POLITECNICO
MILANO 1863

School of Industrial and Information Engineering

Master of Science in Management Engineering

THE ECOSYSTEM OF STARTUPS WORKING IN THE DIGITAL IDENTITY FIELD: AN INTERNATIONAL CENSUS AND AN ANALYSIS FRAMEWORK.

Supervisor: Luca Gastaldi

Author: Clara Pierpaoli, 976444

Academic Year 2021/2022

Contents

Table of figures

Abstract

English version

The rapid expansion of the digital transformation trend and recent global events, characterized by the Covid-19 pandemic, have drastically altered how people around the globe conduct business and interact. To ensure the security of online and offline transactions, from humans to inanimate objects, a dependable and trustworthy digital identity has become fundamental. To understand which policies, technologies, and standards are essential to a successful digital identity system, it is necessary to outline a framework that includes all the entities involved. Therefore, the purpose of this paper is to provide an international perspective on the startup ecosystem in the digital identity sector. The primary objective is to identify the distinctive features and traits of this ecosystem.
Using an empirical framework, a trustable dataset containing 331 startups was compiled to accomplish this goal. The information obtained from the database was combined with secondary sources to create a profile of the various characteristics exhibited by the sampled startups. To answer the report's research question, the subsequent analysis results were reviewed and interpreted in the context of existing literature on the topic.

Keyword: KYC, Biometrics, Self-sovereign, Passwordless, SSI, Identity, E-signature, Onboarding, ID wallet, Authentication.

Versione italiana

La rapida espansione della trasformazione digitale e i recenti eventi globali, caratterizzati in primis dalla pandemia di Covid-19, hanno drasticamente modificato il modo in cui le persone in tutto il mondo interagiscono. Per garantire la sicurezza delle transazioni online e offline, sia tra esseri umani che tra oggetti inanimati, una identità digitale affidabile e di fiducia è diventata fondamentale. Per comprendere quali politiche, tecnologie e standard sono essenziali per un sistema di identità digitale di successo, è necessario delineare un quadro che includa tutte le entità coinvolte. Pertanto, lo scopo di questo lavoro è fornire una prospettiva internazionale sull'ecosistema di startup nel settore dell'identità digitale. L'obiettivo principale è identificare le caratteristiche e i tratti distintivi di questo ecosistema. Utilizzando un framework empirico, è stato compilato un dataset affidabile contenente 331. Le informazioni ottenute dal database sono state combinate con fonti secondarie per creare un profilo delle varie caratteristiche delle startup campionate. Per rispondere alla domanda di ricerca del report, i risultati dell'analisi sono stati poi esaminati e interpretati nel contesto della letteratura esistente sull'argomento.

Keyword: KYC, Biometrics, Self-sovereign, Passwordless, SSI, Identity, E-signature, Onboarding, ID wallet, Authentication.

Introduction

As a core element of economic and social development, digital identity is gaining increasing significance in contemporary society. According to the World Bank, under 850 million people cannot prove their identity— around 1 in 9 globally in 2021, noticing an improvement compared to the data collected in 2018, where around 1.1 billion people didn’t have official proof of ID. This represents a mix of improvements in ID coverage (between 100-200 million), methodology changes and the addition of new data sources used in the analysis (World Bank, 2022). Individuals without certified identity are unable to access basic public and private services, such as healthcare, education, and financial services, without a reliable form of identification. This identity gap is a major barrier to participation in political, economic, and social life (GSMA, World Bank Group, 2016).

The proliferation of the internet has transformed our daily lives, and we are moving toward a world where digital interaction and commerce are the norm. With the development of new technologies such as artificial intelligence and biometrics, the services we receive are becoming increasingly individualized, and identification is of paramount importance.
This presents companies and banks with an opportunity to become multi-sector ID providers. In the coming years, the number of people actively connecting online is expected to increase exponentially. The Internet of Things (IoT) will also grow, with millions of items such as refrigerators and containers becoming internet-connected and requiring identification.

Cybersecurity, which is a growing concern for both businesses and governments, is one of the primary obstacles facing the digital identity space. Identity management is vulnerable to threats such as data theft, password loss or cracking, and impersonation. Large-scale hacking attacks are on the rise, while identity theft is a pervasive problem. As more users' information is dispersed online, data privacy also presents a difficulty. This results in a feeling of lack of control over our digital ID; therefore, regulation plays a crucial role in ensuring the controlled and legitimate use of personal data. To confront these issues since 2018, Europe has implemented the General Data Protection Regulation (GDPR), the most stringent privacy and security law in the world. Even though it was drafted and adopted by the European Union (EU), it imposes obligations on organizations everywhere that target or collect data related to EU residents (European Commission).

Despite the obstacles, establishing one's identity is a fundamental human right. The G20 acknowledged digital identity as a priority for achieving social and economic inclusion during the Italian Presidency in 2021, as part of its larger commitments to advance digital government through the work of the G20 Digital Economy Task Force (DETF). The Universal Declaration of Human Rights also recognizes everyone's right to be recognized as a person before the law (IBM, 2020).

Efforts are being made to establish digital identity frameworks that allow individuals to verify their right to live, work, and study in different countries while protecting their personally identifiable information. The European Commission, for instance, is working to deploy European Digital Identity Wallets, where citizens can securely store their credentials (IBM, 2020). By leveraging digital identity technologies, organizations across all industries have the opportunity to increase efficiency, strengthen security, and create new ways for people to work, shop, and travel (IBM, 2020).

In conclusion, the centrality of digital identity in modern society is growing, and efforts are being made to establish reliable forms of identification while addressing cybersecurity and data privacy concerns.

It is a fundamental human right to be able to demonstrate one's identity, and the adoption of digital identity technologies can increase efficiency, bolster security, and create new opportunities across multiple industries.

Having emphasized the importance of Digital Identity, it is essential to gain a comprehensive understanding of its definition, operation, of the parties involved, and various ecosystems. Furthermore, it is important to comprehend the potential future directions of this industry. Examining the startup ecosystem can yield insightful information about the market and its future evolution.

This thesis intends to investigate the topic of Digital Identity and analyse the startup ecosystem. To achieve this, the work is organized into four chapters.

- Chapter 1 – Literature review: provides an introduction to the subject of Digital Identity. As compiled from various articles, reports, and books, it aims to cover the main aspects and implications of Digital Identity.

- Chapter 2 – Research methodology: describes the entire research procedure, from the theoretical review to the empirical framework. It formalizes and clarifies the employed research methodology.

- Chapter 3 – Results: presents the findings of the analysis and provides an overview of the Digital Identity market for startups.

- Chapter 4 – Conclusions: the findings are summarized, the research question is answered, and potential future in-depth analyses are discussed.

Chapter 1: Literature review

This section presents an analysis of the current literature on digital identity. Although the subject has been examined by a variety of academic fields, including information systems, public administration, and law, a complete viewpoint is still lacking that can help people better comprehend the benefits and difficulties that digital identity presents. A multidisciplinary approach is used to investigate the possible advantages of a digital identity system to address this. The section also discusses the management systems and enabling technologies that are used to manage digital identities, including blockchain technology, biometric authentication, AI, SDK and API.

1.1 Definition

An identity (ID) is a set of one or more attributes that allows an entity or person to be sufficiently distinguished or uniquely identified (GPFI 2018; Sunberg et al, 2018). While the true nature of any identity is multifaceted, the functional purpose is to prove the uniqueness of an individual, ensure accountability, establish trust, and provide a point of reference for legal, social, and economic transactions.

Identification is the process of establishing information about an entity or individual based on a set of attributes that uniquely describes them. Key parameters of an identity are uniqueness, recognition, and coverage.

A digital identity is one where most aspects of the system that enables it are accomplished digitally. While some digital identities are almost entirely digital, many are built upon pre-existing non-digital identification systems with only some aspects being digitalized. In these cases, digitalization can either replace existing mechanisms, or complement them (Kanwar et al., 2022).

The World Economic Forum 2016 defined digital identity as a *"collection of individual attributes that describe an entity and determine the transactions in which that entity can participate*".

McKinsey separates identification by identity*: "identification is the means by which we prove we are who we say we are. This is distinct from identity, which is an individual's unique set of attributes. Identification provides a mechanism to authenticate identity".*

An identification system is defined as the database, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose. (The World Bank Group, 2018a)

According to the definition coined by the Digital Identity Observatory of Politecnico di Milano, *"a digital identity is a set of data that uniquely identifies a person, company or object and that is collected, stored and shared digitally within an ecosystem of actors and through enabling technologies, and that enables access to value-added digital services".*

1.2 Pillars

It is helpful to follow the framework created by the research from the Digital Identity Observatory of Politecnico di Milano in the report “Alla ricerca dell’identità…digitale”, which outlines four pillars of digital identification systems, to continue the analysis of the literature.

The collection of information that makes up an identity profile is the basic tenet of digital identification systems. Both static and dynamic data are included in this. Biographical and biometric information are examples of relatively fixed information known as static data. On the other side, dynamic data describes interactions made possible by a digital identity, like online transactions and activities.

The organization of the ecosystem of actors involved in digital identification is the second pillar of digital identity systems. Depending on the system's concept and architecture, this also includes the numerous people and groups who fill a variety of responsibilities within it. For instance, in a decentralized system, identities may be handled by several different independent entities as opposed to a single authority in a centralized system.

The supporting technologies for digital identity systems make up the third pillar. The three basic categories of these technologies are architecture, integration, and process. While integration technologies are used to link various parts and systems together, architectural technologies relate to the foundation that underpins the digital identity system. Digital identification system processes are managed and carried out using process technologies.

The value-added digital services that can be accessed through the system are the fourth and last pillar of digital identification systems. Both online and offline, these services can be connected to a wide variety of various application domains. Digital identity systems, for instance, can be used to access a variety of services, including e-government, healthcare, and financial services.

1.3 A good digital identity

This paragraph illustrates the primary characteristics of a "good digital identity," which is a precise, secure, and reliable online representation of a person or organization. Nowadays, anyone can create a profile on multiple social networks, but this type of digital identity is typically not regarded as trustworthy because it is not verified by a trusted authority. Typically, social networking profiles are self-reported and can be easily impersonated or fabricated.

Certified digital identities, on the other hand, match the standard for a " good digital identity ", are validated by a trusted authority, and are frequently used for high-risk activities that demand a high level of trust and security. A Certificate Authority-issued digital certificate, for instance, can be used to authenticate a website or secure online transactions.

The McKinsey Global Institute in his report on digital identification has underlined the characteristics of "good digital identity", which should have the following four attributes:

- Verified and authenticated to a high degree of assurance. High-assurance digital ID meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses. This attribute does not rely on any underlying technology.
- Unique. With a unique digital ID, an individual has only one identity within a system, and every system identity corresponds to only one individual.
- Established with individual consent. Consent means that individuals knowingly register for and use the digital ID with knowledge of what personal data will be captured and how they will be used. Protects user privacy and ensures control over personal data.
- Protects user privacy and ensures control over personal data. Built-in safeguards to ensure privacy and security while also giving users access to their personal data, decision rights over who has access to that data, with transparency into who has accessed it.

Others and compatible characteristics with the one above cited of a "good digital identity" were defined by a multistakeholder group curated by the World Economic Forum 2018, individualizing five key components:

- Fit for purpose. A good digital identity offers a reliable way for individuals to build trust in who they claim to be, to exercise their rights and freedoms and/or in their eligibility to carry out digital interactions.
- Inclusive. An inclusive digital identity enables anyone who needs it to establish and use a digital identity, free from the risk of discrimination based on their identity related data, and without facing processes that exclude them.
- Useful. A useful digital identity offers access to a wide range of useful services and interactions and is easy to establish and use. At present, many digital identities have onerous and repetitive requirements and limited uses.
- Offers choice. Individuals have choice when they can see how systems use their data and are empowered to choose what data they share for which interaction, with whom, and for how long.
- Secure. Security includes protecting individuals, organizations, devices and infrastructure from identity theft, unauthorized data sharing and human rights violations. Such security is often inconsistent at present.

1.4 Benefits and challenges

Digital identity is becoming an essential infrastructure to respond to the needs of the twenty-first century.

The COVID-19 pandemic in 2020 and 2021 was a significant factor that accelerated the evolution and adoption of digital identity systems. Those nations with robust digital identity, digital databases, and digital payments prior to the pandemic were able to target new social assistance recipients on a larger scale and make payments more efficiently and securely via digital methods (World Bank Group, 2021).

The recent pandemic has compelled numerous industries to relocate a substantial portion of their operations to cyberspace. simultaneously familiarizing individuals with cyberspace and their new everyday reality. In a sense, this has been even more significant because it has contributed to a cultural and behavioural shift. To cite a real example In Italy, the government has spent nearly a decade attempting to persuade the populace to acquire a digital identity known as the Sistema Pubblico di Identità Digitale, SPID, which is state-issued and grants access to a variety of e-government services. The outcomes have been disappointing. Over the course of several years, only 4 million people (out of 60 million) obtained a SPID, and a small percentage of those individuals used it so infrequently that it expired in many instances. Due to the lockdown and the need to be authenticated online to access services (and, most importantly, to receive subsidies covering the loss of income), SPID adoption has increased by 100% in just two weeks (Saracco R., ITU, 2020).

Consequently, the importance of identification is increasing, as more human activities and transactions are conducted online and are becoming mobile. This trend creates new opportunities and new vulnerabilities and prompts the need for digital identity.

An adequate digital identity system has the potential to unlock a significant amount of value, which McKinsey estimates to be around 3% GDP equivalent for mature economies and 6% GDP equivalent for emerging economies (McKinsey, 2019). Advantages would either be for corporate and public entities, or for individuals.

Referring to individuals the main benefits are:

- Increased use of financial services. Digital ID helps individuals meet Know Your Customer (KYC) requirements and enables remote customer registration for financial services (McKinsey, 2019). Opening the access to financial services and line of credits to people that now can’t have these possibilities.
- Improved access to employment. Better digital talent matching and contracting platforms are enabled by digital ID programs, which allow job seekers to authenticate. The combination of identification coverage and high-assurance digital platforms could also boost labor productivity (McKinsey, 2019).
- Greater agricultural productivity from formalized landownership. By enabling formal land titling, digital ID could help improve incentives to make larger and longer-term investments in farming. This could increase farm yields by roughly 10 percent. Digital ID could also bring benefits to farmers through better targeting of agricultural support, including through crop insurance or agricultural subsidies.

- Time savings. Digitization of sensitive identity-related interactions enables process streamlining and automation while reducing the need for travel, a particular benefit for people who live in rural areas. Digital ID also could facilitate streamlined tax filing by providing the ability to connect information across sectors to prepopulate forms, while separately saving time for tax departments in processing and auditing.

On the other hand, looking at public institutions and private organization the most important benefits are five:

- Time and cost savings. Institutions using high-assurance ID for registration could see up to 90 percent cost reduction in customer onboarding. By enabling streamlined authentication to improve the customer experience in digital channels, institutions could also influence customers to choose digital offerings that are cheaper to provide.
- Reduced fraud. Digital ID can help reduce fraud in a wide range of transactions, from decreased payroll fraud in worker interactions to reduced identity fraud in consumer and taxpayer and beneficiary interactions.
- Increased sales of goods and services. Through digital onboarding, which enables streamlined authentication and improves customer experience in digital channels, institutions could increase uptake of new products and services. Institutions that already rely on some form of high-assurance identities, such as banks and digital gig economy platforms like Uber, have the most to gain. Institutions that interact with individuals without the use of any identities, for example online merchants and informal employers, also will profit, but to a lesser degree.
- Greater employment and labour productivity. Digital ID can help expand and improve talent matching, streamline employee authentication, and enable contracting with non-traditional workers, such as contract and gig workers. As a result, businesses could more rapidly fill open positions and find the right employee for a given position, leading to higher productivity. The need for streamlined employee authentication processes is rising.
- Increased tax collection. Greater revenue facilitated by digital ID could expand the tax base, helping promote formalization of the economy and more effective tax collection. Emerging economies could experience substantial benefits—although to realize such benefits, they would first need to make it an explicit goal and then build the requisite tax collection tools enabled by digital ID programs.

Considering the global strategy for social welfare and sustainable development, it's critical to emphasize, as stated in the report "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation "(GSMA-World Bank Group – Secure Identity Alliance,2016) a broader digital identity adoption could lead to significant improvement in:

- Gender Equality: because of social and economic restrictions, women are less likely than men to have access to a personal identification. They are consequently less likely to be able to exercise their ownership rights over property and financial resources, as well as to obtain public and private benefits and services including welfare payments, medical treatment, and financial services. The inclusion and autonomy of women can be improved through increasing their identity.

- Access to Health Services: Countries must be able to identify potential recipients of health benefits and services to improve access to healthcare and universal coverage (immunizations, insurance, etc.). Furthermore, civil and population registry-based systems for digital identification and vital statistics (CRVS) can be used to track service delivery and monitor health goals.
- Social Safety Nets: Social protection programs, such as those that offer humanitarian and disaster aid, can swiftly, safely, and conveniently reach recipients by using digital transfers when the poor and vulnerable are correctly identified.
- Governance: Systems for digital identity enhance the accountability, transparency, and efficiency of government. Digital ID solutions lower operational expenses and the corruption and theft that occur in paper-based systems, where entitlement payments are diverted from their intended beneficiaries, through online transactions and other e-services. Governmental institutions are improved in terms of effectiveness, accountability, and transparency thanks to authentication processes based on national identity records.

Digital identity has the potential to enable development, but there are challenges that hinder the establishment of official identification systems. These challenges include political factors, outdated legal frameworks, and concerns around data protection, privacy, cost, and sustainability. To create and maintain efficient, reliable, and trusted systems, stakeholders must address and mitigate these risks by implementing appropriate measures to safeguard sensitive information, developing clear legal and regulatory frameworks, and ensuring long-term sustainability and accessibility. Here a list of the most common issues in the digital identity world:

- Insufficient user control: Good digital identities offer users choice in determining how their identity data can be used. Inconsiderate customer data use can cause irreparable reputational damage (Word Economic Forum 2020).
- Improving privacy and security is a critical area for digital identity. Building trust between different parties in the digital world presents new challenges that can multiply potential fraud or misuse of personal data. Governments and non-government organizations have developed principles to guide the treatment of dynamic digital identities considering these risks, including the user control principle, transparency principle, and data minimization principle (Arner et al., 2018).
- Legal certainty is also crucial to guarantee interoperability across different countries and sectors, provide similar experiences for users, and provide business productivity and a level playing field among firms. Countries that adopt digital identity systems must have robust legal and

technical frameworks for data protection and privacy (Krämer et al.,2020). Transparency is key, and the purpose for collecting and using data should be clearly defined and assessed to balance the need to collect and store sensitive personal data and the program's benefits.

- Lack of regulation and interoperability is another challenge in the digital context (Sunberg et al, 2018). Each service provider uses its own functional digital identity that cannot be reused in other domains. Fragmentation leads to a proliferation of accounts whose data is collected and stored in many different places, making it challenging for users to manage. Interoperability is a necessary condition to offer complete solutions, and a global public or private identity is not a viable option in the short term.

1.5 Difference physical and digital identity

Despite evident differences, digital and physical identity are becoming increasingly intertwined, as more and more activities and interactions take place online. To address these complex issues, the Digital Identity Observatory of Politecnico di Milano has identified four key characteristics that distinguish digital and physical identity: proliferation, validity, related ecosystem, and dynamic nature of data.

- Proliferation: In the case of physical identity, each person may own one or many valid and accepted identity tools, which are frequently associated with a physical document, such as a driver's license, identification card, or passport. In the case of digital identity, however, this limitation is more subtle, as multiple online systems and platforms with varying degrees of trustworthiness enable the building of an interoperable data profile within an ecosystem. It is possible to activate and possess multiple digital identities at the same time: from those issued by social networking platforms, such as Google and Facebook, which allow access at other service providers in single-sign-on mode, to digital identities linked to national systems, such as, for example, CIE (Electronic Identity Card) and SPID (Public Digital Identity System), which typically allow access to public services, through identities in the business sphere, such as those issued by Microsoft, IBM, and Oracle.
- Validity: Physical identification documents are often accepted throughout the country and, in many instances, abroad as well. It is feasible to board a flight or request a service at the counter of a public institution with a legally recognized identification paper. Digital identity, on the other hand, follows a fundamentally different logic: it is exclusively recognized inside the ecosystem of actors who have chosen to join the system and established the necessary technological infrastructure to interact with the Identity Provider (IdP).
- Associated ecosystem: Regarding physical identity, the entity that issues the identification document does not participate in later encounters in which it will be exhibited. So, the IdP's duty is restricted to the identification of the applicant and the subsequent issue and administration of the document. But, a significantly different setting emerges for digital identity, whose ecosystem is extremely interdependent. At a minimum, the user, service provider (SP), and identity management commence the exchange of identifying data required for

the delivery of the service requested by the user with each encounter. For a user to access an online service or third-party app, for instance, using Facebook Login, a data transfer (name, email address, date of birth, etc.) must occur between the social network and the service provider.

