pacific, which each account for 6% of all data breaches.
- Social media accounts for 56% of the world's data breaches, with hospitality and technology coming in second with 11% and 5% respectively.

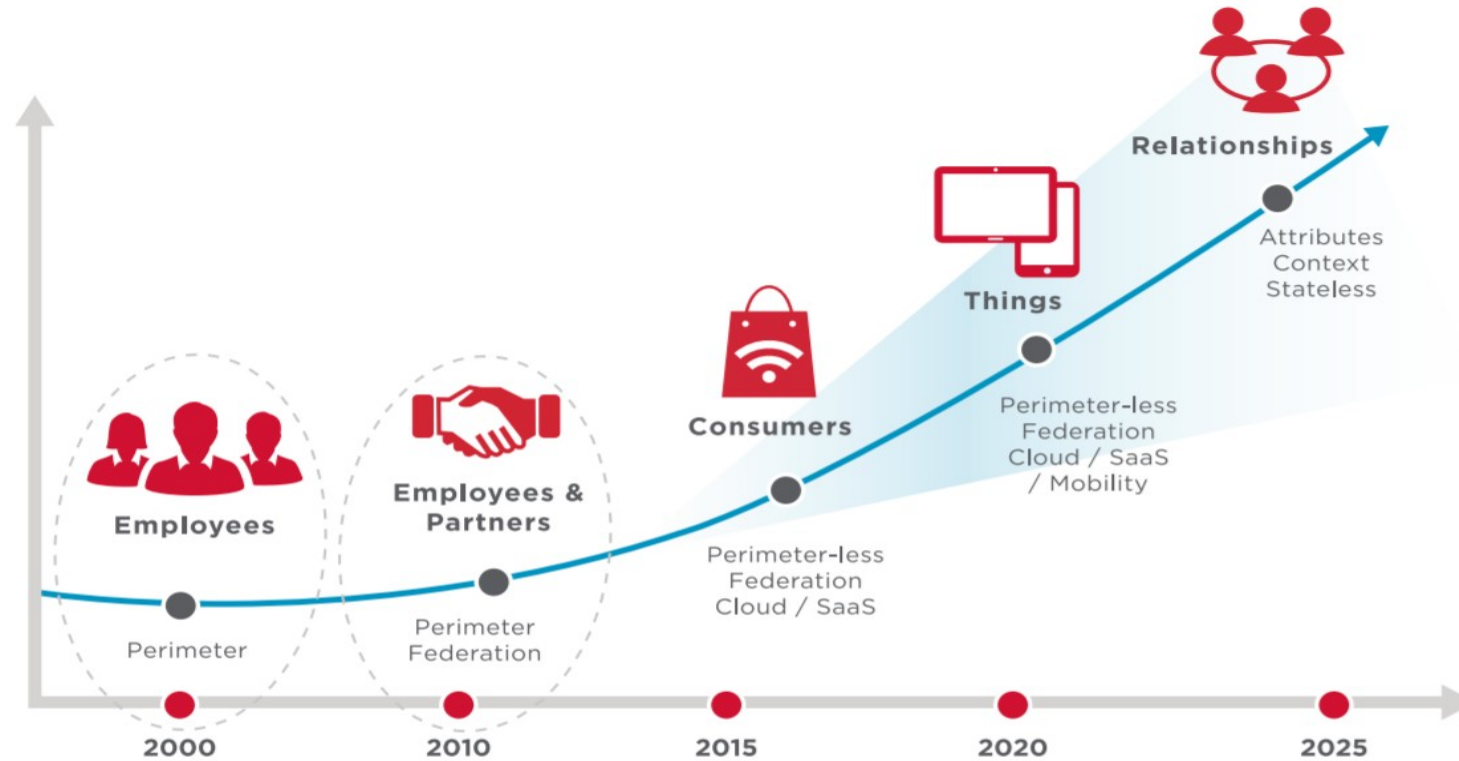


Source:

<https://saasscout.com/statistics/biggest-data-breach/>

# THE EVOLUTION OF DIGITAL IDENTITY

Figure 1: The Evolution of Digital Identity



Source: <https://docs.broadcom.com/doc/the-evolution-of-digital-identity>

# EVOLUTION OF DIGITAL IDENTITY

- Centralized Identity
- Federated Identity
- User-Centric Identity
- Self-Sovereign Identity

## CENTRALIZED IDENTITY

- A centralized identity system is one in which verified credentials are stored and managed by a single central authority, usually in a single database.
- Centralized authorities create and verify digital identities.
- Enhanced by hierarchical trust-structures

### **Problems:**

- Single point of failure
- Users are reliant on root authorities.
- Users must create an account for each "central-authority-system/service," such as Facebook, Google, and others.

## FEDERATED IDENTITY

- A federated identity is a method of connecting a person's electronic identity and attributes that are stored across multiple distinct identity management systems.
- A Microsoft account or MSA (previously known as Microsoft Passport).
  - Microsoft Passport Network is a single sign-on Microsoft user account for Microsoft customers to log in to Microsoft services (like Outlook), devices running on one of Microsoft's current operating systems.
- Sun Microsoft organized the Liberty Alliance (2001)
  - Attempts to steer clear of CA resulted in an oligarchy (divided control of centralized authority amongst several powerful entities.)

