Santander X Innovation Xperts

Citizenship & technology:

Digital identity

JANUARY 2023

By Santander

Table of contents

01 Introduction: **where are we?**

Digital identity is a thriving market and its growth potential will continue rising in the coming years. The shift to digital processes both for public purposes (taxes, grants, public services, voting or digital citizenship, among others) and for a variety of private services (financial services, e-commerce, facilities, social networks, gaming, meta/multiverses, etc.) is conclusive, and, largely accelerated and expanded by the pandemic, it has become irreversible. This constitutes the most obvious baseline for the expected growth of the digital identity market, certainly laying the foundations for the sector to thrive. But some challenging trends are announcing a profound transformation of the market, that requires and will entail a substantial sophistication of digital-identity solutions, involved actors, and users' needs. In facing and internalizing these challenges, routes to take and areas to explore are diverse and multiple. Hence, innovative and strategical responses will make a difference.

The report is structured in three parts in addition to this introduction. Part II (*where are we heading to?*) unveils the main visible trends – expanding 'digital living', identity needs for hybrid contexts, and multiplication of our 'digital lives' (in metaverses and extended/augmented realities) – paving the path towards an increasingly granular, multilayer, versatile, and scalable digital-identity-solutions. Part III (*where could we go?*) maps the principal policy/organizational/technological options to consider on the basis of five factors: control (who is in control), actors (who is involved), inputs (which attributes), outputs (which solutions are provided), and environment (purpose). Part IV (*where should we be looking at?*) explores the less visible but most promising opportunities guided by five key drivers with the capacity to definitively fuel the potential of digital identity in the upcoming years. Main findings are summarized in the final section.

02 **Where are we heading to?** The most visible opportunities for digital identities

Digital identity is a burgeoning market and its potential will continue boosting greatly in the coming years. Our increasingly **expanding 'digital living', the pressing identity needs for physical-digital hybrid contexts**, and the **multiplication of our 'digital lives' (in metaverses and extended/augmented realities)** heavily depend upon and deeply rely on a sound, versatile, reliable, and aspirational global digital-identity framework.

Beyond the evident turning point from paper-based and face-to-face processes to fully digital processes, other challenging trends are leading the path towards an extraordinary rise of digital-identity needs, a sophistication of the identity-requiring situations, and a reinterpretation of digital identity rather far from a mere 'functional equivalence' of the traditional identity formulae.

The main trends that have been identified and will lead the exercise of exploring and spotting promising opportunities to leverage are the following (but will be elaborated in greater detail in the following sections):

I.2.1. The expansion and proliferation of hybrid contexts where identity needs to flow reliably from physical to digital environments and inversely.

The definitive consolidation of tele- and remote working, the increasing remote participation in a variety of social, political and professional situations (events, decision-making bodies, meetings, deliberative committees, business negotiations, learning contexts, etc.), the overwhelmed demand from fully remote/digital onboarding process in a number of services (recruitment, contracting bank services, admission procedures, enrolment, etc.) claim for fluid, versatile identity solutions.

As further detailed below, this trend is being addressed from different and often opposing fronts, and a range of responses are possible, with equally promising opportunities at all ends. Some solutions might coexist, or even complement each other; others represent confronting paradigms in construing and developing the digital identity of the future.

I.2.2. The fascinating expected rise of digital living in metaverses and extended/augmented realities.

Private sector is seriously embarking on planning and devising business strategies to gain presence in the metaverse/s and other extended/ augmented realities: universities and business schools, stores and shopping areas, social event planners, law firms, banks and financial service providers, museums, auction houses, etc. With different levels of reliability, digital identity solutions will be required for educational, professional, entertainment, commercial, or even citizenship-related purposes.

I.2.3. Far from 'monolithic' identities, users are demanding more granular purpose-specific identities with a minimized privacy exposure, and a sense of responsible anonymity.

In a multitude of contexts, solely one (or a few) attributes need to be verified and authenticated (e.g. legal age, nationality, vaccination, enrolled student, employed worker, compliance to tax duties, no pending or delayed payments, etc.) to complete a transaction or to enable the use to access a service. Exposing privacy and all identity attributes in all these recurrent scenarios is undesired, unnecessary, and cost-inefficient.

Users would be willing to preserve their identities and rely on trusted third parties to confirm to the counterparty in each situation that the requirement is met, the attribute has been verified, or even the identity has been authenticated. This entails a granular purpose-specific model where the role of private sector should be essential.

As an illustration, the bank can perform this role leveraging their position and experience in Know Your Customer (KYC) and Anti Money Laundering (AML) processes. Should the user need to prove legal age, nationality, or address, the bank will intermediate by simply confirming the meeting of the requirement without disclosing other unnecessary identity-related data.

