# Digital identity

polygon ID

polygon Labs

Deutsche Bank Corporate Bank

# Digital identity

## How banks can leverage new Web3 tools to create and solve corporate and individual identity problems – a proof of concept with Polygon ID

Identity is everything. It is key to the inner workings of our societies, governments and economies. Without it, we can only have the narrowest of realities: one without legal agreements, banking services, or even getting paid. Identity is the key to trust, and trust, really, is everything.

In our digital world, where software is eating the world, all identity aspires to be digital too. In reality, it is mostly paper-based, splintered, and prone to error.

This paper, published by Deutsche Bank in association with Polygon Labs, explores a natively digital, sovereign, private identity infrastructure, that leverages blockchain and zero knowledge cryptography. Such identities could underpin our future lives: mostly digital, fully integrated, benefiting from the convergence of Web3, IoT, and AI.

**Deutsche Bank contributors**

**Christopher Noone**, Digital Assets & Currencies Transformation
**Thomas Brophy**, Digital Assets & Currencies Transformation
**Dominik Dribusch**, Corporate Bank Transformation
**Jan Schumann**, Commercial Banking Technology

**Polygon ID contributors**

**Antoni Martín**, Founder, Polygon ID
**Boris Spremo**, Tokenisation Lead, Polygon Labs
**Otto Mora**, Technical Sales Americas, Polygon ID
**Silvia Aran**, Technical Sales Director, Polygon ID

Content contributed by Polygon ID is marked by a purple-edged page

*Note: Polygon ID recently rebranded to Privado ID*

Published May 2024

# Contents

# Foreword – Deutsche Bank

**Sabih Behzad,**
Head of Digital Assets and Currencies Transformation, Deutsche Bank

The identity management space is undergoing a period of momentous change. In today's rapidly evolving digital landscape, the need for enhanced authentication and verification methods is more critical than ever for organisations and individuals alike in their online interactions. Recent technology developments, particularly in the generative artificial intelligence (AI) space, have accelerated the development of cyber-attacks and fraud. Tools to create synthetic identities using real and fake personal information are more readily available and with greater levels of sophistication. Cyber criminals using these technologies pose a significant challenge to organisations and other entities seeking to protect their customers and data.

A functional digital identity layer combatting this problem is a significant step towards a frictionless world where corporates and individuals can interact in a trusted manner throughout the online and offline world. In this context, traditional centralised identity systems are being reimagined to enable identity holders to manage their own identities, unlocking an internet of trust. We at Deutsche Bank believe that banks have a significant role to play with a real opportunity to lead in this value creation.

Collaborating with Polygon ID, one of the pre-eminent leaders in this space, we delve into the fundamental principles of self-sovereign identity (SSI). We examine the underlying technologies that power the SSI ecosystem, including blockchain, Zero-Knowledge Proofs and verifiable credentials. Moreover, we explore three proof of concept (PoC) initiatives of SSI that focus on developing the technical groundwork for potential use cases related to the usage of digital identity, both from an on-chain and off-chain perspective.

While there is still work to do and incentive driven models are yet to achieve widespread adoption, the emergence of digital identity marks a revolutionary shift in the financial services landscape. At Deutsche Bank we are committed to driving the conversation and championing its adoption within our organisation and beyond.

# Foreword – Polygon ID

Digital identity has been one of the Internet's biggest flaws, and that's even before we had AI to contend with. That's why we are building Polygon ID, a self-sovereign, decentralised and private identity protocol for the next iteration of the Web.

Identity, in its essence, is not merely a set of attributes or credentials but a comprehensive reflection of one's engagements and interactions within the digital and physical worlds. This is especially true in the digital era, where the complexity of corporate digital identity demands innovative solutions. Recognising this, Polygon ID was created from a deep understanding of the role of identity in commerce, banking and everyday life, with a mission to ensure that individuals and corporations could use their digital identities with ease and transparency.

Our approach is centred around the principles of self-sovereign identity (SSI), a model that empowers individuals with the ownership and control of their personal data. Polygon ID emerges as a leading implementation of SSI, leveraging blockchain technology and Zero-Knowledge Proofs to provide a framework that is both generic and scalable, reliable and privacy-preserving. These technologies are foundational, enabling the creation of digital identities that are portable across platforms and jurisdictions without sacrificing security or privacy. More than that, we believe that such SSI frameworks are the remedy to the seismic wave of AI-facilitated identity theft and manipulation that awaits us in the very near future.

Our collaboration with Deutsche Bank on a proof of concept highlights the practical application and immense potential of SSI in the financial sector. By experimenting with Polygon ID, Deutsche Bank not only addresses the inherent risks associated with digital identities but also paves the way for a future where we can weave in identity in basic banking and capital markets processes, thus making them more efficient and streamlined.

As always, education plays a critical role in the widespread adoption and understanding of any technology. With this paper we attempt to inform both corporations and individuals about the benefits and workings of SSI, as we believe it is the only way for our future societies to fully leverage its potential.

Looking ahead, the road for digital identity and self-sovereign identity appears both promising and challenging. The adoption of SSI is no doubt set to accelerate, driven by the increasing demand for privacy, security, and control over personal data in the digital realm. As the infrastructure and regulatory frameworks evolve, we can anticipate broader acceptance and integration of SSI across various sectors, beyond banking and finance. However, achieving this vision requires concerted efforts in education, technological innovation, and policy development.

The way forward, then, is to foster collaboration, and the first step in any collaboration is dialogue among stakeholders. Consider this paper and its findings an invitation to join us in this dialogue. Together we can navigate the complexities of digital identity, taking us a step further on the journey towards a more informed and empowered digital future.

**Antoni Martin,**
Co-founder, Polygon ID
and Polygon zkEVM

*(Formerly held roles at Citibank and Deutsche Bank before joining the blockchain world)*

# Executive summary

Identity has been a fundamental feature throughout history – from language, objects, and documents to new digitised forms to confirm identity. Digital identity while still an emerging field, is not new, however; its importance has increased dramatically. During and after the pandemic, our interactions have largely shifted into the digital realm, yet the management of identity has not progressed accordingly. This discrepancy has led to a fragmented user experience, exacerbated by the relinquishment of control over our data to platform providers such as the tech giants who we now entrust. These federated identity management models raise privacy implications and make such platforms attractive targets for unauthorised access.

Self-sovereign identity (SSI) is a promising solution to the problems of centralised and federated methods of managing digital identity. SSI promises to empower the user, both individual and corporates, to manage their own identity. Polygon ID developed by Polygon Labs is one such SSI platform that is looking to drive the SSI agenda forward.

Web3 use cases are a natural starting point for SSI solutions as the identity flows need to fit into a purely digital and often self-controlled environment. However, there are also use cases in existing banking processes that can benefit from SSI– such as Know Your Customer (KYC) processes. The proofs of concept (PoCs) performed showcase the potential for leveraging SSI for these and comparable identity management processes in financial services. Through decentralised, blockchain based identification, the PoC not only ensured that the technology is secure and is of benefit in client interactions but can also provide enhanced user privacy and greater control over personal data. Overall, the PoC underscored the technology's capacity to redefine identity paradigms, offering a scalable and resilient solution for the challenges of current authentication methods.

To redefine online trust, SSI will require broad acceptance, an enhanced user experience and greater levels of user education.

- **Network effects are paramount** – identity providers must provide access to substantial number of high-value public and private sector use cases from the outset. Additionally, providers need a broad customer base as consumers will be slow to adopt unproven systems.

- **User experience must be prioritised** – abstracting from the technology is paramount for users that are less well versed in the Web3 world (blockchain, wallets, private keys etc.).

- **Education is essential** – to assist users in grasping the benefits of SSI to lessen the inertia when shifting from conventional identity norms.

Banks can assume a pivotal role not only as custodians of customer data in financial services but also in the future, extending their function to managing identity.

1

# Introduction to identity

## 1.1 Identity in a digital world

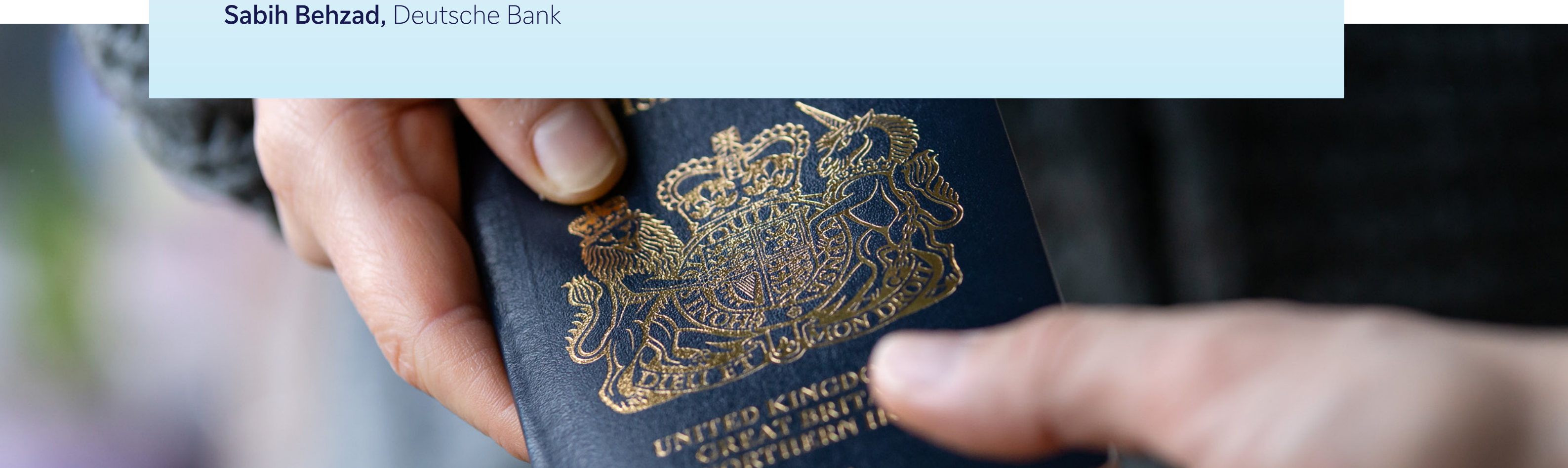
The concept of identity – the distinguishing character or personality of an individual – has been a fundamental feature throughout human history.[1] Thousands of years before our identities were stored digitally in the cloud, humans used language objects and documents to confirm their individuality. By the time of the ancient Greeks, the question "Who are you?" would be answered not only with a name, but personal traits, social standing, and their line of ancestors.[2]

Identity (ID) documents on the other hand have a much briefer history. One precursor to national ID cards was introduced in Napoleonic France as a means of streamlining bureaucracy – and found quick epigones, such as in the Ottoman Empire. Many contemporary ID cards then emerged during The Second World War. While ID cards often form the basis of government services, this is not a global standard. In the US, state-issued ID documents have only followed a common standard since 2005, and no national ID system exists.[3] Globally, 850 million people do not have any identity document.[4] In the analogue world, identity is, therefore, not universal and is somewhat fragmented.

This holds true for a wider definition of identity. The question of an organisational or corporate identity had first been answered in the same wave of bureaucratisation in the 19th century. The UK, for instance, introduced company registration in 1844.[5] Company registers may contain information such as owners, legal name, registration details, director details and business structure, but this may differ depending on a country's legal environment. Furthermore, unlike many features of personal identity, almost every field in a company register is subject to change. Company registers and registration numbers have since remained the non-plus-ultra for corporate identity until very recently.

Amid this all but incomplete ecosystem, a new need for identity emerges. With the rapid digitisation of society, digital identity will form a cornerstone for certain interactions on the internet

> "A bank-issued digital ID enables its corporate clients to access services from third parties that would otherwise be inaccessible due to the costs of onboarding. Of course banks should lead here"
>
> **Sabih Behzad,** Deutsche Bank



But why is a digital identity required for the internet if identity has emerged from state bureaucracy? The internet was originally created as a web of static information, open to anyone. It has since evolved into a more participative internet, where users interact with each other and with service providers. Web services are becoming increasingly embedded into the real world and centred around individual users. At the same time, the internet obscures even basic identity information behind a layer of pseudonymity. A digital identity would enable users to identify themselves to other users on the web – going beyond the original scope of identity. This also extends to organisations and virtual entities that exist solely online. A functional digital identity layer is a significant step towards a frictionless world where corporates and individuals can interact in a trusted manner throughout the online and offline world.

In 2019, The McKinsey Global Institute heralded good digital identity (ID) as a key to inclusive growth. “As an enabler of economic, social, and political activity in digital age, good digital ID is a new frontier in value creation for individuals and institution”, state the consultants in the preface to their report, Digital identification.[6]

Banks have a real opportunity to lead in this value creation and be that enabler, something that Oliver Wyman developed in their paper, *Digital identity – banks must seize the opportunity*, published a year later.[7] “Banks are the right candidate to lead on digital identity because they are still deeply trusted by consumers. And, in combination, as a consortium, they already have the necessary “reach”: a customer base in the tens of millions that comprises the vast majority of economically active citizens,” reflected author Peter Carroll.

“Banks are also deeply trusted by businesses,” reflects Deutsche Bank’s Dominik Dribusch. “They operate as close partners and are integral to client success. With huge amounts of data passing between bank and client – as well as cash, good digital ID not only helps create value for those businesses but protects them from bad actors or fraud,” continues Dribusch.

“A bank-issued digital ID enables its corporate clients to access services from third parties that would otherwise be inaccessible due to the costs of onboarding. Of course banks should lead here,” adds Sabih Behzad.

## 1.2 The evolution of digital identity

While still emerging, the field of digital identity is not exactly brand new. Identity management has grown in importance over the past years due to a sharp rise in the number of digital interactions. According to the MuleSoft/Deloitte 2022 *Connectivity Benchmark Report*, 72% of an organisation's interaction with customers are now digital.[8] The evolution of digital identity until today can be classified into three phases, each giving rise to the next.

### 1.2.1 Phase 1: Centralised identity

During the initial phases of the internet, platforms resolved the identity challenge by granting their users an identity through an account and a password: the account-based identity. Information exchanged in the interactions between that platform and the specific account and password defined the digital identity within that domain.

In this siloed model, users have to maintain many digital identities across numerous online platforms. A study commissioned by password manager NordPass confirms that the average number of passwords a person must remember is one hundred.[9] Compounding this challenge is the dispersion of private data across various platforms, increasing the concerns around data privacy and security and a (perceived) loss of control. Research shows that as few as 10% of consumers feel like they are in complete control of their data and a mere 25% believe that companies handle their personal data responsibly.[10]

Centralised identity remains de facto standard on most websites but has been alleviated by password managers.

### 1.2.2 Phase 2: Federated identity

Prompted by the drawbacks and inefficiencies of the centralised identity model, a more user-friendly solution emerged in the form of federated identity. This phase in identity aimed to alleviate the inconvenience of managing multiple passwords. It also allowed for a portability of (some) online credentials, allowing users direct access to an online platform. Platform providers that rely on federated identity benefit from open standards – making it easy to integrate and manage an identity component – and the guarantees provided by the federated identity provider. In other words, "if Facebook/Meta trusts you, so can I – at the very least you are probably not a robot".