- Dynamicity: Physical identity consists of a specified and static set of data identifying the individual, including biographical data and, in some situations, biometric data gathered and kept during identification. Digital identity, on the other hand, comprises of a potentially much more dynamic data set, characterized by the high frequency of data updates and, ideally, the ability to link additional information pertaining to the user's digital interaction history to the basic profile. Depending on the sector of reference, the digital identity profile may be augmented with legal information, health data, or financial data, for instance. Dynamism and abundance of the data that comprise a digital identity are the characteristics with the greatest potential to generate chances for improvement.

1.6 Models

Once more considering the five models described by the Digital Identity Observatory of Politecnico di Milano in its report “Alla ricerca dell’identità…digitale” in order to comprehend digital identity and the various configurations that comprise it:

- Social ID, which consists of the user's self-reported data when registering for a social site. This model is distinguished by a low level of verification and frequent updates and enhancements. It can also be upgraded for access to low-importance digital services. This concept is illustrated by identities generated on Facebook or Google.
- eCommerce ID, which shares similarities with the Social ID model but is based on eCommerce platforms or marketplaces. Examples of this paradigm include Amazon and Shopify-created IDs.
- eGov ID, which combines government agency-developed and-deployed digital identity technologies. These systems enable citizens to utilize public services by identifying them in a unique manner. This paradigm is exemplified by the CIE (Electronic Identity Card) system in Italy.
- Financial ID, which is the profile of identifying information acquired by a financial institution to identify its customers. This paradigm is enhanced in Single-Sign-On mode at additional service providers. The Swedish BankID system and the identity produced with the PayPal service are examples of this paradigm.
- Mobile ID, which relies heavily on the SIM card as an aspect of security for identity data. This model is often gathered and validated with moderate to high assurance. The Belgian itsme system is a good illustration of this paradigm.

1.7 Phases

This section describes the various stages of the identity management process, including the primary front- and back-end interactions. The focus of the analysis of the life cycle of digital identity will be digital identities representing individuals. It begins when a person applies for a new digital identity and concludes when the record is removed and the identity is invalidated due to death, a request by the individual, or another event (Group of the World Bank, 2018b).

Accordingly, to the report Technology Landscape for Digital Identification by Group of the World Bank 2018 there are five different and subsequent macro-steps:

1. Registration (Identity Proofing)
2. Issuance (Credential Management)
3. Identity Authentication
4. Authorization
5. Identity Management (Identity Maintenance)

1.7.1 Registration

During the registration process, when an applicant provides evidence of his or her identity to the credential-issuing authority, the fundamental aspect of one's identity is established. If the individual identifies themselves in a trustworthy manner, the authority can assert this identity with a certain level of identity assurance.

A digital identification system should ideally be integrated with civil registration, which is the official recording of births, deaths, marriages, divorces, annulments, separations, adoptions, legitimation, and recognition.

Registration may begin with Resolution, the process of distinguishing an individual from others in a given population or setting. Pre-enrolment is the first step in the resolution process. Here, the applicant provides biographical information, breeder documents (such as birth certificates, marriage certificates, and social security cards), and photographs to the issuing authority. The applicant may present these materials in person or submit them online or offline. This is followed by enrolment, which typically takes place in person, so that pre-enrolment information can be validated and supplemented as necessary by the registration authority.

Personal verification is required for the highest level of identity assurance (IAL3).

Typically, after the demographic and biometric information has been validated and enrolled, identity proofing continues with de-duplication to ensure that the individual has not registered under a different claim of identity. This can be achieved by conducting an identification (1:N) search of the entire biometric database using one or more biometric identifiers (physiological and/or behavioural characteristics used to identify an individual).

The next step is Validation, in which the authority determines the authenticity, validity, and accuracy of the identity information provided by the applicant and associates it with a living individual. This is followed by Verification, the process of establishing a connection between the claimed identity and the actual person presenting the evidence. The last step is Vetting/Risk Assessment, which involves comparing the user's profile to a watch list or risk-based model (Group of the World Bank, 2018b).

1.7.2. Issuance (Credential Management)

Issuance is the creation and distribution of virtual or physical credentials, such as decentralized identity proofs, e-passports, digital ID cards, and driver's licenses; and a unique identifier (with central biometric authentication). Maintenance (the retrieval, update, and deletion of credentials) and Revocation (the removal of privileges assigned to credentials) are the other two steps.

As can be seen in the European Union (EU), East African Community (EAC), and West Africa regions, interoperability of these credentials for authentication is becoming increasingly important for intra-country and inter-country service delivery. In the European Union, for instance, electronic identification (eID) and electronic Trust Services (eTS) provide the interoperability framework for secure cross-border electronic transactions of the Digital Single Market in accordance with the electronic IDentification, Authentication, and Trust Services (eIDAS) regulation (Group of the World Bank, 2018b).

1.7.3. Identity Authentication

Authentication is the process of comparing a claimed identity to the registered identity data.

It could be a personal identification number (PIN), a password, biometric data such as a fingerprint, or a photograph, or a combination of these. In this phase, difficulties include reducing processing time, improving the accuracy of matching for authentication, ensuring a seamless experience for applicants, mitigating network connectivity issues, preventing fraudulent behaviour, and locating cost-effective hardware and software solutions (Group of the World Bank, 2018b).

1.7.4. Authorization

Authorization defines access rights (or grants) that a credential-issuing authority has associated with an individual's identity based on the relationship between the individual and the credential issuing authority (e.g., a financial institution)—independent of the Identity Provider (e.g., the National Identification Authority). In more sophisticated authorization schemes, grants are context- and time-sensitive and dynamic. As this report focuses on Identity Providers and the provisioning of identities, and not on Relying Parties and the authorizations they may associate with an identity, it will not examine the various authorization processes and technologies that are currently emerging on the market (Group of the World Bank, 2018b).

1.7.5. Identity Management (Identity Maintenance)

Identity management or maintenance is the persistent retrieval, modification, and deletion of identity attributes or data fields and policies governing user access to data and services. Identity retrieval is the retrieval of a user's identity attributes. To ensure that only authorized users can access, modify, or delete identity information, and that all actions are audited and cannot be disputed, access privileges should be enforced using security policies. This strategy ensures that only authorized users have access to resources in accordance with access policies and attributes. In response to occurrences, credentials may be deactivated, revoked, or rendered inactive, and identity information may be modified or removed. Identity Management challenges include cost-effective system maintenance, utilizing data analysis to improve the system's performance (including its efficiency), ensuring that databases are updated to reflect significant life events (such as birth), and preserving privacy and security controls (Group of the World Bank, 2018b).

1.8 Level of Assurance

When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that she is who she claims to be depends on the level of security assurance provided and the context in which the information is captured; this degree of confidence is referred to as the level of assurance (LOA).

Consequently, the term "level of assurance" *refers to the degree of confidence in the claimed identity of a person* – *how certain a service provider can be that it is you the one using your eID to authenticate to the service, not someone else pretending to be you* (eIDAS, European Commission).

Following the eIDAS Regulation (EU) 910/2014, electronic identification (eID) schemes are classified according to three levels of assurance:

Low: for instance, enrolment is accomplished through self-registration on a website, with no identity verification.

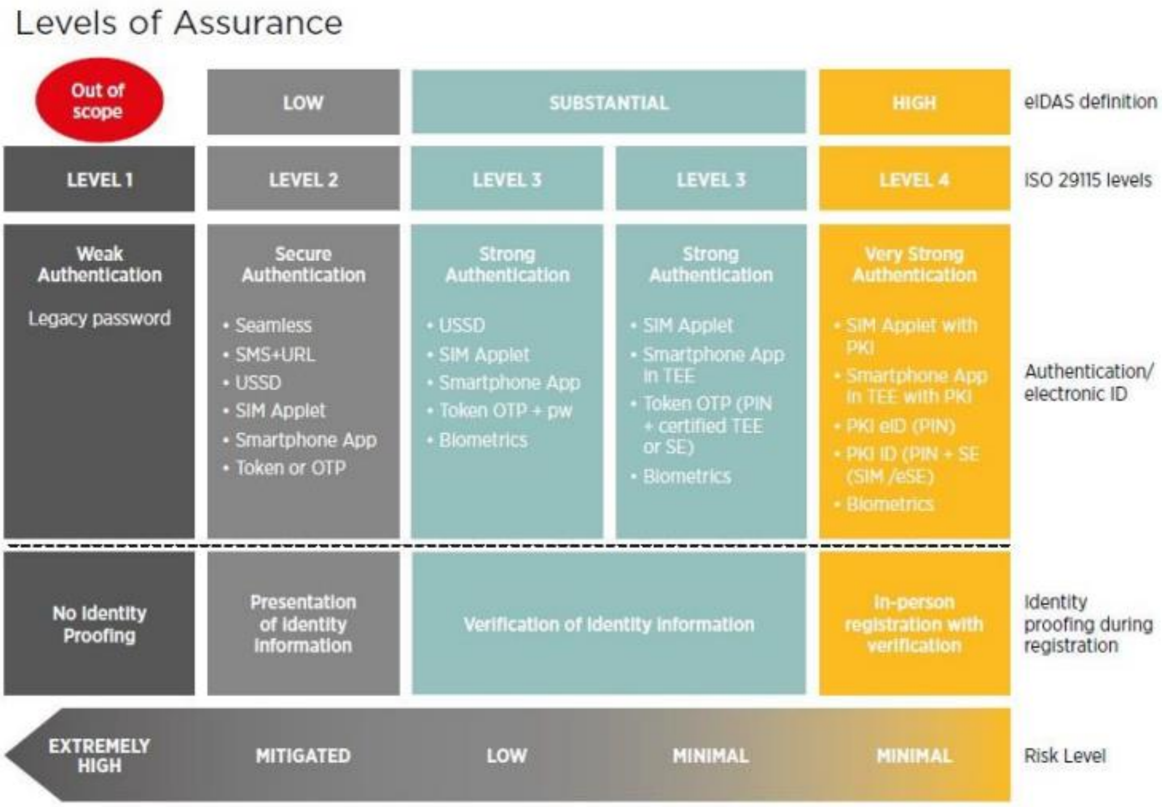
Substantial: for instance, enrolment requires supplying and validating identity information, and authentication requires a username, password, and one-time password given to your cell phone;

High: for instance, enrolment is accomplished by registering in person at an office, and authentication is accomplished by using a smartcard, such as a National ID Card.

In the report "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation" (GSMA-World Bank Group –Secure Identity Alliance, 2016), it is noted that the assurance levels of digital identities depend on the strength of identification and authentication processes, which are vital for controlling access and preventing identity theft. The level of assurance (LOA) indicates the degree of confidence that a service provider has in the validity of a user's credentials. Higher LOA means that a service provider is less likely to accept a compromised credential. The requirement for "identity proofing" varies based on the identification technique used, which can involve collecting different types and levels of personal information and attributes during enrolment, and the degree to which these qualities are verified (i.e., validated)

The strength of the identification credential and authentication depends on the robustness of the employed technology and authenticators. Not all transactions will require the greatest level of LOA; the greater the risk associated with the transaction, the higher the assurance level required. Typically, a single element of verification, such as an ID number or password knowledge, is insufficient to confirm a person's identity or offer correct authentication. Certain applications (e.g., Facebook) may be suitable for this degree of risk, while higher security transactions (e.g., collecting benefits or signing an official document) may require additional or multiple sources of authentication to supplement the user's credentials. These elements must be sturdy and secure. Possession of a secure device, such as a physical token, a mobile phone, or a smartcard, enables secure authentication and can be supplemented with a personal identification number (PIN) or attribute (such as a biometric feature or behavior) to provide a higher level of security.

LoA interacts with every digital identity application; based on how it applies to the aformentioned models, two macro categories can be identified: Social ID and eCommerce ID, which have a medium-low LoA but significant usage, are widely dispersed and utilized in Single Sign-On (SSO) logic to access multiple services with low LoA (Digital Identity Observatory, 2020).



Levels of Assurance

Out of scope	LOW	SUBSTANTIAL		HIGH	eIDAS definition
LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 3	LEVEL 4	ISO 29115 levels
Weak Authentication Legacy password	Secure Authentication • Seamless • SMS+URL • USSD • SIM Applet • Smartphone App • Token or OTP	Strong Authentication • USSD • SIM Applet • Smartphone App • Token OTP + pw • Biometrics	Strong Authentication • SIM Applet • Smartphone App in TEE • Token OTP (PIN + certified TEE or SE) • Biometrics	Very Strong Authentication • SIM Applet with PKI • Smartphone App in TEE with PKI • PKI eID (PIN) • PKI ID (PIN + SE (SIM /eSE) • Biometrics	Authentication/ electronic ID
No Identity Proofing	Presentation of identity information	Verification of identity information		In-person registration with verification	Identity proofing during registration
EXTREMELY HIGH	MITIGATED	LOW	MINIMAL	MINIMAL	Risk Level

Key: OTP = one-time password; PKI = public key infrastructure; (e)SE = secure element or embedded secure element (a tamper-resistant hardware platform); TEE = trusted execution environment (a secure area of the smartphone); USSD = unstructured supplementary service data ("quick codes"). *Note:* NISTIC 800-63A draft standard guidelines on identity proofing also allow for virtual-in person proofing and enrollment transactions[25]

Figure 1.1 LoA (Word Bank Group,2016)

1.9 Factor of authentication

The information that the user could use to prove his own identity is called authentication factors. (The World Bank Group, 2018a). Existing authentication methodologies involve three basic "factors"(K. Abhishek et al,2013):

• Something the user knows: Knowledge Factor, it is the weakest but still the most widely authentication factor. (e.g., password, PIN)

• Something the user has: Inherence Factor something that the user owns (e.g., ATM card, smart card, mobile phone)

• Something the user is: Ownership factor, those include some of the attributes intrinsic to an entity (e.g., biometric characteristic)

One more recent inclusion is the fourth factor that is associated with “Someone you know”: Social Factor.

Accordingly, to this classification, it’s possible to distinguish between:

• Single-factor authentication (1FA): if only one authenticator is used in the process.

• Multi-factor authentication (MFA): if it requires the user to enter some form of additional
code or data that only they possess. Current MFA methods require two or more authentication methods (Willamson et al.,2021).

1.10 Type of data and attributes

As previously stated an identity (ID) is a set of one or more attributes that allows an entity or person to be sufficiently distinguished or uniquely identified (GPFI 2018; Sunberg et al, 2018).

Understanding the nature and value of these attribute is essential.

As noted during the 2016 World Economic Forum, even if the total number of extant qualities is potentially infinite, they can be classified into three major categories:

- Inherent: inherent to an entity and not determined by its relationship to external entities (for example, age, height, date of birth, and fingerprint).
- Accumulated: accumulated or cultivated over time. Throughout an entity's existence, these characteristics may undergo many modifications or evolve (e.g. health records, preferences and behaviours).
- Assigned: associated with an entity but unrelated to its essence. They are subject to change and indicate the entity's relationship with other bodies (e.g., National Identity Number, telephone number, and email address).

These attributes vary for the three primary user groups: individuals, legal entities, and assets.

In conclusion, if the entity being represented is an individual, the following data types may be provided (Mastercard, 2019):

- Biographical data (e.g., name, date of birth, address)
- Biometrics (e.g., fingerprint, face, voice)

- Personal unique identifiers (e.g., passport number, social security number)
- Certifications (e.g., doctor, pilot, university degree)
- Dynamic data from (e.g., financial institutions, retail, mobile) interactions

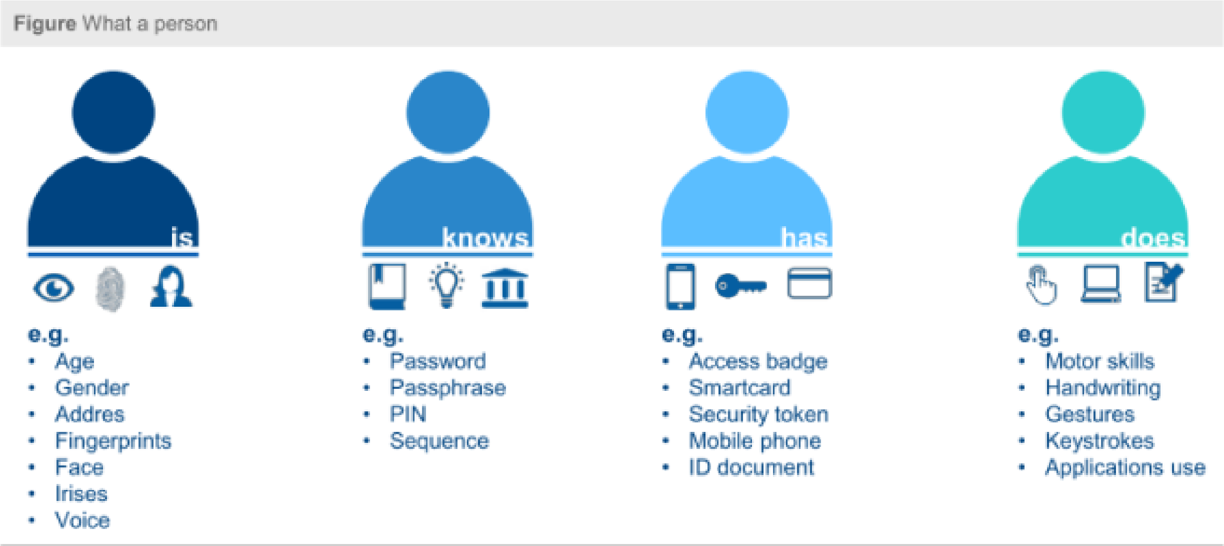


Figure 1.2 Types of credentials (World Bank Group, 2018)

1.11 Identity Management Actors

Once the types of data and attributes that are stored have been grasped, it becomes imperative to determine the entities to which they are ascribed. These entities could include a Person (an employee, a customer, or a citizen), an Organization (a legal entity), a virtual object (like a computer process, application, or text file), a physical object (such as electrical appliances and computers), or any other entity that requires access to a specific resource, as found in an Identity Management System (Jovanovi et al., 2016).

. It's important to understand the different entities that participate in the digital identity ecosystem, and how they interact with each other in the Identity Management System.

An Identity Management System is defined as "*one or more systems or applications that manage the identity proofing, registration, and issuance processes.*" (NIST 2022)

Traditionally, there were only two participants in the "identity ecosystem": the identified and the identifier. Nowadays There are numerous participants in the digital identity ecosystem (World Economic Forum, 2018).

In contrast to the past, where only governments had the authority to manage information regarding citizens' identities, it is now evident that governments are not the only part involved (Lips et al., 2009).

Looking at the guidelines expressed in the report "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation "(GSMA-World Bank Group – Secure Identity Alliance,2016), it's possible to highlight multiples actors, which fits in three categories:

- End-Users (subjects of the ID system) individual citizens and customers are the ultimate users of digital identity systems. Individuals enrol in identity systems and use the credentials they receive to gain access to the benefits and services of a country or business.
- ID Providers (issue and manage identities), there different type of providers here listed the most significant ones:
    - Government bodies: which can act as:
        - Legal registrars, being the entities responsible for providing citizens with legal identification. This may include national identification authorities (NIAs) responsible for the creation and maintenance of national identification cards and other documents, as well as national population registers and birth registers that record life events.
        - Functional registers when they oversee electoral commissions, tax authorities, social security authorities, hospitals, etc. for example. These registries may be linked to legal registries like a national population register, or they may be independent identity systems.
        - eGov service providers, government agencies or platforms that offer online services to citizens or residents who must provide identification and entitlement documentation. They are frequently connected to the national identity system and/or functional registers.
    - Private companies:
        - Commercial service providers, private companies that either use digital identities to provide services to their clients or enable end users to transact in a digital environment by providing digital identity and authentication services.
        - Identity solution suppliers, firms that provide hardware, software, and support for the development of digital identity systems.
    - Digital identities providers, who are those who create digital identities for users by registering them (including enrolment and validation) and issuing documentation or credentials. In general, identity providers also store and manage user information and credentials. In the public sector, legal registers are the most prevalent digital ID providers, although electoral commissions and other functional registers may also create and manage digital identities (e.g., a voter register). Frequently, commercial service providers are also digital identity providers. For instance, mobile companies provide SIM cards and banks issue debit cards after enrolling and verifying their customers' identities. Private identity providers frequently rely on or utilize legal identity provided by the public sector (e.g., your SIM card may be linked to a national identity number).
    - Attribute providers are entities that possess validated user data and either validate or provide these attributes to third parties (subject to user consent).Such information may pertain to the individual's identity data

    (e.g., name, address, date of birth, gender, etc.), data related to the credential device (e.g., network information data about the individual), or any other information about the user.