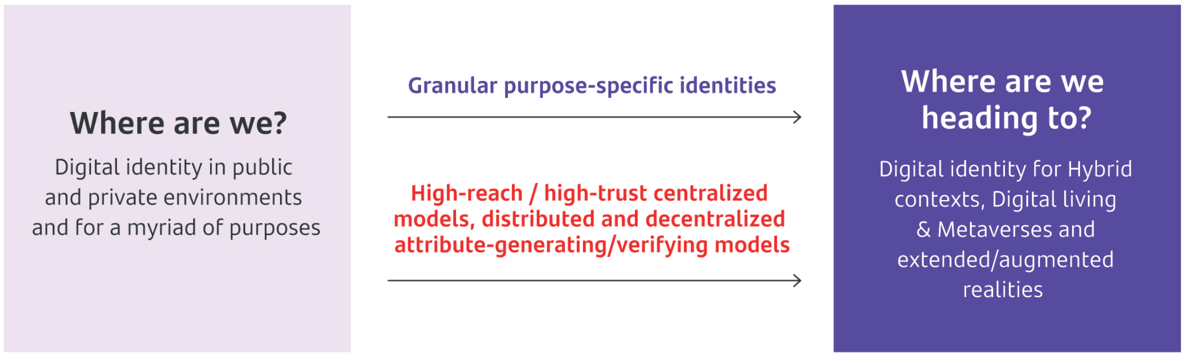
I.2.4. The proliferation of distributed and decentralized attribute-generating/verifying models – for building a genuine DeSoc (Decentralized Society) as a revitalizing transition from a pure DeFi (Decentralized Finance).

In achieving the objectives of purpose-specific, privacy-wise models, as described above, several solutions are operating in the market and can be developed. In particular, solutions based on distributed schemes (or Distributed Ledger Technologies, DLT) are gaining popularity and relevance.

Soulbound tokens, non-transferable tokens that represent a person's identity through the use of blockchain technology, are attracting significant attention.

Likewise, one-use tokens issued by reliable/trusted third parties (from Registers to banks) to prove identity on one or several attributes with minimum exposure are solutions and in-progress projects deserving attention.

Under these trends, assigned attributes and accumulated attributes will thrive – avatars, wallets, one-use tokens, Soulbound tokens, accounts as a single entry, wearables, behavior on metaverses or other extended/augmented realities – and digital identity will become increasingly **granular, multilayer, versatile, and scalable.**



Where are we?

Digital identity in public and private environments and for a myriad of purposes

Granular purpose-specific identities

High-reach / high-trust centralized models, distributed and decentralized attribute-generating/verifying models

Where are we heading to?

Digital identity for Hybrid contexts, Digital living & Metaverses and extended/augmented realities

Digital identity will become increasingly granular, multilayer, versatile and scalable.

03 **Where could we go?** Main challenges for digital identity and policy options

The future of digital identity needs to address three main challenges that gravitate around three clusters of models in tension:

- **Government-led centralized model** v. **Federated Identity models**[1] v. **Self-sovereign models**
- **Solutions integration** v. **Competitive decentralization**
- **Reliable identity** v. **Aspirational anonymity and self-governed privacy**

[1] Federated identity allows authorized users to access multiple applications and domains using a single set of credentials that federated organizations, on the basis of agreements/arrangements, commit to acknowledge.

To strike a stable balance, regulators, market players, and technology producers and solution innovators have to play with five factors: **control** (who is in control), **actors** (who is involved), **inputs** (which attributes are feeding the ID system), **outputs** (which solutions are provided), and **environment** (where the ID system will be used and what for):

Control	**Actors**	**Inputs**	**Outputs**	**Environment**
Higher public control over digital identity (DI)	Governments	Verified attributes	Cross-border recognition	In public spaces and for public purposes
Banks and other services providers	Private entities cooperating with governments to offer integrated and multilayer DI solutions	eKYC Credit scoring AML	Gateways with multilayer use specific DI	Private spaces – duty of companies to accept DI tools
Self-sovereing models	Individual in control	Avatar-generated data	Cross-metaverses recognition	Metaverses

04 **Where should we be looking at?** The most promising opportunities for digital identities

The full potential of digital identity will be unleashed if the policy challenges described above are addressed with effective, innovative, and future-proof solutions: **the most promising, less visible opportunities are there.** According to our own judgement and analysis, **there are five key drivers with the capacity to definitively fuel the potential of digital identity in the next 4-7 years.**

DRIVER 1: Cross-border recognition and global digital identity: the role of private sector

Global recognition of digital identity is critical. It entails various challenges: technological interoperability, enabling legal framework, States mutual cooperation, language considerations, harmonization and shared infrastructures, among others[2].

Although cross-border recognition is a State-based concept, how can private entities add value to their user experience and provide cost-effective solutions without undermining reliability and security? We identify three opportunities to explore:

1. Enablers of the expansion of globally accepted public digital identity

2. Interfaces for authentication

3. Reliable verifiers

Governments are investing heavily in digital identity services (Australia, France as part of NextGenerationEU, Germany, etc.). These initiatives lay the foundations for a global digital identity framework, but they do not suffice. In fact, government-promoted projects may lead to a fragmentary, inharmonious digital identity scenario.

[2] United Nations (UNCITRAL) has just adopted in July 2022 a Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services.

Therefore, ensuring cross-border (or more precisely, international) recognition of digital identity services is instrumental. The establishment of a uniform legal framework as proposed by UNCITRAL in 2022 *(Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services)* is certainly an important step forward.

