WORLD ECONOMIC FORUM

Reimagining Digital ID

INSIGHT REPORT

JUNE 2023

Images: Getty Images, Midjourney

Contents

Executive summary 3

Introduction 4

1 ID Overview 5

1.1 A brief history of ID 6

1.2 Digital ID 6

1.3 Fulfilling the identity life cycle 8

2 Decentralized ID 9

2.1 Why is decentralized ID important? 10

2.2 Principles 13

2.3 Underlying standards and proposals 14

2.4 The Digital ID risks this approach seeks to avoid 17

3 Barriers to implementation 19

3.1 Technical 20

3.2 Policy 22

3.3 Governance and implementation 23

4 Recommendations 25

4.1 Technical 26

4.2 Policy 27

4.3 Governance and implementation 30

Conclusion 32

Contributors 33

Endnotes 36

Executive summary

There are roughly 850 million people who lack legal identification (ID), which makes it difficult or impossible for them to fully engage with society. At the same time, many of those with ID do not have privacy and control over how their data is shared.

Several approaches to digital ID could help broaden access to goods and services and offer individuals greater privacy and control. This report explores one such approach: decentralized ID, which enables users to control their personal data while allowing issuers to contribute attestations, or credentials, about them. If implemented in a trusted, privacy-preserving manner, decentralized ID can increase access and control while enhancing efficiency and effectiveness.

Yet decentralized ID also poses risks and faces challenges. To help realize the benefits and mitigate the risks of decentralized ID, this report provides analysis, tools and frameworks, summarizing the barriers to implementation facing decentralized ID and offering a set of recommendations for stakeholders seeking to adopt this approach.

1 ID overview

For centuries, ID – a means by which people prove attributes about themselves – has played a pivotal role in society. Recognizing this, the United Nations Sustainable Development Goals identify legal identity as a development priority. As people's lives become increasingly mediated by digital technologies, there is a related need to develop digital ID, or a way to make claims about personal data through digital channels. Centralized, federated and decentralized ID systems, as well as hybrid approaches, each with unique advantages and disadvantages, can help fulfil this need.

2 Decentralized ID

Decentralized ID systems use cryptography, digital wallets and related technologies to enable multiple entities to contribute credentials and empower individuals to manage their data. Properly implemented, decentralized ID could enhance privacy, control, efficiency and effectiveness. A wide variety of technologies, standards and proposals – including verifiable credentials and decentralized identifiers, as well as principles and governance frameworks – exist to realize decentralized ID. However, this approach also poses risks.

3 Barriers to implementation

Efforts are already under way to scale decentralized ID. Yet there are a host of barriers to implementation. A lack of widely agreed-upon technologies, standards and proposals limits the reach of these systems. The absence of enabling policy and regulation may curtail their efficacy. Decentralized ID also faces challenges of governance, communications and utility.

4 Recommendations

For stakeholders who decide that decentralized ID is the right approach for their goals, this report offers technical, policy, governance and implementation recommendations. It advises industry that further technological innovation, standards alignment and talent development are necessary to achieve decentralized ID. Public-sector participants can contribute by exploring the development of enabling regulation, setting requirements for interoperability and portability, and fostering collaboration among key stakeholders.

Introduction

For people without official, or legal, identification, it can be difficult or impossible to fully participate in society.

Roughly 850 million people worldwide lack an official ID, making it difficult for them to get a job, access medical care, enrol in a school, open a bank account or cast a vote.[1] At the same time, many of those with ID lack privacy and control over how their data is shared.

Today, innovative approaches to digital ID have been developed that could help expand access to goods and services while offering individuals privacy and control. This report focuses on one approach: decentralized ID, which seeks to enable users to control the sharing of their personal data while allowing multiple entities to contribute attestations, or credentials, about them. These credentials may be as simple as a date of birth or as complex as a citizenship. If implemented in a trusted, privacy-preserving manner, decentralized models of digital ID can offer individuals a secure way of managing their personal data without depending on intermediaries.

While decentralized ID presents opportunities, and has already begun to be adopted, it also poses risks and faces challenges. Many of its underlying technologies, governance frameworks, trust ecosystems and standards are still emerging and remain relatively untested at scale. As with many digital technologies, a misalignment between existing policies and regulatory frameworks and these models of ID could curtail their efficacy and create risks. Without public education, clear utility and incentives, decentralized approaches to ID may be unable to garner the broad stakeholder buy-in and user demand required for mass adoption.

Though decentralized ID offers an opportunity to advance inclusion, effectiveness and privacy, without fit-for-purpose policy, regulation and technology, the potential for these systems to address the limitations of current global ID paradigm while having a socially useful impact will be severely limited.

The aim of this report is to provide an analysis of decentralized ID from a technical and policy standpoint. The product of an international collaboration among experts drawn from industry, government, civil society and academia, the report seeks to offer useful tools, frameworks and recommendations for government officials, regulators and executives seeking to engage with this dynamic area of emerging technology.

Recognizing that the objectives of governments, organizations, communities and individuals differ across jurisdictions, use cases, cultures and more, this report does not provide a one-size-fits-all set of recommendations. Nor does it advocate using decentralized ID over other forms of digital ID – or the use of any form of ID. There are instances in which any form of ID is deemed unnecessary, inappropriate or undesirable.

Rather, this resource notes the advantages and disadvantages of decentralized ID compared to other approaches to ID and flags important considerations for stakeholders in the hope that this approach can aid their development of an effective ID strategy. Should a stakeholder choose to take this approach, the report provides tools to help realize its benefits and mitigate its risks.

1 ID Overview

For centuries, ID, a way for people to prove attributes about themselves, has played a central role in society.

This section provides an overview of important concepts pertaining to ID and digital ID. It offers a brief history of ID, an outline of different approaches to digital ID, and summarizes concepts including foundational and functional ID, the identity life cycle and levels of assurance.

1.1 A brief history of ID

The World Bank estimates that roughly 850 million people lack an official ID.

ID is a means by which people prove that they are who they say they are and various attributes about themselves. For centuries, ID has played a pivotal role in the development of economies and societies around the world,[2] with ID in many cases being required to cross borders, gain labour opportunities, access credit and more. In 1948, with the proclamation of the International Declaration of Human Rights, nations enshrined the right to recognition before the law and the right to have a nationality.[3] Both rights can be facilitated by the possession of proof of legal identity.[4] The United Nations defines legal identity as "[...]the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth".[5]

In 2015, with the adoption of the Sustainable Development Goals (SDGs), the international community recognized legal identity as a development priority. SDG 16.9 aims to "[...]by 2030, provide legal identity for all, including birth registration".[6] Indeed, as the World Bank posits, ID can be a direct or indirect enabler of many sustainable development goals (SDGs), including access to finance, gender equality and empowerment, and migration and labour market opportunities.[7]

While there has been significant progress, SDG 16.9 remains aspirational, with the World Bank estimating that roughly 850 million people lack an official ID. Providing proof of legal identity to those without it will depend on a concerted, multistakeholder effort led by governments as well as the development of robust systems to ensure that credentials provide real-world value to holders. As stakeholders determine how best to achieve SDG 16.9, some are considering developing decentralized ID systems in addition to efforts to provide proof of legal identity. Decentralized ID is a form of digital ID that enables individuals to control the sharing of their data, while allowing multiple entities to issue credentials to them.

1.2 Digital ID

Digital ID provides a means of making claims about personal data through digital channels. Many things can have a digital ID, from hardware such as internet of things (IoT) devices to organizations, including corporate entities. This report focuses on ID for individuals.

The increasing use of digital technology and the development of AI make the creation of digital ID important. According to estimates by the global financial crime watchdog, the Financial Action Task Force (FATF), the number of digital transactions is growing at roughly 12.7 % annually.[8] Whether purchasing an item or accessing an in-person service, transactions are increasingly mediated by digital technologies, necessitating the development of effective forms of digital ID.

Developments in artificial intelligence (AI) have also increased the need for digital ID. AI poses a threat to privacy because it can analyse seemingly unrelated data to reveal attributes about an individual.[9] AI also has the potential to break mechanisms for authentication. These capacities necessitate the development of models of digital ID capable of preserving privacy while providing reliable authentication.[10] AI systems are also now generating content, making it imperative to develop models of ID that can determine what was produced by an AI system.

Despite a sustained focus on ID, the increasingly widespread use of digital technologies, and the rapid development of AI, the internet lacks an ID layer.[11] To fill this gap, stakeholders offer centralized, federated and decentralized forms of ID to help facilitate transactions.[12] Centralized providers establish and manage data on behalf of individuals. Federated solutions allow a single organization or closed network to verify facts on behalf of an individual. Decentralized ID systems, by contrast, allow an individual to control their data, which is verified by other stakeholders.[13] Decentralized ID has elsewhere been referred to as self-sovereign ID, user-managed ID, secure ID and more. The aim of this resource is not to add confusion to these terms, but to encourage standardization around a neutral term.

The table below summarizes these system archetypes and some of their strengths and weaknesses. It should be noted that the

opportunities and challenges presented by each archetype are dependent on context and use case. Likewise, these archetypes are not necessarily mutually exclusive. Hybrid approaches making use of centralized and decentralized elements, for example, can offer a pathway for stakeholders to take advantage of some of the benefits of decentralized ID systems without fully adopting them.

TABLE 1 **ID system archetypes – strengths and weaknesses**

System archetypes	Centralized	Federated	Decentralized
Definition	– A single organization establishes and manages the ID	– Different stand-alone systems, each with its own trust anchor, establish trust with each other	– Multiple entities contribute to a decentralized digital ID; user controls sharing of personal data
Examples	– Government electoral roll, bank, social media platform	– Swedish BankID, Gov.UK Verify, Meta, Google	– VCI, International Air Transport Association (IATA) travel pass, Government of Bhutan National Digital Identity (NDI)
Strengths	– Can be built for specific purposes or for general application – Potential for organizational vetting of data – Potential to enhance features including account recovery – Technology is broadly understood and implementable	– Can enable users to access a wide range of services – Potential to enhance efficiency for organizations – Can be convenient for the individual, with potential for reuse – Can offer reduced risk for organizations	– Can increase user control, maintain privacy and reduce the amount of data stored by intermediaries – Potential to enhance efficiency – Can improve verifiability of data – Can enable data minimization at scale
Challenges	– May limit user control and create centralization risk, potential for surveillance and liability – May not be interoperable with other approaches – Individual may not be able to reuse information across platforms – May create data "honey pots" and require high data security standards to prevent data breaches – Can create over-disclosure	– May limit user control – May not be interoperable with other approaches – Individual may not be able to reuse information across platforms – May create data "honey pots" and require high data security standards to prevent data breaches – Can create over-disclosure – Can facilitate surveillance	– Governance can be complex – Acceptance of and alignment on underlying technologies and standards currently limited, potentially constraining interoperability – Evolving landscape of law and policy, creating complex liability – Can create data risks depending on ecosystem decisions – High technical complexity and high demand on individuals – Full benefit may require the possession of high-assurance credentials[14]

Source: World Economic Forum, Identity in a Digital World: A New Chapter in the Social Contract, September 2018: https://www3.weforum.org/docs/WEFINSIGHT_REPORT_Digital%20Identity.pdf

Each system archetype summarized in Table 1 can support forms of ID that are foundational or functional. The United States Agency for International Development (USAID) defines foundational ID as a national-scale official ID typically issued and managed by a government.[15] For example, leveraging an enrolment process to develop a registry of citizens, governments can create foundational IDs. Issuers, including governments, non-governmental organizations and private-sector enterprises, can also issue functional IDs, which are defined by their capacity to enable individuals to access a discrete good or service or perform a specific action. Driver's licences, health insurance documentation, credit and payment histories and passports are all instances of functional IDs.[16]

While a useful distinction, the boundary between foundational and functional IDs can be blurry. Over time, certain functional IDs, such as the US driver's licence, may accrue such a high level of trust and utility that they become de facto foundational.

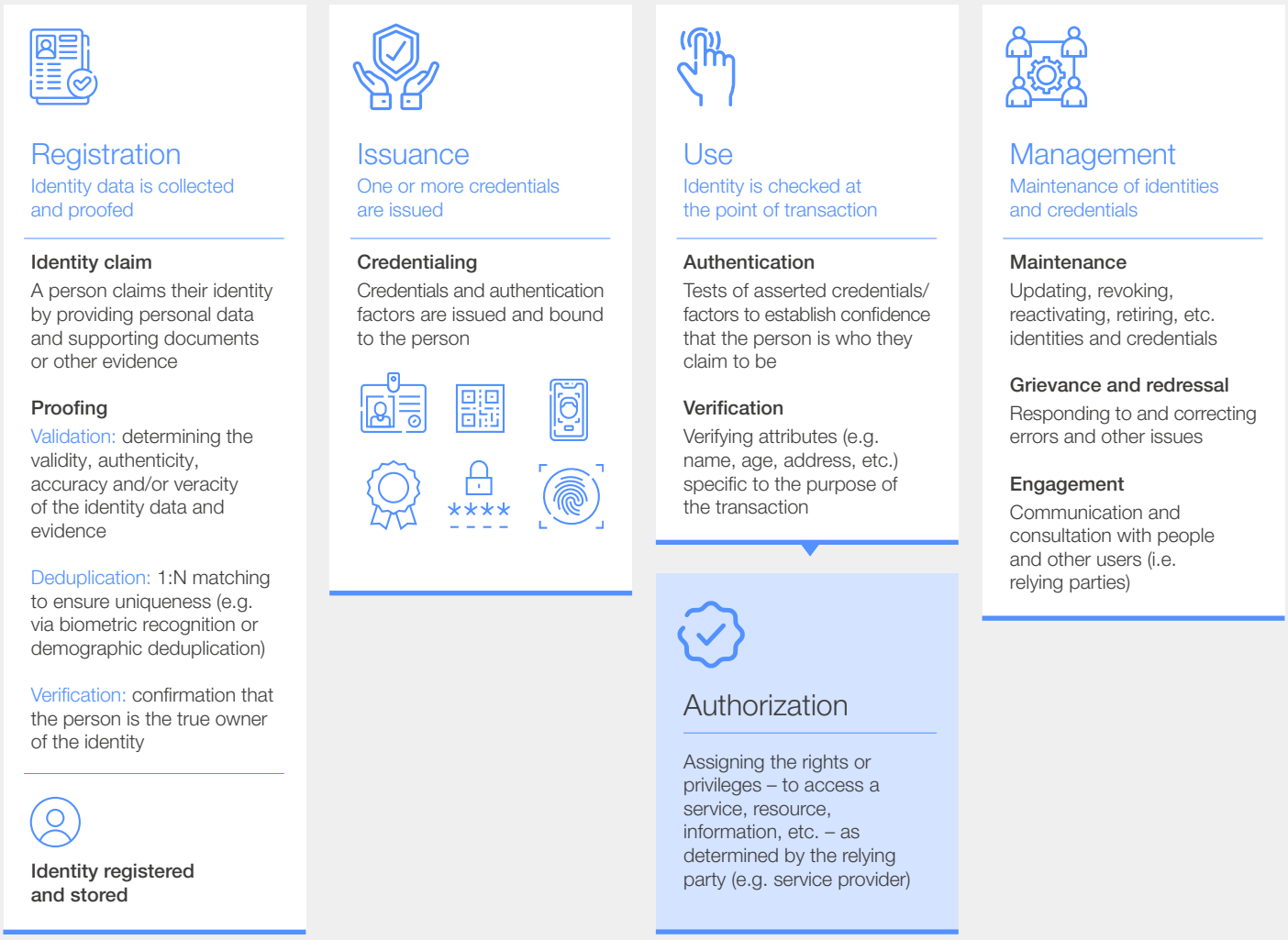
Both foundational and functional IDs can be used in a decentralized ID system. For instance, systems can enable individuals to control their foundational ID credentials, facilitating access to services in a decentralized fashion.[17] Likewise, decentralized ID systems can make use of government registries to provide individuals with official credentials while also allowing non-governmental stakeholders to issue other credentials to them.[18]