Yet, this evolution retains the challenge of entrusting a select few identity providers such as the tech giants with the centralised management of digital identities and data – a situation that transforms these providers into attractive targets for unauthorised access.

### 1.2.3 Phase 3: Decentralised/self-sovereign identity

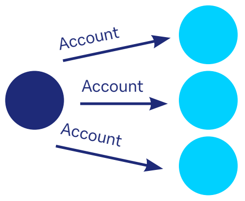
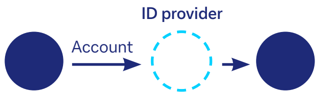
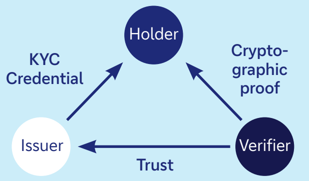
The next phase of identity looks to address this challenge by replacing federated identity providers through a system, known as self-sovereign identity (SSI), which enables identity holders to manage their own digital identities. Rather than storing an identity holder's data remotely at a federated identity provider, its digital identity is kept as cryptographically secured credentials inside a personal wallet. An identity holder may receive a credential, issued by a public body – e.g., representing their ID card or driver's licence. Once stored inside their identity wallet, they can share data contained inside a credential with a verifying party, such as a bank or website provider. Overall, SSI empowers users to have greater control over their digital identities, alleviates the password burden, and ensures that the user's data is only shared with their explicit permission. In turn, verifiers can check the authenticity and validity of data shared through a credential – leading to smoother client onboarding processes and up-to-date user data.

### 1.2.4 ID system archetypes

Until recently the main method of managing digital identity has been the centralised and federated models and there are many instances where these models are used today, each with the challenges summarised below. SSI is still an emerging concept, but we are already seeing how early efforts are transforming the user experience online.

We see this shift from centralised identity models to decentralised models as an essential steppingstone to a more user centric, secure, cost-effective, and interoperable identity management system for the future iterations of the internet.

**Figure 1: ID system archetypes**

| Level of centralisation | Centralised | | Decentralised |
|---|---|---|---|
| **System archetypes** | **Centralised** | **Federated** | **Decentralised/SSI** |
| **Architecture** |  |  |   Holder<br>KYC Credential<br>Crypto-graphic proof<br>Issuer<br>Trust<br>Verifier |
| **Definition** | Single organisation establishes and manages identity | — Trusted third-party services that guarantees a user's identity for another service provider<br>— Single sign on (SSO) | Multiple entities contribute to a decentralised identity. Users manage their own identity |
| **Data ownership** | Centralised – data is owned and controlled by individual organisations | Centralised – data owned by ID provider org and shared with third parties at users' request | Decentralised – data is owned and managed by the user |
| **Strengths** | — Provides security and trust<br>— Technology is universally understood and easily implemented | — Users have access to a broad range of services through a single seamless experience<br>— Semi-portable whereby users can import their basic information into a new app or service | — Single identity with many (verifiable) credentials (e.g., incorporation date, directors' details, ownership) that can be selectively disclosed<br>— Users own and control their data<br>— Instant verification of credentials |
| **Challenges** | — One isolated identity for each platform with single point of failure, increased risk of data breaches<br>— Identity is fragmented, with customers having identity at many third parties that hold various aspects of customer data) | — Complex from a technical and governance perspective<br>— System interoperability causes a disjointed UX<br>— Security and transparency concerns in addition to a high degree of dependence on a single provider | — Complex governance and an evolving landscape<br>— Network effects required which takes time to initiate<br>— Currently, multiple competing platforms, providers, standards |
| **Examples** | Banks, utilities, social media, news publications etc. | Google, Okta, AWS, OneLogin, Microsoft Azure AD, Auth0 | European Blockchain Services Infrastructure (EBSI), Zug ID |

Source: Deutsche Bank

## 1.3 The current state of the digital identity field

### 1.3.1 Key trends

The digital identity field is growing rapidly with varied estimates for the velocity of growth. The 2019 McKinsey Global Institute report noted that by 2030, digital identity had the potential to create economic value equivalent to 6% of GDP in emerging economies and 3% in mature economies, assuming high levels of adoption.[11] Monetary estimates for the market size indicate a global digital identity solutions market size – which was valued at US$25bn in 2021 – projected to reach US$116bn by 2030, growing at a CAGR of 18.6% during the period (2022–2030).[12]

Digital wallets are an important enabler of progress in the identity and payment spaces. Already today, wallets are widely used for digital payments. Juniper research report that in 2023 there were 3.7 billion digital wallet users globally with the expectation that this will exceed 5.4 billion by 2028.[13] A separate study from Juniper found that the value of digital wallet payments will be more than US$16trn in 2028.[14]

Similar to physical wallets, digital wallets do not need to be limited to payments. In Europe, a Thales survey of EU citizens in seven countries found that two-thirds would use a wallet to store their digital identity (rising to three quarters among those who already have some other form of digital identity) additionally two-thirds of Europeans think that a government digital wallet is best, with a third thinking that it should be banks taking the lead.[15]

The digital identity field still undergoes a rapid development. Novel technical approaches get implemented catering for a wide range of use cases, while first industry standards are being defined. Nevertheless, the harmonisation of credential formats, underlying protocols, and wallet infrastructure still pose a key challenge for a greater adoption of digital identity solutions.

### 1.3.2 Public initiatives

Individual digital identity solutions have already been established in a number of regions – however only a few have managed to roll these out at scale. Some of these regions are now looking at the extension of these schemes for corporates. Figure 2 on page 12 provides a summary.

### 1.3.3 Private initiatives

A select few banks have collaborated on establishing KYC utilities to supply corporate identity solutions. Despite no comprehensive offering existing there are a number of utilities that formed, including the SWIFT KYC Registry, Clarient Entity Hub, Invidem (Nordic Banks) in addition to a number of proof of concepts (PoCs) in Europe (with Dutch banks ABN Amro, ING and Rabobank) and the Asia-Pacific region.

Separate to this a number of banks formed private consortia for identity services – examples include ‘itsme’ from a number of Belgian banks for Belgium and recently extended to France, Estonia, Ireland, Italy, Portugal, Romania, Slovakia, Spain, and the United Kingdom. Another recent example from Eight Japanese firms, including banks, announced the formation of a decentralised identity (DID) and verifiable credential co-creation consortium (DVCC).

Industry-leading companies such as Microsoft, Workday, Salesforce, Bosch, SAP, BMW, Novartis and others are exploring SSI to gain a strategic advantage over their competition. Adoption happens globally and in almost every industry (including banking and financial services, insurance, education, commerce, health care, mobility, hospitality, supply chain among others).[16]

Figure 2: Public digital identity solutions

| ID solution | Description | Specific features for corporates |
|---|---|---|
| eIDAS 2.0 | An identity system available to all citizens, residents, and businesses in the EU. Although this framework is expected to prioritise individual digital identity during its initial years, it is noteworthy that it may accommodate the establishment of corporate digital identity in the future and paves the technical foundation for an identity ecosystem | Expected in future |
| iAM Smart | The Office of the Government Chief Information Officer (OGCIO) has been working with the Hong Kong Monetary Authority (HKMA) on a proof-of-concept (PoC) trials and research on the business version of the "iAM Smart", which is an individual digital identity platform | Digital authentication of business identities |
| Canadian digital ID solution | Digital ID and Authentication Council of Canada (DIACC), a non-profit coalition of public and private sector organisations committed to develop Canadian digital identity solutions, launched the Pan-Canadian Trust Framework (PCTF) as "a set of rules and tools designed to help businesses and governments to develop tools and services that enable information to be verified regarding a specific transaction or particular set of transactions" | Verified Organisation Component ("VOC") is the most relevant to corporate digital ID |
| CorpPass | Developed by the Singapore GovTech agency as a centralised corporate digital identity solution for registered businesses in Singapore. Provides a set of credentials which allows individuals acting on behalf of the company to transact with various government agencies online | Unique identifier for organisations and staff |
| IDunion | IDunion aims to create an open ecosystem for decentralised identity management, which can be used worldwide and is based on European values and regulations. The project is funded by the German Ministry of Economics and Climate Actions | Pilot use cases in the field of corporate and product identity |
| GLEIF | The Global Legal Entity Identifier Foundation (GLEIF) was established in June 2014 by the Financial Stability Board. GLEIFs' tasks are to support the implementation and use of the Legal Entity Identifier (LEI). LEIs are linked with corresponding records in OpenCorporates' global database of legal-entity data, thanks a long-standing partnership between the two organisations | Unique identifier for organisations |

Source: Deutsche Bank

### 1.3.4 Other decentralised identity technologies

Credentials stored on blockchain: NFTs (non-fungible tokens) initially designed for the tokenisation of assets, not identity and as a result this approach is less suitable for approaches where data protections apply – but new non transferrable NFTs, 'Soul bound tokens' (SBT) can be useful for services where data protection is not a concern, such as event admission, concert tickets etc. Data is stored on-chain and accessible to all.

SBTs are receiving attention in the Web3 space because they offer a crypto-native way to prove personal facts, which means they can be read by smart contracts. The idea of SBT challenges the traditional NFT model, which allows for easy transferability and trading. It introduces a more personal and authentic dimension to ownership in the digital realm, emphasising the importance of participation, skills, and achievement rather than pure financial transactions. However, implementing and ensuring the non-transferability of these tokens presents technical and privacy challenges that need to be addressed for this concept to fully realise its potential. Given the immutable nature of crypto assets, SBTs may not be changeable or revokable. Moreover, as with many crypto assets, SBTs face an uncertain regulatory landscape.

2

# Self-sovereign identity deep-dive

While decentralised identity frameworks offer a pathway to empower individuals with control over their personal information, their structure is complex, and their use counter-intuitive compared to what we know and rely on now. In this chapter we present a deep dive into the main principles of self-sovereign identity.

## 2.1 Core principles

SSI is underpinned by twelve key principles as defined by the Sovrin Foundation.[17] These principles expand on a vision that was set out by Christopher Allen (a renowned authority on digital identity and also known for his work on the TLS internet standard an end-to-end internet security protocol), for guiding the creation of a new identity system. The Sovrin Foundation twelve principles are set out in Figure 3.

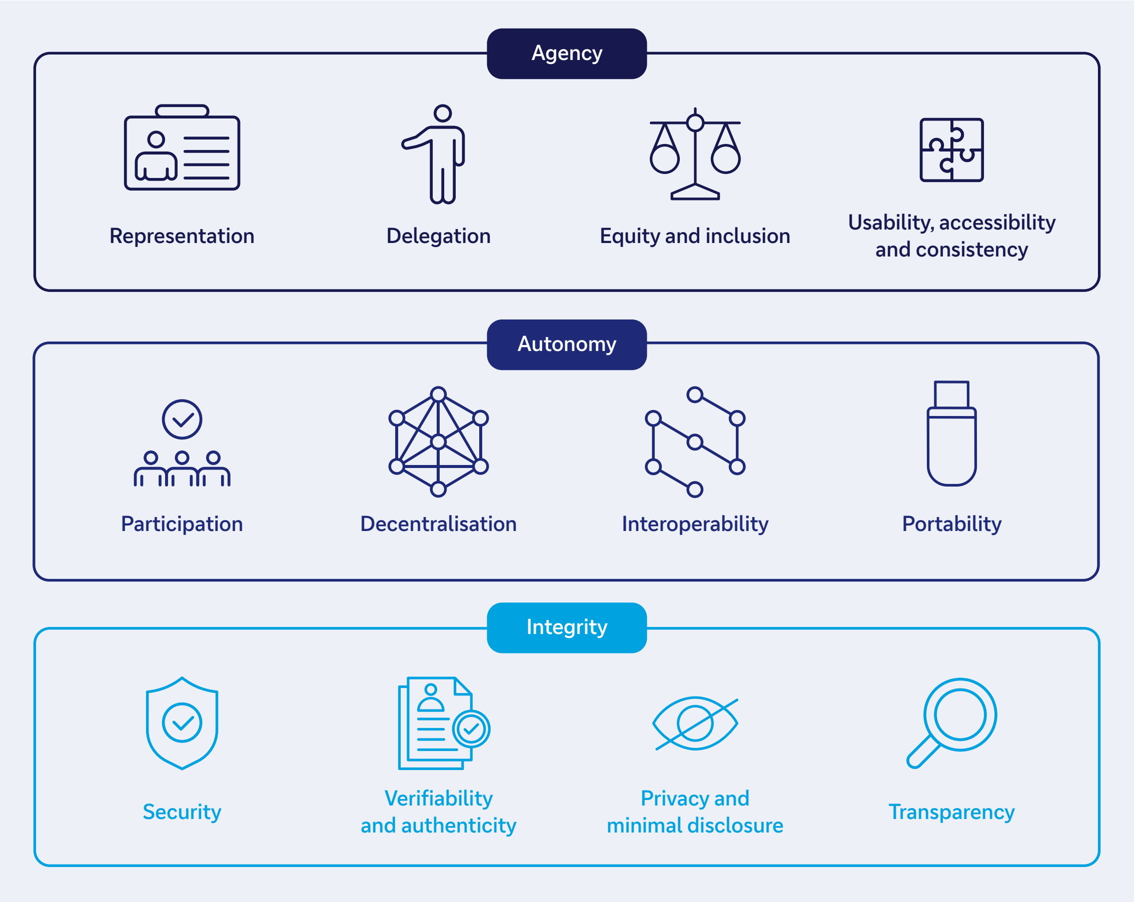
### Figure 3: 12 key principles of a self-sovereign identity ecosystem

| | |
|---|---|
| **Representation** | An SSI ecosystem shall provide the means for any entity—human, legal, natural, physical or digital—to be represented by any number of digital identities |
| **Delegation** | An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity (“Identity Rights Holders”) to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organisations, devices, and software |
| **Equity and inclusion** | An SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope |
| **Usability, accessibility and consistency** | An SSI ecosystem shall maximise usability and accessibility of agents and other SSI components for identity rights holders, including consistency of user experience |
| **Participation** | An SSI ecosystem shall not require an identity rights holder to participate |
| **Decentralisation** | An SSI ecosystem shall not require reliance on a centralised system to represent, control, or verify an entity’s digital identity data |
| **Interoperability** | An SSI ecosystem shall not require reliance on a centralised system to represent, control, or verify an entity’s digital identity data |
| **Portability** | An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice |
| **Security** | An SSI ecosystem shall empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions |
| **Verifiability and authenticity** | An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data |
| **Privacy and minimal disclosure** | An SSI ecosystem shall empower identity rights holders to protect the privacy of their digital identity data and to share the minimum digital identity data required for any particular interaction |
| **Transparency** | An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate |

Source: The Sovrin Foundation

The Sovrin Foundation explains, “These foundational principles of SSI are intended for use by any digital identity ecosystem. Any organisation is welcomed to incorporate these principles into its digital identity ecosystem governance framework provided they are included in their entirety. The Principles of SSI shall be limited only by official laws and regulations that apply in a relevant jurisdiction.” Figure 4 provides a practical summary of their application.

