Digital Identity

Report

FINALLOT

November 2023

Executive summary

The digital identity sector is experiencing a dynamic surge marked by technological innovation and increased global digitalization. Venture capital investments support startups offering secure and privacy-conscious identity solutions. This report analyses the digital identity VC market, overviewing trends, regional landscapes, regulatory impacts, investment trends, risk assessment, and the influence of cybersecurity and emerging technologies on VC funding. The demand for user-centric, privacy-focused digital identities continues to rise, driven by consumer expectations, data breaches, and evolving regulations. VC investors are keen on startups leveraging emerging technologies such as decentralized identity and blockchain-based solutions. The digital identity VC market is poised for sustained growth, propelled by the enduring need for secure, user-centric identity solutions accelerated by the COVID-19 pandemic and the demand for remote services, data privacy, healthcare, cross-border identity, and e-commerce verification. VC investments in this sector are expected to remain robust, emphasizing long-term growth and innovation potential.

Technology Overview

Digital identity technologies encompass a diverse array of tools and methodologies aimed at establishing, verifying, and managing individuals' and entities' online identities in an increasingly interconnected world. These technologies collectively play a pivotal role in enhancing online security, user convenience, and data privacy within the digital ecosystem.

Identity and Access Management (IAM) Systems. IAM systems are designed to manage user identities, access rights, and permissions. They provide administrators with the tools to control who can access specific resources and services within an organization. However, IAM systems require careful implementation to balance robust security and user-friendliness, as overly complex setups can hinder user productivity.

Biometric Authentication technologies, such as fingerprint recognition, facial recognition, iris scanning, and voice recognition, are commonly used to verify an individual's identity. By 2025, biometrics are projected to authenticate over $3 trillion of payment transactions, with mobile payments reaching $1.2 trillion globally by 2027. These technologies offer heightened security and user convenience, reducing reliance on traditional password-based systems.

Decentralized Identity and Verifiable Credential Management. Decentralized Identity (DID) grants individuals control over their digital identities and reduces reliance on centralised authorities. Blockchain and distributed ledger technologies often underpin DID systems. The World Wide Web Consortium (W3C) officially recognized Decentralized Identifiers (DIDs) as a web standard on July 19, 2022. Decentralized identity is often used interchangeably with Self-Sovereign Identity (SSI), an approach that empowers individuals to control their identities through three core components: blockchain for secure data storage, verifiable credentials for presenting secure information, and DIDs for personally identifiable information-free identifiers.

Passwordless Authentication technology enables users to access their digital accounts and services without traditional passwords, relying on alternative, secure factors like biometrics or registered devices, enhancing security and user experience. Passwordless authentication reduces fraud risk from vectors like phishing and brute force attacks, shifting fraudster focus to vulnerabilities like synthetic identity. Examples of passwordless authentication methods include One-Time Password (OTP) / One-Time Code (OTC), TOTP (Time-Based One-Time Password), HMAC (Hash-based Message Authentication Code), Magic Links and others.

Biometric Liveness Detection technology verifies that a biometric input (e.g., a fingerprint or facial scan) comes from a live and not a static source, enhancing security by preventing the use of fake or stolen biometric data. Liveness detection methods in biometrics include eye blinking, blood flow detection, pupil dilation, voice response, and keystroke dynamics, among others, to ensure that the collected biometric data is from a living person.

Mobile-Based Authentication. Mobile devices are often used for identity verification, either through biometrics (e.g., fingerprint or face recognition) or mobile-based authentication apps. Mobile devices also generate one-time passwords (OTPs) for MFA.

Zero Trust Security Model assumes no trust by default, requiring continuous verification and authentication of users and devices, regardless of their location or network. This approach helps protect digital identities in a perimeterless environment. Yet, implementing Zero Trust can be hindered by complexities, resource requirements, interoperability issues, encryption needs, user experience concerns, and other challenges, yet the potential benefits are significant when executed carefully.

Privacy-Preserving Technologies include homomorphic encryption, differential privacy, and zero-knowledge proofs. Such technologies enable data verification without revealing sensitive information. Homomorphic encryption, while powerful, introduces computational overhead and limits the types of computations. Zero-knowledge proofs offer enhanced privacy but can be complex to implement and face interoperability challenges. Balancing their benefits with practical complexities is essential for successful adoption.

Persona and Signals-Based Intelligence (PSBI) is an advanced approach to enhancing data personas by incorporating various data elements with AI and machine learning. It provides a comprehensive and context-aware understanding of consumer behavior, aiding businesses in decision-making, predicting outcomes, and optimizing revenue, customer satisfaction, and fraud prevention. PSBI adapts to changing data patterns, offers actionable guidance, and is a proactive strategy for shaping customer behavior, making it a valuable tool for fraud prevention and data-driven decisions.