    - Digital authentication providers validate a user's attributes or identity to determine his or her eligibility to access a service or benefit. In the public sector, authentication providers are typically those agencies that are directly involved in delivering services that require verification, such as functional registers and eGov service providers. In certain instances (such as Aadhaar), national ID authorities will authenticate on behalf of a service provider. Users are authenticated by commercial service providers in the private sector.
    - Service providers are entities that provide services to end-users directly (citizens and clients). This may include both public and private service providers, such as functional registrars and eGov service providers. Service providers may be digital ID and authentication providers themselves, or they may outsource these responsibilities to other organizations.
- Enabling and supporting actors (support the development, implementation and oversight the ID system)
    - Regulatory and oversight agencies and organizations oversee, regulate, and audit digital identity systems. This consists primarily of national-level public sector agencies and supranational authorities, such as the European Data Protection Board and EU MSs Supervisors, in accordance with eIDAS requirements.
      The aim of these parties is to ensure that providers of digital identity and authentication adhere to legal requirements and best practices for the collection, storage, and utilization of personal data.
    - Standard-setting bodies, organizations that provide protocols for digital identification and authentication are. This includes public sector organizations like the European Committee for Standardization (CEN) and the National Institute of Standards and Technology (NIST), as well as private and non-profit organizations like the ISO standard body, the Open ID Foundation, FIDO Alliance, GSMA, and Secure Identity Alliance. The purpose of these organizations is to increase interoperability and develop scalable, open identity solutions.
    - Identity organizations and trust frameworks define the technical, operational, legal, and enforcement mechanisms for identity management information exchange. This includes both public and private sector actors.
    - Donor organizations and development partners, such as the World Bank and regional development banks, the European Union, IOM, IMCPD, UNHCR, UNDP, UNICEF, USAID, and the Gates Foundation, provide funding and technical assistance for the development of digital identity systems.

1.12 Configurations

There are three types of identity systems available: centralized, federated, and decentralized. As their names imply, their essential architectures distinguish them from one another, with repercussions for adoption and trust levels, as well as benefits and problems for digital entities (Word Economic Forum 2018). In addition, nowadays Self-Sovereign Identity (SSI) category must be considered.

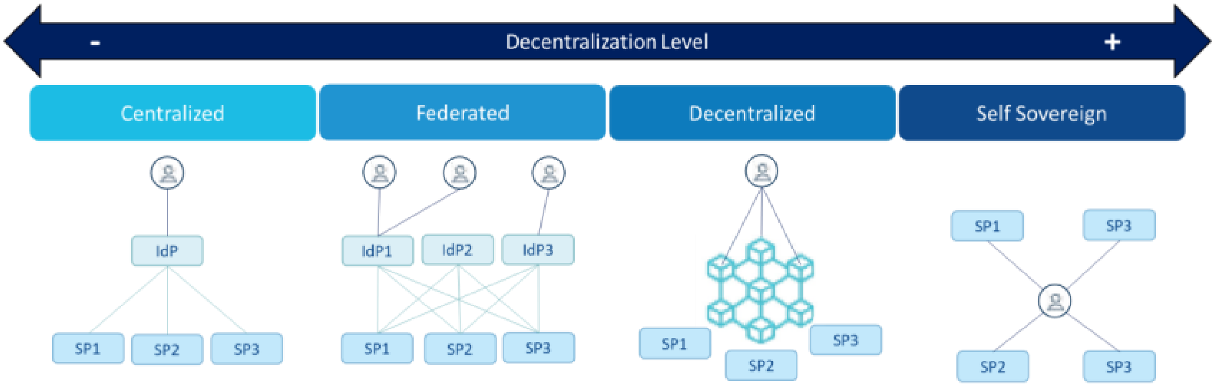


Figure 1.3 Types of ecosystems (Digital Identity and Blockchain and Distributed Ledger Observatory, 2020)

1.12.1 Centralized

The traditional system by which an individual gains access to the services of an organization that manages or owns the identity system is centralized configuration. The system owner collects, stores, and makes use of the individual's identity and associated data. Currently, private organizations such as banks, social media companies, and even governments are proposing such systems. Nowadays, centralized identity systems are so widely adopted. Currently, most authentications are established by matching a login and password. A digital account is typically created by the user and stored in the service provider's database. A user usually has one account for each service provider (Dib and Toumi, 2020).

Today, digital identities are governed primarily centrally, within siloed infrastructures. Typically, a legal entity must identify itself to each service provider in order to establish its digital identity. Under this arrangement, the service consumer has minimal control over its own identities and related characteristics and must adhere to the service provider's terms and conditions to develop and maintain its digital identity. It must rely on the service provider's processes and have faith in the service provider's ability to handle its identity securely, which imposes responsibilities on the service provider and incurs costs. (Word Economic Forum, 2019).

Clearly, this method has successfully enabled a digital representation of an entity, thereby facilitating a vast array of online services (Zhu, X. and Badr, Y., 2018).

Once accepted into the system, users have access to the owner's offerings, whether they be public services, banking services, or social media networks. The owner of the system determines the extent of identity verification due diligence based on regulatory and compliance requirements, risk tolerance, and policies, potentially fostering high levels of individual confidence. Additionally, the owner can serve as a gatekeeper to prevent the dissemination of false information.

Many owners negotiate with other reliant parties to accept the identity documents issued to individuals, such as passports, identification cards, and bank statements, thereby granting individuals access to a broader range of services (Word Economic Forum, 2018).

Today's centralized identification systems are well-established, with well-defined standards and procedures, and this is presumably why the majority of blockchain solution providers rely on them.

Nonetheless, it is necessary to highlight the primary issues associated with this system: Individuals typically have limited control over how their personal data is used within centralized systems, representing a possible lack of privacy. . Some systems only support a limited number of transaction types and are incompatible with other system, creating an extremely fragmented landscape. Centralized architectures may represent "honeypots" of individuals' identity information, making them enticing targets for hackers, and may concentrate risk and liability on the system owner. Lastly centralization also gives owners power, which, if unchecked, can lead to abuses such as surveillance, tracking, and profiling; exclusion and discrimination; and political repression of individuals (Word Economic Forum 2018).

1.12.2 Federated

A trust relationship between an organization and a person is the foundation of federated identity management. A federated identity enables the end user to use a single set of credentials to access information from a related company without establishing new trust relationships.
A collection of organizations that establish trust relationships that allow them to send attribute assertions about user identities to grant access to their resources.

A user's credentials (both for authentication and authorization) from one or more identity providers may be used to access other sites (service providers) within the federation (Chadwick, 2008).

Federation has emerged as an important identity management concept. Its primary objective is to share and distribute attributes and identity information across diverse trust domains in accordance with predetermined policies. The federation model enables users of one domain to access the resources of another domain seamlessly and securely, without the need for duplicate login procedures. Specifically, the most prevalent use case is Single Sign On (SSO), which enables users to authenticate at a single site and gain access to multiple sites without providing additional information (Cabarcos, 2008).

The concept of federated identity is gaining popularity, especially in the consumer arena, where Facebook and Google are trusted by many apps via established protocols. Federated identity solutions have been created to address the issue of needing to register digital identities with each service provider, which can be time-consuming and cumbersome (Jensen H. and Hewett N., 2019).

Notably, most of these federated identification services continue to rely on a central system to create and maintain trust.

Compared to solitary centralized systems, federated networks can provide individuals access to a greater variety of transactions using a single set of credentials. This interoperability provides users with greater convenience.

It can also help the system's multiple owners more efficiently manage individual identities and access.

Like centralized systems, federated systems may provide individuals with limited control over the use of their data. Complexity arises for system owners due to the potential requirement for legal agreements, including the allocation of risks and liabilities, as well as shared data and technical standards.

This complexity may make implementation costly and prevent the system from incorporating many of the services that individuals desire (World Economic Forum, 2018).

1.12.3 Decentralized

Decentralized identity provides the user with complete control of their digital identity. It is completely independent of any centralized digital identity issuance or management authority. Users are frequently exposed to the risk of data breaches, identity misuse, and identity theft by a centralized authority. Users cannot gain control over their digital identity without this (Stockburger et al., 2021).

Decentralized identity solutions have been developed in recent years to combat the issue of third-party management of business or government identities. Decentralized identity is a relatively new and developing system that requires extensive further development.

This archetype is novel and is predominantly present in the pilot and proof-of-concept phases.

In the public sector, the government of Malta is piloting a program where educational institutions can issue credentials (such as diplomas and professional certifications) to an individual, who can access and manage them via a mobile application, using blockchain technology.

Looking for examples in the private sector banking consortiums are piloting shared know-your-customer and other decentralized identity (World Economic Forum, 2018)

Furthermore, decentralized identity infrastructure permits legal entities to have self-managed, service-provider-independent digital identities. This eliminates the current identity isolation and enables each legal entity to manage its identity, associated verifiable credentials, and their usage throughout global supply chains. A verifiable credential is a piece of digitally signed information issued by a reliable entity, such as an Authorized Economic Operator or a custom brokerage license. Before granting access to a service, service providers can verify these credentials before distributing them (Jensen H. and Hewett N., 2019).

Even though DID technologies are revolutionizing the web, the security of these systems is contingent on a strong assumption regarding the underlying storage system (DLT).

Specifically, identities are tamper-proof and highly accessible without centralized trusted parties. Existing DIDs are incapable of detecting the misuse of compromised credentials, so achieving identity sovereignty comes at a cost. Particularly, it is impossible to detect that a user's credentials have been compromised and used by an adversary to authenticate them with a service provider in a fully decentralized system. Compared to centralized identity systems that log all authentication events, this is a limitation (Allangot et al. ,2023).

Technologies and standards to enable decentralized identity systems are gaining momentum rapidly, but the majority of current operating models and regulatory frameworks are designed for centralized systems; they will need to evolve in order to govern decentralized systems. Assigning responsibility for potential violations or abuses can be particularly complicated. Individuals may require education to adopt and use decentralized systems responsibly (World Economic Forum, 2018).

However, it’s important to highlight one of decentralized system's main strength: the control and transparency it affords the individual user, control over what identity-related information to share, with whom to share it, and for how long. Decentralized systems can also facilitate a more enticing digital consumer experience, as individuals expect and are able to manage greater personalization and transparency. Verifiable claims can also facilitate interoperability between existing, isolated systems (World Economic Forum, 2018).

1.12.4 Self-sovereign identity

Decentralized identity over a blockchain is referred to as a self-sovereign identity or SSI (Kubach et al., 2020).

SSI is a decentralized digital identity model that provides entities in the world with a digital identity that enables secure, privacy-protected, trusted, and self-governed access to various digital services using verifiable credentials. Using this model, the owner of an identity has control over his identity and its associated attributes and can decide with whom and for what purpose to share his personal information. DLTs are utilized to achieve decentralization, allowing users to conduct transactions without requiring authorization from a central authority. As a result of reducing the number of issues, SSI not only gives users more control, but also makes the identity management process much more efficient and less burdensome for organizations (Kronfellner B. et al, 2021).

In an SSI ecosystem there are three primary roles:

To better comprehend how SSI ecosystem’s function, consider them as three-sided marketplaces where individuals and organizations can play three distinct roles:

Issuers - Organizations that store identity-related information about citizens, customers, employees, or other stakeholders and "issue" this information to its associated individuals, things, or organizations ("Holders") in the form of digital credentials. Issuers are the SSI ecosystem's original data sources. A government, for instance, may issue digital passports to its citizens, or a university may issue digital diplomas to its graduates.

Holders – Individuals or organizations that receive digital credentials containing information about themselves from diverse sources ("Issuers"). By aggregating and storing such credentials in so-called "wallets", Holders can construct comprehensive digital identities that are entirely under their control and can be easily shared with third parties ("Verifiers").

Verifiers - Parties that rely on data to provide products and services can verify and process data provided by their stakeholders ("Holders") in a dependable manner. Verifiers are also referred to as "relying parties," and they are typically organizations or professionals. After the verifiable credential is created, it is significant to note that the issuer is no longer involved in the process.

SSI can generate substantial value for organizations.

Frictionless Interactions: SSI can eliminate passwords, forms, and cumbersome identification processes to increase conversion rates by up to 40 percent and reduce help desk requests by up to 50 percent (Gartner,2019).

Reliable Information: Currently, 41% of customers provide false information due to security and privacy concerns (RSA). SSI can reduce this number to zero by removing consumers' concerns and enabling them to share trustworthy digital credentials signed by reputable third parties, such as governments.

Fraud Prevention: SSI enables service providers to verify consumer data in terms of data validity, integrity, authenticity, and provenance in an almost instantaneous manner. This will prevent identity theft and document forgery.

Data Breach Prevention: SSI can significantly reduce the risk of data breaches by removing common risk factors such as password-based authentication and aggregated data storage.

Regulatory Compliance: SSI includes user-centric data management and methods to enhance user privacy (such as selective disclosure) to ensure compliance with data protection regulations (e.g.,GDPR).

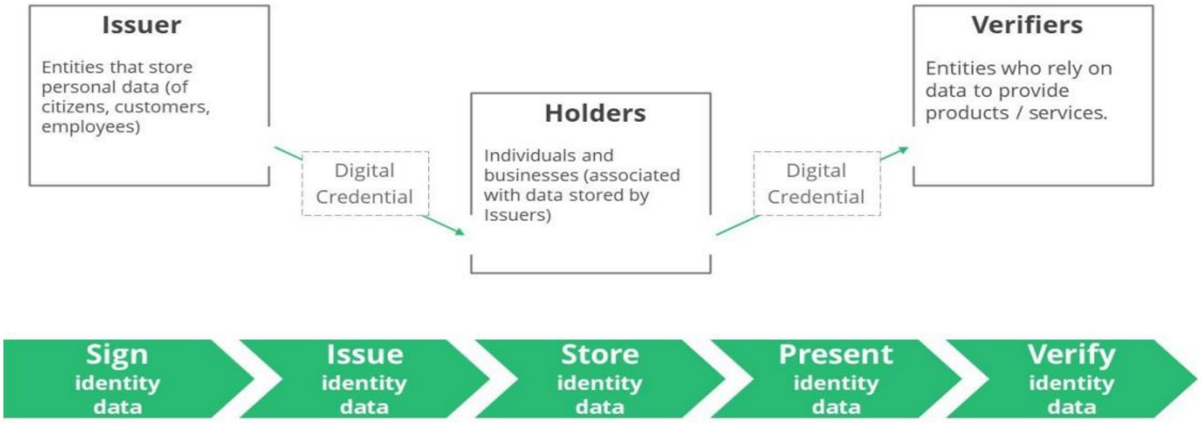

Issuer
Entities that store personal data (of citizens, customers, employees)
Digital Credential
Holders
Individuals and businesses (associated with data stored by Issuers)
Digital Credential
Verifiers
Entities who rely on data to provide products / services.
Sign identity data
Issue identity data
Store identity data
Present identity data
Verify identity data

Figure 1.4 Illustration of how SSI ecosystems work (BCG, 2021)

1.13 Technologies

Emerging technologies enhance the capability, speed, and efficacy of identity management systems, enabling businesses to eliminate unnecessary processes and paperwork and enhancing the customer experience.

The analysis is conducted using the framework designed by the World Bank Group as a reference, putting particular focus on the technologies that are mapped in the census and are the most used in the startup landscape.

Following the cited report, it’s possible to categorize technologies into macro-groups:

● Credential technologies: considering a credential as “*mechanism, process, device or document that vouches for the identity of a person through some method of trust and authentication*.” (The World Bank Group, 2018b):

- Biometrics: Biometric recognition identifies and verifies an individual's identity by utilizing his or her unique physiological and behavioural characteristics (The World Bank Group, 2018b).

  When determining how to incorporate in a biometric-recognition system, decision makers must consider several criteria: accuracy(which is measured by the false acceptance rate (FAR) and false rejection rate (FRR) under operational conditions), universality(which refers to the presence of the trait in members of the relevant population),stability(which refers to the permanence of the trait over time or after disease or injury), collectability(which refers to the ease with which good quality samples can be acquired), resistance to circumvention, acceptability(which refers to the degree of public openness for use of the modality),usability and cost.

  To evaluate how well different biometrics meet these criteria for effectiveness, they can be classified into two major categories: primary biometrics, such as fingerprint, face, and iris recognition, which have low error rates and are used for identification searches; and soft biometrics, such as keystroke patterns, signature, and gait, which have higher error rates and are used for continuous authentication.
  While developing a biometric-recognition system, it's essential to consider the type of attribute collected, which is called the modality. Several biometric recognition methods are currently in use, each with its own strengths and weaknesses. The most prevalent biometric recognition modalities include fingerprint, face, iris, voice, behaviour, and vascular recognition.

  - Fingerprint recognition is a prevalent technique that employs various types of sensors to detect the presence and location of unique characteristics on the surface of a fingertip. These features are unique to the individual and can be used to create a unique template that can be compared against a database for identification purposes.
  - Face recognition is a widely employed technique that employs two-dimensional and three-dimensional facial-

recognition systems and algorithms to analyse the face's various features. This includes the brow ridge, cheekbones, edges of the mouth, and distance between the eyes, which do not change significantly with age. Face recognition is popular in both security and consumer applications.

- Iris recognition, the coloured portion of the eye, the iris, is illuminated by near-infrared light (NIR) for iris recognition. Specific patterns in the iris can be identified and used to generate a unique template (iris code) based on its characteristics. The iris is an excellent biometric identifier because it remains relatively constant throughout a person's lifetime.
- Voice recognition utilizes both physiological and behavioural biometric characteristics. Two types of voice recognition systems exist: speaker verification and speaker identification. Speaker-verification systems verify whether the voice sample presented by a person matches the voice sample stored in the database. This is a process of exact matching. Speaker-identification systems attempt to match a given sample of a speaker's voice with the samples in a database in order to identify the speaker. This is a 1:N matching process. Two types of speaker-verification systems predominate: text-dependent, which requires the speaker to say the enrolled or given password exactly, and text-independent, where the speaker's identity can be verified without a constraint on the speech content.
- Behaviour recognition, usually, behavioural biometrics are combined with one or more other modalities. They are primarily used for continuous authentication to ensure that a user who was authenticated at the beginning of a session remains the same throughout the duration of the session. Behavioural biometrics identify and verify users based on patterns such as signature dynamics (speed, pressure), gait, keystroke dynamics, mouse usage, and touchscreen interactions.
- Vascular recognition is a less frequent technique that uses sensors to capture and match unique vein patterns while NIR light illuminates veins just under the skin. Each person has a unique pattern of veins that can be used for identification purposes. Vascular recognition is often used in high-security applications where accuracy is paramount (The World Bank Group 2018b).

The biometrics industry is experiencing substantial growth, with predictions forecasting a remarkable increase in cumulative global revenue over the period from 2016 to 2025. The anticipated growth rate is expected to reach a staggering 22.9% compound annual growth rate (CAGR), resulting in an estimated revenue of nearly 70 billion USD (European Commission 2016).

- Cards and supporting technologies.: cards can be read by specialized data input devices or card readers that use technologies to capture and interpret bar codes or text through optical character recognition (OCR), magnetic-stripe readers, contact and contactless smart card readers, and other RFID readers (The World Bank Group, 2018b).
- Mobile and other devices: phone and tablet-based hardware and software solutions used to register, authenticate, and verify an individual's identity.

● Analytics Technologies: Analytics technologies use mathematical, statistical, and predictive modelling techniques that leverage a variety of data sources to find meaningful insights and patterns in data (The World Bank Group, 2018b).

- Machine learning and artificial intelligence; Risk analytics could help predict fraudulent and delinquent behaviour; predictive analytics uses algorithms to predict the probability of future biometric changes based on historical data. Business activity and operations analytics aid in real-time analysis of digital identity data and statistics (The World Bank Group, 2018b). Widespread are applications that use machine learning and AI for real-time verification and identification of individuals' digital identities. Further advances in artificial intelligence will enable more secure authentication methods that reduce fraud risk and streamline the onboarding process. It will also aid in the protection of banks' sensitive data by monitoring where it is stored and who has access to it, among other measures. AI will increase the amount of data that can be analysed, and algorithms will enable the development of user identification processes and patterns (Enriquez M. and Segovia A., 2019).
- Other analytics: risk analytics (mainly to forecast fraudulent and delinquent conduct and assign a risk score based on financial or social history, criminal records, and loan defaults.), predictive analytics (use historical data to anticipate future results), business activity and operational analytics (to real-time analyse operational data to optimize company processes), and biographic matching (the so called fuzzy search for identity data matches below 100%. Fuzzy matching normalizes and de-duplicates biographical data from many sources.).

