THE DECENTRALISED FINANCIAL PASSPORT

Regulated financial institutions must, by law, operate expensive, time-consuming customer due diligence processes (KYC, KYB etc) to continuously understand who their customers are. Those customers are increasingly managing their finances from smartphones and soon they will be doing that without passwords, pin numbers, memorable questions or ever having to rekey their identity data. There will be no need to rely on paper credentials or overshare personal information; this will be liberating for both customers and financial institutions.

The Decentralised Financial Passport concept relies on decentralised identity technology and the open standards that are fast becoming real world infrastructure. This new global identity layer enables reputable institutions to issue **portable digital identity credentials** that are controlled by their customers. This streamlines onboarding, reduces complexity, reduces costs and vastly improves data security. New revenue streams and business models will emerge.

This briefing is for innovators at UK financial institutions. It introduces the concepts, opportunities and challenges around decentralised identity, plus a roadmap for adoption.

CBOXX

Al Sherriff

September 2019

The Decentralised Financial Passport Concept

UX Concept by CBoxx for a Decentralised Financial Passport

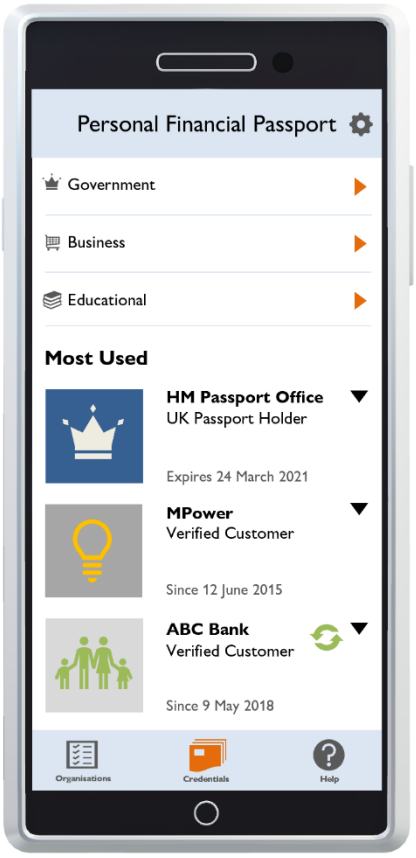
Conceptually, a **Decentralised Financial Passport** is simply a smartphone app used by customers to digitally prove who they are with a single tap when accessing any of their bank accounts, pensions, loans, savings, mortgages, insurance policies, credit cards etc held at financial institutions.

After initial registration, a returning customer can simply tap a notification on their phone to confirm they want access to an online financial service. This action simultaneously grants their consent to the financial institution to cryptographically verify their digital identity credentials and authorise access.

Crucially, customer identity credentials can be verified totally independently of their issuers. For example, if a bank needs to check a proof of residency credential issued by a utility company, they do not need to build an integration with that utility company or any utility companies their customers use.

Financial institutions will soon be creating and issuing portable, digital KYC credentials for their customers as a valuable new service that will become expected as standard.

Customers will organise and manage their digital credentials using apps similar to the Decentralised Financial Passport. Decentralised KYC credentials will be portable and reusable by customers with other financial institutions who choose to trust their issuer. They can be reviewed and revoked by their original issuers at any time. **The opportunity for portable, digital KYC credentials therefore applies to both issuing and relying institutions.**



This is the foundation for secure, portable KYC using decentralised identity technology - also known as **"self-sovereign identity"** or **"self secured identity"**. Decentralised identity is becoming real world technology infrastructure right now, bringing streamlined customer onboarding, improved customer service, reduced operational costs and reduced risk with hugely enhanced data security.

Global decentralised identity networks will benefit financial institutions and their customers. They will bring in new customers, simplify switching and are thought by many to be a prerequisite for much broader financial inclusion.

