To Be, To Have, To Know

Smart Ledgers & Identity Authentication

February 2019

To Be, To Have, To Know
Smart Ledgers & Identity Authentication

February 2019

Author

Hugh Morris
Senior Research Partner, Z/Yen Group

Editors

Professor Michael Mainelli
Executive Chairman, Z/Yen Group

Kathleen Tyson
Chief Executive, Granularity Ltd

Foreword

The twenty-first century holds both exciting new horizons and practical challenges as we journey through the digital era of human development. In this context, few matters are more pressing than those related to identity authentication and management in general, and to digital identity in particular. To access digital government, the digital economy, social media or any other online services, we all have to face the challenge of proving who we are. Greater complexity creates barriers to access and trade.

As those who would hijack our identity for illicit purposes become more sophisticated, so legitimate providers and users of the digital world have to implement ever more sophisticated mechanisms for identity authentication and personal data management. Data security and privacy issues come evermore to the fore as scandals like the Facebook and Cambridge Analytica misuse of individuals' data demonstrates. We are caught on a dilemma of needing clever ways of proving our identity without revealing more information about us than necessary, for fear of its unauthorised use. Spurred on by the World Bank, governments of developing nations have been pursuing an agenda to implement national identity systems as a stimulus to economic development. Whilst this goal is laudable, it raises questions around state use of individuals' information together with questions as to how securely that data is held.

Smart Ledgers, distributed ledger technology, and blockchains are all technologies with the potential to help us realise the sort of world we want for identity regimes and systems. This report sets out to address some of the challenges, examining a myriad of issues relating to identity authentication and personal data management, from the history of identification verification techniques to current technologies, their uses and advantages and drawbacks. It poses questions for legislators, regulators and policy makers, as well as for commercial corporations and identity authentication and management system designers. The paper engages with competing factors and considerations in the hope of, ultimately, enabling us all to participate actively in the digital world - by verifying who we are, protecting our personal data and allowing us to securely articulate our consents and preferences.

Lord Holmes of Richmond
Author, Distributed Ledgers for Public Good
Vice-Chairman, All-Party Parliamentary Group on Blockchain

Contents

Preface

What is fascinating about Hugh Morris's report is the delineation of the looming battle between four very different views of identity and privacy, the EU, the USA, China, and India. There are other models of course, not least Estonia with its e-ID, or the UK with its defunct 2006 identity cards, and more recent GOV.UK Verify, but population size matters in a global economy. "To Be, To Know, To Have" sets out the three basic approaches to establishing identity, from antiquity to today.

Identity is a subject dear to our hearts, as the first thing about a Smart Ledger is who is trying to do what with whom. I recall studying with Robert O Nozick at Harvard the Theseus Ship puzzle in the text. A man goes round the world in a wooden boat stopping for a bit of maintenance at each port. By the time he returns to his home port every bit of the boat has been replaced. Is this the same boat? Further confusing matters, another man has been sailing behind him picking up the pieces at each port. He too returns to the home port and rebuilds the first boat. Which of these is the original boat, the first or the second?

We were out sailing on our Thames Sailing Barge Lady Daphne a few years ago (as you do) discussing philosophy (aka having drinks). We raised this old identity chestnut for fun (well, we weren't that inebriated) and our mate Denis Johnson solved it. He pointed out that, rather obviously, the first boat is the same and the original. The obvious reasoning - 'It still encloses the original space.' A diffuse 'boat' system surrounds 'boat' space.

Recently, in the National Archives, I came across the cataloguing problem for a book of patterns and cloth. Sure, we can catalogue the book, but its contents ranged from exquisite porcelain designs to samples of cloth, all seeking 'design' intellectual property protection. How do you catalogue the (literally) thousands of design sketches contained in a large volume? A diffuse book system surrounds 'design' space, but doesn't make the identity or cataloguing any easier.

Where Smart Ledgers provide some help, is that they offer the opportunity to reshape the markets for identity and other personal information, making it practically feasible to send data, or a proof relating to the properties of that data (for example an eligibility or compliance test result, credit score, mandate, token or consent) without divulging the actual data, to people or organization yet keep some control over the use, onward sending, and who accesses it over time, as we reported on in 2018, “Information Rules: Smart Ledger Architectures & Distributed Permissions”. Our 2014 www.idchainz.com project is one such prototype; there are many others.

Clearly, the obstacles are not technical. Smart Ledgers provide the means, but the will is often weak, or rational behaviours from incumbents delay progress. As this report notes, there are at least four (leaving Bitnation, fascinating as it is, to one side) boring approaches, private monopoly (extremely undesirable), public monopoly (only marginally less extremely undesirable), multiple government identity (healthier, but), competing private sector (healthy, but the public need to accept the possibility of ‘failure’). Of course, competing private sector solutions can be healthy, but the price for the resilience and trust is complexity, regulation and supervision.

There are no simple solutions, as Hugh makes clear. However, there are some clear ‘don’ts’, private or public monopoly, and some clear ‘explores’, establishing semi-competitive voluntary standards market approaches. Along the way, this report makes the case for a variety of policy considerations, such as liability capping (as in the US Commonwealth of Virginia), liability frameworks (as with some European banks’ IdenTrust, but brought up-to-date with Smart Ledgers), regulators (particularly in financial services) applying risk-based penalties to mis-applied identity, or (my favourite) why not have governments mandate the right of all citizens and corporates to a digital ID, combining personal data store and digital signature to be recognised by both state and private sector. Notaries will scream, but the rest of society will be more efficient, faster, and simpler.

Anyway, what a good read this report is. I commend it to anyone who cares about citizen rights, privacy, information ownership, global trade, technology, and finance (even fintech). But we have a long way to go to avoid Orwell’s 1984.

Professor Michael Mainelli
Executive Chairman, Z/Yen Group

Introduction

This report will highlight the increasing importance of identity stewardship for government and private sector digital engagement, and show how identity management and authentication solutions can exploit the emerging Smart Ledger Technologies. It will also explore the social, economic, and political challenges of standardising and rationalising digital identification methods nationally and globally by evaluating alternative models for managing digital identity and balancing the needs of nation states, businesses, policy makers, regulators, and individuals.

Identity management and authentication systems make good servants and poor masters. If you check into a luxury hotel where all the staff appear to know you, your likes, your previous stays at the hotel or other hotels in a chain, then you tend to be imbued with a sense of well-being and a feeling that the hotel organisation really does value your custom.

On the other hand, identity management can be a threat. Those controlling identity might be able to restrict travel, block bank transactions, and otherwise use identity validation as a tool of state authoritarianism. The darkly comic side of such authoritarianism is embodied in the character Doc Daneeka in Joseph Heller’s novel, Catch 22, who is supposedly on a flight where the pilot crashes the aircraft into a mountainside. Doc didn’t get onto the plane, but the US army has recorded him as being on the flight and so declares him dead, informs his wife accordingly, and eliminates him from their records. He then struggles to survive.

In the real world, thousands have found themselves blocked from opening bank accounts, making payments, or travelling by false positives thrown up by KYC/AML checks or travel black lists because of an unfortunate similarity of name to those individuals or entities on a sanctions list, with the veil of national security around the composition of these lists an impediment to proving innocence. Hundreds of thousands have been victims of identity fraud, often only learning of the crime when they apply for credit and find their credit rating has been compromised by fraudulent loans obtained in their names.

Identity is complicated, both in theory and in practise, making better identity management both a political issue and a technological challenge. Individual identity involves parental or birth associations (age, birthplace, and name), self-determination or achievements (diet preferences, career, and education), state assignment of defined characteristics (nationality, tax status, and benefit eligibility), relationships with others (spouse, partner, children); event driven changes (moving house, marriage, divorce, retirement), variable and elective factors (job, address, political affiliation, and income); geographic and temporal concerns (e.g., how long and where you have lived affects your eligibility to a free Scottish University Education); unalterable physical characteristics (fingerprints and iris scan), physical characteristics that change over time or may now be reassigned (DNA, gender, weight); self-association with groups (religion, business customer, loyalty scheme, or club membership), professional qualifications and licences (membership of the BMA or a DVLA licence) and external perceived similarities between individuals and other individuals (risk assessment and profiling). This is then combined with the transactional events that occur in our daily lives; our bills, our web searches, our phone calls. These allow analysis to suggest what is normal behaviour for a given person; that analysis is critical to identity security as individual patterns are incredibly hard to forge unless you literally live another person's life for them.

Identity is a civil rights issue. In many countries it is mandatory to obtain an official identification document issued by a state authority. In the UK it is considered an infringement of civil liberties to require any formal identification. Even in countries with mandatory official identification, the laws or courts may restrict whether or how businesses and others can use that identification in the private sector. In the European Union the General Data Protection Regulation (GDPR) attempts to assign control of data to individuals as an extension of civil rights. In all countries the legal system and regulation will impose greater or lesser obligations and assign liability for use and misuse of identity data. The credentials upon which such identities are built thus vary from country to country, and just like the humble passport in which some passports from some countries are more useful than others, then some identities from some providers will carry more trust and security than others, and relying parties will need to weigh differences in order to make commercial or state decisions.

Identity is closely guarded and raises security risks. Identity fraud has grown to become a systemic challenge as criminals use real identities or fabricate synthetic identities to steal money, obtain credit, or otherwise commit crimes. Not a week passes without some revelation about hacking of databases that puts hundreds of thousands or millions at risk. Because the theft of data and fraud often occur without immediate detection, and criminals and victims are often in distant countries, it is difficult to combat identity theft pro-actively except by improving systems security and individuals' security practices. The stakes are rising with regulatory changes such as the pension freedoms we now enjoy – with fraud victims averaging a loss of £91,000.[1] This highlights the need for robust identity systems to not just prove that a person physically exists and is a natural or legal person, but that the person asserting that identity is actually the individual who is legally entitled to do so. Family members often share PIN numbers for bank cards, , usernames, and passwords, despite the terms and conditions of use prohibiting sharing. Where the cost of loss to the individual is low, some compromises of security may be acceptable. Where the cost is potentially the home, the pension or a life's savings, the level of assurance must be much higher and ensure the physical person asserting an identity is that person.

Identity is complicated by differing standards for data collection and use. There are many global identity requirements and data format standards, which means no standard dominates. Names can be spelled variously, especially when translated into foreign languages and characters. William Shakespeare chose to use multiple variants of his own name, with publishers and others adding to the variants.[2] Addressing conventions vary widely from country to country – and the local need for addressing is often different from the needs of a postal system especially for international post (one typically writes the destination country and region in language of the originating country for the benefit of the outbound postal service, and the house, street and person name in the language of the destination country – for the benefit of the delivering postal service). In some communities, we find houses with a single front door with multiple dwellings behind it (HMOs or Houses of Multiple Occupation). The communities in those dwellings may be diverse, but often there may be one or more individuals sharing similar or identical names. Postal address is also linked to the ability to deliver post. If there is no postal point, there is no postal address. GPS co-ordinates are also weak, with a high-rise block of flats potentially offering hundreds of dwellings with front doors all at the same co-ordinates. The local authorities in the UK sought to collaborate in order to fix some of the addressing challenges through the National Land and Property Gazetteer[3] - but this service is unknown and alien to most people, and we invariably rely on GPS or Postal Address, which just isn't good enough.

Although fingerprints and retinal scans were once thought to be a solution for universal identification, even these methods have persistent error rates and

[1] http://www.bbc.co.uk/news/business-45170408

[2] http://en.wikipedia.org/wiki/Spelling_of_Shakespeare%27s_name

[3] http://www.geoplace.co.uk/

data security vulnerabilities. Know Your Customer (KYC) and Anti-Money Laundering/Counter-Terrorism Finance (AML/CTF) regulations have led to a global industry in solutions for filtering transactions, but there are still many issues and exceptions making this activity complicated and expensive. Vulnerabilities may also emerge over time, either affecting a class of reader, or the biometric itself. Also, those responsible for collecting and linking biometrics must have the trust of those who rely on them. Biometrics can be used to remove friction, but must typically be used in combination with knowledge, devices, two-factor authentication, or other security checks. The MIDAS Alliance has been working with various government departments, regulators, financial institutions and other experts to create a global BSI and ISO standard (the working title is PAS499) to facilitate this.[4]

Identity presents a civil rights challenge for balancing state power and corporate power against individual freedoms and protections. In China identity management is built into state monitoring of individuals for total control from birth to death, with scoring for social contributions and state interactions. In the United States, corporations have been leading the development of laws and regulations on identity data use and protection, concerned principally with profitability. In the European Union there is wide variation on government collection and use of data, but individuals have regained some control of private sector data through the General Data Protection Regulation (GDPR). There is even a Data Privacy Day on 28 January in the EU.

Identity data is a national security concern. Since 9/11 many countries have implemented sanctions regulations applying to travel and business transactions that imposed a substantial systems and operations burden on affected businesses, requiring persistent validation of individuals' status against lengthening sanctions lists. Many of the changes found in the Fifth Money Laundering Directive can trace their origins back to 9/11, such as the changes made to the maximum value that may be stored on a pre-paid cards and the channel of use (in store or online), before KYC must be performed.[5] Scandals such as the involvement of Facebook, Cambridge Analytica, and hostile states in data profiling and message targeting to influence the British Brexit Referendum and US presidential election in 2016 have raised identity protection as a matter of wider national security interests. Spyware preinstalled on mobile phones has also been found. Identifying actors and their motivations is, of course, never simple in this shadowy world. For example, WIRED Magazine recently covered

[4] http://standardsdevelopment.bsigroup.com/projects/2016-01438

[5] http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935

the discovery by security firm Kryptowire which claimed that millions of Android devices would secretly send full text messages, contact lists, call history, location data, and other sensitive information to servers overseas.[6]

Scale and critical mass are also major challenges for harmonising identity management, within states and globally. It isn't in the interests of any one shop to build a six-lane divided highway outside the storefront, yet the whole economy benefits from a nationwide highway network with common rules of the road that makes travel, transport, and logistics easy, fast, efficient, predictable, and safe. Similarly, it is beyond the scale of any individual government department or business to resolve the challenges of digital identity management, but the digital world would benefit from standardised methods of identity management that make digital interactions easy, fast, efficient, predictable and safe. One of the biggest challenges faced by the Government's Verify programme was that most citizens don't interact with government more than once a year, typically to file a return. During that period, their digital ID credentials are forgotten, along with how to use them. A sustainable solution must fit into our everyday lives, which means either working with the actors we connect with on a daily basis, who already have a need to reliable identity. In the UK, over 70% of the population currently bank using a mobile phone, and banks have legal and commercial obligations to maintain identity credentials to a standard above that which government does, plus they are able to apply commercial liability to those decisions – which is far more attractive to relying parties. The banks also face a wave of new compliance work to support the Wire Transfer Regulations, Secure Customer Authentication for Open Banking and the Payments Service Directive 2, and the Fifth Money Laundering Directive. It is self evident that no other sector has the obligations and ability to deliver high quality verified identity services upon which we can achieve the ubiquity and reuse across state and private sector use cases. The challenge is to find a trust model and economic model that does not create new liabilities for banks, improves their own product distribution channels, does not open them to unfair competition from start-ups who are not subject to the same scrutiny and overheads, meets the needs of the consumer, and allows us to grow the pie for all. The banks in The Netherlands seem to have found a way, but that builds upon the culture and values of the Dutch and existing state and private sector services, infrastructure, culture and laws[7]. The UK is different, and thus to achieve the same, a different pathway may be required.

[6] http://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box/

[7] http://www.thepaypers.com/interviews/exclusive-interview-with-rabobank-how-do-the-dutch-identify-themselves-with-idin-of-course/773164-38

Despite these considerable challenges, better identity stewardship is urgent. The United Nations Sustainable Development Goals adopted by all members in 2015 as an agenda for 2030 include SDG 16: “Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels”[8] SDG 16.9 clarifies a commitment on identity: “By 2030, provide legal identity for all, including birth registration.”[9] As a universal and shared objective, it is timely to consider universal and shared standards and methods to provide citizens not just with a legal identity but with a digital identity that enables them to interact with all governments and businesses securely and reliably while respecting privacy and data protection interests. Shinzo Abe has made privacy and data protection a primary agenda item for the G-20 summit in Osaka in June 2019.

Best practice methods for establishing **individual** identity have developed considerably in recent years. Typically these include:

- Something you **are** (e.g., fingerprint, retina scan),
- Something you **have** (e.g., mobile device, key or token),
- Something you **know** (e.g., password, response to a pre-set question).

The difficulty is that as more interactions move online, more individuals become frustrated by the diversity of systems involved and methods in use. As more identity fraud and data abuse revelations are revealed in the news, more people become wary of the risks of data theft and insecure transactions. Despite rising costs of fraud and customer services, governments and businesses are reluctant to implement new controls due to costs, legacy system complexity, project risks, and adverse impact on the customer experience. A digital identity can prove who you are, can provide and revoke consents to share, and can exchange tokens of encrypted data without compromising the data store. At its simplest level, buying alcohol requires me to prove I am over 18. My date of birth never needs to be shared. Imagine walking into a bar, as you approach the till, your mobile phone’s unique ID is detected and a tokenised interaction with the age verification service begins. The individual who owns the phone has authorised all pubs and bars to display his verified photo on the POS and a tick next to the photo indicates he is over 18. The bar staff visually check the face and the photo

[8] http://sustainabledevelopment.un.org/sdg16

[9] *ibid*

match, with CCTV available for retrospective audits, and a frictionless experience is achieved.

Establishing identity for **entities** (e.g. businesses, sports teams, charities, government departments etc.) is even more complex. The tests that can be applied for individuals do not function well for establishing the identity or capacity of a legal entity. Entities are created by legal recognition of an organisation as separate from its founders or constituent individuals, and the standards for units of government, incorporation, charitable status, partnership, and membership organisations vary from state to state.

There are no 'hard and fast' rules to prove conclusively what constitutes an entity in all circumstances or who has capacity to make decisions for the entity and bind it to obligations over time. Identity for businesses has developed to be context dependent. Tellingly, 'corporate identity' is only concerned with branding, not functional validation of capacity to act.

Historically, proving corporate identity typically involved issuing a letter on corporate letterhead signed by a director or company secretary, sometimes authenticated by a notary or endorsed with the imprint of a company seal. As the world integrated technology and automated processing into corporate interactions, the solutions adopted for entity identification became specific to individual businesses and closed networks, with different data standards defined for each industry. Closed networks limit competition and innovation and these legacy systems now present a challenge for integration and modernisation. Also, the issuing bodies who record incorporation must have water tight processes for linking legal persons to genuine natural persons which is one of the challenges currently faced by Companies House as noted by the ICSA: The Governance Institute.[10] The needs of each identity system will focus on the needs of its community, yet for society to benefit, interoperability between the multiple systems that will emerge is essential. Distributed ledger technology is an ideal candidate solution to this challenge allowing changes to propagate swiftly as and when required.

Legal Entity identity management is particularly problematic over time. Entities can merge, be taken over, divest, become insolvent, and re-invent themselves in ways which escalate the complexity of establishing capacity or authority. Directors, executives, partners, or other empowered individuals change jobs,

[10] http://www.icsa.org.uk/knowledge/governance-and-compliance/analysis/companies-house-online-registration-kevin-brewer

retire, or die, and records for many relevant individuals are difficult to maintain completely and accurately for verification of authority.

Even after a corporate entity has been sold, the law may continue to obligate former directors or shareholders, confusing assignment of identity. The bankruptcy of the BHS group in the UK in April 2016 gave rise to claims against the owners of Arcadia Group following discovery of a massive deficit in pension provision for BHS workers. In 2017, Sir Philip Green paid £363 million into the BHS pension scheme in settlement of the claim.. Despite the 2015 sale, former owners were still regarded as legally obligated in 2017. Financial institutions acquiring others may find themselves liable for the misdeeds of the previous owners. This is nothing new though. Back in 2001, it was reported how GAN Life, a subsidiary of the French Mutual Groupama (a firm ostensibly owned by the members like a UK building society) , had acquired a UK firm known as General Portfolio. Prior to the acquisition, the firm had engaged in mis-selling, resulting in the net value of Groupama being reduced in order to pay tens of millions of pounds in compensation, and ultimately, being a mutual, these costs were passed on to the French members who became the ultimate victims.[11]

Plutarch was amongst the first to articulate the classic puzzle of the challenges in determining the nature of persistent identity of with the conundrum of Theseus's ship:

> The ship wherein Theseus the youth of Athens returned from Crete had thirty oars, and was preserved by the Athenians down even to the time of Demetrius Phalereus for they took away the old planks as they decayed, putting in new and stronger timber in their places, insomuch that this ship became a standing example among the philosophers, for the logical question of things that grow; one side holding that the ship remained the same, and the other contending that it was not the same.[12]

Persistence of identity is also the subject of a one-line story of an axe: "I have my grandfather's axe, my father put a new head on it and I replaced the handle."

In practice commercial due diligence currently requires validation of an entity against public data such as Companies House records or the Register of Charities in the UK, and maintenance of documentation evidencing authority such as a

[11] http://www.theguardian.com/business/2001/nov/29/10

[12] Plutarch*Theseus* (23.1) .

register of authorised signatories. Maintaining the accuracy of static data for entities over time is a continuing challenge and often the cause of reconciliation errors and transaction delays.

