innovate identity

Self-Sovereign and Shared Ledgers

A new dawn for Digital Identity?

WRITTEN BY EWAN WILLARS
WITH SPECIAL THANKS TO EMMA LINDLEY AND DAVID BIRCH

JANUARY 2019

ACKNOWLEDGEMENTS

We would like to thank the following people:

Emma Lindley for her very significant role in bringing this report together, and to thank her for her assistance and very valuable input throughout the project.

David Birch for his help in developing this report. We were keen to enable readers without an identity background to access some more technical information regarding the structure of digital identity solutions and shared ledgers, should they wish to. David's input was crucial in achieving this.

The 20 self-sovereign and blockchain companies we interviewed as part of our research into this subject.

Contents

	Foreword	02
	Executive Summary	03
1	Introduction	05
2	Digital Identity in Action	07
3	Self-Sovereign: an emerging approach to digital identity	11
4	Self-Sovereign and Shared Ledger: a powerful combination	15
5	Benefits and Challenges	19
6	Conclusions	22
	Glossary	24
	Technical Notes	26

There are now more than **3.7 billion people online** globally

Creating the connections between the real world and the virtual world which can enable online transactions to take place with trust and confidence is a huge challenge.

Foreword

The digital identity landscape is confusing and fragmented. We have government schemes, bank schemes, mobile operator schemes, collaborations between cross-sector organisations, social media log-ins and companies going it alone to try and create a market.

We have centralised schemes, distributed schemes, federated schemes, closed schemes, schemes with hubs, and schemes using APIs. Open standards. No standards. Oh yes, and we have shared ledger technology come to the party as well. Sovereign identity. Self-sovereign identity. No identity.

It feels like progress has been very slow. Is it any wonder?

Doing digital identity is difficult. Very difficult. It is expensive. It needs scale. It needs collaboration. It needs impetus.

Every so often a new technology comes along that has the potential to create that impetus to change thinking. In the identity space, none more so than shared ledgers. Shared ledger technology was purported to be the answer to identity. It has attracted huge media interest and huge investment. But closer examination has questioned why this should be the case. The case is based on "doing identity" differently. Having a means to collect and store immutable evidence about who we are and relying less on more established means. Our buying patterns, behaviours and social lives are all part of our identity. It's our identity, not governments or banks and we have a right to create our own – in other words, a self-sovereign identity. But the reality is that's not how we currently do identity.

Taking a traditional sovereign approach to identity, based on how we are known to our national state, and trying to make it fit in a digital world is proving hugely challenging. It is inconvenient, insecure and exposes us to all manner of financial and other risks.

Should we be starting from a different place? Do we need to rethink digital identity? Would self-sovereign identity, delivered with shared-ledger technology, better fit today's digital needs?

In this report, we consider these questions.

Taken together, could they solve the challenges faced today; what are the issues that would still need to be surmounted and how, if self-sovereign and shared ledgers are to be a new dawn for digital identity.

Rob Laurence
Director, Innovate Identity Ltd
Rlaurence@innovateidentity.com
+44 (0)7538 683917

Executive Summary

The digital identity industry worldwide has been subjected to a series of over-hyped innovations – new technology and new approaches that each promise to be the vanguard of a bright new digital identity world, but which have seldom delivered on the initial excitement. This leaves potential users and relying parties unsure what to believe, and whether substance lies beneath the promise of innovation.

The latest approaches to enter the spotlight have been the concepts of *self-sovereign identity* (where you control your personal identity data locally, often on a device and with a personal key of some kind), and *shared ledger technologies* (where a common digital ledger of transactions and data is updated across all the scheme users). When applied individually, and particularly when applied collectively, these two approaches have generated significant interest and coverage.

This report examines what has generated such excitement, unpicks what these approaches actually entail in practice, and looks for any evidence to suggest that these approaches may succeed when so many others have fallen by the wayside.

Self-sovereign identity is a child of its time and, as such, **its relevance can't be ignored.**

KEY FINDINGS

The moment feels right for self-sovereign

Self-sovereign feels like an approach that is emerging at the right time. Whether birthed by the new move towards ensuring that people have better control over their personal data, or merely in alignment by chance, self-sovereign feels very 'of the moment'. This is one source of hype: effectively self-sovereign has gone viral.

When the hype is carefully peeled back, the natural alignment between a self-sovereign approach and recent data protection regulation is laid clear, with both providing for individuals to have greater control over how, where and when their personal data is stored and used. Self-sovereign is a child of its time, and as such its relevance can't be ignored.

Shared ledger technology can unlock the potential of self-sovereign

Neither self-sovereign nor shared ledgers are dependent on each other; other forms of personal attribute storage and transmission are available, such as via personal cloud-based data vaults, and greater user-centricity can also be delivered via a federated system, although via a naturally more centralised architecture.

However, when combined, self-sovereign shared ledgers provide a means to maintain a common, trusted record of attributes and events, putting users in direct control of their personal identity data, and remove the need to rely on large central hubs to provide route data to the relying party.

Self-sovereign and shared ledgers are fast emerging as credible ways to assist individuals suffering identity challenges

The lack of a means to demonstrate one's identity, to assert who you are at crucial times, is a major issue for a billion or more people around the world. The UN Sustainable Development Goals seek to ensure a legal identity is available to all by 2030; digital identity is one (perhaps significant) means to achieve that goal.[1]

Providing every individual with a way to demonstrate their identity is critical to ensure individuals can access services such as banking and healthcare. In particular the shared ledger approach, where individuals can 'build' a trusted digital identity over time even in the absence of traditional identity credentials, is a potentially very positive development.

1 https://sustainabledevelopment.un.org/sdg16

Despite the potential, significant barriers to adoption still remain.

- ✓ Self-sovereign and shared ledger approaches could be used across a wide range of relying parties and for a huge variety of uses, given the right regulation and commercial models.
- ✓ Self-sovereign has great potential to reduce the growing regulatory burden, recently created by the consent regimes of GDPR and other personal data regulation.
- ✓ The use of shared ledgers can build a unique identity even for those with no access to more traditional and formal means of identifying themselves.
- ✗ The terminology used for both shared ledgers and self-sovereign approaches is often opaque and varies a great deal, and this adds to perception that they lack maturity.
- ✗ The current deployments often lack interoperability. This reflects the lack of commonly accepted standards, which in turn fragments the market and diminishes the level of trust in the data provided by schemes.
- ✗ Ongoing regulatory uncertainty will continue to create uncertainty and a barrier to adoption, particularly for highly regulated industries such as financial services. As it stands, financial service firms in many jurisdictions may be unable to rely on trusted data from digital identity sources, due to existing anti-money laundering regulations. In the EU, the Fifth Money Laundering Directive will change this in late 2019, enabling digital identities to be more readily used by banks provided they align to the eIDAS standards, or the scheme is accepted by the local regulator.[2]
- ✗ Federated identity schemes have both attribute providers and relying parties within their trust framework, with banks often playing a part in both roles. However, self-sovereign schemes do not start with a 'ready-made' roster of relying parties – and without a sufficient level of utility for the end user, digital identity schemes of any design are doomed to failure.
- ? A fundamental, but as-yet unanswered question is whether a sufficiently high number of people actually want (or even have the capacity) to effectively manage their personal data themselves. The future of self-sovereign identity solutions depends on confirming the appetite and likely rate of adoption by users.

WHAT NEXT?

It remains too early to reasonably predict the future success or otherwise of the self-sovereign approach, although shared ledgers are becoming much more widely deployed. Yet the principles at the heart of combined self-sovereign shared ledger approach – recording consent and what transactions take place, enabling the individual's control over their personal data, the empowering of the individual to call forth their own identity attributes in a variety of circumstances, particularly online – very accurately reflect and address many current digital identity challenges.

There will need to be further exploration and test deployments before widespread adoption – regulators in particular need to demonstrate their understanding and create a path for such innovation to flow through to the mass market. Industry 'sandboxes', such as that introduced by the UK Financial Conduct Authority, are a positive development, somewhat de-risking the testing of new solutions. It also allows regulators to consider new approaches in practice, how they might be appropriately regulated, and the potential need for new industry standards to be developed.

While neither self-sovereign nor shared ledgers can provide a general panacea for every digital identity challenge, both approaches have hugely exciting potential, particularly when combined. But after the hype has died down, only the identity market, and acceptance by relying parties and consumers, will decide if they will ultimately deliver on their very significant promise.

The principles at the heart of a combined self-sovereign, shared ledger approach accurately **reflect and address many digital identity challenges.**

2 AMLD5 Revised text, paragraph (22): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

1 Introduction

Along the road to developing digital identity solutions around the world, there has been extensive hype generated by the emergence of one approach or another. Yet in truth, successful digital identity schemes, i.e. *those that are established, frequently used and widely relied upon* remain few in number, despite repeated narratives promising much wider digital identity adoption.

Instead, while the digital economy has boomed around the world, it remains surprisingly difficult to prove who we are online, at least to a high degree of confidence. Those with 'thin files', for example, a new arrival to a country, those leaving education, or other state institutions are disproportionately affected by digital identity shortcomings. In developing countries it is often an even more profound challenge, particularly impacting the poor, or those with limited access to modern communications infrastructure, for example in rural or remote areas.

With each step forward in technology or identity methodology, new claims are made for how they will solve the identity conundrum. However, few if any have yet lived up to the initial excitement. The latest digital identity approaches to be hyped have been self-sovereign identity, and decentralised, shared ledger technologies. In truth, both approaches have been explored in some detail for a number of years, however interest has grown recently, particularly around the potential to combine the approaches, and this could be an opportune time for self-sovereign shared ledgers to enter the mainstream.

With each step forward in technology, or identity methodology, **new claims are made for how it will solve the identity conundrum**. However, few if any have lived up to the initial excitement.

THE DIGITAL IDENTITY CONUNDRUM

There are now more than 3.7 billion people online globally,[3] and in recent years digital technologies have dramatically increased access, efficiency and innovation for people, businesses and governments around the world.[4]

Yet despite so many more interactions, services and transactions now taking place online, we still have a fundamental challenge; there remains no simple way to know for certain who someone (or indeed something) is when transacting with them digitally. For those people whose circumstances leave them with few or no formal means of identification, or a very limited digital footprint, this is a particular problem, often preventing them from gaining access to even basic services, such as healthcare, education or welfare.