Notably, the current revision of the eIDAS (electronic IDentification, Authentication and trust Services, referring to a range of services that include identity verification of individuals and businesses online and authenticity verification of electronic documents) Regulation[3] will set the scene for the future development of digital identity in Europe and point to innovations and solutions needed for the implementation of the revised framework. At the State of the Union speech, the Commission was invited to come forward with a proposal by mid-2021 on an interoperable digital signature. With such a sound, decisive backing, the prospects for the digital identity market in Europe are extremely promising. In fact, as per the Commission Communication '2030 Digital Compass: the European way for the Digital Decade', a target has been set for 80 % of EU citizens to use a digital eID solution by 2030; and on the horizon, the strategy for shaping Europe's digital future envisages a universally accepted public electronic identity.

The eIDAS expert group adopted on 22 February 2022 the *European Digital Identity Architecture (EUDI) and Reference Framework - Outline*[4] that provides a summary description of the EUDI Wallet concept – objective, roles of the actors of the ecosystem, wallet's functional and non-functional requirements, and potential building blocks. The document points some of the key issues to be included in the Toolbox and the technical Architecture and Reference Framework (ARF) – a set of common standards and technical specifications and a set of common guidelines and best practices.

The opportunity for the private sector: beyond a citizen-centric model and a government-to-government scheme. Given that a purely government-to-government scheme is neither advisable nor optimal for the purpose, the involvement of private

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.

[4] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

entities and public-private cooperation will be key to deploy an agile, dynamic, fit-for-purpose global digital identity model. Furthermore, it should be noted that the proposal ambitiously envisages a requirement for each Member State to issue a European Digital Identity Wallet within 12 months after the Regulation enters into force. In this context, the role of private sector as an accelerator for the eIDAS framework will be crucial and was expressly noted in the Evaluation Report[5].

[5] Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). COM/2021/290 final.

The involvement of private entities and public-private cooperation will be key to deploy an agile, dynamic, fit-for-purpose global digital identity model.

In focus

Reasons to endorse a public-private cooperative framework

Several reasons advise against a purely State-led model and endorse a public-private cooperative framework.

1. Government-led initiatives tend to deploy **citizen-centric models.** Such an approach entails that recognition is not always sufficiently fluent for travelers, visitors, migrants or tourists, and the role of private sector can be crucial to narrow these gaps. From health certificates for traveling purposes to professional qualifications and education credentials, non-citizen identification and authentication are required in a multitude of contexts where private entities can take the lead.

2. An increasing number of digital-identification-requiring contexts are **sole-attribute situations** - the user has to prove that has been invited to the event, legal age, proper vaccination, access permission, or enrollment in the course, for example. Full identification and official authentication are neither desired nor advisable in such circumstances. It is not only unreasonably costly, but also disproportionate for the purpose and risky for privacy.

In this line, the evaluation of the eIDAS Regulation[6] revealed the emergence of a new environment transiting from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities.

[6] Report on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), 3.6.21, COM (2021) 290.

Private sector is in the position of providing and implementing fit-for-purpose, highly-efficient, privacy-friendly, identification and authentication models for such contexts. To that end, private sector can develop a second layer in the digital authentication to be stacked on the State-led digital identification frameworks.

3. Third, attempts to ensure cross-border recognition and global enforceability of identity credentials fail in the absence of standardized digital identity credentials. States should promote standardization, but it requires intense, and world-wide cooperation. Sovereignty sensitiveness, political issues, or simply practical obstacles can jeopardize standardization or hinder a full collaboration. Private sector will find a relevant gap to narrow and a niche to focus on. Should official identity credentials be not standardized, data could.

Business opportunities for both emerging actors and incumbents point to the following business and investment opportunities:

A. providers of identity-linked services – electronic attestations of attributes

B. 'intermediary' interfaces collecting the relevant data from official identity credentials and providing standardized templates vis-à-vis the party requesting identification for each specific purpose: health-status credential for travelling, legal age, insured patient, etc.

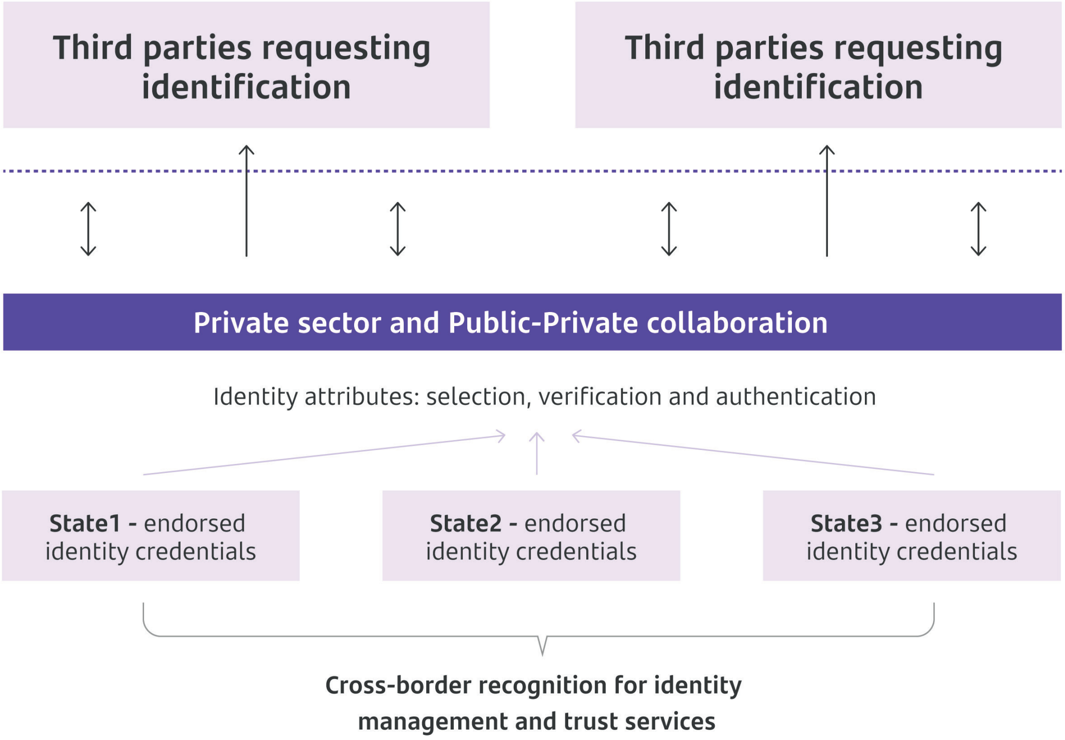
C. reliable verifiers attesting in each circumstance that the official credential of one jurisdiction is valid and enforceable in another jurisdiction – a sort of comparator of credentials.