1.3 Fulfilling the identity life cycle

ID can be thought of as a process for fulfilling the identity life cycle, which according to the World Bank encompasses registration, issuance, use and management processes. In a government ID program, for example, during registration personal data is provided, validated for accuracy, deduplicated to ensure uniqueness, and verified to confirm that the data corresponds to the individual.

An individual can then be issued credentials, which may themselves be based on pre-existing documents, and use those credentials to access a good or service. When they do so, they are authenticated, verified and authorized. All of these processes are ongoing events subject to management – maintenance, redressal and engagement.[19]

FIGURE 1 **Identity life cycle**



Source: The World Bank ID4D, Practitioner's Guide: Identity Lifecycle: https://id4d.worldbank.org/guide/identity-lifecycle

Depending on how it is performed, each step in the identity life cycle is executed to a different level of assurance. Assurance levels correspond with the degree of confidence attributed to a given form of ID, as well as to the number of IDs created. Government-issued IDs can offer a high level of assurance depending on factors such as how well the government performed an identity-proofing procedure to establish uniqueness within a population.

In a risk-based authentication process, transactions are conditioned upon meeting or exceeding a certain level of assurance.[20] In general, the assurance level for a given transaction is the lowest assurance that has been achieved during the registration, issuance and use processes. As there can be a tendency to require overly high levels of assurance, setting assurance levels in line with the risks posed by a given use case is one approach stakeholders can take to minimize data collection.

2 Decentralized ID

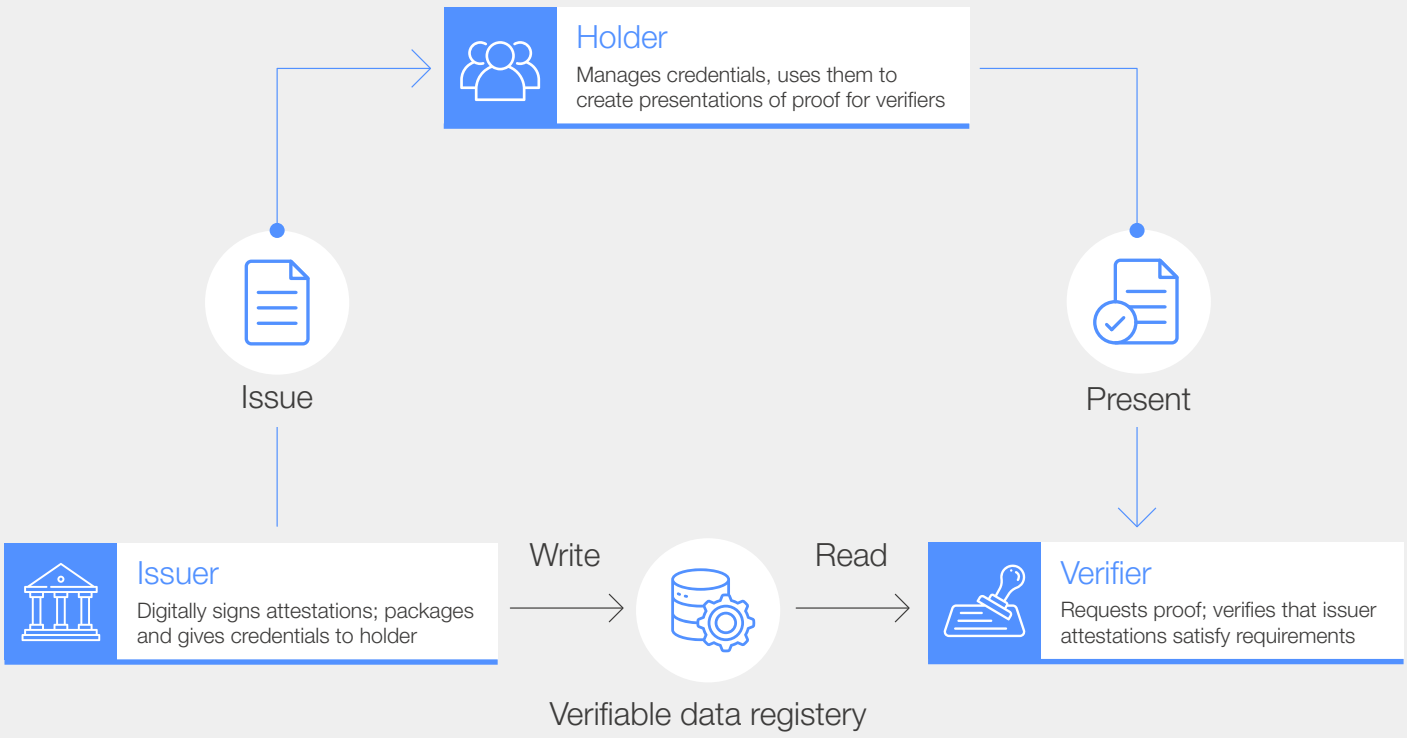
Decentralized ID could enhance individual privacy and control, while increasing efficiency and effectiveness.

As described in Section 1, there are several approaches to digital ID that could expand access and improve user outcomes relative to the status quo. This report explores one approach: decentralized ID. Section 2 provides an overview of this approach, situating it in the context of the wider ID landscape and articulating the opportunities it creates as well as the risks it poses, then offers a summary of some of the key principles, technologies, proposals and standards that support it.

2.1 Why is decentralized ID important?

Decentralized ID uses cryptography, digital wallets and related technologies to enable multiple entities to contribute credentials and empower individuals to manage their data. Decentralized ID systems create a trust triangle that links issuers, holders and verifiers: issuers are entities that digitally sign attestations and provide them to holders; holders, such as individuals, manage their credentials and use them to prove claims about their data; and verifiers assess these attestations to determine whether they satisfy requirements.[21] This process, which can be facilitated by a verifiable data registry, is discussed further in Section 2.4.

FIGURE 2 **Verifiable credential trust triangle**



Source: Alexis Hancock, Digital Identification Must Be Designed for Privacy and Equity, Electronic Frontier Foundation, 31 August 2020: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

Decentralized ID could offer a means of improving individual control and access while enhancing efficiency and effectiveness. Decentralized ID systems attempt to empower holders to manage their credentials, increasing their control. If a diverse, trusted system of issuers and verifiers exists, holders can use their credentials to access a host of goods and services. Decentralized ID may also increase efficiency. Instead of entrusting a third party to store, manage and transmit data on their behalf, individuals can use decentralized ID systems to exchange credentials directly with one another or a service provider, reducing the number of intermediaries and increasing efficiency.

Decentralized ID systems may also enhance effectiveness by reducing the number of times information has to be verified, which could increase convenience, reduce risk and diminish costs. Evolving use cases, such as education and skills credentials and public authority identity credentials, exemplify some of the benefits of decentralized ID (see Boxes 1 and 2).

BOX 1

Education and skills credentials

Decentralized ID offers a way for individuals to verifiably prove that they have attained a skills credential or received a degree or high-school diploma. Academic degrees and professional certificates can be issued on trusted, distributed, shared infrastructure that can enable individuals to prove facts about their personal data without compromising their pseudonymity.[22] These systems can enable distributed, inexpensive proofs that lower the risk of identity fraud and enable an individual to receive attestations from multiple entities.[23]

BOX 2

Public authority identity credentials

Public authority identity credentials offer a means for individuals to manage credentials from public-sector agencies without depending on a centralized intermediary. For example, by using a wallet and decentralized identifier (see Section 2.3) within the European Self-Sovereign Identity Framework (ESSIF), which is being implemented in collaboration with the European Commission, individuals can request credentials from public authorities that can then be used to attest to facts about their personal data in order to gain access to goods and services. Because ESSIF credentials are compliant with relevant public authorities, they can be used to facilitate access to services requiring high levels of assurance while still offering individuals control.[24]

Decentralized ID attempts to strike a balance between two paths: to protect individual privacy and control while facilitating compliant access to goods and services.

The benefits of decentralized ID may be best understood by contrasting this approach with the contemporary ID paradigm.[25] While there is no monolithic global ID regime, a collection of laws, policies and practices varying across jurisdictions, use cases and cultures underpin ID practices today. This report refers to this status quo broadly as the contemporary ID paradigm and draws examples of it from Web3, social media companies and financial services providers. In this section, it briefly summarizes the challenges created by this paradigm and considers how decentralized ID could address them.

To identify the opportunities created by decentralized ID, it is illustrative to consider the state of privacy in the blockchain-enabled ecosystem known as Web3 where, on the one hand, open, public protocols such as Bitcoin and Ethereum provide transparency, enabling anyone with sufficient expertise to access detailed information. On the other hand, protocols such as the virtual currency mixer Tornado Cash offer anonymity by aggregating several transactions to obfuscate their origins and destinations.[26] Decentralized ID attempts to strike a balance between these two paths: to protect individual privacy and control while facilitating compliant access to goods and services.

Just as decentralized ID provides a counterpoint to the poles of transparency and obscurity that characterize Web3, it also presents an alternative to the centralized and federated models of ID that dominate the internet. Today, platforms and corporations, such as social media companies, provide federated ID services. These services pervade the web. This centralization of power has precipitated what the Electronic Frontier Foundation and many others view as the rise of surveillance and data harvesting at the expense of institutional security and individual control.[27] As the scholar Shoshana Zuboff has argued, these practices may not only imperil privacy, but could also threaten the basic principles of democracy.[28]

The centralizing tendencies that suffuse the internet also permeate parts of the global economy. Although ID laws, regulations and processes vary across jurisdictions, organizations, use cases and more, many share an emphasis on intermediated compliance, where governments collaborate with industry actors to enforce policies.

For example, the US Bank Secrecy Act (BSA) and an expansive set of related laws mandate that financial institutions collect customer identity (ID) records and report crime to governmental agencies. Carrying out know your customer (KYC), anti-money laundering (AML), combating the financing of terrorism (CFT) and other due diligence processes requires financial intermediaries to collect and process personal data. As some have argued, regulations and guidance may have the effect of compelling financial services providers to compromise individual privacy by divulging personal information.[29]

While these centralizing systems play an important role in preventing crime and tax evasion, they may also have the effect of undermining individual privacy and access and creating insecurity and high costs. By contrast, decentralized ID aims to restore control of their data to individuals, while increasing access and security and lowering costs.

Privacy is important to individuals and governments, alike. A 2019 survey conducted by the digital communications corporation Cisco of 2,600 adults worldwide revealed that 32% of respondents said they care about privacy, are willing to act to enhance their control of information and have done so by switching companies or providers over data or data-sharing policies.[30] This consumer sentiment is mirrored by recent regulatory developments. The European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and more recent regulatory frameworks attempt to realize greater privacy and consumer protection for individuals.

According to the World Bank, as of 2021, 24% of adults around the world do not have an account at a bank or regulated institution.

Nonetheless, the current ID paradigm continues to centre on intermediated compliance, compelling organizations to collect, store and disclose personal data. Indeed, the current paradigm may even encourage organizations to over-collect personal information and in many cases duplicate the efforts of other stakeholders, resulting in a profusion of personal data in multiple places and creating cybersecurity risks. Decentralized ID could address these challenges by enabling individuals to securely manage and reuse credentials across use cases.

The contemporary ID paradigm also creates exclusion. According to the World Bank, as of 2021, 24% of adults around the world do not have an account at a bank or regulated institution.[31] According to the Financial Action Task Force (FATF), of these 1.7 billion unbanked adults worldwide, 26% cite lack of documentation as the primary barrier.[32] Policies can magnify this challenge by requiring ID, exacerbating exclusion in countries where adults lack an official ID.[33]

Addressing the ID gap will require extensive effort and collaboration on the part of governments, international organizations and other stakeholders to provide access to official ID. It may be possible to additionally use decentralized ID to help expand access while preserving privacy and control. For example, decentralized approaches to ID make possible the use of attestations from multiple parties, which when used over time may be able to accrue a high level of assurance. This model of layered credentials could present an opportunity to support government-led efforts to close the global ID gap.

Existing ID compliance regimes are also extremely costly. According to some estimates, the total cost of financial crime compliance across financial institutions worldwide was $274.1 billion in 2022, up from $213.9 billion in 2020.[34] This may be due in part to the tendency to use manual processes, over-collect personal data and redundantly perform due diligence checks.[35] Compliance costs also accrue to the public sector. Enforcement of due diligence and data protection rules, for example, can create high costs for government departments. Properly implemented and regulated decentralized ID could reduce costs stemming from compliance checks by enabling institutions to reuse high-assurance credentials to fulfil their obligations. Nonetheless, the efficacy of these processes will depend in large part on legal and regulatory considerations.