As such, proving who they are remains a barrier for some, whether online or in person. For others it is asserting their identity online that is the major issue. Creating connections between the real world and the virtual world which can enable online transactions to take place with trust and confidence is a huge challenge.

- To be able to identify an individual or organisation digitally, and to a high degree of confidence, is more challenging as many of the identity proofs we have come to rely upon (such as passports, utility bills, driving licences) are not easily transferred to a digital environment.
- Ensuring digital security and data privacy is another big challenge and has been a key tenet of recent regulation around the world, such as the EU's General Data Protection Regulation (GDPR).
- The reliance placed upon a small number of globally dominant technology companies – such as Google, Apple, Facebook and Amazon (GAFA) – to collect, store and utilise enormous quantities of personal data, while also providing a range of digital identity management services, has become a growing concern for state regulators and citizens alike. Digital platform providers' own lack of accountability is amplifying that concern.
- Providing digital identity solutions can be a catalyst for inclusion, opening up access to critical services. Digital identity is too often seen as a developed world challenge, but that is not the case – how can we make digital identity work for all?

3 www.internetlivestats.com/internet-users/
4 documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

Navigating new regulation such as GDPR, the difficulty addressing financial and identity exclusion, market inertia, perceived liability issues and a fear of failure has created extremely challenging conditions for the development of any large-scale digital identity solution. The problem of finding a way to provide citizens, organisations and other entities with safe, secure and easy ways to assert themselves online, with a level of trust that enables the full potential of the online world, therefore remains.

In contrast to large-scale centralised implementations, by putting the individual in control of their own data, and moving away from a single or centralised solution provider, self-sovereign identity delivered via a shared ledger is increasingly being seen by some as a viable answer.

Can this possibly be true?

REPORT AIMS

In the face of challenges such as stiffening data regulation, the market dominance of global tech firms, and the need to find inclusive, accessible solutions, the report will examine how likely it is that new self-sovereign approaches will succeed, with or without shared ledger.

In this report, we aim to provide executives with the high-level understanding and an appraisal of the potential benefits of these emerging digital identity approaches.

Doing identity in the way we always have **doesn't mean that it's the way we always should**.

2 Digital Identity in Action

Digital identities can be used to electronically represent individuals (or other entities) as agents and/or proxies with the full rights, entitlements and accountabilities enjoyed by their physical counterparts. This can be done safely and securely, providing the necessary levels of assurance about the real-world identity, without sharing real-world information, and potentially allowing the end user to have full control over the attributes they consent to share.

In the case of individuals, we each assert our identities in different ways depending on the context. Some identity requirements are driven by law or regulation – for instance the need for some businesses to establish your identity with confidence to prevent money laundering (e.g. via a 'Know Your Customer' or KYC process), or to enable a person to travel across an international border.

Other data is required by a relying party because it is industry best practice; to protect further against fraud or money laundering, or to inform a risk-based assessment. Alternatively, the identity information may be required to underpin a transaction of some sort, such as to make a payment, or to establish a change of ownership.

DIGITAL IDENTITY USE CASES

Different regulatory contexts, the needs of relying parties, and the nature and sensitivity of the task or transaction in hand will all form the specific collection of identity attributes required for any given task, and the level of assurance required as well.

The data that will make up the specific digital identity for a given task will therefore need to map to the regulatory and business needs of the relying party. The following three case studies demonstrate the wide variety of digital identity uses in practice.

These are explored in more detail in Technical Note No. 1.

USE CASE A

Digital identity solutions are beginning to help young children in developing countries to ensure they have access to education and healthcare.

The United Nation's Sustainable Development Goal 16 aims to ensure everyone across all 193 member countries has a legally recognised form of identity by 2030.[5] Yet at present many young children are not formally registered; the lack of a birth certificate affects their ability to gain access to basic services such as primary education.

However, close to 90% of children in developing countries do receive access to a formal immunisation,[6] under a variety of support initiatives. A number of innovative digital identity schemes are being trialled which create a unique digital identifier for each child, and keep a digital record of health visits, immunisations, and their interaction with trusted parties such as aid organisations. New, innovative schemes such as these, and the roll-out of digital identity schemes more widely can have a significant positive impact in enabling those without a formal means of proving their identity to do so in future.

USE CASE B

The international air travel industry carries a number of responsibilities to check passengers' identities prior to their journey, each time they travel. To put this in a global context, there were around four billion journeys by air last year with this number expected to double by 2030.[7] The ongoing reliance on a physical form of identity via a person's passport creates friction and inefficiencies for passengers and airlines.

The information required to be provided by a passenger to an airline prior to travelling internationally – Advanced Passenger Information System (APIS) data – consists of information concerning the identity of the travelling individual (name, address, DOB), their right to travel (passport details, visa), flight details and possibly accommodation details. This mix of attribute data is legally required, to:

- Verify the passenger's right to travel and to enter their country of destination.
- Enable the airline and border control to authenticate that the person whose information has been provided is the person who actually travels.
- Check against other biographic and system information.

5 https://sustainabledevelopment.un.org/sdg16
6 www.who.int/immunization/sage/meetings/2016/october/3_Regional_vaccine_action_plans_2016_progress_reports.pdf
7 oixuk.org/blog/2018/08/08/biometric-boarding-using-identity-as-a-service/

The use of a digital identity has been explored in some depth and could have a number of advantages for passengers and airlines alike:

- A digital identity solution could potentially provide the required APIS data ahead of departure.
- This could be a single, convenient low-friction transaction for the passenger, without the need to type out complex data.
- Over time, repeated use of trusted data in this manner can help the airline identify low-risk passengers, allowing a more efficient allocation of staff resource at the boarding gate.
- Digital identity schemes, such as the US 'Traveller Verification Service' enables automated biometric checking of passengers' identity, which is quicker, more efficient, and more accurate than current physical passport checks.

USE CASE C

Finally, perhaps the most complex common identity use may be that required to open a bank account, particularly online. The financial services sector around the world is one of the most heavily regulated industries, and financial institutions are required to undertake a variety of checks prior to providing an account. The bank may be required to establish to a varying degree of confidence (amongst other things):

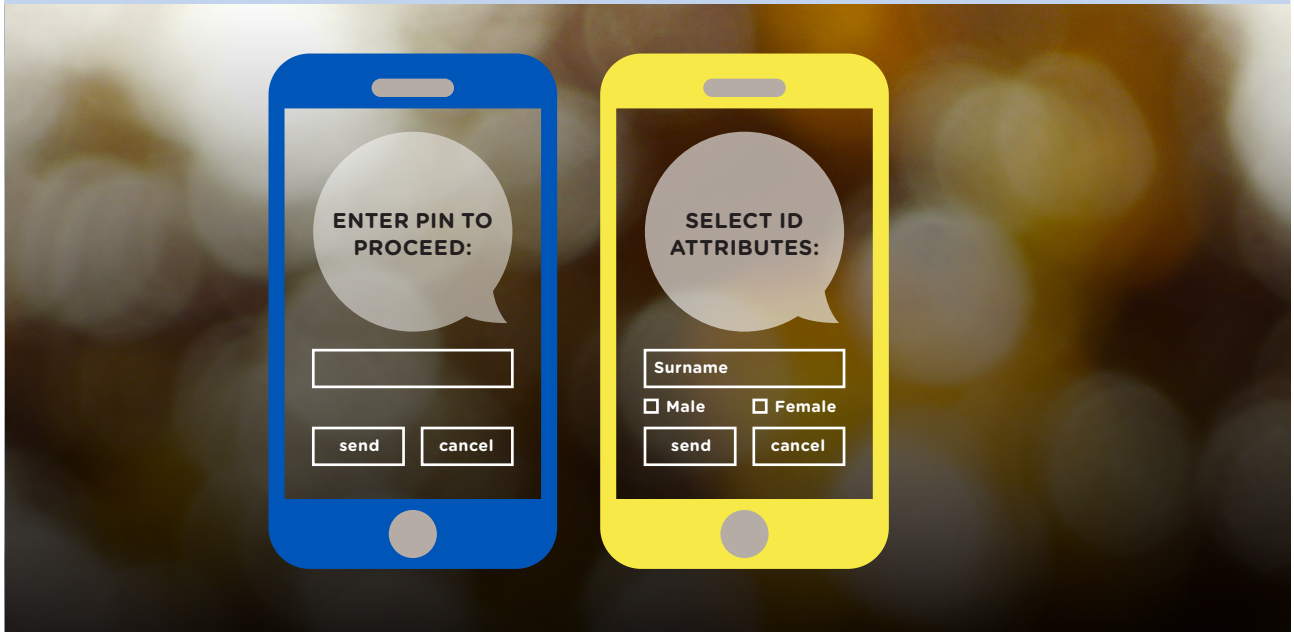
- The applicant's name, date of birth and address to prevent fraud and deception.
- The source of their funds and beneficial ownership of any assets.
- Their employment status.
- Their family and dependents.
- Their legal right to remain in the country.

The bank is required to have a particularly high degree of confidence in the customer's identity information – therefore it is required to be provided from 'trusted sources', i.e. from passports, driving licences, or to establish an address by seeing recent correspondence from a regulated entity or government organisation.

A digital identity solution that allows the individual to assert their identity credentials to the bank, and the additional personal attributes required, to a prescribed level of confidence or trust, could:

- Significantly improve the digital experience for new and existing customers.
- Potentially reduce identity-based financial exclusion.
- Enable the bank to control the rising costs of KYC.
- Enable new ways to reduce the risk of identity theft and financial crime.
- Enable customers to more easily access financial services from wherever their location, potentially across national borders.

FIGURE 1: SELF-SOVEREIGN USE CASES



CRITICAL CHALLENGES FOR DIGITAL IDENTITY SOLUTIONS TO OVERCOME

Globally there are many significant barriers to overcome *if* digital identity schemes are to thrive, and *if* self-sovereign is to provide a new and truly global digital identity approach.

1 Identity Exclusion

The World Bank have reported there are as many as 1.1 billion people without the ability to prove their identity,[8] that is one in every seven individuals. The majority live in Africa and Asia, and more than a third are under the age of 18. In these markets, these people simply do not have some attributes like a defined address or personal identifiers and credentials, e.g. birth certificates, passports and driving licences. The lack of 'originating' documents such as these has a huge impact, preventing access to healthcare, education and basic financial services, and puts many at increased of risk human trafficking, early child marriage and slavery.