## FEDERATED IDENTITY

- A federated identity is a method of connecting a person's electronic identity and attributes that are stored across multiple distinct identity management systems.
- A Microsoft account or MSA (previously known as Microsoft Passport).
  - Microsoft Passport Network is a single sign-on Microsoft user account for Microsoft customers to log in to Microsoft services (like Outlook), devices running on one of Microsoft's current operating systems.
- Sun Microsoft organized the Liberty Alliance (2001)
  - Attempts to steer clear of CA resulted in an oligarchy (divided control of centralized authority amongst several powerful entities.)



## USER-CENTRIC IDENTITY

- Local administrative controls without requiring a federation
- Users are in the middle of the identity process
- Increases decentralized identities to make federated identities interoperable, but has centralized control to control identity access
  - Attempts to steer clear of CA resulted in an oligarchy (divided control of centralized authority amongst several powerful entities.)
- **Goal:**
  - Create long-lasting online identities
  - Everybody should have the right to control their own online identity.
  - let users fully control their digital identities

## SELF-SOVEREIGN IDENTITY

- Self-sovereign identity (SSI) is a digital identity model that gives users control of their digital identities
- Addresses the difficulty of establishing trust in an interaction.
- Users control the verifiable credentials that they hold and their consent is required to use those credentials
- Holders generate and control unique identifiers called Decentralized Identifiers.
- The European Union is creating an eIDAS compatible European Self-Sovereign Identity Framework (ESSIF).
- The ESSIF makes use of decentralized identifiers (DIDs) and the European Blockchain Services Infrastructure (EBSI).

## NEED BLOCKCHAIN FOR DIGITAL IDENTITY

- Blockchain identity management systems could be used to eradicate current identity issues:
  - **Inaccessibility:** The primary obstacles in regards to identity documents are lengthy processes, expenses, lack of access, and a lack of knowledge regarding personal identity.
  - Half of the 2.7 billion unbanked people have smartphones, which will allow for blockchain-based mobile identity solutions better suited to vulnerable people.
  - **Data Insecurity:** Currently, we store our most important identification information on central government databases that are supported by outdated legacy software.
  - According to a recent study, personally identifiable information (PII) makes up 97% of all breaches in 2018.

## NEED BLOCKCHAIN FOR DIGITAL IDENTITY

- **Fraudulent Identities:**

- There is no agreed-upon format for inter-platform use of data.
- Digital/offline identities' connection makes it relatively easy to fabricate identities.
- The advent of blockchain technology has enabled us to create new identity management systems based upon the concept of decentralized identifiers (DIDs).

## DECENTRALIZED DIGITAL IDENTITIES (DID)

- A pseudonymous profile, such as a randomly generated unique ID, could be used as a digital identity.
- Biometrics, Behavioral, Biographic are the modals that make up a person's identity.
- One person can have many DIDs, thus limiting the range of activities over which they can be tracked.
- Securing decentralized identities relies on cryptography. A key's private or public designation depends on the context of use.
- A QR code tied to a decentralized identity allows users to present their verified identity and gain access to certain services.
- Verify the identity by checking the proof of control or ownership of the presented attestation

# DECENTRALIZED DIGITAL IDENTITIES (DID)- DESIGN GOALS

Goal	Description
Decentralization	Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, <a href="#">services</a> , and other information.
Control	Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
Privacy	Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Security	Enable sufficient security for requesting parties to depend on <a href="#">DID documents</a> for their required level of assurance.
Proof-based	Enable <a href="#">DID controllers</a> to provide cryptographic proof when interacting with other entities.
Discoverability	Make it possible for entities to discover <a href="#">DIDs</a> for other entities, to learn more about or interact with those entities.
Interoperability	Use interoperable standards so <a href="#">DID</a> infrastructure can make use of existing tools and software libraries designed for interoperability.
Portability	Be system- and network-independent and enable entities to use their digital identifiers with any system that supports <a href="#">DIDs</a> and <a href="#">DID methods</a> .
Simplicity	Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
Extensibility	Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

Source: <https://www.w3.org/TR/did-core/>

# DECENTRALIZED DIGITAL IDENTITIES (DID)- DESIGN GOALS

Goal	Description
Decentralization	Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, <a href="#">services</a> , and other information.
Control	Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
Privacy	Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Security	Enable sufficient security for requesting parties to depend on <a href="#">DID documents</a> for their required level of assurance.
Proof-based	Enable <a href="#">DID controllers</a> to provide cryptographic proof when interacting with other entities.
Discoverability	Make it possible for entities to discover <a href="#">DIDs</a> for other entities, to learn more about or interact with those entities.
Interoperability	Use interoperable standards so <a href="#">DID</a> infrastructure can make use of existing tools and software libraries designed for interoperability.
Portability	Be system- and network-independent and enable entities to use their digital identifiers with any system that supports <a href="#">DIDs</a> and <a href="#">DID methods</a> .
Simplicity	Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
Extensibility	Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

Source: <https://www.w3.org/TR/did-core/>



# DID STRUCTURE



Figure 2 `did:example:12345abcde`

Source: <https://w3c-ccg.github.io/did-primer/>

**TAL  
TECH**

***Thank you very much for your attention!***

***Q & A?***

Reference: Arumaithurai M., Introduction to Blockchains, Tallinn, Estonia 2019, <https://tinyurl.com/n2y3k5pu>