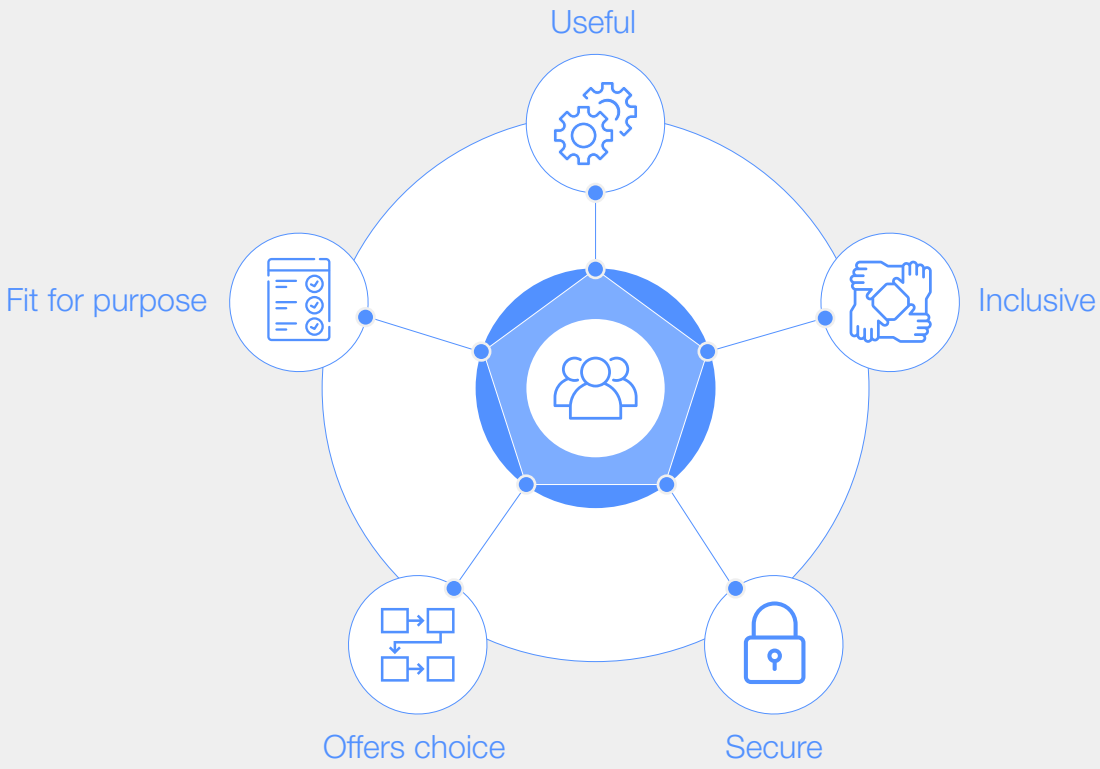
In contrast to the status quo, decentralized ID systems attempt to empower individuals while enhancing public- and private-sector efficiency and effectiveness. By enabling individuals to manage their information, decentralized ID systems enhance privacy, control and the ability to verifiably prove data. Decentralized ID systems can also reduce the amount of data shared by enabling individuals to share information in a more granular way. Rather than storing data with intermediaries, individuals can present credentials directly to service providers. Likewise, instead of repeatedly performing due diligence checks, actors can reuse credentials, which could diminish costs and reduce risks. Limiting the amount of data stored by centralized intermediaries could also reduce their liability and diminish their data-management responsibilities. Still, realizing these benefits requires not just technical innovation but also enabling policy and regulation. Section 4 provides an overview of the crucial steps needed to achieve this vision.

2.2 Principles

The objectives of those choosing to adopt decentralized ID systems, in whole or in part, will likely differ across jurisdictions, security systems, use cases, cultures and more. However, many implementations share a common set of principles. This section offers an overview of some of the essential principles underlying this approach.

This report is not proposing a new set of principles – rather, it emphasizes the values of privacy, security, inclusiveness, utility, appropriateness and choice, and asserts the importance of undergoing a principle-setting exercise to identify priorities and mitigate risks.[36] Resources such as the World Economic Forum's *Digital Identity Ecosystems: Unlocking New Value* may aid this process.[37] Likewise, mechanisms to certify compliance with principles can help stakeholders achieve their goals. ID2020 certification,[38] for example, provides a means of evaluating solutions against its technical requirements and principles, which are summarized below.

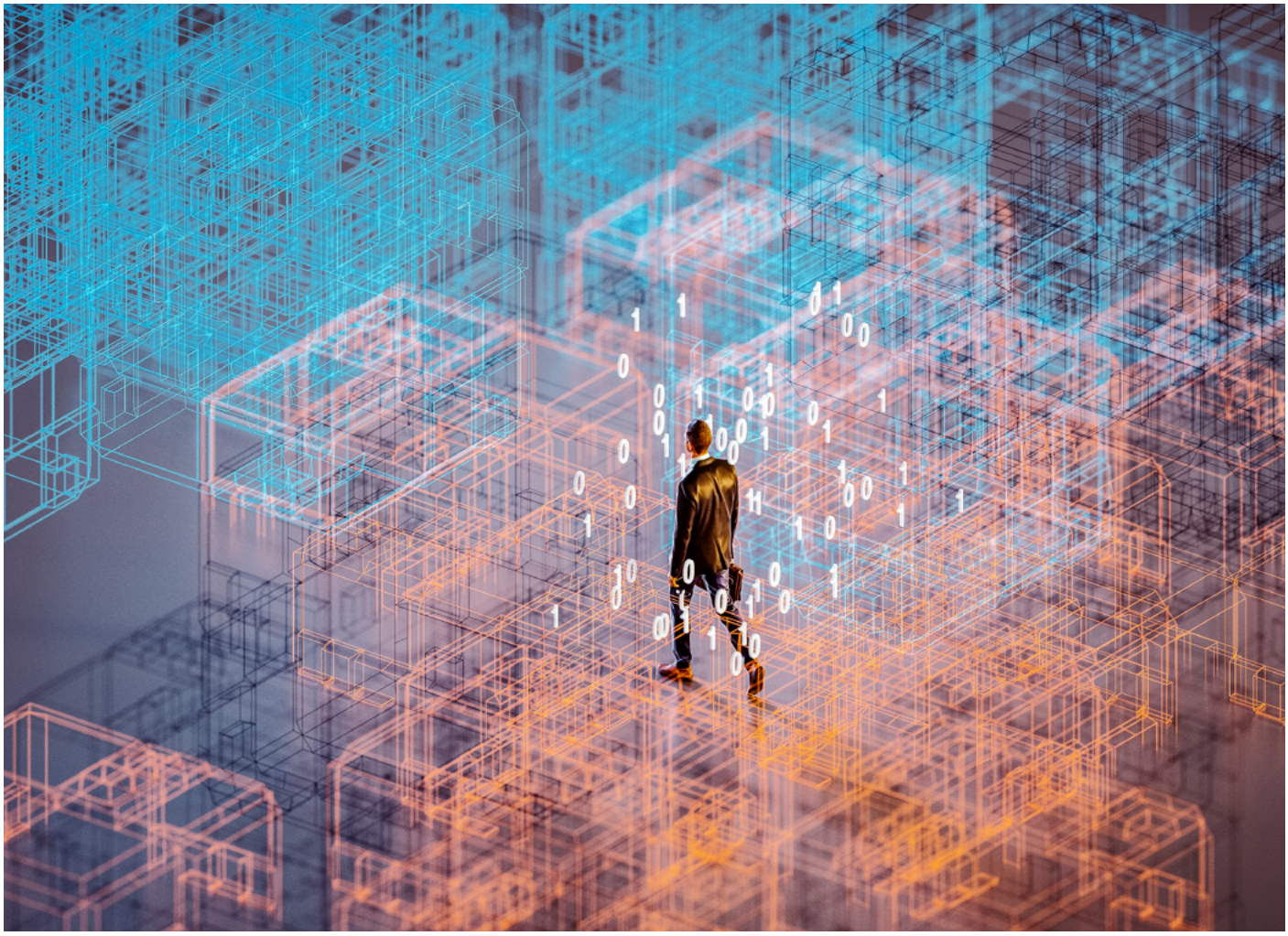
FIGURE 3 **Digital ID principles**



Source: World Economic Forum, Identity in a Digital World: A New Chapter in the Social Contract, September 2018: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

While there are differences among existing sets of principles, they generally converge on the importance of privacy, data minimization, user-centricity, choice, security and inclusiveness. For example, in the Laws of Identity[39] and Principles of SSI,[40] authors outline the importance of agency, consent and minimal disclosure. These principles align with those of the Omidyar Network, which prioritizes five features of ID to support individual empowerment and equity: privacy, inclusion, user value, user control and security.[41]

The World Bank's Identification for Development (ID4D) initiative advocates for 10 principles on identification for sustainable development under three pillars: inclusion, design and governance. ID4D calls for ensuring universal access, planning for financial and operational sustainability, establishing clear institutional mandates and accountability and more.[42] The ID2020 Alliance, a public-private partnership focused on improving lives through digital identity, offers a manifesto on digital ID along with a set of technical requirements detailing how to implement digital ID systems that adhere to its principles in practice.[43]



2.3 Underlying standards and proposals

Decentralized ID uses cryptography, digital wallets and related technologies to enable multiple entities to issue credentials, while empowering holders to manage their data. If implemented in a trusted, privacy-preserving manner, this could provide a means of enhancing control and access while improving efficiency and efficacy.

A variety of innovations underpin decentralized ID. For readers new to the topic, this section offers a brief overview of the standards and proposals that support this approach; for more technical readers, it also analyses their potential and limitations.

Verifiable credentials (VCs) are cryptographically secured digital credentials that aim to be tamper-proof, secure and verifiable. VCs enable issuers to make provable statements about subjects while making it possible for verifiers to assess the authorship of these statements without depending on intermediaries.[44] The VC data model was developed by the World Wide Web Consortium (W3C) to enable issuers to create credentials, holders to manage their credentials and verifiers to check that the holder's attestations meet basic requirements (see Figure 2).[45]

In this model, issuers create credentials by digitally signing attestations. Once received, verifiers retrieve the cryptographic public keys of the issuer to run cryptographic calculations on the proof of the cryptographic signature of the VC contained in the verifiable presentation. Issuers and holders are commonly identified in the VC by decentralized identifiers (DIDs), which provide a mechanism for cryptographic key resolution. A verifiable data registry may be used to enable DID resolution or the discovery of other data required in credential validation (for example, retrieving lists of trusted issuing authorities or checking the revocation status of the VC).

The W3C VC standard[46] defines only a common base data model for VCs; it does not define how to issue, exchange or prove ownership of a VC. Nor does it define the protocols that connect issuers, holders and verifiers. Issuers are expected to extend the W3C base data model to support their own use cases. The W3C Credentials Community Group (CCG), Decentralized Identity Foundation (DIF), OpenID Foundation (OIDF) and Hyperledger Aries have been working to develop the missing protocol layers among the different roles – a crucial step towards interoperability.[47]

> Without a well-designed and implemented privacy strategy, VCs can be over-requested by parties, which could contribute to data exploitation.

The W3C CCG supported the development of the Verifiable Credential API to enable large institutions that already have established business processes to use this API as the issuance and presentation protocol for VCs among the different roles.[48]

The OpenID Foundation (OIDF) defined **OAuth2** and **OpenID** protocol extensions for the issuance and presentation of VCs. These extensions are also known as **OpenID for Verifiable Credentials** (OpenID4VC).[49] While OAuth2 and OpenID are often associated with centralized ID providers, OpenID4VC can be implemented in a fully decentralized fashion.[50] The Architecture Reference Framework (ARF) that was proposed as a technical framework for the implementation of the proposed electronic identification and trust services (eIDAS) 2.0 regulation in Europe requires the OpenID4VC specifications for online use cases.[51]

Although VCs are fairly mature compared to related innovations, they still have their limitations. For example, a VC approach does not, in and of itself, guarantee interoperability and data portability. However, semantic interoperability[52] may be achieved through JavaScript Object Notation for Linked Data (JSON-LD) data representation within VCs as a way of supporting data legibility across contexts. For example, using the Credential Transparency Description Language (CTDL) hosted by Credential Engine, higher education institutions are working to develop a vocabulary for all credentials across US higher education. Nonetheless, JSON-LD signature suites remain novel compared to more mature standards. Some have also criticized the VC model for lacking an adequate incentive model to achieve scale (see Section 3.1). Moreover, without a well-designed and implemented privacy strategy, VCs can be over-requested by parties, which could contribute to data exploitation (see Section 2.4) and may fail to comply with regulatory requirements.[53] Issuers can, for instance, hold data on the credentials they issue while verifiers tend to store data due to business and regulatory requirements. VC-based approaches may also encounter challenges in low- and no-connectivity environments, although there are efforts to develop workarounds for such contexts.

The W3C's **decentralized identifiers** (DIDs) standard defines a minimum viable mechanism for creating, reading, updating and deleting identifiers that enable cryptographic verification. DIDs are strings, like URLs, that resolve to DID documents. While VCs are stored with an individual or organization, DID documents can be stored on a blockchain, in a DNS record, at a web address or generated from the DID itself. DID documents can also be stored on non-blockchain verifiable data registries such as decentralized databases. DID documents typically contain information about public cryptographic key material that can be used to authenticate the controller of that DID.

VCs and DIDs may be used together. DIDs may be used to identify and authenticate the issuer and the holder of a VC. One DID can be associated with multiple VCs. DIDs are created and optionally registered on a verifiable data registry such as a blockchain, and represent an entity, such as an organization or an individual. VCs contain data written about that user, and can be stored locally or in an encrypted cloud database that the user's keys control.