● Authentication and Trust Frameworks: "*Federated authentication provides a standards-based solution to the issue of trusting identities across diverse organizations which may even be across countries. This solution requires the establishment of a trust framework between the identity provider and the relying party. A trust framework is a set of business, legal, and technical rules that members of a community agree to follow to achieve trust online*." (The World Bank Group, 2018b)

- Fido; Fast Identity Online (FIDO) alliance was created to address strong authentication device compatibility and user difficulties with numerous usernames and passwords. Universal Authentication Framework (UAF), where users register their device and then perform local authentication on that device, and Universal Second Factor (USF),which enables phishing-resistant authentication using dedicated end-user hardware as Bluetooth, USB, or biometric devices, are FIDO Alliance specifications for simpler, stronger authentication (U2F).

- OpenID Connect; is an open standard that helps developers design secure and usable mobile authentication solutions.
- OAuth 2.0; is a token-based open-standard Internet delegated authorization mechanism. Client applications have secured delegated access.
- SAML(Security Assertion Markup Language); is an open standard based on XML. Web services enable this protocol's permission and authentication of business partners. Single-sign-on lets consumers access exclusive content across many sites or apps.
- Blockchain: also referred to as distributed ledger technologies (DLT), is an emerging technology that records transactions in a decentralized ledger hosted on nodes or servers in a peer-to-peer infrastructure (Lee, 2017). Any corrections or modifications to an existing record necessitate the creation of a new record, whose authenticity is verified by a consensus mechanism. The consensus mechanism employed depends on the blockchain's architecture and usage.

  Blockchain technologies are being investigated as an identity trust fabric, which would enable individuals to control their decentralized identity, including when and where identity attribute information is shared. This type of digital identity is usually referred to as a sovereign digital identity (SSID).

  Depending on how users are granted access to view, read, and write data on the chain, there are three types of blockchains. Public and permissionless blockchains are accessible to the public for reading, writing, and validating blockchain-based transactions. Public and permissioned blockchains are managed by a predetermined set of nodes, typically a consortium of participants who have established a legally enforceable trust framework. Private and permissioned blockchains use the same consensus mechanism as public and permissioned blockchains, but only network participants can view transactions. Due to increased transaction speeds and improved data privacy, permissioned ledgers are more commonly used by trusted parties for digital identity applications. Even though blockchain technologies are in their infancy, they offer significant benefits in decentralized identity management, providing individuals with greater control over their identity attributes and preventing arbitrary or sudden identity changes (The World Bank 2018).

SDK and Application Programming Interface (API)

SDK stands for software development kit. Also known as a devkit, the SDK *is a set of software-building tools for a specific platform, including the building blocks, debuggers and, often, a framework or group of code libraries such as a set of routines specific to an operating system (OS)* (IBM).

Typically, at least one API is also included in the SDK because, without the API, applications cannot communicate and collaborate.

API is a set of routines, protocols, and tools needed to build software applications. An API specifies how software components should interact and provides building blocks, making it easier to develop a programme (Sonpatki et al, 2021).

Whether working as a standalone solution or included within an SDK, an API facilitates communication between two platforms. It does this by allowing its proprietary software to be leveraged by third-party developers. The developers can then enable their own users to indirectly use the service or services provided by the API solution (IBM). By enabling platform and ecosystem business models and agile business processes, application programming interface (API) programs play a crucial role in facilitating digital transformation and innovation.

1.17 Literature gap

Since the onset of the COVID-19 pandemic, the scope and significance of digital interactions and services have expanded. As the physical and digital aspects of everyday lives become increasingly intertwined, how people identify and verify themselves, as well as the entities with which they interact, will also need to evolve. This is where digital identity comes in; regardless of whether interactions are physical or digital, it provides a way for all parties to prove they are who they claim to be (Word Economic Forum 2021).

A well-designed digital identity system, complemented by effective regulations, technology, and business models, has the potential to generate significant economic and social advantages. However, there is still considerable uncertainty regarding the appropriate standards for future digital identity systems, including the most effective business models, technologies, and areas of application. While established corporations tend to focus on refining existing products and services, startups possess a competitive edge rooted in their agility and adaptability, driving innovation and new perspective (Thiel, 2014).

By analysing digital identity startups, particularly those that have achieved success, it becomes possible to gain insight into the current trends and favoured solutions within the field.

Chapter 2-Research methodology

This chapter provides a comprehensive overview of the research process, beginning with an explanation of the project's motivations and concluding with a description of the steps taken to obtain the results described in Chapter 4. The research question that prompted the study is presented in detail, followed by a discussion of the methods employed to answer it.

The first section focuses on the analysis of scientific literature. This required a comprehensive review of the relevant existing literature, including academic articles and reports. The objective was to identify the most important themes and concepts explored in the field and to gain a deeper understanding of the subject.

This second section describes the process of reviewing, expanding, and analysing a database of startups. Specifically for this research project, a database containing information on a variety of startups in the relevant industry was compiled. Reviewing the database required collecting information about each startup, including its business model, target market, and funding sources. This data was then analysed to determine industry patterns and tendencies.

2.1 Digital identity observatory

The project was executed in conjunction with the Osservatori Digital Innovation of the Politecnico di Milano School of Management. This collaboration allowed access to a wealth of accumulated knowledge, such as scientific databases, archives, and censuses. The Osservatori Digital Innovation also aided throughout the research process by providing news and relevant articles on the topic, sharing software tools, and assisting with the data extraction and integration process outlined in the empirical framework.

Specifically, the collaboration with the Osservatori Digital Innovation was conducted in conjunction with a group of digital identity-focused researchers, belonging to the Digital Identity Observatory. Their assistance and knowledge were useful in ensuring the project's success.

Initiated in 2020 as a Working Table, the Digital Identity Observatory aims to comprehend the potential offered by digital identity systems and to contribute to the growth of the Italian market. In accordance with Research 2023, the Observatory intends to:

- comprehend how the national and worldwide landscape of digital identity solutions is evolving;
- monitor the level of dissemination and growth of the principal recognition systems in the Italian setting;
- examine the prospects offered by PNRR for market participants in digital identity;
- See the most cutting-edge advancements in onboarding and digital recognition solutions and their applications;

- watch the regulatory evolution to comprehend the ramifications for market participants;
- Explore the synergies that digital identities provide in other fields, such as cybersecurity and digital payments;
- Examine the technological architecture of the wallet model, the acceptance of this paradigm by governments, private companies, and users, as well as its effects on the ecosystem;
- explore the primary strategies and applications of decentralized identity frameworks;
- Monitor the level of uptake and utilization of various identity and recognition systems among end users and service providers.

Through analysis and empirical research aimed at defining the characteristics and opportunities for the development of digital identity, the Observatory intends to establish a qualified and impartial table where cross-industry discussions between market participants can be encouraged.

2.2 Research Question

With many unanswered customers' needs and potential solutions that could establish companies as market leaders, the market for digital identity offers substantial opportunities. To comprehend new directions in which the market could find new solutions and to identify the initiatives that would propel the sector forward, it is useful to examine the activities of startups. Startups are the players that are most likely to innovate and develop business models that can allow them to scale. Their solutions can add value to the system by fostering the development of private solutions or assisting central governments in resolving issues and enhancing existing models. However, it is essential to comprehend where startups are located, how much capital they have raised, the technologies they employ, the industries they target, the value proposition they offer, and the services they are developing and providing.

The primary research question that will be addressed is:

RQ: what are the characteristics of the entrepreneurial and startup ecosystem for Digital Identity?

Digital identity has been the subject of very little market research, despite the sector's rapid expansion. The academic literature has addressed the topic from a purely legal or technological perspective, and there is still a lack of consensus regarding the subject's definitions. On the other hand, decision-makers, entrepreneurs, and managers in numerous industries, such as finance, insurance, betting and gambling, and public administration, are confronted daily with new challenges in digital identity management.

In this context, a detailed and trustworthy identikit of the entrepreneurial ecosystem formed by the sector's startups can aid in identifying innovation opportunities, technological trends, and successful business models. After constructing a suitable and trustworthy information database to assist in defining the boundaries of this ecosystem, it will be possible to investigate a series of additional questions whose answers are valuable to both public and private institutions. In what entrepreneurial ecosystem, for instance, are digital identity startups gaining traction? What are the most significant technological innovations and business applications introduced? How much funding have digital identity solution-providing startups received? How can companies that develop digital identity solutions be categorized? What options could be associated with increased funding?

This thesis aims to contribute to the development of the digital identity sector and assist decision-makers, entrepreneurs, and managers from a variety of industries in navigating this rapidly changing landscape by addressing these questions and proposing new research directions.

2.3 Theoretical review

To gain a comprehensive understanding of the Digital Identity topic, it was necessary to conduct an analysis that could bring together the scattered information related to the theme, and identify intersections and research gaps. To collect the relevant documents, Scopus was used as the primary source database, which helped to gather all the reports and articles connected to the main topic. All the most recent reports on digital identity were read in order to have a global framework of the topic and to utilize the sources shared by the digital identity working table's researchers. The process involved three main steps: extraction, screening, and analysis.

- During the extraction phase, all the material related to the topic was downloaded from the database, using the Article title, Abstract and Keywords command with "Digital identity” and adding filters such as English language and subject area (Computer science, Engineering, Business management and Accounting). The output was a CSV file containing the abstracts and citation information for all papers that matched the two keywords, sorted by relevance.
- In the screening phase, the first abstracts were read to determine their relevance, and classified as relevant or not relevant. The relevant documents were downloaded and organized for deeper analysis.
- In the analysis phase, the papers classified as relevant were classified based on the authoritativeness of the publication journal. The documents were read entirely to have a complete view of the state of the art of the theme and categorized based on the research question and the topic described.

The output of the theoretical review was an Excel file containing the key points of all the documents read. Additionally, a few other documents were extracted from Google Scholar and ResearchGate to enrich the collected information.

2.4 Empirical framework

Several phases comprised the process of conducting a descriptive analysis of the digital identity startup ecosystem. A secondary data source was chosen to compile a list of startups operating within the digital identity ecosystem. The full description of each startup was read to conduct a preliminary screening and eliminate those that were irrelevant to the research scope or lacked primary sources. Each startup's description was also enriched with additional analytical dimensions. Actual data extraction produced a database containing 173 distinct startups, each with multiple information variables. This database served as the starting point for the ecosystem's descriptive analysis. In the following paragraphs, the entire process, including the skimming steps to ensure relevance, will be described in detail.

Figure 2. 1 gives an overview of the different phases of the research.

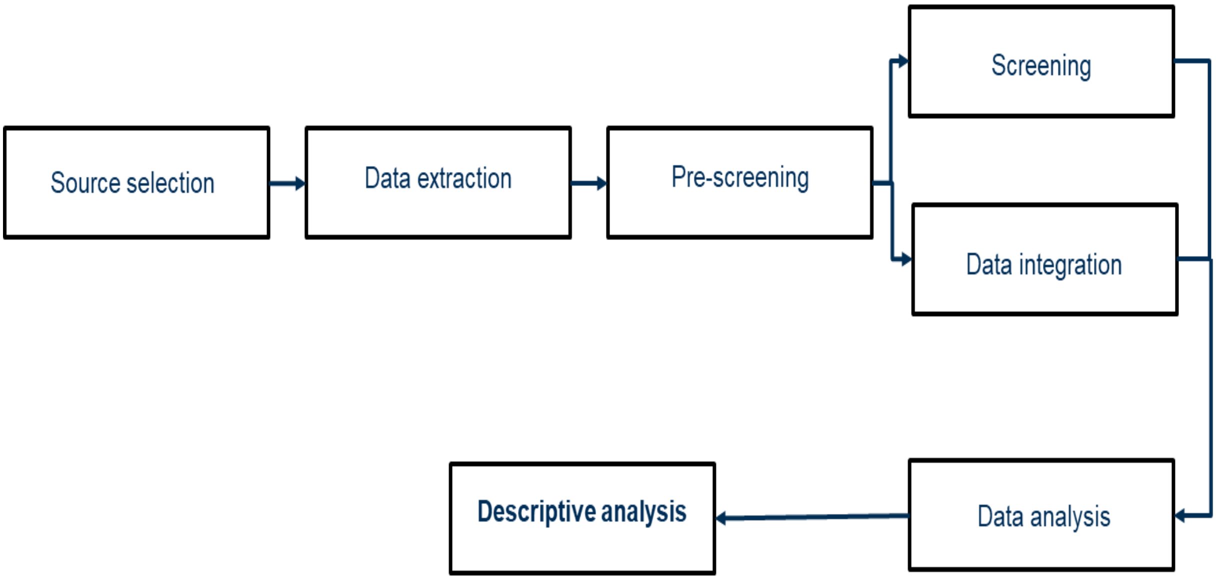


Figure 2.1 Research phases

2.4.1 Source Selection & Data extraction

Crunchbase, the largest database of startups in the world, was chosen as the database for the extraction. It is one of the most well-known American business information platforms. Crunchbase was established in 2007 and collects global data on companies, investors, funding rounds, and key players in the entrepreneurial ecosystem (Ferrati and Muffatto, 2020).

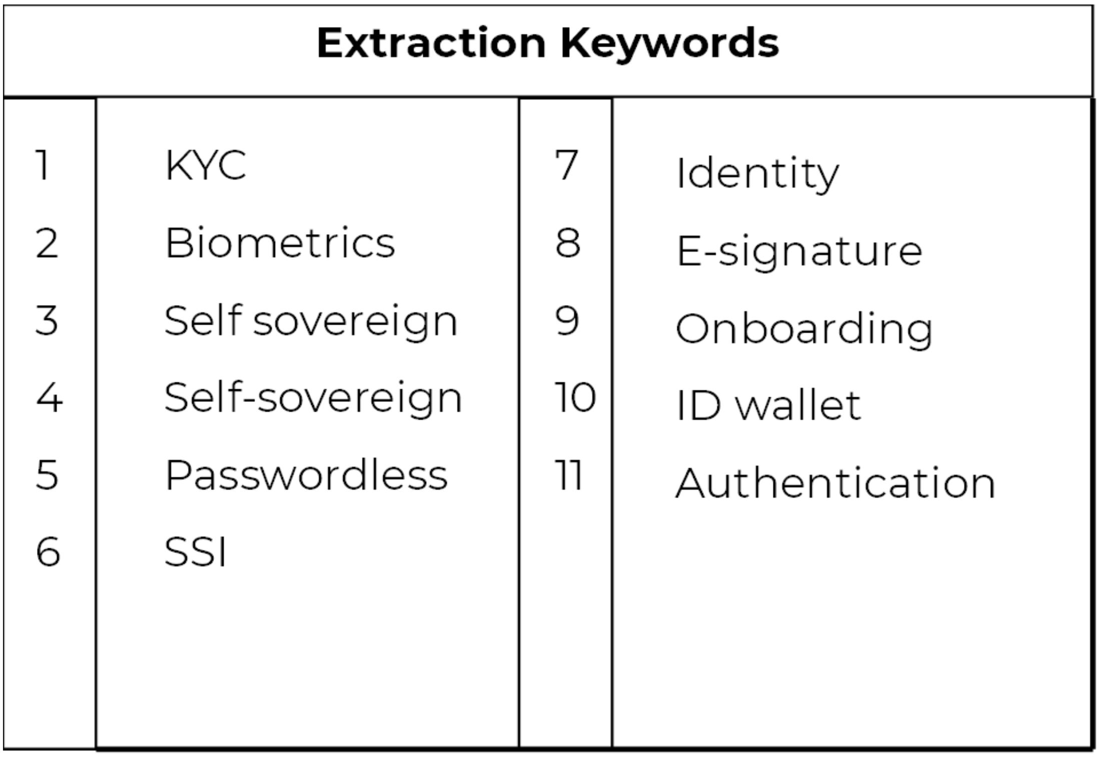
To ensure that only companies that we consider to be startups are extracted, three inclusion criteria pertaining to the date of establishment, the most recent funding received, and the operational status have been established. Only businesses with the following characteristics were evaluated in detail:

1. Founded after 1st January 2017 (last five years);

2. Received their last funding after 1st January 2020 (last two years);

3. Operating status "Active".

Once the research field was limited to only startups, it was necessary to establish an additional filter that would allow the extraction of only Digital Identity companies. It was necessary to compile a list of keywords to search for within the "full description" of the startups for this purpose. The definition work was performed by a team consisting of the undersigned and subject matter experts. There was a total of 11 keywords defined. Table 2.1 provides a summary of the keywords used for extraction.



Extraction Keywords			
1	KYC	7	Identity
2	Biometrics	8	E-signature
3	Self sovereign	9	Onboarding
4	Self-sovereign	10	ID wallet
5	Passwordless	11	Authentication
6	SSI		

Table 2.1 Extraction keywords

Then, all startups containing at least one of the just-listed keywords and meeting the three initial criteria were extracted. At this time, it has been determined not to exclude any information fields in order to prevent the loss of potentially relevant data. This operation produced a single CSV file which represent the starting point of the analysis conducted in the Excel file.

2.4.2 Screening

Due to the initial highly inclusive extraction policy, it was necessary to implement a screening phase to identify startups that, despite the presence of keywords, were outside the scope of the research. The screening phase consisted of two primary steps:

1. Pre-Screening: classification of startups into three categories ("relevant", "not relevant", and "possibly relevant") based on the analysis of the "Long Description";

2. Screening: detailed analysis of startups previously classified as "possibly relevant" based on the analysis of the corporate's online footprint.

All startups' "Long descriptions" were read and evaluated during the pre-screening phase to determine their eligibility. This first phase resulted in a subdivision into:

- "relevant" for startups offering products or services related to Digital Identity;
- "not relevant" for startups with no connection to the theme;
- "possibly relevant" for startups deemed borderline.

During the screening phase, "possibly relevant" startups were thoroughly examined.

The company's website was the primary source of information, while authoritative social networks (such as LinkedIn and Twitter) and newspapers provided additional data.

Throughout the process, alignment meetings have been scheduled between the undersigned researcher and the other two researchers to keep us up-to-date and address any questionable or unusual instances. The process began with the analysis of 729 startups and resulted in a database of 331 "relevant" startups whose products or services are closely related to the digital identity and access management industry.

The final database included over a hundred distinct variables for each startup. Table 2.2 provides a summary of the most significative:

CATEGORY	**VARIABLE**	**DESCRIPTION**
General	Startup name	Organisation’s name
	Startup Url	Crunchbase page of the firm
	Website	The startup website
	Full description	A comprehensive startup’s description
	Founded date	The date in which the startup was founded
	Headquarter location	The city and the state in which the HQ is located
	Headquarter region	The continent in which the HQ is located
	Contact email	The email to contact the startup
	Phone Number	The phone number to contact the startup
	Founders	Who founded the startup
	Total funding	Tot funding received in USD currency
	Last funding	Last funding received in USD currency
	Last funding date	Last date in which the startup received a funding

Funding	Top 5 investors	The 5 major investors of the startup
	Industries	In which industries the startup is working
	Number of investors	How many investors fund the startup
	Number of founders	How many people started the startup

Table 2.2 Variables extracted from Crunchbase.com

2.4.3 Data integration

Despite the vast amount of data extracted from Crunchbase, it was necessary to add a second set of useful variables for contextualizing startups within the digital identity ecosystem. The data integration activity occurred concurrently with the screening phase and consisted of analysing the online footprints of the startups in order to obtain relevant data. In fact, after a careful analysis of the literature described in the preceding chapter, a series of questions concerning seven macro categories emerged:

- Target: What kind of customers does the startup target?
- Technologies: What are the enabling technologies of the startup business model?
- Application sector: In which market segments does the startup operate?
- Identified entity: What kind of entity is represented by the startup? In what role can the individual use digital identity?
- Value proposition: What kind of service does the startup enhance?
- Step ID process: In which phase/phases of the digital identity management process is the startup involved?
- Barycentrism: is digital identity the primary value proposition (VP) for the startup?