Figure 4: 12 principles of SSI



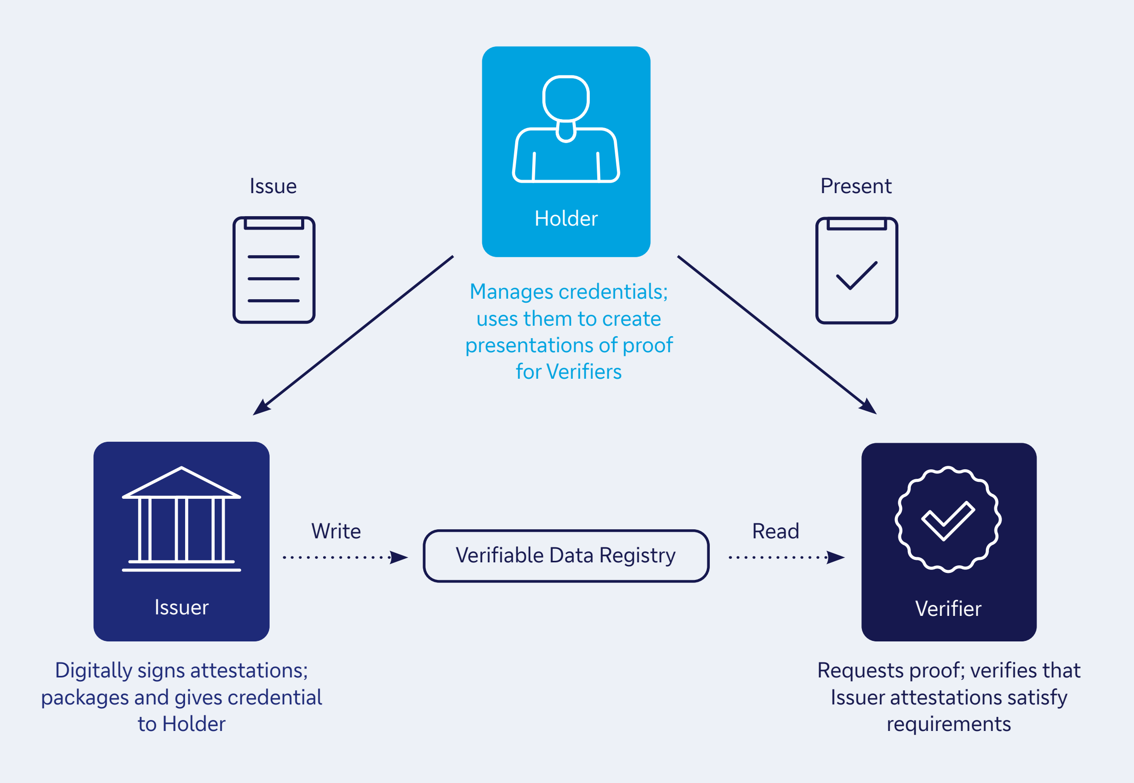
Source: The Sovrin Foundation

## 2.2 Tripartite ecosystem

The vision behind SSI describes an ecosystem that is made up of three parties *(see Figure 5)*:

1. **Identity holder.** Person, legal entity or Internet of Things (IoT) device holding a credential.
2. **Issuer.** Trusted entity by the verifier and the identity holders that issue credentials containing information about the identity holder, e.g., governments, banks or educational institutions.
3. **Verifier.** Entity interested in receiving data contained in credentials presented by the identity holder.

**Figure 5: Parties involved in the SSI ecosystem**


Holder
Issue
Present
Manages credentials; uses them to create presentations of proof for Verifiers
Issuer
Write
Verifiable Data Registry
Read
Verifier
Digitally signs attestations; packages and gives credential to Holder
Requests proof; verifies that Issuer attestations satisfy requirements

Source: Deutsche Bank

In this SSI ecosystem the verifier can interact in a trust less manner with the identity holder because the trust is being provided by the issuer (a real-world trusted party by the verifier) and transfer to the identity holder in the form of a tamper-proofed verifiable credential.

## 2.3 How the SSI ecosystem solves problems

Corporates today are often faced with lengthy approval processes, multiple requests for the same information and limited or no visibility into the progress of the Know Your Customer (KYC) process. Transitioning from traditional methods of identification to decentralised digital identity offers several immediate benefits to address these challenges. The most significant benefits that digital identity solutions offer centre on improved user experience, faster turnaround times, reduced operational costs and reduced fraud.

Primarily, digital identity offerings improve the customer experience for corporates in their online interactions with their banks. Financial institutions face increasingly stringent rules on gathering, retaining and updating KYC data, which translates to a struggle for corporates – with the burden placed on them due to many requests for information from each financial institution that they have a relationship, and in varying formats.

Anecdotal evidence suggests that digital identity could shorten the time required for a financial institution to complete its KYC, customer due diligence (CDD), anti-money laundering (AML)/ combating the financing of terrorism (CFT) and other due diligence procedures for onboarding a new corporate customer – from typically reported ranges of several weeks, to within a few days or even less for small and medium-sized enterprises (SME).[18] The current process is a significant challenge for all parties and fraught with issues, and 84% of businesses have had a bad experience of KYC processes according to a Reuters survey.[19] Another issue is the cost of the current process can exclude smaller businesses because the resulting business is less likely to be profitable – thus contributing to financing gaps.[20]

The enhancement to the customer experience is attained through a streamlined onboarding process, whereby physical documentation is replaced with verifiable credentials. This reduces human intervention and reduces repeat requests for information. The streamlined process catalyses a reduction in operational costs for corporates, thus boosting efficiency levels and leading to more optimal deployment of resources. It should be noted that the time can vary greatly depending on the banking products concerned, in addition to the geographies involved. The processes are often complex, due to financial institutions writing many client contracts individually to comply with differences in local regulations.

Beyond this, a widely trusted corporate digital identity can also have benefits for FIs including reduced complexity and thus operating costs, reduced fraud,[21] improved accuracy and potential revenue opportunities from new digital identity business models.

# 3

# Polygon ID

**This technical section, authored by the Polygon ID team, provides a detailed explanation of what SSI frameworks are before setting out the architecture of the Polygon ID offering.**

## 3.1 SSI frameworks: A primer

Before delving into the details about Polygon ID, the SSI toolkit featured in this paper, let's try to understand more about the basic building blocks of any self-sovereign identity solution.

Self-sovereign identity is a specific form of digital information, and all digital information relies on data. Data is dynamic: it needs to be stored, often in databases, updated by the owner, and manipulated by software logic in order to become useful over its lifecycle. A special kind of software logic used for self-sovereign identity, is what we call a self-sovereign identity framework. Think of it as a suite of software tools needed for operational use of decentralised identity.

### 3.1.1 The importance of cryptography

Because SSI frameworks attempt to balance usability with privacy and security, they heavily rely on cryptography, the use of complex mathematics as a way of keeping information safe so that only the people meant to see it can understand it.

The principles of basic cryptographic operations have remained unchanged for decades, and modern commerce and banking – indeed the internet itself – would be entirely unusable without them. They are:

1. **Encryption/decryption:** Encryption transforms your personal information into a secret code, safeguarding it from unauthorised access. Decryption is the process of using a special key to decode this information, making it readable again. This ensures that only those with the correct key can access and understand the encrypted data, keeping sensitive information secure from prying eyes.

2. **Hashing:** A cryptographic hash is like a digital fingerprint for data. Imagine you have a letter that you want to keep private, but you also want to make sure it hasn't been tampered with. You pass the letter through a special machine (the cryptographic hash function) that reads every word and turns it into a unique, short code –let's call it the letter's fingerprint. If the data changes, so does the fingerprint, and thus the recipient can detect tampering.

3. **Digital signature and verification:** A digital signature is like a tamper-proof seal on a document but in digital form. It verifies the document's sender and confirms it hasn't been altered after signing. By using a unique digital key, the sender "signs" the document. When you receive it, you can use a matching public key to check the signature. If it matches, you know the document is genuine and unchanged, ensuring trust and authenticity in digital communications.

   While all of these are relevant, digital signatures are the most important building block for self-sovereign identity frameworks and blockchain networks that SSI often relies on. Each blockchain transaction is, indeed, merely a string of information specifying origin, recipient, amount, and some freeform data, digitally signed by the initiating party, and verified by the network. But how do we create digital signatures?

### 3.1.2 Not your keys, not your identity

Notice the use of phrases “special key” and “unique digital key” in the previous section. These keys indeed exist, and we call them cryptographic keys. Without them, we couldn’t encrypt, decrypt, or sign digitally. The keys themselves seem like long strings of random characters – in other words, gibberish – but they are as critical to our digital lives as our house keys are to our physical comfort and security.

Cryptographic keys (in our case these are organised into pairs by a set of policies and procedures called Public Key Infrastructure – PKI) were the original digital ID and privacy system for the internet. They helped ensure that when you’re dealing with someone online, they are who they say they are. Your counterparties proved their identity by the use of their private cryptographic keys: if they didn’t have these keys, they could never have decrypted a piece of information you sent to them, or digitally signed a piece of information that they sent to you.

Cryptographic keys are now omnipresent: Most of our personal internet connections are encrypted, especially ones relating to private information (e.g. email), or financial transactions (e.g. card payments, online banking); our passwords are – at least –hashed, if not hashed and encrypted; browsers prevent us from accessing a website whose keys are out of date, or unattested to by a certificate authority (itself an ancient identity mechanism which is both primitive and prevalent); virtually every enterprise system designed in the last decade encrypts all of its interfaces, and digitally signs all of its payloads. Without cryptographic keys we wouldn’t dare use the internet as freely as we do now, for fear of breach of privacy and financial loss.

Where PKI applies, cryptographic keys come in pairs: public key and private key. A key pair is like a lock and key for your digital information. One key locks (encrypts) your information so no one else can read it, while the other key unlocks (decrypts) it. This ensures that only you and the intended recipient can access the information. Keys are also used to sign information before sharing it with someone else.
It follows from the above that anyone is allowed to have your public key, while only you can have your private key (otherwise someone else might pretend to be you).

So, if the sanctity of your private keys is crucial to your identity, wealth, and privacy, how do you protect them? That is the perennial problem, because a cryptographic key that is perfectly protected is perfectly unusable. A cryptographic key can be stored on anything from a scrap of paper to a highly secure computer system called a Hardware Security Module (HSM), but for purposes of usability most users rely on cryptographic wallets.

A cryptographic wallet acts like a secure digital keychain, holding the cryptographic keys you use to access your digital assets (including your self-sovereign identity) online. When you want to perform a cryptographic operation, your crypto wallet uses these keys to securely sign, encrypt or decrypt arbitrary data, ensuring that only you can access and manage your assets.

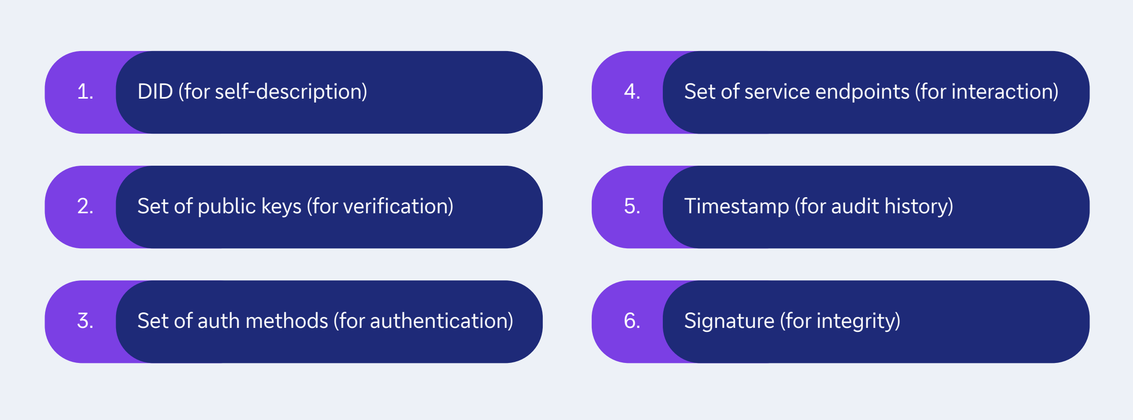
Your wallet can be managed by yourself (where you truly own your identity with the associated responsibility of the custody of your cryptographic keys), or by a third party (e.g. your bank) that enables day to day use, but also recovery in case of loss.

### 3.1.3 Trust the system, not the actors

As mentioned previously, self-sovereign identity relies on two types of data structures for its functionality: decentralised identifiers (DID) and verifiable credentials (VC).

Decentralised Identifiers are a way for entities to identify themselves online without relying on a central authority, like a social media platform or a bank. It gives individuals more control and privacy, allowing them to prove who they are on the internet on their own terms. A DID can relate to a natural person, a legal entity, or an IoT device. DIDs do not, however, prove anything about the entity – they are just uniquely linked to the owning entity.

Figure 6: The standard element of a DID document



1. DID (for self-description)
2. Set of public keys (for verification)
3. Set of auth methods (for authentication)
4. Set of service endpoints (for interaction)
5. Timestamp (for audit history)
6. Signature (for integrity)

Source: W3C

The DID specification, maintained by the World Wide Web Consortium (W3C), provides a framework for expressing the abstract concepts and properties of a DID, while individual DID methods represent a set of rules that explain how to create, update, and deactivate a decentralised digital identity on a specific network or system. Each method is designed to work with specific systems or protocols and can be used to interface with blockchains, distributed ledgers, or other types of decentralised data stores that can support the operations required by the DID method.

For instance, a DID method might define:

— Syntax. The format of the DID and DID documents specific to the method.

— Operations. How to perform the CRUD operations (create, read, update, and delete) for DIDs and their corresponding DID documents within the system.

— DID document structure. The structure and possible attributes of a DID document, which typically includes public keys, authentication methods, service endpoints, and other metadata related to the DID subject.

— Security and privacy considerations. Protocols to ensure the integrity, confidentiality, and privacy of the DIDs and DID documents.

Verifiable Credentials, on the other hand, are digital documents (like a digital driver's licence, university degree, or employment verification) that are cryptographically signed and can be instantly verified anywhere in the world. They are issued by a trusted entity and attributed to the owner of the identity, who can then share them as needed to prove certain aspects of their identity or qualifications without revealing all their personal information. VCs are expressed in a way that is tamper-proof, which means that any unauthorised alteration of the credential after it has been issued can be detected.

The key components of a verifiable credential include:

— **Issuer identity.** The DID or another identifier of the entity that issued the credential.