When combined with VCs, DIDs attempt to offer a means of fulfilling the identity life cycle. VCs allow for flexible signature suites, including options enabling selective disclosure, or the ability to share information granularly. In paper-based ID systems, an individual may be required to overshare by default. For example, when attempting to gain access to an age-gated service such as a bar, individuals may use an ID card that contains more information than a binary yes/no attesting to whether they are of age. Selective disclosure enables an individual to demonstrate only the minimally necessary amount of information to gain access to a service.[54] While selective disclosure is not an inherent capability of the VCs and DIDs approach, when used in combination with zero-knowledge proofs and novel signature schemes such as SD-JWT BBS+, this feature can be achieved.[55] However, techniques for realizing selective disclosure are still evolving and may fail to pass regulatory barriers.[56]

A ZKP allows one party to convince another party that a certain statement is true, without revealing the underlying data that proves the statement is true.

The trust model supporting the **mobile driver's licence** (mDL) standard (ISO 18013-5) is based on X.509 certificates and uses a public key infrastructure (PKI) provided by each issuing authority. The credentials are secured using conventional cryptography and support selective disclosure of individual claims from the mDL. Stakeholders are taking steps to clarify the benefits and drawbacks of mDL compared to VCs.[57]

Recently, stakeholders have begun to define a new standard series (ISO/IEC 23220) to normalize building blocks for identity management via mobile devices that will reuse the mobile identity document credential format and protocols from the ISO 18013-5 standard.[58]

ISO 18013-5 offers an optional feature to enable a verifier to request data from an issuer via an online protocol. This feature allows parties to access fresh data, but, if used, it may compromise user privacy. Nonetheless, it is optional and discouraged by certain jurisdictions because it can lead to data tracking. Regular updates to the mDL guidelines are published that do not recommend using this protocol. Ultimately, it is up to issuers and wallet vendors to decide whether to support this feature.

Zero-knowledge proofs (ZKPs) have been proposed as offering a way to enable private transactions. A ZKP allows one party to convince another party that a certain statement is true, without revealing the underlying data that proves the statement is true. For example, an individual could demonstrate that they are eligible to receive a discount, such as a senior citizen discount, without demonstrating anything else about their identity, including their exact age. In this case, they would prove in zero knowledge that they are of requisite age.[59] The European Parliament has noted the potential value of ZKPs to complete processes without identifying an individual.[60]

However, as some have noted, ZKPs remain relatively immature. Their underlying standards are still evolving, and it may take years for the cryptography underlying ZKPs to be documented and standardized. Their deployment may create security risks in implementations at scale.[61] New control mechanisms will also likely need to be developed for use in regulatory contexts, or depending on the risk profile of a given application.[62]

Soulbound tokens (SBTs) are a proposal for enabling non-transferrable cryptoassets that represent commitments, credentials and affiliations. SBTs were proposed by E. Glen Weyl, Puja Ohlhaver and Ethereum co-founder Vitalik Buterin to address limitations in Web3.[63] Internet-native, community-governed decentralized autonomous organizations (DAOs), for example, face ID challenges in voting processes.[64] Likewise, a lack of verifiable ID can create platform dependency; some non-fungible token (NFT) artists, for instance, are reliant on platforms such as OpenSea and Twitter to prove provenance. SBTs attempt to solve these problems by providing a crypto-native way of proving facts about oneself.

SBTs are receiving attention in part because they can be readily adapted. SBTs are natively readable by smart contracts, or automatically executing promissory code, which means they can be used to automatically enable or disable access to goods and services. SBTs provide a means of offering crypto-native credentials. By contrast, VCs currently lack native Web3 wallet support as there is no equivalent widely adopted standard that allows VCs to be instantly recognizable and usable in a Web3 context. On a related point, some organizations are developing approaches that bind VCs with tokens in such a way that tokens are bound to an identity owner, a form of ID-bound NFTs.[65]

> Given the immutable nature of cryptoassets, SBTs may not be changeable or revokable. Moreover, as with many cryptoassets, SBTs face an uncertain regulatory landscape.

Through the issuance of publicly visible, non-transferable SBTs, individuals could prove ownership over assets and, over time, develop a rich array of verifiable personal data, from affiliations to memberships. Individuals who meet certain criteria are eligible to mint SBTs to their wallets, and the ownership of that SBT can be used to unlock certain privileges – for example, access to gated online community spaces.

SBTs face a host of challenges. By design, SBTs are public, meaning that the information contained in an SBT is conveyed to all, which could limit the use of privacy-enhancing features such as selective disclosure. There are considerable privacy and data-protection challenges with storing anything on-chain. This is especially alarming in the context of sensitive personal data. Given the immutable nature of cryptoassets, SBTs may not be changeable or revokable. Moreover, as with many cryptoassets, SBTs face an uncertain regulatory landscape.

Another concern with SBTs is lack of consent from the user. The issuing of smart contracts can be programmed to mint the token to a receiving address, but the recipient must receive the token and any data attached to it. Many proponents of SBTs argue that this is a feature, not a bug, yet this may come into conflict with privacy and user control. Nevertheless, stakeholders are developing proposals to address this challenge.

2.4 The Digital ID risks this approach seeks to avoid

Just as decentralized ID has the potential to address the shortcomings of the current ID paradigm, increasing efficiency and privacy while expanding access, it also poses significant risks. This section offers an overview of some of the risks created by digital ID, generally, that decentralized ID systems seek to avoid. It identifies when decentralized ID systems share the same risks and when they may offer a way to mitigate them.

It is worth noting that many of the risks discussed below also apply to analogue, or paper-based, forms of ID. While decentralized ID may mitigate some of these, requiring any form of ID risks exacerbating fundamental social, political and economic challenges as conditional access of any kind always creates the possibility of discrimination and exclusion.[66]

That is why, in some cases, providers may choose to avoid the use of ID altogether. Certain humanitarian organizations, for instance, may opt to provide services to beneficiaries irrespective of their possession of an appropriate ID. As Access Now's #WhyID campaign advocates, governments, organizations and other stakeholders engaging with any approach to ID should carefully weigh the costs and benefits of implementing any approach to ID.[67] Nonetheless, the use of ID is in many cases required by law. The tension between the opportunities and risks created by decentralized ID is further explored in Section 3.

Political risks

The Trust Over IP Foundation, an initiative focused on advancing internet digital trust hosted by the Linux Foundation, has recently released a paper warning that, in some cases, digital ID may weaken democracy and civil society.[68] For example, digital IDs issued by social media companies can contribute to political polarization by reinforcing group identities. While decentralized ID offers a way for individuals to exercise greater control over their personal data, depending on its use context, it could still contribute to polarization.

Data exploitation

Certain forms of digital ID risk opening the door to data exploitation. If credentials are stored centrally, or accessible by organizations seeking to commodify data, then creating expansive digital ID ecosystems could increase the risk that personal data becomes marketized.[69] Sensitive data, such as biometrics, carry a high risk of exploitation. For instance, biometrics can be exploited through "man-in-the-middle" attacks, where attackers gain access to biometric data that they can in turn use to access an individual's financial resources. This is especially concerning in the case of marginalized communities such as refugees because it can facilitate discriminatory targeting.[70] Generally, the best policy when it comes to highly sensitive data such as ethnic affiliation is to not collect it at all because these are likely vectors for marginalization or oppression.

Decentralized ID aims to mitigate this risk by enabling individuals to store their data themselves or in a way that provides greater user control, preventing organizations from accessing their information without consent. A crucial aim of decentralized ID, but one that is difficult to achieve, is to create accessible, easy-to-use tools that enable anyone to exercise control over their information. However, if individuals use third-party intermediaries to help manage their data, the risk of data exploitation could return.

Much of this risk stems from linkability. If a party can link data across domains through the use of a common identifier, then individuals may be tracked by parties seeking to exploit their data. This challenge stems from the use of the same identifier, or from data being stored in the same location. Implementation choices, including how wallets manage decentralized identifiers (see Section 2.3), can enable decentralized ID systems to minimize these risks. Decentralized ID systems are not a panacea for the risk of data exploitation, but, through careful choices, they can help mitigate it.

Technical risks

Digital ID also creates technical risks. Even if data collection is minimized, digital ID systems still give rise to the possibility of data leakage or theft. These risks can be compounded by digital technologies. A stolen digital credential can be used to rapidly access services against the wishes of the holder. Likewise, issuers of credentials may not be able to maintain the identity life cycle, which could weaken the trustworthiness of the credential.

Although decentralized ID aims to minimize data collection and data storage, it still risks increasing the collection of sensitive personal data, opening the possibility of theft or leakage. Moreover, decentralized ID systems have technical risks and limitations of their own, as discussed in detail in Section 2.3.

Risks of exclusion, marginalization and oppression

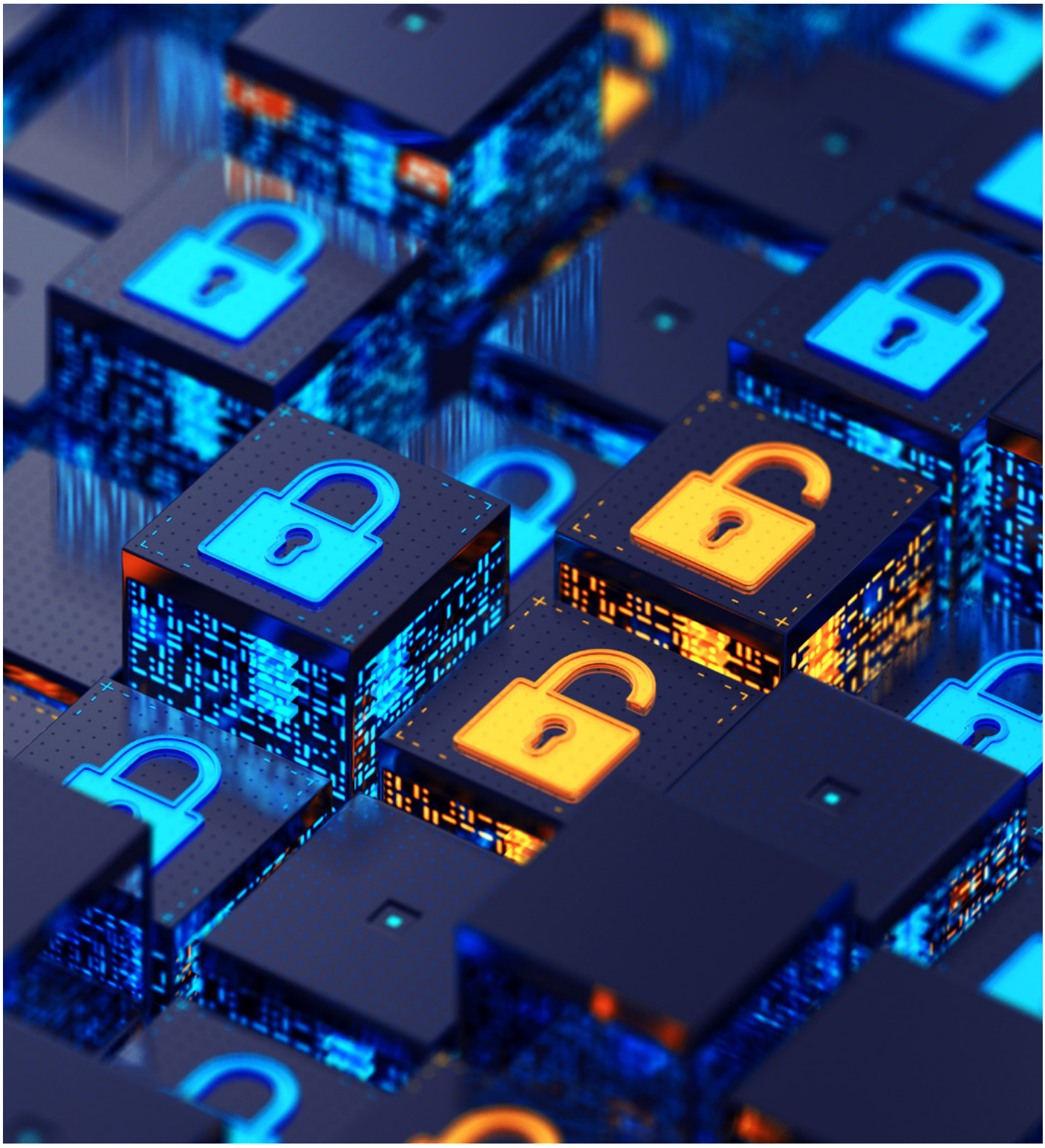
Perhaps the greatest risks arising from digital ID are exclusion, marginalization and oppression. As Privacy International has argued, the potential social risks of digital ID are great; it could enable discrimination and exclusion and magnify existing forms of discrimination, exclusion and inequality.[71] These challenges are not limited to low- and middle-income countries, but are prevalent across many jurisdictions. Indeed, about 21 million Americans do not possess official ID.[72] Several reports have identified a link between a lack of official ID and exclusion from full participation in society. Yet by reifying conditional access, ID is, by its very nature, exclusionary. It is often members of historically marginalized groups who face the harshest forms of exclusion.[73] The majority of digitally excluded individuals worldwide are women.[74] In cases where sensitive data is collected, there are also risks of marginalization and oppression, with ID being used to facilitate the identification, surveillance and persecution of individuals or groups.[75]

Moreover, even if a programme is designed with inclusion as an explicit goal or requirement, implementations may encounter challenges of coerced consent stemming from power imbalances. Indeed, mandating inclusion does not necessarily address the risk of bad actors using data maliciously. As an ID system expands, the consequences of not participating in it can become so severe as to make registration effectively unavoidable.[76] When access to a good or service is conditioned upon the possession of a form of ID, and that ID is widespread, individuals may be effectively coerced into obtaining that form of identification, even if there is no legal basis for requiring it. Likewise, for populations lacking digital literacy, it may be impossible to obtain meaningful informed consent. As Section 4 explores further, stakeholders must critically examine the benefits and risks of an ID system and act accordingly.

Although possible features of decentralized ID such as selective disclosure may offer individuals more opportunities to reduce information-sharing, broader social, economic and political considerations may make non-registration effectively impossible. While many of the above risks are a product of sociopolitical dynamics, some can be mitigated by technology, policy and governance. Section 4 provides recommendations on how to do this.

3 Barriers to implementation

Efforts are already being made to scale decentralized ID. The European Digital Identity initiative, for example, will offer a personal digital wallet for EU citizens, residents and businesses to gain access to public and private EU services.