CATEGORY	**VARIABLE**	**DESCRIPTION**
Target	B2B	The startup is targeting firms
	B2B2C	The startup is targeting firms, which provides solutions for customers
	B2C	The startup is targeting customers
Technologies	Blockchain	Use of blockchain technology
	Cloud	Use of cloud computing technology
	API&SDK	Use of API&SDK technology
	Open standard (OIDC/SAML)	Use of open standard technology
	AI& Analytics	Use of Artificial Intelligence technology

	Biometrics	Use of biometrics recognition
	Mobile device	Use of mobile device, not considering smartphone
	Proximity device	Use of proximity device technology
	Native	Use of technology already embedded in the software / device
Biometrics	Face	Use of facial recognition
	Voice	Use of vocal recognition
	Fingerprint	Use of fingerprint recognition
	Vein	Use of vein recognition
	Palm	Use of palm recognition
	Finger bones	Use of finger bone recognition
Sector application	General	Solution developed for general purpose
	eCommerce&retail	Solution developed for eCommerce and retail firms
	Finance	Solution developed for financial institutions
	Telecommunications	Solution developed for telco companies
	Healthcare	Solution developed for healthcare management
	Travel &Tourism	Solution developed for travel and tourism
	eGovernment	Solution developed for digital government services
	Security	Solution developed for security
	Mobility	Solution developed for mobility
	Education	Solution developed for education
	Legal	Solution developed for legal purpose
	eGaming&Gambling	Solution developed eGaming and gambling
	Humanitarian	Solution developed for humanitarian organization
Authorization	Phisycal access	Allowing physical access
	Logical access	Allowing logic access
	End user	The solution identifies the end user
	Employee	The solution identifies an employee

Identified entity	Legal entity	The solution identifies a legal entity
	Animal	The solution identifies an animal
	IDot	The solution identifies an object
Value proposition	ID	The VP offers an identity
	e-signature	The VP offers a certified digital signature
	ID+e-signature	The VP offer both ID and e-signature
Link to a physical document	Identification phase	Uploading of a physical doc in the identification phase
	Authentication phase	Uploading of a physical doc in the authentication phase
Work with PA		Official collaboration with public administration
Identification step	Identification support	The services support the identification phase
	Data integration	The service provides data integration from different sources
	Authentication optimization	The service enhances authentication
	Id-wallet support	The service provides a better ID-wallet management
	Authentication+Identification	The service at the same time authentication and identification
Barycentrism	ID as primary VP	ID is the main service of the startup
	ID as secondary VP	ID is the complementary service

Table 2.3 Variables used into the census

2.4.4 Descriptive analysis

The output of data extraction, cleaning, and integration was an Excel database containing 331 distinct startups. Each startup was connected to a large number of information variables grouped into 10 macro-categories.

The objective of the descriptive analysis was to reorganize the numerous information variables to generate significant insights that would answer the research question. In order to create a graphical and easily comprehensible representation of the digital identity startups ecosystem, variables were individually analysed before being combined and rearranged. The presented descriptive analysis was finally categorized according to various study perspectives:

- Geographic distribution: It is possible to identify the leading innovation hubs for digital identity by continent, country, and city, thanks to the granularity levels available.
- Funding: using multivariable graphs, it is possible to determine the characteristics of the sample's investment concentration.
- Foundation trend: how the number of startups founded changed during the five years considered.
- Market: target and application segment
- Value proposition: value proposition, ID step process and barycentrism

Chapter 3 - Result

In the following chapter, the report goes deeper into the specifics of the preceding technique that was discussed in the earlier section and reveals the findings that were obtained as a direct result of that procedure.

Cross-referencing data graphs and tables have been generated because of conducting research into several different sample factors and characteristics. Utilizing the graphs that were produced, the research intends to cluster startups from a variety of viewpoints and achieve a more in-depth understanding of the major patterns that are involved in the ecosystem of digital identity startups. In the next chapter "Conclusions" will be summed up the key points that emerged that allowed to answer the research question.

The total sample of analysis includes 331 startups, for 261 of them is known the amount of funding received.

The analysis, as aforementioned, has be conducted under different perspectives:

- Geographical distribution
- Funding
- Foundation trend
- Market: target and application segments
- Technologies
- Value proposition

3.1 Geographical distribution

The geographical distribution analysis is based on information taken from Crunchbase.com pertaining to the location of the startup's headquarters. Nonetheless, it should be remembered that startups may also operate in other regions of the world. Understanding the geographical dominance of digital identity startups is facilitated by the emphasis on headquarters location. In addition, when this data is analysed alongside funding obtained, it can highlight connections between the entrepreneurial ecosystem and a startup's success in securing capital.

Despite various levels of concentration, the sample of companies analysed for this study includes representatives from all six continents, showing the worldwide significance of digital identity.

Figure 3.1 depicts the geographical distribution of startups by continent, including the percentage of startups on each continent, the average amount of investment per startup on each continent, and the total amount of funding received on each continent.

The characteristic connected to headquarters location is regarded as the major technique of determining which regions are most involved in this business given the global scope of digital identity firms. By studying the distribution of startups throughout the six continents, key centres of activity can be identified.

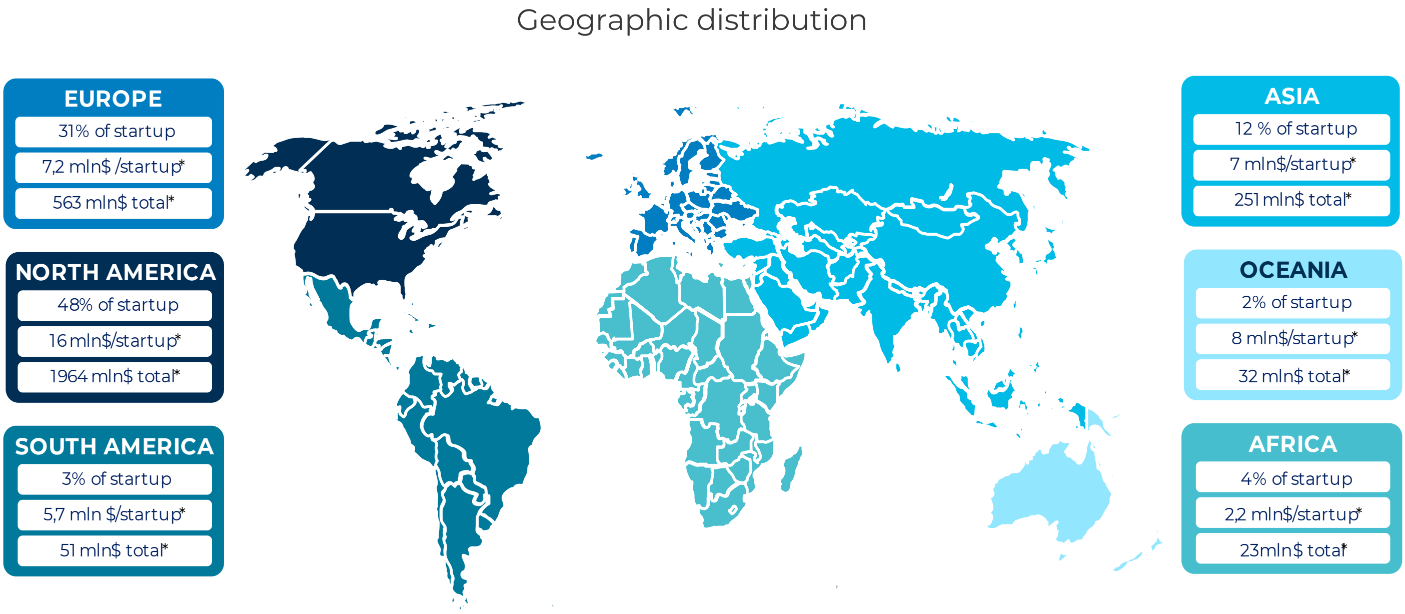


Figure 3.1 Geographical distribution of startup and funding received (total and average)

As previously suggested, there is a correlation between a company's ability to obtain capital and its connections to the entrepreneurial ecosystem. Both the number of startups and the amount of funding received are increasing, highlighting the prominence of North America and Europe.

North America is the continent with the greatest number of startups, with 158, followed by Europe and Asia, with 102 and 42 enterprises, respectively.

The dominance of these three continents is clear, as they account for 91% of all startups, leaving South America, Africa, and Oceania with only 29 companies.

It is interesting to observe how the value proposition of a firm is influenced by the various countries. With Africa's company, for instance, the focus is on offering people who lack a formal identity the opportunity to obtain one.

Startups are present in 49 states overall.

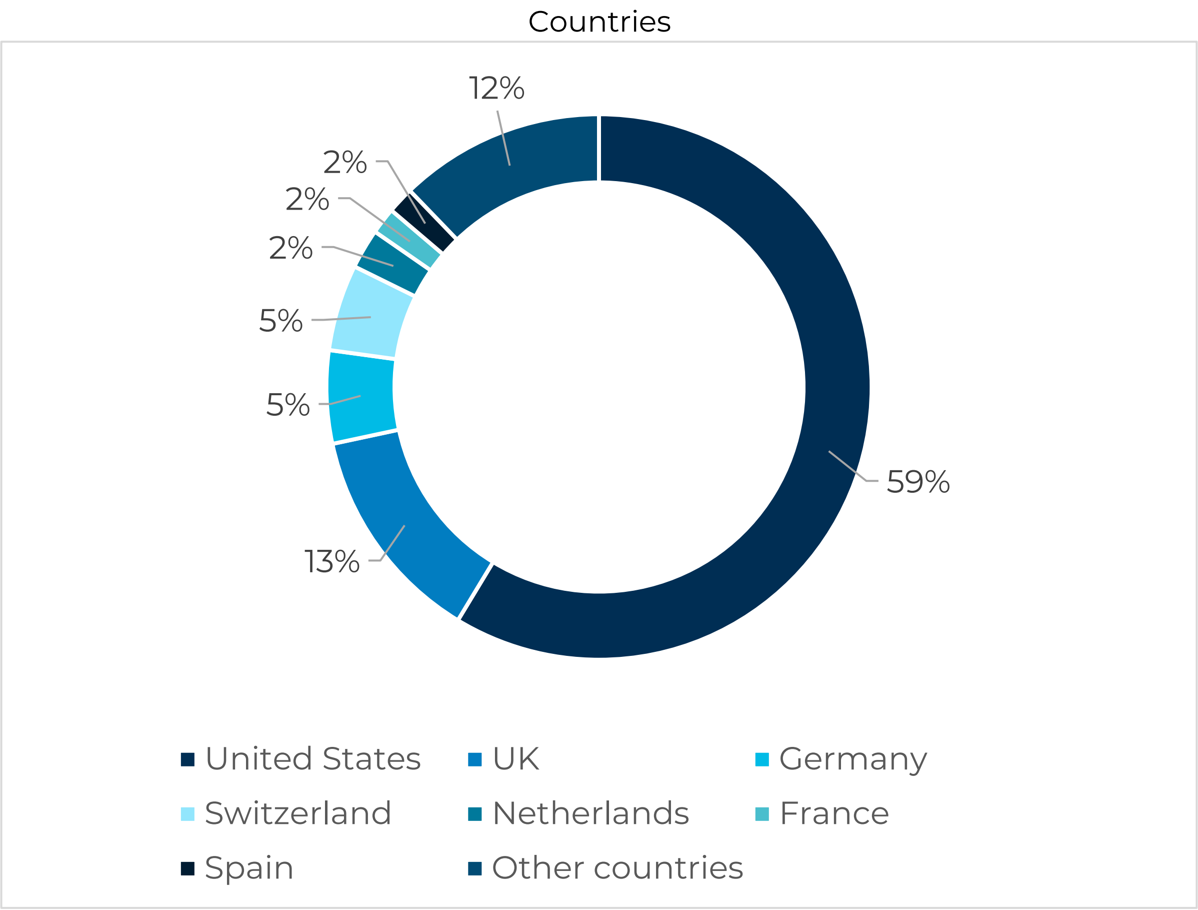


Figure 3.2 Startup in different countries

Figure 3.2 depicts the percentage of the total for the top seven most-represented nations.

As expected, the United States is the nation with the most startups, with a total of 149 accounting for 45% of the overall sample. The United Kingdom and Germany follow with 33 and 14 enterprises, respectively.

Even within specific nations and continents, there are huge differences in population size.

It is worthwhile to examine the locations of startups in the United States.

Surprisingly, California is home to 53 businesses, or over a third of all US startups (36%), with nearly half (23) of them situated in San Francisco. Due to its history of attracting talent and finance for high-tech firms and its closeness to Silicon Valley's entrepreneurial ecosystem, California remains the region with the greatest innovative ferment.

New York, Delaware, and Texas also have a significant number of digital identity startups, with 24, 9, and 8 firms, respectively.

State	N of startup
California	53
New York	24
Delaware	9
Texas	8
Florida	6
Massachusetts	6
Colorado	4
Georgia	4
Pennsylvania	4

Table 3.1 Startup in US state

Also, within European borders, there is a disparity in the number of entrepreneurial activities between nations. Table 3.2 depicts the geographical distribution of startups across Europe's represented nations. With 33 startups, the United Kingdom leads the ranking, followed by Germany and Switzerland with 14 and 13 companies, respectively. These three nations alone account for over fifty percent of all European startups.

London, and by extension the United Kingdom, has the highest proportion of startups (29) among EU nations, likely due to the city's extensive global connections and large talent pool.

State	N. Of startup
UK	33
Germany	14
Switzerland	13
The Netherlands	6
France	4
Spain	4
Sweden	3

Table3.2 Startup in EU states

Lastly looking at the main hubs, always remembering that the results could be biased by where the society decides to locate the headquarters, it’s noticeable that most of them are metropolis: London (29), San Franciso (23), New York (23) , Singapore (8) and Tel Aviv(7) .

This may be due to the inherent nature of cities, which may make them the best location for startups to easily gain access to the resources, talent, and opportunities required for growth and success.

3.2 Funding

The funding data were extrapolated from Crunchbase.com; however, the total amount of funding for the entire industry may be greater due to the delay in reporting the most recent amount of funding on the platform and the lack of funding data for each company in the census.

The number of startups for which the amount of funding received is known is 261 out of 331 considered, totalling 2.80 billion dollars, with an average funding amount of 11.05 million dollars per startup. During the subsequent analyses, the average amount of funding is determined by considering the number of companies whose funding amounts are known.

Always referring to the figure 3.1 above, the total amount of funding and the average per startup can be observed.

The geographical distribution of funding is extremely unbalanced, with North America accounting for 1964 million dollars (on average 16 mln$ per startup) and almost double the average funding for each startup compared to the rest of the world.

Europe with 563 million dollars (on average 7,2 mln$ per startup) and Asia with 251 million dollars (on average 7 mln$ per startup) are the two other regions with the highest average funding per startup.

The other three continents, which were already underrepresented in terms of population, received less funding: 51 million dollars for South America, 23 million dollars for Africa, and 32 million dollars for Oceania, even though the average amount of funding for Oceania was greater than that of Europe and Asia, which reported 8 million dollars for startup. Again, mentioning the possible bias introduced by Crunchbase.com, the result of the analysis indicates that both finance and entrepreneurial spirit are concentrated in the United States.

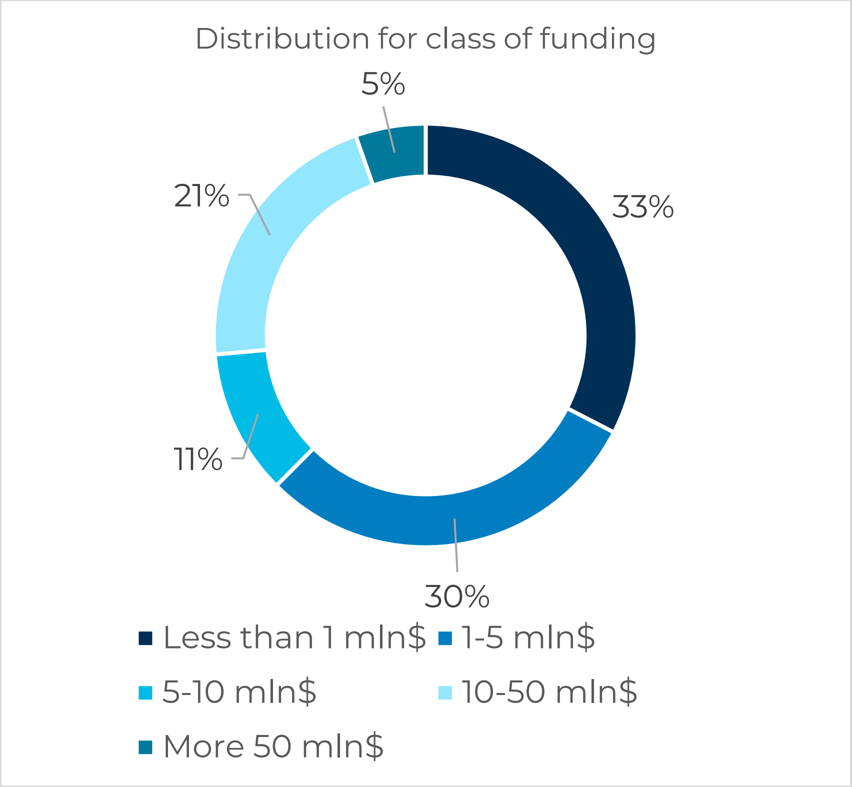


Figure 3.3 Distribution for class of funding

In order to gain a better understanding of the funding distribution, the census sample of 261 startups was divided into five funding categories. Due to the fact that only 21% of the sample has received funding of $10 million or more, the sector can be characterized as highly concentrated, with a small number of players receiving the majority of funding. 63% of startups have received less than five million dollars in funding, and 33% have received less than one million dollars. Typically, startups in the digital identity industry receive less than $5 million in funding, indicating that investors favor small investments.

Globally, it is interesting to note that 15% of the sample size (40 startups) received 2 billion dollars, which represents 72% of the total amount of funding, nearly following a Pareto distribution.

persona
BEYOND IDENTITY
STYTCH
veza
SEON

The five most funded startups account for 766,5 million dollars, or 42.6% of the total funding. Four of them are American, while one is Hungarian.

Following is a brief description of the top five most-funded startups for the sake of completeness:

- Persona (217.500.000$, General Purpose)

  Persona provides businesses with the ability to confirm customer identities (B2B2C), which enhances trust in online transactions and supports age verification, fraud prevention, and account recovery. Its range of automated identity verification features can be customized, branded, and themed to create tailored verification processes. The entity verified is the end user.

- Beyond Identity (205.000.000 $, General Purpose)

  Beyond Identity equipes secure digital commerce by substituting passwords with highly secure X.509-based certificates (for B2B and B2B2C). Creating a comprehensive Chain of Trust including the identity of users and devices, along with an up-to-the-minute assessment of the device's security status for flexible risk-based authentication and authorization. The entities verified can be end user or employee.

- Stytch (126.250.000$, General Purpose)

  Stytch improves security and user experience with password less authentication. Working with B2B2C helping to verify end users.

- Veza (110.000.000$, Enterprise)

  Veza is a data security platform that leverages authorization to enhance security working for B2B, giving the possibility to a better employee management. The platform is designed for multi-cloud environments to help use and share personal data.

- SEON (107.823.964$, General Purpose)

  SEON develops fraud detection software that uses machine learning and human intelligence to analyze transactional data, email verification, and IP address analysis to identify and report fraudulent activity in real-time checking end user identity. Helping businesses eliminate fraudulent activities and safeguard their data.

3.3 Foundation

From 2017 to 2021, the number of startups founded annually varies slightly.

The year 2018 has the highest number of startup establishments, 95, representing the most innovative entrepreneurial spirit.

High probability exists that the small number of startups founded in 2019 is influenced by the timing of data extraction. The database used for the analysis was extrapolated from Crunchbase.com in early 2022, which is likely affected by data update delays. The date constraint restricted the database to companies founded within the last five years. Since 2018, the number of startups has decreased, possibly as a result of digital identity breaches and competition from larger companies for resources and capital. This suggests that the maximum number of startups foundings may have already peaked, and a normal downward trend is currently underway.