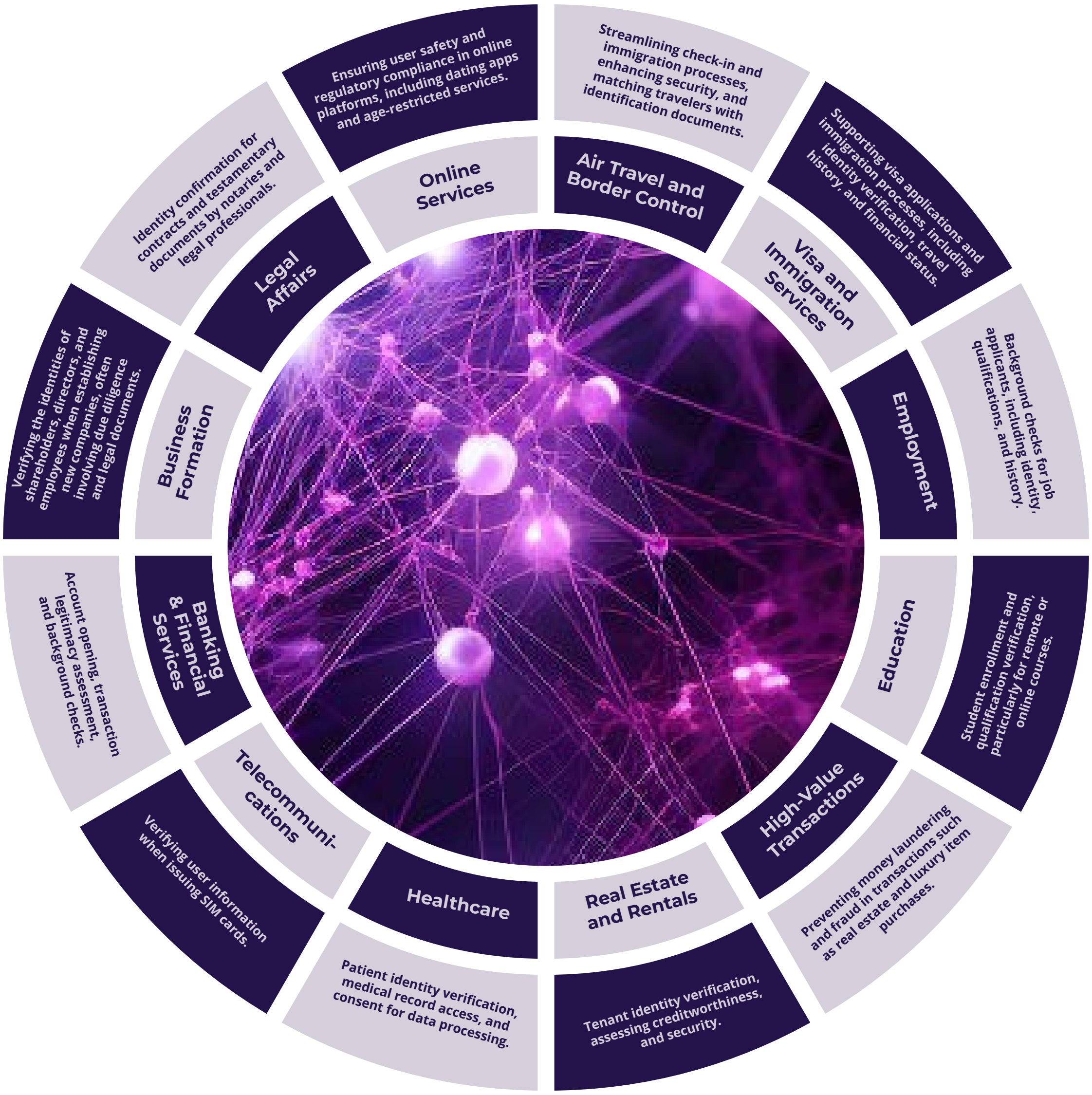
User and Entity Behavior Analytics (UEBA) is a cybersecurity technology that monitors and analyzes the behavior of users and entities in a digital environment. By establishing normal behavior patterns, UEBA identifies anomalies and potential security threats that may evade traditional security measures. It employs machine learning to create user and entity profiles, offers real-time monitoring, generates alerts for suspicious behavior, and often integrates with other security systems for a comprehensive security approach. UEBA is particularly valuable in detecting insider threats and enhancing proactive threat mitigation and incident response, which has been highlighted by over 65% of organizations integrating UEBA into their identity and access management systems.

IoT using Blockchain. As the Internet of Things (IoT) ecosystem continues to expand, the need to secure machine identities becomes paramount. Projects like Keyfactor, a machine identity management platform, help organizations secure the growing number of devices in IoT networks. A study by IoT Analytics predicts that by 2030, there will be over 50 billion connected IoT devices, emphasizing the critical role of machine identities in maintaining the integrity and confidentiality of data exchanged within these networks.