These opportunities are fully aligned with the potential roles of actors in the EU Digital Identity (EUDI) ecosystem[7]. Hence, private sector is in a position to leverage their EU-wide footprint to global scale.

[7] eIDAS Expert Group, European Digital Identity Architecture and Reference Framework – Outline, 22 February 2022.

In performing and implementing the EUDI Wallet functionalities, some existing technologies are available and may fulfil the envisaged role. The functionalities to be provided by the EUDI Wallets can be grouped in five building blocks: user interface, data storage, complex functions/cryptographic protocols, sensitive cryptographic material, and eID means module[8].

On the one hand, form factors can be implemented by mobile applications, web applications, and/or secure applications on desk devices. On the other hand, the required supporting building blocks can rely on: backend server, official electronic identity documents, secure external hardware token, cryptographic service provider, trusted execution environment (TEE).



Third parties requesting identification

Third parties requesting identification

Private sector and Public-Private collaboration

Identity attributes: selection, verification and authentication

State1 - endorsed identity credentials

State2 - endorsed identity credentials

State3 - endorsed identity credentials

Cross-border recognition for identity management and trust services

[8] The eIDAS expert group lists the required functionalities as follows:

1. Perform electronic identification, store and manage qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA) locally or remote;
2. Request and obtain from attestations from providers, qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA);
3. Provide or access cryptographic functions;
4. Mutual authentication between the EUDI Wallet and external entities;
5. Selecting, combining and sharing with relying parties PID, QEAA and EAA;
6. User interface supporting user awareness and explicit authorization mechanism;
7. Signing data by means of qualified electronic signature/seal (QES);
8. Provisioning of interfaces to external parties.

DRIVER 2: Self-sovereign Use-specific Digital Identity models

Digital Identity Wallets encapsulate two key features of the future for digital identity: digital identity is user-centric and user-controlled. Users' identity will be assessed and verified only when needed (pertinence), to the extent that it is fit for purpose (fit-for-purpose), and exclusively revealing the essential information (minimization) – e.g. checking the age does not require to reveal date of birth, eligibility does not need to reveal the specific details of the required conditions, location does not need to disclose personal address. Emerging actors and incumbents can add significant value acting as 'identity hubs' or (one-use) identity/attribute tokens. A number of reasons and concurring factors (as listed below) endorse a particularly favorable position of banks to effectively perform this role.

As explained before, **the need to identify and verify the identity of individuals and organizations is gaining granularity, transversality, and versality.** Not only our increasingly active digital living leads to a myriad of situations requiring identification – online shopping, online banking, tax payment -, but also hybrid contexts or transactions where a prior online identification leads to the exercise of rights or the performance of obligations in person (for example in the gig economy, confirming that you are the expected passenger and that the driver holds a valid license; or to buy the medicine prescribed by the doctor in an online appointment or via an automated diagnosis app). These diverse contexts often share certain specific features:

A. Low sophistication but high need of trust. In many of these contexts, the level of technological sophistication is relatively low, for instance in P2P (peer-to-peer) transactions, but the need for reliability is still high as well as the private expectations.

B. Atomized situations. Situations where identification is required are sporadic, frequently informal, and often concluded at a swift pace – e.g. users of a P2P car-sharing app need to identify themselves before starting the journey.

C. Attribute-specific identification. Identification in these situations may require exclusively verification of one identity attribute.

As far as our digital lives expand and hybrid physical-digital contexts multiply in a wide variety of sectors and social environments, ever-growing means of digital identification and verification inundate daily relationships. Confusion, mistakes, costs, and frustration discourage users[9] and flood with inefficiencies business and social processes.

[9] Onboarding is one of the most crucial areas where providers are failing. Application abandonment by frustrated users unable to complete the onboarding process is now higher than ever, reaching as high as 70% in some countries (https://d2qcmozihn2auk.cloudfront.net/whitepapers/SG-Battle-to-onboard.pdf).