Establishing persistent identity can have material commercial implications. As of writing there is a debate within Formula 1 as to whether the new Racing Point UK team, which acquired the assets of the Force India team, is the same as the team whose assets it acquired. At stake is the accelerated payout of 'Column 1' prize money (for which teams normally wait two years) due to be paid to Force India and which the Racing Point UK team needs to enable them to continue to race their cars. Payment of this money requires the agreement of all the other Formula 1 teams, one of which is questioning whether Racing Point UK has acquired the same identity as Force India.

This report is focused on individual and entity identity management and authentication for digital interactions online. It is worth noting, however, that identity management can encompass many other objects and applications in the real world. Some other use cases for improving identity profiling and management include:

- Food chain logistics (sourcing and processing of food from field to shop);
- Animals (breeding, tracing & animal products in the food chain);
- Land and property (geolocation of property, development rights, investment claim, mortgage interests, etc.);
- Stock control and inventory management;
- Supply chains and logistics.

During the 1960s, the English Electric factory at Brough, East Yorkshire, manufactured the Lightning fighter aircraft for the UK Royal Air Force (RAF). In 1964, there was a panic. Sitting on the apron at the factory was Lightning number '66'. Records showed that planes up to and including Lightning '64' had been delivered to the RAF. But there was no sign of Lightning '65'. After a thorough search of the facility, which revealed no evidence of the missing aircraft, a six-man team was formed to trace Lightning '65' through the manufacturing process to see what had gone wrong. This team had been diligently at work for some six months when someone happened to take a closer look at Lightning '66' still sitting on the airfield to discover that it was, in reality, Lightning '65' with the wrong number painted on the tail fin. Misidentifications and supply chain disruptions can be costly and embarrassing in every industry. With global supply chains, just-in-time production, ever more stringent food safety standards it is critical that we develop identity management solutions that can scale and adapt to meet the complexity of modern economies.

The ICAEW recently attempted to price the costs of bad data upon firms. They highlighted the fact that 1-10-100 rule fairly accurately quantifies this when it comes to the output cost of bad data. Estimates suggest that if the cost to fix a data error at the time of entry is £1, the cost to fix it an hour after it's been entered escalates to £10. Fixing it months later costs £100. Something the tale of Lightning 65 highlights.[13] This attitude to data may also explain some of the productivity gap in the UK compared with countries who are naturally better at record keeping and process following. The same report highlights a UK financial services company that achieved 25% growth in overall revenues having fully cleaned its data: proving that with the right level of real-time visibility any garbage coming in can turn to gold on the way out. Identity Services and communication via Distributed Ledgers promises to ensure that at least if something is wrong, it is consistently wrong from start to end, and fixing it is much simpler.

Identity Management and Authentication

There are at least five major dimensions of identity management and authentication that can be considered, namely:

(1) **Commercial** (e.g. how to meet know-your-client [KYC] requirements in financial services, how to engage with the millions of individuals currently excluded from commercial activities?);

(2) **Political** (e.g. how does a government know who to tax and for how much, how to identify refugees in an era of persistent, widespread migrations?)

(3) **Sociological** (e.g. how does an individual demonstrate identity for the purpose of participating in democracy through voting, how to use identity management as a tool for societal progress?);

(4) **Psychological** (e.g. the challenges posed by conditions such as schizophrenia, memory loss);

(5) **Philosophical** (e.g. what makes it true that a person, or object, at one time is the same thing as a person, or object, at another time?).

In addition, this problem is not one to be considered from the perspective of ivory tower. There are identity assets out there in operation today, and infrastructure that can be repurposed. Any national scale green field project seems to come in years behind schedule, with budget overspends of several

[13] http://economia.icaew.com/opinion/july-2013/the-unseen-cost-of-bad-data

hundred percent. The costs of onboarding the UK from scratch and educating everyone could be potentially eye watering, unless we can build identity into the products and services we already use today, so adoption becomes like osmosis. This may be using secure forms of identity from the big tech firms, drawing on the assets of the financial services and fin tech communities, or working with existing identity providers such as the Credit Reference Agencies. If your bank app suddenly said "Hey, you have a digital identity – activate with a selfie and your passport", most people would not find it unusual as they know and trust the banks and their security. One challenge faced by HM Government's Verify solution was that the trust providers were either not known to the public, or were resented.

Different states, businesses and individuals have made many different choices about requiring, providing, maintaining, and using individual and entity identity data for many different purposes. For this report we will look at models which address the commercial, political and sociological dimensions of identity stewardship, recognising that standards and methods are still evolving, and nation states are actively considering the need for changes in laws, regulations, and data security methods.

Options for Identity Management and Authentication Implementation

In the practical world, identity management and authentication systems have to be provided by an entity – either some form of state-run system or a private sector facility. In each case the entity providing identity stewardship is subject to laws and regulations of one or more jurisdictions. Although innovators such as Bitnation are promoting pan-global identities this isn't deemed practical in the near term.[14]

Four models for identity management are shown in Figure 1 below for comparison, contrasting state vs commercial ownership, single vs multiple providers:

[14] http://www.tse.bitnation.co

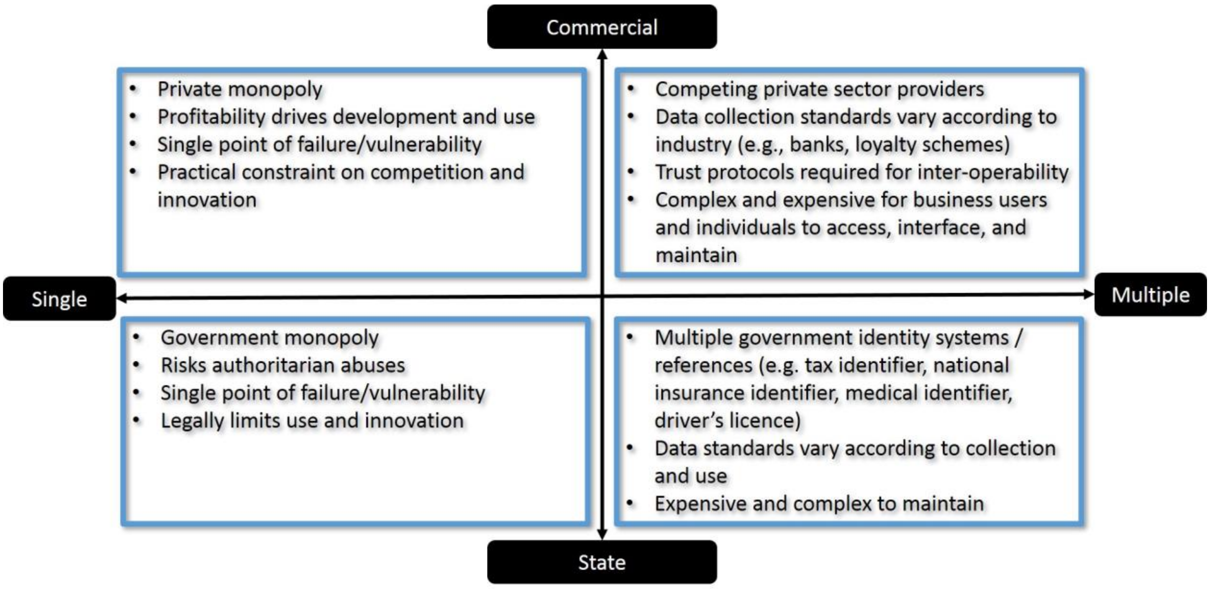

Commercial
Private monopoly
Profitability drives development and use
Single point of failure/vulnerability
Practical constraint on competition and innovation
Competing private sector providers
Data collection standards vary according to industry (e.g., banks, loyalty schemes)
Trust protocols required for inter-operability
Complex and expensive for business users and individuals to access, interface, and maintain
Single
Multiple
Government monopoly
Risks authoritarian abuses
Single point of failure/vulnerability
Legally limits use and innovation
Multiple government identity systems / references (e.g. tax identifier, national insurance identifier, medical identifier, driver's licence)
Data standards vary according to collection and use
Expensive and complex to maintain
State

Figure 1. Alternatives for implementing identity management and authentication systems

These options, state vs. commercial and single vs. multiple, model real world implementations of identity management and authentication systems currently used or proposed. None of them is perfect or operates seamlessly with other systems.

Commercial Monopoly

The commercial monopoly option is highly undesirable, with clear scope for abuse of monopoly position. Any commercial monopoly managing identities will seek to maximise the revenues of its system rather than serve the broader public interest objectives of protecting users from abuse or crime and ensuring respect for civil liberties. The UK considered putting an identity system out to private provision, through a public procurement tender, but neither the UK nor any other government has yet thought it appropriate to proceed.

Whilst it is not a perfect analogy (because Facebook is not a 'monopoly' as such), the issues uncovered at Facebook in 2018, when it permitted Cambridge Analytica to harvest personal data of thousands of individuals through the "This is Your Digital Life" app, and the subsequent, undisclosed use of that data for political influence campaigns, starkly demonstrate the challenges that a private monopoly could pose. Profit would drive decision-making. As a result, the commercial monopoly implementation option is not considered a realistic option for identity management implementation.

Many industries have developed shared-services networks and infrastructure to meet the challenges of digitalisation while maintaining some degree of shared governance and oversight. These solutions have been essential to globalisation of commerce in banking, telecoms, and other industries, but also provide some cautionary lessons. Shared-services systems can be slow to adapt, hampering innovation, and governance by incumbents can protect those incumbents from new entrants or competition.

The global bank network provider SWIFT delayed providing an internet protocol network with XML messaging into this century to protect dominant banks from competition and preserve higher cost per-message revenue streams for transaction processing. Similar issues for the UK payments services provider have led to imposition of regulation to promote openness to new market entrants, both banks and non-banks. Shared services infrastructure also presents a single point of failure or vulnerability, so that the undisclosed monitoring of the SWIFT network by US national security authorities and incidents of unauthorised hacking have both impaired global confidence in the network's integrity.

Where shared innovations occur, some actors may seek to hold on to them to get a commercial advantage before collaboration. This is standard in many sectors including the provision of ATMs. Originally, banks would only allow their own customers to use them. The location of the ATM was a source of advantage – one that could persuade customers to switch banks. The building societies who lacked the branch networks of the banks realised that co-operation made sense – and formed the LINK network, and gained a huge advantage. The commercial model that underpins LINK where a customer's financial institution is able to instruct another to release money, potentially via a non-bank 3rd party, and in which all parties receive fair recompense based on value added, is a model of inspiration for the commercial underpinnings of a digital identity ecosystem. It also explains perhaps why some banks (and big tech firms) are less willing than others to collaborate at this moment in time, and it is incumbent on government to provide the regulatory and commercial incentives to do so.

State Monopoly

A number of governments have sought to implement monopoly identity card systems for their citizens (see text boxes below on Aadhar in India, China's citizen identity card, Estonia's ID-kaart, and the failed attempt to introduce identity cards in the UK, as examples). The earliest systematic introduction of a modern national identity scheme was Sweden's creation of the Personnummer in 1947, which today drives government registration, health service identification, individual identification for schools and universities, and is also used for identification by banks. In Belgium, it is illegal to stray more than 200m from your home address without your ID card, which includes a digital certificate that is recognised across Europe for digitally signing documents and contracts remotely under the eIDAS regulations.

Concerns surrounding such monopolistic state systems were exceptionally well summed up by the London School of Economics (LSE) when they published their critical report into the UK's proposed identity card scheme.[15]

Among other concerns, the LSE highlighted the following risks:

- Using biometric identity data is not entirely reliable. Iris scans are, at best, only around 96.5% reliable (which means that nearly 4 people in 100 could be mis-identified and therefore, say, prevented from boarding a flight) and fingerprint recognition methods can produce a false positive on a partial match. There are also trades, such as general heavy manual labour or specific trades, like glass blowing, which wear off fingerprints, so individuals literally do not possess them as a means of identification any more. Additionally, all biometric methods that are widely used have been successfully 'spoofed' (for instance, iris recognition systems can typically be fooled by a high quality photograph of a subject's face). At a national scale, even the 1 in a million false positive rates claimed for finger veins would lead to chaos if not supported by a reliable unambiguous second factor. This is due to a mathematical problem called the Birthday Paradox[16] What this means is practical terms is that in a class of 30 odd children, two of them almost always share a birthday. The maths is interesting, and well documented on the web. What it results in when applied to national systems is that given the population UK of 70m people, even a false positive rates of 1 in a million will cause massive numbers of problems on a regularly used system for large numbers of people. Bank cards have a PIN number, typically 4 digits, and typically you get 3 chances to guess it before the card locks. The probability of guessing it at random is thus 1 in 3333. The reason this works is that all bank cards are unique, and the PIN is confirming you own it, not the source of the identity in the

[15] http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf

[16] http://en.wikipedia.org/wiki/Birthday_problem

first place. Biometrics are best used either with pre-registration, or with unique IDs, or in some use cases, in combination with other biometrics.

- A single system implies a single point of failure and vulnerability. All this identity data stored in one single repository creates a single point of failure which has to be managed and secured rigorously. Typically, the database will be large, as substantial quantities of data need to be held to capture all citizens. The centralised storage of so much identity information creates an almost-irresistible target for hackers. Most national identity databases have been hacked already. As an example, the data for some 50 million Turkish citizens was hacked and put online in 2016.[17] It would be a major catastrophe if both the primary source and back-ups of one of these databases was simultaneously destroyed or rendered unusable. A federated or truly distributed system seeks to mitigate this challenge by having each identity service provider develop their own security protocols. If one provider fails, the others should not be vulnerable to the same flaw. Of course, we are dealing with systemic behaviours, and where any component becomes systemically prevalent, it has the ability to become a critical weakness. Both Apple[18] and Android[19] have had recent vulnerabilities which allowed hackers to attack other systems that had previously been secured and access the information to cause real damage. We must ensure that identity services are fault tolerant. They need to be resistant to systemic failure and that includes failures in institutions, devices, protocols, networks, algorithms & maths, hostile acts by foreign powers, disruptive technologies, obsolescent technologies, weak standards and so on. We should expect such failure as inevitable and ensure the underlying ecosystem, is capable of detection, recovery, remediation, adaptation and enhancement in response, without throwing the proverbial baby out with the bathwater – at great expense and on a national scale.

- Authoritarian misuse of identity data raises civil liberties concerns. Increasingly, personal identity information that is provided to governments for the purposes of issuing national identity cards is being

[17] http://www.aljazeera.com/news/2016/04/turkey-investigate-massive-leak-personal-data-160406082317417.html

[18] http://www.theguardian.com/technology/2019/jan/29/facetime-security-bug-apple-privacy-iphone

[19] http://www.zdnet.com/pictures/the-most-dangerous-vulnerabilities-security-flaws-found-in-google-android-apple-ios-over-2018/

used more widely – sometimes to the benefit of citizens, but not always. For instance, when Bangladesh started to issue identity cards in 2016, banking, passport details, driving licences, trade licences, tax payments, and share trading are among the 22 services that can be accessed through the cards, with more to follow. The cards will also be associated with an individual's mobile phone SIM card, providing advanced security and authentication features.[20] However, it is also clearly possible to use the identity data for less benign purposes, profiling individuals' movements and enabling surveillance in ways which may be considered incompatible with civil liberties. The ability of the state to use or to misuse its citizens' identity information is an inherent risk.

- IT security and integrity requirements for a state citizen identity database are stringent, involving advanced security techniques and, typically, some form of encryption. At the end of the day, hackers will always try to breach such security and, whilst they only have to succeed once, defences against them have to be maintained to anticipate an ever-increasingly sophisticated, organised range of attacks. In their attempts to gain unauthorised access, hackers are assisted by Moore's law (computing power in a microchip doubles about every two years[21]) and, whilst the Moore's Law trend may show some more recent signs of slowing down, passwords of 10 digits that include only alphanumeric characters, can now be cracked by the application of raw computing power in two hours[22].

[20] http://advox.globalvoices.org/2016/10/07/bangladesh-introduces-smart-national-identity-cards/

[21] http://en.wikipedia.org/wiki/Moore%27s_law

[22] http://keithieopia.com/post/2017-12-13-passwd-crack-time/

Case Study: India

The Unique Identification Authority of India (UIDAI) claims that "Aadhaar is the world's largest biometric ID program", An Aadhaar ID consists of a unique, random 12-digit number issued by UIDAI on registration, based on production of documentary identification and proof of address. As of 2017, 1.14 billion Aaadhaar numbers had been issued to Indian citizens.

The original purpose of Aadhaar (derived from the Sanskrit word for 'foundation') is somewhat disputed. It is claimed that its objectives were to enable unique identification of benefits claimants and to improve financial inclusion amongst India's poorest citizens but, further back in history, recommendations were also made that an identity card should be mandatorily issued to residents of border villages following the Kargil war with Pakistan in 1999 (5).

Aadhaar captures three types of biometric data: all ten fingerprints, a photograph of the subject, and an iris scan. Despite the Indian government's intention to make the ID mandatory, the Indian Supreme Court decreed enforcement of compulsory IDs would infringe constitutional privacy rights. A further Supreme Court ruling upheld the Indian government requirement of an Aadhaar number for receiving welfare benefits and filing income tax returns but has banned schools and private sector companies (bank, mobile operators, etc.) from requiring the ID for their services.

The UIDAI, which manages Aadhaar, was established by executive order in January 2009. Aadhaar was formally launched in April 2010 and enrolment commenced. After a number of both political and constitutional challenges, legislation covering Aadhaar was finally passed in 2016 through the 'Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Bill 2016'.

The penetration of Aadhaar is expanding both within and beyond the original objectives of managing state benefits and enhancing financial inclusion. Over 74% of beneficiary names for social protection programmes are now linked to Aadhaar numbers. As of 2017, 33% of social protection payments to beneficiaries are being dispersed through the Aadhaar Payment Bridge System (ABPS). Aadhaar is further being used for e-KYC purposes, as well as for payments / micro-payments through the Unified Payments Interface (UPI) and the Aadhaar Enabled Payments System (AEPS).

However, the penetration of these payment mechanisms is limited currently; as of 2017, they only accounted for 6.67% of transactions and 0.06% of value of payments in India. There are also pilots being conducted in linking Aadhaar to healthcare access, as well as virtualisation of physical documents through a 'DigiLocker' application, and an 'e-Sign' application to allow digital signature of documents through use of the Aadhaar number.

There are some serious integrity and security concerns relating to Aadhaar. UIDAI has set a target of a 0.5% error rate for its data accuracy. Whilst this is a small percentage, when the base number is 1.2 billion, there are likely to be over 600,000 Aadhaar records in error. There are also the classic risks of a single point of failure from having one centrally held government database of Aadhaar numbers, with its links to other government-held records of identity.

Furthermore, there have been some extensive Aadhaar data security breaches, the latest of which was reported in January 2018, claiming that details of over 135 million Indian citizens was now in the hands of hackers. It seems that more work remains to be done to manage the vulnerability of a single, central database holding key personal details of most Indian citizens.

The drive towards implementing state monopoly provision of identity management and authentication systems around the world has recently been boosted by the United Nations' Sustainable Development Goals SDG 16.9 which states its aim is to "By 2030, provide legal identity for all, including birth registration".[23] Whilst SDG 16.9 does **not** explicitly require identity registration through state monopoly , institutions like the World Bank have proceeded assuming that this is the most rapid (whether or not optimum) means of delivery and have promoted development of state systems accordingly. As the World Bank provides investment for national identity card systems and regularly reports on progress against these goals, there is a risk that state monopoly identity systems become a *de facto* default model. By way of example, the World Bank has recently been lauding endeavours in Peru to implement a national identity card scheme in their October 2018 identity progress bulletin, despite wide concerns about the authoritarian nature of the government.[24]

Once state monopoly identity management and authentication systems are established, another issue arises: how does the state use the resulting information that is held about on their citizens? Sadly, the behaviour of a number of governments around the world indicates that this information becomes a tool for state control of citizens (e.g. in China), although there are more enlightened administrations (e.g. Estonia) pursuing a more benign agenda. The Economist summarised the issue in December 2018:

> The fact that this [identity] service depends on the state raises problems. Identity, like tokens of monetary value, can be taken away by the state that issues it. A hundred years before India's government declared, in 2016, that all 500- and 1000-rupee notes would cease to be legal tender, the Italian authorities invalidated all passports belonging to military-age men with immediate effect, causing confusion on a similar scale.[25]

A central repository of identity information on citizens will always present scope for abuse. Wherever such state monopoly identity authentication and management systems have been implemented, for example, they are always available to, and accessed by, that country's intelligence services, with little public knowledge and often without even government oversight or accountability.

Just as an individual has the right to remain silent to prevent self-incrimination, the government should consider whether similar principles should apply to a digital self[26]. This will of course create an outcry from some, especially in the

[23] *ibid*

[24] http://blogs.worldbank.org/category/tags/national-identity

[25] http://www.economist.com/christmas-specials/2018/12/18/establishing-identity-is-a-vital-risky-and-changing-business?frsc=dg%7Ce

[26] http://en.wikipedia.org/wiki/Right_to_silence

cases which are outliers and test the law. However, the state has already established that it may act differently if an individual chooses later to rely on evidence that could have been provided during questioning. For most people, we would choose to share data when it is a pre-requisite for a benefit we want. An individual wanting to claim child benefit needs to prove their identity and that of the child along with relevant income. This can be done, and the cryptographic proof of the evidence behind this shared from individual to state without any data ever leaving an individual's digital identity. As such, with distributed technologies, it may be possible for a wise state, to protect its future self from over-reaching what society needs or desires.