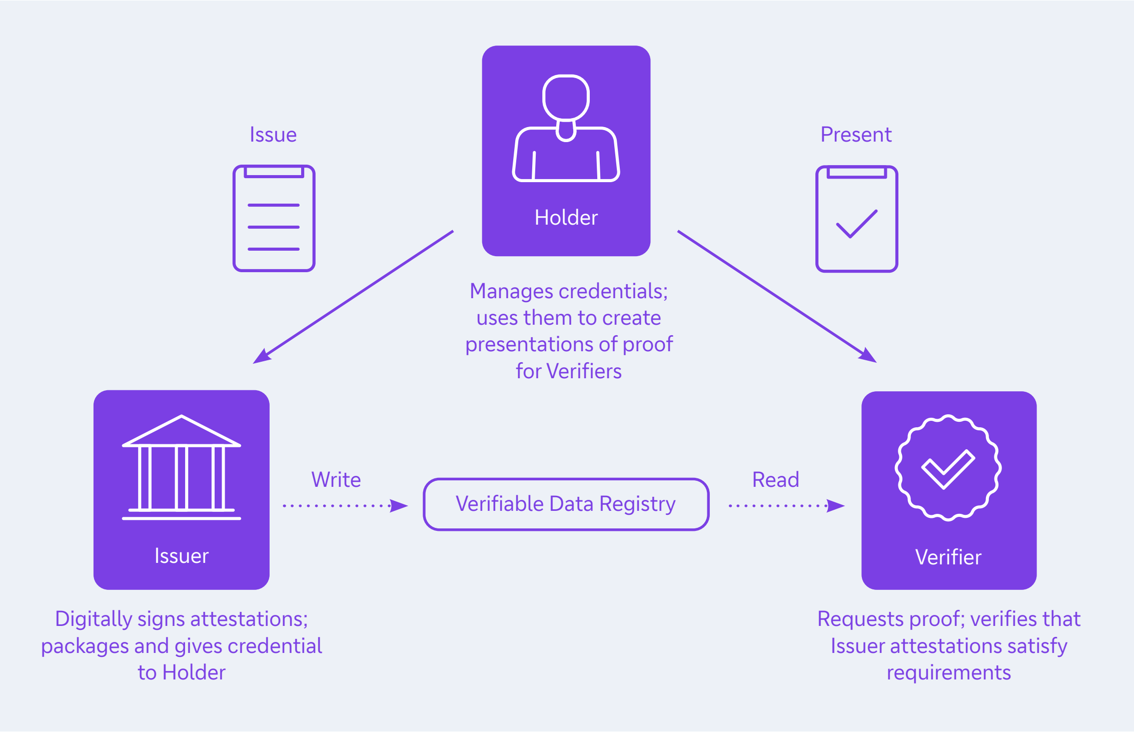
— **Subject identity.** The DID or another identifier of the entity the credential is about.

— **Claims.** The statements made by the issuer about the subject.

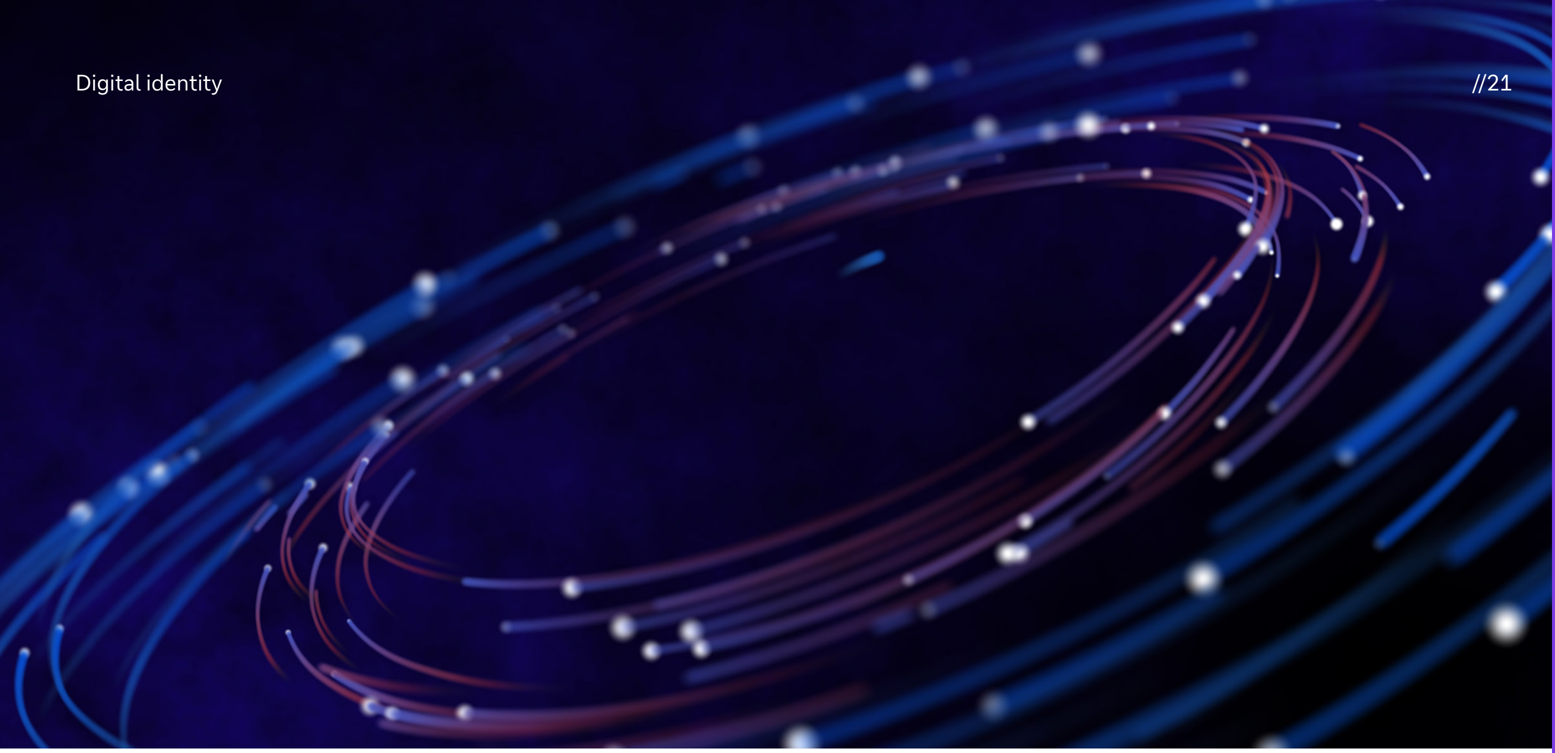
— **Proofs.** Cryptographic evidence such as digital signatures that can be used to verify the claims and the identity of the issuer.

The relationship between DIDs and VCs is symbiotic. DIDs provide a secure and privacy-preserving foundation for identity on the internet. When a DID is used in conjunction with VCs, it allows individuals to prove who they are and that their credentials are legitimate without having to disclose the credential itself or rely on a central authority for verification. This process ensures that personal data remains in the control of the individual, enhancing privacy and security in digital transactions and interactions.

### Figure 7: Parties involved in the SSI ecosystem


Issue
Holder
Present
Manages credentials; uses them to create presentations of proof for Verifiers
Issuer
Write
Verifiable Data Registry
Read
Verifier
Digitally signs attestations; packages and gives credential to Holder
Requests proof; verifies that Issuer attestations satisfy requirements

Source: Deutsche Bank



Together, DIDs and VCs form the backbone of self-sovereign identity frameworks that give individuals more control over their personal information, reduces the risk of identity theft, and simplifies the process of proving personal credentials in a secure and verifiable manner.

As useful as they are, DIDs and VCs are merely data, and data needs to be accessed and maintained in a secure manner. For their use to be practical, we need what is known as a Verifiable Data Registry.[22]

In essence, the Verifiable Data Registry is a key infrastructure element that underpins the trust model of SSI, enabling individuals and entities to control and share their identity information securely and privately, without depending on any central authority. It often leverages blockchain to ensure that data is immutable, transparent, and resistant to tampering.

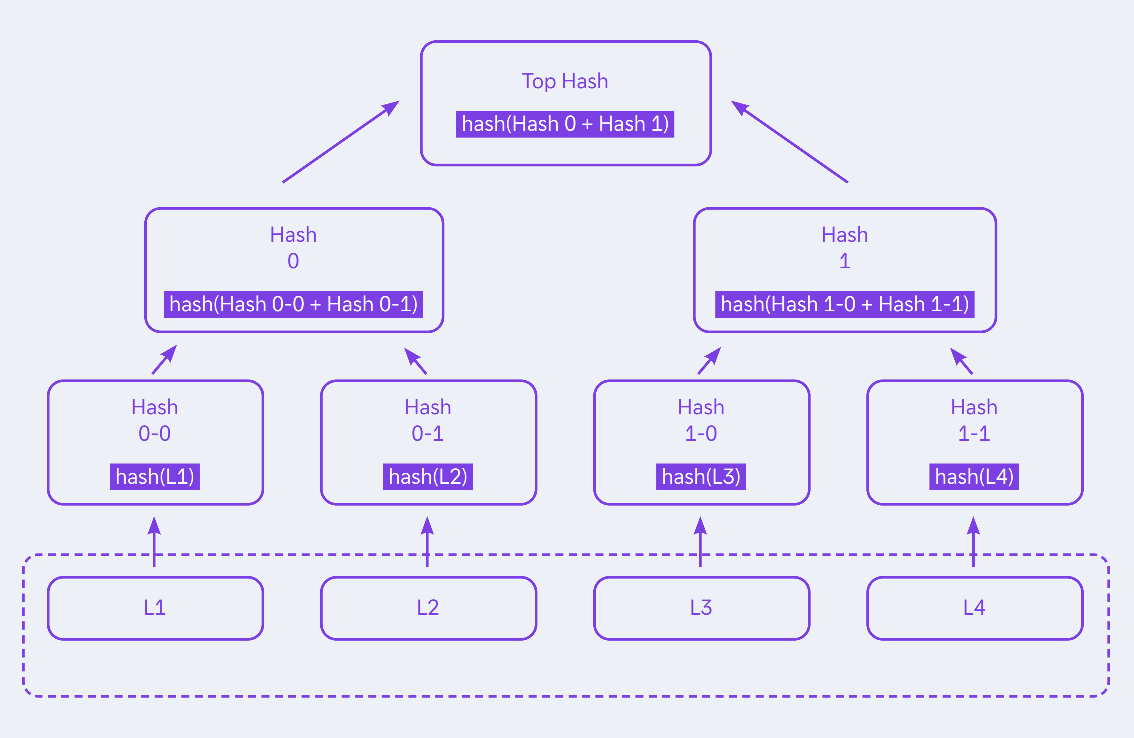
Think of blockchain as a database that is great at maintaining data integrity whilst being accessed by multiple unknown parties: a digital ledger or record book that's shared across many computers, and designed to increase transparency while eliminating tampering. Each entry in the ledger is cryptographically protected and verified, making it immutable. This technology is behind cryptocurrencies such as Bitcoin and Ethereum, and can make financial transactions safer and more transparent. Because of that it is increasingly finding use in the regulated financial services industry.

Within a blockchain, data is organised into "Merkle trees". These are cryptographically secured hierarchical data structures that let you quickly check if a specific name is on the list without going through each leaf of the tree. It is precisely within those Merkle trees that we store references to DIDs and VCs, their histories and validity, available for anyone to easily check the veracity of someone's claim.

In other words, with the help of DIDs, VCs and blockchain, we invert the conventional wisdom: instead of having to trust individuals and institutions (who sometimes abuse our trust), we can now trust the system because it has been designed so it "can't be evil".[23]

> "With the help of DIDs, VCs and blockchain, we invert the conventional wisdom: instead of having to trust individuals and institutions (who sometimes abuse our trust), we can now trust the system because it has been designed so it "can't be evil""
>
> **Boris Spremo,** Polygon ID

Figure 8: Merkle tree data structure



Source: Wikipedia

### 3.1.4 Essential processes

Now that we have defined the key building blocks and actors for self-sovereign identity, let us briefly define how they interact together. Below you can see a list of key processes in the SSI lifecycle:

**Identity creation.** Holders create their digital identity on a decentralised network. This involves generating a unique identifier, often in the form of Decentralised Identifiers (DIDs), that does not rely on any centralised authority for validation or control.

**Claim issuance.** Trusted organisations or entities (Issuers) issue digital claims or credentials (e.g., a digital diploma, driver's licence, or employment verification) to the individual. These credentials are cryptographically signed, making them tamper-evident and verifiable.

**Credential storage.** Holders store their credentials securely in a digital wallet or a similar personal repository. This wallet is protected by cryptographic keys only the individual controls, ensuring that only they can access or share their credentials.

**Credential sharing.** When a Holder needs to prove something about themselves (e.g., age, qualifications), they share their verifiable credentials selectively with others.

**Verification.** The party receiving the credential (Verifier) checks its authenticity and integrity. They use public keys to verify the digital signature on the credential, confirming it was issued by a trusted entity and has not been altered.

**Revocation and update.** Issuers have the means to revoke or update credentials. Revocation lists or status registries are updated to reflect changes, ensuring that verifiers can check not just the validity but the current status of any shared credential.

**Consent management.** Throughout this process, the Holder's consent is paramount. They control which credentials to share, with whom, and for how long, ensuring privacy and data minimisation principles are upheld.

## 3.2 What is Polygon ID?

Polygon ID is a self-sovereign identity (SSI) framework. As a reminder (*see section 3.1*) this is a set of tools for developers that can be used to "facilitate trusted and secure relationships between apps and users".[24] Polygon ID is an implementation of the iden3 protocol, which has been in development since 2018. The protocol has a strong focus on privacy, decentralisation and user data self-sovereignty. Developers can use it to enable the exchange of cryptographically secured verifiable credentials and the blockchain. Polygon ID supports both the W3C open-source identity standards[25] and the ability to be integrated with common types of blockchains.

In February 2023, Polygon ID registered its own DID method (did:polygonid / did:iden3 Method Specification) with the Decentralised Identity Foundation, and its implementation is based on the use of decentralised identifiers and verifiable credentials (VCs).[26]

### Key definitions

**Verifiable credentials.** A set of tamper-evident claims and metadata that cryptographically prove who issued it

**Iden3 protocol.** A next-generation private access control based on self-sovereign identity, designed for decentralised and trust-minimised environments

Polygon ID is being developed by Polygon Labs, which creates Ethereum scaling solutions. Since 2017, the Polygon protocols have seen widespread adoption with tens of thousands of decentralised apps, unique addresses exceeding 391 million, 1.9 million smart contracts created and 3.3 billion total transactions processed since inception. In addition to Polygon ID, Polygon Labs solutions include Polygon PoS (an Ethereum scaling solution), Polygon zkEVM (a roll-up on Ethereum), and Polygon Chain Development Kit (a software development kit for building custom app-chains). The existing Polygon solutions are used by some of the largest financial institutions as well as enterprises and Web3 projects. While Deutsche Bank is on a proof of concept journey (hence this paper), marquee users include HSBC, Siemens, ABN Amro, Monetary Authority of Singapore (as part of project Guardian), Blackrock, Mastercard, Stripe, Hamilton Lane, Franklin Templeton, Mirae Asset Management, and more.