Providing a means to store a local, encrypted record of 'trusted events' alongside a unique identifier, such as can be achieved by shared ledgers, can help to build a trusted digital identity that can be used in the absence of traditional identity documents.

Self-sovereign, by removing the need for a centralised 'hub' and by not necessarily requiring continual network connectivity to function, has particular advantages when delivering identity solutions for remotely located individuals.

2 Data Security

Cyber threats are ever evolving. Hacking and the associated fraud has grown exponentially over the last few years,[9] in the US alone breaches increased by 29% during 2016 – 2017.[10] Centralised schemes that store data in bulk, or without suitable encryption and security, merely create a new honeypot for hackers. Information about people's identity attributes (date of birth, address, gender, address) that they may have used to register for services, and the identifiers they may have shared (such as social security numbers or passport details) are constantly at risk from hacking, and are stolen at an estimated rate of almost five million records per day.[11] In the hands of criminals, stolen identity attributes are then used to 'take over' the identity and associated accounts.

Identity schemes all include a variety of security measures, such as the use of private keys, multi-factor authentication, and encryption of data. Emerging technologies may provide more secure means to share and store data, however no system has yet proven to be infallible.

These are explored in more detail in Technical Note No. 2.

Removing the need for attributes to be stored in a central repository, or to pass through just a few hubs, self-sovereign shared ledgers may be a means to provide additional security and protection.

3 Privacy concerns

Concerns about the degree to which individuals consent to and control the use or sharing of their personal data is also on the rise, with UK adults expressing a fear of their personal data being sold for marketing almost equal to it being stolen.[12] 70% of people in Greece, 56% in Australia and 32% in Nigeria are concerned with the amount of personal information that companies know about them.[13] There are many markets where there is little or no regulation and therefore no consumer protection.

Recent initiatives like GDPR are providing individuals with greater control over their personal data under law, limiting how and where it is processed, and with whom it is shared. The post-GDPR paradigm could provide individuals with the means to have a more meaningful relationship with their data, within the safeguards needed to ensure good data governance, privacy and security. In future, identity solutions need to enable personal control to be exerted, putting users at the centre of new scheme design.

While it's not impossible via other means, self-sovereign is by its very nature based on personal data rights and the consensual sharing of data – the very essence of what GDPR is trying to achieve.

8 www.worldbank.org/en/programs/id4d
9 www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
10 https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout
11 breachlevelindex.com
12 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/06/consumers-taking-action-over-mistrust-of-organisations-handling-personal-data/
13 connectedlife.tnsglobal.com

4 The Lack of International Digital Identity Standards

The creation of digital identity standards has been a slow process in most markets, with little to provide an interoperability framework or common standard around which schemes can be developed. There are standards that exist, such as the EU rules that have developed common levels of assurance, via the Electronic Identification, Authentication and Trust Services (eIDAS) Regulations,[14] but such standards as do exist are usually poorly aligned.

A common framework, providing interoperable national and international identity standards applying to the creation and use of digital identities, would be a significant facilitator to the development of digital identity services, and their wider use.

This may be a challenge that disproportionately impacts self-sovereign, and perhaps to a lesser extent shared ledgers. Developing standards and changing regulation are not quick processes. Given the relative recency of self-sovereign and shared ledgers' emergence into the spotlight, it may be some time to come before robust standards and frameworks are established for their use.

5 Putting Individuals in Control of their Personal Data

Recent regulation has sought to put the user more in control over their personal data. The 'right to be forgotten' in various guises has followed recent court rulings, and GDPR has put tighter restrictions around the need for specific and demonstrable consent from the consumer before certain data is shared or processed.

Explored in the next chapter, many different models of digital identity schemes can store attribute data in different places, whether centrally, at source, or stored by the individual themselves.

Providing an individual with the means to update and share their data at a time and manner of their choosing lies at the very heart of a highly user-centric digital identity model, and is a foundation to all self-sovereign digital identity approaches.

Different use cases have differing identification requirements. **Can one digital identity approach meet every requirement?**

14 https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

3 Self-Sovereign: an emerging approach to digital identity

Self-sovereign is a fundamentally different concept to most of the digital identity approaches that have been developed previously. It puts the end user, the individual, in total control of their data, and potentially enables them to manage their own personal identity attributes, the levels of trust ascribed to the data, and when and how it is shared. The individual can consent to its sharing to the recipient only, providing only the data necessary.

But how is this different from what's come before?

APPROACHES TO DIGITAL IDENTITY

Over time, different models or types of digital identity have emerged. There are many different descriptions used amongst the identity community, but for the purposes of this report we are going to call them *centralised* (often also called *sovereign*), *federated* and the most recent addition, the *self-sovereign* concept, which is a *decentralised* approach.

The essence of these different digital identity approaches is rooted in who can create, read, update and delete the digital identity, and who it can be used by.

Christopher Allen,[15] principal architect at Blockstream, last year put forward a set of principles for self-sovereign identity that serve to define it.

These are explored in more detail in Technical Note No. 1 and/or No. 3.

This taxonomy shown in Figures 2 and 3 distinguishes between 'sovereign' identities created by service providers (whether private or public) and 'self-sovereign' identities created by the real IDs (or the owners of the real IDs). We further divide the digital IDs that are not created by the end user into sovereign identities that are used only by their creators and 'federated' identities that are used by others beyond the creators. Self-sovereign identities are also intended to be used by a wide range of relying parties.

15 https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

DELIVERY MODELS FOR DIGITAL ID

While each of the approaches above is differentiated by who creates and uses the digital identity, there are also differing models affecting how identity data is stored, how it is retrieved, and how the permissioning and sharing of identity takes place.

Some identity schemes store attributes, and/or the trust and event-data relating to them, in a central repository. However, given that such schemes present significant targets for hackers, security is a very significant concern for such approaches, and must be overcome via encryption and other security measures.

Other identity schemes are based on a hub-based model. Here, a person's trusted digital identifier is used to 'unlock' and then share attributes that remain stored at their point of origin (such as at a bank, a government register). The hub model is a means to transmit the data, and/or provide assurances regarding the trust status of those attributes, to a relying party, in a standardised manner.

Shared ledger technologies are another means, explored in more detail below, where data, transaction records or attribute events are recorded via a commonly distributed ledger, and a 'key pair' is used to unlock and share the data.

FIGURE 2: DIGITAL IDENTITY APPROACHES

LAYER	CENTRALISED	FEDERATED	DECENTRALISED
WHO CREATED IT?	Created by someone else, e.g. a bank, government or other institution	Created by someone else, e.g. a bank, government or other institution	Created by the end user
WHO CAN IT BE USED BY?	End user can only use the digital identity for transaction with the creator	End user can use the digital identity for transaction with multiple service providers	End user can use the digital identity with multiple service providers

FIGURE 3: DIGITAL IDENTITY TAXONOMY

Digital Identity Schemes in Practice

There are currently many efforts underway worldwide to try to bring solutions to the digital identity market to solve online identity challenges, by governments, private sector organisations, e.g. banks, technology providers, NGOs, FinTechs and through collaborations between some or all of these.[16]

To date the vast majority of these solutions can be characterised as being either *centralised* or *federated* approaches.

Self-Sovereign Identity

More recently the self-sovereign approach has emerged. It is agnostic of technology or platform, however, as we will discover in the next chapter, it may have particular potential when considered in tandem with shared ledger.

Self-sovereign identity – the idea of providing individuals with a means to control, share and store their personal attribute data themselves, even locally on their own device – is a reflection of the emerging thinking around the privacy and use of personal data.

10 Principles of Self-Sovereign Identity

The essence of self-sovereign lies in its user-centricity, transparency and portability, which are all reflected in the 10 key principles that underpin the concept.

These are explored in more detail in Technical Note No. 4.

Self-sovereign identity in practice

A federated or sovereign identity in use requires that the user share a unique identifier and a second form of authentication (a password, or biometric record) to enable their identity to be asserted to a relying party. This information is used, commonly via a hub, to contact the identity provider (a third-party organisation) to check that the identity is current, and to check against or share the attributes with the relying party. It is therefore reliant on a hub provider, and identity provider, and connectivity to enable this to take place.

Using a self-sovereign identity is a significantly different process. Here, the attribute information is held by the individual themselves, either on their own device (commonly a smartphone), or in the cloud, and this data can be accessed or shared by the user using their personal (private) key, and usually a second authenticating factor, such as a biometric record, in combination with the public key held by the relying party, which will identify the specific information required for the task in hand.

For example, to provide proof that the user is over 18, rather than the user needing to access this information via a third-party hub and then via an identity provider,

FIGURE 4: 10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY

PRINCIPLE	DEFINITION
EXISTENCE	Users must have an independent existence in the 'real world'
CONTROL	Users must control their identities
ACCESS	Users must have access to their own data
TRANSPARENCY	The systems and algorithms used must be transparent
PERSISTENCE	Identities must be long-lived
PORTABILITY	Information and services about identity must be transportable
INTEROPERABILITY	Identities should be as widely usable as possible
CONSENT	Users must agree to the use of their identity
MINIMALISATION	The disclosure of claims for a given transaction must be minimised
PROTECTION	The rights of users must be protected

16 www.openidentityexchange.org/cost-of-doing-nothing/

in a self-sovereign example that information (that they are over 18) is held on their device. This may be physically on the device in an encrypted form, or held in the cloud. In either case the relying party will provide a public key (which is specific to an age-verification process), and this combined with the user's private key enables the information to be provided to the relying party. Usually in age verification this can be achieved via a simple yes/no answer, which prevents their actual date of birth from being shared unnecessarily.

A knowledge-based or biometric verification at the time will ensure that the identity record belongs to the intended individual.