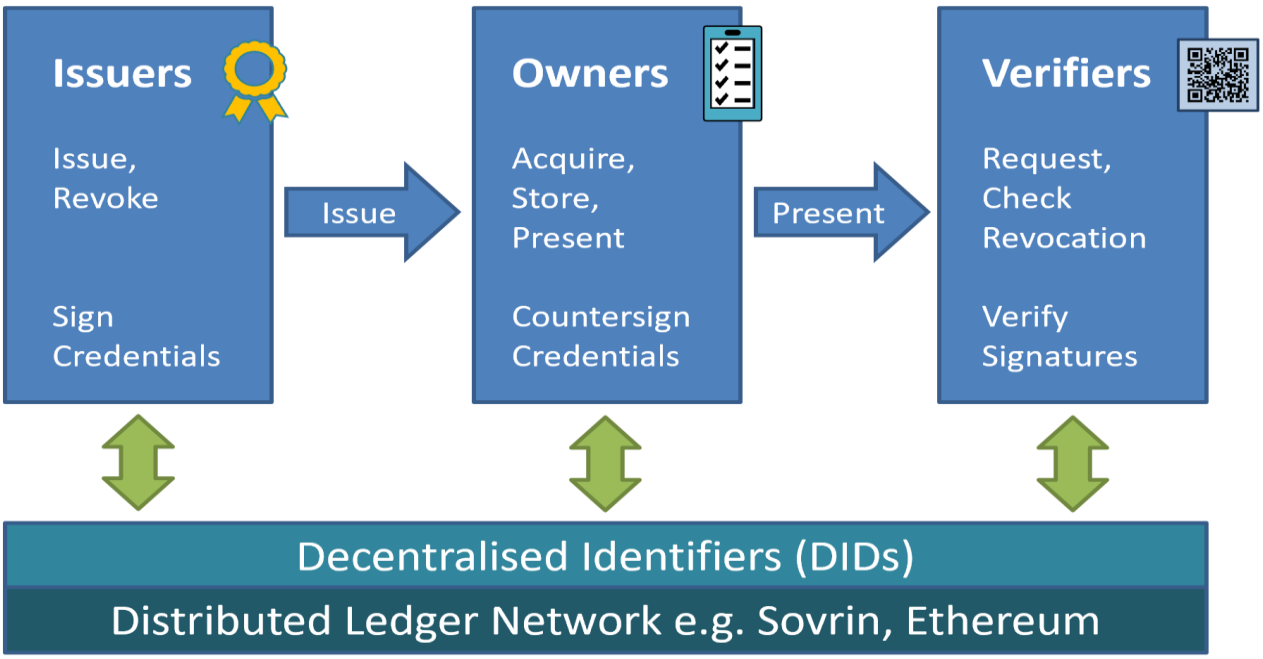
Global Decentralised Identity Networks

> The Internet was built without a way to know who and what you are connecting to.
>
> The Laws of Identity by Kim Cameron, Microsoft Architect of Identity in 2005

Decentralised identity is founded on the emergence of global decentralised identity network infrastructure built around open standards and designed at the core to provide interoperability and integration with existing systems.

Decentralised identity networks exist now, such as Sovrin that officially went live in 2017; while others are in incubation. Their success will rest on the widespread adoption of open standards such as **W3C Verifiable Credentials** coupled with **Decentralised Identifiers (DIDs)**. DIDs enable the management of Verifiable Credentials completely independently of centralised authorities or registries because they are cryptographically anchored to a Decentralised Identity Network.

> "**Credentials** are a part of our daily lives; driver's licenses are used to assert that we are capable of operating a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. These credentials provide benefits to us when used in the physical world, but their use on the Web continues to be elusive."
>
> **Abstract from W3C Verifiable Credentials specification**



The identity network actors are **Issuers, Owners** and **Verifiers**. Issuers will include government agencies, financial institutions, corporations, educational establishments and NGOs who will all generate digital verifiable credentials for Owners who will use their Identity app to store and then present them on request to Verifiers who can reliably and independently check them.

Decentralised identity Issuers and Verifiers can operate independently of each other by adopting open standards and building one connection to a decentralised identity network.

Governance, Governments and Regulation

> "...control over users' data and digital possessions and activity is rapidly moving from an asset to a liability.
>
> **Vitalek Buterin**, Ethereum Founder, May 2019

Vast pools of personal identity data have been collected, stored and controlled by public and private organisations over the past two decades or more. These hackable honey pots have become hugely attractive to attackers as the value and power of the data economy has been growing.

The driving force behind decentralised identity is the elimination of identity theft and fraud at scale. There has been a growing public reliance on private corporations such as the social media and tech giants to diligently protect their vast silos of customer identity data. Control and consent over the use of personal data must shift back to individuals to effectively tackle this problem. Identity theft and misuse has caused enormous damage to individuals, corporations and governments, rightfully giving rise to increasingly strict and punitive personal data privacy regulations such as GDPR in the EU.

Fundamental to a Decentralised Identity Network is a **governance structure** that ensures no individual member can dictate the behaviour and rules of the network or associated ecosystems. The most advanced example at present is the Sovrin Network created to function as a global public utility for self-sovereign identity. The Sovrin Foundation is a not-for-profit constituted to recruit and organise a global collection of Stewards who are trusted to collectively abide by the rules of the foundation to operate the network nodes. At the time of writing there are 59 Stewards listed, including IBM and Cisco. The Sovrin Network itself is Distributed Ledger Technology (Hyperledger Indy) which means that technical consensus and trust between Stewards is enforced by code and no single Steward can subvert the network.

> "We welcome in particular the work of the Decentralized Identity Foundation (DIF) for distributed identifiers, the Worldwide Web Consortium (W3C) for verifiable claims and the Open ID Foundation in driving open identity standards.
>
> **Mastercard**, Restoring Trust in a Digital World, March 2019

The **Decentralised Identity Foundation (DIF)** is a growing global co-operative that is collectively building the tools and technologies around decentralised identity open standards with the goal of establishing an open, healthily competitive ecosystem. DIF is working at the coalface of decentralised identity with 79 members so far. Members include Microsoft and Mastercard who announced their own collaboration at the turn of 2019 to create an international Digital ID based on decentralised technologies, standards and infrastructure.