*The Polygon ID team recently spun off from Polygon Labs and is now operating as an independent entity.*

### 3.2.1 The magic of zero knowledge cryptography

What sets Polygon ID apart from other SSI frameworks and makes it uniquely suitable for financial markets use cases, is the use of Zero-Knowledge Proofs. Zero-Knowledge Proofs (ZKPs) are a cryptographic method that allows one party (the prover) to prove to another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. This is akin to proving you have the answer to a puzzle without revealing what the answer actually is.

**Zero-Knowledge Proofs (ZKPs)** are a cryptographic method that allows one party (the prover) to prove to another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself.

In the context of SSI, ZKPs offer a powerful tool for enhancing privacy and security in the way personal information is shared online. For example, ZKPs allow individuals to share proof of certain attributes (e.g., age, nationality, or net assets) without revealing the actual data. You can prove that you are a qualified investor without revealing any material information about yourself.

If ZKPs sound a little bit like sorcery, then they must be, albeit in the way that Arthur C. Clarke once described it: “Any sufficiently advanced technology is indistinguishable from magic”.

Here are 3 key benefits of using ZKPs for SSI in financial services:

— Trust and Verification. ZKPs provide a way for credentials to be verified without needing to see the credentials themselves; building trust between parties in digital transactions, as verifiers can be confident in the authenticity of the claims being made.

— Increased Security. Since ZKPs do not require the sharing of actual data, the risk of sensitive information being intercepted, stolen, or misused is significantly reduced. This makes identity verification processes more secure. ZKPs can streamline verification processes by reducing the need for extensive data exchanges.

— Empowering Individuals and Businesses. By allowing people to prove aspects of their identity without revealing the underlying data, ZKPs put control back in the hands of the individual. This aligns with the core principles of SSI, which emphasise user control, consent, and autonomy over personal data.

Zero-Knowledge Proofs, therefore, play a crucial role in realising the vision of Self-Sovereign Identity for financial institutions, enabling more secure, private, and efficient interactions in the digital world.

### 3.2.2 How Polygon ID makes use of ZKPs

Connecting the concepts introduced in previous sections with the key processes in the SSI lifecycle, we can see how the use of ZKPs has helped to implement a solution aligned with the core principles of SSI:

**Polygon ID uses sparse Merkle trees to quickly prove inclusion and exclusion of keys and credentials, as well as proving which credentials have been revoked via an on-chain revocation tree published by the issuer, more details available in the Iden3 protocol documentation.**

Identity creation. Each identity has a Genesis ID, the initial identity state, from which the original DID is being derived. Using Zero-Knowledge Proofs the identity can prove that it has control over a set of keys. This mechanism decouples the identity from the keys and allows for creation of additional identifiers (DIDs or profiles) and key rotation, which improves security (and is equivalent to periodically changing the lock on your front door).

Claim issuance. As a Polygon ID wallet holder, the user can expose any of the DIDs controlled by the holder to which they would like to have their credential attached to. Once a verifiable credential is issued (in the form of a special data structure called JSON-LD), the credential is then stored locally by the holder and the attributes of the credential are added to a local Merkle tree (a process called "Merklisation") which allows the generation of ZK proofs at a later stage.

Credential querying and sharing. At a later stage, the Polygon ID wallet holder can interact with a verifier that can ask queries about any of the credential attributes by using the ZK query language defined by the protocol. These queries can take the form of true/false (e.g., an answer to question "Are you eligible to operate a motor vehicle?"), range values (e.g. "Are you between the ages of 18 and 25, which would place you in the category of higher risk drivers, and thus increase your premiums?"), or comparison values (e.g. "Is your age now higher than 80, which means you have to take a medical assessment before renewing a driving licence?"). The credential holder will then use the Merklised values from their credentials and input the information into ZK logic to generate the cryptographic proof from their device, without revealing any personal information.

Additionally, the verifier can also request to obtain a set of field(s) from the credential by requiring the holder to perform a selective disclosure of the information.

The usage of Merkle trees and ZKPs also allows the credential holder to use any of the identifiers attached to their wallet when presenting the ZK proof or selective data disclosure. The presentation also includes an additional Merkle tree proof demonstrating that the credential has not been revoked.

Verification. The verifier upon receiving the proof validates the correctness of the proof by running it through ZKP logic with only the public input values, as well as verifying that the credential has not been revoked by checking that Merkle tree proof is valid and comparing it to the issuer's on-chain revocation tree.

The proof can also be submitted to an on-chain verifier (smart contract) that will verify the validity of the proof received. This allows proofs derived from off-chain credentials to be used in on-chain interactions.

Revocation and update. Each issuer has a claims tree and a separate revocation tree. An issuer can specify that a claim is no longer valid by adding the revocation nonce of the original claim as a leaf in its revocation tree.[27]

A credential issuer can also update a credential after it has been issued, this could be relevant for credentials that are going to expire or whose data can change over time, such as a credential related to a credit score, account balance or non-inclusion in a sanctions list. This feature called "dynamic credentials" is implemented via a service that is integrated on the issuer's server, and the refresh protocol is implemented on the wallet holder's device.

Consent management. As part of user awareness, the Polygon ID enabled wallet notifies the user when credentials are being provided by third parties, as well as when ZK proofs from their credentials are requested by verifiers.

Of course, there is more than meets the eye. As complicated as the use of SSI may seem to the reader of this paper, the real complexity runs much deeper, and requires careful design to cover all eventualities. Identity, after all, is a major pillar of our lives, possessions, and businesses, and the status quo is unable to cope with the increasing demands of modern societies.

### 3.2.3 Why Deutsche Bank and Polygon ID?

After almost a decade of institutional experimentation and limited production deployments, it has become clear that the next generation of financial markets infrastructure will rely on blockchain technology. To fully deliver on the promises of increased capital efficiency, reduced costs, and greater regulatory compliance (not to mention a plethora of net-new innovations such as autonomous assets and full vertical integration of portfolios and balance sheets), a decentralised, private, and reusable representation of digital identity is a necessity.

Polygon ID is particularly well suited for the purpose because it facilitates both privacy and interoperability through the use of zero-knowledge technology. Zero-Knowledge Proof (ZKP) technology is at the forefront of the Polygon offering, enabling the ability to cater for data privacy requirements which is of utmost importance for banks – for instance a bank could verify a user's eligibility for a service without knowing specific details of the user's identity.

It is one of the main reasons it has been chosen as the partner for this proof of concept (PoC) where our joint goal is answering the following questions:

1. Can decentralised identity and zero-knowledge technology serve existing KYC/AML needs, and thus fulfil the basic compliance requirements?

2. Can decentralised identity facilitate next-generation FMI, such as institutional DeFi and fund tokenisation?

Achieving positive answers to these questions opens the space for further experimentation with the entire FMI/FI value chain, which will eventually lead to the emergence of improved financial markets infrastructure, and new asset classes.

4

# Proof of concept (PoC) activity

The intention and scope of the PoC activity focused on developing the technical groundwork for potential use cases related to the usage of digital identity/SSI frameworks, both from an on- and off-chain perspective. Commercial drivers and incentive schemes are equally important, but a holistic analysis goes beyond the scope of this project and summarising paper which only describes the general dynamics and considerations. As such, Web3 use cases are a natural starting point as the identity flows need to fit into a purely digital and often self-controlled environment. However, also use cases in existing (banking) processes could benefit from SSI solutions – e.g., in relation to client onboarding in KYC processes.

### Key definitions

**Web3.** Can be considered as the next generation of the world wide web which is based on blockchain technology and a decentralised virtual economy where the user is at the centre having full ownership and control over personal data and virtual assets being shared and traded

**Off-chain.** Off-chain transactions are confirmed outside of the main blockchain network, often resulting in a cheaper and faster process for the user

**On-chain.** On-chain transactions take place on the blockchain, the public ledger that keeps track of every transaction

## 4.1 Digital identity for traditional onboarding and ongoing KYC processes

Establishing trust between organisations is time-consuming and cost-intensive, caused by manual, paper-based and labour-intense KYC processes. SSI-based digital identity provides banks with a major opportunity to address the challenge of KYC during new client onboarding. Clients would receive their KYC files back as a verifiable credential, which they then can use at any other (financial) institution to quickly open an account. The relying bank can draw upon the KYC credential and either onboard the new client right away, or perform automated screenings given that they have a complete data set to hand. This poses a significant cost saving potential. Beyond mere cost reduction, a corporate digital identity scheme can lead to fewer days to revenue, improved client retention and an overall improved customer experience.

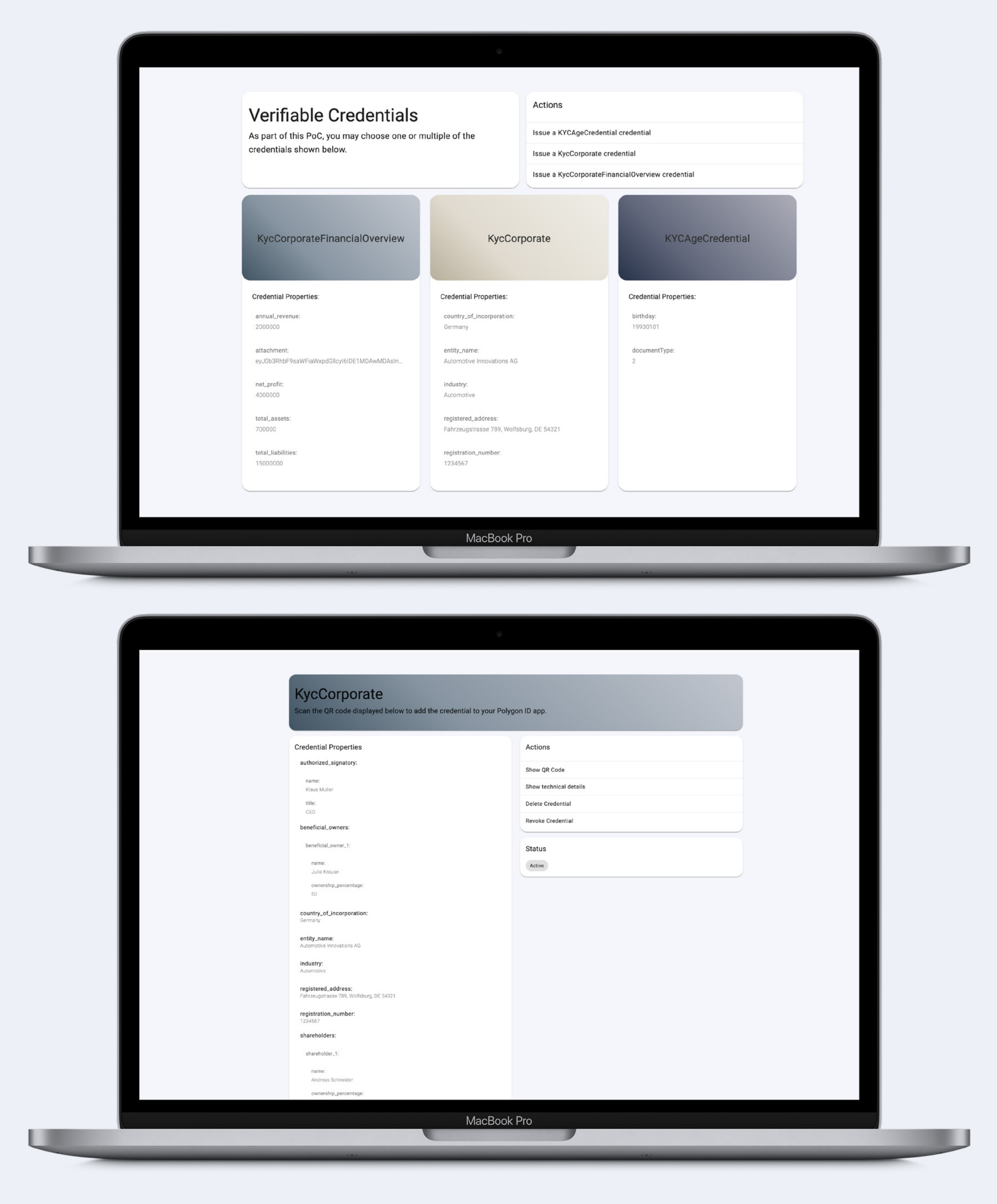
In addition to process improvements, a bank-issued digital ID can also enable its corporate clients to access services from third parties that would otherwise be inaccessible due to the costs of onboarding. For example, where a start-up is offering a financial service that is not in the issuing bank's product portfolio, a corporate client could utilise a KYC credential to onboard to the start-up and gain access to the product. Previously, this would not only have come at the expense of a lengthy onboarding process but would also often fail at the high economic burden of new client onboarding.

Finally, the identity holder is not limited to applications in financial services but is free to present the credential in any situation that they deem appropriate. For example, they may use the KYC credential to identify suppliers or buyers along the supply chain.

### 4.1.1 Technical overview

As part of the PoC's KYC use case, a software prototype was implemented, that integrated core components of Polygon ID's product offering. Most notable, the prototype supports the issuance of credentials to identity holders and the generation of verification requests requiring identity holders to disclose information from previously received credentials.

## Figure 9: Issuance of credentials and example of a corporate credential



Verifiable Credentials

As part of this PoC, you may choose one or multiple of the credentials shown below.

Actions

Issue a KYCAgeCredential credential

Issue a KycCorporate credential

Issue a KycCorporateFinancialOverview credential

KycCorporateFinancialOverview

Credential Properties:

annual_revenue:
2000000

attachment:
eyJ0b3RhbF9saWFiaWxpdGllcyI6IDE1MDAwMDAsIn...

net_profit:
4000000

total_assets:
700000

total_liabilities:
15000000

KycCorporate

Credential Properties:

country_of_incorporation:
Germany

entity_name:
Automotive Innovations AG

industry:
Automotive

registered_address:
Fahrzeugstrasse 789, Wolfsburg, DE 54321

registration_number:
1234567

KYCAgeCredential

Credential Properties:

birthday:
19930101

documentType:
2

KycCorporate

Scan the QR code displayed below to add the credential to your Polygon ID app.