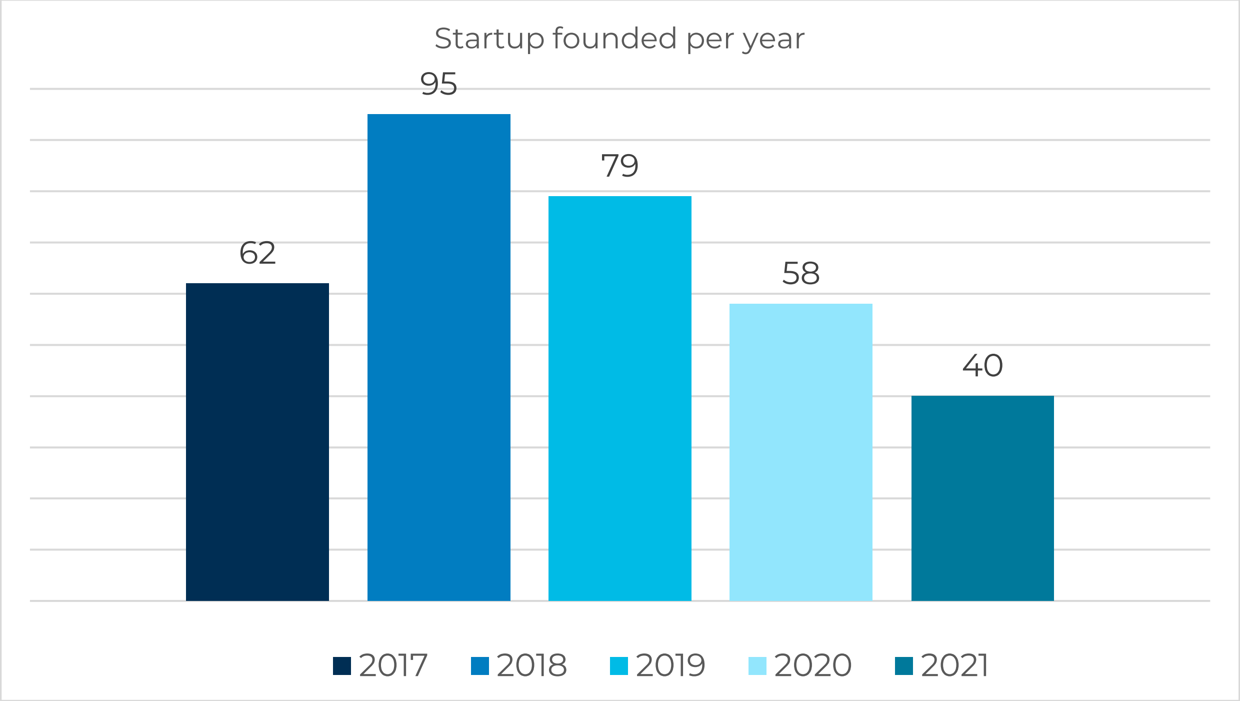


Figure 3.4 Startup founded par year.

3.4 Market

In the next section, it will be shown how startups engage with the market. First, it has been highlighted who they're trying to reach, and then in which industries are more likely to utilize digital identity.

3.4.1 Target

The business model of a digital identity solution provider can target business to business, business to consumer, or business to business to consumer transactions. Figure 3.5 depicts the distribution of the sample by customer type. About 227 of the startups are B2B2C-focused, 91 are business-to-business-only, and the remaining 40 target both types of customers temporarily. There is the possibility that a business targets multiple customer types.

The relationship between target customers and financing received is depicted in Figure 3.6. The first axis represents the total amount of funding received, while the second axis represents the average amount of funding. Companies targeting the B2B2C market have received the lion's share of funding, totaling $1,902 million, which is not surprising given the number of startups in this industry. However, B2B startups receive the most funding on average (15,1 million dollars), doubling the average funding received by B2C startups (6.8-million-dollar average)

Even though the majority of startups in the digital identity industry operate under a B2B2C model, the higher average funding received by B2B-focused startups suggests that investors may be more attracted to enterprise-level client solutions.

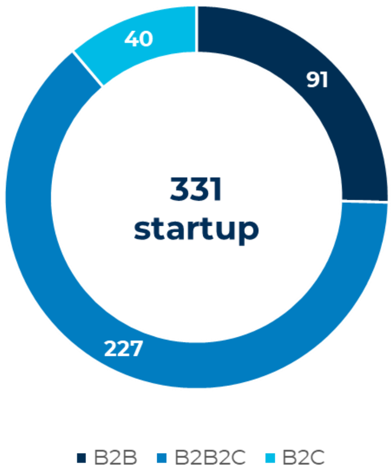


Figure 3.5 Target startup

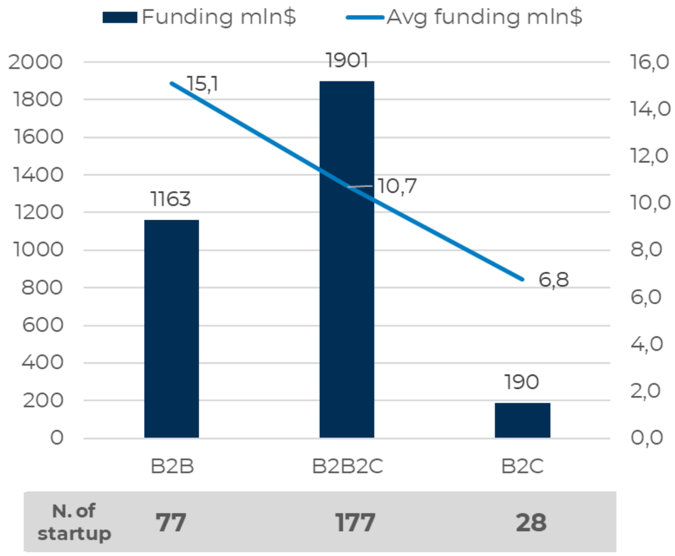


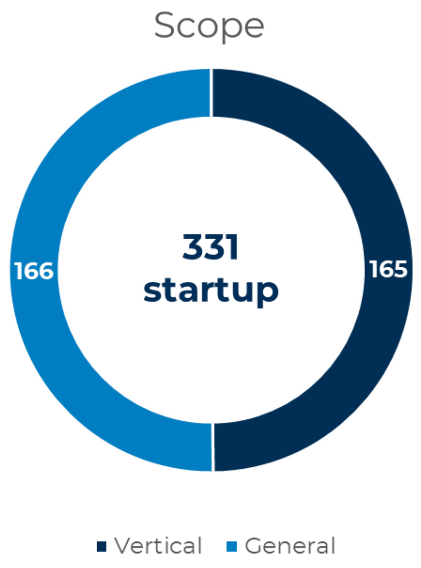
Figure 3.6 Fundation per target

3.4.2 Sectors of application

This analysis was conducted to determine which industries are most targeted by startups operating in the digital identity ecosystem, as well as the financing associated with them.

There are two categories of startups: general purpose and verticals. The first group is comprised of startups that are developing a solution for a wide variety of unrelated industries. It has been decided to include startups with four or more possible application fields in this category. Vertical startups, on the other hand, have a value proposition that is more focused on a particular industry. It has been decided to include startups with a maximum of three application fields in this category (for this reason, the total number of vertical application fields is greater than the number of "vertical" startups). eCommerce&Retail, Finance, Security, Telecommunications, Healthcare, Travel&Tourism, eGovernment, Legal, eGaming&gambling, Enterprise, Humanitarian, Mobility, and Education are the twelve vertical application fields considered.

In the General-purpose category, 166 startups have raised $1,586,000,000 (56%) of the total funding.



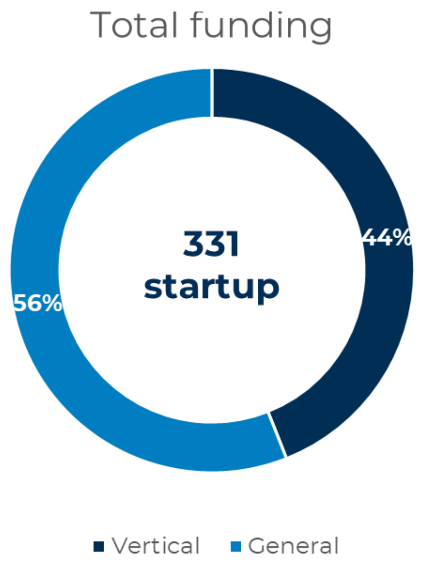


Figure 3.7 Number of startup par scope

Figure 3.8 Total funding par scope

The digital identity industry's startup landscape is well-distributed across various sectors, indicating widespread interest. Enterprise is the sector with the most startup companies, with 86, followed by Finance with 60 and Legal with 11.

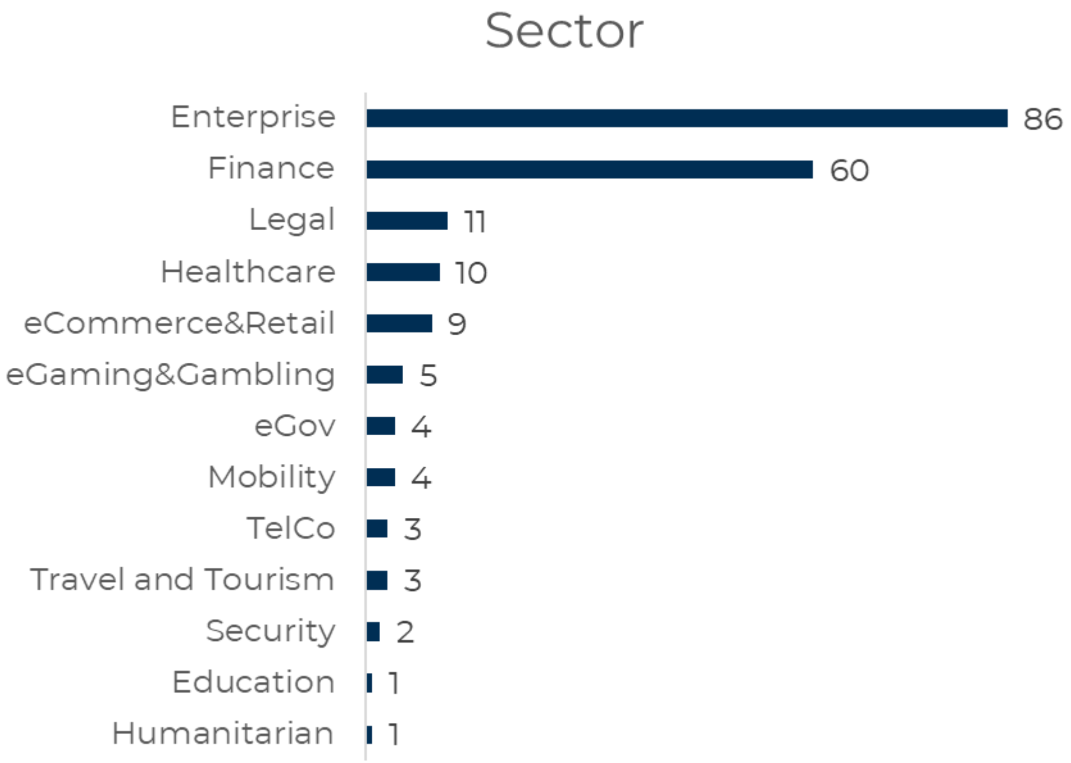


Figure 3.9 Startup in different application sector

Enterprise solutions has the largest number of startups, surpassing the Finance for the first time in the history of this census, which may be due to the growing demand for digitalization of internal processes, ranging from employee management to customer interactions within the organization.

For a better understanding of the trend, the following four examples of enterprise-focused startups are provided:

- Ermetic's SaaS was founded California, in 2019. The platform helps to prevent cloud infrastructure breaches by decreasing the attack surface and implementing least privilege on a large scale, even in the most complex environments. The platform offers comprehensive cloud security for AWS, Azure, and GCP by covering both cloud infrastructure entitlements management (CIEM) and cloud security posture management (CSPM). Cloud and API technologies are being employed to streamline the employee identification process, improving authentication procedures working with a B2B target.

- TECH5 was founded in Switzerland, in 2018. It is a technology company that specializes in developing cutting-edge biometric and digital ID solutions using AI and Machine Learning technologies. To enhance employee authentication, facial, fingerprint, and iris recognition technologies are being utilized. TECH5's target markets include both government and private sectors, and its products power Civil ID, Digital ID, and Authentication solutions, providing identity assurance for various use cases. It works with businesses, having a B2B target.
- OLOID was founded in California, in 2018. It offers a modern mobile access solution that replaces outdated workplace access management systems. OLOID integrates smoothly with existing technologies and the daily lives of users, enhancing the employee experience. With intelligent technology, API, cloud and biometrics OLOID provides improved control, usability, and trust in workplace access management. Its aim is bringing the future of mobile access to the workplace. Its target is B2B.
- EON was founded in New York, in 2017.It is a cloud platform developer that transforms physical products into intelligent and interactive assets, creating item-level digital identities for brands. The software, using API and blockchain, acts like an operating system, enabling companies to manage billions of products, driving sales, new applications, and partnerships across industries. EON collaborated with industry leaders to develop the CircularID™ Protocol, the language for products in the circular economy, allowing for communication across the value chain, crucial for scaling new business models such as resale and rental. Improving the authentication and identification process. Working for a B2B target.

To continue with the analysis, it is necessary to examine the funding received by each sector. The total funding ranking follows the same pattern as the number of startups: firms specializing in the enterprise sector account for $1,586 million, finance for $364 million, and mobility for $85 million. Those industries that have received the most funding are likely to offer the most lucrative and secure returns.

Particularly, eGovernment and telecommunications received the least amount of funding in the census, a possible indication that the interest in government applications is still at an early stage, likely due to the need for a high level of cooperation between different parameters, and that Telco is a field where startups are not interested due to the sector's high concentration.

The average financing is an interesting and informative index: Travel and Mobility sectors received the highest average amount, maybe with companies seeking out for new solutions using digital identity and covid effects.

At the same time these 2 sectors are the ones that have received the highest push for the digitalisation due to the COVID-19 pandemics.

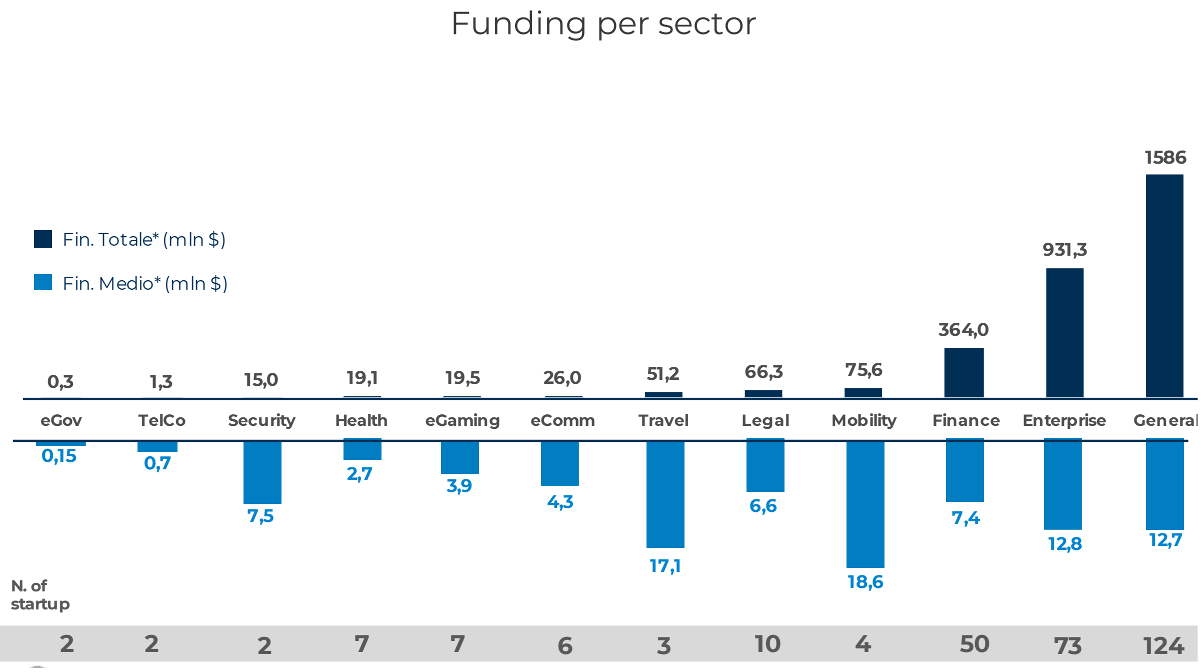
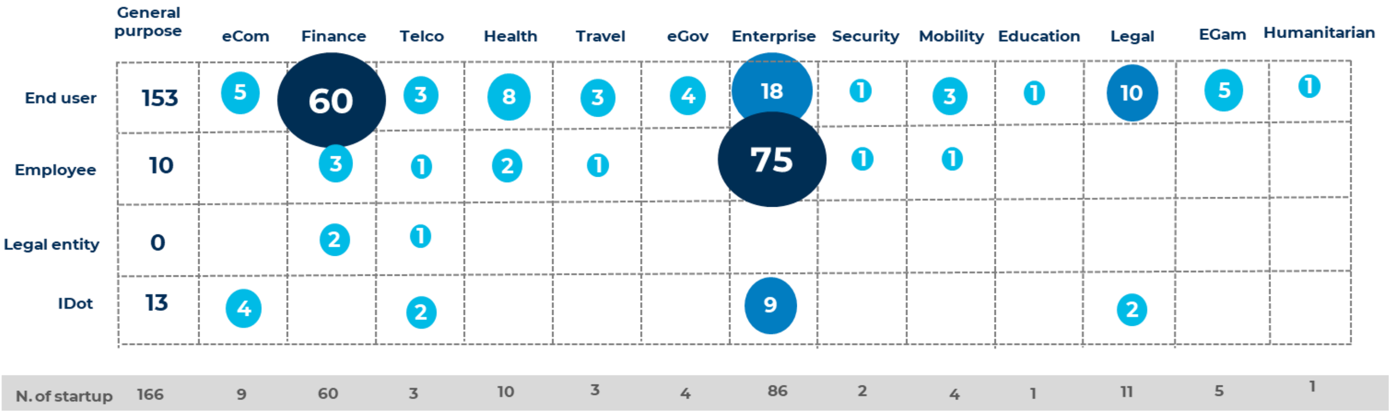


Figure 3.10 Funding in sector application

By cross-referencing data obtained from the census, it's possible to gain valuable insights about various sectors and entities verified. In particular, the significance of identity authentication for individuals is evident in both end-users and employees, who are prevalent across many sectors. In the finance sector, the focus is primarily on end-users who utilize banking services, especially with the growing popularity of home banking, as well as those engaged in the expanding world of cryptocurrency.

In contrast, enterprises are more interested in identifying their employees for efficient organization management.

It is not surprising that iDot identity authentication is critical for e-commerce, given that e-commerce is primarily focused on the selling of goods and services online, and for enterprises which often deal with document management.



	General purpose	eCom	Finance	Telco	Health	Travel	eGov	Enterprise	Security	Mobility	Education	Legal	EGam	Humanitarian
End user	153	5	60	3	8	3	4	18	1	3	1	10	5	1
Employee	10		3	1	2	1		75	1	1				
Legal entity	0		2	1										
IDot	13	4		2				9				2		
N. of startup	166	9	60	3	10	3	4	86	2	4	1	11	5	1

Figure 3.11 Interaction between identified entity and application sector

3.5 Technology

The subsequent analyses were conducted by analysing the startup's primary sources, such as their website and a few articles they had published. The analysis focuses on the technology used by new companies to provide their services to determine which trends are more diffuse, which ones attract more funding, and which could represent the future. Clearly, a single startup can utilize various technologies simultaneously. The various technologies are at different levels of development and maturity.

The ones taken into consideration are: blockchain, cloud, API & SDK, Open Standard (OIDC/SAML), AI and analytics, mobile device (smartphones are not considered), proximity device, and biometrics, which had its subcategories (face, voice, fingerprint, iris, vein, palm, finger bone, behaviour).

Considering the whole census, API&SDK (232), biometrics (133), and AI&analytics (118) are the most used technologies, providing respectively: integration of digital identity verification and authentication capabilities into different applications, secure and reliable means of verifying the identity of an individual and analyze vast amounts of data and identify patterns and anomalies that may indicate fraudulent activity or security (figure 3.12).