There are other relevant technologies focused on digital security and identity management that take on the marker. For instance, Public Key Infrastructure (PKI) operates as a foundational framework, employing asymmetric cryptography to oversee digital certificates and keys, ensuring secure communication and authentication. Trusted certificate authorities issue digital certificates, serving as a cornerstone in verifying the identity of users and devices. Concurrently, OAuth and OpenID Connect, recognized open standards for authorization and identity authentication, are widely adopted in single sign-on (SSO) solutions, enabling users to access multiple applications seamlessly with a unified set of credentials. Identity as a Service (IDaaS) platforms further revolutionize identity and access management (IAM) by offering scalable and cost-effective cloud-based services, encompassing user provisioning, authentication, and access control. Complementing these, Self-Service Password Reset solutions empower users to reset passwords, reducing dependence on IT support autonomously. Finally, Digital Identity Wallets securely store and manage individuals' digital identity information, granting users control over their data and facilitating selective sharing with relying parties or services as needed. This ensures a tailored and secure digital identity experience.

Major trends

The digital identity market today is characterized by rapid growth and diversification. It is widely anticipated to be the next disruptive technology in the market, impacting the lives of millions. Most recently, a TechCrunch C-level executive acknowledged that, based on their latest survey conducted among their investors, everyone expressed a strong interest in the digital identity space. Digital identity technologies are widely adopted across various sectors, including finance, telecommunications, healthcare, real estate, and more, to enhance security and streamline processes.



Online Services: Ensuring user safety and regulatory compliance in online platforms, including dating apps and age-restricted services.

Air Travel and Border Control: Streamlining check-in and immigration processes, enhancing security, and matching travelers with identification documents.

Visa and Immigration Services: Supporting visa applications and immigration processes, including identity verification, travel history, and financial status.

Employment: Background checks for job applicants, including identity, qualifications, and history.

Education: Student enrollment and qualification verification, particularly for remote or online courses.

High-Value Transactions: Preventing money laundering and fraud in transactions such as real estate and luxury item purchases.

Real Estate and Rentals: Tenant identity verification, assessing creditworthiness, and security.

Healthcare: Patient identity verification, medical record access, and consent for data processing.

Telecommunications: Verifying user information when issuing SIM cards.

Banking & Financial Services: Account opening, transaction legitimacy assessment, and background checks.

Business Formation: Verifying the identities of shareholders, directors, and employees when establishing new companies, often involving due diligence and legal documents.

Legal Affairs: Identity confirmation for contracts and testamentary documents by notaries and legal professionals.

The digital identity market's importance is propelled by mounting security concerns, user demand for superior experiences, and evolving regulatory requirements. It plays a pivotal role in data protection, fraud prevention, and identity theft mitigation within the broader technology and cybersecurity landscape.

Key trends in Digital Identity include

1 **Tech-First Approach**: VC investors prioritize startups adopting cutting-edge technologies like blockchain for Decentralized Identifiers (DIDs) and biometric authentication. These forward-thinking startups are gaining significant investor interest.

2 **Regulatory Considerations**: VC firms rigorously assess startup compliance with complex and evolving data protection and privacy regulations in the digital identity space, influencing investment decisions.

3 **User-Centric Solutions**: Startups offering user-centric digital identity solutions, prioritizing seamless and privacy-respecting experiences with strong security, are attracting investor attention. UX approaches among digital identity startups can be categorized as:

- *Those resembling Metamask or similar crypto-wallets (e.g., AltME, Selfkey, Idena, GlobalID);*
- *Startups with generally subpar UX (e.g., Polygon ID, Nametag, BrightID, Midy, Validated ID, Lissi, Gataca, CorePass, Holdr+);*
- *Projects striving to enhance usability on top of an intuitive UX (e.g., GlobalID, Yoti, Bloom ID, Nuggets, etc.).*

4 **Cybersecurity Investment**: VC firms are increasingly directing investments toward startups that focus on robust cybersecurity within the digital identity space. With the growing concerns around security breaches and data leaks, investors are seeking to mitigate these risks by supporting startups that emphasize security in digital identity solutions. This trend underscores the significance of cybersecurity within the digital identity sector.

5 **Decentralized Identity (DID) Adoption**: The digital identity market is witnessing increased interest and investment in decentralized identity solutions. Decentralized Identifiers (DIDs) provide users with more control over their digital identities and reduce reliance on centralized authorities.

Major players

Traditional industry incumbents

Google is a prominent player in the digital identity space, and offering a range of identity and access management services, including Google Sign-In and Google Cloud Identity. These services are widely adopted by both businesses and consumers, facilitating secure and streamlined authentication processes.

Microsoft delivers a suite of identity solutions, with Microsoft Entra ID at the forefront. These offerings are tailored to meet the needs of enterprises and government agencies, ensuring robust identity management and access control.

Okta (as well as Okta Personal) stands out with its specialization in identity and access management services, providing businesses with secure and user-friendly authentication solutions.

Ping Identity offers an extensive portfolio of identity and access management solutions, with a particular emphasis on customer identity and access management. Their services enable businesses to manage customer interactions securely, fostering trust and convenience.