Case Study: China

Prior to 1984, citizens in China were not required to possess an identity card. In 1984, the State Council of the People's Republic of China published the 'Identity Card Provisional Bill', followed up in 1985 by the 'Identity Card Bill of the People's Republic of China' enacted by the Standing Committee of the 12th National People's Congress. From then on, carrying identity cards was mandatory for anyone aged 16 and over. It is estimated that nearly 1.2 billion Resident Identity Cards (RICs) are carried by a population of 1.3 billion people. The RICs are issued and managed by the Public Security Bureau.

The RIC is based on an 18 digit Citizen Identification Number which embeds:

- an address code
- date of birth code
- an 'order number' to distinguish between people who have the same address and date of birth codes (men are issued with odd numbers, women with even numbers)
- a check digit to confirm the validity of the preceding values.

The RIC also includes full name, gender, ethnicity, date of birth (Gregorian calendar-based, in Chinese characters and western format), period of validity (which is not included in the digital information stored on the RIC's chip, so can only be determined by manual inspection), address and a photograph. RICs are registered on a national identity database which also records work history, educational background, religion, police record, medical insurance status, landlord's phone number, and personal reproductive history. The RIC is used as proof of identity for obtaining residence permits and driving licences, opening bank accounts, checking into hotels, purchasing high-speed railway tickets, and boarding domestic flights.

Early RICs were not digital and, when they became digital, were not encrypted, so that the data could be lifted by card readers operating in proximity to the card. This led to RICs being relatively easy to forge and counterfeit although the scale of the problem Is difficult to quantify. The current generation of RICs contains a chip with the information digitally embedded and encrypted, which is harder to forge or counterfeit, but can still be vulnerable to persistent attempts to replicate. There is a further issue in that lost or stolen RICs cannot be wholly deactivated because their unique number is the same as the Citizen Identification Number which must, of course, remain valid for the lifetime of an individual.

Currently, the Chinese government is working with TenCent to create a fully digital RIC, which will be based on their WeChat (known as Weixin in mainland China) app. This will create a wholly digital version of the RIC which can then be accessed from smartphones. The Chinese government aims to be the global leader in the virtualisation of identity authentication.

The World Bank is promoting state development of identity systems through a specific department, ID4D (IDentity for Development):

> We believe that every person has the right to participate fully in their society and economy. Without proof of identity, people may be denied access to rights and services—they may be unable to open a bank account, attend school, collect benefits such as social security, seek legal protection, or otherwise engage in modern society. No one should face the indignity of exclusion, nor be denied the opportunity to realize their full potential, exercise their rights, or to share in progress. No one should be left behind.[27]

Other organisations, such as Access Now, have grave concerns about this trend toward state control of identity, often implemented to be mandatory and constrain the use of alternatives:

> As an organisation committed to defending and extending the digital rights of users at risk, Access Now has deep concerns about any initiative to legally mandate a centralised national digital identity programme. These programmes pose significant risks for human rights. Specifically, they threaten to undermine the right to privacy and chill freedom of movement, the freedom of expression, and other protected rights. Further, since they typically entail the creation of centralised troves of sensitive personal data, susceptible to breach by malicious actors or abuse by public authorities, they also carry risks for cybersecurity and information disclosure. Such centralised programmes have the potential to turn a digital ID into a pervasive means of identification, tracking, or control, especially when such identities are biometrically linked and made mandatory.[28]

State monopolies also present difficult international coordination challenges. National systems are idiosyncratic to national priorities and legacy infrastructure and do not adapt readily for interoperability. Refugees provide a particularly acute problem. Globally, the number of refugees and displaced persons increases every year and is now in the tens of millions annually. Under the 1951 UN Convention covering the Status of Refugees, it is ultimately the responsibility of the state to which refugees flee to establish their identity.

[27] http://id4d.worldbank.org/

[28] http://www.accessnow.org/national-digital-identity-programmes-whats-next/

Given the circumstances under which refugees leave their homes, they are relatively unlikely to possess proof of identity (and, indeed some refugees deliberately abandon or destroy identity documents, for a variety of reasons). Identity documents can be lost, destroyed or stolen during a refugee's flight. It is unreasonable to expect refugees themselves to seek identity documentation from the governments they flee at risk of persecution. These governments may be unwilling to assist them even if asked, or worse, may see an opportunity for retribution. The Adnan Khashoggi murder signalled the risks of seeking identity data from an authoritarian regime. Mr Khashoggi was required to prove his marriageable status prior to re-marrying, and so sought validation of his earlier divorce from the Saudi authorities in Istanbul; when he returned he was murdered at the consulate. Problems with identity documentation can also apply to individuals in conflict zones who do not migrate. For example, it has become nearly impossible for individuals in Syria to replace or apply for new identity documents since the civil war commenced.

The United Nations High Commissioner for Refugees (UNHCR) is co-ordinating a number of initiatives around the globe, including with The World Bank, to find solutions to the issue of refugee identity authentication and management. There are a number of alternative models being adopted, e.g. in Kenya, where a national ID card system exists, the Refugee Affairs Secretariat issues a separate refugee ID card (called an 'alien' card) which enables the holder to access services within the country.

Generally speaking, in high income countries, the state will manage the registration of refugees, typically through a national ID card system. In middle income and poorer countries, voluntary agencies play an increasing role in supporting refugee registration and may issue their own identity documents. As yet, there is no easy, or internationally consistent, answer to the thorny issue of refugee identity management and authentication.

Commercial Multiplicity

Commercial multiplicity of provision is the default situation in many geographies where there are multiple identity authenticators, frequently acting as service providers in financial services, industry, gaming or social media. These organisations need to ensure that they can verify the identity of new and existing clients, purely for their own commercial purposes – but the standards for this must also comply with the regulations of the state. The obligations placed upon such entities by the state have grown over time, not in the interest of the institution, but in the interest of the state, which is hopefully in the interest of wider society. Such rules prevent tax evasion, money laundering, organised crime and stop terrorists getting access to funds. These are generally accepted as a social good.

Typically, each commercial entity which needs to establish client or customer identity (or is required by local law or regulations so to do) has its own system for establishing that identity. Multiple provision of these systems is hugely wasteful and distorts markets by discouraging competition, new entrants, and rationalisation of redundant processes. For example, every bank, solicitor and financial advisor in the UK must independently verify customer identity by requiring production of passport or driving license, and each must independently store the record of the document to meet KYC and AML/CTF compliance. That creates a large number of records of the same document with identity-critical data, any of which may be compromised by hackers who gain access to a system. When identity theft is finally noticed by a victim, it may be impossible for law enforcement authorities to determine which system was compromised. It's not just banks though. Criminals have identified other channels through which to launder money which brings other sectors into the scope of KYC regulations.[29]

Because commercial multiplicity makes identity fraud very difficult to prevent, detect, or punish, very often the public policy response is to assign legal liability. Banks and credit card companies increasingly act as insurers against fraud, bearing legal liability if their customers become victims. Another policy response is education, teaching the public to be aware of the risk of fraud and to take precautionary measures against data sharing that could put them at risk. Cifa, the body responsible for fraud prevention in the UK, has recently introduced lesson plans for schools to teach the young about identity fraud, as the young are increasingly at risk.[30] This liability question also provides a strong clue as to which actors must be part of the solution. The state will never wish to indemnify others against the fraudulent acts of others where it is the intermediary. It is a recipe for fraud, and politically fraught with danger. Banks, however, are used to assessing and measuring risks, pricing risks, and wrapping risk management into services. Any institution wishing to rely on a credential

[29] https//assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686127/High_Value_Dealers_Guidance.pdf

[30] https//www.cifas.org.uk/insight/public-affairs-policy/anti-fraud-lesson-plans

needs to either have the ability to reverify data to its own satisfaction (e.g. a bank will never rely on data from another bank due to the liabilities that arise from such a decision); or the issuing party must be able to offer insurance or liability cover around that data - much in the way our credit cards and bank payment such as the Direct Debits scheme does today. We trust utilities to debit any amounts of money from our banks because if it all goes wrong, the bank will refund any loss, and if the bank can't afford to and becomes insolvent, the FSCS will step in and protect us.

State Multiplicity

State multiplicity of identity management and authentication systems is the default position in many western democracies – in addition to a commercial multiplicity of identity provision. Government systems for interacting with citizens have developed piecemeal and associated identity management and authentication systems have often been implemented in isolation from each other. The fragmentation of government systems creates the often-articulated challenge of implementing 'joined up government'.

In the UK, for instance, an individual could have the following different identification references by being enrolled in different identity management and authentication systems for interaction with UK governmental institutions:

- Universal Tax Reference (UTR) with Her Majesty's Revenue and Customs (HMRC)
- Value Added Tax (sales tax) reference with HMRC
- Child benefit reference (state subsidy for children)
- National Insurance number (for social welfare payments)
- Driver's licence number (for permission to operate a motor vehicle)
- Passport number (for international travel)
- Birth certificate (for proof of citizenship)
- Marriage certificate (for proof of marital status)
- National Health Service (NHS) number (for access to free healthcare)
- British Army, Royal Navy or Royal Air Force service number (for those serving in the armed forces)
- Shotgun or firearms certificate number (for permission to possess firearms)
- Council tax reference (for local property taxation)
- Housing benefit reference (for subsidised accommodation)

- London congestion charge account number (for those who drive in London and have to pay the associated toll)
- Oyster card number and associated account number (for those who travel by public transport in London and the south east of the UK)
- Library card.

The above list excludes both the criminal justice system systems for individual identity record keeping, and the myriad of licences and permits that are required to carry on a number of specific professions or trades (e.g. doctor or pharmacist, firearms dealer, dog breeder, fish farmer, wild animal keeper).

In the UK, some limited efforts have been made to connect these different identity management and authentication systems across government departments; for instance Universal Tax References and National Insurance Numbers have been linked within the UK tax system for some time. However, within the same UK government department, HMRC, UTR and VAT numbers are not connected or cross referenced, so obvious efficiency gains are not realised.

In Australia, the Centrelink initiative, dating back to 1997, provides unified online access to a range of government benefits and services from a single identity reference. The reference is issued based on production of three types of identity document (possession factor), of which the document containing photo ID (inherence factor) must be presented in person at an authorised agent or Centrelink service centre.

At one level, there is obvious inefficiency and waste in the systemic friction that a multiplicity of identity management and authentication systems introduces to an individual’s interactions with government, central and local. The current state of affairs in the UK is nowhere near the simplicity and automation offered by Estonia’s ID-kaart identity scheme.

Case Study: Estonia

In 1999, the Estonian government passed the Identity Documents Act making it mandatory for all ID card. This Act was followed up in 2000 by the Digital Signature Act, which together paved the way for the first national ID card based on blockchain technology.

In 2002, the Estonian government commenced the roll out of the digital ID cards (ID-kaarts), which can both be used as physical evidence of identity and for digital authentication for such activities as voting, buying travel tickets etc.

The Estonian government is rightly proud of its achievement in creating and implementing an ID card serving various physical and digital functions. However, their scheme also demonstrated the vulnerability of 'advanced' digital identity mechanisms implemented through a monopoly system. In 2017, it was revealed that the cryptography used to manage the Estonian public and private keys used a 'weak' cryptographic method, such that it was relatively straightforward to calculate probable private key values from analysing the public key.

The Estonian government issued a 'patch' which contained a certificate upgrade to fix the issue, but had to reserve a period where certificate upgrades could only be registered by Estonian government officials and doctors, to prevent mass public access to the ID system crashing it through traffic volumes to the site.

The Estonian government continues to innovate in how the ID-kaarts can be useful to citizens. Using the X-Road open source backbone, there are now more than 2,600 services that can be accessed where the ID-kaart is accepted as proof of identity.

However, that very friction does enable compartmentalisation of identity information, in case hackers illegally access stored data. If someone nefariously obtains an individual’s Oyster card details, they cannot use the information to access that person’s tax records. In aggregate, information is more securely held through fragmentation, than if it was all contained in one consolidated government database (as was proposed with the UK’s Identity Card scheme – see text box). There is a trade-off between efficiency, on the one hand, and privacy and collateral security of information storage with the associated friction and inefficiency, on the other.

Case Study: UK

There are no mandatory identification documents in the United Kingdom; both passports and drivers licences are elective. In 2006 Parliament passed The Identity Cards Act which, if implemented, would require mandatory ID cards for UK citizens, combining a personal identification document and an EU travel document. The details of all UK citizens were to be held on a National Identity Register which would also connect to all other government indices of citizens (e.g., National Insurance Numbers, HMRC Unique Tax References). The Register was to be managed and maintained by a rebadged Passport Service, then to be called the Identity and Passport Service.

Over the next four years, development of the identity platform proceeded, accompanied by repeated warnings of ever escalating complexity and costs. Projected costs rose from the original estimate of £88 per card rose to a forecast range of £157 - £285, assuming full cost recovery for the scheme over ten years and cards issued to 67.5 million people. 2010 saw pilot rollouts issued cards in Manchester and the North West of England, and also airport and airline staff. Faced with public antipathy and further project delays, in 2010 the implementation was abandonned and the 2006 legislation repealed by a further act of Parliament.

There was always public concern in the UK that a compulsory ID card would lead to civil liberties abuses. While initial public support among 'stakeholder groups' showed 61% of respondents (2,606 of 4,241 respondents) were in favour of IDs, 38% were against and just 1% were neutral. By 2006, even before the Identity Cards Act was passed, support had dropped to 52% as measured in a Daily Telegraph / YouGov poll.

There was even more opposition to the National Identity Register. In another Daily Telegraph / YouGov poll in December 2006, only 41% were happy, with 52% unhappy at the prospect of having their data recorded. Only 11% trusted the government to keep the data confidential.

The project was rendered unsustainable by the ballooning costs and publication of a damning report from the London School of Economics' Identity Project entitled 'The Identity Project: an assessment of the UK Identity Cards Bill and its implications' published in June 2005 (http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf). Its summary conclusion was that "the proposals currently being considered by parliament are neither safe nor appropriate". The report laid out concerns around many aspects of the proposed UK Identity Card implementation:

- Iris scan and fingerprinting biometrics to be used were not entirely reliable and had been successfully 'spoofed';
- The effectiveness of Identity Cards as an anti-terrorism measure was of negligible value;
- Identity Cards were not required by international obligations;
- Identity Cards would not materially counter identity theft;
- Identity Cards might promote questionable law enforcement practices;
- Any connection to the reduction of illegal immigration was unsubstantiated;
- The National Identity Register as a single central source of identity information would present a data security vulnerability;
- The overall IT design and architecture for the Identity Cards and the National Identity Register was problematic and expensive.

These remain live issues around the implementation of any identity management and authentication system. The report remains a valuable source of important considerations for the implementation of any identity management system in the UK.

Trust Structures

Looking forward it seems probable that the systems for managing identity must evolve from these existing, unsatisfactory, inconsistent and irreconcilable models. The World Economic Forum has evaluated Centralised, Federated and Decentralised developments for improving digital identity management and authentication systems. [31] The report assessed the advantages and disadvantages of each alternative as:

- Centralised
  - Strengths
    - Individuals can access the system owner's offerings, whether public services, banking services or social media networks etc. The system owner determines the level of due diligence carried out for proof of identity, based on regulation and compliance requirements and internal policies
  - Challenges
    - Centralised systems typically offer individuals little choice over how their personal data is used. Centralised architectures may represent 'honeypots' of individuals' identity data which can be attractive to hackers. Centralisation also gives owners power that could be abused

- Federated
  - Strengths
    - Federated networks can offer individuals access to a wider range of transactions, using a single set of credentials. Their inter-operability provides greater convenience for users
  - Challenges
    - Like centralised systems, federated systems usually give individuals little choice over how their data is used. For the providers, complexity arises from associated legal agreements, laying out risks and liabilities. The associated complexity makes implementation more expensive

[31] WEF Insight Report – Digital Identity – September 2018 pp.13-15

- Decentralised
    - Strengths
        - The core strength of a decentralised system is the control and transparency it offers: control over what identity information to share, with whom to share it and for how long. Decentralised systems can also support a more appealing consumer experience
    - Challenges
        - For a decentralised identity authentication and management system to operate, institutions like banks and government agencies, will probably need to contribute verified identities. Many such organisations are currently running centralised systems, where they own the user relationship, and they may be reluctant to surrender this control.[32]

The World Economic Forum also identifies the critical role of '**trust**' relationships in the operation of federated and decentralised identity management and authentication systems, backed by contractually enshrined rewards and obligations between participants. In the context of identity authentication, trust represents the extent to which an organisation or business seeking to confirm an individual's identity can rely upon previously established identity authentication for that individual completed by another organisation. Trust also involves agreed, contractual recourse from one organisation to another, in the event of fraudulent or inaccurate identity confirmation. The establishment and operation of these trust relationships is both complex and still in its infancy.

There have been a number of initiatives, in the financial services sector in particular, to establish an international framework for trust relationships between financial institutions, of which the most successful is probably IdenTrust, founded by a collective of UK and US banks in the late 1990s. IdenTrust created an international trust framework for banks which would cover a number of classes of information exchange, including B2B and B2C proof of identity. Although the programme never quite achieved its original ambitious goals, it still offers a model for further use. The PLOT artefacts (Policies, Legal framework, Operations hosting and Technology support) are available to subscribers to support further development of global trust infrastructure.[33] Regulated global financial services providers were the original designers of IdentTrust, so the PLOT artefacts provide a valuable starting point for ensuring

[32] ibid
[33] http://www.identrust.co.uk/certificates/learn/identrust-trust-network-blueprint

compliance across multiple jurisdictions. A bank that has conducted KYC due diligence in one geography can share the resulting identity credentials both with operations of the same bank in other geographies, and with other banks, who can then rely on the identity information without repeating the KYC processes. The single execution of the KYC validation offers clients notable benefits, e.g. for faster account opening, or establish capacity of the client to do business with another bank in another place. Individuals and businesses using IdenTrust PLOT with their banks and other financial institutions are able to execute business online confidently, because its credentials are broadly recognised across the globe. The IdenTrust framework can be used to:

- Open and maintain numbers of accounts across multiple jurisdictions, and with many financial institutions
- Provide identity management and authentication for individuals
- Deliver a single set of trust protocols which support many-to-many, international transactions while remaining regulatorily compliant.

Within the EU, there has also been related work in the trust arena, notably in the field of electronic signatures as proof of originator identity, without requiring a physical signature. However, nothing has yet been specified in the EU covering trust in terms of the inter-reliance of different organisations on each other's identity authentication processes. The rules as currently defined are contained in the eIDAS (electronic IDentification, Authentication and trust Services) regulations.[34]

The eIDAS initiative could form the basis for developing a broader set of EU identity authentication and management regulations, as well as establishing interoperability between organisations for the purposes of sharing individual identity information. The core challenge remains: what liability exists between an entity-confirming organisation and an entity that relies on this confirmation, if it subsequently turns out to be inaccurate or fraudulent? There is little by the way of inter-organisational alignment of view in this sphere at any level and no sign of any obvious current work that could lead to a future set of standards or agreements in the trust space.

A basic requirement for the successful operation of a market where there is a multiplicity of commercial identification authentication and management systems, is a **regulatory framework** for their operation. The market then needs

[34] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

to be curated and supervised by an appropriate regulatory authority. In the UK, regulatory oversight is provided by the Information Commissioner's Office (ICO), based on the rules contained within the EU-wide General Data Privacy Regulations (GDPR). It is notable that the US has no equivalent to GDPR and no overall regulator supervising and monitoring the use of individuals' data, including identity information.

The regulator provides the parameters within which commercially operated identity authentication and management systems can function. The regulations define what identity (and other) data can be acquired, for what purposes, who can access it, how long it can be retained, how it must be stored, obligations to enable individuals to access their data as held by identity authenticators, and its destruction (the right to be forgotten). GDPR provides a common framework for these regulations across Europe. Many geographies in Latin America and the Caribbean, Asia and Africa have also implemented similar frameworks.

Private sector initiatives to promote trust frameworks are emerging, recognising that without trust frameworks, progress on decentralised or federated identity systems will be strictly limited.[35] However, such programmes are in their infancy and will take some time to develop to the point where they form a reliable, usable framework.

A basic requirement for the successful operation of a market where there is a multiplicity of commercial identification authentication and management systems, is a **regulatory framework** for their operation. The market then needs to be curated and supervised by an appropriate regulatory authority. In the UK, regulatory oversight is provided by the Information Commissioner's Office (ICO), based on the rules contained within the EU-wide General Data Privacy Regulations (GDPR). It is notable that the US has no equivalent to GDPR and no overall regulator supervising and monitoring the use of individuals' data, including identity information.

The regulator provides the parameters within which commercially operated identity authentication and management systems can function. The regulations define what identity (and other) data can be acquired, for what purposes, who can access it, how long it can be retained, how it must be stored, obligations to enable individuals to access their data as held by identity authenticators, and its destruction (the right to be forgotten). GDPR provides a common framework

[35] The Kantara Initiative is seeking to define an interoperable trust infrastructure and profile existing specifications for identity Trust Frameworks. http://www.kantarainitiative.org

for these regulations across Europe. Many geographies in Latin America and the Caribbean, Asia and Africa have also implemented similar frameworks.