Digital identity delivers many envisaged benefits, so why is it **so difficult to deploy?**

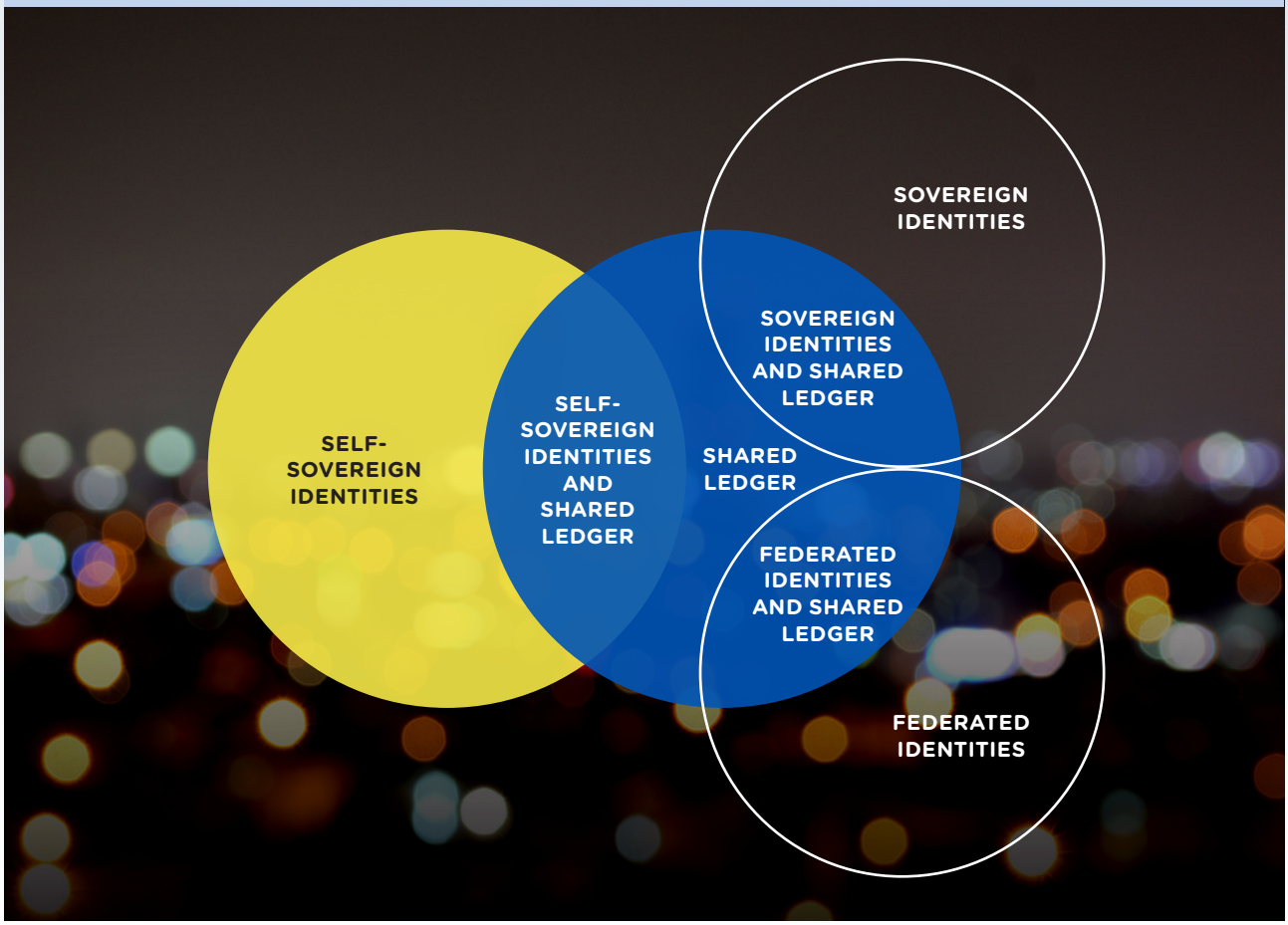
4 Self-Sovereign and Shared Ledger: a powerful combination

In recent years, alongside (and even preceding) the emergence of self-sovereign, there has been a great deal of hype regarding Blockchain and the broader concept of Shared Ledger technologies that underpin a new approach to storing, updating and sharing information.

The early hype has now developed into a growing maturity for shared ledger approaches, and they are being used for a growing variety of digital identity schemes, as well as other types of data management uses across multiple sectors, and of course underpinning crypto-currencies.

Self-sovereign identities are not dependent on any specific technology type, there are cloud or device-based examples that do not include a shared ledger at all. However, of late shared ledger technology has been mooted as the ideal approach to making self-sovereign identities a more viable option, by providing an underlying technology and scheme architecture capable of delivering a truly decentralised but secure solution, and increasing the degree of trust in the data, due to the relative immutability of the ledger record.

FIGURE 5: THE FLEXIBILITY OF SHARED LEDGER APPROACHES



WHAT IS A SHARED LEDGER?

A ledger is a view of the current state of a marketplace, and all the transactions that led to that current state. A shared ledger provides a shared view of the 'truth' about the current state of the marketplace. In pre-digital times, we used to have to trust someone to maintain this ledger of transactions. Then a federated approach began to develop in which each organisation maintains its own part of the ledger.

Today, technological advances in networks and device-based storage and capabilities mean that it has become possible for all market participants to be able to store everything and to resolve, in a reasonable time, discrepancies between the different copies. Massive replication of data across devices and organisations is the core principle of the shared ledger technology.

These kinds of shared ledger promise a new way of addressing the old problem of maintaining a transaction ledger across multiple organisations, which is to give them all a copy of all the data.

Note that this does not mean that all organisations can read or understand all of the data, merely that they are holding a copy of it. A 'key' is required to be provided to unlock data pertinent to a particular entity or transaction.

These are explored in more detail in Technical Note No. 5.

Ultimately, whilst the original blockchain model has useful elements, and indeed is able to provide a shared ledger function, its original purpose was infrastructure for the cryptocurrency Bitcoin. This means that there are areas of the bitcoin blockchain design, such as its permissionless nature, that are challenging for the purpose of delivering digital identity. However other variants of shared ledgers hold great promise for digital identity.

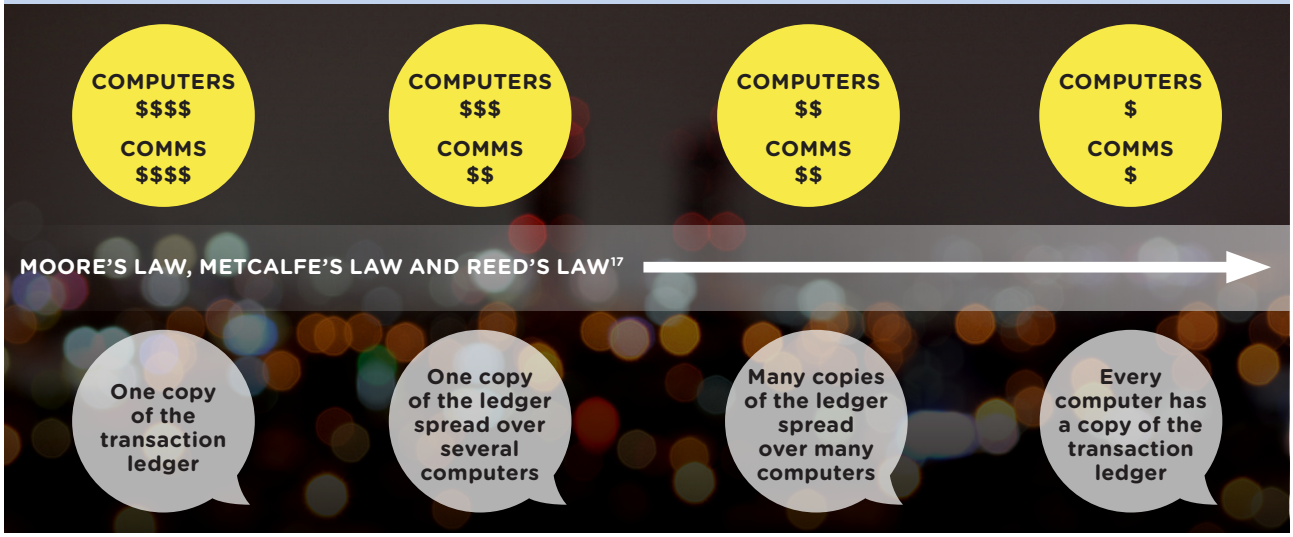
IS IT BLOCKCHAIN OR SHARED LEDGER? I'M CONFUSED!

Even after many years of commentary, many remain confused regarding the often-conflated terms 'blockchain' and 'shared ledger'. Let us remind ourselves of their origins…

In November 2008, a paper was posted to a cryptography mailing list under the name Satoshi Nakamoto, entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*. This paper detailed innovative methods of using a peer-to-peer network to generate what was described as "a system for electronic transactions without relying on trust". Whilst perhaps not the first, it is the most discussed *blockchain* example, implemented in 2009.

The word 'blockchain' itself actually describes a specific format of data ('blocks') which are linked by cryptography that makes up a blockchain ledger. The bitcoin blockchain design has subsequently been the inspiration for other variants of this type of decentralised technology. We call this larger family of distributed ledger approaches 'shared ledgers'.

FIGURE 6: HOW THE EVOLUTION OF LEDGERS RELATES TO THE SCALE OF TECHNOLOGY AND NETWORKS



17 Moore's Law refers to the doubling of computer processing power on average every two years. Metcalf's Law and Reed's Law are differing ways to value a network based on its size.
http://www.mooreslaw.org
www.networkworld.com/article/2225509/cisco-subnet/understand-and-obey-the-laws-of-networking.html

TYPES OF SHARED LEDGER

Permissionless (public ledgers)