The principles of the European Digital Identity align with the vision of decentralized ID, and its adoption could provide access to this model for hundreds of millions of EU citizens.[77] Similar efforts are ongoing in other regions across the globe.

Yet despite the many years of work by government, industry, civil society and academia to address the problems with the current ID paradigm, alternative approaches to ID have yet to achieve mass adoption. To understand how to address the shortcomings of the current ID paradigm, it is useful to explore why decentralized ID, one approach to potentially enhancing privacy, access and effectiveness, has not yet been widely adopted.

This section offers an overview of some of the major possible reasons why decentralized ID has not yet been widely adopted. The causes can be divided into technical, policy, and governance and implementation challenges. Where helpful, case studies are provided to ground the analysis in practice. These case studies span centralized and decentralized systems and are intended to illustrate the points being made.

Section 4 provides a set of recommendations for how to implement and scale decentralized ID by addressing these challenges.

3.1 Technical

Switching to a decentralized model can require high upfront development costs and even in some cases necessitate the overhaul of legacy systems.

A variety of technical challenges are slowing the development of these systems. This section focuses on technical immaturity and a lack of standards alignment, fit-for-purpose user-experience design and more.

Perhaps most critically many of the underpinning technologies (outlined in Section 2.3) remain relatively immature. The underlying standards and proposals remain subject to redesign and redevelopment, which can necessitate changing protocols and sometimes even entire solutions. For example, developers are still experimenting with ZKPs to make features such as revocation, recovery and back-ups practicable.[78]

The quickly evolving nature of these technologies can make some organizations hesitant to engage with decentralized ID. Because models of decentralized ID necessitate a paradigm shift with respect to how data is verified, recorded, stored and released, switching to a decentralized model can require high upfront development costs and even in some cases necessitate the overhaul of legacy systems. While a hybrid approach, where providers gradually shift from centralized to decentralized, or use decentralized components, may be possible, these strategies are still likely to face technical challenges.

For example, the VC data model and key technical standards underpinning decentralized ID continue to undergo revisions. The W3C VC Data Model v1.0 was approved in September 2019 and subsequently updated to v1.1, released in March 2022. However, the W3C Verifiable Credentials Working Group was reconvened in September 2022, and a V2.0 standard is expected in September 2024. Even if robust standards do exist, stakeholders may not be aligned on their approach.

Challenges of standardization can create obstacles to achieving interoperability, or the capacity of systems to exchange information. Without interoperability, digital ID systems risk creating vendor lock-in, effectively forcing individuals to use a single provider or set of providers due to the high costs of switching to a new vendor. Without the ability to port data from system to system, decentralized ID implementations cannot achieve their vision of user-centricity.

Many decentralized approaches also lack effective user-interface and user-experience design. The difficulties of managing cryptography-based assets using present-day technology are well documented.[79] Developing similar systems for the management of ID credentials could result in many of the same challenges. Some of these challenges stem from a lack of technical development. For instance, user account key changes and recovery continue to be areas requiring fit-for-purpose technical solutions. Others require the attention of designers, users and other stakeholders.[80] Still, even if these technologies become easier to use, their scale will depend in part on user education and the extent to which individuals are able to develop the skills necessary to manage wallets and private keys.

BOX 3 | IATA Travel Pass

IATA Travel Pass was a decentralized ID system designed to enable airlines, governments and others to verify credentials while preserving the privacy and security of personal data. It was devised in 2020 by the International Air Transport Association (IATA), a trade association representing roughly 300 airlines in 120 countries carrying 83% of the world's air traffic. Travel Pass, a response to the COVID-19 pandemic, used a decentralized credential exchange platform developed by decentralized digital identity company Evernym (now part of Gen Digital [Norton/Avast]) to enable users to control their data while gaining access to services.[81]

The Travel Pass app, now decommissioned and absorbed into IATA's OneID initiative, was created to help citizens, airlines and governments facilitate a safe return to travel during the pandemic. The International Civil Aviation Organization (ICAO) estimates that the COVID-19 pandemic resulted in the loss of roughly $372 billion gross passenger operating revenues for airlines in 2020 alone, as compared with 2019 levels.[82] By providing credentials attesting to the veracity of claims of an individual's COVID-19 status, Travel Pass aimed to help airlines access information on individuals without compromising individual privacy.

Rather than use analogue documents, Travel Pass provided VCs to facilitate airline processes. Likewise, Travel Pass used a decentralized approach to data storage, where personal data was stored by individuals on their local device. Individuals controlled access to their data, with no information stored in a central database.[83]

Travel Pass implemented privacy-enhancing techniques through the use of VCs and DIDs. With Travel Pass, a test lab issued a credential to an individual's local device. With a new identifier generated for each interaction, every relationship was unique, decreasing the chance of reidentification through correlation.

With the COVID-19 pandemic dramatically reducing air travel, a moment of crisis created the opportunity to implement Travel Pass as the losses accruing to the travel industry galvanized an effort to create a safe return to travel. Initiatives such as the Good Health Pass Collaborative offered a forum for creating cross-sectoral collaborations to this end.[84]

Nevertheless, Travel Pass encountered user-experience and system-development challenges. Its design was not user-friendly, which made it difficult for some users to take advantage of its privacy-preserving benefits. Travel Pass also faced business limitations that made it difficult to scale.

As countries and airlines recovered from the impacts of COVID-19, the Travel Pass project was retired. The learnings and feedback from this new credentials-based approach to digital ID have been transferred to other parts of IATA, including the New Distribution Capability (NDC)[85] and OneID[86] programmes. Further work on travel standards and passenger experiences using verifiable credentials continues.

Some decentralized ID systems may also confront infrastructure limitations. Although only some decentralized ID systems use distributed ledger technology (DLT), those that do may face issues of technical scalability. As has been well explored, due to its computation-intensive nature, blockchains that use certain consensus mechanisms, such as the proof-of-work-driven Bitcoin blockchain, may face scaling challenges.[87] Likewise, blockchains using alternative consensus mechanisms may risk centralization. Nonetheless, a wide variety of efforts are under way to try to address the scaling challenges faced by blockchains.[88]

Certain supporting technologies, proposals and standards for decentralized ID may also encounter their own privacy challenges. VCs, for example, if over-requested by many parties, could contribute to data exploitation and may encounter regulatory challenges.[89] If issuers decide to hold data about the credentials they issue and verifiers store data to fulfil business and regulatory requirements, data can become partially centralized, which risks recreating some of the challenges of the contemporary ID paradigm.

Likewise, decentralized ID is also adversely affected by proprietary technologies and centralizing practices. The widespread use of federated ID systems managed by large, centralized organizations using proprietary technologies can engender practices of control that favour the status quo, reinforcing the current ID paradigm. This can have the effect of creating vendor lock-in, limiting individual choice and habituating users to legacy approaches to ID.

3.2 Policy

There are also policy challenges to the development of decentralized ID; this section offers a summary of these, including a lack of high-assurance official ID and enabling policies. Policy objectives vary by jurisdiction; when presenting a policy challenge limited to a specific jurisdiction, the report notes it as such. This section also provides examples of government-led ID programmes and an overview of resources offering guidance for addressing these limitations.

One reason why policy can limit the utility of this approach is that certain jurisdictions may not be committed to providing high-assurance official ID. Roughly 21 million Americans, for instance, do not possess official ID.[90] Those who do have a form of ID are often dependent on functional IDs, such as driver's licences and passports, to vote, cross borders, open bank accounts and more. Many of these functional IDs lack high-assurance verifiability, increasing the possibility of identity fraud and exclusion and limiting utility.

Although decentralized ID is inherently multistakeholder, governments are likely to play an important role in ID ecosystems, given their ability to provide official ID for identity binding, which is the process by which a holder and a credential are linked. While users may benefit from decentralized ID without an official ID, its utility may be curtailed.

BOX 4

Government of Kazakhstan GovTech

As part of its GovTech Pyramid, which consists of infrastructure, data, business processes, identification and service layers, the Government of Kazakhstan reports that it has transferred 90% of its public services online while providing access for citizens through a centralized ID system. Via their digital ID, people can perform functions such as registering for e-government services and obtaining digital signatures and services. Through an easy-to-use app, they can obtain digital documents to access services – for example, they can submit an electronic application for marriage registration. Registration certificates are issued and revoked by the relevant ministry.

In some cases, lawmakers may face challenges when creating regulatory frameworks that support the use of this approach to ID. For example, in the US, an absence of sufficiently enabling policy effectively discourages leveraging reusable credentials to fulfil know-your-customer processes.[91] More broadly, existing regulations that are premised upon the existence of an intermediated compliance regime could obviate many of the benefits of decentralization.[92]

BOX 5 | **Opportunities and Challenges of New Technologies for AML/CFT**

The Financial Action Task Force (FATF), an intergovernmental organization focused on developing policies to combat money laundering, has produced guidance on digital ID policies, providing recommendations for virtual asset service providers and other stakeholders to help them implement new technologies in pursuit of effective AML/CFT measures in their operations.

The FATF argues that properly implemented digital ID can enhance the efficiency, accessibility and security of financial transactions. It identifies money laundering, terrorist financing and other forms of financial crime as risks. To combat these risks, FATF recommends that digital ID be accompanied by the development of robust, fit-for-purpose AML/CFT regulations. FATF recommends that government and industry keep pace with technological change by encouraging stakeholder engagement, implementing uniform regulations where possible, developing technical and cybersecurity expertise to improve data management, and attempting to educate and raise awareness of the potential of these technologies.

A lack of political will may also be an obstacle to achieving decentralized ID. Without a mandate to foster innovation, stakeholders may not be sufficiently incentivized to take the steps necessary to achieve enhanced user privacy and security. Without action from policy-makers to provide incentives for the development of privacy-enhancing technologies, such systems may not be realized. Existing regulations such as the EU's GDPR and proposed regulations such as the American Data Protection and Privacy Act (ADPPA) attempt to help fill this gap. While these privacy regulations are not directly related to digital ID, developing privacy-preserving models of ID could help fulfil their goals. There remains a need for policy to help realize the principles articulated in section 2.2. To this end, Section 4 offers several recommendations for policy-makers.

BOX 6 | **Louisiana Wallet**

Louisiana Wallet, an implementation of the mDL standard, was released in 2018 as a multi-credential digital identity wallet. Upon its initial release, some residents did not find the wallet useful, though later usage rates were significantly higher.

At release, Louisiana Wallet encountered difficulties due to a lack of enabling policy, utility and app errors. Initially, the mobile driver's licence contained in the app was only legally required to be accepted in interactions with law enforcement. As of 2021, many retail establishments and restaurants still did not accept the app as a form of identity/age verification, even though the state had since passed legal requirements to do so.[93] Many of these establishments cited a lack of enforcement penalties, combined with the technical difficulty of retaining identity and age verification logs for compliance purposes, as the main reason why they continued to refuse the app for verification even after being required to do so by law. Moreover, the app continues to have technical errors.[94]

There has been an improvement in enforcement since 2021, and many technical issues have been addressed since release. Some Louisiana residents have found the multi-credential digital ID wallet useful. Now, in addition to driver's licences, it can hold hunting and fishing licences and has been downloaded on roughly 1.5 million Louisiana residents' smartphones.[95]

3.3 Governance and implementation

There are several reasons in addition to technology and policy why it remains difficult to realize decentralized ID. This section offers an overview of the governance and implementation barriers, which include communications, utility, economic viability and exclusion-related obstacles. It also provides examples spanning centralized and decentralized ID, where helpful, to further illustrate the analysis.

Broadly, decentralized ID systems face a communications challenge. Explaining the benefits of any novel technology can be difficult; this is especially true for a solution such as decentralized ID that combines several technologies. Yet in the case of ID, there is an especially high communications barrier, made worse by the myriad conspiracy theories linking digital ID to untrue and malicious speculations.[96] Moreover, although many institutions and individuals continue to push for enhanced privacy, many may not recognize the relationship between digital ID and personal data and how developing decentralized ID systems could help improve individual privacy. Additionally, while individuals may in theory want greater privacy, convenient technologies that offer less privacy may be more appealing to them in practice. A lack

“ Fully addressing the challenge of exclusion requires grappling with the digital divide and developing systems that can function in low- and no-connectivity environments.

of recognition of the importance of digital ID can create a lack of user demand, stymieing efforts to scale decentralized ID.

The communications challenge stems in part from a lack of clear utility. While ID underpins many critical social, economic and political activities, it is fundamentally a means to an end; developing a compelling case for any form of digital ID requires demonstrating clear utility to important stakeholders including governments, organizations, communities and individuals. Without an understanding of how ID will help achieve tangible goals, implementers will likely continue to face challenges.

Decentralized ID stakeholders also face the challenge of developing effective business models. Without a viable set of incentives, networks of issuers and verifiers may not be able to scale. Some stakeholders believe that ID ought to be a public good. Scaling decentralized ID, they argue, requires public-sector investment in ID.[97] For example, some nations are beginning to understand digital ID as a prerequisite to developing a central bank digital currency (CBDC) and other payment innovations. If approached as a digital public good, with governments shouldering the burden of cost, decentralized ID may be able to achieve scale without an effective business model. For those who believe that these systems require a viable commercial model to succeed, a prevalence of closed-loop applications and a lack of open ecosystems create challenges.

It can also be difficult for participants to align on a trust or governance framework for implementation. Governance frameworks provide tools for decision-makers and implementers to specify the policies and rules that the members of a community must follow to enable effective, trustworthy implementations. Such governance frameworks may help address questions of liability in decentralized systems. However, since the effectiveness of a decentralized ID system is dependent upon the stakeholders participating in an ecosystem, developing governance models that incentivize each participant while providing effective rules of the road is imperative.

Another difficulty is the absence of effective mitigation strategies for the challenge of exclusion. Even in implementations that explicitly focus on advancing inclusion, exclusion remains a persistent challenge. Without effective guardrails against exclusion, making the case for any form of digital ID becomes more challenging still. Fully addressing the challenge of exclusion requires grappling with the digital divide and developing systems that can function in low- and no-connectivity environments. Fragmented and uneven access to digital tools and services, as well as a lack of basic digital literacy, can stymie the progress of any technical solution, especially one as complex as decentralized ID. Indeed, even in areas with connectivity, individuals can be excluded from participation in the digital world due to factors including cost, language and literacy.