Case in point

TISA Project

Barclays, Signicat, OneSpan and Daon are among the leading firms joining the TISA (The Investing and Saving Alliance) Digital ID programme. The objective of TISA's project is to create a Digital Identity scheme that allows consumers to set up and reuse an identity to interact with financial institutions. This can then be used when applying for financial products and services, such as opening a new bank account, transferring a pension or applying for a mortgage. Financial services providers can easily verify and then authenticate a customer's Digital Identity.

Case in point

Reusable ID

There are business opportunities in providing Reusable know your customer (KYC) verifications. The main aims are to reduce duplication and redundancy in the authentication process, and streamline onboarding. Companies are developing blockchain-based solutions to facilitate reusable KYC. Once an entity has verified a user, other companies can leverage this KYC. The mutual recognition if based on trust among authenticating entities and KYC-importing entities. The incentives to share KYC and allow re-usage are economic and strategic. Authenticating entities are compensated for their verifications as well as they gain and retain customer relation.

Business opportunities for financial institutions lie in **acting as single identity point for users.** Single identity points can operate at the two ends of the communication line:

- On the one hand, the user benefits from a single interface and the service provider manages, selects, and interact with the third-party requesting identification. As an illustration, biometric-recognition app developed by Apple in their iPhones provides a single point of entry for the user to multiple third-party services. On average, each individual maintains around 100 passwords. And this number increased by 25% in 2021 alone[10]. Biometric recognition interface enables the user to manage a wallet of passwords and credentials with minimum interaction and high ease.

[10] https://tech.co/password-managers/how-many-passwords-average-person

- On the other hand, business-centric apps can assist companies and authorities in easing the identification of users in multiple contexts, for multiple purposes, and within minimum privacy- exposure. It is forecasted that by 2025, more than 6.2 billion digital identity apps will be in use, exacerbating existing problems arising from fragmentation of the market[11]. An increase of 20% in income compared to competitors is predicted for digital businesses that offer their customers a better experience during identity corroboration[12].

[11] https://www.biometricupdate.com/202010/digital-identity-apps-to-outnumber-cards-by-2023-juniper-research

[12] https://www.gartner.com/en/documents/3697317

In focus

A strong case for the role of banks as 'secure identity hubs'

Banks' efforts to implement KYC and AML obligations have placed them in an incomparable position to act as a type of **'secure identity hub'**, underpinned by public sector credentials. Leveraging these capabilities could enable new trusted identity services with user choice.

A. Trust

Successive international studies have shown that consumers trust banks the collection and the processing of their personal data. A recent Bank for International Settlements (BIS) report[13] highlighted this preference for banks over other possible actors across all demographic segments. For reasons of privacy and data protection, consumers may prefer private sector firms to handle the sensitive data attributes that comprise their 'identity', as well as the transactional history of what they buy and who they correspond with[14].

[13] Whom do consumers trust with their data? US survey evidence, BIS Bulletin, No 42, 7 May 2021 by Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster and Kelly Shue.

[14] M. Baradaran, (2015), How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy, Harvard University Press; I. Fu (2021), "The Freedman's Bank and the Persistence of Mistrust", mimeo; y E. Vaportzis et al. (2017), "Older adults' perceptions of technology and barriers to interacting with tablet computers: a focus group study", Frontiers in Psychology, n.º 8(1687).

B. Minimization and Purpose-Specific

Bank authentication is instrumental to minimize privacy exposure and ensure fit-for-purpose identification/authentication. On the basis of each transaction or authentication-requiring situations, it is decided which consumer's data needs to be passed[15].

'Zero knowledge proof' (ZKP)[16] models are highly promising, insofar as nothing additional is revealed. ZKP is a verification method between a prover and a verifier. The prover is able to prove to the verifier that they have the knowledge of a particular piece of information without revealing the information itself. In practice, the prover can prove that a given statement is true without conveying any additional information apart from the fact that the statement is indeed true. Remarkably, data minimization and user control are embedded in the design. These solutions are privacy-friendly and purpose-specific by design[17].

C. User-Centric, High-Trust Third Parties: the merits of centralized trusted third party to stave off disintermediation

There is a highly promising strategic opportunity in leveraging the dynamic between two factors: trust and reach. While Big Techs have gained a worldwide scale and taken advantage of their footprint in the digital economy by providing a very simple experience as 'identity hub' (high reach), the broad adoption of these simple solutions is instable as it is not backed by high levels of certainty and reliability.

[15] OpenID Foundation standards for Financial-grade APIs: this model envisages that consumer (or small business end-user) could instruct one of their existing trusted counterparties (such as a bank or telco or energy retailer) to verify their identity - https://openid.net/.

[16] The concept of ZKP was first described by Goldwasser, Micali & Rackoff (1989) in their paper 'The Knowledge Complexity of Interactive Proof Systems, SIAM J. COMPUT., Vol. 18, Num. 1, pp. 186-208, February 1989. In the paper ZKPs are defined as 'those proofs that convey no additional knowledge other than the correctness of the proposition in question'.

[17] Global Assured Identity Network (GAIN) - https://gainforum.org/. 'Instead of logging in directly, a user asks a trusted and regulated provider (e.g., their bank, telecommunications provider, or another regulated entity) to verify that they are the person and/or have the credentials that they claim'.

Authentication solutions provided by these platforms are convenient for users but do not provide security or verification of the identity behind an account or username[18].