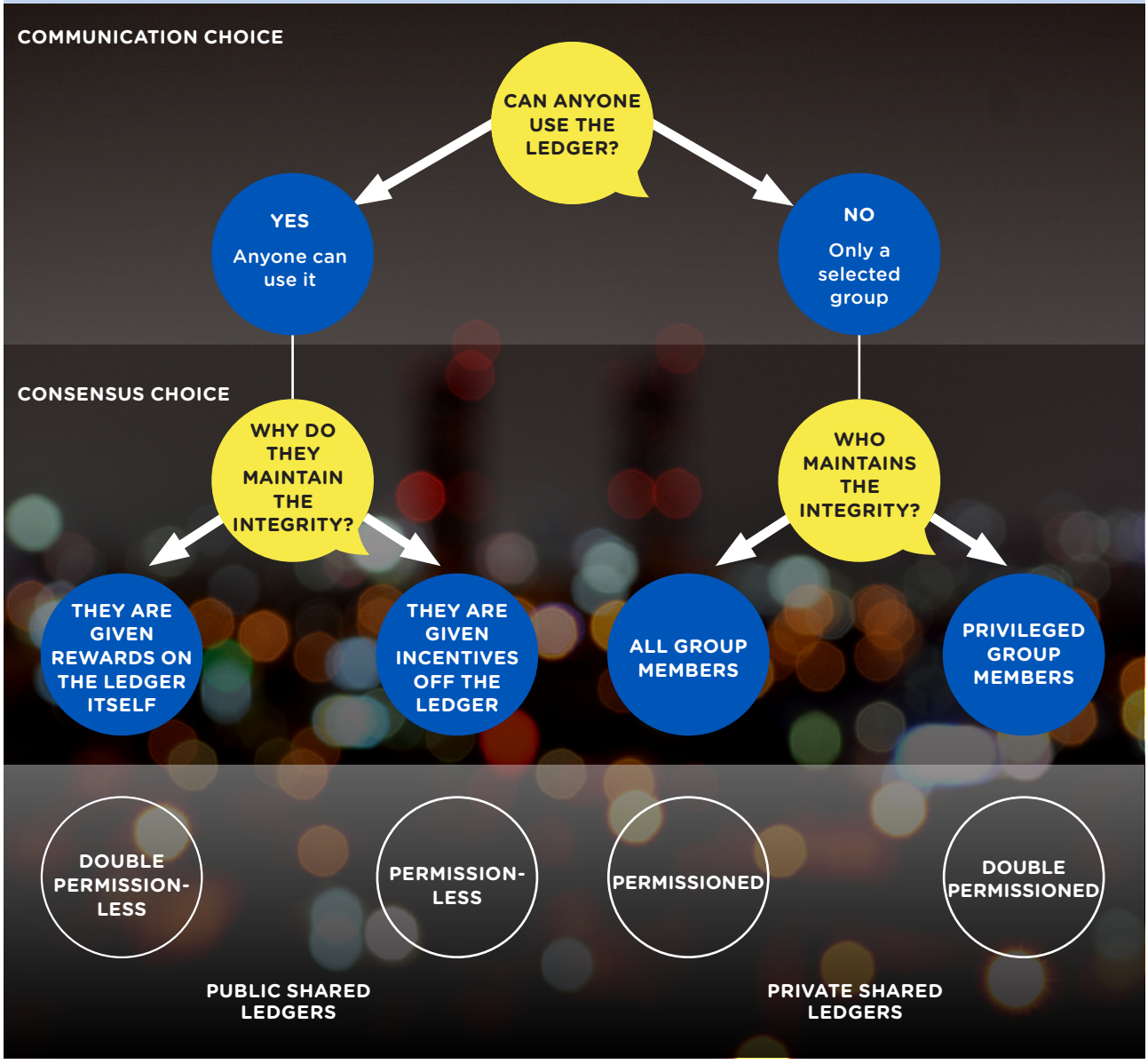
Despite being the most widely known type of shared ledger, Bitcoin is a very special case, an instance of a so-called 'permissionless' shared ledger. A permissionless ledger is open to everyone to use, there is no need for any individual or organisation to allow you to be a part of the ledger: to view, transact or maintain it. Instead, in building a system that does not rely on trusted entities to maintain the ledger, the breakthrough of Bitcoin was to create the closest system yet to 'digital cash', a digital asset that you can own outright and transfer to anybody else without permission.

Permissioned (private ledgers)

For most other situations, the maximum degree of decentralisation provided by Bitcoin presents problems relating to confidentiality and data protection, and for this reason many stakeholders are looking closely at permissioned (i.e. private) ledgers as an alternative. In permissioned ledgers all parties to the transactions in a given system are known, identified ('permitted' to use it), and thus able to be held accountable for their actions. A permissioned ledger may therefore prove more attractive to regulated uses.

These are explored in more detail in Technical Note No. 6.

FIGURE 7: SHARED LEDGER CLASSIFICATIONS



SO WHY SHARED LEDGERS?

There is a fundamental question to ask about this focus though: why? If you do not have protection from censorship as your business objective, and therefore looking to a private ledger, why look at a shared ledger at all?

Rather than maintaining a central database or network of interconnected databases, a shared ledger means we can build more robust solutions where database attacks or corruption do not stop the replicated ledgers from working. This would mitigate the problems encountered when a centralised identity system fails, paralysing the transactional space dependent on it. A shared ledger has inherent redundancy built within it; it is a resilient solution.

Shared ledgers can solve another problem relevant to self-sovereign approaches: if marketplace participants all run similar systems to keep track of self-sovereign digital identities, then all participants are paying to maintain these duplicated undifferentiated records. And, because they may be slightly different, each participant needs to reconcile them with others all the time to make sure they agree. One argument for using private shared ledgers is therefore that you can mutualise the cost of running and securing a single logical ledger, with relevant data copied across organisations so each has its own copy and is not reliant on a powerful central entity for access.

PERMISSIONED VS PERMISSIONLESS LEDGERS

The permissioned ledger also provides a cross-organisational transparency, integrity and accountability that is appealing to regulators as well as participants.

Permissionless ledgers, while reflecting the 'pure' essence of self-sovereign via a truly decentralised system open to any user, the challenges in adopting this for identity uses will be in the relative open governance and challenges in tracking events and attributing the events to individual users. This may be suitable for some uses, but a closed permissioned ledger is usually deemed more suitable for B2C uses, which make up the majority of identity transactions.

The greater governance and audit trail enabled by a permissioned ledger makes commercialising the processes involved in identity transactions much easier and enables a defined trust environment to be developed amongst relying parties and users.

However, permissioned ledgers are not without their challenges – as a closed system it can be less advantageous in terms of providing wide access, and can further fragment the identity market. Finding ways to enable interoperability between permissioned ledgers, probably by developing common and robust standards, may be crucial before mass adoption can be achieved.

A shared ledger has inherent redundancy built within it; **it is a resilient solution**.

5 Benefits and Challenges

In this next section, we review some of the benefits and considerations when looking at the application of self-sovereign and shared ledger approaches in the context of bringing identity solutions to the mass market, and meeting the challenges explored earlier in the report.

Where a number of organisations are developing exciting solutions is in the intersection between both shared ledger and self-sovereign identity, which in theory look like highly aligned approaches.

Supporters of this combined approach see specific benefits, by allowing users to prove things about themselves using decentralised, verifiable identifiers and by so doing replicating the way they do it offline today; rather than sharing their physical proofs of identity, they are enabled to do so digitally.

ASSESSING THE POTENTIAL BENEFITS AND CHALLENGES

What benefits and challenges arise from the application of self-sovereign digital identity in practice?

Self-sovereign identities could **enable individuals to build an identity over time** from multiple sources.

The approach places a lot of responsibility on the individual, much more than is the case today. **Are we ready for this level of responsibility?**

SELF-SOVEREIGN IDENTITY: BENEFITS

IDENTITIES CAN BE CONTROLLED BY THE INDIVIDUAL Ultimately, because the individual user is the best source of information about their life (e.g when they were born, opened their first bank account, took out their driving licence) they are best placed to connect this information versus an organisation trying to do this for them. This means service providers could enable the individual to curate the information they need (assuming the information can be trusted), leaving less onus on the organisation.

SUPPORTS COMPLIANCE WITH PRIVACY REGULATIONS Self-sovereign identities may help reduce the burden of privacy regulations such as the GDPR, as the user is in control of their identity and data, and consent can be actioned and recorded. This may mean that the service provider may be able to reduce their data compliance burden, by reducing their need to hold personal data about the customer.

IDENTITIES THAT CAN GROW OVER TIME Self-sovereign identities could enable individuals to build an identity over time from multiple sources; these may include both *traditional sources* (e.g. driving licences and passports), which may not be available to some users, and a record of their *transactions, interactions* and *attribute events* that can collectively build a trusted identity. This approach may help to address inclusion issues and lack of foundational identity in some countries and regions. It may also enable financial service firms to improve the trust they hold in an existing customer's identity, reducing their risk exposure.

IDENTITIES THAT CANNOT BE TAKEN AWAY Supporters of self-sovereign (and many within the identity community more widely) see identity as a fundamental human right, and as such discourages political and commercial structures that would seek to undermine that right, intentionally or otherwise. The degree of encryption, personal control and the historical ledger available from a self-sovereign shared ledger approach help to protect an individual's identity from interference.

RESOURCE EFFICIENT The widespread adoption of smartphones in many countries has brought a great amount of decentralised processing power into the hands of individuals. Centralised digital identity schemes suffer from issues of accommodating scale, and significant design complexity, with significant cost to build the infrastructure required. However, decentralised approaches, particularly self-sovereign, mutualise costs and the provision of processing power.

SELF-SOVEREIGN IDENTITY: CHALLENGES

IDENTITIES NEED TO BE TRUSTED *Providing identity assurance* – If a user self-asserts their identity, the collection of trusted identity attributes does not in itself provide an assurance that the individual in question is who they purport to be (apart from their say-so). This assurance needs to come from somewhere.

Trusted sources – the solution also needs to provide sufficient assurance that other service providers would trust. For example a bank might trust a government's own records about a user's identity, and so on. Authoritative sources are a critical part of the self-sovereign ecosystem, to validate that the information being presented is correct. How these organisations are incentivised to participate and gaining scale of participating organisations is as yet unproven.

ARE USERS READY? Self-sovereign requires the user to be provided with a means to manage their private cryptographic keys (e.g. through a specific key) which can then be used to access or share their personal data. The potential for an individual to lose access to their self-sovereign identity (e.g. through loss or theft of their private keys through losing their smartphone, or having it stolen) could be catastrophic to the individual. This places a lot of responsibility on the individual, much more than is the case today. Are we ready for this level of responsibility?

SELF-SOVEREIGN IDENTITIES RELY ON THE AVAILABILITY OF TECHNOLOGY AND INTERNET INFRASTRUCTURE Most of the self-sovereign solutions are reliant on a smartphone being available to the individual, as this is used for key management. The rate of smartphone penetration is below a third of the population in the least developed and developing countries in the world.[18] There is some way to go to make solutions reliant on smartphone technology a viable option in these regions.

UNCLEAR HOW CRITICAL MASS CAN BE ACHIEVED Gaining critical mass in identity systems is the primary challenge. The concept of self-sovereign identity may be unfamiliar to organisations could potentially become relying parties for self-sovereign identities. While in the long term the concept may be attractive, in the short term this will require a network effect to gain traction through compelling use cases. The type of rapid and immediate enrolment and adoption that has been achieved by bank-led schemes, in the Nordics for example, is likely not to be a realistic option for emerging self-sovereign schemes, however achieving adoption is a make-or-break factor for any identity scheme.