Regulators and legislators can also provide valuable rules and laws to support the development of digital identity authentication and management services. In this sphere, the US has made some notable progress, first through the creation of The National Strategy for Trusted Identities in Cyberspace (NSTIC), which is a US government initiative announced in April 2011 to improve the privacy, security and convenience of online commercial activities, including identity authentication and management. The NSTIC was created through collaboration with the private sector, interest groups, the US government agencies, and other bodies so represents a broad spectrum of interests.

This was followed up by the US National Institute of Standards and Technology publishing guidelines for digital identity implementations in the form of its Special Publication SP 800-63, of which the latest version is SP 800-63-3 published in June 2017 which lays out the requirements for 'proving' identity to different levels of assurance.[36] SP 800-63-3 provides very useful analysis on the issues and needs for implementing federated or decentralised identity management and authentication systems.

Legislators have also been giving trust legal issues relating to liability and obligation consideration in some parts of the world. The furthest advanced is probably the State of Virginia in the US, which passed the Virginia Digital Identity Law, approved on 23 March 2015.[37] The Virginia Digital Identity Law legislation creates an environment which holds identity verifiers harmless from subsequent liability, if they can demonstrate that they have exercised appropriate due diligence in verifying identities to different LOAs, even if subsequently those identities prove to be inaccurate. For commercial federated or decentralised identity management and authentication systems to thrive, these are the types of trust environment required to enable such systems to develop.

Optimising Identity

There are a number of factors to weigh to determine the optimum identity system:

[36] http://csrc.nist.gov/publications/detail/sp/800-63/3/final

[37] http://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483

- **Reliability** – What is the risk of mis-classification or false positives or false negatives?
- **Security** – How safely is identity data stored against unauthorised, access, modification or destruction?
- **Usability** – How easy is a system to access and use, when required?

The World Economic Forum report developed a set of tests for individual identity authentication and management systems which provides a useful framework: [38]

- Useful
  - Portable – so can be moved around and used in remote places to enable those populations living far away from infrastructure still to enrol;
  - Interoperable – will work with other identity management and authentication systems, with individuals ideally being offered a choice of identity management and authentication systems, as well as providing access to services for those enrolled;
  - Acceptable – has public support and is not repressive or controlling;
  - Responsive – can be adapted with relative ease as circumstances change;

- Inclusive
  - Universal – available to all from every socio-economic or demographic segment and considers and designed for differences in abilities, age, digital literacy, access to technology and use-cases;
  - Non-discriminatory – treats all individuals equally, no matter what their socio-economic or demographic background and sets standards for data to be captured and trust anchors to be used, so all enrolled individuals have consistent information;
  - Accessible – can be readily and easily used by all types of individuals, e.g. both able bodied and disabled;
- Secure
  - Trusted – data is not mis-used and the use of identity management and authentication systems is appropriately regulated with independent oversight;

[38] WEF Insight Report – Digital Identity – September 2018 pp.18-23

  - Secure – data is held securely and safely to reduce cyber-crime and prevent disasters, with processes for remediation in the event of breach or accident;
  - Do no harm – not used as an instrument of social control or repression;
  - Auditable – individuals have the right to access and correct the data held;
- Offers Choice
  - Protects user rights – facilities are implemented to ensure security, privacy and no mis-use of the data held, with individuals able to control who accesses their data and for what purposes;
  - Transparent – the information held can all be accessed by relevant and authorised individuals, e.g. the subject;
  - User-managed – individuals control their own data both that is stored and the information that is made available to those wishing to confirm an individual's identity;
  - User-centric – puts the needs of individuals using the system first;

- Fit for Purpose
  - Accurate – contains only valid and correct information and is up-to-date;
  - Sustainable – can be upgraded as data volumes increase and technologies advance, backed by policies that evolve as circumstances change, and a financial model that generates sufficient revenue;
  - Acceptable – has public support and contains only the minimum data required;
  - Unique – does not contain duplicate information for a given individual.

With regard to the use of these criteria going forward, the World Economic Forum representative for the identity initiative, Manju George, elaborated that the criteria were not just recommendations but could form the basis for ongoing assessment of identification systems: *"[W]e wish to see tools that can measure how solutions stack up in line with the five principles and we may even seek to assess systems' performance against them."*

Smart Ledger Identity Systems

Given that no system for identity management and authentication will be infallible, the search is on for techniques and solutions which optimise the objectives of **secure, usable** and **reliable**. Distributed ledger technologies using 'blockchain' based information storage and retrieval methods can provide a significant advance in decentralising and securing identity data, and make it useable to a wider array of applications.

Blockchain technology is frequently implemented in the form of 'mutual distributed ledgers' which can be used to store any type of information. Smart Ledgers combine mutual distributed ledgers with processing applications. Smart Ledgers are particularly attractive for maintaining critical identity management and authentication information because they are highly secure, adaptable to meet diverse needs, and all alternations of records are transparent and auditable.

A technical solution to this sensitive issue could adopt Smart Ledgers for data storage using cryptographically secure, blockchain technology as described in "The Use of Distributed Ledgers for Storing Identity Information" by Professor Michael Mainelli, who writes:

> The problem with a central database like the ones used to house social security numbers, or credit reports, is that once it's compromised, a thief has the ability to copy all of the information stored there. Hence the huge numbers of people that can be affected — more than 140 million people in the Equifax breach, and more than 50 million at Home Depot — though perhaps Yahoo takes the cake with more than three billion alleged customer accounts hacked. Of course, if you can find a distributed ledger online, you can copy it, too. However, a distributed ledger, while available to everyone, may be unreadable if its contents are encrypted. Bitcoin's blockchain is readable to all, though you can encrypt things in comments. Most distributed ledgers outside cryptocurrencies are encrypted in whole or in part. The effect is that while you can have a copy of the database, you can't actually read it.[39]

[39] https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data

A Smart Ledger combines a mutually distributed ledger with sophisticated applications to perform functions needed by a network of users of the recorded data. The key innovation is a public blockchain that eliminates the need for a state or commercial actor to run the network; instead a decentralised peer-to-peer network relies on advanced cryptography. Replication of the data across all network nodes secures against single point of failure data loss or corruption.

Smart Ledgers are inherently secure and recorded data is less vulnerable to unauthorised access or corruption. Smart Ledgers also provide immutability and longevity of storage in that, whilst records can be added to the blockchain, there is no mechanism for modifying or deleting information that has previously been stored. The technology is inherently attractive for storing identity information, which needs to be retained securely and maintained rigorously over time.

Smart Ledgers both hold the subject information as well as maintaining a record of all access requests. Maintaining a record of information access requests provides a history of who has attempted to view or append Smart Ledger information, which can be valuable where the Smart Ledger subject data relates to identity. An individual may well want to know who has accessed their identity data, when and how often, even where permission to view that identity data has been granted. Maintaining an access audit trail is potentially an important safeguard which could be offered to identity system users, for example where governments insist on collecting identity information about their citizens.

The nodes on a Smart Ledger network each hold a copy of the Smart Ledger and all follow a common protocol to add new transactions. The protocol to add data is distributed using a peer-to-peer application architecture to ensure all nodes have the correct protocol.

The data itself is almost invariably stored using one of the three most popular options, which, in increasing order of security, are:

- **Unencrypted**, which means that all data stored in the Smart Ledger can be read by all ledger participants, providing for full transparency, but much lower levels of security then other options within the Smart Ledger;
- **Encrypted**, which can only be read by the Smart Ledger participants with the relevant decryption key;
- **Hashed**, where only an encrypted reference (a 'hash') for the actual Smart Ledger data is stored on the blockchain, while the data itself is stored elsewhere and can then be retrieved when required, but not otherwise.

For identity management and authentication systems, the encrypted and hashed options are clearly the most appropriate. Just because an individual has registered their identity information with a Smart Ledger identity system, doesn't mean that they should be able to access all other users' data or other users access their information.

Smart Ledgers can be used as a platform for centralised identity management and authentication systems, as well as federated and decentralised identity management and authentication archetypes. Indeed, for distributed identity management and authentication systems it is difficult to envisage that any alternative technology would support functionality for users with equal efficiency and effectiveness.

An increasing number of calls are being made to implement decentralised identity management and authentication systems using blockchain technology, which leads to an individual's ability to manage and control their identity information securely. This concept is called 'Self-sovereign Identity'. A recent example from Germany published in November 2018 is:

> The identity working group of the German Blockchain Association presents this position paper on the emerging paradigm of self-sovereign identity. As a novel framework for the creation, management and interaction of digital identities, self-sovereign identity represents a major leap for both digital and analog interactions. We are convinced that blockchain and other decentral technologies represent a fundamental infrastructural innovation, that has the potential to enable a fair and inclusive digital economy.[40]

There are also three different types of access to Smart Ledger or blockchain applications, each appropriate for different circumstances:

- **Un-permissioned** (also known as public) Smart Ledger or blockchain, where access is open and uncontrolled. For instance, Bitcoin, allows any individual full access. Anyone can read, or make changes to, the blockchain, like adding a new block or maintain a full copy of the entire blockchain;

[40] http://www.bundesblock.de/2018/10/23/position-paper-self-sovereign-identity/

- **Permissioned** Smart Ledger or blockchain, which maintains access control to permit actions to be performed only by certain participants. Permissioned Smart Ledgers or blockchains require prior authority to be granted to participants to read, access, and write information to them. Examples include Ripple, which determines roles for its Smart Ledger participants;
- **Private** Smart Ledger or blockchain, which will only permit known nodes to participate in the ledger. For example, a financial institution may establish a private blockchain which only allows access from nodes within its own organisation.

Many perceive the permissioned Smart Ledger as the most appropriate option as it offers the security of oversight of access and control of use. Access to the system is granted only to 'permitted' users, thus restricting the ability to read or write identity data to authorised individuals or organisations. A permissioned Smart Ledger can be configured to recognise different tiers of access rights, for example authorising one user to amend a record but providing 'read only' access to other users.

Usability is also a key attribute for identity authentication and management systems. Many users of the current security features for digital services, whether through governments or the private sector, find the multiplicity of different passwords, security features, confirmation tokens, and other barriers to use confusing and discouraging. Help desks dealing with customer problems are a big element in operations costs. The need to balance security and usability has led to significant debate and consideration, both within organisations evaluating systems improvements and among organisations trying to define a collective path forward.

One outcome of those debates is the international standard, ISO9241, which covers 'the ergonomics of human–system interaction'.[41] In the ISO9241 standard, usability is defined as:

> The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

[41] http://www.iso.org/standard/52075.html

ISO standard provides parameters for identity management and authentication systems to deliver. However, there are a number of challenges in real world implementations. One challenge is that, frequently, establishing proof of identity still involves the production of physical documents (or at least images of those documents). Managing the use of physical documents is inherently cumbersome and, whilst often unavoidable, is no friend of efficiency or satisfaction. Its effectiveness can even be questioned, given the instances of forgery and counterfeiting.

Usability for IT systems is formally defined by International Standards' Organisation (ISO) standard ISO 9241 Part 11 and states that it has to be measured within the context of use of a system, dealing with a number of dimensions to that system's use, namely:

- Who is using the system;
- For what they are using it;
- The environment in which they are using it.

Measurement of usability, according to the ISO standard, has a number of dimensions:

- Effectiveness (can users achieve their objectives?)
- Efficiency (how much effort and resource is required?)
- User satisfaction (how was the experience?).

In identity authentication and management systems, effectiveness is frequently the enemy of efficiency and of user satisfaction. The more secure (effective) a system is, typically the less user friendly it is and the more challenging or cumbersome (inefficient, unsatisfying) it becomes to use. A four-digit PIN as proof of identity is relatively convenient, but highly insecure (ineffective) having only 10,000 combinations, many of which may be obvious if a fraudster has knowledge of the victim.

At the other end of the scale, some identity authentication and management systems spend much of their existence keeping out authorised users, they are so cumbersome and unwieldy to manipulate (e.g. requiring a biometric scan and a token and a pass phrase and a challenge and response, as some identity authentication systems do). There is no right answer. Any solution is a balance of trade-offs and depends upon the context and criticality of the identity authentication process as well as the risks or losses resulting from mistaken identification.

The third factor to consider in the context of implementation of identity management and authentication systems is **reliability** (at least 96th+ percentile accurate). If an identity management and authentication system's approach to identity confirmation is so flawed that it either rejects a substantial proportion of authorised users, or validates a substantial proportion of unauthorised users, then it is of little utility. The costs of exceptions resolution would quickly outweigh any benefits.

There are a number of dimensions to reliability, notably:

- **Universality** - How likely is it that an individual will be able to enrol in an identity management and authentication system? (e.g., If it is mandatory that an individual can write or access the internet, in many parts of the world substantial proportions of the population will be excluded.);
- **Permanence** - How likely is it that an individual's ability to use an identity management and authentication system over a long period of time persists? (e.g., Faces of young people change with age and therefore impair facial recognition systems over time.);
- **Environment sensitivity** - How likely is it that environmental factors will interfere with an identity management and authentication system? (e.g., Voice recognition systems can easily be affected by background noise.);
- **Vulnerability** - How easy is it to fool an identity management and authentication system? (e.g., Iris scan recognition systems can be relatively easily fooled by a high quality colour photograph of an individual's iris.).

The above factors all need to be considered, when assessing or deciding on a specific identity management and authentication system, as critical factors in the effectiveness of any given solution.

To Be, To Know & To Have

ISO 9241 has led to an evolving 'industry standard' that identity authentication will ideally be made up of three separate components:

- **What you are** (often described as the inherence factor) – customarily involving biometric information;

- **What you have** (possession factor) – for instance, having a token; and
- **What you know** (knowledge factor) – which can include PINs, passwords, pass phrases, zero knowledge proofs etc.

Many mobile phones, tablets and laptops have replaced more traditional 'what you know' access controls with 'who you are' authentication, so devices now frequently deploy fingerprint recognition as a replacement for passwords or PINs. As the devices already have the hardware and software for fingerprint assessment and validation, the functionality can be integrated more widely with other online and device applications.

The requirement to pass multiple identity tests is known as multifactor authentication, or MFA. MFA combines two or more of these approaches: what the user is (biometric verification), what the user knows (password), what the user has (security token). The goal of MFA is to create a defence that has multiple layers and to make it much more challenging for unauthorized access to replicate individual identity authentication. If one factor is compromised or broken, the attacker still has more levels to breach before being able fraudulently to claim to be an individual.

For example, online banking applications' identity authentication processes generally need both a password or passphrase, and information derived from a token or dongle that generates verification codes. The exchange often takes the form of a 'challenge – response' format where the user keys something generated by the online banking application into the token and the token generates a response to be entered into back into the bank's online system.

The UK government now offers users of the Government Gateway with the option of increased security through validation codes sent to mobile devices. This has the security advantage of being instantaneous with user access attempts, with the validation number expiring if not used within a time limit.

It has been suggested, that as well as the three identity authentication factors described above, a further two factors could also be invoked, namely:

- Location factor – which could be confirmed through GPS technology on the near-ubiquitous on mobile devices;
- Time factor – for example, it would not be possible for someone to confirm their identity in, say, London, England, and one hour later seek to authenticate their identity in Sydney, Australia.

Implementation Considerations

Inheritance (to be), knowledge (to know), possession (to have) are all factors that can be developed and enhanced to build multi-layered authentication systems more resistant to attack and abuse, but without standardisation of methods and harmonisation of identity management frameworks the scope for efficiency gains remains limited. The globalised world of digital commerce and mobile populations requires better solutions, but the path forward is uncertain and complicated.

What you are (inherence) – biometric identity authentication & management

Biometric systems are becoming more and more widely used for identity authentication and management and their use is set to grow further as is shown in Figure 3 below:

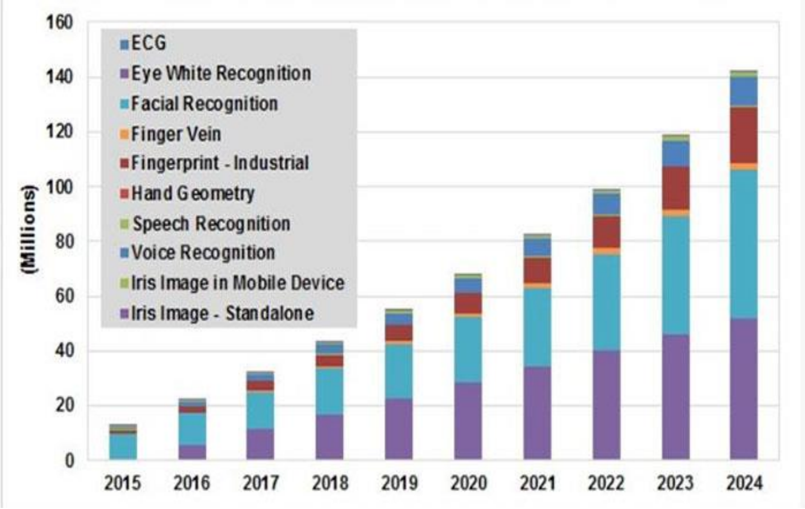


Figure 3. Enterprise biometrics devices and licences, World Markets: 2015 – 2024 (source *Tractica*)

No biometric identity system is 100% reliable. Nor is any biometric modality ('modality' is shorthand for expressing a way a record of a biometric characteristic has been created) 100% reliable. What needs to be achieved for better biometric identity management and authentication systems is a balanced improvement to diminish two problematic outcomes.

The two undesirable results are:

- **False Acceptance Rate** (FAR) which is 'the measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorised user. A system's FAR is typically stated as the ratio of the number of false acceptances divided by the number of identification attempts'; [42]

- **False Recognition Rate** (FRR) which is 'the measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorised user. A system's FRR is typically stated as the ratio of the number of false recognitions divided by the number of identification attempts'.[43]

Typically, there will be a trade-off involving an optimum balance between these two undesirable results, where identity recognition calibration can be set to vary between them. Therefore, as the FAR declines, it is highly likely that the FRR will increase. Real world implementations need to take this trade off into account when determining how to set up biometric identity management and authentication systems. The question that must be answered is: What is the risk associated with letting false identities through versus the risk of inconvenience or annoyance or a problem arising from failure to recognise an authorised individual?

Summarised in Figure 4 below is an assessment of the major biometric modalities for individual identity management and authentication, which are also briefly described below. Other biometric modalities exist (e.g. behavioural biometrics from analysing data, such as gait when moving) but these are used for individual identification, rather than identity authentication, purposes so are not discussed here.

Modality / Characteristic	**Intrusiveness**	**Permanence**	**Universality**	**Environment Interference**	**Template Storage**	**Difficulty to 'Spoof'**	**Reliability FAR/FRR**	**Cost of Equipment**
Fingerprint recognition	High	High	High	Low	Low	Medium	FAR/FRR 0.001 claimed	Low
Palm vein recognition	Medium	High	Very high	Low	High	Very high	FAR/FRR 0.01 claimed	Medium
Hand geometry	Medium	Medium	High	Low	Medium	High	FAR 14.6 FRR 0.2 claimed	Low
Iris scanning recognition	Very high	High	High	Medium	High	Medium	FAR 0.2 FRR 0.0001 claimed	High
Retinal scanning	Very high	High	High	Low	Low	Very high	FAR/FRR close to 0 claimed	High

[42] http://www.webopedia.com/TERM/F/false_acceptance.html

[43] http://www.webopedia.com/TERM/F/false_rejection.html

Eye vein scanning	High	High	High	Low	High	High	Lack of published data	Low
3D Facial recognition	Medium	Medium	Very high	Low	High	High	FAR/FRR 1.5 – 3.0 claimed	Low
Voice recognition	Medium	Medium	High	High	High	Low	FAR/FRR 10.0 claimed	Low
Dynamic Signature recognition	Medium	Low	Medium	Low	Low	High	FAR/FRR 2.0 claimed	Low
DNA recognition	Very high	Very high	Very high	High	High	Very high	FAR/FRR 0.5 claimed	Very high

Figure 4. Summary assessment of major modalities for biometric individual identity management and authentication

It should be noted that the FAR and FRR rates claimed above, whilst verified, were frequently measured in test or laboratory conditions. Real world experience may well demonstrate significantly less reliability due to environmental and other factors.

It is notable that there have been no major breakthroughs in developing new biometric modalities for identity authentication and management in the last twenty years or so. It may be that developing hardware and software for a new modality is too daunting in scale now that fingerprinting and iris recognition are commonplace, but innovation in this area should be encouraged. Listed below are the modalities currently used in identity authentication and management.

A **fingerprint** is an impression of the friction ridges of all or any part of the finger. Very little time is required for data capture (enrolment) with a fingerprint scanning system, it is quick to use. Fingerprints are a unique identifier, specific to an individual, and most people are familiar with the use of fingerprints for identification purposes.

Fingerprints are probably the most commonly used biometric modality deployed for identification. They are widely accepted, especially by law enforcement agencies and forensic scientists (people can be convicted of crimes based on fingerprint evidence) and have been used for a century or more. They do not vary with age and are permanent (*pace* the individuals whose work may result in loss of fingerprints, e.g. manual laborers and glassblowers).

It should be remembered that the method used by fingerprint scanning devices is always based on a probabilistic match, as a finger may only give a partial scan or may have acquired a small scar, for instance, and the data acquired is then subject to an algorithm which seeks to identify the probability of a match based on the information provided. The quality of data obtained needs to be combined with a mathematical algorithm to produce the resulting identity authentication outcome, which is true of all biometric modalities which require a marching algorithm as well as input data.