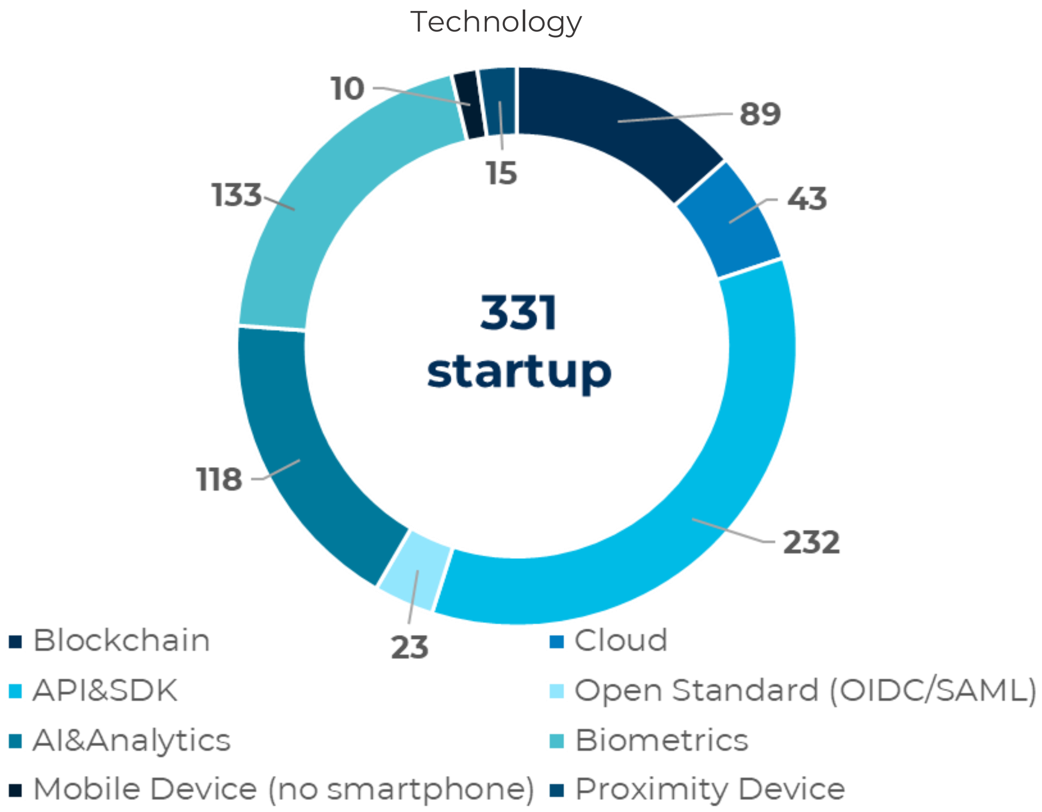


Figure 3.12 Startup working with different technologies.

It is important to study their distribution and relationship to the average funding received. Figure 3.13 shows the distribution of some of the leading enabling technology used by the startups in the sample. Startups leveraging on API&SDK received highest financing (2460 mln$). It follows cloud and biometrics with 1102 mln $ and 677 mln$ respectively.

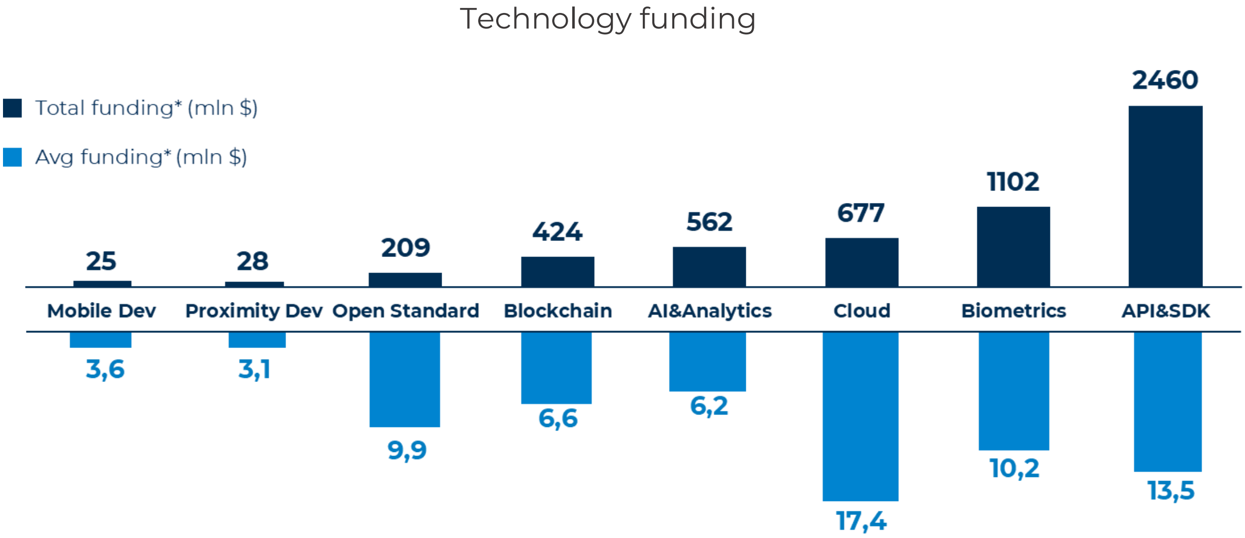


Figure 3.13 Funding per technology

The significance of biometrics and its various modalities merits a deeper analysis. Figure 3.14 depicts the frequency of various factors in the digital identity solutions provided by the sample startups. The face recognition system is used by 97 startups, followed by native (22), fingerprint (13) and voice (10). Others are less pervasive because they are novel types of solutions; therefore, time is required to develop and disseminate suitable hardware to support these recognition systems.

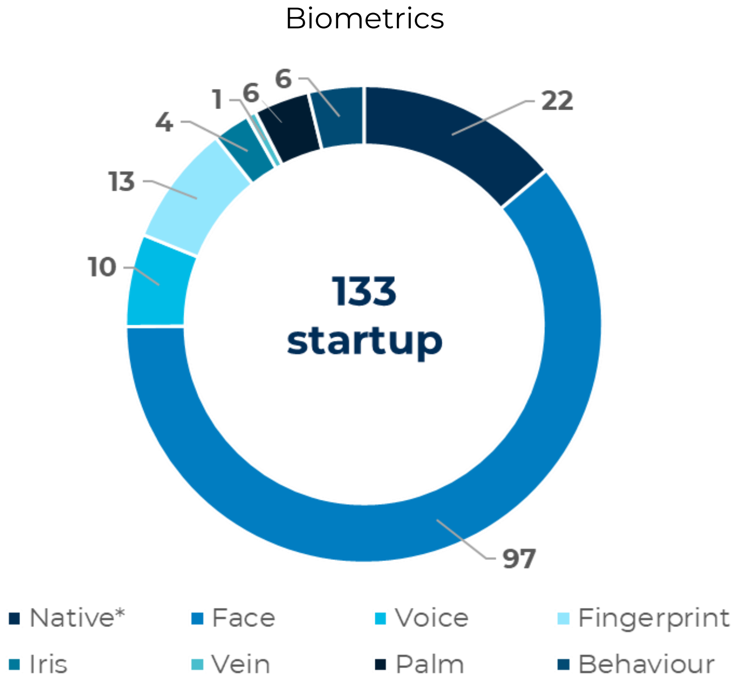


Figure 3.14 Biometrics application

Taking into account the funding received by each modality, facial recognition is the most prevalent and well-funded (584,7 mln$) form of biometric recognition, possibly due to his long-term implementation.

Native, which refers to the use of biometric sensors and algorithms that are built directly into a user device, received the highest average amount of funding (26,9 million dollars), likely because it can ensure seamless and secure identity verification and authentication without requiring additional hardware or software.

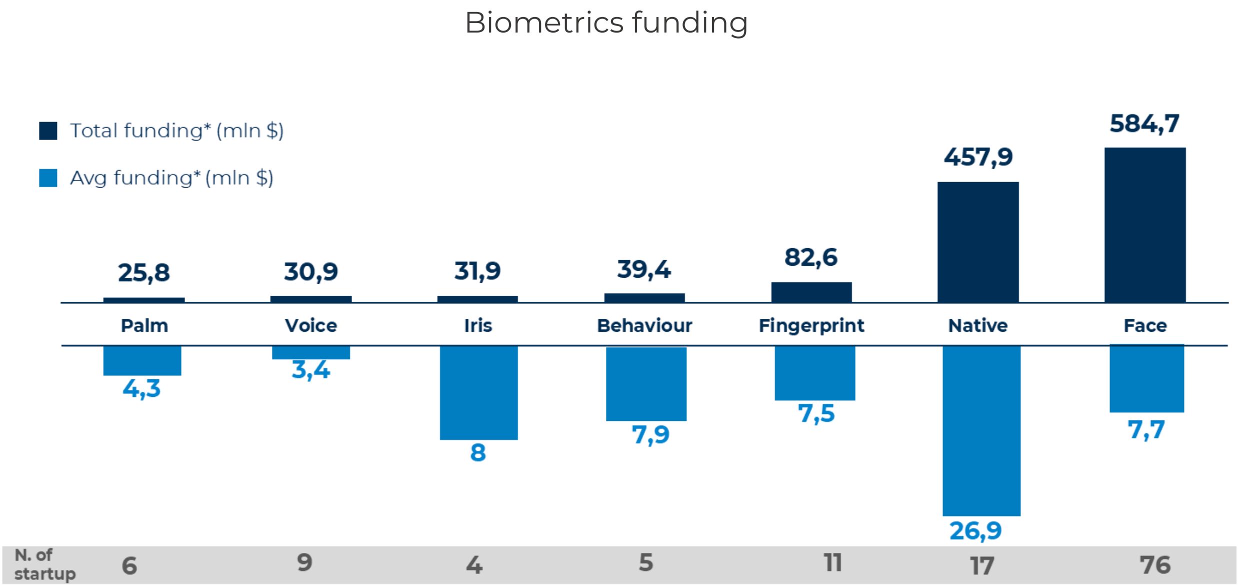
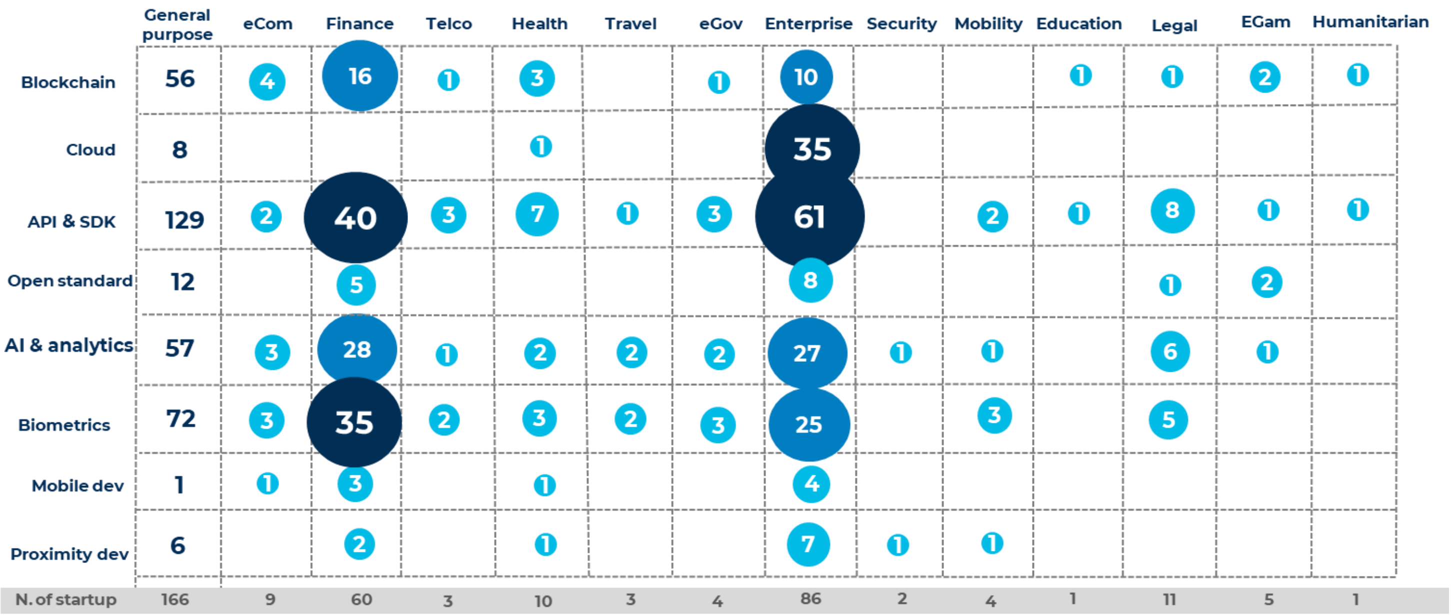


Figure 3.15 Funding in different biometrics application

As was done previously, it is possible to cross-reference data to gain a better understanding of the situation. In this instance, the relationship between the technology adopted and the application sector is highlighted.

The technology most utilized in almost every sector is API and AI&Analytics (the first one for the interoperability needs and the second supporting biometrics) particularly in the enterprise and finance sector API dominates (due to the interoperability and integration that companies' system needs).

At the second-place biometrics is present in almost every sector, confirming the importance of electronic recognition with user-friendly methods. Lastly, blockchain is present in a variety of industries, with extensive use in Finance and business to protect highly sensitive data.



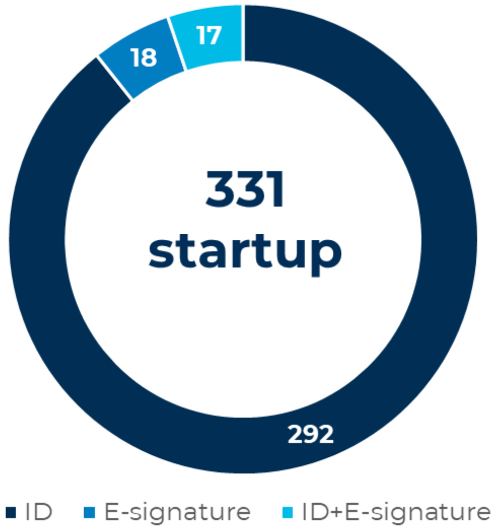
	General purpose	eCom	Finance	Telco	Health	Travel	eGov	Enterprise	Security	Mobility	Education	Legal	EGam	Humanitarian
Blockchain	56	4	16	1	3		1	10			1	1	2	1
Cloud	8				1			35						
API & SDK	129	2	40	3	7	1	3	61		2	1	8	1	1
Open standard	12		5					8				1	2	
AI & analytics	57	3	28	1	2	2	2	27	1	1		6	1	
Biometrics	72	3	35	2	3	2	3	25		3		5		
Mobile dev	1	1	3		1			4						
Proximity dev	6		2		1			7	1	1				
N. of startup	166	9	60	3	10	3	4	86	2	4	1	11	5	1

Figure 3.16 Interaction between technology and application sector

3.6 Value proposition

3.6.1 Value proposition definition

Considering the value proposition of the startup in the sample it's clear that considering only the quantity of startup or also the total and average funding received the primary focus remains on identification, even though some firms also provide e-signature services. Particularly 292 out of 331 startups provides identification, receiving a total amount of funding of 2748.3 million dollar, which is a significant difference from the amount received from e-signature, which has similar results as startups that offer both identification and e-signature, receiving $76.5 million and $57.3 million, respectively.



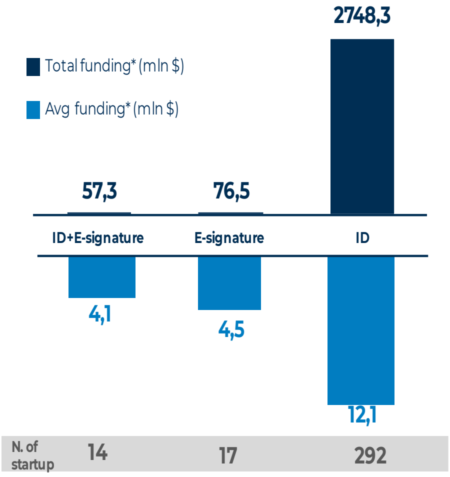


Figure 3.17 Value proposition

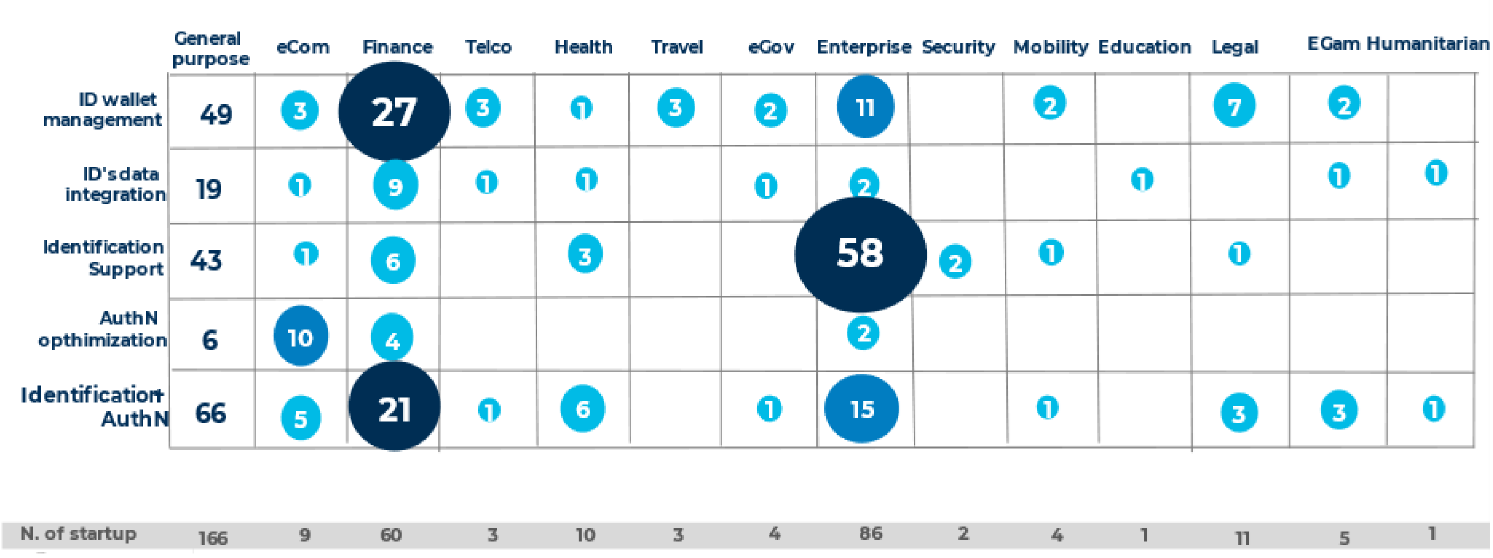
3.18 Funding among different value proposition

3.6.2 ID step process

As previously mentioned, startups that specialize in identification services offer a range of support throughout the identification process, which includes ID wallet management, ID data integration, identification support, authentication optimization, and identification and authentication services combined. These different offerings represent various opportunities for companies and governments to improve their business. Cross-referencing these steps with the application sector allows for a deeper comprehension of the situation.

As shown form the table one key sector that can benefit significantly from these services is the finance industry, where accurate and reliable identification is critical. Finance companies typically focus on ID wallet management and identification and authentication services, particularly in areas such as banking and cryptocurrency. With the rise of digital banking and the increasing use of cryptocurrencies, the need for secure and efficient identification solutions is more significant than ever. These services can help financial institutions verify the identities of their customers, prevent fraud, and improve overall security.

Another sector that can benefit from identification support services is the enterprise industry. These companies often require streamlined processes to facilitate internal operations and reduce operational costs. Identification support services can help in this regard by simplifying the process of employee identification and access control, reducing the risk of errors and increasing efficiency. By integrating identification technology into their operations, enterprises can improve their security measures and reduce the risk of data breaches or unauthorized access.



	General purpose	eCom	Finance	Telco	Health	Travel	eGov	Enterprise	Security	Mobility	Education	Legal	EGam	Humanitarian
ID wallet management	49	3	27	3	1	3	2	11		2		7	2	
ID'sdata integration	19	1	9	1	1		1	2			1		1	1
Identification Support	43	1	6		3			58	2	1		1		
AuthN opthimization	6	10	4					2						
Identification AuthN	66	5	21	1	6		1	15		1		3	3	1
N. of startup	166	9	60	3	10	3	4	86	2	4	1	11	5	1

Figure 3.19 Interaction between ID step process and application sector

As evidenced by the data presented in the table, there is a discernible trend in the amount of financing received by startups that specialize in identification services. Specifically, the areas of authentication and optimization, identification support, and identification and authentication combined have received the highest amounts of funding.

It is worth noting, however, that when comparing the average funding values across all steps of the identification process, there are no significant differences. This suggests that there is a general and comprehensive interest in investing in all aspects of the identification process, rather than a narrow focus on only a few specific areas.