REGULATORY AMBIGUITY For many sectors who may be willing to accept self-sovereign identities, there will be significant regulatory barriers to cross. Financial services markets with their KYC and Anti-Money Laundering requirements may find there is a perceived change in risk of accepting an identity that is self-sovereign which may slow down adoption, particularly given the few existing or established industry standards for digital identity generally, and self-sovereign identities specifically.

18 https://www.indexmundi.com/g/r.aspx?v=4010

Shared ledger approaches also have a number of issues arising, both positive and more challenging in nature:

SHARED LEDGER: BENEFITS

MORE EFFECTIVE PREVENTION OF BAD ACTORS CONTINUING TO CIRCULATE Ledgers are not a good place to store personal data (see challenges) but could be a good place to store ancillary information which supports identity systems. These mechanisms could be leveraged to combat some of the longer-standing issues with identity infrastructures. If in practice the identity information is stored off the ledger, but the cryptographic key mechanisms to access it are dealt with on the ledger, then if an identity is compromised that information can be shared easily (because it's a shared ledger) rather than (as is the case today) relying on a central authority to deal with it.

The ability to provide a consistent and robust mechanism for cryptographic key revocation is critical to identity solutions. Shared ledgers offer a way to remedy this long-standing issue with identity systems, in a more robust way than has been possible before, and at minimal expense.

PROVIDES TRANSPARENCY By retaining a ledger of previous 'attribute events' and transactions concerning the use of the individual's identity attributes, shared ledgers can provide a vital chain of trust and a transparent (and securely encrypted) record of an individual's transactions and their changing attributes over time.

REMOVES A SINGLE POINT OF FAILURE The nature of a shared ledger means it is stored and operated in many places. This means there is not a single point of failure (for any of the information which is being stored and accessed on the ledger) because it is replicated in other locations. This removes the reliance on a single central authority, and if one actor goes down it does not affect the network.

SHARED LEDGER: CHALLENGES

IT'S NOT USEFUL FOR ALL TYPES OF DATA SHARING The fact that ledgers are immutable means they are not a good place to store personal data directly (e.g. identity attributes), even if the data is encrypted. This is because this method of storage of personal data would conflict with many privacy laws (e.g. The General Data Protection Regulation where the GDPR requires users to be able to request the deletion of their personal data, an immutable ledger by its very nature makes this impossible).

THERE ARE NO ACCEPTED STANDARDS OR PROVEN GOVERNANCE MODELS Very few standards or established models exist concerning how digital identity on shared ledgers should work in practice. Governance issues may be more difficult to resolve in a decentralised system unless clear rules are set out for actors in the network. A trust framework in a decentralised scheme still needs to be developed, yet very few working examples exist as a reference point.

INCENTIVES AND COST In relation to those identity services that use shared ledger technologies there are a number of considerations concerning the types of ledger, whether permissionless, double permissionless, permissioned or double permissioned:

1. Any identity built upon a financially incentivised permissionless ledger has an inherent cost (e.g. bitcoin). This cost may destroy the viability of identity use cases.
2. The alternative would be a permissioned ledger where there is no financial incentive. However, because there is a processing cost to users becoming a node on the network, nodes (users) would be incentivised to remain part of the network. As the network scales, so would the cost of running a node.
3. The third alternative is a double permissioned ledger which is funded between organisations. This would not be open to pricing volatility nor would it require external funding.

6 Conclusions

In practice, it is true that neither a self-sovereign approach, shared ledger technology, nor the application of both combined can completely address all of the many identity challenges experienced by individuals, nor the barriers to market success faced by traditional digital identity schemes.

That said, it's clear that a combined approach could deliver a number of valuable benefits:

- By building up an immutable record of trusted attribute events and identity transactions and engagements of a variety of types, a trusted identity can be developed over time, even in the absence of traditional identity documents such as birth certificate, passport or driving licence.
- A self-sovereign shared ledger approach therefore has significant potential to overcome some identity access and inclusion challenges, particularly in developing economies, but only if the technology isn't prohibitively reliant on access to smartphones.
- The need to provide the user with a greater degree of personal data control can be solved with a number of scheme architectures, but only the self-sovereign approach takes an inherently user-centric model, providing unparalleled level of user-control, consent management and ultimately access to data, and removes the reliance on a small number of identity providers, whether GAFA or government.
- The fact that self-sovereign approaches are not dependent on major infrastructure providers and third-party organisations inherently makes such systems more robust and less at risk of single-points of failure.

Yet there remain some challenges to overcome:

- If barriers to accessing new forms of digital identity remain unsolved, new technology will merely replace existing solutions – great for those who can already access them, but of no advantage to those currently suffering from various forms of identity exclusion. The self-sovereign and shared ledger approaches provide no general panacea when considered in isolation – improving access is critical whatever the shape of the solution.
- The degree of innovation involved, and the departure from existing 'traditional' identity processes involved in deploying a self-sovereign shared ledger approach is itself a potential barrier to adoption, particularly for heavily regulated relying parties.
- The adoption of digital identity, and self-sovereign approaches in particular, have yet to be considered in depth by most (if not all) national regulators, which adds to regulatory risk for relying parties. The lack of national and international standards limits interoperability between identity solutions, whatever their base architecture, and makes it much harder to create trust frameworks between users, scheme operators and relying parties.

A combined self-sovereign, shared ledger approach is hugely exciting in its potential. The recent technological advances in mobile technology, the need to address ongoing identity exclusion, and the sheer cost of meeting tighter KYC and AML requirements will provide fertile ground for the development of a new digital identity meta, given time.

WHAT IS THE RECIPE FOR FUTURE SUCCESS?

Greater Confidence in the Technology

Widespread awareness and confidence in the technology will grow over time. The adoption of new technologies often grows slowly at first, and then something serves as a catalyst for more rapid adoption – the start of the 'hockey stick' graph. Shared ledgers are making a more noticeable impact for businesses across a range of uses, and deployment is certainly increasing, and this should help raise awareness and confidence, but self-sovereign remains a relatively under-exposed approach at present.

Developing Standards

Technical standards to underpin these technologies, and digital identity more widely, remain relatively few at present, particularly internationally. Until the growing need for common standards in this space is more fully addressed, whether by regulators, government or industry itself, market fragmentation will not be addressed, and the development of trust frameworks will be more challenging.

Regulatory Clarity

Alongside the development of standards, consideration of these technologies by regulators, and how they sit within the rules and best practice relating to KYC/AML will be critical to enable regulated industries to adopt these types of solutions.

Relying Party Uptake

The take-up by relying parties – and the three factors highlighted above will help to facilitate that – will be critical. Without organisations willing to accept a self-sovereign identity, it becomes worthless to the creator, and the operator of the system that underpins it. Having a range of relying parties is probably THE critical success factor for identity schemes.

Ultimately, it remains too early to judge if the self-sovereign and shared ledgers approach will genuinely live up to the hype and become the new dawn for digital identity.

But watch this space...

Glossary

TERM	DESCRIPTION
ATTRIBUTES	Attributes are unique traits relating to an individual, such as name, DOB and address.
ATTRIBUTE EVENT	See 'Trusted event' below.
ASSURANCE	A level of confidence and certainty.
AUTHENTICATION	Establishing truth or genuineness, generate an assurance of credential or identity.
BIOMETRICS	Biometrics refers to measurements related to human characteristics. In an identity sense this may be a recording of fingerprints, a facial image or iris scan, but also includes behavioural characteristics.
BIOMETRIC AUTHENTICATION	Biometric authentication is the use of a biometric check to authenticate an identity or claim against previously verified biometric data.
BLOCKCHAIN	A public ledger used to register transactions, and often utilised to enable a market in digital currencies.
CREDENTIALS	A credential is a set of claims made by an entity about an identity.
CRYPTOGRAPHY	An advanced form of encryption, based on mathematical formulas and advanced technology.
DIGITAL IDENTITY	A digital reference or designation used to distinguish a unique and particular person, organisation, or device.
ENCRYPTION/ DECRYPTION	Encryption is the process of converting ordinary information (plaintext) into unintelligible text (ciphertext). Decryption is the reverse, moving unintelligible ciphertext back to plaintext.
END USERS	The entities trying to assert proof of their identity in an identity system, e.g. individual people.
FEDERATED IDENTITY	An identity scheme created by a collection of organisations operating as a federation, to share trusted data between them. The resulting identities can be used across the various entities participating in the scheme. The federation is usually supported by a trust framework and standards to support interoperability.
FIXED CHARACTERISTICS	Inherent characteristics about an individual that do not change over time, e.g. Date of Birth,
HASHES OF DATA	A hash function is used to map data of arbitrary size to data of a fixed and pre-determined size.
KEY / CRYPTOGRAPHIC KEY	A string of unique data using cryptographic techniques, that can be used to unlock encrypted specific data.
KNOW YOUR CUSTOMER (KYC)	KYC is the process many organisations have to undertake to establish a customer's identity, and to support a risk-based onboarding process. It is designed to limit the incidence of financial crime.
METADATA	Metadata describes other data. It provides information about a certain item's content.
IDENTIFIERS	Issued usually through some kind of process, possibly a verification and validation process of characteristics and attributes. Different identifiers have different levels of assurance dependent on the process behind them.
MULTI-FACTOR AUTHENTICATION	An authentication process requiring at least two independent sets of credentials – e.g. a password and a successful biometric check.
RELYING PARTY	A service provider who is using the trusted identity credentials provided by a third party.
SELF-SOVEREIGN IDENTITY	The concept of portable, decentralised digital identity, based on individuals storing their personal identity data locally, often on their own devices, and able to assert it to relying parties at a time and manner of their choosing.
SHARED LEDGER	A replicated and immutable ledger of transactions.
SOVEREIGN IDENTITY	An identity solution created and managed by a single entity, and that can only be used in transactions with that originating entity.