4 Recommendations

Technical, policy, governance and implementation tools are available to stakeholders seeking to realize decentralized ID.

Attempts to develop decentralized ID encounter barriers to mass adoption. Section 2 offered an overview of this approach to ID and Section 3 theorized on the obstacles to realizing it. This section offers practical recommendations for stakeholders seeking to realize decentralized ID.

Rather than advocate for the development of these systems, this report advises stakeholders to carefully weigh the benefits and drawbacks of different approaches to ID, including using none at all. For those who decide that adopting decentralized ID, either in whole or in part, is the right approach for their goals, this section offers a set of recommendations.

Critically, though this section is divided into technical, policy and governance and implementation recommendations, digital ID requires collaboration across technology and policy. Indeed, developments in policy, technology and implementation will have important ramifications for one another. Thus, while this section divides these recommendations into three sections, it also includes recommendations for each key audience (policy-makers, regulators and executives) across these categories as a way of advocating for a holistic approach to the development of an ID strategy.

4.1 Technical

There are a variety of ways in which stakeholders can contribute to the development of decentralized ID systems from a technical standpoint, including investing in technology and standards development, sharing lessons learned and collaborating with designers.

1 Invest in technology development and implementation

To mature this approach's underpinning technologies, stakeholders can invest in their development and, if necessary, close funding gaps that prevent scaling this vision. Areas that require continued technical development include developing technology and proposals to support key changes, recovery and revocation. Stakeholders can derisk upfront investment in technical development by taking an ecosystem approach to funding, reducing upfront costs for individual participants, and by considering market dynamics in structuring such approaches. Several resources exist to aid this process.[98] Likewise, by committing to piloting and implementing these systems, stakeholders can further support their development.

2 Allocate resources to standards development and alignment

Directing financial and knowledge capital can help fill crucial gaps in the decentralized ID environment. Developing fit-for-purpose technical standards may also have the effect of improving other models of digital ID. It may be useful to engage existing public-private partnerships and standards-setting organizations in developing technical standards and generating buy-in to help realize shared objectives such as interoperability. For example, the OpenWallet Foundation is a consortium collaborating to advance the adoption of secure, interoperable digital wallets. Likewise, governments can work to create greater collaboration between industry-led standards-setting bodies and public-sector agencies. In this process, existing organizations such as the W3C can be helpful resources. In addition to developing standards, it is also critical that stakeholders collaborate to align on standards. On a related point, stakeholders developing technical standards should consider whether there is a possibility to apply specifications across use cases.

3 Support a multi-ecosystem approach

While convergence on underlying standards is crucial to digital ID, future implementations will likely feature multiple distinct ecosystems of verifiers and issuers, each of which may need to develop or adapt its own technical standards, governance frameworks and more. Developing foundational standards that can support this multi-ecosystem approach to ID could help scale this approach. Likewise, creating processes to foster a robust ecosystem of verifiers, such as standards on trusted verifiers, can help decentralized ID scale.

4 Capture and share lessons

Generally, there is a need to move beyond a one-off pilot-based approach to decentralized ID. If an organization is piloting technology relevant to this model, it can benefit the ecosystem by ensuring that pilots are not only open-sourced but also sufficiently well documented so that learnings can be disseminated widely.

5 Invest in private-sector talent development

To address the challenges of change and process management, stakeholders may benefit from investing in talent development focused on decentralized ID. Where helpful, training and certification programmes can provide a mechanism for development as well as a means of providing incentives for individuals. Supporting and resourcing cross-organizational collaboration such as in open-source, open-standards and co-development organizations is one way to bolster skills and cultural development.

6 Collaborate with designers

To overcome design obstacles, stakeholders can collaborate with experienced product leaders, human-centric design researchers and other experts to develop enhanced user-interface and user-experience designs for these systems. One area of development that could benefit from design thinking is simplifying user-management processes for ID credentials.

4.2 Policy

Policy objectives, as well as available mechanisms, vary by jurisdiction. This subsection provides generic policy recommendations that can be adapted according to locale.

1 Evaluate existing regulatory frameworks

A crucial first step towards realizing the benefits and mitigating the risks of this approach to ID is to examine existing regulatory frameworks for any alignment or misalignment with the objectives of decentralized ID. Lawmakers should consider whether laws, policies or regulations entrench systemic barriers to this approach. They should also consider what unique benefits these systems could bring to their constituents – for example, such approaches to ID facilitate dynamic policy refresh, where policies can be updated at predetermined intervals.

2 Consider altering existing policies

If specific laws and policies curtailing this approach exist, such as policies preventing or discouraging reusable credentials, officials may seek to alter them. Critically, stakeholders should attempt to understand how any policy changes would affect the liability of the various parties in a credential

exchange. Addressing issues of liability may require governments to establish rules and processes for trusted issuers and validators, creating criteria regarding which stakeholders can become validators and how validation ought to occur.

3 Explore the development of enabling regulation

Governments can also explore the development of enabling regulation. For instance, there remains a need for governments to define requirements for verifiers and wallets. Developing an auditing process can also help to ensure conformity with requirements. Certification processes developed through public-private collaboration can help implement policies on trusted validators. Authorizing legislation can enable governments to provide clear objectives for industry without prescribing specific technologies or approaches.

Governments should resist the tendency to look at decentralized ID as primarily a banking and KYC issue, and consider the broad contexts in which ID is used in society. They should seek to understand how decentralized ID could further policy objectives and how enabling regulation could help progress them. Furthermore, governments should seek to balance competing priorities, such as security and privacy, in developing enabling regulation that suits a given set of policy objectives. One example of government-led enabling regulation is the European Union's eIDAS, which ensures that individuals can use national ID schemes to access public services across the EU and creates a European internal market for trust services.[99] Building upon this effort, the proposed EU-wide digital wallet initiative is an effort to initiate a scheme for member countries to create interoperable digital wallets for EU citizens. European digital identity wallets will need to be approved and built with privacy-by-design, security-by-design and open-source software. The European Digital Identity Framework Board will develop an updated governance framework and collaborate with the European Union Agency for Cybersecurity in applying eIDAS regulation in relation to cyberthreats.[100]

4 Provide incentives for the development of privacy-enhancing technologies

Whether creating new policies or enforcing existing ones, government stakeholders can help realize the benefits of decentralized ID by providing incentives to develop privacy-enhancing technologies. For instance, sweeping data-protection regulations such as the EU's GDPR designed and enforced at the national level can create incentives for parties to produce technologies in line with privacy and user-centricity. Without new rules, it may be difficult to achieve adequate incentives for the development of these technologies. Moreover, by addressing centralizing practices that entrench current approaches to ID, governments can help avoid vendor lock-in and encourage innovation. Governments can also explore funding projects where there is the possibility of developing advances in privacy-enhancing technologies.[101]

5 Consider developing data portability policies

By enshrining and enforcing policies on data portability, governments can help ensure that ID systems are open and competitive. For example, to avoid lock-in effects, the European Digital Identity wallet mandates that users must have full control of their data.

6 Set requirements for interoperability

Rather than attempting to develop these systems themselves, governments can set requirements for the development of an interoperable, open ID system and allow industry to develop solutions according to set criteria. Such an approach is being trialled in the European Union with the proposed EU Digital Identity Wallet initiative.

7 Explore the use of transitional mechanisms

Policy-makers and regulators may find benefits in transitional mechanisms such as the creation of a regulatory sandbox to enable innovators to experiment with new technologies, gaining useful insights and then improving upon them. And policy-makers may find the use of safe harbour provisions to support innovation in sandboxes advantageous. However, if governments decide to develop a sandbox, they should seek to provide clarity to stakeholders about its role in broader efforts. These transitional mechanisms can enable governments to explore hybrid approaches to implementing decentralized ID systems that integrate some components of legacy systems with newer models.

8 Consider creating specialized regulatory units

Governments may benefit from developing specialized regulatory units with qualified staff to undertake these efforts to create a decentralized ID system. Through collaborating with industry and other governments, such units can draw attention to areas in need of review. A nuanced understanding of the benefits of decentralization is crucial to the development of an effective ID strategy. To facilitate this, governments can consider funding research efforts to clearly identify the benefits for their citizens of decentralized ID, while also flagging its risks.

9 Consider equipping agencies to develop future-forward policies

There is considerable dynamism in digital ID, and the technologies, policies, standards, markets and stakeholders are continuously evolving. To shepherd positive outcomes in digital ID and other fast-moving technology sectors, government entities should consider equipping existing agencies with the tools required, or in some cases creating agencies, to support the development of future-forward technologies capable of achieving policy objectives.

10 Invest in public-sector talent development

Broadly, governments and regulatory agencies may find benefit in investing in developing in-house expertise on these topics. There is a need for more educational opportunities for policy-makers focused on different models of ID, especially programmes capable of articulating the connection between digital ID and various policy objectives. By using existing training programmes, as well as fora for collaboration, agencies can upskill their staff to better keep pace with technical developments. Further, by promoting opportunities for technologists and policy-makers to communicate directly and learn from each other, both groups will be better able to articulate the relevant technical and policy capabilities and goals, leading to technical artefacts that will be better crafted to meet current and future policy requirements.

11 Encourage public-private collaboration

Government stakeholders can also foster collaboration across the public and private sectors, where possible using existing initiatives, to ensure a robust flow of information between government and industry. These efforts should help to clearly articulate the benefits and risks of this vision of ID to lawmakers and their constituencies. Governments can also use international fora to ensure that their efforts and any lessons learned are shared across jurisdictions to facilitate a flow of best practices and other useful information. Policy-makers may also need to consider allocating funds to subagencies to modernize IT infrastructure to ensure it conforms with the principles articulated in Section 2.2.

12 Develop high-assurance credentials

Although decentralized ID makes possible an approach in which credentials are issued by participants throughout the system, official IDs issued by governments remain a crucial ingredient if individuals are to receive the full benefits of digital ID. In jurisdictions where individuals lack an official ID, government stakeholders may address this by increasing access to high-assurance credentials. These efforts should seek to evaluate the level of assurance of the credentials created, considering factors such as the method of identity-proofing.

13 Leverage governance frameworks

Another approach to enhancing these systems is to use governance frameworks, which provide tools for decision-makers and implementers to specify the policies and rules that the members of a community must follow to enable effective, trustworthy implementations. Examples of governance frameworks include the Trust Over IP Foundation's Governance Architecture Specification and Governance Metamodel Specification.[102] Forthcoming outputs will offer stakeholder-specific recommendations for developing trustworthy ID ecosystems.[103] These governance frameworks may also be helpful in addressing questions of liability in decentralized systems.

4.3 Governance and implementation

Beyond policy and technology, there are a variety of ways in which stakeholders can help realize a decentralized approach to ID. This subsection offers governance and implementation recommendations on topics ranging from communications to utility to ethical standards, which stakeholders may draw upon to develop effective decentralized ID systems.

1 Clearly communicate the benefits and risks

As explored in Section 3.3, one obstacle to decentralized ID is a lack of user demand, stemming in part from communications challenges. To address this, stakeholders can create and disseminate accurate, coherent explanations of this approach and how it can help individuals, highlighting benefits such as privacy, control and efficiency. These communications campaigns should explain the link between privacy and digital ID and seek to counter misinformation and conspiracy theories related to digital ID. They should also clearly articulate the risks of these systems.

2 Increase system utility

Another way to address the issue of user demand is to develop decentralized ID with a clear use case or function. By increasing the utility of decentralized ID

systems, stakeholders will be able to demonstrate their benefits more clearly. For example, governments wishing to develop a useful ID system could create systems that enable access to public assistance. Linking ID with a variety of uses can also expand the network of stakeholders committed to this. Existing initiatives may offer an opportunity for governments to modernize their approach to ID, by creating enabling environments for the development of trusted, privacy-preserving ID systems.

3 Target use cases with low barriers to entry

In developing a utility-based approach to scaling decentralized ID, it is worth considering what use cases exist with relatively low barriers to entry. For example, efforts to develop education or skills credentials are likely to encounter fewer regulatory barriers than financial services use cases. Groups such as the Digital Credentials Consortium and Learning Economy Foundation are already exploring these use cases. When considering use cases, it can be helpful to take a risk-based approach, mapping out potential obstacles to scale and identifying achievable goals – for instance, easier-to-adopt use cases that can be implemented by private-sector providers and provide clear utility.

4 Develop and enact strategies to mitigate exclusion, marginalization and oppression

There remains a need for industry, government, civil society and academia to develop strategies to address exclusion, marginalization and oppression. Basic functional requirements for digital ID systems can serve as a starting point for doing so. For example, stakeholders can consider reducing barriers to the development of digital ID by lowering the costs of foundational technologies and working with designers to make these solutions accessible for users with minimal digital literacy. This is especially crucial in environments where a lack of infrastructure and connectivity limits the effectiveness of digital tools. Likewise, by developing trusted wallets that are easy to use, stakeholders can enable broader access to services.

Fully addressing the issue of exclusion also requires closing the digital divide. By providing digital tools, services and education to individuals who need them, stakeholders can broaden access. Where providing digital tools is not possible, stakeholders may also find benefit in using analogue approaches to ID that preserve privacy. In developing strategies to address these challenges, stakeholders should seek to assess whether a given use case requires ID at all. Just because the technologies exist to support these approaches does not mean that they should be required in all cases. Indeed, there are some instances where requiring any form of ID is deemed unnecessary or undesirable.

5 Leverage localized research and ethical standards

Stakeholders seeking to implement this vision can also benefit from context-specific, on-the-ground research assessing the potential for exclusion and developing mitigation strategies. Resources modelling a human-centric approach to ID research exist.[104] Assessing exclusionary potential should be done on a regular basis as circumstances can shift rapidly due to sociopolitical factors. Law and policy, as well as governance frameworks, can also be used to help counter the risk of exclusion. Nonetheless, efforts aimed at addressing exclusion should carefully consider the potential for coerced consent, especially among vulnerable populations. Likewise, using established and trusted ethical standards throughout the design, development and implementation phases can help mitigate risks.

Conclusion

Decentralized ID has the potential to increase access and privacy while improving efficiency and effectiveness. Yet it also poses risks of its own and faces obstacles.