Credential Properties

authorized_signatory:

name:
Klaus Muller

title:
CEO

beneficial_owners:

beneficial_owner_1:

name:
Julia Krause

ownership_percentage:
50

country_of_incorporation:
Germany

entity_name:
Automotive Innovations AG

industry:
Automotive

registered_address:
Fahrzeugstrasse 789, Wolfsburg, DE 54321

registration_number:
1234567

shareholders:

shareholder_1:

name:
Andreas Schneider

ownership_percentage:

Actions

Show QR Code

Show technical details

Delete Credential

Revoke Credential

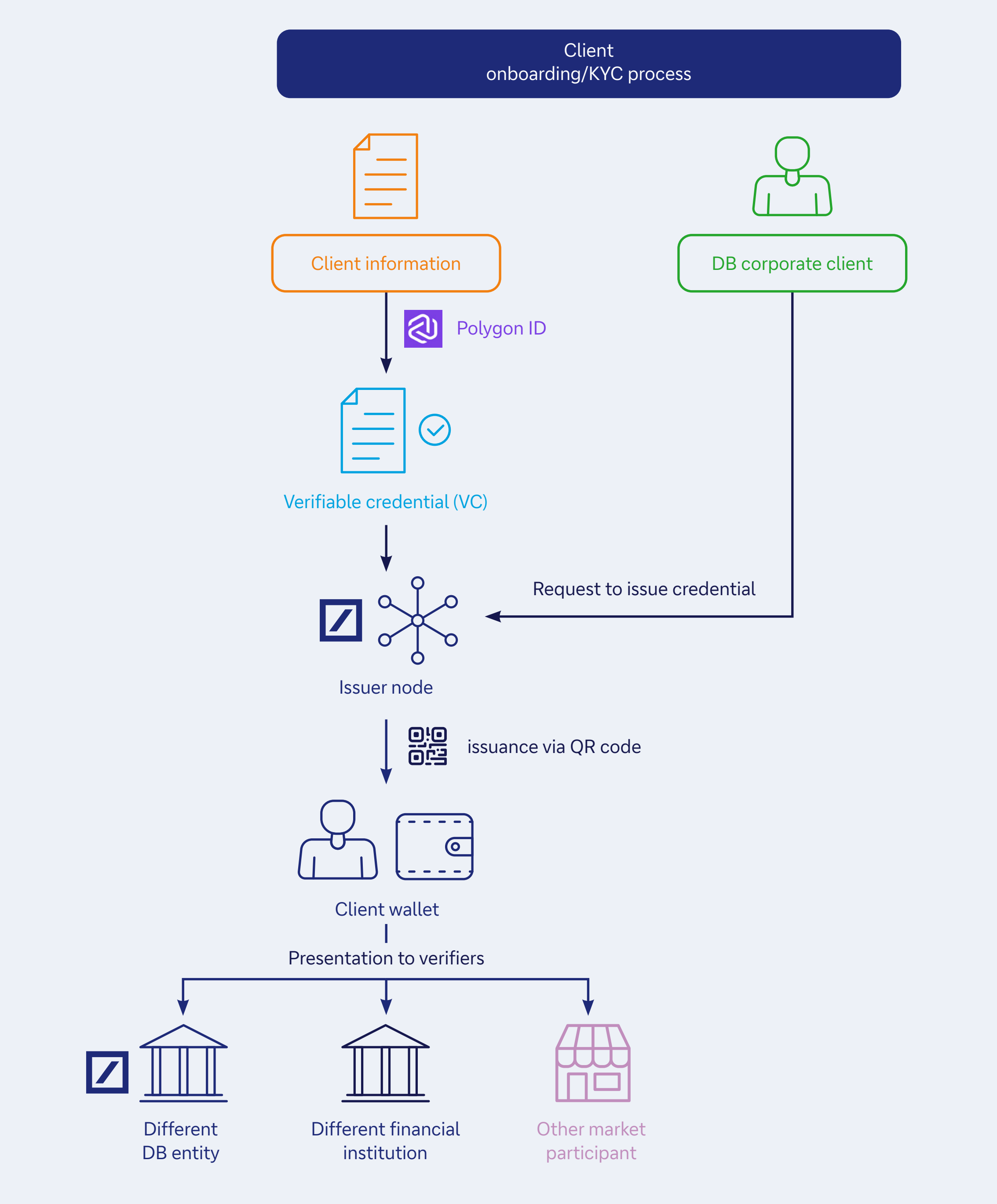
Status

Active

Source: Deutsche Bank

For issuing credentials the prototype relies on Polygon ID's self-hosted issuer node, which provides an API (application programming interface) for importing, creating, and provisioning credentials. Once a credential is created an invitation to accept it can either be sent as deep link or QR code to the identity holder. The invitation as QR code can be sent via email or as in the PoC, displayed on a website. A credential holder can in turn scan the credential invitation and thereby add a credential to its identity wallet.

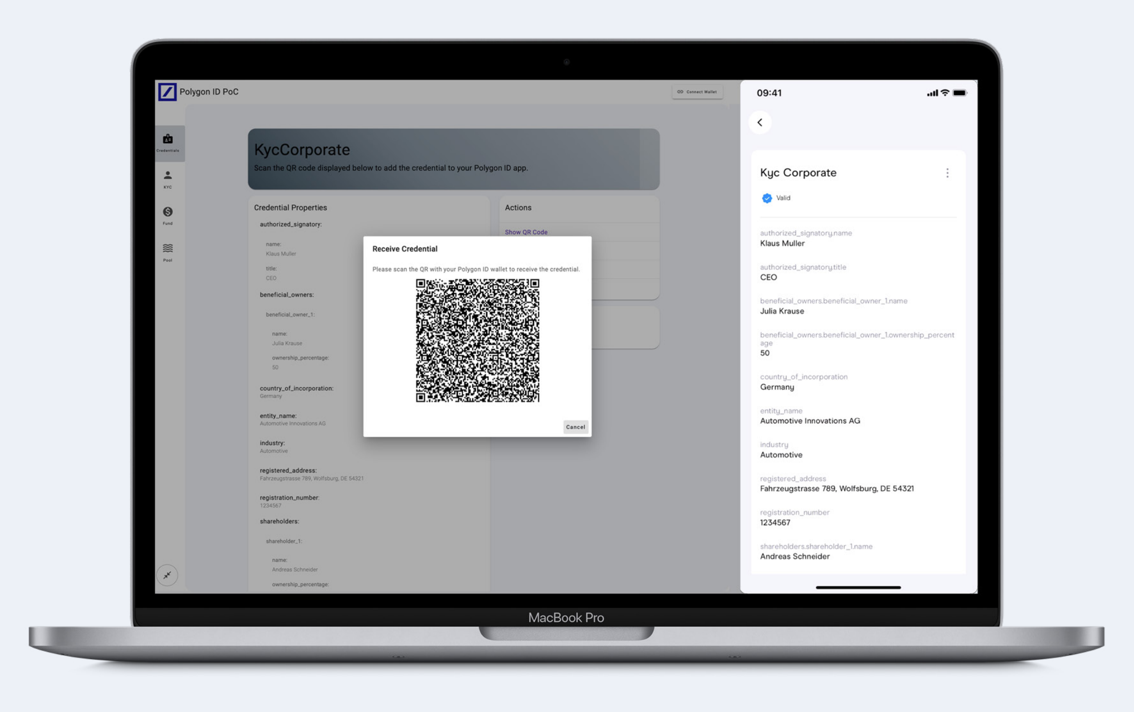
### Figure 10: Client onboarding/KYC process flow



Source: Deutsche Bank

For the PoC, Polygon ID's reference mobile wallet is used, enabling the storage, management, and presentation of credentials. However, Polygon ID also offers a wallet SDK (Software Developer Kit) that can be integrated into existing mobile applications.

## Figure 11: Issuance of a KYC credential using a QR code



Polygon ID PoC

KycCorporate

Scan the QR code displayed below to add the credential to your Polygon ID app.

Credential Properties

authorized_signatory:

name:
Klaus Muller

title:
CEO

beneficial_owners:

beneficial_owner_1:

name:
Julia Krause

ownership_percentage:
50

country_of_incorporation:
Germany

entity_name:
Automotive Innovations AG

industry:
Automotive

registered_address:
Fahrzeugstrasse 789, Wolfsburg, DE 54321

registration_number:
1234567

shareholders:

shareholder_1:

name:
Andreas Schneider

ownership_percentage:

Receive Credential

Please scan the QR with your Polygon ID wallet to receive the credential.

09:41

Kyc Corporate

Valid

authorized_signatory.name
Klaus Muller

authorized_signatory.title
CEO

beneficial_owners.beneficial_owner_1.name
Julia Krause

beneficial_owners.beneficial_owner_1.ownership_percentage
50

country_of_incorporation
Germany

entity_name
Automotive Innovations AG

industry
Automotive

registered_address
Fahrzeugstrasse 789, Wolfsburg, DE 54321

registration_number
1234567

shareholders.shareholder_1.name
Andreas Schneider

Source: Deutsche Bank

After a credential is added to a holder's identity wallet, the holder can decide to share claims from the credential with any verifier.

Information may be requested from an identity holder by leveraging Polygon ID's verifier software development kit (SDK). It supports the selective disclosure of claims and the attestation that a predicate holds true such as that a person's income level exceeds a specified threshold. In doing so, the verifier only receives the information that a statement holds true without gaining any knowledge of the precise underlying value. Those Zero-Knowledge Proofs are well-suited for a range of use cases such as age or income attestations.

The PoC focused on the issuance and verification of credentials containing KYC data. We were able to verify that Polygon ID's solution for issuing and verifying credentials is suitable for exchanging KYC data.

## 4.2 Digital ID to enable a compliant and efficient investment process

### 4.2.1 Storage of verifiable credentials (VC)

Project DAMA (Digital Assets Management Access) – A collaboration between Deutsche Bank and Memento Blockchain[28] sought to address the challenges associated with launching and servicing digital funds. A component of the PoC involved using Soulbound token (SBT), a modified non-transferable ERC protocol, as a customisable method of digital identification of qualified investors' wallet address and thus the owner of the wallet.

The SBT held Boolean or binary values related to application specific information like investor type, risk appetite, residency, regulatory limits and others. It is designed to identify a given wallet address – and the owner of the address by default - and to allow or disallow certain operations based on the values stored in the SBT. As a Trust Anchor, the issuer of the SBT could perform governance activities like effective sanctions filtering or transaction pattern forensics.

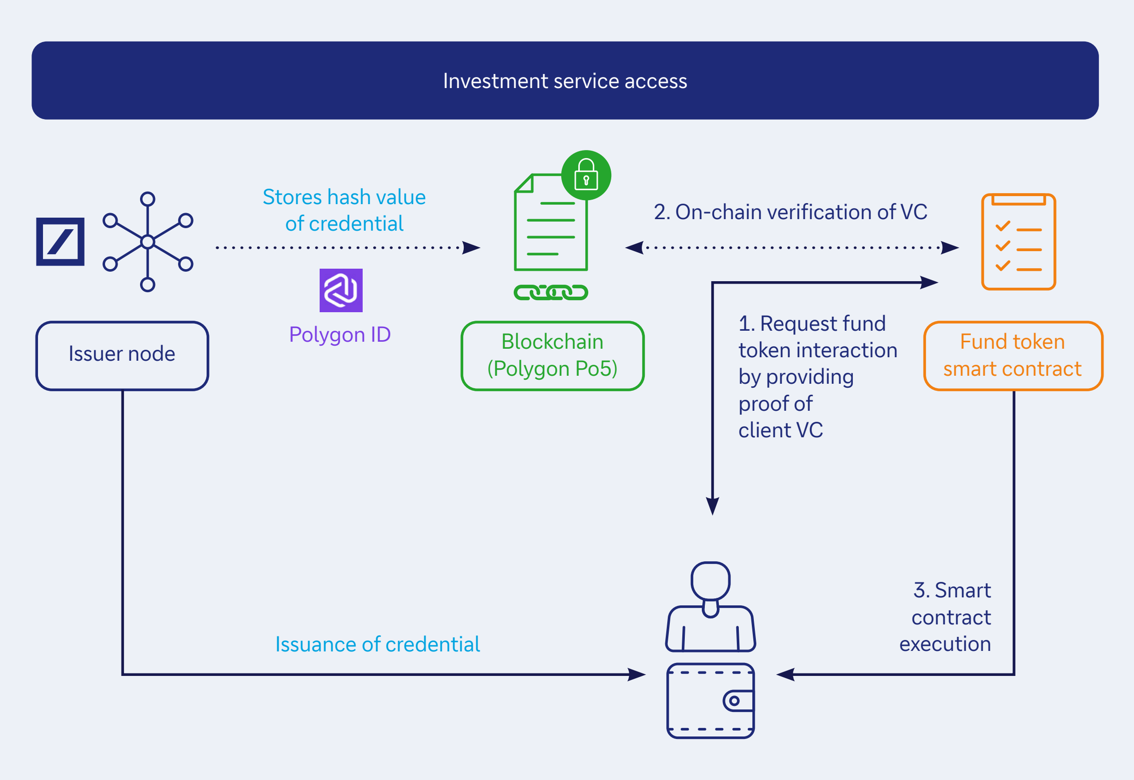
SBTs offer a straightforward approach to on-chain identity with PII stored off chain. They offer a mechanism whereby applications can check the investor profile, via its wallet that authorises the access to services. SBTs did not contain confidential or personal (identity) information as they are written directly to the blockchain.

Contrasting with the SBT as an identity tied to a wallet (in the DAMA PoC), Polygon ID is a user-centric self-sovereign identity that allows users to approve the verification of certain information ("claims") that an application can request. Polygon ID credentials are stored off-chain but may still be used on-chain by publishing a hash value that corresponds to a credential. This value does not expose any personal data but can be used to verify that information presented by an identity holder was indeed taken from a valid credential. This property is useful to restrict a smart contract's functionality to parties that can provide a valid verifiable credential. In the context of tokenised assets, where an asset is represented as fungible ERC-20 or non-fungible ERC-721 token, Polygon ID verifiable credentials can be used to restrict a token's transferability or enable only an authorised party to mint a token.

### 4.2.2 Technical perspective

The credential issuance process between the first and second use case remain almost identical. Only the proof type property of a credential needed to be adjusted to support sparse Merkle tree proofs. However, the verification process is set-up in quite a different way, as the fund token serving as introductory example, is implemented via an ERC-20 smart contract and deployed on the Polygon testnet. By inheriting from Polygon ID's verifier contract, the smart contract functionality is restricted to identity holders that were able to provide a valid KYC credential, stating that one of the credential's attributes exceeded a desired threshold.

### Figure 12: Investment service access process flow


Investment service access
Stores hash value of credential
Polygon ID
2. On-chain verification of VC
Issuer node
Blockchain (Polygon Po5)
Fund token smart contract
1. Request fund token interaction by providing proof of client VC
3. Smart contract execution
Issuance of credential

Source: Deutsche Bank

Once the zero-knowledge request was in place, the contract was ready to accept user requests. Like in the first use case, the user is prompted to confirm a request by scanning a QR code, this time containing the smart contract's address, a reference to the Blockchain it resides on and a link to the credential's JSON-LD context. Having scanned the QR code, the user is asked to establish a connection to a crypto wallet installed on their smartphone. Following which, a Zero-Knowledge Proof is generated, and the user is prompted to confirm the blockchain transaction.