TERM	DESCRIPTION
TRUSTED SOURCE	Most commonly considered to be a regulated or government organisation or register.
TRUSTED EVENT	An observed and verifiable interaction involving a new or changed attribute claim involving one or more trusted sources. This can both build trust in the claimed attribute and help to build a trusted identity itself over time.
UNIQUE IDENTIFIER	A numeric or alphanumeric string that is generated automatically and that uniquely distinguishes between persons without the use of any other identity attributes.
VARIABLE CHARACTERISTICS	Inherent characteristics about an individual that can change over time, e.g. biometrics such as fingerprints, or gender.
VALIDATION	The process of ensuring that the characteristics, attributes and identifiers exist.
VERIFICATION	The process of ensuring that the characteristics, attributes and identifiers belong to that individual.
VIRTUAL IDENTITY	An identifier and a collection of identity attributes, entitlements and authentications claimed by an individual, held in computers and other digital storage.
ZERO-KNOWLEDGE PROOFS	A zero-knowledge proof is when a prover convinces a verifier that they have some secret knowledge, without revealing the knowledge directly. In other words, a program can have secret inputs and the prover reveals nothing to the verifier.

Technical Notes

Technical Note No. 1
BUILDING BLOCKS OF DIGITAL IDENTITY

A *digital identity* is not a *real-world identity* (whatever that may be) that exists entirely independently from computers and networks, nor is it simply a *virtual identity* made up of an individual's attributes, entitlements and authentications that exist within computers and networks.

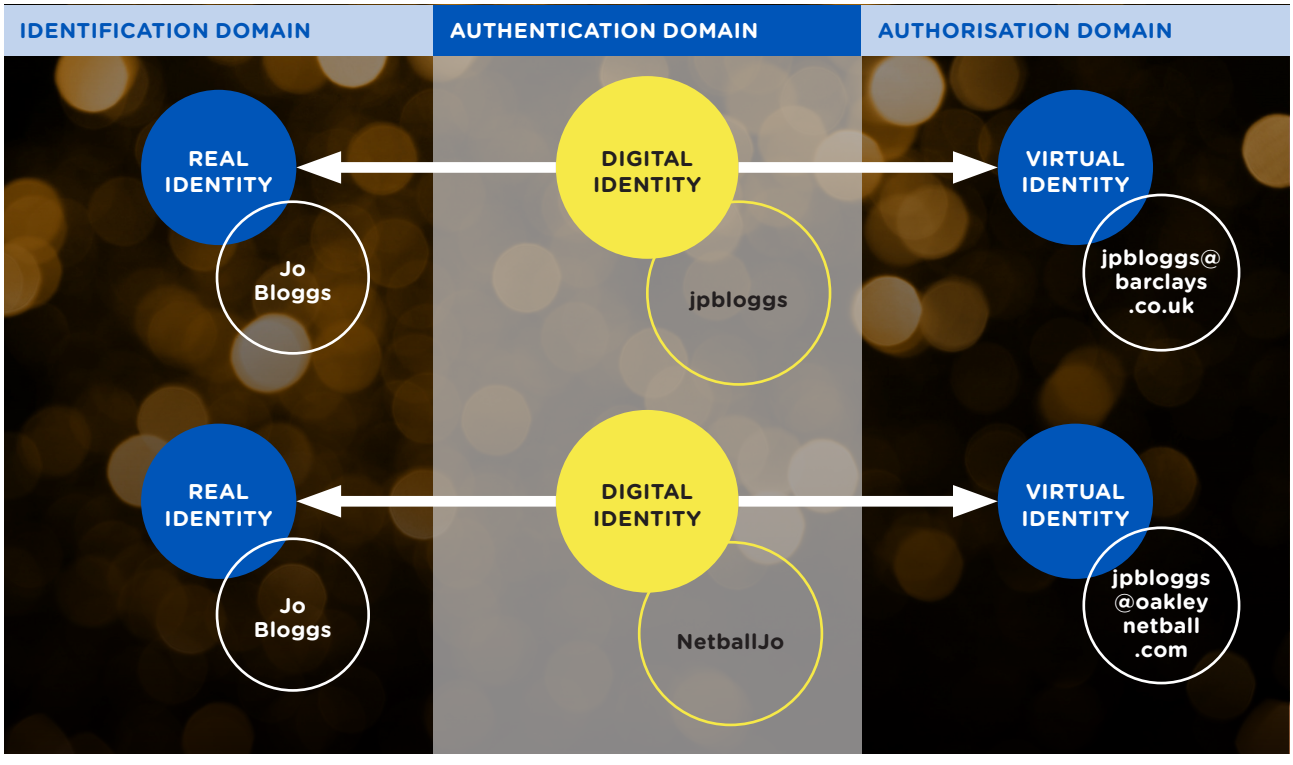
Instead, the specific collection of data and connections that make up a digital identity will vary depending on the individual, its context or use, and other factors defining the intended transaction.

Indeed, an individual can have a number of digital identities. There may be several reasons why people may choose to do so. For one example, there are probably several executive officers of a major company who are signatories to the corporate bank accounts and legally able to form contracts on behalf of the company.

Conversely, there may be digital IDs that are linked to a great many virtual IDs, each representing specific collections of attributes, entitlements and credentials. An individual, let's say *Jo Bloggs*, may have a Tesco ID, a British Airways ID, a Shell ID and a Boots ID that are all connected to the same 'Jo at home' digital ID.

Quite separately she may have an Innovate Identity ID and an Omidyar Network ID, also linked to a separate 'Jo at work' digital ID. As shown in Figure 8, we assume that people are in practice likely to have a small number of digital IDs from different sources, just as they tend to have a small number of credit cards from different sources.

FIGURE 8: PEOPLE WILL HAVE MULTIPLE DIGITAL IDS



Technical Note No. 2
CRYPTOGRAPHY, AND PUBLIC AND PRIVATE KEYS

Cryptography can be used to create a cryptographic 'key pair', one public and one private, perhaps held via an app on a smartphone or computer. As it sounds, the public key can be made public to anyone, while the private key must be known only to the party who will decrypt any data, i.e. the end user.

Users can freely distribute the public key, for example with anyone or organisation with whom they wish to assert their digital identity, while keeping the private key secret. This cryptography enables higher levels of security to be achieved in digital identity systems.

Keys provide the means to unlock identity. The link between real identity and digital identity is the binding of a private key to something in the real world, and the link between a person's digital identity and their virtual identity (identity attributes, entitlements and authentications) as the binding of a public key to information held in the virtual world. To take an obvious example, a 'chip and PIN' card contains just such a key pair.

Connecting the public and private key is the manner in which an identity is shared between the two parties involved in a transaction.

Technical Note No. 3
DIFFERENT IDENTITY DOMAINS

Asserting an identity digitally is a process that is often described as taking place in a number of 'domains'. In the *identification domain* a binding is created between something in the real world (such as a person) and a digital ID. For example, to create a Bank ID, a person might need to provide a passport and a proof of address via a utility bill for the bank to make the binding. In practice, we connect the thing in the real world to a private key.

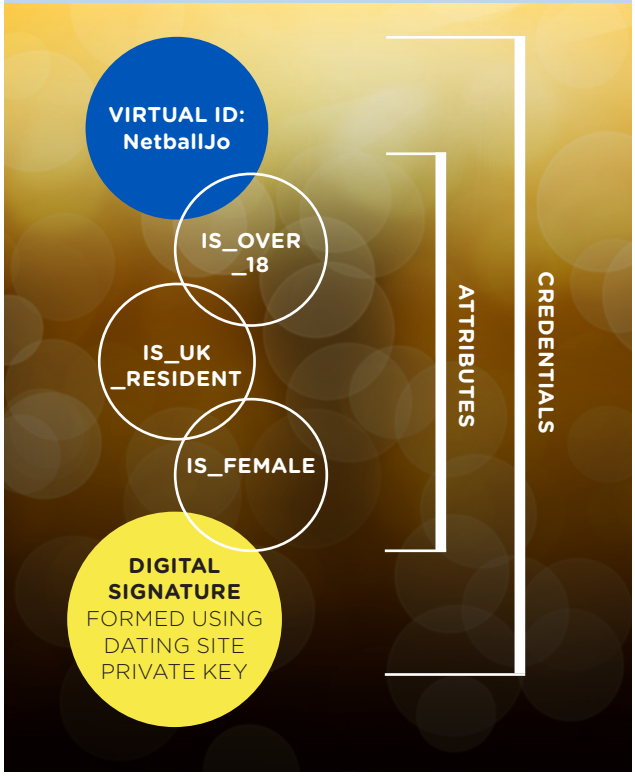
In the *authentication domain*, a real identity can demonstrate their control over a private key, for the purposes of completing a transaction, through an authentication process of some kind (e.g. a PIN, or a biometric reading).

In the *authorisation domain*, virtual IDs are bound to digital IDs. This is achieved by binding the public key of the digital ID to an identifier, often with a few different attributes required for the transaction to take place.

As shown in Figure 9, these attributes become credentials that are of value in transactions when associated with the public key. This can be achieved in this model by having a third party digitally sign the combination of the public key and the attributes.

Therefore, the transactions between entities take place in the authorisation domain. There are many reasons for wanting this to be the case: we want transactional privacy (we do not need real IDs for almost all transactions), we want attribute-based authorisation, and we want to allow a defence against correlation.

FIGURE 9: A VIRTUAL ID IS AN IDENTIFIER AND A SET OF CREDENTIALS



Technical Note No. 4

THE PRINCIPLES OF SELF-SOVEREIGN IDENTITY

The 10 Principles of self-sovereign identity are expanded here, to provide a more technical understanding of what they entail.