ForgeRock is a player in the digital identity landscape, specializing in identity and access management solutions for both enterprises and Internet of Things (IoT) devices.

Verification-oriented digital identity & decentralized identifiers

Worldcoin, or World ID, strives to build the world's largest identity and financial network with a motto: "Worldcoin: for every human." Positioning itself as a public utility, it has gained traction among users, with an impressive user base of 130,000 in November 2021, skyrocketing to 2,000,000 by May 2023. The project has secured substantial funding, having raised $125 million, and a total valuation of $3 billion, with a remarkable cost of $50 per user. With around 180 employees, it's actively expanding, indicating the ambitious scope of its objectives in the field of identity and finance.

TBD, a crypto venture by Block, was founded in July 2021 in San Francisco. Not live yet, it operates as Block's business unit, focusing on building an open-source developer platform in financial services. Led by CEO Jack Dorsey (co-founder and former CEO of Twitter, CEO of Square), TBD's motto is to make a decentralized world accessible to all. The aim of the company is to utilize open-source technology to restore ownership and control over finances, data, and identity. TBD is a Bitcoin-focused project striving to simplify the creation of non-custodial, permissionless, and decentralized financial services. The company's whitepaper outlines their vision, emphasizing decentralized identity for trusted exchanges and economic transactions. The tbDEX protocol is a key example, allowing direct on-ramping and off-ramping between traditional and decentralized financial systems.

GlobalID, launched in January 2016 and led by Greg Kidd, an early investor in Square and Twitter, GlobalID is a pioneer in digital identity. It focuses on providing users with an efficient platform for managing identification documents. GlobalID encourages users to sign a Global Identity Declaration, emphasizing the "thing in itself" concept through action. While the platform facilitates cryptocurrency transactions, including sending and receiving crypto, it does not support purchases and card integration. Despite steep transaction fees, transactions function well. GlobalID supports document verification through Veriff, recognizing national passports but encountering issues with certain residence permits and expired driver's licenses. Additionally, it enhances security by including the user's selfie.

Yoti, founded in 2014 and headquartered in London, is a pioneering force in the realm of digital identity verification. The company provides a free consumer app that conveniently stores user ID on a mobile device, with over ten million worldwide downloads. Yoti has expanded its offerings to include business solutions like identity verification, age estimation, e-signatures, and AI anti-spoofing technologies. The user-friendly mobile signup employs a 5-Pin security measure and robust identity verification for name, surname, and dateof birth, cross-checked against sanction lists. Users can link multiple email addresses and mobile numbers, supporting one-to-many ID verifications, including passport and residence permit verification via NFC technology. The platform allows manual address input, encourages state ID confirmation for added security, and provides Google-based account recovery. Yoti ensures a sleek interface for an exceptional user experience, complemented by a desktop-only e-signature service, enhancing its identity and document management capabilities.

Bloom ID, founded in February 2018 in Miami, is a comprehensive solution for obtaining and managing a credit score, encompassing email, mobile, address, and SSN verification. Bloom has further demonstrated its commitment to regulatory compliance by seeking SEC registration for its $BLT token, positioning itself as one of the first registered tokens with the SEC. The company has garnered significant attention and support, with investors such as 1confirmation and Signia Venture Partners contributing to an $8 million Series A funding round in 2018. By 2019, Bloom had already reached the impressive milestone of 1 million users, marking rapid growth in its user base. Their ID verification process requires both SSN and the relevant identification document, along with address and mobile number confirmation, focusing on alignment with the country of the verified ID, often utilizing Cognito for these checks. However, some state-issued IDs may face rejection, and there may be occasional delays with the verification of a second ID. The integration with Metamask verifies an Ethereum wallet, but it sometimes experiences delays in updating its status. On the other hand, Bloom successfully verifies bank accounts through Plaid and income sources via Netchex, with additional free tracking for stolen passwords, akin to Google Account protection. Users can also access transparent Politically Exposed Persons (PEP) base screening results. Bloom's interface allows for smooth integration with LinkedIn profiles and other platforms.

Nuggets, established in London in August 2016 by an ex-Skype executive Alastair Johnson and Seema Khinda Johnson. Branded as the "only identity super wallet," Nuggets provides a unique solution for verified self-sovereign decentralized identity, compliance, and multi-rail payment services. Nuggets sign-up process includes a 6-pin code and biometrics for strong user protection, while offering a resilient recovery process. Their verification options are diverse, covering various aspects of user identity, including ID verification through Onfido for different countries and documents, alongside text recognition. Address verification is streamlined via driver's licenses, though manual address addition remains unverified. Nuggets also facilitates bank card addition through transactions and supports a range of document types, albeit with a focus on the UK market. Despite its less visually appealing design, the application shines in

Utility-oriented digital startups

Nansen ID addresses the challenge of identity verification, compliance, and financial access in sanctioned countries and high-risk regions. It offers a solution with an identity-first open banking platform, providing users with a verified digital identity. This grants them access to partner banks and fintech providers, streamlining both fiat and cryptocurrency account management within a user-centric interface. Nansen ID leverages in-depth information gathering, alternative data sources, a "social endorsement" mechanism, and re-usable identity data to ensure convenience and security. By bridging the identity and financial service gap, it transforms financial access in sanctioned regions, promoting inclusivity and transparency.