Contrariwise, financial Institutions are in a very favorable position in terms of trust, as described above, and have intensely developed fundamental skills, practices, and experiences in KYC, AML, and authentication that can effectively be extrapolated wide-reach authentication solutions. Reach has to be built on cooperation agreements and collaboration models among financial institutions and with other entities[19]. Trust is a strength, while limited reach is still a weakness: the strategic opportunity is in reinforcing both.

D. Need to Unify the Fragmented Identity World

Financial institutions are in a position to leverage a window of opportunity by catalyzing a decentralized, globally collaborative, and technically interoperable identity network that overcome the limitations of citizen-centric, government-led models and gain scale and reach by stacking on trust.

Completeness is one of the key challenges of digital identity. Therefore, enabling completeness and traceability provide business opportunity to explore. Global iD[20] is working on this challenge by operating a sort of 'DNS for identity'. Identity verifications are linked to a name listed in GlobaliD's public namespace. Even if users are entitled to hold several names, and, therefore, meet their privacy-preserving expectations), traceability to create a complete view of the user is enabled by GlobaliD. Acting as an identity backbone, GlobaliD connects to identity verifiers across silos, including self-sovereign identities.

[18] WEF, A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity, August 2016.

[19] Example of a collaboration project: ID2020 Alliance - https://id2020.org/alliance

[20] https://www.global.id/

DRIVER 3: Digital identity as a revival of responsible anonymity

Digital identity tools must satisfy an increasing demand for 'responsible anonymity' in digital environments. A delicate balance needs to be struck: reliable, certain identity with higher standards of identity protection and a growing demand to minimize privacy exposure.

It can be observed how several of the identified drivers jointly explain the emergence of certain solutions, and how certain models are devised and evolved in response to several of these drivers. In particular, the investment in responsible anonymity is bringing about solutions, applications, and business opportunities that concurrently reinforce Self-Sovereign Identity, and provide purpose-specific identity solutions (driver 2), while demanding user-centric solutions performed by private actors beyond citizen-centric solutions led by governments and public authorities (driver 1).

Under this driver, attention is caught by two promising models:

A) Soulbound Tokens

The authors of the recent paper on Decentralized Society[21] who have coined the concept of Soulbound Token encapsulate this emerging paradigm in the following description:

> *Rather than privacy-as-transferable-property-right, a more promising approach is to treat privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information. Under such a paradigm, every SBT—such as an SBT that represents a credential or access to a data store—would ideally also have an implied programmable property right specifying access to the underlying information constituting the SBT: the holders, the agreements between them, the shared property (e.g., data), and obligations to 3rd parties (p. 15).*

[21] Weyl, Eric Glen and Ohlhaver, Puja and Buterin, Vitalik, Decentralized Society: Finding Web3's Soul (May 10, 2022). Available at SSRN: https://ssrn.com/abstract=4105763 or http://dx.doi.org/10.2139/ssrn.4105763

Soulbound tokens allow users to prove who they are without disclosing their identity or having a central authority vouch for them. Thus, they enable privacy-friendly identity tool, as well as the exercise of responsible anonymity. Users can have multiple anonymous but verifiable identities known as Souls using Soulbound Tokens.

Soulbound tokens are held by Souls. A Soul is the account or wallet of a user that can hold Soulbound tokens. A Soul can be a person, an institution, or any entity. In principle, as a user can have several Wallets to hold crypto assets, NFTs or any type of digital assets, they can also have several Souls. However, and interestingly, only a specific Soulbound token can be held in one Soul and it cannot be transferred to another Soul.

Unlike the centralized, bureaucratic schemes to confer identity in the current economy (a "driver's license"), the new paradigm of a Decentralized Society relies on horizontal ("peer-to-peer") social attestations with Soulbound Tokens. Thus, Soulbound tokens are permanent, non-transferable, non-fungible tokens (NFTs). Soulbound Tokens, as essential catalyzers of the transition from DeFi (Decentralized Finance) to DeSoc (Decentralized Society) have no significant financial value. The value that Souldbound Tokens provide is proof of the Souls' history or connected communities.

Among the possible applications, Soulbound Tokens can provide person-centric solutions for the following purposes: identity and authentication, credit scoring, KYC requirements, DAOs (Decentralized Autonomous Organization) and a variety of cooperative forms, verified contributors, or voting. Soulbound tokens will be multiple and varied, as they can be issued under diverse modes or in different conditions. Some examples can illustrate different possibilities to explore:

- Some issuers would choose to make Souldbound tokens wholly public.
- Some Souldbound tokens, such as a passport or health records, would be private in the self-sovereign sense with unilateral rights to disclose by Souls who carry the Souldbound tokens.
- Others, such as Souldbound tokens that reflect membership of a data cooperative, would have multi-signature or more sophisticated community voting permissions, where all or a qualified majority of token holders must consent to disclosure.

In focus

Who is issuing Soulbound Tokens?

Binance is issuing Soulbound Tokens as identity credentials for users who completed KYC verification. It is called Binance Account Bound (BAB). Binance is a blockchain ecosystem and cryptocurrency infrastructure provider that includes the largest digital asset exchange by volume. The Soulbound token, BAB, displays in the wallet to accredit that the holder has been assessed by Binance as per KTC requirements.