The **palm vein (finger vein) pattern** recognition biometric modality uses an image taken by an infrared sensor of the unique pattern made by the veins in the palm (finger) of an individual's hand (which can also be applied to fingers) for identity management and authentication. These veins show up as blue lines under infrared light. The palm vein pattern recognition modality has the advantage of being based on something internal to the body, so is much more difficult to replicate fraudulently. It also requires both the raw scan data and an algorithm which then interprets the information to confirm a match or otherwise.

Real world implementations of palm vein pattern recognition are unusual. BT ran a very successful finger vein pilot for VIP guests to pay for drinks at a music festival in Port Meirion in September 2012, but subsequent take up of the modality has been limited.

Hand geometry is a biometric modality that identifies individuals by the precise measurement of the shape of their hands. The hand geometry modality requires a reader that calibrates an individual's hand along many dimensions for identity authentication. A combination of both prisms and light emitting diodes are used from within the scanner to capture the raw images of the hand. All sides of the hand are measured, including the front, the back, and the palm. After these raw images are taken, a composite 3D picture of the hand is then created and fed into the matching algorithm to confirm identity.

To capture the optimum images, five guiding pegs are located just beneath the camera to help the individual properly position her or his hand. It has been used since it was invented in the 1980s and one of its earlier scale implementations was when it was installed at the 1996 Olympic Games to control access to the Olympic Village.

Iris scanning is one of the most reliable biometric modalities. It is a method of identification that uses pattern recognition techniques in an algorithm that operates on the unique shapes made by fibres on the ring-shaped region surrounding the pupil of the eye (the iris). The iris usually has a brown, blue, grey or greenish dominant colour (or some combination), with complex, visible patterns.

Retinal scanning is also a very reliable biometric modality. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique (even within identical twins). However, retinal scanning requires substantial co-operation from the end user to collect high quality data. The modality requires that the individual must be in very close proximity to the retinal scanner.

It was as far back as the 1930s that researchers first observed that the pattern of blood vessels in the retina differs between individuals and that it could be used as a mechanism for identity management and authentication.

Eye vein scanning involves taking images of the veins in the white of the eye (sclera) which can be scanned when an individual looks to either side, providing four images – one for both outer parts of each eye. One of the strengths of the eye vein scanning modality is the stability of the pattern of eye blood vessels. They are also sufficiently obvious that they can be scanned by most smartphone cameras.

This modality is relatively recent in origin. It was developed by a pioneer in the US and was patented in 2008. The same researcher has also gone on to patent equipment in 2012 to deliver this modality, but its practical implementation has been limited to date.

Facial recognition is a very well established biometric modality. However, until relatively recently, it was (and still is) performed manually, e.g. passport and immigration control on arrival in a country or being stopped for a potential traffic offence by the police. Now scanners and software are being used to automate this job. 3D facial recognition scanners are far more reliable than 2D scanners and process such data as length of the jawline, cheekbones shape, distance between the eyes, depth of the eye sockets and the width of the nose. Facial recognition software can be deployed in contexts without people even being aware of it. For example, every time Facebook users upload a picture and tag their friends in it, the Facebook facial recognition algorithm receives more information with which to improve its accuracy (it is now more accurate that the FBI's equivalent system).

Real world experience is varied. It has been used a number of times relatively successfully (e.g. UK border and immigration control for confirming the identity of travellers against their passports), but recent reports in the UK of research by Cardiff University into South Wales Police's use of facial recognition software, cited a confirmation rate of only 76% for accurate identification, with 68% of images being of insufficient quality to use by the facial recognition software deployed[44]. It is also (December 2018), being trialled by the Metropolitan Police in London.

Voice recognition is a biometric modality that works by analysing the elements of speech that differ between individuals. Every individual has a unique way of speaking arising from the size and shape of their mouth, throat and chest together with behavioural differences, such as the pitch of their voice, their style of speaking and their accent.

With the **dynamic signature recognition** biometric modality, it should be noted that it is not the image of the signature which is compared; rather, it is the patterns created by the process of signing which are used. The factors measured include timing, pressure, pauses and speed of creating the signature. Although it is relatively easy to duplicate appearance of a signature, it is very difficult to duplicate these characteristics.

The **DNA fingerprinting** biometric modality has been in use since 1984. Its use to date has largely been confined to criminal justice, other forensic purposes, and paternity testing. Public perception in general is that providing DNA samples is highly intrusive and gives rise to serious civil liberty concerns. To date, there are few, if any, proponents of it as a routine, practical identity management and authentication modality, given the specialist equipment, dedicated personnel, and timescales required. The reason for the FAR / FRR rating in the above table being as high as 0.5 is due to the risk of sample contamination and analysis process errors. DNA itself is completely reliably unique to an individual.

The advantages and disadvantages of each of these biometric modalities are set out in more detail in Appendix 1.

[44] http://www.bbc.co.uk/news/uk-wales-46359789

What you have (possession factor) – possession-based identity authentication and management

Historically, 'what you have' was often the only form of individual identity authentication and management that existed and that was also reliable, such as a letter of introduction or bank account book. These documents could frequently be critical for sanctioning individuals or their actions.

In the sixteenth century, when there was only a very limited formal British navy, Queen Elizabeth I issued 'letters of marque' (licences to sail an armed vessel for the purposes of capturing enemy shipping from a nation at which the issuing nation state, or its sovereign, was at war and which were issued from the thirteenth to the nineteenth century) to a number of privateers to plunder Spanish silver ships returning from the New World. Sir Francis Drake and Sir Walter Raleigh both conducted their naval actions under the auspices of letters of marque issued by the queen and both, accordingly, greatly profited from their adventuring. Without these documents, authenticating the identity of these captains as agents of the English crown, the actions of these men, and others, would have been regarded as criminal piracy.

The number of **items of possession**, historic and current, carried by individuals for the purposes of identity authentication and management is legion, including (but in no way limited to):

- Beads (recently discovered in South Africa, Algeria and Israel; the oldest dating back to approximately 100,000 years ago that conveyed identity information)
- Wood and wax diptych (used in Roman times as a combined birth certificate and citizenship certificate)
- Seal (typically used to authenticate documents or letters to prove their originator and that they have not been altered since creation)
- Signet ring (as above)
- Letter of introduction
- Letter of safe passage (originating in the Holy Roman Empire and continuing to exist through Medieval Germany, where the owner of a road committed himself to pay damages if a traveller was robbed, by issuing letters of authority to that effect to individuals using the road)
- Letter of credit (for accessing financial facilities away from one's home base or for proof of financial solvency)
- Letter of marque (see above)

- Birth certificate
- Freedom certificate from the City of London, or other city
- Passport
- National citizen ID card
- Foreign citizen ID card
- Corporate, government or military ID card
- Military ‘dog tags’
- Social welfare card
- Driver’s licence
- Firearms or shotgun certificate
- Building or facility access card, security tag or ‘dongle’
- ‘Token’ for access to online services (typically for banking or secure corporate access applications).

The vast majority of these items functioned to confer rights beyond identity authentication. For example, the Roman wooden diptych confirmed that an individual was a Roman citizen with the right to:

- Be free
- Vote
- Serve in the military
- Attend public entertainment
- Be exempt from certain taxes
- Invoke the protection of Roman law (for justice, inheritance, marriage and property contract purposes)
- Be spared some punishments, e.g. crucifixion.

Similarly, letters of credit allow access to financial resources; driver’s licences confirm what types of vehicle can be lawfully operated by the holder; passports confirm citizenship; firearms certificates confirm the legal right to possess guns etc. Many items that confirm identity have other embedded meaning associated with them too.

Since these identity items customarily embody significant value to the holder, whether in authenticating the identity of the carrier or possessing meaning beyond that, keeping them secure from forgery or counterfeiting has always been important. As the technological sophistication of counterfeiters and forgers has increased, so the response has been to make the items more difficult to modify or recreate.

Where individuals' objects of possession for identity purposes are concerned, this has generally meant the inclusion of a microchip in identification objects (the result being usually referred to as 'smart' cards, but with biometric information also embedded in passports), combined with other with anti-fraud measures. Very often biometric information about the individual is included to make convincingly authentic unauthorised creation or modification 'impossible'. As a minimum, the biometric information would be the holder's photograph, but increasingly including other biometric data too.

Tokens are an increasingly popular class of possession-based identity, because they have the capacity to 'prove' possession remotely. Almost all the possession-based identity objects listed above require physical presence of the carrier, the item, and an inspector, to be certain that their possession is legitimate. Tokens enable remote delivery of proof of possession by generating (usually) numbers (often in response to a prompt) that can be entered into an application to show the user does, indeed, have possession of the token. The downside is that tokens must be physically distributed to individuals and periodically replaced, and then re-distributed, which is a relatively cumbersome and expensive process.

What you know (knowledge factor) – knowledge based identity authentication and management

Knowledge based proof of identity surrounds us in everyday life. We need to know **passwords** (or, increasingly **pass phrases**) or **PINs** to access almost everything in the virtual world and many things in the physical world. The author, who considers himself to have a limited footprint in the internet world (e.g. has no presence on social media), counted up how many such passwords or pass phrases or PINs are required for his day-to-day existence and came up with:

- 5 x PINs for credit and debit cards
- 3 x passwords for online banking (plus needing to possess a 'token' – see below)
- 6 x passwords for email addresses (4 x work related, 2 x personal)
- 1 x pass phrase for a further work email address
- 1 x PIN for mobile 'phone
- 26 x passwords for online Apps.

Increased security can be provided for passwords by requesting that only certain characters in the password, e.g. the second, fourth and fifth digit, are entered. Using selected characters is designed to make it more difficult for 'brute force replay' attacks simply to bombard an application with many thousands of automatically generated password attempts to 'guess' the password which authenticates an individual.

In addition, many applications now require the registration of **responses to questions**, either as a further layer of identity authentication or as a contingency measure in the event of a mislaid password or pass phrase. These can take two forms of challenge and response:

- The individual can register a question and its response, which is less usual, or
- More commonly, the application already has set questions to which a response is required (which can be a single question, multiple questions, or an opportunity to select a single question from a limited range and enter a response).

Yet another variation is registering a **memorable word** and also registering a 'hint' in the event of being unable to remember the memorable word (clearly not always that memorable!).

The level of security represented by passwords is entirely in the hands of users. Often, daunted by the complexity of managing too many difficult passwords, users opt for common choices. '123456' overtook 'password' as the commonest password in 2013 – but 'password' still remained the second commonest password in western countries in 2017.[45] Many applications now 'score' an individual's password, when it is originally set up, against a scale from 'weak' to 'strong' to help guide users to registering an effective password.

PINs are highly insecure, as mentioned previously, having only 10,000 combinations for a customary 4-digit value which, in terms of vulnerability to raw computing power combination generation, is very vulnerable. PINs are usually associated with a credit or debit cards or mobile phones. Cash machines and other devices that accept these cards seek to compensate for this finite number of combinations by only permitting a limited number of tries before a

[45] https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

credit or debit card is retained or further attempts at the PIN are prevented (in the case of a mobile phone, the device is 'locked').

A large proportion of card fraud in the UK is associated with criminals using phones to take a picture of a customer card as it is being inserted or withdrawn from an ATM and memorising the four-digit PIN while it is used. With the 16-digit card number readable in a photograph and the PIN memorised and then recorded with the picture, they have the data needed for basic card fraud.

Relatively recently, **one-time pass codes** (also known as 'one time passwords' or 'one time PINs') have started to be issued as an additional identity authentication proof. They are based on a combination of 'what you know', in terms of the one-time passcode, and 'what you have', in the form of a mobile -phone to which the passcode is sent, usually via SMS. The major advantage of this authentication approach is that it is not vulnerable to 'replay' attacks as the code changes frequently.

Typically, one time pass codes are implemented as part of logging on to an application (whether a government department, such as HMRC in the UK, a financial institution e.g. for online banking, or other application provider, e.g. Salesforce – the latter only applying this test if it is accessed by a user from a device other than that customarily used to logon to the product). After entering the usual user ID and password, the application sends the one-time pass code, which then needs to be keyed in as part of the logon sequence. In theory at least, one-time pass codes provide a further level of security in authenticating an individual seeking to use an online service.

A more sophisticated modality for confirming 'what you know' is represented **by zero knowledge proofs**. These have been in existence since the mid-1980s. Wikipedia contains a useful illustration of how a zero knowledge proof works:

> There is a well-known story presenting the fundamental ideas of zero-knowledge proofs, first published by Jean-Jacques Quisquater and others in their paper "How to Explain Zero-Knowledge Protocols to Your Children". It is common practice to label the two parties in a zero-knowledge proof as Peggy (the prover of the statement) and Victor (the verifier of the statement).
>
> In this story, Peggy has uncovered the secret word used to open a magic door in a cave. The cave is shaped like a ring, with the entrance on one

> side and the magic door blocking the opposite side. Victor wants to know whether Peggy knows the secret word; but Peggy, being a very private person, does not want to reveal her knowledge (the secret word) to Victor or to reveal the fact of her knowledge to the world in general.
> They label the left and right paths from the entrance A and B. First, Victor waits outside the cave as Peggy goes in. Peggy takes either path A or B; Victor is not allowed to see which path she takes. Then, Victor enters the cave and shouts the name of the path he wants her to use to return, either A or B, chosen at random. Providing she really does know the magic word, this is easy: she opens the door, if necessary, and returns along the desired path.
>
> However, suppose she did not know the word. Then, she would only be able to return by the named path if Victor were to give the name of the same path by which she had entered. Since Victor would choose A or B at random, she would have a 50% chance of guessing correctly. If they were to repeat this trick many times, say 20 times in a row, her chance of successfully anticipating all of Victor's requests would become vanishingly small (about one in a million).
>
> Thus, if Peggy repeatedly appears at the exit Victor names, he can conclude that it is very probable — astronomically probable — that Peggy does in fact know the secret word.[46]

Zero Knowledge Proof is important for maintaining the future of distributed ledger data integrity. Zero Knowledge Proof assurance can allow data to be consensually pushed to relying parties, enable customers to see how far the data has gone, revoke permissions, and signal changes – without revealing or moving data from where it is securely stored.

There is also a specific authentication variant, called a zero-knowledge password proof, or ZKPP, which was first defined in 1992. It is possible to include ZKPP-type modalities in 'what you know' identity authentication systems and these are considerably more secure than passwords, or even pass phrases, and are certainly harder to access fraudulently than PINs.

The most frequent use of the ZKPP modality is in cryptographic exchanges known as password-authenticated key exchanges (PAKE) which use a protocol

[46] http://en.wikipedia.org/wiki/Zero-knowledge_proof

to agree a cryptographic key based on mutual knowledge of a password and where a very limited number of tries are permitted to demonstrate knowledge of the password, making external unauthorised intervention difficult. Whilst the password protection in itself may not be very strong, the PAKE protocol compensates for this limitation and ensures that the key exchange is subject to appropriate, strong overall security. PAKE is not a 'pure' zero knowledge proof of identity instance, but it is a practical derivation that has widespread application in authentication protocols.

Conclusion and Recommendations

The paper has briefly considered identity management and authentication for individuals and entities to improve digital interactions with governments, the private sector, and each other. It demonstrated the challenges that practical implementations of identification authentication and management systems for individuals pose. The considerations have been assessed against the ideal of proving three dimensions of identity in terms of:

- **What you are** (the inherence factor)
- **What you have** (the possession factor)
- **What you know** (the knowledge factor).

The first conclusion must be that there is no 'silver bullet' that provides the ideal of a 100% secure, convenient and cost-effective implementation identity management and authentication. Progress has been made, but the range of systems being used by governments and private sectors is massively diverse and largely incompatible with ambitions for wider interoperability. Progress has also been made on standards, on methods, on technologies, on cooperative governance, but no solution has the critical mass that will deliver a globally secure, usable, cheap solution in the near term.

Policy makers at a national level, implementers at an institutional level and designers at an application level should consider the World Economic Forum's tests (see 'Alternative Options for Identity Management and Authentication Systems' above) for the features and characteristics that identity authentication and management systems should incorporate. There are obviously trade-offs between some of the WEF criteria (e.g. between 'Useful' and 'Secure'), but overall the Forum's model is a helpful framework. As so often with technology, the fundamental trade-off is between ease-of-use, reliability and security. The three factors (inherence, knowledge, and possession) of identity management can be onerous to meet in themselves and if each of them is implemented in a manner that is cumbersome to operate, the resulting approach to individual identity authentication and management can be virtually unusable.

Establishing identity can be a critical capability for an individual to function economically, socially and politically in the twenty-first century. However, across the world, the debate rages as to the benefits and drawbacks of the implementation of universal identity through the most popular option namely, a state monopoly identity authentication and management system, which usually takes the form of national ID cards. While state initiatives may be the fastest route to providing identity management for the greatest number of people, and India and China offer examples of extraordinary achievement, there remains a discomfort with the potential for state identity systems to lead toward greater repression rather than greater opportunity.

Whether systems being developed by states as monopolies deliver benefits for their peoples or further authoritarian oppression will be determined by the outcomes as the intent is often expressed in lofty terms though implementation can carry darker purposes.

Whilst the debate about the balance between use and misuse of identity data occurs at its most visible around national identity management and authentication systems, it is equally applicable at institutional, commercial or App level. Facebook's undisclosed release of user data to preferred advertisers, including those with political influence ambitions, has changed the international dialogue. Google's growing dominance of access to information and profiling of individuals raises similar concerns. Being able to prove individual identity is now critical for the provision of increasing numbers of services, especially financial services, but it can equally be used for unfair profiling by those same institutions to the detriment and exclusion of individuals or societies.

It is the role of governments and the relevant regulators to curate the activities of both governments and companies to ensure that identity authentication and management is not used inappropriately or discriminatorily. Regulatory oversight forms a balance that constantly shifts as political and economic circumstances evolve. The authorities need to promote acquisition and use of identity information against a balanced set of priorities for individuals' rights and protection and institutional ambitions for open markets and competitive services.

Furthermore, the critical issue of trust, in the form of agreements on how to rely on third parties' identity authentication and management systems and processes and their appropriate limits of consequential liability, requires much further development. Legislators and regulators need to consider a risk-based approach to identity authentication and management that tolerates some imperfection. They need to consider legislative and regulatory evolution toward trust frameworks which limit the liability of identity verifiers to subsequent third party users and the scope for collective liability insurance. Better legal and risk management foundations can promote federated and decentralised identity authentication and management systems that better meet the objectives of security, ease of use, and cost-effectiveness.

As has been highlighted, one critical concern with all identity management and authentication systems is the security requirements for storing individuals' identity information, especially biometric data. The unique challenge that biometric identity authentication and management data presents is that an individual cannot reset the information in the event that unauthorised access to that data is obtained. Your fingerprints, or your iris patterns, are yours for life and cannot be practically modified in the event that the data relating to them is hacked.

Encryption is the key to better protecting identity authentication and management information to safeguard critical, sensitive individuals' data while simultaneously extending the scope of systems beyond national borders. Smart Ledgers offer a solution that securely encrypts data, regulates access and amendment, and records for audit who has accessed or changed data on the record. Combined with cooperative development of standards and liability principles, Smart Ledgers would provide a powerful platform to move the global digital economy forward.

Z/Yen created a prototype for such a Smart Ledger approach in 2014 for an Australian client, but it went no further than the proof-of-concept stage. The obstacles to implementation were not technological, but rather the need for a legal and liability framework for participants, perhaps in the form of "a mutual". Appendix 2 explains IDChainZ in its current guise, with refinements since 2014, to demonstrate how a decentralised model could operate. Appendix 2 should be read in conjunction with Appendix 3 which examines the relationship between Smart Ledgers and GDPR. There are numerous proposals for identity data management on Smart Ledgers using similar distributed ledger architectures.

While future methods for identity management and authentication remain diverse and uncertain, and current methods grow ever more complicated and more vulnerable, the only certainty we can predict is change.

It seems that we all could, and should, try harder.