ID.ME is a startup founded in 2010 as TroopSwap, which has evolved into a digital identity verification platform, particularly serving the American military community. The company offers a verified digital ID card that allows users to access government services and benefits, including managing SSA benefits and IRS online accounts. With a valuation of $1.5 billion and widespread adoption in 22 U.S. states, ID.me has secured significant funding, totaling $240 million, establishing itself as a prominent player in the digital identity verification industry. Currently, it provides consumers with a digital wallet, allowing them to access substantial discounts and earn cashback while shopping. The company streamlines access to offers from over 5,000 stores. This ensures consumers have a simplified solution to save on their preferred brands and products.

Plumia has introduced a solution known as the Nomad Border Pass. This digital identity program allows nomad users to obtain a single visa, providing them with pre-approved access to a network of participating countries for up to 90 days. By simplifying the process of global mobility, Plumia empowers digital nomads to seamlessly pursue their remote work lifestyles while contributing to economic growth and innovation.

Baseflow has taken on the challenge of simplifying the path to obtaining citizenship through investment programs. These processes are often burdened with legal requirements and complexities. The company offers a comprehensive digital identity solution that streamlines the entire journey. By providing an all-in-one platform, Baseflow eases the challenges faced by individuals aspiring to become citizens of progressive nations.

State-level digital identity initiatives

Aadhaar (India). Launched in 2009 by the Unique Identification Authority of India (UIDAI), Aadhaar is India's pioneering biometric identity project. It is the largest in the world as it has provided digital IDs to over a billion Indian citizens. It serves as a fundamental component of various government programs and services and continues to expand its services and integration with various government services for broader accessibility.

ID4D (UN & World Bank). Developed collaboratively by the United Nations and the World Bank, the ID4D project has been instrumental in advancing global digital identity efforts with a focus on inclusivity. Launched to set international standards and facilitate knowledge sharing among countries and organizations, it aims to promote equitable access to digital identities.

MitID (Denmark). Launched in 2021, the MitID project is supported by the Danish government and represents a significant milestone in enhancing digital identification for Danish residents. It was initiated to improve online security and is steadily progressing with widespread adoption. Future plans involve ongoing refinements and adaptations to meet the evolving digital landscape and security requirements.

POPIA (South Africa). South Africa's Protection of Personal Information Act (POPIA) is actively supported and enforced by the South African government. Launched to safeguard individuals' digital identities and personal data, it aims to protect data privacy. The future focus remains on maintaining compliance and adapting to changing data protection needs.

Lei Geral de Proteção de Dado (Brazil). Launched in 2020, Brazil's Lei Geral de Proteção de Dado is supported by the Brazilian government and aligned with global data protection standards. It is aimed at preserving data privacy, with a focus on ensuring the adherence of organizations to these regulations and consistently adapting to emerging data privacy challenges.

myGovID (Australia). Supported by the Australian government, myGovID is continually evolving to offer a secure and convenient digital identity solution for its citizens. Launched to simplify access to government services, it continues to expand its capabilities and services, making it even more user-friendly and versatile.

Common weaknesses of digital identity startups

Emerging digital identity startups often face three common challenges:

1. Lack of targeted go-to-market strategy: Many startups attempt to serve a broad and diverse audience across various regions simultaneously, resulting in inefficiencies, a diluted value proposition, and an inability to address specific user segments or industries effectively.

2. Compliance and integration issues: Failure to consider existing regulations and integration requirements can lead to compliance problems, data privacy concerns, and trust issues with users. Understanding the legal framework and data interoperability is essential.

3. Balancing assurance and utility: Overemphasizing verification through intense focus on encryption and authentication can lead to user frustration. Subjecting users to a cumbersome verification process, only to discover a lack of meaningful functionalities or services in their digital identity profiles, emphasizes the need to prioritize utility. Adopting a Jobs-to-be-Done approach becomes crucial, highlighting the importance of ensuring that the digital identity ecosystem not only establishes strong verification mechanisms but also provides tangible services to enrich the overall user experience.

Addressing these challenges is crucial for the success of digital identity startups. A targeted go-to-market strategy helps identify niches and create tailored solutions, while compliance and integration efforts ensure legal operation and effective collaboration. Emphasizing utility and user-centric services enhances the user experience and demonstrates the value of digital identity solutions beyond mere verification, positioning startups for long-term growth and competitiveness in the evolving digital identity landscape.

Regulatory landscape in Digital Identity

The digital identity sector operates within a complex regulatory landscape, with each region or country imposing its own rules and standards.