Central to developing effective approaches to ID is asking what purpose ID should serve in modern society. While the existing laws, policies and practices to which this report refers as the contemporary ID paradigm are central to safeguarding individuals and institutions, they also create inefficiencies and risks, undermine privacy and exclude the roughly 850 million people worldwide without any form of official ID.[105] Decentralized ID is one approach that has the potential to address some of the shortcomings of this paradigm. Yet it also poses risks and faces significant obstacles in scaling.

This report has provided an assessment of decentralized ID from a policy and technical standpoint. It has offered tools, frameworks and recommendations for lawmakers, regulators and industry leaders seeking to engage with decentralized ID. Recognizing that ID strategies will vary across jurisdictions, use cases, cultures and more, it has not provided a one-size-fits-all set of recommendations but an overview of the advantages and disadvantages of decentralized ID compared to other models of ID. For stakeholders choosing to take this approach, tools and recommendations were provided to help them realize its benefits and mitigate its risks.

As with all forms of ID, implementing this model is a complex undertaking that should not be separated from its social, political and economic contexts. It remains to be seen whether this approach will achieve mass adoption and what its real-world impact will be.

While proponents see it as a means of expanding access and enhancing privacy, critics view it as immature and risk-prone. If efforts to realize decentralized ID have yet to provide answers to fundamental questions about the role of ID in modern society, they have raised important considerations that can be used to help stakeholders reimagine – and perhaps even realize – ID in a manner that is more effective, inclusive and empowering.

Contributors

World Economic Forum

Lead Author

Aiden Slavin
Project Lead, Crypto Impact and Sustainability Accelerator, World Economic Forum, USA

Working Group Chairs

Kim Hamilton Duffy
Director of Identity Standards, Centre, USA; Chair, Technical Working Group, World Economic Forum Digital ID Initiative

Justin Newton
Chief Executive Officer, Netki, USA; Chair, Policy Working Group, World Economic Forum Digital ID Initiative

Ethan Veneklasen
Head of Advocacy and Communications, ID2020, USA; Chair, Impact Working Group, World Economic Forum Digital ID Initiative

Acknowledgements

Sincere appreciation is extended to the following working group members, who committed hours to offering expert insights and providing feedback on drafts. Their efforts are foundational to the success of this work.

Sylvia Aran
Technical Sales Director, Polygon Labs, Switzerland

Daniel Bachenheimer
Global Lead Unique Identity Services, Accenture, USA

Moushmi Banerjee
Senior Software Architect, Okta, USA

Justin Banon
Co-Founder, Boson Protocol, United Kingdom

Chancellor Barnett
Chairman, Jewel Bank, USA

Erick Xavier Franco Bass
Sr Associate Technical Sales, Polygon Labs, Spain

Duane Block
Managing Director, Accenture, USA

Joni Brennan
President, Digital ID & Authentication Council of Canada, Canada

Juan Caballero
Executive Director, Chain Agnostic Standards Alliance, Germany

Ben Cessa
Chief Technology Officer, AID:Tech, Mexico

Wayne Chang
Chief Executive Officer, Spruce Systems, USA

Paola Del Vitto
Digital Identity & Artificial Intelligence Strategy Lead, Italian Banking Association, Italy

Eugenio DiMira
Vice-President Revenue and Product Strategy, Finclusive, Canada

Amos Doornbos
Director of Strategy & Systems, World Vision, United Kingdom

Edward Duffus
Director of Product Strategy and Sustainability, OpenCRVS, France

Johannes Ebert
Business Developer, Spherity, Germany

Cecilia Emilsson
Policy Analyst, Organisation for Economic Co-operation and Development, France

Chris Ferreira
Senior Program Manager, Digital ID & Authentication Council of Canada, Canada

Tom Fisher
Senior Research Officer, Privacy International, United Kingdom

Merryl Ford
Digital Transformation Specialist, Council for Scientific and Industrial Research, South Africa

Lucia Gallardo
Chief Executive Officer, Emerge, United Kingdom

Daniel Goldscheider
Founder, OpenWallet Foundation, Switzerland

Dakota Gruener
Independent, USA

Trev Harmon
Director of Technology, ID2020, USA

Nicky Hickman
Advisor, cheqd, United Kingdom

Jake Hirsch-Allen
Advisor, Readocracy, USA

Sanjay Jain
Partner, Bharat Innovation Fund, India

Taylor Kendal
President, Learning Economy Foundation, USA

Nichanan Kesonpat
Head of Platform, 1kx, Thailand

Sina Kian
Chief Operating Officer, Aleo, USA

Tobias Looker
Chief Technology Officer, MATTR, New Zealand

Dane Lund
Head DAO Architect, Alliance DAO, USA

Viky Manaila
Trust Services Director, Intesi Group, Italy

Victor Mapunga
Chief Executive Officer, FlexID Technologies, Singapore

Niall McCann
Policy Advisor, United Nations Development Programme, Ireland

Luke McIntyre
Chief Product Officer, MATTR, New Zealand

John Medel
Public Policy Manager, Coinbase, USA

Calanthia Mei
Co-Founder, Masa Protocol, USA

Otto Mora
Tech Sales Lead, Polygon, Costa Rica

Massimo Morini
Chief Economist, Algorand Foundation, Italy

Monique Morrow
Independent Board Director, Hedera, Switzerland

Darrell O'Donnell
Technology & Strategy Advisory, Continuum Loop, Canada

Scott Onder
Chief Investment Officer, Mercy Corps, USA

Alex Popowycz
Chief Information Officer, Hedera, USA

John Reynolds
Product Manager, Aleo, USA

Bryn Robinson-Morgan
Vice-President, Mastercard, United Kingdom

Nilmini Rubin
Head of Global Policy, Hedera, USA

Jonathan Rufrano
Public Sector & Institutions Lead, Spruce Systems, USA

Erica Salinas
Principal Tech Leader Web3, Amazon, USA

Pierre Samaties
Partner, Roland Berger, United Arab Emirates

Clive Smith
Executive Director, ID2020, United Kingdom

Jamie Smith
Product Director, Gen Digital, United Kingdom

Max Song
Chief Executive Officer, Carbonbase, Hong Kong

Carsten Stöcker
Chief Executive Officer, Spherity, Germany

Elisabeth Sylvan
Managing Director, Berkman Klein Center for Internet & Society at Harvard University, USA

Linda Taylor
Technical Program Manager, Digital Square at PATH, South Africa

Stephen Taylor
Chief Delivery Officer, Simprints, United Kingdom

Joel Telpner
Chief Legal Officer, IOHK, USA

Oliver Terbu
Director Identity Standards, Spruce Systems, Germany

Yiannis Theodorou
Global Lead Digital Identity, Tony Blair Institute for Global Change, United Kingdom

Tomicah Tillemann
Chief Policy Officer, Haun Ventures, USA

Andrew Tobin
Commercial Director Digital Trust Services, Gen Digital, United Kingdom

Barbara Ubaldi
Acting Head of the Division on Open and Innovative Governments, Organisation for Economic Co-operation and Development, France

Jacques von Benecke
Chief Technology Officer, Druk Holdings and Investments, Bhutan

Benjamin Welby
Policy Analyst, Organisation for Economic Co-operation and Development, France

Tom Wilkinson
Chief Data Officer, The Scottish Government, United Kingdom

Danielle Zimmerman
Special Counsel, Coinbase, USA

Sincere appreciation is also extended to the Crypto Impact and Sustainability Accelerator (CISA) team, CISA Steering Committee and the following expert reviewers and advisers for offering insights and providing feedback on the drafts.

Hayley Anna
Program Assistant, Blockchain Law for Social Good Center, University of San Francisco School of Law, USA

Shlomit Azgad-Tromer
Chief Executive Officer, Sealance, USA

Kimmy Bettinger
Expert & Knowledge Communities Lead, World Economic Forum, USA

Kevin Collins
Fellow, World Economic Forum, USA

Raquel de Horna
Product & Marketing Lead – Digital Identities, Giesecke+Devrient, Spain

Eileen Donahoe
Executive Director Global Digital Policy Incubator, Stanford University, USA

Andrew Gallucci
Director of Regulatory Strategy, Circle, USA

Caroline Hill
Senior Director of Global Policy & Regulatory Strategy, Circle, USA

Rostislav Konyashkin
Chairman of the Board, JSC National Information Technologies, Kazakhstan

Stephanie Llamas
Lead, Metaverse Governance, World Economic Forum, USA

Brynly Llyr
Head, Crypto Impact and Sustainability Accelerator, Blockchain and Digital Assets, World Economic Forum, USA

Brett McDowell
Chair, Hedera, USA

Jordan Miller
Senior Regulatory Policy Specialist, Circle, USA

Bagdat Mussin
Minister of Digital Development, Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan, Kazakhstan

Ntsibane Ntlatlapa
Centre Head, Centre for the Fourth Industrial Revolution South Africa, South Africa

Matthew Price
Fellow, World Economic Forum, USA

Drummond Reed
Director Trust Services, Gen, USA

Anna Schilling
Fellow, World Economic Forum, USA

Kristin Toretta
Global Financial Services Lead, Security Assurance, AWS, USA

Asset Turyssov
Vice-Minister, Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan, Kazakhstan

Pramod Varma
Former Chief Architect, Aadhaar & India Stack, India

Thilo von Bredow
Business Development & Financial Lead Digital Identities, Giesecke+Devrient, Germany

Samantha Weinberg
Project Specialist, Crypto Impact and Sustainability Accelerator, World Economic Forum, USA

Kathryn White
Fellow, World Economic Forum, USA

Kaliya Young
Founding Partner, Identity Woman in Business, USA

Askar Zhambakin
Vice-Minister, Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan, Kazakhstan

We are also grateful to those who contributed their insights via interviews and workshops, including those not listed above.

Production

Laurence Denmark
Creative Director, Studio Miko

Sophie Ebbage
Designer, Studio Miko

Alison Moore
Editor, Astra Content

Oliver Turner
Designer, Studio Miko

Endnotes

1. The World Bank ID4D, ID4D Global Dataset: https://id4d.worldbank.org/global-dataset.
2. See, for example: Adam M. McKeown, *Melancholy Order: Asian Migration and the Globalization of Borders*, Columbia University Press: http://cup.columbia.edu/book/melancholy-order/9780231140775.
3. United Nations, Universal Declaration of Human Rights: https://www.un.org/en/about-us/universal-declaration-of-human-rights.
4. The World Bank ID4D, Practitioner's Guide: Types of ID Systems: https://id4d.worldbank.org/guide/types-id-systems.
5. United Nations, Department of Economic and Social Affairs, Statistics Division, United Nations Legal Identity Agenda: https://unstats.un.org/legal-identity-agenda/#:~:text=Legal%20identity%20is%20defined%20as,following%20the%20occurrence%20of%20birth.
6. United Nations, Department of Economic and Social Affairs, Sustainable Development, The 17 Goals: https://sdgs.un.org/goals.
7. The World Bank ID4D, Practitioner's Guide: Good ID Supports Multiple Development Goals: https://id4d.worldbank.org/guide/good-id-supports-multiple-development-goals.
8. Financial Action Task Force, Guidance on Digital ID, 6 March 2020: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html.
9. Jayanth Kancherla, Re-identification of Health Data through Machine Learning, SSRN, 30 November 2020: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794927.
10. At the same time, AI can also help facilitate the development of more advanced digital ID systems. For example, deep learning-based systems can help with ID verification. AI can also help detect identity deepfakes.
11. It does, however, run on identifiers that individuals may acquire from private entities such as email service providers (Yahoo, Aol., Gmail) social media services (Twitter, Facebook, Instagram) or globally managed registries (ICANN for domain names, or ITU-T for phone numbers).
12. While useful analytically, these categories can be further subdivided and analysed. For one such elaboration, see: Kaliya Young, *The Domains of Identity: A Framework for Discernment of How Identity Works in Contemporary Systems in Society*, Anthem Press: https://identitywoman.net/wp-content/uploads/Domains-of-Identity-Highlights-1.pdf.
13. World Economic Forum, Identity in a Digital World: A New Chapter in the Social Contract, September 2018: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.
14. This table updates Figure 3 in a previous World Economic Forum report, Identity in a Digital World: A New Chapter in the Social Contract, September 2018: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.
15. United States Agency for International Development, Identity in a Digital Age: Infrastructure for Inclusive Development: https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf.
16. Ibid.
17. For example, the Government of Bhutan has reported the development of a decentralized biometric digital ID system.
18. In this case, accessing government-issued credentials in a decentralized system may require registration with a government to establish uniqueness within a target population.
19. The World Bank ID4D, Practitioner's Guide: Identity Lifecycle: https://id4d.worldbank.org/guide/identity-lifecycle.
20. Paul A. Grassi, Michael E. Garcia and James L. Fenton, Digital Identity Guidelines, NIST Special Publication 800-63-3, US National Institute of Standards and Technology, June 2017: https://pages.nist.gov/800-63-3/sp800-63-3.html.
21. Alexis Hancock, Digital Identification Must Be Designed for Privacy and Equity, Electronic Frontier Foundation, 31 August 2020: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10.
22. NIST Computer Security Resource Centre, Glossary: Pseudonymity: https://csrc.nist.gov/glossary/term/pseudonymity.
23. W3C Working Group Note, Use Case 2.11: Public Authority Identity Credentials (eIDAS), 17 March 2021: https://www.w3.org/TR/did-use-cases/#publicAuthorityCredentials.
24. Ibid.
25. While there is no single, monolithic ID regime, this section considers the policies, practices and technologies that produce dominant ID processes today.
26. Tomicah Tillemann, What is Web3 Good For?, Project Syndicate, 7 September 2022: https://www.project-syndicate.org/commentary/web3-improve-financial-system-for-privacy-security-and-law-enforcement-by-tomicah-tillemann-2022-09.
27. Bennett Cyphers and Cory Doctorow, Privacy Without Monopoly: Data Protection and Interoperability, Electronic Frontier Foundation, 12 February 2021: https://www.eff.org/wp/interoperability-and-privacy.
28. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019.