Bibliography

1. Bertino, Elisa; Kenji Takahashi. “Identity Management: Concepts, Technologies, and Systems”, 2011
2. Birch, David. “Digital Identity Management: Technological, Business and Social Implications”, 2016
3. Cover, Rob. “Digital Identities: Creating and Communicating the Online Self”, 2016
4. Harvard Business Review, “Blockchain Will Help Us Prove Our Identities in a Digital World”, 16 March 2017
5. Holmes, Chris, Baron Holmes of Richmond, “Distributed Ledger Technologiess for Public Good”, http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf
6. Laurent, Maryline; Bouzefrane Samia. “Digital Identity Management”, 2015
7. London School of Economics. “The Identity Project: an assessment of the UK Identity Cards Bill and its implications”, 27 June 2005
8. Mainelli, Michael. “Blockchain Could Help Us Reclaim Control of Our Personal Data”, Harvard Business Review, Harvard Business School Publishing Corporation (5 October 2017) - https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data.
9. Mainelli, Michael. “Blockchain Will Help Us Prove Our Identities In A Digital World”, Harvard Business Review, Harvard Business School Publishing Corporation (16 March 2017)
10. Singh, Simon. “The Alternative History of Public Key Cryptography.” In The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Crytography (pp.279-92), 6 October 1999
11. Sporny, Man., An Introduction to Credentials on the Web (video), YouTube.com, February 2015
12. The Economist. “Establishing Identity Is a Vital, Risky and Changing Business”, 18 December 2018
13. The Economist. “Estonia Takes the Plunge: A National Identity Scheme Goes Global.” The Economist, 28 June 2014
14. W3C. Identity Credentials 1.0, Draft Community Group Report, 5 August 2015
15. WEF Insight Report. “Digital Identity”, September 2018
16. Williams, Nick. “What is a blockchain?”, 12 April 2015
17. Williamson, Graham; Yip David; Sharoni Ilan; Kent Spaulding. “Identity Management: A Primer”, 2009

Appendix 1 – Comparison of Biometric Identity Authentication and Management Modalities

Fingerprint recognition: The advantages and disadvantages of fingerprints as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Widely recognised and accepted, used for over a century, accepted by legal community, law enforcement agencies and forensic scientists	User consent required to obtain and cannot be obtained or verified from a distance
Permanent and stable (unless the individual is subject to finger pad injury or loss of a finger) and do not change much, if at all, with age	But fingers need to be dry and clean and free from skin disease for imaging
Medium universality – most individuals do possess fingerprints	Some individuals do not have fingerprints
Relatively small footprint for scanning equipment and not subject to environmental factors when collecting (e.g. ambient light, background noise)	Intrusive – individual is required to touch the equipment in order to present a biometric sample
Limited template storage requirements for resulting data, frequently encrypted to prevent 'reverse engineering' of a fingerprint from the data, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric fingerprint data is stored unencrypted). You can reset your password, you cannot reset your fingerprints
Medium difficulty to 'spoof' requiring access to the relevant fingerprints and some specialised equipment	However, techniques for how to create fake fingerprints are easily available on the Internet. They are not hugely challenging to use[47] and can even involve only using a publicly available photograph as a source[48]
Reasonably reliable, in terms of achievable FAR and FRR (however, at least one company is claiming almost perfect (0.001) FAR / FRR scores when presented with two fingerprints[49]). Low incidence of duplicates (how unique fingerprints are is disputed)	No corresponding disadvantage, although other biometric modalities claim superior FAR / FRR rates to those generally claimed for fingerprint recognition
Relatively low cost of equipment (especially compared with other biometric scanners)	No corresponding disadvantage

[47] http://www.wikihow.com/Fake-Fingerprints

[48] http://www.popsci.com/photograph-can-help-fool-your-phones-fingerprint-sensor

[49] http://www.neurotechnology.com/megamatcher-algorithm-tests.html

Palm (finger) vein pattern recognition: The advantages and disadvantages of palm vein pattern recognition as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Newer technology based on pattern capture of palm (or finger, but the palm has a more complex vascular pattern than a finger, so provides greater reliability of identity confirmation) veins at enrolment for subsequent individual identity authentication	Lower take up than fingerprint recognition techniques. User consent required to obtain and cannot be obtained or verified from a distance
Permanent and stable (unless the individual is subject to hand injury) and do not change much, if at all, with age	No corresponding disadvantage
High universality – all individuals who possess hands have vein patterns	A limited number of individuals do not have hands
Not subject to environmental factors when collecting (e.g. ambient light, background noise) or localised issues (such as can occur with fingerprints)	Less intrusive – individual needs to place their hand near the equipment in order to present a biometric sample, but does not need to touch it
Increased template storage requirements for resulting palm vein pattern data (compared with fingerprints) and should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric palm vein pattern data is stored unencrypted). You can reset your password, you cannot reset your palm vein patterns
High degree of difficulty to 'spoof' because of the challenge of accessing the palm vein pattern information of an individual which is internal to the hand	No corresponding disadvantage
Very reliable, in terms of achievable FAR and FRR (less than 0.01% reported[50]), and palm vein patterns are unique, even to individuals who are identical twins, according to Fujitsu research[51]	No corresponding disadvantage
No corresponding advantage	Relatively high cost of scanning equipment (much more expensive than those required for fingerprint authentication) and bulkier (some integrated scanners can now handle all of fingerprint, finger vein and palm vein scanning and authentication)

[50] http://www.researchgate.net/publication/238774666_Palm_Vein_Authentication_System_A_Review

[51] http://www.bayometric.com/compare-fingerprint-recognition-and-palm-vein-technology/

Hand geometry recognition: The advantages and disadvantages of hand geometry as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Relatively simple technology based capturing a series of measurements of an individual's hand at enrolment for subsequent identity authentication	User consent required to obtain and cannot be obtained or verified from a distance
Relatively stable in many adults (unless the individual is subject to hand injury), but has some drawbacks – see corresponding disadvantage	Changes with age, so is unsuitable for use with children and may be affected later in life by long terms wearing of rings, weight loss and gain or conditions such as rheumatoid arthritis
High universality – all individuals who possess hands have hand geometry measurements	A limited number of individuals do not have hands
Not subject to environmental factors when collecting data (e.g. ambient light, background noise) and can be used in challenging environments	Moderately intrusive – individual needs to have their hand touching the equipment in order to present biometric hand geometry data
Low template storage requirements for resulting hand measurement data (compared with pam vein patterns) and should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric hand geometry data is stored unencrypted). You can reset your password, you cannot reset the dimensions of your hand
High degree of difficulty to 'spoof' as a full 3D image of an individual's hand is required	No corresponding disadvantage
No corresponding advantage	Far from the most reliable modality, in terms of achievable FAR and FRR, (reported FAR 14.6 and FRR 0.2 in tests[52]) because hand measurements are rather less unique than other biometric modalities with a noticeable percentage of duplicates in existence
Relatively low cost of hand geometry scanning equipment	Hand geometry scanning equipment is somewhat bulky

[52] http://www.radioeng.cz/fulltexts/2007/07_04_082_087.pdf

Iris scanning recognition: The advantages and disadvantages of iris scanning as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Easy to use and scalable – has been used in a number of large-scale environments for enrolment	User consent required to obtain and cannot easily be obtained or verified from a distance
Stable (unless the individual is subject to eye injury)	No equivalent disadvantage, although repeated scanning of the iris with infrared light may cause some eye damage if frequently used
High universality – all individuals who possess eyes have irises that can be scanned	A limited number of individuals are blind or lack eyes through genetics, disease or injury. A few types of contact lenses or spectacles can interfere with the pattern recognition for iris scanning
No equivalent advantage	Needs stable environmental factors – e.g. lighting. Less intrusive – individual needs only to undergo the equivalent of taking a photograph – but does need to remain still during the scan
Substantial template storage requirements for resulting iris scan data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric iris scan data is stored unencrypted). You can reset your password, you cannot reset your iris patterns
Claimed to be difficult to 'spoof', but see corresponding disadvantage where one commonly available scanner was deceived	The Samsung Galaxy S8 iris scanner has been fooled by a colour photograph[53]
Very reliable modality, in terms of achievable FAR and FRR, (reported FAR 0.2 and FRR 0.0001 in tests[54])	No corresponding disadvantage
No corresponding advantage	Relatively high cost of iris scanning equipment (c.5x the cost of fingerprint scanners)

[53] http://www.bleepingcomputer.com/news/security/samsung-galaxy-s8-iris-scanner-fooled-by-a-photo/

[54] http://ieeexplore.ieee.org/abstract/document/6224358

Retinal scanning recognition: The advantages and disadvantages of retinal scanning as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
No corresponding advantage	User consent required to scan an individual's retina and data must be obtained or verified with the individual being a very short distance from the scanner on enrolment and subsequent verification
Stable (unless the individual is subject to eye retinal injury, or disease – such as cataracts, glaucoma, high blood pressure, cardiac disease and a number of other conditions) over an individual's lifetime	Cataracts, glaucoma, high blood pressure and cardiac disease are not uncommon, all of which will affect blood vessels in the retina
High universality – all individuals who possess eyes have retinas that can be scanned	A limited number of individuals are blind or lack eyes through genetics, disease or injury
Since the retina is located within the eye, retinal scanning is not subject to external environmental factors	Intrusive – individual needs to be very close to the retinal scanner. There is substantial resistance by the public to the act of placing one's eye in a receptacle where an infrared light is shone into it (possibly repeatedly, as getting an accurate scan can be challenging)
Limited template storage requirements for resulting retinal scan data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric retinal scan data is stored unencrypted). You can reset your password, you cannot reset the blood vessel patterns in your retina
Virtually impossible to 'spoof' because of the challenge of accessing the retinal blood vessel pattern information of an individual which is internal to the eye	No corresponding disadvantage
Very reliable modality, in terms of achievable FAR and FRR – almost 0	No corresponding disadvantage
No corresponding advantage	High cost of retinal scanning equipment – equivalent cost to iris scanners

Eye vein scanning recognition: The advantages and disadvantages of eye vein scanning as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
No corresponding advantage	User consent required to obtain on enrolment and data cannot easily be obtained or verified from a distance
Stable (unless the individual is subject to eye injury)	No equivalent disadvantage
High universality – all individuals who possess eyes have corresponding sclerae that can be scanned	A limited number of individuals are blind or lack eyes through genetics, disease or injury
Eye vein scanning will work with contact lenses and spectacles	Moderately intrusive – the scanner needs to be held close to an individual's eye
Substantial template storage requirements for resulting eye vein scan data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric eye vein scan data is stored unencrypted). You can reset your password, you cannot reset your eye vein patterns
Supposedly difficulty to 'spoof', but eye vein scanning is a recent technology (invented in 2008), so this could change	No corresponding disadvantage – unknown at this time whether an eye vein scanner can be spoofed using colour photographs
Claimed to be a reliable modality, in terms of achievable FAR and FRR, but published data is scarce	No corresponding disadvantage
Relatively low cost of eye vein scanning equipment (can use a mobile 'phone to collect eye vein image data)	No corresponding disadvantage

Facial recognition (3D): The advantages and disadvantages of facial recognition as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Facial recognition can be done passively without any action or participation on the part of an individual since facial images can be acquired from a distance	No equivalent disadvantage
Medium permanence and stability (see disadvantage)	Faces change with age (especially in children and young people)
High universality as practically everyone has a face	Faces are not especially unique – unrelated people can look very like each other and there are relatively significant numbers of identical twins
Facial recognition will usually work with contact lenses and spectacles being worn. Relatively unobtrusive – the scanner does not need to be held close to an individual's face – e.g. immigration / passport facial scanners	No equivalent disadvantage
Substantial template storage requirements for resulting facial recognition data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric facial recognition data is stored unencrypted). You can reset your password, you cannot easily reset your facial appearance
Difficult to 'spoof' where 3D facial recognition scanning is deployed (whatever the Mission Impossible film series wants us to believe about the effectiveness of latex masks)	Relatively easy to 'spoof' 2D facial recognition scanning by using colour photographs or masks (some facial recognition software now includes detecting whether individuals blink to defeat these techniques)
No corresponding advantage	Moderately reliable – FAR / FRR rates quoted for facial recognition in controlled environments are in the range of 1.5 – 3.0 (although recent reports of research by Cardiff University into South Wales Police's use of facial recognition software cited an accuracy of only 76% for accurate recognition, with 68% of images being of insufficient quality to use by the facial recognition software deployed[55]. It is also now (December 2018), being trialled by the Metropolitan Police in London)
Relatively low cost of facial recognition scanning equipment	No corresponding disadvantage

[55] http://www.cardiff.ac.uk/news/view/1383278-evaluating-the-use-of-automated-facial-recognition-technology-in-major-policing-operations

Voice recognition: The advantages and disadvantages of voice recognition as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Not overly intrusive. Voice recognition can be done without an individual having to get too close to a microphone on enrolment and subsequent verification	The voice recognition software has to be trained to recognise an individual's voice by reading 'training' passages of text to enable the software to establish the voice print
Medium permanence and stability (see corresponding disadvantage)	Voices change with age (especially in children and young people) and can be subject to certain common illnesses, such as a cold, which alter an individual's voice
Medium-high universality as most people can speak	No equivalent disadvantage, except for individuals who are mute
No corresponding advantage	Voice recognition requires an environment with little or no ambient background noise to obtain quality results
Substantial template storage requirements for resulting voice recognition data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric voice recognition data is stored unencrypted). You can reset your password, you cannot reset the way you speak
No corresponding advantage	Relatively easy to 'spoof' with a voice recording – there is evidence in the US of fraudsters making spam calls and trying to get bank customers to say 'yes' which they record then to incur fraudulent credit card or utility charges, or to 'prove' that a victim owes them money for services never ordered[56]
No corresponding advantage	Relatively unreliable – FAR / FRR rates quoted for voice recognition (where FAR and FRR are the same value – and therefore represent the optimum performance tuning between the two undesirable outcomes) is reported to be in the region of 10.0[57]
Low cost for a microphone and relatively low cost for voice recognition software	No corresponding disadvantage

[56] https://www.csoonline.com/article/3196820/security/vocal-theft-on-the-horizon.html

[57] https://www.researchgate.net/figure/FAR-FRR-plots-of-speaker-identification-with-the-use-of-vector-quantization-VQ_fig4_267970188

Dynamic signature recognition: The advantages and disadvantages of dynamic signature recognition as an identity management and authentication modality can be summed up as:

Advantages	Disadvantages
Not intrusive in that all that is required is an individual to sign their name using a pen and a special writing tablet on enrolment and subsequent verification	No equivalent disadvantage
Low permanence and stability (see disadvantage)	Signatures can change with age and some individuals can change their signatures very rapidly. Some individuals cannot sign their name. It is mostly used for verification (e.g. for a transaction) rather than for identity management and authentication
Medium universality as confined to those individuals who can write	Many individuals around the world are illiterate and therefore cannot sign their name
Environmental factors are unimportant as long as a signature can be made on the equipment	No equivalent disadvantage
Low volume template storage requirements for resulting signature recognition data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric signature recognition data is stored unencrypted)
Relatively easy to 'spoof' on appearance alone	Very hard to spoof in terms of dynamic signature recognition
No corresponding advantage	Relatively unreliable – FAR / FRR rates quoted for signature recognition at 2.0 or greater, because of variances in legitimate signatures (e.g. a signature made by an individual standing up, will have different dynamic signature recognition features when made by the same individual sitting down)
Low cost for signature recognition equipment and software	No corresponding disadvantage

DNA recognition: The advantages and disadvantages DNA fingerprinting as an identity management and authentication modality can be summed up as:

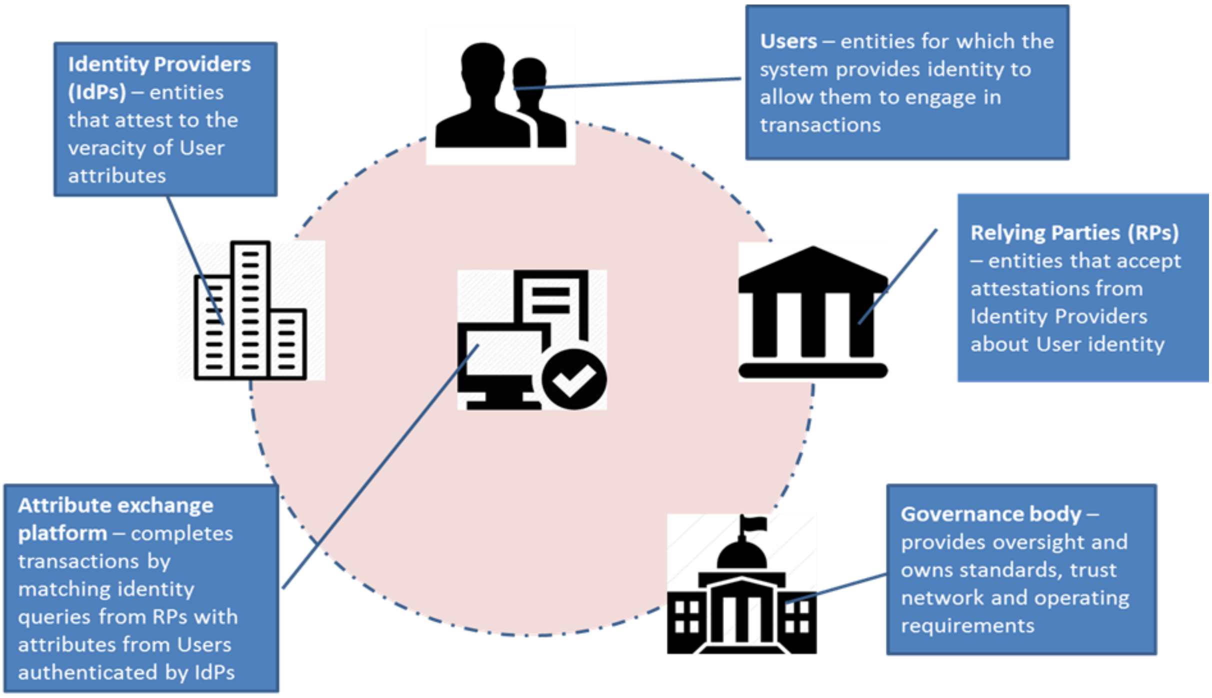
Advantages	Disadvantages
No equivalent advantage	Seen as highly intrusive on both enrolment and subsequent verification. Usually taken through a swab, with multiple samples needing to be provided to ensure reliability of results. Customarily, laboratories conduct two tests on four samples to seek to eliminate errors
Permanent and stable – an individual's DNA does not change	No equivalent disadvantage
Universal	No equivalent disadvantage
No equivalent advantage	Highly sensitive to contamination of samples or testing error (hence the use of repeat tests). Requires specialist equipment and personnel, so exceptionally unlikely to be useful as an on-the-spot identity authentication and management modality
High volume template storage requirements for resulting DNA fingerprinting data which should be encrypted, although the presence of a central database of biometric information will always be a potential 'honey pot' to attract unauthorised attempts at accessing	In common with all biometric methods, gives individuals a significant identity management and authentication challenge if their biometric data is obtained by unauthorised methods (which risk is increased if the biometric DNA fingerprint data is stored unencrypted). You can change your password, you cannot change your DNA fingerprint
Impossible to 'spoof'	No equivalent disadvantage
Highly reliable – FAR / FRR rates quoted for DNA fingerprinting at 0.5	However, the process of obtaining and analysing DNA fingerprints is highly complex and DNA samples can easily be contaminated
No corresponding advantage	Very high cost of DNA fingerprint analysis equipment together with specialist personnel required and several days needed to produce results

Appendix 2 – IDChainZ Smart Ledger Prototype for Identity Management and Authentication

IDChainZ was created as a prototype Smart Ledger application to demonstrate the practicality of Smart Ledger implementations for identity management and authentication. One design choice was that the individual or entity (the subject) should control access to, and maintain control of, their identity data (Self-Sovereign Identity or SSI), but other choices could have been made for permissioned control, tiered control, or even central governance.

The prototype was developed from 2014 to 2018, beginning with an insurance company for anti-money laundering and know-your-customer strategic thinking. IDChainZ modelled the participants in a network for identity management and authentication as:

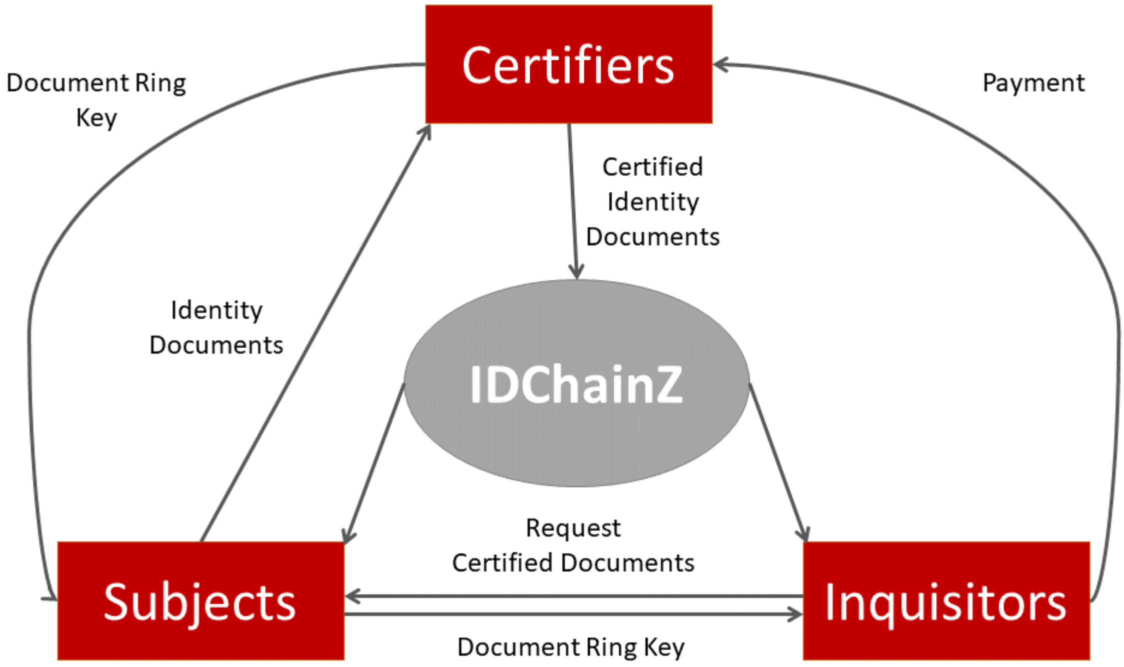
- Users – individuals or entities for whom the identity management and authentication system provides proof of identity information;
- Identity Providers – which are entities that attest to the accuracy and reliability of an individual's or an entity's identity information;
- Relying Parties – which require access to identity information and accept its veracity, based upon user identity authentication by Identity Providers;
- Attribute Exchange Platform – which is the system (in this case IDChainZ) which enrols and stores identity information and matches requests for identity information with that data, based upon user access permissions;
- Governance Body – that curates the system, provides regulatory oversight, maintains the associated trust network, and manages standards and other operating requirements.