FIGURE 10: 10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY

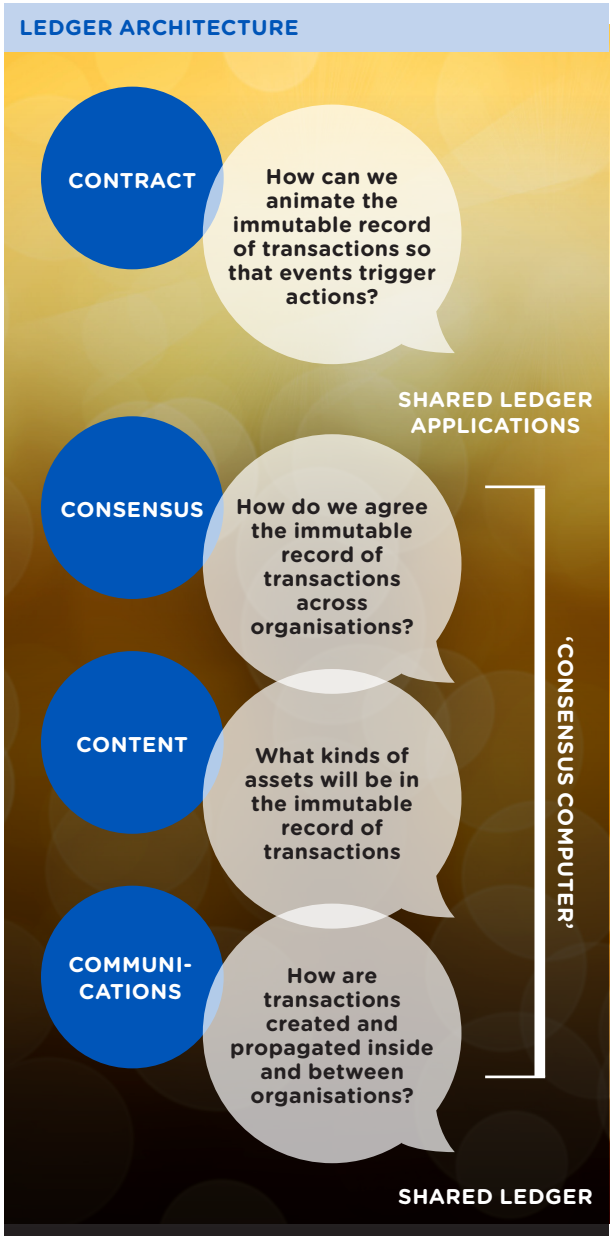
PRINCIPLE	DEFINITION	NOTES
EXISTENCE	**Users must have an independent existence**	Any self-sovereign identity is ultimately based on the ineffable 'I' that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the 'I' that already exists.
CONTROL	**Users must control their identities**	Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer to it, update it, or even hide it. This doesn't mean that a user controls all the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.
ACCESS	**Users must have access to their own data**	A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. It does not mean that users have equal access to others' data, only to their own.
TRANSPARENCY	**Systems and algorithms must be transparent**	The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture.
PERSISTENCE	**Identities must be long-lived**	Preferably, identities should last forever, or at least for as long as the user wishes, or until they've been outdated by newer identity systems. Though private keys might need to be rotated and data might need to be changed, the identity remains. This must not contradict a 'right to be forgotten'; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time.
PORTABILITY	**Information and services about identity must be transportable**	Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear, or users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity.
INTEROPERABILITY	**Identities should be as widely usable as possible**	Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.
CONSENT	**Users must agree to the use of their identity**	Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. *[Note that this consent might not be interactive, but it must still be deliberate and well-understood.]*
MINIMALISATION	**Disclosure of claims must be minimised**	When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques. Non-correlatability is still a very hard (perhaps impossible) task but applying minimalisation supports privacy as best as possible.
PROTECTION	**The rights of users must be protected**	When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralised manner.

Technical Note No. 5

THE BUILDING BLOCKS OF SHARED LEDGERS

One way to consider how shared ledgers work in practice is to start by considering the basic building blocks of the shared ledger. We see these comprising four layers, shown in Figure 11 below. These are the communications, contents, consensus and contracts layers, each of which leads to a different driver for the use of a shared ledger rather than a database.

FIGURE 11: A FOUR LAYER MODEL FOR LEDGER ARCHITECTURE



Source: Consult Hyperion[19]

Communication Layer

This layer is where shared ledgers use consistent cryptographic rules to create transactions and propagate them across networks, and which ensure the security and robustness of the system.

Content Layer

This layer records the ownership of 'assets' in the immutable ledger of transactions in a standardised way. These assets need not be limited to finance, and when *smart contracts* (see below) are paired with '*smart property*' — where deeds, titles and other certifications of ownership are put in digital form — these contracts can allow for the automatic transfer for ownership of a physical asset.[20]

Consensus Layer

This layer provides a mechanism to reach system-wide agreement over the things that are written into the ledger, to maintain the integrity of the transaction history. Since copies of the ledger are held by some or all of the participants, there must be a mechanism for determining which copies are true in the event of discrepancies that might be caused by delays, errors or fraud. This is known as a 'consensus mechanism' and it varies according to the type of ledger.

Contract Layer (aka Smart Contracts)

Above the consensus layer is what has become known as the contract layer, also referred to as Smart Contracts, that serves to add enhanced business logic to the shared ledger. Smart contracts might be better labelled shared ledger application programs (SLApps).[21]

Control Layer (aka Governance)

Private (permissioned) ledgers also add a further fifth layer to the model to manage identities of the participants, and 'permissions' given to them on the ledger. Such a governance layer is a main point of organisational control for shared ledger: it manages the admission to use the ledger, distribution of roles and permissions and resolutions of disputes. The control layer is especially important in the context of SLApps that are executed autonomously after the conditions are pre-established and agreed upon between parties.

19 www.chyp.com/shared-ledger-applications-and-the-bouvier-sams-boundary/

20 Vigna, P. and M. Casey, The Everything Blockchain, in The Age of Cryptocurrency—How Bitcoin and Digital Money Are Challenging the Global Economic Order. p. 219-245 (St. Martin's Press: New York, NY: 2015).

21 Birch D. Brown R. and S. Parulava. 'Towards ambient accountability in financial services: shared ledgers, translucent transactions and the legacy of the great financial crisis.' Journal of Payment Strategy and Systems, Vo. 10, No.2. p.118-131 (2016).

Technical Note No. 6
WHAT IS BEING STORED ON THE LEDGER?

Figure 12 divides the specific data that is stored on the ledger into four categories of increasing complexity and functionality.

The first use of the ledger in our diagram below is to store the *hashes* relating to data that is held elsewhere, thus providing a timestamp and integrity check on the data. So, for example, a system might take an image of a driving licence, store that image in a database somewhere, and then store the hash and the timestamp on the ledger. Someone accessing the image of the driving licence could then go to the ledger and obtain the hash which would tell them that the document has not been tampered with or altered and further obtain the timestamp to know when the licence was scanned.

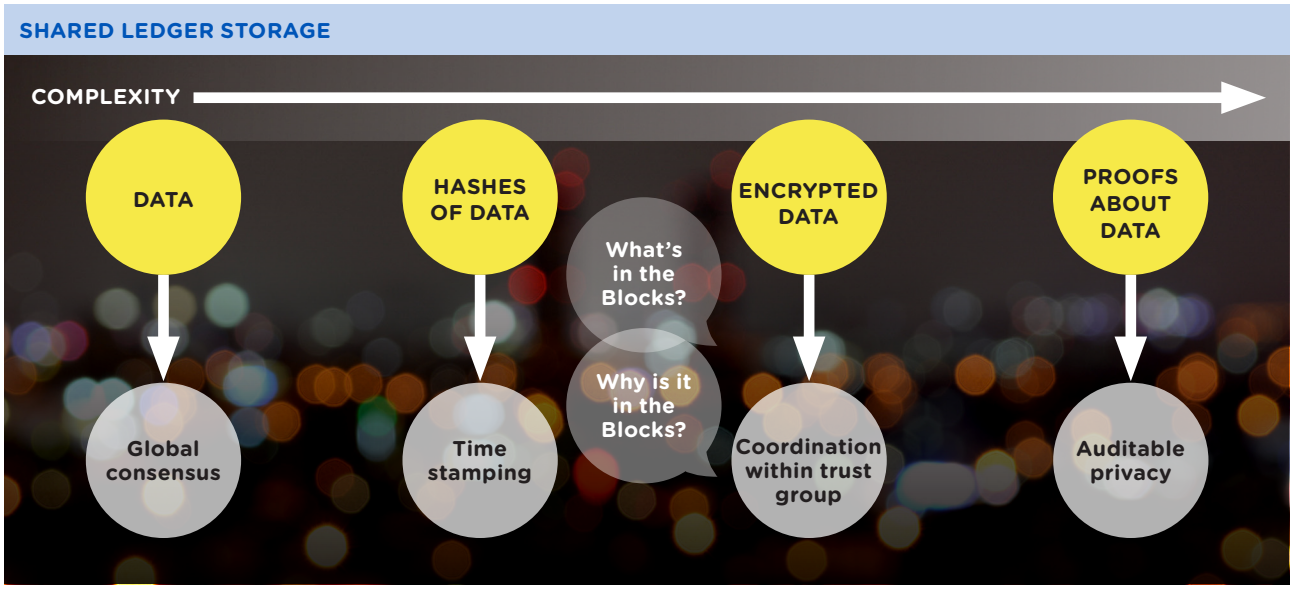
The second use of the ledger may be to store the data itself. So, to compare with the previous example, a system might take an image of a driving licence and store that image on the ledger. However, an obvious issue with this use of the ledger is that the data is available to all users of the ledger.

Given the restrictions of GDPR and other privacy concerns, this may not be the most appropriate way to handle digital IDs and their bindings to personal data, and so this leads us to a third possibility, which is to store identity information on the ledger but to store it in an encrypted form so that only authorised users can decode and use the data.

This could be a good solution in theory, given recent advances in encryption, although it could be argued that it merely shifts the problem of key management from the ledger to somewhere else without ameliorating the fundamental problem.

Ultimately, storing and managing personal data, even if it's encrypted, on a shared ledger is a **bad idea**.

FIGURE 12: WHAT KIND OF INFORMATION IS STORED ON THE LEDGER?



WHO WE ARE

Innovate Identity is an award-winning business with a highly-experienced team of consultants specialising in digital identity, security and privacy.

Our team has vertical industry expertise in financial services, payments, government, travel, telecoms and technology, as well as breadth of geographical knowledge across multiple global jurisdictions.

We are independent of any technology vendor and do not promote or sell any products. We are committed to providing our clients transparent, impartial advice.

We work with governments and multi-national corporations to small start-ups, and our main source of new business is through referral.

We are widely recognised as thought leaders in the field of identity and have been invited to speak at numerous global identity conferences, written many articles on identity for industry and technical publications, and acted as an expert witness in legal proceedings.

DESIGNED BY THE LANGTONS
WEARETHELANGTONS.COM

If you would like more information about Innovate Identity or you would like to get in touch with us, please visit our website or email us as follows:

www.innovateidentity.com

hello@innovateidentity.com

Innovate Identity Ltd
71-75 Shelton Street
Covent Garden
London
WC2H 9JQ