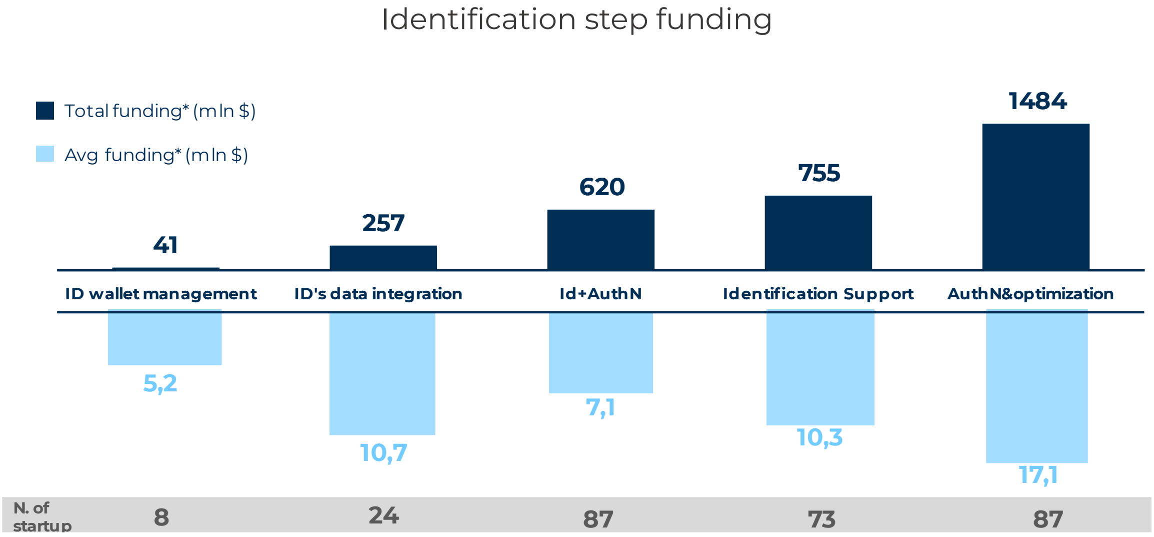


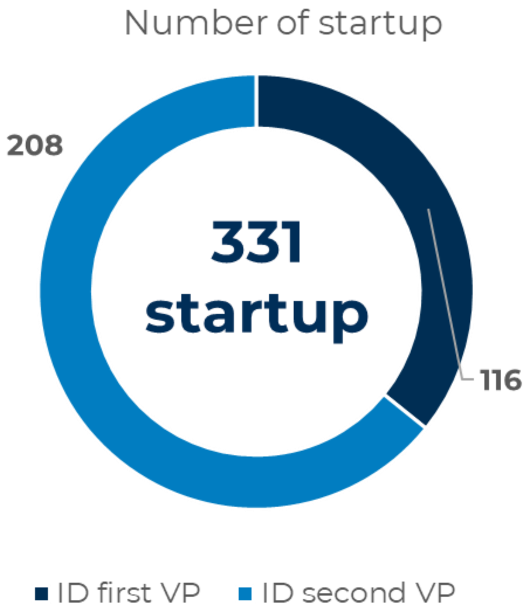
Figure 3.20 Funding of the ID step process

3.6.3 Barycentrism

Considering the barycentrism of the startups, 116 of them offer digital identity as a principal service while 208 for completing the offering.

Even if digital identity has become increasingly important, the number of startups that has in only as a second VP almost double the ones with ID as first VP, may be due to a focus on other areas or a need for digital identity features as a complementary or supporting function.

Looking at the total financing obtained, the ID as first value proposition collects 556 million dollars, while ID as secondary value proposition accounts for 2194 million dollars. More interesting is looking at the average funding, where the two categories report different result with ID as second VP more than double the average of ID as first VP.



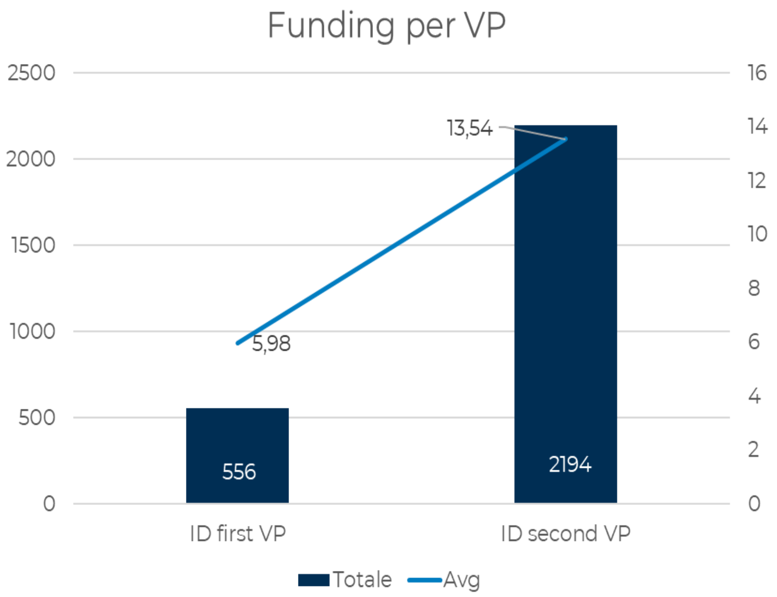


Figure 3.20 Startup VP *3.21 Funding per VP*

As a result of the considerations made prior even cross-referencing barycentrism data with application sector, the preponderance of ID as a second value proposal is evident.

In certain industries, digital identity is the primary value proposition, indicating the need for a dedicated offer. In the Humanitarian sector, for instance, where digital identity can play a crucial role in providing aid and assistance to those in need, it is understandable why some startups may prioritize digital identity as their primary product. In the Telco and eCommerce industries, where digital identity can facilitate secure and efficient transactions, a specialized offering can be a competitive advantage. The Mobility sector is another case, as digital identity can be used to facilitate access to transportation services, such as car rentals or bike sharing. In this case, having a dedicated digital identity offering can help streamline and simplify the process for users.

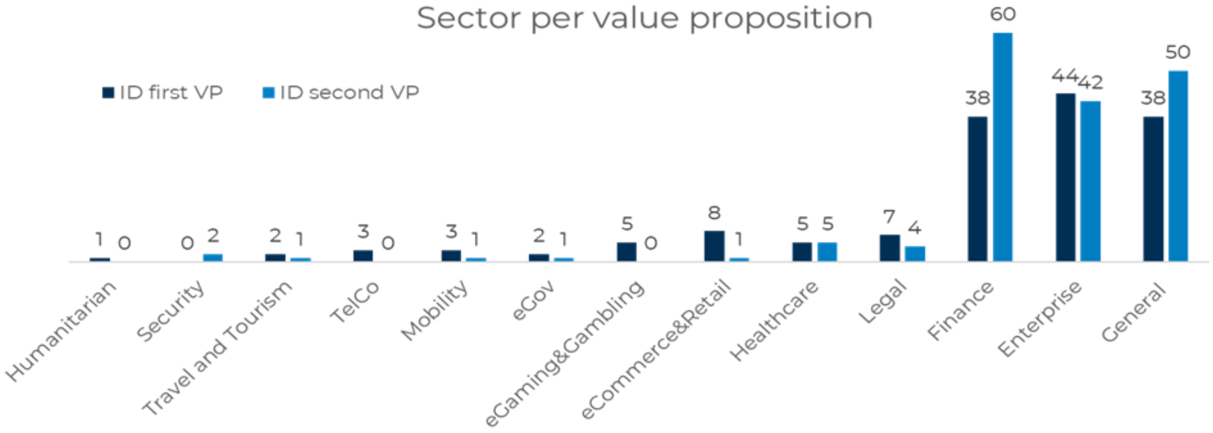


Figure 3.23 Interactions between sector and value proposition

4. Discussion

This chapter discusses the results of the analysis described in the preceding section. By summarizing the data of the descriptive analysis conducted on the sample startups, it will be possible to outline the distinctive characteristics of the digital identity startups ecosystem, thereby answering the research question that inspired this thesis. The conclusion of the section will address the limitations of this study and possible directions for future research.

The results presented in Chapter 3 demonstrate the existence of a global entrepreneurial ecosystem that focuses specifically on digital identity solutions.

This is an attempt to comprehensively describe this ecosystem of startups as a phenomenon distinct from other well-known domains such as Blockchain, Artificial Intelligence, and Big Data, with which it undoubtedly intersects. Following the same path of the other two census conducted under the guidance of the Digital Observatory of Politecnico di Milano in the last two year.

Even though digital identity startups are still a small portion of the vast technology industry, both in terms of number and funding received, a comparative analysis with other digital industries reveals that this cluster of startups possesses enormous and promising potential.

The vast majority of startups are located in North America, with the United States constituting a large proportion of the sample firms. Europe is also an important reality on the global stage, with the European Union promoting a project to establish a common standard for a valid digital European identity. It is essential to note that in both the United States and Europe, there are significant disparities between nations, with startup activity concentrated in specific regions, such as California and United Kingdom. Other continents have a startup presence, but at a significantly lower density.

Analysing the received funding reveals a huge disparity on a global scale. The average funding for each startup is nearly doubled in North America and Silicon Valley compared to the rest of the world, making it the most robust entrepreneurial ecosystem for attracting venture capital investment.
The trend is also confirmed by examining the five most funded startups, which account for 42.6% of the total global funding; four out of the five are American companies.

The concentration of investments in the dataset appears to follow a Pareto distribution, with 15% of the startups receiving approximately 72% of the total funding.

Since 2018, the number of startups founded has declined, due to digital identity breaches and competition for resources and capital from larger companies. This indicates that the maximum number of startup establishments may have already been reached, and a normal decline is currently occurring.

Analysing how startups engage with the market, it is evident that B2B2C solutions predominate, even though the greater average investment received by B2B-focused companies indicates that investors may be more interested in enterprise-level client solutions.

Secondly, from a market perspective, the analysis identifies the sectors of application spots, highlighting a balanced situation between general purpose, not targeting specific sections, and vertical purpose propositions. Regarding vertical solutions, the digital identity industry's startup landscape is well-distributed across multiple sectors, indicating widespread interest.
Enterprise is the prevailing industry for startup companies, and their primary focus is on employee identification, authentication, and document management. With Enterprise, Finance, Mobility, and Travel sectors represent some of the most founded startups on average, demonstrating the significance of new trends such as home-banking or cryptocurrency while also considering the effects of COVID-19, which heavily impacted these industries.

The analysis of enabling technologies reveals that API&SDK, biometrics, and AI&analytics are the most widely used, providing fundamental functions such as integration of digital identity verification and authentication capabilities into different applications, secure and reliable means of verifying the identity of an individual, and analysis of vast amounts of data and identification of patterns and anomalies that may indicate fraudulent activity or security risks.

Taking into account the investment received, there are differences; startups utilizing API&SDK, Cloud, and biometric technologies have received more than double the average funding received by companies utilizing the other technologies evaluated.

Focusing on biometrics modalities, facial recognition is the most pervasive and well-funded, presumably due to his long-term implementation, followed by native, which received the highest average amount of funding probably because it can ensure seamless and secure identity verification and authentication without the need for additional technology. Moreover, fingerprints continue to dominate in terms of quantity and funding.

The significance of biometrics and API&SDK is visible once one examines the vast number of applications in multiple sectors.

In the analysis of the value proposition, various information has been highlighted; it is evident that the startup's numerical and financial focus is on identification, and that identification and identification&authentication are the predominant process steps. On the other hand other there are services which expand a startup's offering, and the analysis reveals different application such as ID wallets, which are used to manage multiple identities, and ID’s data integration, which will assure better information exchange, will grow in the next years, favoured by services digitalisation.

Even though digital identity has become increasingly significant, the number of startups with digital identity as a secondary value proposition is nearly double that of those with digital identity as their primary value proposition. This may be due to a focus on other areas or a requirement for digital identity features to serve as a complementary or supplementary function. Also looking at funding received the barycentrism trend is similar. Nevertheless, it’s important to highlight how in certain industries (e.g.

Humanitarian, TelCo, eCommerce and Mobility), digital identity is the primary value proposition, indicating the need for a dedicated offer.

Conclusions

On the basis of the preceding arguments, it can be concluded that the startup digital identity ecosystem is expanding rapidly. Although the ecosystem is still in its early life, it is receiving significant funding, indicating that it has a high potential for future growth and development. As digitalization continues to expand across a variety of industries, the significance of digital identity solutions for individuals and organizations will only increase, creating more opportunities for startups in this space.

The methodology presented in the results chapter has been designed and reviewed throughout the report to obtain a research process that is as rigorous and replicable as possible, contributing to create a reliable information source on the Digital Identity startup ecosystem.

On the other hand, it is crucial to consider the limitations of resources and data collection, as well as the possibility of introducing bias:

- Starting from the information source origin, Crunchbase.com is the database from which the data were extrapolated. This site was selected due to its dependability and breadth; it compiles data on businesses from a variety of other online sources. However, it does not include every startup in the world, and as an American website, it may offer an unbalanced perspective that favors American startups. In addition, its upkeep necessitates a delay of a few months, so the most recent dataset may be partially insufficient.
- During the extraction phase, a complete series of keywords were used to evaluate and extract only those startups deemed relevant to the thesis. The selection of keywords was completed with the assistance of specialists in the field. Even so, it is possible that some significant startups were omitted from the count due to the absence of this information in their Crunchbase description.
- The data obtained from Crunchbase.com has been integrated with several information that emerged from startup sites and official social network pages. The outcome of the process in considering pertinent information may have been affected differently by the author's viewpoint. Furthermore, the same objectivity of the data present on institutional websites could be doubted.
- The final challenge to the process of gathering and integrating data is the scarcity of scientific information on the area being investigated. Due to the novelty of the topic in management discourse, a portion of the evaluated scientific information comes from multiple research streams and authoritative reports, as opposed to scientific papers.

Due to the novelty of the arguments, this thesis represents one of the first approaches to this topic. This work could be a starting point for future research, for which new directions may be outlined:

- The database should be reviewed and updated periodically to account for the growth and evolution of the startup ecosystem. Adding a second source of information could significantly improve the collected data's reliability.
- A case study focusing on one or more wildly successful startups could aid in enlightening best practices in digital identity reality.

- Utilizing questionnaires allows for the incorporation of information variables related to specific startups. The database, which already contains email addresses and telephone numbers, provides a foundation for further quantitative analysis.
- Using a regression analysis, it will be possible to better understand the relationship between two or more variables of the startups, having a deeper insight of the ecosystem. This analysis could reveal, for instance, which characteristic are more important to receive fundings.

Bibliography

Alangot, B.;Szalachowski, P.; Dinh, T.T.A.;Meftah, S.; Gana, J.I.; Aung, K.M.M.;Li, Z. (2023). “Decentralized Identity Authentication with Auditability and Privacy.” Algorithms 2023, 16, 4.

Alsadeh, A.; Yatim, N.; Hassouneh, Y. (2022). “A Dynamic Federated Identity Management Using OpenID Connect.” Future Internet

Arner, D. W.; Barberis, J. N.; & Buckley, R. P. (2018). “Regulating a revolution: From regulatory sandboxes to smart regulation.” Journal of Financial Perspectives: FinTech, 2(2), 1-14.

Atick,Joseph J; Gelb,Alan Harold; Pahlavooni,Seda; Gasol Ramos,Elena; Safdar,Zaid.Word Bank Group (2014). “Digital identity toolkit: a guide for stakeholders in Africa”

Kronfellner B.; Merey T.;, Beron D. and Terbu O. ; BCG(2021) “Me, myself and (SS)I Why everybody must have a Self-Sovereign Identity in 5 years”

Cabarcos P.(2010)”Dynamic Trust Relationship Establishment in Federated Identity Management”

Chadwick, D. W. (2009). “Federated identity management.” Foundations of Security Analysis and Design, 96-120

Clark J.; Metz A. and Casger C.;Word Bank Group(2021). “ID4D GLOBAL DATASET Volume 1 | 2021 Global ID Coverage Estimates”

Dib O. and Toumi K.(2020) “Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions”

FATF (2020) “Digital Identity.”

Gartner (2019) “Critical Capabilities for Full Life Cycle API Management”

Gartner (2019) “Innovation Insight for Bring Your Own Identity”

Gartner (2019) “Magic Quadrant for Full Life Cycle API Management”

GSMA,World Bank Group, and Secure Identity Alliance (2016). “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation”

Hirsch-Allen J.; Figge H. and Kaplan A.; IBM (2022). “The next evolution of digital identity: Scalable, secure, and trusted digital credentials”

ISO/IEC 24760-1:2019. “Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts.”

Jensen H. and Hewett N.; World Economic Forum(2019).”Inclusive Deployment of Blockchain for Supply Chains Part 2 – Trustworthy verification of digital identities”

Jovanović B., Milenković I., Sretenović M.B. and Simić D. (2016) “Extending identity management system with multimodal biometric authentication”, Computer Science and Information Systems, vol.13, pp. 313-334.

Kanwar S.; Reddy A.; Fellow; Kedia M.; Manish M.; ADBIinstitute (2022). “The Emerging Era of Digital Identities: Challenges and Opportunities for the G20”

Krämer, J., P. Senellart and A. de Streel (2020). “Making data Portability More Effective for The Digital Economy,” https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). “Self-sovereign and decentralized identity as the future of identity management?” Open Identity Summit 2020.

Lee Jong-Hyouk (2017). “BIDaaS: Blockchain Based ID As a Service”

Manyika, J. et al. (2016). “Digital Finance for All : Powering Inclusive Growth in Emerging Economie”, McKinsey Global Institute. 107

Mastercard (2019) “Restoring Trust in a Digital World, Media Trust in a Digital World.” doi: 10.1007/978-3-030-30774-5.

NIST(2022) “Announcing the Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors”

O’ Halloran D.; Manju G.; Spelman M.; Duda C.; Glowacki M et al.; World Economic Forum (2020). “Reimagining Digital Identity: A Strategic Imperative”

OECD (2011). “DIGITAL IDENTITY MANAGEMENT Enabling Innovation and Trust in the Internet Economy”

OECD (2021). “Report for the G20 Digital Economy Task Force”

Osservatorio Digitale Politecnico di Milano (2020). “Alla ricerca dell’identità…digitale”

Osservatorio Digitale Politecnico di Milano (2020).“L’IDENTITÀ DIGITALE: DEFINIZIONI E SCENARIO GENERALE”

Pöhn, D.; Grabatin, M.; Hommel, W. (2021). “eID and Self-Sovereign Identity Usage: An Overview. “Electronics 2021,

Pwc (2019) “Blockchain and Digital Identity: the path to Self Sovereign identity.”

Rose J., Rehse O. and Bjorn R.; BCG (2012) “The value of our digital identity.”

Saracco R., (2020). “An accelerated digital transformation, courtesy of the recent pandemic”, 2020 ITU Kaleidoscope: Industry-Driven Digital Transformation,

Enriquez M. and Segovia A.; BBVA (2019) “Digital Identity: the current state of affairs.” BBVA Research.

Sonpatki S.; Seksaria R.; Raina M.; Chehal H.; Banka L.; Hebbar P. and Bhaskar V Deloitte (2021) “API-enabled digital ecosystems”

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). “Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation.” Blockchain: Research and Applications, 2(2), 100014.

Sullivan, C. (2018).”Digital identity – From emergent legal concept to new reality”

Sundberg N.; Maddens S.;Huseinvoci K.; Simpson K. and Friedmann B.;ITU (2018). “Key considerations for e-Identification interoperability”

Sundberg N.; Maddens S.;Huseinvoci K.; Simpson K. and Friedmann B.; ITU(2018). “Digital identity in the ICT ecosystem: An overview.”

The United Nations (2015). “About the Sustainable Development Goals - United Nations Sustainable Development, Sustainable Development Goals.”

The World Bank Group (2018a). “G20 Digital Identity Onboarding.”

Thiel, P. (2014) “Zero to One - Notes on startups, or how to build the future.” Crown Business - New York.

The World Bank Group (2018b) “Technology Landscape for Digital Identification, Technology Landscape for Digital Identification.”

The World Bank Group (2017). “Principles on Identification for Sustainable Development : toward the digital age. “

Wang, Y., Qin, X., Lu, Y., & Lou, W. (2018). “Hybrid authentication with a password and a fingerprint for web applications.” IEEE Transactions on Information Forensics and Security, 13(3), 531-546.

White O.; Madgavkar A.; Manyika J.; Mahajan D.; Bughin J.; McCarthy M. and Sperling O.; McKinsey (2019).” Digital Identification: A Key to Inclusive Growth. “ Available at: www.mckinsey.com/mgi.%0Ahttps://www.mckinsey.com/~/media/mckinsey/featured insights/innovation/the value of digital id for the global economy and society/mgidigital-identification-a-key-to-inclusive-growth.ashx

Williamson C. (2021). “The Role of Multi-factor Authentication for Modern Day Security”

Word Bank Group (2022). “ID4D Annual report”

World Bank (2018a) “Private sector economic impacts from identification systems”

World Economic Forum (2016) “A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity, World Economic Forum, Future of Financial Services Series.” Available at: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

World Economic Forum (2018). “Identity in a Digital World A new chapter in the social contract”

Y. Cao and L. Yang (2010). “A Survey of Identity Management Technology”. In: IEEE International Conference on Information Theory and Information Security, Beijing, 17-19 December 2010, pp. 287-293.

Zhu, X. and Badr, Y., (2018). “Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors, 18(12), pp. 4215.