As announced by Binance, its Soulbound Tokens (BAB) have the following features. First, BAB are non-transferable. Thus, users cannot transfer BAB tokens to other users. Second, BAB are revocable. So, users can revoke their BAB tokens. Third, BAB are unique. Hence, one verified Binance user ID allows the user to mint one BAB token only on a certain chain.

Upon the announcement of the issuance, fourteen leading web3 projects have adopted Soulbound Tokens and give BAB token holders exclusive incentives. For instance, BAB holders will have special voting rights to enhance DAO governance and dispute handling; BAB holders are exempted from KYC and are granted voting rights; and it will be displayed on a user's profile to signify a real user (not bots).

B) One-use tokens issued by reliable entities on identity and/or certain attributes

This model combines the business opportunity of acting as a 'secure identity hub', the goal of minimizing privacy exposure with attribute-specific solutions, and the benefits of decentralized society with NFTs.

A trusted third party (registrar, financial entity, reliable actor, etc.) issues, upon request of the user, a one-use token related to the user's identity and/or one or several attributes. The user employs that token to be identified, access a service or accredit a required attributed (legal age, enrolment, tax compliance, employee, etc.).

DRIVER 4: Biometric recognition and authentication services for a physical-digital living

Face biometrics will push an innovative, promising digital identity market. A number of hybrid physical-digital contexts will benefit from ease, reliable face biometric identification and authentication. Several converging factors predict an encouraging expansion of the sector.

A. No face-to-face interactions. As a by-product of the social-interaction restrictions implemented to contain the COVID pandemic, many 'contactless', distance-respectful devices have been deployed for identification and authentication in physical environments. From access control for employees to public buildings, universities or private companies, to passport control, biometric recognition is widely used.

B. The unprecedented growth of tele- and remote working brings about a multitude of professional and labor situations where an immediate, effective identification of individuals is needed. Facial recognition can be used for working-hour assessment, for training attendance verification, for guaranteeing eligibility to confidential or restricted meetings, spaces, or data.

C. The popularity of mobile applications (including other handheld devices) has enabled a widespread implementation of facial recognition for unblocking devices, accessing apps, expressing consent in a variety of transactions (confirming funds transfer, modifying relevant personal details, signing or downloading digital content), or making payments.

D. Traditional onboarding processes are aimed to migrate to purely digital activities – opening an account, KYC checking, ALM (Application lifecycle management) processes, asking for a loan, etc.

E. Verification in the platform economy is gaining scale and relevance. Interestingly, the recently adopted DSA[22] provides for KYBU (Know-Your-Business-User) requirement for online B2C marketplaces.[23] Accordingly, online platforms 'allowing consumers to conclude distance contracts with traders shall ensure that traders can only use those online platforms' if, prior to that, they obtained certain information of the trader and make best efforts to ensure that is complete and reliable.

In all these scenarios, facial recognition together with video identification and authentication may enable to unblock many hurdles of onboarding processes, streamline recurrent identifications processes in professional, political, or educational environments (voting, authorized employees, enrolled students, etc.), and enhance security and certainty in a multitude of business and social contexts (business meetings, social events, seminars, etc.).

As per the most recent Gartner Hype-Cycle (2022), third-party biometrics is going now through the stage of disillusionment. That means to estimate between 2 to 5 years to reach the plateau of productivity. Within such a time frame, interests are still attracted by biometrics-related solutions. Video identification, in particular, in the most biometrics-intensive modalities can be still raising high levels of expectations and providing, in the specific societal and technological circumstances, effective solutions in developing economics – paired to the high penetration of mobile devices for financial services and contracting (m-money and m-commerce).

In focus

Where to look at? The possibilities and the limitations of video identification

Customer onboarding is a key bottleneck process for many sectors (particularly critical for some of them, such as financial, banking or insurance). It is a costly, time-consuming, and complex task that is normally initiated or completed with face-to-face interactions. However, a thriving digital economy cannot depend upon face-to-face processes.

Video identification is a burgeoning solution to look at. Video identification is a process of identification and verification of identity based on a high-definition video that is recorded, showing the person and their document live, in great detail. The video is recorded and sealed electronically for its integrity, as well the primary data such as IP address, device and location as main electronic evidence of the identification

An enticing variant of facial recognition is 'Smile ID'. The user's identity is authenticated by recognizing and verifying their smile. It is a quick, easy, and effective method that may entail the minimization of the privacy exposure. It may reduce the scope and the amount of the collected and stored biometric data. Thus, the cybersecurity risk of authorized access, or cloning is limited.

Within this realm, some companies are leveraging the combination of biometrics with mobile phones to enable authentication in developing economies in Africa and Southeast Asia, while others are similarly leveraging biometrics, and other advanced techniques, to enable mobile authentication globally.

DRIVER 5: Digital identity in the extended/augmented realities

Digital identity will become a cluster of digital identities accompanying our 'digital living' in the metaverses and other extended/augmented realities. Digital identity concept and tools must evolve to embrace, enable, and innovate in the promising and complex phenomenon of multiple digital identities: portability, avatar-generated reputation, manifestation of private rights, extension of personal data, extended and augmented reality. The new immersive technologies will not function and flourish without a sound, reliable digital identity. An effective way to implement general-purpose digital identity is still to emerge and expand.