United States

In the United States, digital identity technology operates under a regulatory framework comprising federal and state-level laws. While a comprehensive federal data privacy law is absent, individual states like California have introduced significant legislation, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), impacting how companies manage consumer data. Additionally, the National Institute of Standards and Technology (NIST) provides guidelines and standards for digital identity and authentication, shaping industry best practices. Moreover, the U.S. government offers the Cybersecurity Framework with guidance on managing cybersecurity risks, particularly relevant to digital identity security.

China

China's digital identity sector is influenced by the government's focus on digital transformation and innovation. Regulatory elements include national standards for digital identity, mandating specific technical requirements and security measures for companies operating in this space. Government oversight is run by agencies like the Cyberspace Administration of China (CAC), which is crucial in ensuring compliance with these regulations and national standards. Additionally, Chinese regulations demand the localization of personal data storage within the country, potentially impacting foreign digital identity companies' operations. This regulatory landscape prioritizes data protection and security, with fines of up to $77,000 for data security breaches. Severe data exposure consequences, such as system malfunctions or extensive breaches, can lead to fines of up to $300,000, operational shutdowns, and license revocations.

India

India's digital identity landscape revolves around the Aadhaar system, one of the world's largest biometric identification programs. The Aadhaar Act provides the legal foundation for utilizing Aadhaar in various applications, both in government and the private sector. India is also in the process of enacting a comprehensive data protection law, which will affect how digital identity companies handle user data, with potential fines of up to Rs. 250 crore (around $3.3 million) for mishandling or failing to protect digital data. Furthermore, Know Your Customer (KYC) regulations for financial institutions, governed by the Reserve Bank of India (RBI), further shape the digital identity landscape, requiring banks to establish comprehensive policies covering KYC standards and Anti-Money Laundering (AML) measures.

European Union

The European Union is at the forefront of data protection and privacy regulations, with key regulatory aspects including the General Data Protection Regulation (GDPR), which comprehensively addresses data processing, including digital identity. The eIDAS Regulation, adopted in 2014, establishes the framework for electronic identification and trust services, promoting electronic transactions in the internal market. Additionally, EU regulations prioritize "privacy by design," urging companies to incorporate privacy features into their digital identity solutions from the early stages of system planning, a concept introduced in the 1970s and integrated into the Data Protection Directive RL 95/46/EC in the 1990s.

United Kingdom

The UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1) outlines standards and guidelines for digital identity providers, certifying bodies, and various stakeholders. It focuses on ensuring the security, privacy, and interoperability of digital identity services, setting the rules and principles for different service providers and certifying bodies. The Data Protection and Digital Information Bill is expected to provide a legal framework for identity and eligibility checks against trusted government-held data, aiming for the reliability and trustworthiness of digital identity services.

Israel

Israel's rising influence in the digital identity technology arena is underpinned by its strong regulatory framework. The Israeli Privacy Protection Authority regulates personal data handling and affects digital identity solutions. Furthermore, the nation's stringent cybersecurity regulations have implications for digital identity companies, especially those engaged in safeguarding critical infrastructure.

Government policies on VC investment

Governments across these regions have policies that either encourage or regulate VC investments in the digital identity sector. These policies can include tax incentives, grants, and investment support for startups in the field, specific for every country: the United States, the European Union, the United Kingdom, China, India, Israel. Additionally, some governments may limit foreign investments in strategic areas of digital identity for security reasons.

Top 5 large venture deals in 2021-2023

Worldcoin: blockchain innovations

The preeminent leader in blockchain-based digital identities, both in terms of funding size and media coverage, is undoubtedly Worldcoin. The company has managed to secure a remarkable $125 million in funding over two rounds with a $3 billion valuation, with their latest round achieved through an Initial Coin Offering on March 23, 2022. This substantial influx of capital has established Worldcoin as a unicorn in the world of cryptocurrency and blockchain startups. Notably, the project has garnered the support of 20 investors, among them high-profile figures like Andreessen Horowitz, underlining the interest that this innovative venture besides some controversy over its seemingly dystopian nature.

SpruceID:
a lifecycle of digital credentials

Spruce, a dynamic player in the world of startups, has successfully secured a total of $41.5 million in funding across four funding rounds, with their latest financing round taking place on February 28, 2022, in the form of a Series A round. With the support of 26 investors, including prominent names like Y Combinator and Orange DAO, Spruce demonstrates its appeal and potential within the investment community, positioning itself for further growth and innovation in its field.

Yoti: digital ID and customer verification

Yoti, a company specializing in secure digital identity management, has successfully raised a total of £26 million in funding through four rounds, with their most recent financing round taking place on March 9, 2023. With support from four investors, including notable names like Lloyds Banking Group and Future Fifty, Yoti's innovative approach to digital identity management continues to gain traction and investment interest, positioning the company for further advancements in the realm of secure online identification.

Trinsic: verifiable credentials infrastructure

Trinsic, a comprehensive self-sovereign identity platform that empowers users to share and verify their personal data online securely, has made significant strides in its development. With a total of $17.5 million raised in funding through two rounds, its most recent financial boost came from a Seed round on June 29, 2022. Trinsic is backed by a group of seven investors, highlighting the growing interest and confidence in the platform's potential to reshape how individuals manage and protect their digital identities.