Identity Providers (IdPs) – entities that attest to the veracity of User attributes
Users – entities for which the system provides identity to allow them to engage in transactions
Relying Parties (RPs) – entities that accept attestations from Identity Providers about User identity
Attribute exchange platform – completes transactions by matching identity queries from RPs with attributes from Users authenticated by IdPs
Governance body – provides oversight and owns standards, trust network and operating requirements

Specifically, for IDChainZ, the proof of concept prototype is envisaged to operate as follows:

1. Users provide identity documents for authentication to Identity Provider(s) to prove their identity;
2. The Identity Provider(s) validate(s) the user's identity documents, by establishing their authenticity, matching them with and confirming official records (such as birth certificates or passports or company registrations), and accessing third party bureaux for infoirmation (e.g. Equifax, Experian, WorldCheck);
3. The Identity Provider loads the certified identity documents, together with a digital signature confirming authenticity, onto IDChainZ and geenerates a master document ring key;
4. The Identity Provider then issues the master document ring key to the User which controls access to the certified identity documents. The master ring key is unique, secure and irreplaceable. If a User mislays their master document ring key, then the certified identity documents are locked away forever and the User will have to go through the processof resubmitting identity documents to the Identity Provider to repeat the authentication and certification process;
5. Relying Parties (or, potentially, Users) pay the Identity Provider(s) for their services, in return for being able to access the authenticated information;

6. A User wishes to do business with a Relying Party, which must authenticate the User's identity for Know Your Client (KYC) and Anti Money Laundering (AML) purposes. The User grants permisison (which can be limited by time, information shared, number of accesses, be granted temporarliy or permanently) to the Relying Party to access their certified identity data by providing a specific document ring key which includes the limits to the permission granted;
7. The Relying Party accesses the User's certified identity documents, confirms their identity, and satisfies itself that the User is not sanctioned for trading under the organisation's KYC and AML policies.



The KYC and AML identity confirrmation process within the Relying Party is shown in more detail below, where the **business process** uses IDChainZ as the technology **attribute management infrastructure** to access **underlying data** which confirms identity.

CDD/KYC/AML Architecture	Components	Perrformed By
Financial Institution Specific CDD/KYC/AML Business Process	• Sanctions Lists • PEP Criteria • Risk Weightings • Joint Money Laundering Steering Group Guidance	• Relationship Managers • Branch Staff • CDD/KYC/AML Team • Compliance/Regulatory
Identity Attribute Management Infrastructure	IDChainZ	Market Utility • Works for current CDD/KYC/AML model and future-proofed • Scalable
Underlying Data	• Proof of identity (e.g. passport) • External credit references (e.g. Experian, Worldcheck) • Evidence of existing debts (e.g. Equifax)	• Buy side customer • Various external agencies

The detailed work steps to complete the flow consist of, first, the User providing identity documentation to the Identity Provider for validation and authentication would consist of:

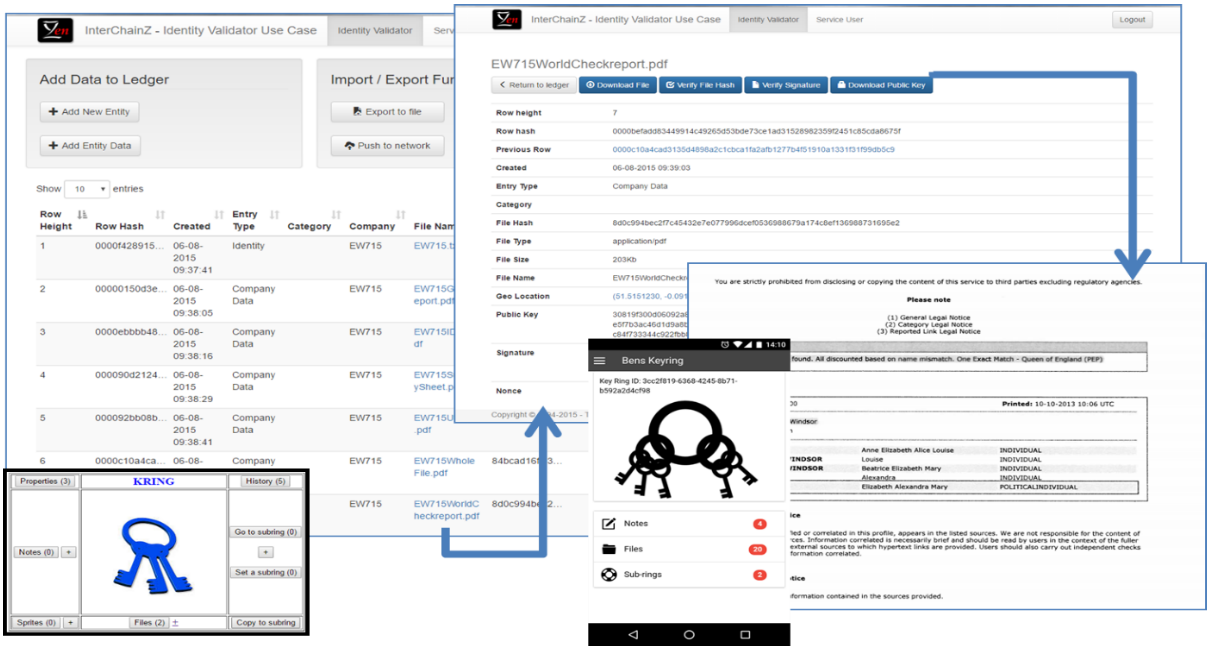
User
Identity Provider

User provides Identity Provider (IdP) with Identity documentation (e.g. Passport etc.)

Identity Provider
IDchainZ

1) IdP creates a IDchainZ master ring for User
2) IdP creates an Identity sub-ring
3) IdP encrypts certified documents and background checks with their private key
4) IdP adds encrypted certified documents and background checks to the User's Identity sub-ring
5) IdP publishes public key and also adds it to the Identity sub-ring

The Identity Provider would then generate the Master Ring to store the encrypted, certified identity documents, together with the results of third party validation checks and any other relevant documents:



InterChainZ - Identity Validator Use Case

Add Data to Ledger

Import / Export Fun

Show 10 entries

Row Height	Row Hash	Created	Entry Type	Category	Company	File Nam
1	0000f428915…	06-08-2015 09:37:41	Identity		EW715	EW715.t
2	00000150d3e…	06-08-2015 09:38:05	Company Data		EW715	EW715G eport.pdf
3	0000ebbbb48…	06-08-2015 09:38:16	Company Data		EW715	EW715ID df
4	000090d2124…	06-08-2015 09:38:29	Company Data		EW715	EW715S ySheet.p
5	000092bb08b…	06-08-2015 09:38:41	Company Data		EW715	EW715U .pdf
6	0000c10a4ca…	06-08-	Company		EW715	EW715Whole File.pdf
					EW715	EW715WorldC heckreport.pdf

InterChainZ - Identity Validator Use Case

EW715WorldCheckreport.pdf

Row height	7
Row hash	0000befadd83449914c49265d53bde73ce1ad31528982359f2451c85cda8675f
Previous Row	0000c10a4cad3135d4898a2c1cbca1fa2afb1277b4f51910a1331f31f99db5c9
Created	06-08-2015 09:39:03
Entry Type	Company Data
Category	
File Hash	8d0c994bec2f7c45432e7e077996dcef0536988679a174c8ef136988731695e2
File Type	application/pdf
File Size	203Kb
File Name	EW715WorldCheckr
Geo Location	(51.5151230, -0.091
Public Key	30819f300d06092a8 e5f7b3ac46d1d9a8b c84f733344c922fbb
Signature	
Nonce	

Copyright © 4-2015 - 1

You are strictly prohibited from disclosing or copying the content of this service to third parties excluding regulatory agencies.

Please note

(1) General Legal Notice
(2) Category Legal Notice
(3) Reported Link Legal Notice

found. All discounted based on name mismatch. One Exact Match - Queen of England (PEP)

Printed: 10-10-2013 10:06 UTC

Windsor

	Anne Elizabeth Alice Louise	INDIVIDUAL
INDSOR	Louise	INDIVIDUAL
INDSOR	Beatrice Elizabeth Mary	INDIVIDUAL
	Alexandra	INDIVIDUAL
	Elizabeth Alexandra Mary	POLITICALINDIVIDUAL

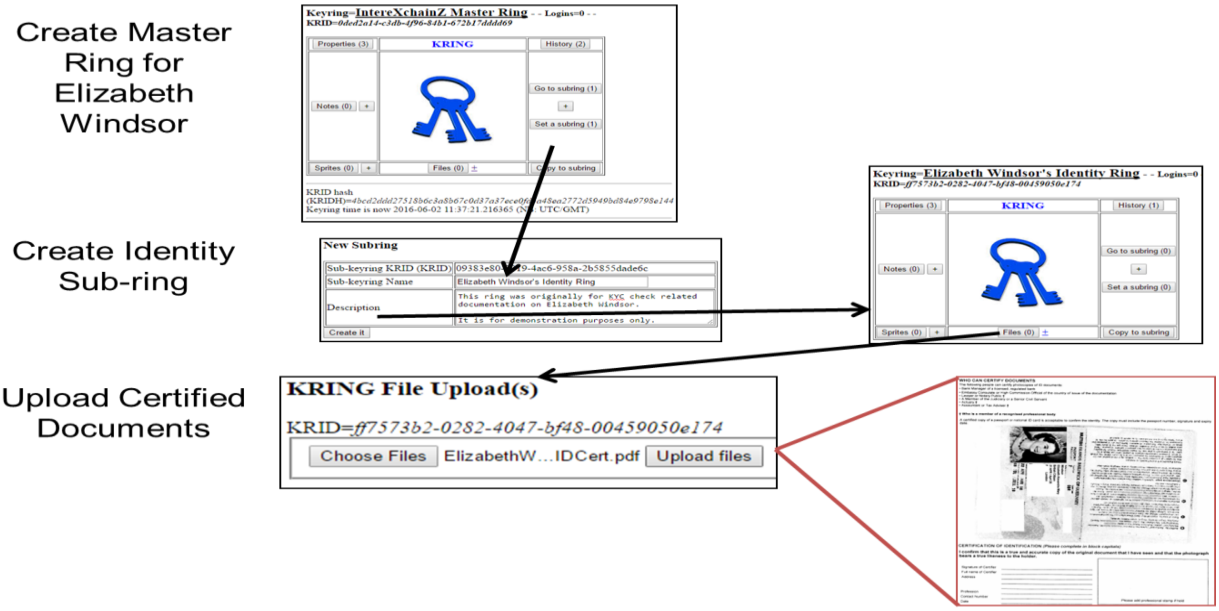
ied or correlated in this profile, appears in the listed sources. We are not responsible for the content of ces. Information correlated is necessarily brief and should be read by users in the context of the fuller external sources to which hypertext links are provided. Users should also carry out independent checks formation correlated.

formation contained in the sources provided.

Bens Keyring

Key Ring ID: 3cc2f819-6368-4245-8b71-b592a2d4cf98

Once the Master Ring has been created, then Sub Rings could be established for each of Identity, Health, Education etc. and the certified documents could be loaded onto the relevant Sub Ring:



Create Master Ring for Elizabeth Windsor

Keyring=InterXchainZ Master Ring - - Logins=0 - -
KRID=0ded2a14-c3db-4f96-84b1-672b17dddd69

KRID hash (KRIDH)=4bcd2ddd27518b6c3a8b67c0d37a37ece0f a48ea2772d5949bd84e9798e144
Keyring time is now 2016-06-02 11:37:21.216365 (N : UTC/GMT)

Create Identity Sub-ring

New Subring

Sub-keyring KRID (KRID)	09383e80 9-4ac6-958a-2b5855dade6c
Sub-keyring Name	Elizabeth Windsor's Identity Ring
Description	This ring was originally for KYC check related documentation on Elizabeth Windsor. It is for demonstration purposes only.

Keyring=Elizabeth Windsor's Identity Ring - - Logins=0
KRID=ff7573b2-0282-4047-bf48-00459050e174

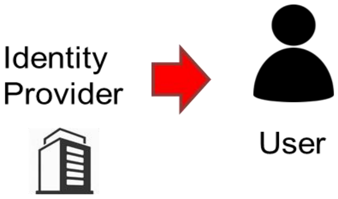
Upload Certified Documents

KRING File Upload(s)

KRID=ff7573b2-0282-4047-bf48-00459050e174

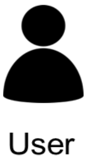
WHO CAN CERTIFY DOCUMENTS

The Identity Provider then woulld pass control of the Master Ring, and Sub Ring(s) created to the User:

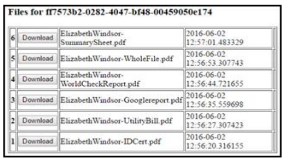


1) IdP gives User the key to their master ring
2) IdP destroys their copies of the key and the underlying documents

Master Ring Key:
280d98e3-361f-491b-8631-5c19e942d6d1
Access:
1) by App
2) or https://185.77.66.18:3000/api



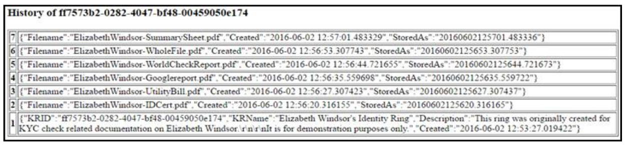
User uses master ring key to view the certified files and monitor activity on the ring



Files for ff7573b2-0282-4047-bf48-00459050e174

6	Download	ElizabethWindsor-SummarySheet.pdf	2016-06-02 12:57:01.483329
5	Download	ElizabethWindsor-WholeFile.pdf	2016-06-02 12:56:53.307743
4	Download	ElizabethWindsor-WorldCheckReport.pdf	2016-06-02 12:56:44.721655
3	Download	ElizabethWindsor-Googlereport.pdf	2016-06-02 12:56:35.559698
2	Download	ElizabethWindsor-UtilityBill.pdf	2016-06-02 12:56:27.307423
1	Download	ElizabethWindsor-IDCert.pdf	2016-06-02 12:56:20.316155

View Files



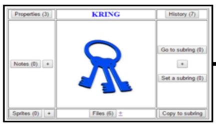
History of ff7573b2-0282-4047-bf48-00459050e174

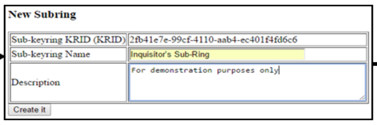
7	{"Filename":"ElizabethWindsor-SummarySheet.pdf","Created":"2016-06-02 12:57:01.483329","StoredAs":"20160602125701.483336"}
6	{"Filename":"ElizabethWindsor-WholeFile.pdf","Created":"2016-06-02 12:56:53.307743","StoredAs":"20160602125653.307753"}
5	{"Filename":"ElizabethWindsor-WorldCheckReport.pdf","Created":"2016-06-02 12:56:44.721655","StoredAs":"20160602125644.721673"}
4	{"Filename":"ElizabethWindsor-Googlereport.pdf","Created":"2016-06-02 12:56:35.559698","StoredAs":"20160602125635.559722"}
3	{"Filename":"ElizabethWindsor-UtilityBill.pdf","Created":"2016-06-02 12:56:27.307423","StoredAs":"20160602125627.307437"}
2	{"Filename":"ElizabethWindsor-IDCert.pdf","Created":"2016-06-02 12:56:20.316155","StoredAs":"20160602125620.316165"}
1	{"KRID":"ff7573b2-0282-4047-bf48-00459050e174","KRName":"Elizabeth Windsor's Identity Ring","Description":"This ring was originally created for KYC check related documentation on Elizabeth Windsor.\r\n\r\nIt is for demonstration purposes only.","Created":"2016-06-02 12:53:27.019422"}

View Ring History

When a Relying Party wants to access a User's Identiity information, the User would create a new Sub Ring specifically for that Relying Party to access, including the permissions which constrain the Relying Party's ability to read the Identity information:

1) User saves selected Identity ring files onto a new sub-ring for the Relying Party

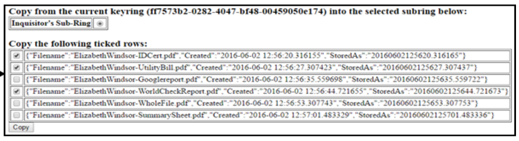




New Subring

Sub-keyring KRID (KRID)	2fb41e7e-99cf-4110-aab4-ec401f4fd6c6
Sub-keyring Name	Inquisitor's Sub-Ring
Description	For demonstration purposes only

Create it



Copy from the current keyring (ff7573b2-0282-4047-bf48-00459050e174) into the selected subring below:

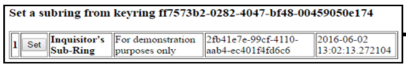
Inquisitor's Sub-Ring

Copy the following ticked rows:

☑	{"Filename":"ElizabethWindsor-IDCert.pdf","Created":"2016-06-02 12:56:20.316155","StoredAs":"20160602125620.316165"}
☑	{"Filename":"ElizabethWindsor-UtilityBill.pdf","Created":"2016-06-02 12:56:27.307423","StoredAs":"20160602125627.307437"}
□	{"Filename":"ElizabethWindsor-Googlereport.pdf","Created":"2016-06-02 12:56:35.559698","StoredAs":"20160602125635.559722"}
☑	{"Filename":"ElizabethWindsor-WorldCheckReport.pdf","Created":"2016-06-02 12:56:44.721655","StoredAs":"20160602125644.721673"}
□	{"Filename":"ElizabethWindsor-WholeFile.pdf","Created":"2016-06-02 12:56:53.307743","StoredAs":"20160602125653.307753"}
□	{"Filename":"ElizabethWindsor-SummarySheet.pdf","Created":"2016-06-02 12:57:01.483329","StoredAs":"20160602125701.483336"}

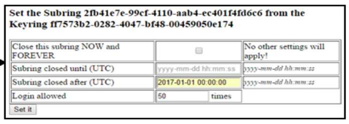
Copy

2) User sets time and use limits on the Relying Party's ring



Set a subring from keyring ff7573b2-0282-4047-bf48-00459050e174

1	Set	**Inquisitor's Sub-Ring**	For demonstration purposes only	2fb41e7e-99cf-4110-aab4-ec401f4fd6c6	2016-06-02 13:02:13.272104



Set the Subring 2fb41e7e-99cf-4110-aab4-ec401f4fd6c6 from the Keyring ff7573b2-0282-4047-bf48-00459050e174

Close this subring NOW and FOREVER	□	No other settings will apply!
Subring closed until (UTC)	yyyy-mm-dd hh:mm:ss	*yyyy-mm-dd hh:mm:ss*
Subring closed after (UTC)	2017-01-01 00:00:00	*yyyy-mm-dd hh:mm:ss*
Login allowed	50 times	

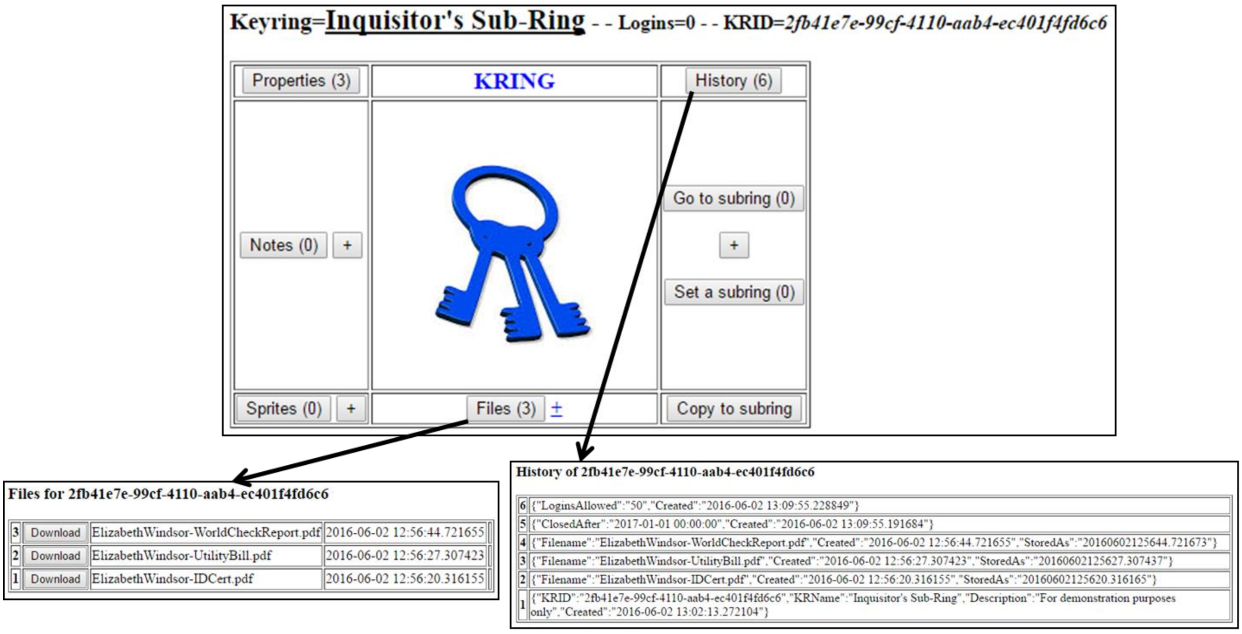
Set it

3) User sends the Relying Party the key for this limited access ring

Inquisitor's Ring Key:
2fb41e7e-99cf-4110-aab4-ec401f4fd6c6
Access:
1) by App
2) or https://185.77.66.18:3000/api