Identity solutions in the metaverse need to provide effective, easy mechanisms to access and build meaningful connections between the user's identity, their devices and their avatars. Portability will be crucial. Companies that wish to attract more users will need to enable them to carry their digital identity across the metaverse, regardless of the entry point or platform — for example, implementing the universal virtual studio technology (VST)-like standard for audio avatars.

Case in point

On which solutions are companies working?

Tools that abstract the onerous key management process, enabling end-users to log-in into dApps (decentralized applications) without the use of third-party software. dApps are decentralized applications that run on a blockchain or peer to peer network of computers instead on relying on a single one. Thus, dApps are outside the purview of and free from interferences of a single authority. Developed solutions allow the user to easily integrate their app with the Ethereum blockchain, whether the user already has a dApp integrated with web3 or is starting from scratch.

Privacy-preserving browsers or browsers compatible with a tokenized identity system specifically designed to work with a variety of decentralized apps, or dApps, as well as provide deeper functionality than a traditional browser that has a basic web wallet add-on. The browser also includes a new native non-custodial crypto wallet which allows you to access your crypto or sign into dApps directly from the browser, without installing any extensions.

In focus

Challenges in the metaverse… that can be a strategic opportunity

1. Securing IoT devices

Our ‘immersion’ in the metaverse and our interaction with a variety of extended/augmented realities depend upon and are ‘interfaced’ by a universe of devices - Augmented Reality (AR) glasses, Virtual Reality (VR) Headset, VR gloves, Wrist-Based Bands, etc. These interconnected devices are instrumental to ensure a safe, reliable, and quality immersive experience in metaverse and augmented/extended realities. Risks related to are numerous and varied, from the security of the hardware devices, to the protection against vulnerabilities and exposures of firmware and software.

Which solutions are being developed?

- Solutions to ‘monitor traffic between devices and cloud environments in order to detect behavioral anomalies or traffic patterns which could be indicative of a threat or data exfiltration’.
- Solutions to protect IoT/OT devices from firmware security issues, common vulnerabilities and exposures (CVEs), insecure secrets, and a multitude of other security problems in plugin IoT devices and embedded firmware.
- Solutions and services on asset discovery, vulnerability management, and continuous monitoring of threats.

2. Data and privacy:

Privacy exposure is a risk to counter in the metaverse and in augmented/ extended realities. The immersive and the sensitive characteristics of these experiences may aggravate the severity of the privacy exposure and/or the gravity of the impact in case of infringement. On the other hand, in the absence of sound and reliable identification mechanisms (digital identity solutions) in these scenarios, risks for impersonation, fraud, unauthorized uses, or untraceable transactions raise. Consequently, business opportunities flourish both in the realm of privacy-protection solution and in the scope of identity-verification ones.

Which solutions are in the market?

- Investigation software that connects cryptocurrency transactions to real-world entities, examining criminal activity, such as the movement of stolen funds, as well as legitimate activity like flash loans and NFT transfers.
- Account takeover and fraud prevention solutions - collection of recaptured data from breaches, malware-infected devices, and other underground sources.

05 Final Insights

Digital identity is a thriving market. Five drivers fuel its growth and expansion potential in the coming years. Value creation and innovation and investment opportunities gravitates around the trends traced (or pointed) by these five drivers.

Digital identity is veering towards granular, purpose-specific models. The most promising solutions pivot on the possibilities of providing, verifying, and authenticating digital identity or specific attributes for a specific purpose (legal age, vaccination, eligibility, etc), with low privacy exposure, and high versatility. Two models, as discussed, are aiming to face this trend. On the one hand, centralized models with 'secure identity hub' (trusted third parties), but also aggregators, interfaces, and verified one-use tokens. On the other hand, decentralized or distributed solutions such as Soulbound Tokens and functionally equivalent solutions.

Against such a backdrop, **cross-border digital identity models are going to be instrumental in the next years.** The EUDI model provides an incomparable opportunity to test solutions and will reveal enticing areas for investment. Close attention should be paid at the standards and technical requirements that the implementation of the EUDI Wallet and the development of the toolbox will point to.

The potential of biometrics identification is still expanding and proves to provide a versatile solution for online, offline, and hybrid environments. Despite the fact that some solutions, such as the video identification, seem to have lost momentum, biometric applications pervade a wide variety of identity-requiring, and identification-requiring situations.

A forward-looking strategy needs to integrate and address other challenges posed by a 'multiplied' digital living in extended/augmented realities. An integral, comprehensive protection of digital identity in the metaverse and augmented/extended realities require a combination of solutions for securing the devices, protecting the firmware/software, and preserving the data and digital content.

Author

Teresa Rodríguez de las Heras Ballell

Professor of Commercial Law at University Carlos III of Madrid, Spain

Academic Visitor at the Faculty of Law, University of Cambridge, 2022-2023; Sir Roy Goode Scholar at UNIDROIT, 2021-2022. Arbitrator at the Court of Arbitration of Madrid and of Spain. Member of the following EU Expert Groups assisting the EU Commission: Expert Group on Liability/Technologies formation authoring the Report Liability for AI and other emerging technologies; Expert Group to the EU Observatory on Platform Economy; Expert Group on B2B Data Sharing and Cloud Computing.

esade

Santander X Innovation Xperts

www.santander.com/santander-x-innovation-xperts-en

By Santander