CLEAR: biometric identity verification

An example of a later-stage company, CLEAR, specializing in biometric identity verification and expedited security screening, has successfully raised a substantial $135 million in funding across six rounds, with their most recent funding coming from a Private Equity round on February 8, 2021. Trading under the ticker symbol NYSE:YOU, and having $4.5 billion in IPO valuation, CLEAR debuted in the stock market on June 30, 2021. Notably, CLEAR has garnered support from 17 investors, with prominent names like LionTree and Liberty Media contributing to its growth. Furthermore, CLEAR's expansion efforts were evident in its acquisition of Whyline on January 4, 2022, underlining its commitment to enhancing its service offerings in efficient and secure identity verification.

Market potential

The digital identity market seeks to disrupt established markets in areas such as traditional identification processes, financial services, online security, and data privacy by offering innovative and secure solutions that empower individuals and businesses to take control of their digital identities and safeguard sensitive information.

The general overview of market development shows that the market size evaluation started at a benchmark of around 23.3 billion dollars in 2020 and 2021, 34.5 billion dollars in 2023, with a compound annual growth rate (CAGR) projected to be between 15.5% and 19.3% over the forecast period (most research chooses a 7-8 year projection horizon). The market is forecasted to reach 70.7 billion dollars in 2027 and 82.2 billion dollars in 2028, which places the digital identity market in the category of not only emerging markets but also as one of the fastest-growing markets.

Regional patterns in the digital identity field exhibit distinctive trends and developments. The Americas and Europe have placed a significant emphasis on decentralized solutions, emphasizing user control and privacy. In contrast, Asia, with particular prominence in China and India, has made remarkable progress with centralized digital identity solutions, often government-controlled. This top-down approach helps ensure a higher pace of adoption and standardization, facilitating widespread use of these solutions within their borders. However, it poses challenges in terms of interoperability with international services, as well as vulnerabilities associated with potential abuse of power of the centralized solutions. In the West, access to venture capital and substantial investment has played a pivotal role in driving technological advancements and innovation, contributing to the growth and maturation of digital identity solutions, following a bottom-up approach, in contrast to the market development pattern in the East.

COVID-19 impact on digital identity market

The COVID-19 pandemic significantly reshaped the digital identity VC market. Initially, the pandemic led to an increased demand for remote identity verification solutions as businesses and organizations sought secure ways to authenticate customers and employees without physical contact. This demand fueled a boost in global spending on digital identity verification technology, which is anticipated to reach $16.7 billion by 2026, a 77% increase from the projected $9.4 billion in 2021.

The pandemic accelerated the digital transformation efforts of many businesses, driving interest in digital identity solutions that facilitate secure and contactless transactions. Heightened security concerns related to identity theft, fraud, and data breaches, as even companies like Facebook, LinkedIn, and X/Twitter have been affected. This led to a greater focus on startups offering advanced cybersecurity and identity verification solutions. In the long term, the shift to remote work and digital services is expected to persist, sustaining the demand for digital identity solutions that enable secure access and verification. Increased emphasis on privacy and data protection, an evolving regulatory landscape, collaboration with healthcare and health passport solutions (e.g., Clear Health Pass, CommonPass), vaccine verification (e.g. EU Digital COVID Certificate), and secure health data management (e.g. IBM iDoctor), and continued investment in biometric and contactless technologies are among the lasting effects of the pandemic on the digital identity sector.

Investment horizons and expected returns

Investing in digital identity startups requires a nuanced understanding of investment horizons and the potential returns investors can anticipate. Digital identity startups typically traverse different phases, influencing the duration of investment and the expected outcomes.

Early-stage investments, such as seed and Series A, usually demand a more extended investment horizon, spanning 3 to 7 years. During this phase, startups are in their initial development stages and need time to establish and scale their digital identity solutions. Investors in this stage target substantial returns, often aiming for a range of 10x to 30x their initial investment, with exit strategies including acquisition by tech giants or initial public offerings.

Growth-stage investments, typically occurring in Series B and beyond, come with a slightly shorter horizon of about 3 to 5 years. Startups in this stage have already demonstrated market traction and seek expansion and market dominance. Investors anticipate returns in the range of 5x to 15x their initial investment, often realized through acquisitions, strategic partnerships, or further funding rounds that enhance the startup's valuation.

Risk assessment

Investing in the digital identity sector involves evaluating several risk factors. VC investors must navigate complexities in sales cycles, such as prolonged contract negotiations and user adoption challenges. Geopolitical risks, including international regulations and export controls, may impact market access. Compliance with data privacy and cybersecurity regulations is crucial to avoid penalties and maintain trust. The competitive landscape poses challenges, particularly when competing against established players and in crowded markets. Investors must assess a startup's technological capabilities and cybersecurity measures, considering the potential impact of economic downturns. Lastly, exit opportunities and market saturation can affect the returns on investment.