The Relying Party could then access the User's Identity information, subject to the constraints tthat the User has set for that access:

- ♦ Relying Party can only see the contents of the Relying Party's ring and its time and use limits



Keyring=Inquisitor's Sub-Ring - - Logins=0 - - KRID=2fb41e7e-99cf-4110-aab4-ec401f4fd6c6

Files for 2fb41e7e-99cf-4110-aab4-ec401f4fd6c6

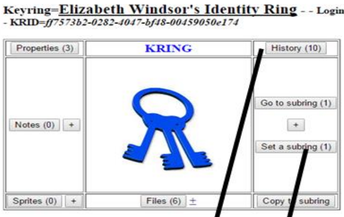
3	Download	ElizabethWindsor-WorldCheckReport.pdf	2016-06-02 12:56:44.721655
2	Download	ElizabethWindsor-UtilityBill.pdf	2016-06-02 12:56:27.307423
1	Download	ElizabethWindsor-IDCert.pdf	2016-06-02 12:56:20.316155

History of 2fb41e7e-99cf-4110-aab4-ec401f4fd6c6

6	{"LoginsAllowed":"50","Created":"2016-06-02 13:09:55.228849"}
5	{"ClosedAfter":"2017-01-01 00:00:00","Created":"2016-06-02 13:09:55.191684"}
4	{"Filename":"ElizabethWindsor-WorldCheckReport.pdf","Created":"2016-06-02 12:56:44.721655","StoredAs":"20160602125644.721673"}
3	{"Filename":"ElizabethWindsor-UtilityBill.pdf","Created":"2016-06-02 12:56:27.307423","StoredAs":"20160602125627.307437"}
2	{"Filename":"ElizabethWindsor-IDCert.pdf","Created":"2016-06-02 12:56:20.316155","StoredAs":"20160602125620.316165"}
1	{"KRID":"2fb41e7e-99cf-4110-aab4-ec401f4fd6c6","KRName":"Inquisitor's Sub-Ring","Description":"For demonstration purposes only","Created":"2016-06-02 13:02:13.272104"}

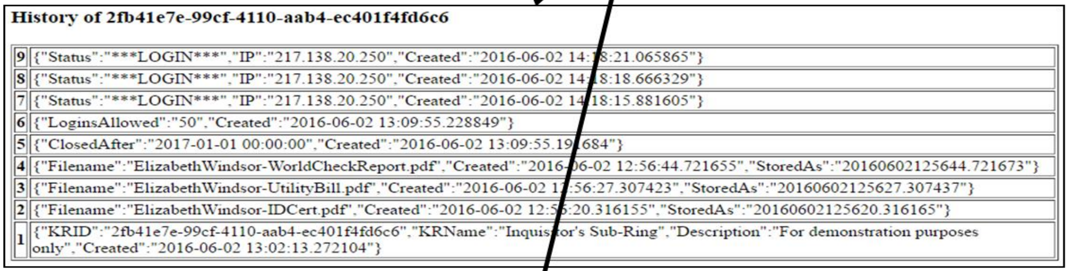
Identity Documents **Time & Use Limits**

The User would then be able both to monitor and control the access to Identity documents by the Relying Party. The User could revoke the Relying Party's access rights at any time:



Keyring=Elizabeth Windsor's Identity Ring - - Logins=0 - KRID=ff7573b2-0282-4047-bf48-00459050e174

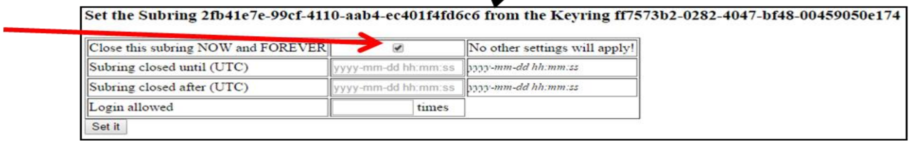
- ♦ User can monitor access to the ring by the Relying Party



History of 2fb41e7e-99cf-4110-aab4-ec401f4fd6c6

9	{"Status":"***LOGIN***","IP":"217.138.20.250","Created":"2016-06-02 14:18:21.065865"}
8	{"Status":"***LOGIN***","IP":"217.138.20.250","Created":"2016-06-02 14:18:18.666329"}
7	{"Status":"***LOGIN***","IP":"217.138.20.250","Created":"2016-06-02 14:18:15.881605"}
6	{"LoginsAllowed":"50","Created":"2016-06-02 13:09:55.228849"}
5	{"ClosedAfter":"2017-01-01 00:00:00","Created":"2016-06-02 13:09:55.191684"}
4	{"Filename":"ElizabethWindsor-WorldCheckReport.pdf","Created":"2016-06-02 12:56:44.721655","StoredAs":"20160602125644.721673"}
3	{"Filename":"ElizabethWindsor-UtilityBill.pdf","Created":"2016-06-02 12:56:27.307423","StoredAs":"20160602125627.307437"}
2	{"Filename":"ElizabethWindsor-IDCert.pdf","Created":"2016-06-02 12:56:20.316155","StoredAs":"20160602125620.316165"}
1	{"KRID":"2fb41e7e-99cf-4110-aab4-ec401f4fd6c6","KRName":"Inquisitor's Sub-Ring","Description":"For demonstration purposes only","Created":"2016-06-02 13:02:13.272104"}

- ♦ User can revoke the Relying Party's ring



Set the Subring 2fb41e7e-99cf-4110-aab4-ec401f4fd6c6 from the Keyring ff7573b2-0282-4047-bf48-00459050e174

Close this subring NOW and FOREVER	☑	No other settings will apply!
Subring closed until (UTC)	yyyy-mm-dd hh:mm:ss	yyyy-mm-dd hh:mm:ss
Subring closed after (UTC)	yyyy-mm-dd hh:mm:ss	yyyy-mm-dd hh:mm:ss
Login allowed	times	

Set it

The entire identity management and authentication process would be managed seamlessly through the IDChainZ Smart Ledger blockchain platform, which supports the end-to-end identity process, the roles described above, and the transactions required for full lifecycle support. The IDChainZ platform would be based on a very fast blockchain (homologated in excess of 10,000 transactions / second) and currently very cheap to use (1p in GBP for each read or write access). IDChainZ is an example of what could be achieved to support a widely available (it would be entirely accessed through an internet browser), low cost of use, ubiquitous identity management and authentication platform.

Appendix 3 - Smart Ledgers & GDPR

At the same time that Smart Ledgers and distributed ledger technology generally have been gathering public attention, the EU has been transitioning to a new data protection framework under GDPR, which aims to update EU data protection laws to address new technologies. GDPR was adopted in 2016 and took effect on May 25, 2018, and because distributed ledger technology has been advancing so rapidly, the drafters of GDPR were unable to take this technology into account.[58] The result is a potential disconnect between GDPR framework and Smart Ledgers.

Although such issues require careful analysis, there seem to be clear ways through the challenges for Smart Ledgers. In this appendix, we address four principal GDPR challenges that have been identified for distributed ledgers:

- the **permanent availability** of data on distributed ledgers to all who have access to the ledger;
- the **widespread and ongoing processing of ledger data**;
- the potential difficulty of **identifying data controllers** (*i.e.*, persons or entities responsible for data processing under GDPR) **and data processors** (*i.e.*, persons or entities that process data on behalf of a data controller) in the context of a distributed ledger; and
- the potential use of distributed ledgers for **automated decision-making**.

The first two issues are particular challenges for distributed ledgers and relate directly to the use of an immutable, distributed ledger. The latter two issues apply in a variety of data protection contexts but present some specific issues for distributed ledgers. We consider each of the four issues in turn below.

1. Data Permanence

The most frequently identified tension between GDPR and distributed ledger technology involves the inherent immutability of distributed ledgers. Immutability is a key feature of distributed ledgers, enhancing their security and allowing them to provide a permanent, verifiable, public record of transactions.

[58] *See, e.g.,* Blockchain Bundesverband (the German Blockchain Association), “Blockchain, data protection, and the GDPR”, p. 2 (25 May 2018), (“GDPR was created before Blockchain and is already outdated, since it doesn't account for decentralized technologies.”), http://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf

However, this immutability presents a potential for conflict with GDPR principles, especially:

- the **storage limitation principle** under GDPR Art 5(1)(e) that "personal data shall be … kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"; and
- the **right to erasure** (also known as the 'right to be forgotten') under GDPR Art 17, which provides an obligation on data controllers to erase data under specified circumstances.

As noted above, the main reason for the tension between these principles and distributed ledger immutability appears to be, simply, that the authors of GDPR did not anticipate distributed ledgers at the time that GDPR was adopted. But this does not mean that GDPR prevents or seriously impedes the deployment of these technologies, for two main reasons.

First, neither of the above principles is absolute. The storage limitation principle only restricts ongoing storage for "longer than is necessary for the purposes for which the personal data are processed". Since immutability is a fundamental feature of distributed ledgers, it follows that with adequate advance notice of these functions users of the technology can be considered to have accepted that use inherently involves permanent storage and that this is "necessary for the purposes for which the personal data are processed".

Likewise, the right to erasure applies only in specified circumstances – most importantly where (a) the "personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed", (b) the data subject has withdrawn consent (if processing is based upon consent) or (c) the data controller processes personal data based on its "legitimate interests" without adequate justification.[59] Where permanent storage is *required*, as in the case of distributed ledgers, there are likely to be relatively few circumstances in which these bases for erasure would be applicable. Among other things, processing in the distributed ledger context is frequently justifiable as necessary to perform a contract with the user[60] (in which case withdrawal of consent is likely to be irrelevant).

[59] GDPR Art. 17(1)(a)-(c). The other circumstances giving rise to a right of erasure involve unlawful processing, legal requirements for deletion and data regarding children. GDPR Art. 17(1)(d)-(f).
[60] GDPR Art. 6(1)(b).

Second, it is possible to design a distributed ledger to allow for the effective erasure of personal data, by storing that data off the ledger itself, or alternatively on the ledger in encrypted form that can only be decrypted by the holder of a private key. These approaches allow the data in question to be 'erased' by (a) deleting pointers to off-ledger data and/or (b) deleting private keys used for storing data either on-ledger or off-ledger (this latter options requires private keys to be assigned in a sufficiently granular fashion – *e.g.*, for particular data items or sets of data).[61] Indeed, some data protection authorities have already concluded that irreversible encryption constitutes erasure,[62] and both of these methods can involve irreversible encryption (the latter always does, and the former does if off-ledger data is encrypted).

2. Widespread and Ongoing Processing of Ledgers

Although distributed ledgers have been used for decades,[63] their recent explosive growth was initially driven by the Bitcoin protocol, which allows trust-free transaction verification through a proof of work consensus protocol.[64] This protocol requires every node of the Bitcoin network that wishes to engage in 'mining' of new bitcoins to repeatedly process new blocks of transactions (each time with a different 'nonce', or padding data) using a hash algorithm, until the calculated hash is below a certain value. Some have argued that this repeated processing – to the extent the processed blocks include personal data – conflict with GDPR principles, especially:

- the **data minimisation principle** under GDPR Art 5(1)(c) that "personal data shall be … limited to what is necessary in relation to the purposes for which they are processed"; and
- the **right to restriction of processing** under GDPR Art. 18 and the **right to object to processing** under GDPR Art. 21, which require data controllers to terminate or restrict the processing of personal data upon request in certain circumstances.

[61] Andries Van Humbeeck, "The Blockchain-GDPR Paradox", wearetheledger blog, *Medium* (21 November 2017), http://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

[62] *See* Hogan Lovells, "A guide to blockchain and data protection", p. 15 (September 2017), http://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

[63] See Arvind Narayanan & Jeremy Clark, "Bitcoin's Academic Pedigree", ACM Queue (29 August 2017), http://queue.acm.org/detail.cfm?id=3136559 ("Bitcoin's ledger data structure is borrowed, with minimal modifications, from a series of papers by Stuart Haber and Scott Stornetta written between 1990 and 1997 (their 1991 paper had another co-author, Dave Bayer).").

[64] *See* Bitcoin Wiki, "Proof of work", http://en.bitcoin.it/wiki/Proof_of_work

The conflict between these provisions and distributed ledgers is less obvious than with respect to data permanence. Furthermore, similar to the case of data permanence, there are two main bases for addressing any legal concerns.

First, the principles themselves are subject to significant limitations. With respect to the data minimisation principle, there is a good argument that multiple hashing of personal data does not mean that such data are not "limited to what is necessary in relation to the purposes for which they are processed". That is, multiple hashing does not increase the *amount of personal data* that is processed – which is the core focus of the data minimisation principle – but rather relates to the *number of times* that the data are processed.

Likewise, the right to restriction of processing and right to object to processing apply only in specified circumstances, which are narrower than those triggering the right to erasure, *i.e.*, where (a) there is a challenge to processing based upon "legitimate interests" (as for the right to erasure), (b) there is a challenge to accuracy of personal data, (c) processing is unlawful, (d) the data controller no longer needs the data but the data subject (*i.e.*, the individual to whom the data relate) wishes the data to be retained for reasons related to legal claims, or (e) the processing involves use of profiling for direct marketing.[65] On a distributed ledger, there may be no way to entirely stop processing of the ledger in any of these circumstances; however, it is entirely possible to design distributed ledger solutions so that any personal data is encrypted and cannot be processed in a manner that discloses the data in these circumstances.

Second, not all distributed ledger protocols are created equal. For example, many newer distributed ledger protocols include consensus protocols that undertake significantly less frequent processing or confirmation of ledger transactions than does a proof-of-work consensus protocol. This is the case, for example, for 'proof of stake' consensus protocols like those proposed by Cardano[66] and EOS[67] protocols, and planned for Ethereum.[68] There are numerous proposals for alternative architectures where perhaps the only common elements binding them together as 'Smart Ledgers' are 'immutability' and 'embedded computer code that can be executed at a future date'.

[65] GDPR Arts. 18(1), 21(1) & 21(2).

[66] Ourobouros Proof of Stake Algorithm, http://cardanodocs.com/cardano/proof-of-stake/

[67] Brady Dale, "EOS Is Coming, If Anyone Can Figure Out How To Vote", *Coindesk* (30 May 2018), http://www.coindesk.com/eos-coming-anyone-can-figure-vote/

[68] Shiraz Jagati, "Ethereum Proof of Stake Protocol Under Review", *CryptoSlate* (22 April 2018), http://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/

3. Identifying Data Controllers & Data Processors

Unlike the previous two issues, the challenge of identifying data controllers and data processors is not specific to distributed ledgers. GDPR defines 'controller' as:

> "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[69]

'Processor' is defined as:

> "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[70]

Applying these definitions to complex, multi-party applications and technical ecosystems (consider, for example, the interactions of buyers, sellers and payment providers on a platform like Amazon or eBay) is a frequent challenge for data protection practitioners. However, despite potential ambiguities, it is our experience that a practical, good faith approach to defining controller and processor roles is generally effective from a regulatory perspective.

For example, the following approach appears sensible:

- users that store data and build applications on a distributed ledger are data controllers with respect to any personal data that they process or store;
- distributed ledger nodes are data processors when they process transactions for others; and
- the operator of a distributed ledger (*i.e.*, one that is not purely decentralised) is a data controller with respect to personal information of individuals with which it interacts in order to operate the ledger.

[69] GDPR Art. 4(7).

[70] GDPR Art. 4(8).

This approach to defining roles of data controllers and data processors is consistent with approaches recently recommended by the German Blockchain Association[71] and others.

4. Automated Decision-Making

Like the previous issue, the question of automated decision-making is not specific to distributed ledgers. Article 22 of GDPR restricts automated decision-making without human involvement "which produces legal effects concerning [an individual] or similarly significantly affects him or her." This provision has generated substantial interest and concern in the technology community because a wide variety of emerging applications – particularly those involving artificial intelligence and machine learning – use automated decision-making.[72] For distributed ledgers, the Article 22 restriction is only relevant to a distributed ledger application to the extent that the application uses automated decision-making. Whether any application in fact does so must be assessed on a ledger-specific and application-specific basis. Furthermore, there are important exceptions to the Article 22 restriction, including where:

- there is a 'human in the loop' in some non-trivial respect – *i.e.*, decision-making is not purely automated;
- an automated decision does not produce "legal effects" or similar effects;
- the automated decision or processing "is necessary for entering into, or performance of, a contract between the data subject and a data controller" (GDPR Art. 22(2)(a)); or
- the automated decision is made with the data subject's explicit consent.

[71] *See* Blockchain Bundesverband (the German Blockchain Association), "Blockchain, data protection, and the GDPR", pp. 5-7 (25 May 2018), ("GDPR was created before Blockchain and is already outdated, since it doesn't account for decentralized technologies."), http://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf

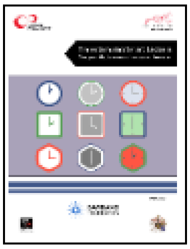
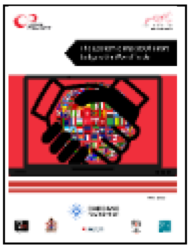
[72] *See, e.g.*, Pomin Wu, "GDPR and its impacts on machine learning applications", Medium (7 November 2017), http://medium.com/trustableai/gdpr-and-its-impacts-on-machine-learning-applications-d5b5b0c3a815

Author

Hugh Morris
Senior Research Partner, Z/Yen

Hugh has over 35 years' business experience and has deep expertise in technology and financial services. He specializes in leading IT and business services companies, delivering profitable entrepreneurial growth. He was a Global Managing Partner at Accenture where he led the technology and outsourcing practices in the UK, led the public sector practice in Scandinavia, UK, Ireland and South Africa and, subsequently, the global Transition and Transformation practice for the outsourcing business of the firm. He was then an Executive Director at Xchanging plc where he led the HR outsourcing business and then integrated the company's global IT and operations infrastructure. He then started his own business, Laureate Legal Services, aimed at delivering BPO services to leading UK law firms. He worked at Genpact leading business development in EMEA for financial services and then as Sales and Marketing Director for TORI Global, a financial-services focused consultancy. He is now working in a pluralist mode.

Selected Distributed Futures Publications

	Title	Authors	Year	Publisher
	Information Rules – Smart Ledger Architectures and Distributed Permissions	Maury Shenk and Professor Michael Mainelli	2018	Long Finance (November 2018), 62 pages.
	Smart Ledgers & Collective Defined Contribution Pensions	Iain Clacher, Con Keating, and David McKee	2018	Long Finance (July 2018), 47 pages.
	Timestamping Smart Ledgers - Comparable, Universal, Traceable, Immune	Sam Carter	2018	Long Finance (June 2018), 55 pages.
	The Economic Impact Of Smart Ledgers On World Trade	Centre for Economics and Business Research	2018	The Worshipful Company of World Traders and Long Finance (April 2018) 78 pages.
	Get Smart About Scandals: Past Lessons For Future Finance	Professor Tim Connell and Bob McDowall	2018	Long Finance (March 2018), 102 pages.
	Responsibility Without Power? – The Governance Of Mutual Distributed Ledgers (aka Blockchain)	Simon Mills and Bob McDowall	2017	Long Finance (July 2017),47 pages.

Distributed Futures is a significant part of the Long Finance research programme managed by Z/Yen Group. The programme includes a wide variety of activities ranging from developing new technologies, proofs-of-concept demonstrators and pilots, through research papers and commissioned reports, events, seminars, lectures and online fora.

Distributed Futures topics include smart ledgers, artificial intelligence, cryptocurrencies, blockchains, FinTech, RegTech, and the internet-of-things. www.distributedfutures.net

Cardano Foundation is a blockchain and cryptocurrency organisation based in Zug, Switzerland. The Foundation is dedicated to act as an objective, supervisory and educational body for the Cardano Protocol and its associated ecosystem and serve the Cardano community by creating an environment where advocates can aggregate and collaborate.

The Foundation aims to influence and progress the emerging commercial and legislative landscape for blockchain technology and cryptocurrencies. Its strategy is to pro-actively approach government and regulatory bodies and to form strategic partnerships with businesses, enterprises and other open-source projects. The Foundation's core mission is to "standardise, protect and promote" the Cardano Protocol. www.cardanofoundation.org

“When would we know our financial system is working?” is the question underlying Long Finance’s goal to improve society’s understanding and use of finance over the long term. Long Finance aims to:

- expand frontiers - developing methodologies to solve financial system problems;
- change systems - provide evidence-based examples of how financing methods work and don’t work;
- deliver services - including conferences and training using collaborative tools;
- build communities - through meetings, networking and events.

www.longfinance.net

Z/Yen is the City of London’s leading commercial think-tank, founded to promote societal advance through better finance and technology. Z/Yen ‘asks, solves, and acts’ on strategy, finance, systems, marketing and intelligence projects in a wide variety of fields. Z/Yen manages the Long Finance initiative.

Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
+44 (20) 7562-9562 (telephone)
hub@zyen.com (email)

www.zyen.com

Price: £10
ISBN: 978-1-912908-56-7