By confirming the transaction, a method provided by Polygon ID's verifier contract is executed, which validates the provided proof and executes a desired function afterwards. That mechanism is well suited to restrict the execution of functions requiring limited arguments such as a mint function. However, the verifier contract's design could be improved to accommodate function calls requiring a set of multiple arguments more easily.

## 4.3 Digital ID for Institutional DeFi liquidity pool access

### 4.3.1 Decentralised finance momentum

In recent years DeFi (decentralised finance) has gained momentum as a form of financial intermediation relying on automated protocols or smart contracts based on decentralised applications. The fundamental aim is to replicate existing products & services known from the traditional financial system with minimised reliance on centralised intermediaries. To bring the benefits of DeFi closer to the traditional financial markets value chain tokenised forms of existing assets can be integrated into the DeFi protocols and technology stack. One promising approach is the usage of automated market making (AMM) based on liquidity pools. The concept not only exists in the 'pure' DeFi world where those liquidity pools are predominantly filled with different crypto currencies but has also been tested previously with the engagement of financial institutions and regulators (for example, the Monetary Authority of Singapore's Project Guardian[29]).

As one of the most important and liquid markets the OTC FX market reached an average daily turnover of almost US$10trn in 2022 taking worldwide transactions and derivatives into account.[30] Similarly, SSA (sovereign, supranational and agency) bonds reached a volume of US$88trn in notional outstanding in 2020.[31] By utilising dedicated liquidity pools to trade different pairs of high quality liquid assets (HQLAs) such as government bonds and fiat currencies – both in a tokenised form – current challenges in the market ranging from frictions caused by multiple intermediaries in the trading value chain to fragmented liquidity due to changing counterparties could be addressed. A more efficient and frictionless set-up can be achieved via atomic settlement of assets in conjunction with trading against common liquidity pools rather than single counterparties, e.g., in a centralised order book.

The challenge in such a more decentralised setting is that a fast and secure way of identifying and screening participants interacting with the liquidity pools is required. Verifiable credentials (VCs) can exactly mitigate this problem and ensure scalable participation by eligible participants. The core feature is represented by trusted entities which could be banks or other (financial) institutions that issue dedicated credentials being accepted by the smart contract/verifier of the respective liquidity pool.

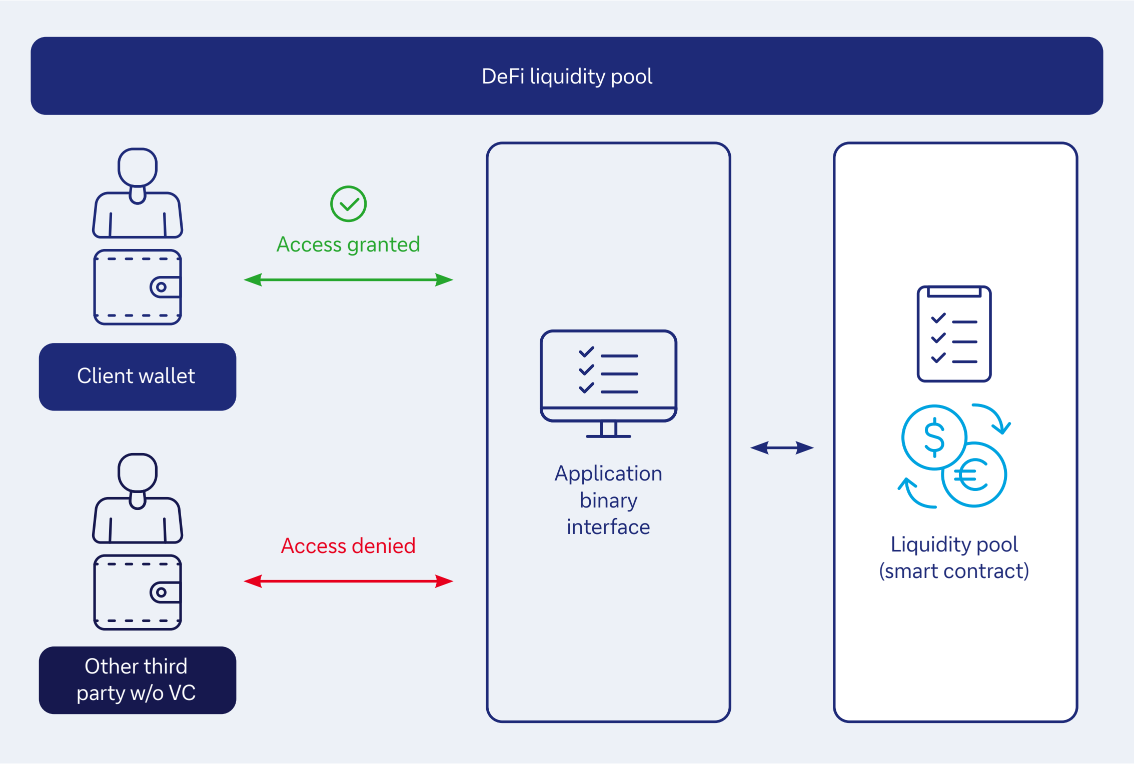
As part of this PoC a basic liquidity pool smart contract was created to simulate an AMM trading facility which also entails a verifier function that acts as a gatekeeper to decide whether specific (client) wallets can interact with the pool. In principle, the verifier contract may also accept verifiable credentials issued from other trusted entities and a verifiable credential can be revoked if a client / participant does not fulfil pre-defined criteria related to KYC or other commercial factors.

### 4.3.2 Technical perspective

As part of the PoC, we have implemented a prototypical liquidity pool contract supporting deposition, withdrawal and exchange of two underlying tokens. As in the previous PoC, the smart contract is deployed on the Polygon testnet alongside two token contracts. We used vanilla ERC-20 token contracts to represent a digital currency and a high-quality liquid asset, respectively.

As the previously fund token contract, the liquidity pool builds on Polygon ID's verifier contract ensuring that only authorised parties can deposit and exchange tokens. Depending on the desired function, the user receives a QR code containing a request to present a valid credential, that's accepted using his Polygon ID wallet that triggers the invocation of the pool's contract.

**Figure 13: DeFi liquidity pool process flow**



Source: Deutsche Bank

While we have not focused specifically on the commercial aspects of the liquidity pool in this PoC, there are several factors to be considered for this institutional DeFi model to operate efficiently from an identity management perspective. The trusted entities need to have sufficient reputation in the market and need to be incentivised for providing their services which entails in many cases detailed and costly KYC processes. Those processes need to be based on commonly accepted controls and need to be maintained on a continuous basis. Last, privacy concerns for trading activity in the respective pools need to be mitigated together with general challenges in the institutional DeFi space around the required regulatory landscape and sound legal basis which is still to be developed in relevant jurisdictions.

5

# Where next?

## 5.1 A reliable alternative to federated ID systems

Decentralised identity offers an efficient and reliable alternative to federated identity systems. Centralised credential issuers will continue to control a large part of digital identities in the medium-term due to (existing) customer relationships and market structures but the use of secure technologies including DLT and cryptographic methods such as ZKP offer immense potential in providing entities with greater ownership of their identity. However, while we can clearly see the advantages of SSI there are a number of factors to be addressed before realisation and widespread adoption of the technology.

For instance, interoperability through international standards and protocols that facilitate compatibility are essential to enable the effectiveness of digital identities across a broad range of platforms and services. The ability to use the same digital identity across many platforms is one of the strongest reasons for adoption – but so far this remains a promise as no standard is universally accepted. No solution will be purely technology in nature, multiple stakeholders need to be involved with regards to common data standards, governance and regulatory alignment. This will require greater industry cooperation between parties such as governmental agencies and the private sector for the development of a fully interoperable digital ID ecosystem.

## 5.2 Key adoption factors

Network effects are paramount for the widespread adoption and success of the ecosystem – creating somewhat of a chicken and egg situation as identity providers need to ensure to offer access to a substantial number of high-value public and private sector use cases from the outset. Providers need a broad customer base as consumers will be slow to adopt unproven systems with small numbers of users – further slowing the development of the services.[32] The pace of change will likely be moderate and incremental, where a series of increments will offer improved efficiencies and greater resiliency.

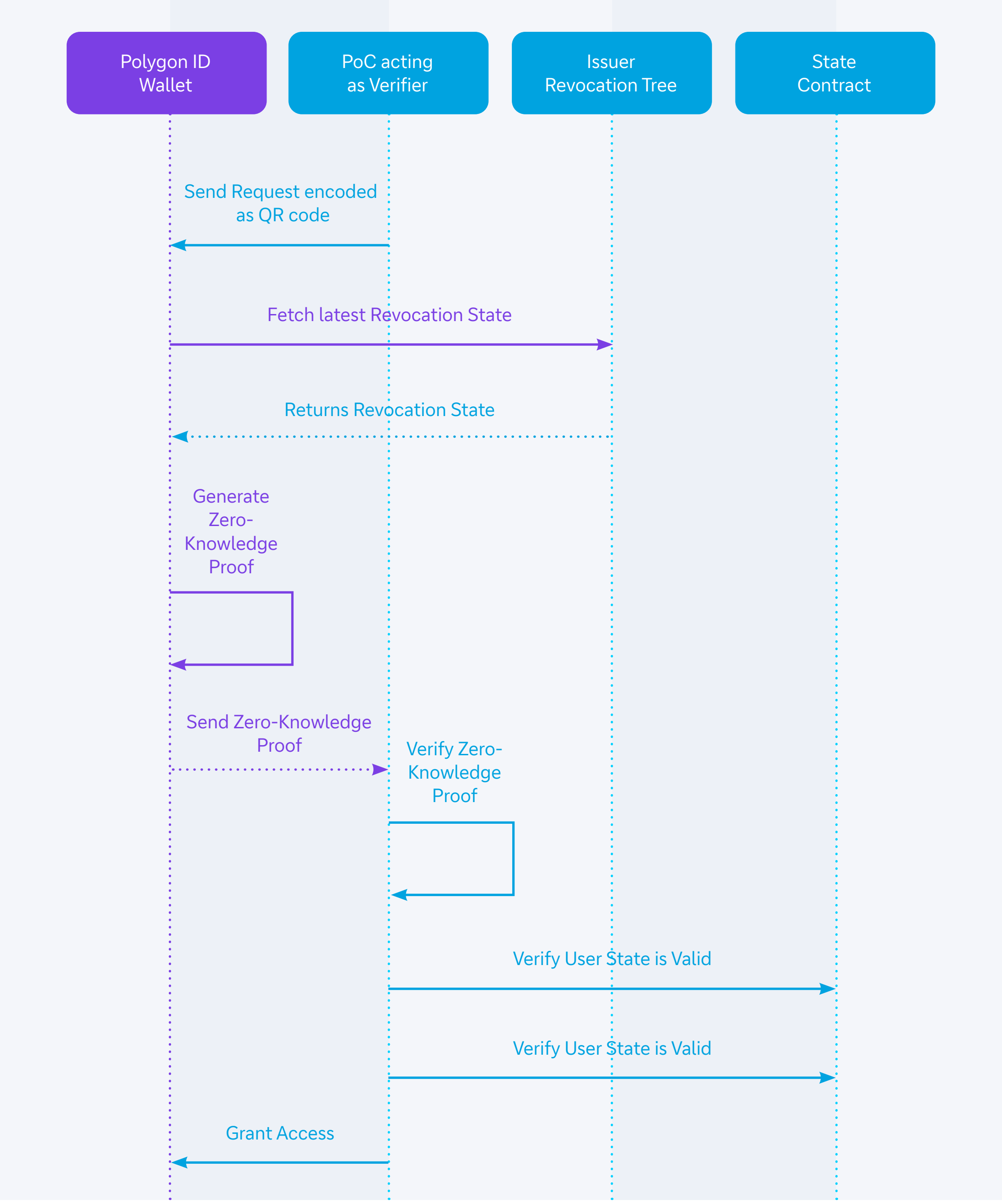
Prioritising the user experience will ensure the current positive momentum continues. Solution providers will need to reduce the burden on the user's side, where users must at present learn to use and interact with the technology (wallets, blockchain, key management i.e., no 'password reset' for lost Private Keys etc.). This abstraction from the technology is pertinent for users that are less well versed in Web3 worlds – while at the same time we would expect to see some Web3 aspects infiltrate daily life from other use cases, increasing user's familiarity with digital wallets (through loyalty schemes, ticketing and payments) and QR codes (event tickets, payments etc.).

These UX advancements will reduce the inertia to shift from identity norms. The convenience of registering with a username and password is difficult to outweigh the advantages that SSI presents – as the benefits are not fully understood. We see this shifting over time with education – and as data breaches, privacy and vendor lock-in continue to be a concern.

Banks can play a vital role in future identity ecosystems – currently a data manager for clients from a financial services perspective, in future this could extend to managing identification and identification data. As banks are already obliged to verify customer information, they are predestined to be important players in an open identity ecosystem and could serve as trust anchors. To achieve this, sufficient incentives, need to be in place to cover for incremental risks which could be achieved by new monetisation models for credential presentations and ultimately can give rise to an SSI-based data economy.