Evaluating cybersecurity measures in digital identity startups

Cybersecurity holds paramount importance in the digital identity sector, directly influencing the trust and security of identity verification processes. VC investors closely examine cybersecurity measures during the due diligence process to ensure startups can meet the critical security standards required for their success.

VC firms evaluate a range of cybersecurity best practices, starting with the strength of a startup's authentication methods. This includes assessing multi-factor authentication (MFA) and other techniques such as biometric and behavioral-based authentication including among others voice or speaker recognition, signature analysis, and keystroke dynamics. **Robust data encryption**, and protocols (e.g. TLS/SSL, IPsec, SSH, PGP, S/MIME, Kerberos) ensure compliance with industry standards.

Secure data storage, **continuous monitoring** for potential threats, and **regulatory compliance**, particularly with GDPR and **industry-specific regulations**, are essential considerations. Investors examine **incident response policies**, incident **recovery plans**, and whether the startup undergoes security audits and penetration testing. Protecting user data is a priority, with **data minimization** collecting only necessary user data and disposing of it when it's no longer needed. User consent for data collection and processing is expected to **be transparent** and well-documented to build trust among users.

The presence of well-defined **cybersecurity policies** is closely scrutinized, ensuring startups have procedures for incident response, data breach notifications, and the protection of customer data. Additionally, startups are expected to have robust incident recovery plans that demonstrate their preparedness to mitigate the impact of potential breaches.

Security audits, **penetration testing**, and certifications are essential components of cybersecurity assessment. VC firms may seek independent third-party audits to ensure objectivity and transparency in evaluating the startup's security measures.

Specialized funds that invest in the sector

Andreessen Horowitz, established in 2009 by Marc Andreessen and Ben Horowitz, is a Silicon Valley-based venture capital firm. They primarily focus on investing in technology startups, with a diverse portfolio covering sectors like software, cryptocurrency, and biotechnology. The firm has $35 billion in total assets under management.

Bain Capital Crypto is a subsidiary of the global investment firm Bain Capital. Founded in 2021, it specializes in investing in cryptocurrency and blockchain-related ventures. The firm has a growing portfolio of investments, although the exact total investment amount may not be publicly disclosed.

Binance Labs and Binance Smart Chain. Binance Labs is an initiative of the cryptocurrency exchange Binance, launched in 2017. It focuses on nurturing and investing in blockchain and crypto-related startups. Binance Smart Chain is a blockchain platform that also supports various projects. Recently, Binance Labs has grown its assets up to $7.5 billion; both companies have collectively invested millions of dollars in blockchain and DeFi projects.

CoinFund, led by Jake Brukhman, is a blockchain-focused investment firm established in 2015. It invests in early-stage blockchain and cryptocurrency projects. In 2022, it launched a $320 million venture fund for early-stage web3 rounds. They have a diverse portfolio, spanning areas such as decentralized finance (DeFi), non-fungible tokens (NFTs), and blockchain infrastructure.

Distributed Global, established by Dominik Schiener, David Sønstebø, and Sergey Ivancheglo, is an investment firm that primarily focuses on blockchain and distributed ledger technologies. They have invested in various blockchain projects and startups, contributing significantly to the growth of the blockchain industry with $1.04 billion in assets under management and with a minimum investment of $1 million.

Future Fifty is a UK-based government-backed program that supports and promotes growth-stage technology companies. It provides a platform for high-growth businesses to connect with investors, mentors, and government resources, helping them scale and expand their operations.

LionTree is an independent investment and merchant banking firm specializing in technology, media, and telecommunications. Founded by Aryeh Bourkoff in 2012, LionTree has $1.6 billion in assets under management.

Lloyds Banking Group is a British financial services institution founded in 1995. It operates as a major retail and commercial bank, offering various banking and financial services, including retail and commercial banking, insurance, and wealth management. Lloyds is one of the largest banking groups in the United Kingdom; with £173 billion in AUM.

Orange DAO is a decentralized autonomous organization (DAO) that operates in the cryptocurrency and blockchain space. DAOs are blockchain-based entities with decentralized decision-making processes. Orange DAO focuses on fostering community-driven initiatives and projects in the crypto ecosystem.

Techstars, founded in 2006 by David Cohen, Brad Feld, and David Brown, Techstars is a global startup accelerator and investment company. Techstars nurtures and invests in early-stage companies in various industries, including technology, healthcare, and consumer products. They have invested in over 2,300 startups, including Uber, Twilio and Scopely, resulting in their portfolio worth is more than $185 billion.

Y Combinator, founded by Paul Graham, Jessica Livingston, Robert Morris, and Trevor Blackwell in 2005, is one of the most renowned startup accelerators and venture capital firms in the United States. Y Combinator provides early-stage funding, mentorship, and resources to startups, helping them grow and succeed in their respective industries. Many successful tech companies, including Dropbox and Airbnb, have emerged from its accelerator program.