29. Nicholas Anthony, The Right to Financial Privacy: Crafting a Better Framework for Financial Privacy in the Digital Age, CATO Working Paper No. 69, 14 October 2022: https://www.cato.org/sites/cato.org/files/2022-10/working-paper-69.pdf.
30. Cisco, Consumer Privacy Survey: The Growing Imperative of Getting Data Privacy Right, Cisco Cybersecurity Series 2019: https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf.
31. The World Bank, The Global Findex Database 2021: Executive Summary Visualization: https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization.
32. Financial Action Task Force, Guidance on Digital ID: https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html.
33. Louis de Koker, Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion, Journal of Financial Crime, 1 January 2006: https://www.emerald.com/insight/content/doi/10.1108/13590790610641206/full/html.
34. LexisNexis Risk Solutions, 2022 True Cost of Financial Crime Compliance Study – Global Summary: https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report.
35. McKinsey & Company, Transforming Approaches to AML Financial Crime, September 2019: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/transforming%20approaches%20to%20aml%20and%20financial%20crime/transforming-approaches-to-aml-and-financial%20crime-vf.pdf.
36. World Economic Forum, Identity in a Digital World: A New Chapter in the Social Contract, September 2018: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.
37. World Economic Forum, Digital Identity Ecosystems: Unlocking New Value, September 2021: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf.
38. ID2020, Certification: https://id2020.org/certification.
39. Kim Cameron, The Laws of Identity, May 2005: https://www.identityblog.com/?p=352.
40. Sovrin, Principles of SSI V3: https://sovrin.org/principles-of-ssi/.
41. Omidyar Network, Omidyar Network Unpacks Good ID, May 2019: https://omidyar.com/wp-content/uploads/2020/09/ON-Unpacks-Good-ID_Final_3.7.19.pdf.
42. Principles on Identification for Sustainable Development: Toward the Digital Age: https://www.idprinciples.org/.
43. ID2020, Technical Requirements: V1.01, 28 April 2019: https://id2020.org/uploads/files/ID2020-TAC-Requirements-v1.01.pdf.
44. Daniel Hardman, A Gentle Introduction to Verifiable Credentials, Evernym, 24 October 2019: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/.
45. W3C, Verifiable Credentials Data Model V2.0 Publication History: https://www.w3.org/standards/history/vc-data-model-2.0.
46. W3C, Verifiable Credentials Data Model v1.1, 3 March 2022: https://www.w3.org/TR/vc-data-model/.
47. The two most important protocols in this regard are the following: 1) the issuance protocol that enables a holder to request a VC from an issuer and enables an issuer to send a VC to the holder; 2) the presentation protocol that enables a verifier to request VCs from a holder. For the latter, the verifier might also request that the holder can prove that the holder is the intended, rightful or designated holder of the VC and has not received an erroneous copy from somebody else to prevent identity fraud. Also note that a few different options exist for both protocols.
48. Its development was prompted by the Silicon Valley Innovation Program (SVIP) of the Department of Homeland Security (DHS), which made it a requirement of the companies they contracted with to develop an open API standard to prevent proprietary API lock-in.
49. Kristina Yasuda, Torsten Lodderstedt, David Chadwick, Kenichi Makamura and Jo Vercammen (eds.), Open ID for Verifiable Credentials: A Shift in the Trust Model Brought by Verifiable Credentials, OpenID, 23 June 2022: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf.
50. In this regard, OpenID4VC demonstrates an alternative approach or an addition to the specifications developed in W3C CCG. These extensions include the self-issued OpenID Provider v2 (SIOPv2), OpenID for Verifiable Presentations (OpenID4VP) and OpenID for Verifiable Credential Issuance (OpenID4VCI) specifications.
51. European Commission, Shaping Europe's Digital Future: The European Digital Identity Wallet, Architecture and Reference Framework, 10 February 2023: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.
52. European Commission, NIFO – National Interoperability Framework Observatory, Glossary: Semantic Interoperability: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/glossary/term/semantic-interoperability.
53. Daniel Hardman, A Gentle Introduction to Verifiable Credentials, Evernym, 24 October 2019: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/
54. Andrea De Salve, Andrea Lisi, Paolo Mori and Laura Ricci, Selective Disclosure in Self-Sovereign Identity Based on Hashed Values, IEEE: https://ieeexplore.ieee.org/document/9913052.
55. Brent Zundel, Why the Verifiable Credentials Community Should Converge on BBS+, Evernym, 24 March 2021: https://www.evernym.com/blog/bbs-verifiable-credentials.

56. Achieving selective disclosure at scale may require having issuers sign each statement on a VC separately. The EU Digital Wallet Architecture Reference Framework (ARF) enables several formats that separately sign claims within credentials such as SD-JWT with JSON or JSON-LD, mDL/mdoc (ISO 18013-5) with CBOR and LD-Proofs with BBS+ to secure a JSON-LD payload.

57. Identity Woman in Business, Where Can the W3C VCs Meet the ISO 18013-5mDL?: An Open Letter to the Two Standards Communities as Well as All Interested Parties, 4 December 2022: https://medium.com/@identitywoman-in-business/where-can-the-w3c-vcs-meet-the-iso-18013-5-mdl-b2d450bb19f8.

58. In parallel, work on ISO 18013-7 has started to define the protocols for online presentation of mDLs as well. The idea is that ISO 18013-5 and ISO 18013-7 will become mDL-specific profiles of the building blocks defined in ISO/IEC 23220.

59. Joseph Burleson, Michele Korver and Dan Boneh, Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs: Full Paper, a16zcrypto, 16 November 2022: https://a16zcrypto.com/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/.

60. European Parliament, ***I Report on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity, 2 March 2023: https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.pdf.

61. Sriram Darbha and Rakesh Arora, Privacy in CBDC Technology, Bank of Canada Staff Analytical Note 2020-9, June 2020: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.

62. Nonetheless, there are solutions based on ZKPs that allow the revocation and back-up of credentials.

63. E. Glen Weyl, Puja Ohlhaver and Vitalik Buterin, Decentralized Society: Finding Web3's Soul, SSRN, 11 May 2022: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763.

64. World Economic Forum, Decentralized Autonomous Organizations: Beyond the Hype, 23 June 2022: https://www.weforum.org/whitepapers/decentralized-autonomous-organizations-beyond-the-hype/.

65. Keith Kowal, The Rise of the Identity Token, Hedera, 24 February 2023: https://hedera.com/blog/the-rise-of-the-identity-token.

66. Trust Over IP Foundation, Overcoming Human Harm Challenges in Digital Identity Ecosystems, 16 November 2022: https://trustoverip.org/wp-content/uploads/Overcoming-Human-Harm-Challenges-in-Digital-Identity-Ecosystems-V1.0-2022-11-16.pdf.

67. Access Now, An Open Letter to the Leaders of International Development Banks, the United Nations, International Aid Organisations, Funding Agencies and National Governments: https://www.accessnow.org/whyid/.

68. Trust Over IP Foundation, Overcoming Human Harm Challenges in Digital Identity Ecosystems, 16 November 2022: https://trustoverip.org/wp-content/uploads/Overcoming-Human-Harm-Challenges-in-Digital-Identity-Ecosystems-V1.0-2022-11-16.pdf.

69. Ibid.

70. Margie Cheesman, Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics 27 (1), 2022: https://www.tandfonline.com/doi/full/10.1080/14650045.2020.1823836.

71. Privacy International, The Looming Disaster of Immunity Passports and Digital Identity, 21 July 2020: https://privacyinternational.org/long-read/4074/looming-disaster-immunity-passports-and-digital-identity.

72. Jordan Sandman, It's Time for IDs to Go Digital, New America, 24 August 2021: https://www.newamerica.org/the-thread/its-time-for-ids-to-go-digital/.

73. Emrys Schoemaker, Paul Currion and Bryan Pon, Identity at the Margins: Identification Systems for Refugees, Caribou Digital, 2018: https://www.cariboudigital.net/wp-content/uploads/2020/03/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf.

74. Organisation for Economic Co-operation and Development, Bridging Digital Divides in G20 Countries, 20 December 2021: https://www.oecd.org/digital/bridging-digital-divides-in-g20-countries-35c1d850-en.htm.

75. Silvia Masiero, Digital Identity as Platform-Mediated Surveillance, Big Data & Society 10 (1), January–June 2023: https://journals.sagepub.com/doi/epub/10.1177/20539517221135176; Monique J. Morrow and Mehran Zarrebini, Blockchain and the Tokenization of the Individual: Societal Implications, Future Internet 11 (10), Blockchain: Current Challenges and Future Prospects/Applications, 2019: https://www.mdpi.com/1999-5903/11/10/220.

76. Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, Washington University Law Review 96 (6): Trust and Privacy and in the Digital Age, 2019: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview.

77. European Commission, European Digital Identity: Digital Identity for All Europeans: A Personal Digital Wallet for EU Citizens and Residents: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

78. Daniela Pöhn, Michael Grabatin and Wolfgang Hommel, eID and Self-Sovereign Identity Usage: An Overview, Electronics 10 (22), 2021: https://www.mdpi.com/2079-9292/10/22/2811#B41-electronics-10-02811.

79. Kyle Becker, Lauren Serota, Sabrina Scuri and Tricia Wang, UX in Cryptocurrency: An Overview of User Experience in Cryptocurrency Applications, CRADL Report, August 2022: https://docs.google.com/presentation/d/1s2OPSH5sMJzxRYaJSSRTe8W2iloZx0PselV-WeZWD1s/edit#slide=id.p.

80. Vitalik Buterin, Where to Use a Blockchain in Non-Financial Applications, 12 June 2022: https://vitalik.ca/general/2022/06/12/nonfin.html.

81. Introducing Travel Pass: The Easiest, Safest Way to Verify Travel and Health Credentials, Evernym: https://www.evernym.com/travelpass/#:~:text=What%20is%20IATA%20Travel%20Pass,secure%20and%20privacy%2Dpreserving%20manner.

82. International Civil Aviation Organization, Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis, 27 January 2023: https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf.

83. Introducing Travel Pass: The Easiest, Safest Way to Verify Travel and Health Credentials, Evernym: https://www.evernym.com/travelpass/#:~:text=What%20is%20IATA%20Travel%20Pass,secure%20and%20privacy%2Dpreserving%20manner.

84. Good Health Pass, What Is a Good Health Pass?: https://www.goodhealthpass.org/.

85. Sabre, New Distribution Capacity, 5 January 2022: https://www.sabre.com/insights/new-distribution-capability/.

86. OneID: https://oneid.uk.

87. Ahmed Alrehaili, Abdallah Namoun and Ali Tufail, A Comparative Analysis of Scalabillty Issues within Blockchain-Based Solutions in the Internet of Things, International Journal of Advanced Computer Science and Applications 12 (9), 2021: https://thesai.org/Downloads/Volume12No9/Paper_55-A_Comparative_Analysis_of_Scalability_Issues.pdf.

88. Abdurrashid Ibrahim Sanka and Ray C. C. Cheung, A Systematic Review of Blockchain Scalability: Issues, Solutions, Analysis and Future Research, Journal of Network and Computer Applications 195, 1 December 2021: https://www.sciencedirect.com/science/article/abs/pii/S1084804521002307.

89. Daniel Hardman, A Gentle Introduction to Verifiable Credentials, Evernym, 24 October 2019: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/.

90. Jordan Sandman, It's Time for IDs to Go Digital, New America, 24 August 2021: https://www.newamerica.org/the-thread/its-time-for-ids-to-go-digital/.

91. See, for example: Coinbase, Re: Ensuring Responsible Development of Digital Assets; Request for Comment, 1 November 2022: https://assets.ctfassets.net/c5bd0wqjc7v0/4QJpib4JJ4AYCpOiuYavSP/3670f91940053f7e16760d1d74f9051f/Coinbase_Comments_-_Treasury_RFC.pdf.

92. Michael J. Casey, A Reckoning Looms for America's 50-Year Financial Surveillance System, Cato Institute, Cato Journal, Spring/Summer 2021: https://www.cato.org/cato-journal/spring/summer-2021/reckoning-looms-americas-50-year-financial-surveillance-system.

93. Donovan Jackson, LA Wallet Digital Driver's License App Not Accepted Everywhere, WAFB, 14 August 2019: https://www.wafb.com/2019/08/14/la-wallet-digital-drivers-license-app-not-accepted-everywhere/.

94. Justuseapp.com, LA Wallet Status, 13 February 2023: https://justuseapp.com/en/app/1386930269/la-wallet/problems.

95. LAWallet, Louisiana's Legal Digital Driver's License: https://lawallet.com/.

96. See, for example: European Union External Action, "My Friend Thinks Bill Gates Will Microchip Humanity". Now What?, 5 March 2021: https://www.eeas.europa.eu/eeas/%E2%80%9Cmy-friend-thinks-bill-gates-will-microchip-humanity%E2%80%9D-now-what_en.

97. See for example: Gitcoin, Introducing Passport – Digital Identity as a Public Good, 29 August 2022: https://go.gitcoin.co/blog/intro-to-passport.

98. See, for example: World Economic Forum, Digital Identity Ecosystems: Unlocking New Value, September 2021: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf.

99. European Commission, Shaping Europe's Digital Future: eIDAS Regulation: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

100. European Commission, European Digital Identity: Digital Identity for All Europeans: A Personal Digital Wallet for EU Citizens and Residents: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

101. The OECD recommends ensuring that digital ID offers a clear utility to individuals, that user experience be optimized and that legal, regulatory and trust frameworks are required to realize the benefits of this innovation. A set of OECD recommendations on the governance of digital ID systems is forthcoming.

102. An example of a governance framework is the Pan-Canadian Trust Framework (PCTF), which was developed with the 14 governmental jurisdictions in Canada to align the steps in the identity verification and proofing process. The Open Identity eXchange and Trust Over IP Foundation both provide resources for those seeking to understand and develop governance frameworks for identity ecosystems.

103. Trust Over IP Foundation, The TOIP Foundation Releases Its First Official Governance Specifications, 1 February 2022: https://trustoverip.org/news/2022/02/01/the-toip-foundation-releases-its-first-official-governance-specifications/.

104. Caribou Digital, When ID Works for Women: Experiences and Challenges of Women in Bangladesh and Sri Lanka, June 2020: https://www.cariboudigital.net/wp-content/uploads/2020/08/when-ID-works-for-women-report.pdf.

105. The World Bank, ID4D Global Dataset: https://id4d.worldbank.org/global-dataset.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org