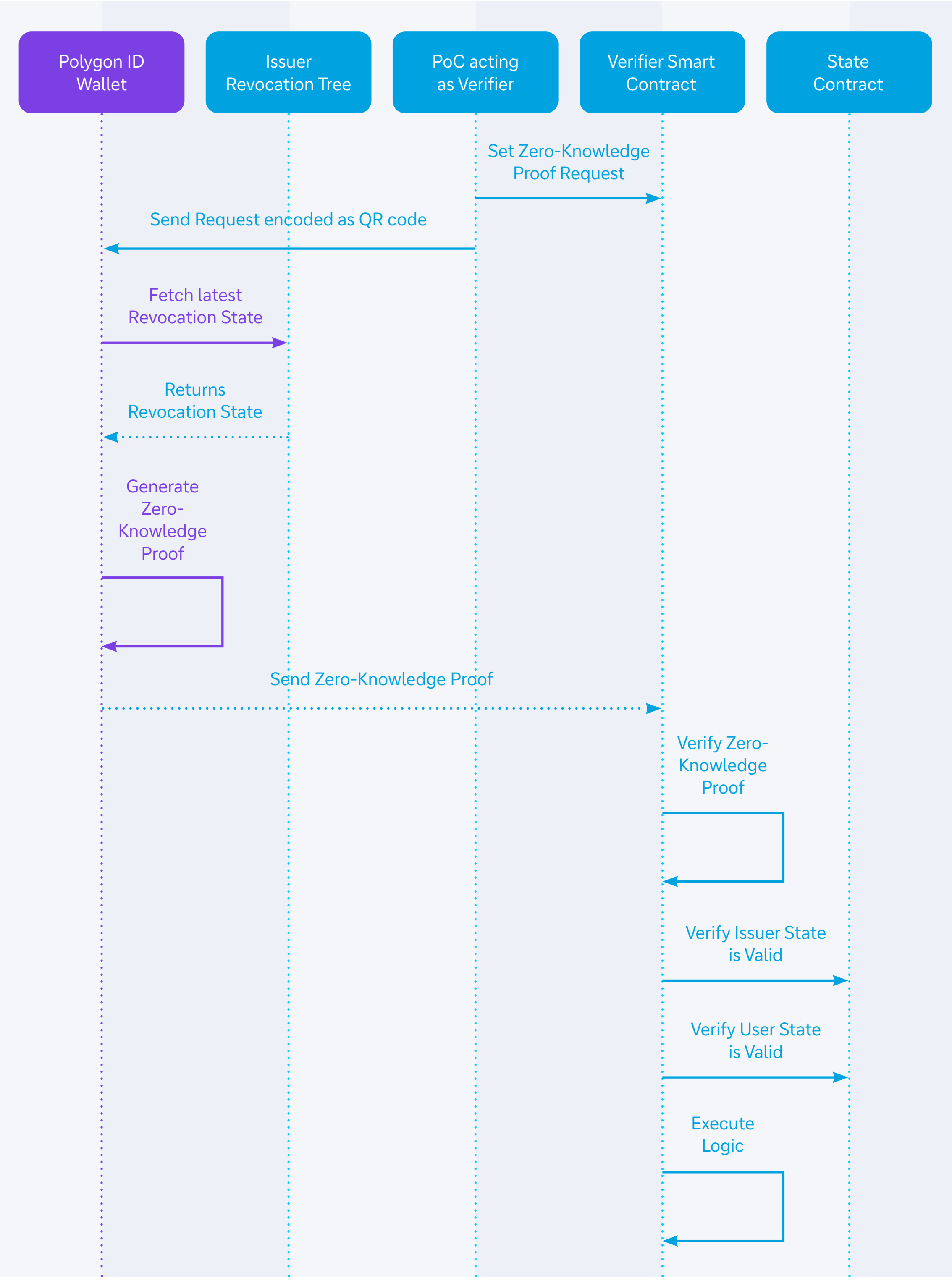
# Appendix 1: off and on-chain verification flows

### Figure 14: Off-chain verification flow


Polygon ID Wallet
PoC acting as Verifier
Issuer Revocation Tree
State Contract
Send Request encoded as QR code
Fetch latest Revocation State
Returns Revocation State
Generate Zero-Knowledge Proof
Send Zero-Knowledge Proof
Verify Zero-Knowledge Proof
Verify User State is Valid
Verify User State is Valid
Grant Access

Source: Deutsche Bank

## Figure 15: On-chain verification flow


Polygon ID Wallet
Issuer Revocation Tree
PoC acting as Verifier
Verifier Smart Contract
State Contract
Set Zero-Knowledge Proof Request
Send Request encoded as QR code
Fetch latest Revocation State
Returns Revocation State
Generate Zero-Knowledge Proof
Send Zero-Knowledge Proof
Verify Zero-Knowledge Proof
Verify Issuer State is Valid
Verify User State is Valid
Execute Logic

Source: Deutsche Bank

# Glossary of terms

**AML/CFT**
Anti-Money Laundering / Combatting the Financing of Terrorism: Policies and measures to prevent criminals and terrorist from abusing the financial system

**Application programming interface (API)**
A set of defined rules that enable different applications to communicate with each other

**Blockchain**
An advanced database mechanism that allows (transparent) information sharing based on blocks of records that are securely linked by cryptographic means

**CAGR**
Compound annual growth rate is the mean annual growth rate over a specified period of time longer than one year

**Crypto-native**
Specific to the crypto, or Web3 space

**Cryptographic proofs**
Mathematical algorithms that are used to prove the authenticity of a statement, or piece of information

**Customer Due Diligence (CDD)**
A process used to collect and evaluate relevant information about a customer, or potential customer

**Customer experience (CX)**
Encapsulates everything a business or an organisation does to put customers first, managing their journeys and serving their needs

**Decentralised Identity Foundation**
An engineering-driven organisation focused on developing the foundational elements necessary to establish an open ecosystem for decentralised identity

**DID**
DID or Decentralised Identifiers is a new type of identifier that enables verifiable, decentralised digital identity

**DID method**
The mechanism by which a particular type of DID and its associated DID document are created, resolved, updated, and deactivated

**ERC-20 token**
ERC-20 tokens are sets of ‘fungible’ digital tokens that live on the Ethereum network

**ERC-721 token**
ERC721 is a standard for representing ownership of ‘non-fungible’ tokens (NFT), that is, where each token is unique

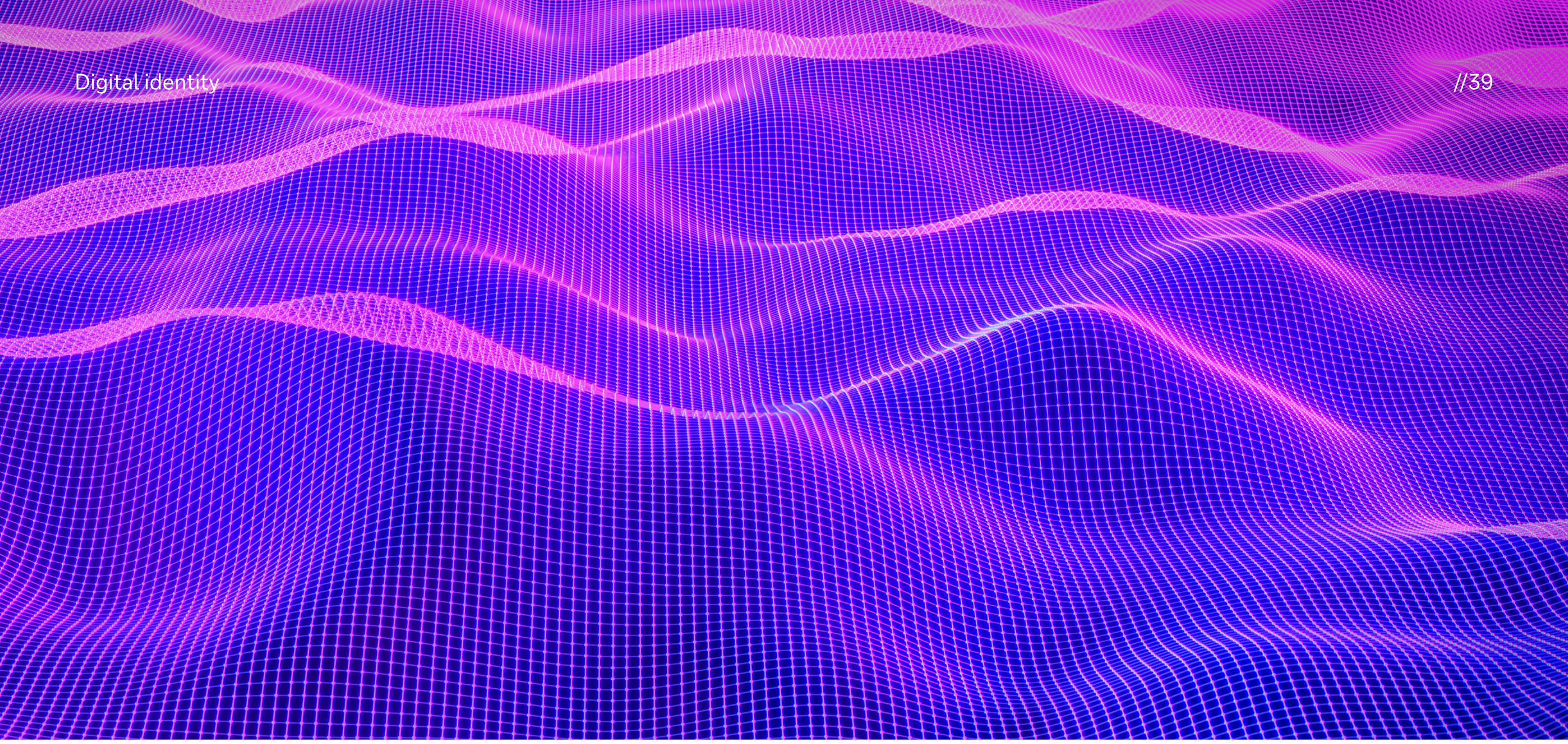
**Genesis ID**
The initial identity state, from which the original DID is being derived

**Iden3 protocol**
A decentralised protocol built on top of the Ethereum blockchain that uses Zero-Knowledge Proofs to enable users to prove the ownership of their identity claims [Polygon]

**Key pairs**
Like a lock and key for your digital information. One key locks (encrypts) your information so no one else can read it, while the other key unlocks (decrypts) it

**KYC utilities**
A customer due diligence tool that involves collecting and sharing information among member banks

**KYC**
‘Know Your Customer’ or KYC is the process of verifying the identity of a client (person or company)



### Method

A set of code which is referred to by name and can be called (invoked) at any point in a program simply by utilising the method's name

### Mint

The process of generating new coins by authenticating data, creating new blocks, and recording the information onto the blockchain

### Non fungible tokens (NFTs)

A record on a blockchain which is associated with a particular digital or physical asset or reference that can be utilised for ownership certification and authenticity. Ownership can be transferred by the owner allowing NFTs to be sold and traded

### Off-chain

Off-chain transactions are confirmed outside of the main blockchain network, often resulting in a cheaper and faster process for the user

### On-chain

On-chain transactions take place on the blockchain, the public ledger that keeps track of every transaction.

### PoC

A proof of concept (PoC) is a demonstration of a product in which work is focused on determining whether an idea can be turned into a reality.

### Private ledger

In distributed ledger this means a permissioned network, where only selected participants can join the network e.g. R3's Corda, Hyperledger Fabric

### Public key infrastructure (PKI)

A technology for authenticating users and devices in the digital world

### Public ledger

In distributed ledger this refers to an open-access network; anyone can join at any time – e.g. Bitcoin and Ethereum blockchains

### QR code

A quick response (QR) code is a type of barcode that stores information and can be read by a digital device, such as a mobile phone

### Schema builder tool

A tool created to simplify the process of creating schemas by using an intuitive user interface and enabling everyone to check previously made schemas

### Selective disclosure

A privacy feature that allows end users to choose what, and how much, information they share on a case-by-case basis

### Single sign on (SSO)

User authentication that enables end users to securely access multiple services, or applications using a single set of credentials

### Software Developer Kit (SDK)

An SDK is a set of tools to build software for a particular platform – in this case Polygon ID

### Soul bound tokens (SBTs)

Specific form of NFTs -Digital identity tokens that represent traits, features and achievements that make up a person or entity. These tokens are issued by 'Souls' which represent blockchain accounts or wallet and cannot be transferred

**Sparse Merkle tree**
A type of Merkle tree where the contained data is indexed, with each datapoint placed at the leaf the corresponds to that datapoint's index

**SWIFT**
The Society for Worldwide Interbank Financial Telecommunications. Network that banks use to communicate with each other securely, mainly to give instructions for transferring funds between accounts

**Testnet**
An instance of a blockchain powered by the same or a newer version of the underlying software, used for testing without risk to real funds or impacting the main blockchain

**TLS internet standard**
A cryptographic protocol that ensures secure communication over a computer network, such as the internet

**User experience (UX)**
Encompasses all aspects of an end users interaction with a company, its services and its products

**Verifiable credentials (VC)**
A set of tamper-evident claims and metadata that cryptographically prove who issued it

**W3C open source identity standards**
An official web standard from W3C that defines a standard way to express credentials on the web

**Wallet**
A wallet is a device or program that stores cryptographic keys and allows access to digital identification credentials or other digital assets

**Web3**
Can be considered as the next generation of the world wide web which is based on blockchain technology and a decentralised virtual economy where the user is at the centre having full ownership and control over personal data and virtual assets being shared and traded

**Zero-Knowledge Proof (ZKP)**
A cryptographic method used to prove knowledge about a piece of data, without revealing the data itself.

**ZK query language**
The Query Language on Polygon ID is a tool that allows developers to design customised authentication requirements based on users' claims

## References

1. Identity Definition & Meaning – Merriam-Webster
2. In Search of an Identity – Ideas | Institute for Advanced Study (ias.edu)
3. A Brief History of National ID Cards – FXB Center for Health & Human Rights | Harvard University
4. 850 million people globally don't have ID—why this matters and what we can do about it (worldbank.org)
5. Companies and businesses – The National Archives
6. Digital identification, a key to inclusive growth, McKinsey Global Institute, 2019
7. Digital Identity_Final_Report.pdf (oliverwyman.com) (2020)
8. 2022 Connectivity Benchmark Report. Mulesoft Research
9. https://tech.co/password-managers/how-many-passwords-average-person
10. The Evolution of Identity Verification in the Marketplace, Know Identity
11. Digital identification: A key to inclusive growth, McKinsey
12. Digital Identity Solutions Market Size is projected to (globenewswire.com)
13. https://www.juniperresearch.com/pressreleases/digital-wallets-ericsson-comviva-and-huawei
14. https://www.juniperresearch.com/infographics/digital-wallets-market-statistics-infographic
15. https://www.forbes.com/sites/davidbirch/2023/02/01/the-wallet-wars-are-not-about-money-they-are-about-identity/?sh=3a2c9140314a
16. Me, myself and (SS)I, BCG and walt.id
17. Principles of SSI V3 – Sovrin
18. Corporate digital identity: no silver bullet, but a silver lining, Bank for International Settlements
19. Business Banking Cannot be Disrupted Without Digital in Onboarding (internationalbanker.com)
20. Global Trade Finance Gap Expands to $2.5 Trillion in 2022 | Asian Development Bank (adb.org)
21. Fighting trade-related fraud – Deutsche Bank (db.com)
22. https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries
23. https://www.coindesk.com/markets/2017/08/27/cant-be-evil-the-google-inspired-case-for-blockchain/
24. Polygon ID
25. https://www.w3.org/TR/did-core/
26. https://identity.foundation/
27. https://docs.iden3.io/protocol/spec/#revocation-tree
28. Simplifying digital fund management and investment servicing – Corporates and Institutions (db.com)
29. https://www.mas.gov.sg/schemes-and-initiatives/project-guardian
30. https://www.statista.com/statistics/1219222/average-daily-turnover-otc-forex-instrument-country/
31. https://www.icmagroup.org/market-practice-and-regulatory-policy/secondary-markets/bond-market-size/
32. Self-Sovereign Identity: Foundations, Applications, and Potentials of Portable Digital Identities, Fraunhofer FIT

www.db.com/flow

This document is for information purposes only and is designed to serve as a general overview regarding the services of Deutsche Bank AG, any of its branches and affiliates. The general description in this document relates to services offered by Deutsche Bank Corporate Bank within Deutsche Bank AG, any of its branches and affiliates to customers as of May 2024, which may be subject to change in the future. This document and the general description of the services are in their nature only illustrative, do neither explicitly nor implicitly make an offer and therefore do not contain or cannot result in any contractual or non-contractual obligation or liability of Deutsche Bank AG, any of its branches or affiliates.

Deutsche Bank AG is authorised under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin)) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorisation and supervision by these authorities are available on request.

Deutsche Bank Corporate Bank

polygon ID

polygon Labs