The growing awareness, understanding and acceptance of decentralised identity within regulated environments, is demonstrated by a rising number of digital identity projects within the UK Financial Conduct Authorities 'Regulatory Sandbox' program. Cohort 5 of the FCA

Sandbox includes active DIF members Evernym, Onfido and uPort working together with Deloitte and Signicat as "Fintech Delivery Panel Partners" to conduct …

> "A test that is looking to show that consumers can take control over their digital identities and 'port' previously verified digital identities across different companies that rely on them to satisfy their customer due diligence and KYC obligations related to identity verification."
>
> **FCA Regulatory Sandbox – Cohort 5 – Fintech Delivery Panel Partners**
> https://www.fca.org.uk/firms/regulatory-sandbox/cohort-5

Self-Sovereign Identity was a popular topic at the **Think Digital Identity for Government** event in London in early June 2019 where on a panel of public sector Digital Identity Leaders, the Deputy Director of Identity at the UK Department for Work and Pensions (DWP) declared that she "loathed" (!) Self-Sovereign Identity but is now coming around to the idea. With a prescient piece of agenda planning, an NHS group then demonstrated their pilot to solve chronic problems with the management of Doctors identity credentials, using portable self-sovereign identity on Sovrin developed using the W3C Verifiable Credentials and DID open standards.

A week later Facebook announced Libra and central banks and regulators took serious notice of a potentially systemic economic event. Libra intends to create a global digital currency, based on the principles of decentralisation and **stablecoin technology**. The Identity community drew attention to an important clause in the Libra Association White Paper…

> "An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition.
>
> **Facebook**, Libra Association White Paper, page 8, June 2019

Facebook believe that decentralised identity must go hand-in-hand with the Libra global payments system and is therefore vital in proving their trustworthiness to regulators.

Decentralised identity technology goes a long way towards delivering the absolute trust required by financial regulators and data protection authorities. Libra plans to deliver in 2020 indicating they will move fast and will need to adopt existing open standards. This notion is reinforced by the presence of active DIF members amongst the Libra Association founders such as Mastercard and PayPal (via Cambridge Blockchain).

Despite current politics, the UK government direction on digital identity must align with the EU and other national standards. Arguably, Brexit will accelerate the automation of processes due to an increase in cross border administration. eIDAS is the EU regulation for "electronic identification and trust services". It references a range of services to verify the identity of individuals and businesses online and the authenticity of electronic documents. In the UK it is supervised by the ICO (Information Commissioners Office) who also supervise GPDR. The goal

of eIDAS is to provide a cross border legal framework within the EU that will generate greater trust in electronic transactions between businesses, people and public authorities.

In the UK, eIDAS has been implemented by the federated **GOV.UK Verify scheme** that while serving nearly 5 million users today, is deemed to have been largely a failure and is now in a period of transition. It is due to have all public funding withdrawn by April 2020 and access opened up to the private sector. https://www.gov.uk/performance/govuk-verify

The focus of UK government departments such as DCMS (Department for Digital, Culture, Media & Sport) and GDS (Government Digital Services) is a drive towards the widespread adoption of interoperable standards as indicated by **GPG45 (Good Practice Guide 45)** that has been specifically designed to align with eIDAS, NIST and other national trust frameworks. At the core of GPG45 lies four Levels of Identity Assurance (LOA) supported by GOV.UK Verify:

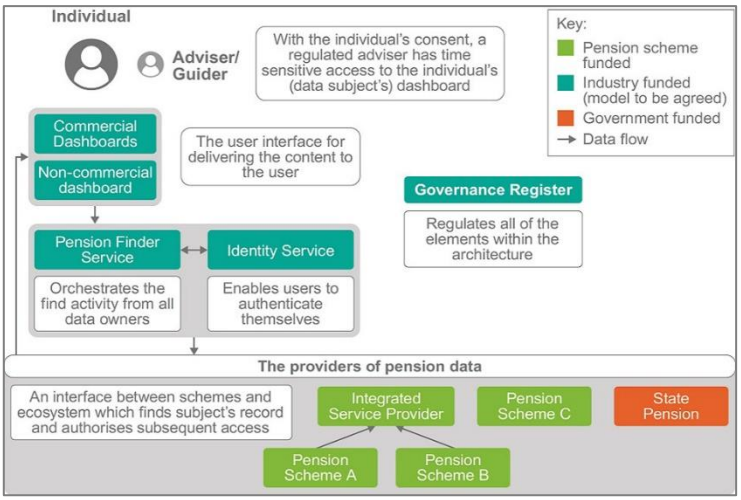
- **LOA1 – Low Risk.** UserId/Password and/or Social Media Account access are sufficient.
- **LOA2 – High Risk of Identity Fraud e.g. protecting money or licenses.** The relying party must know on the balance of probabilities who the user is and that they are a real person. Two Verifiable Claims are required: Proof of Identity (e.g. Passport, Birth Certificate) and Proof of Account Ownership e.g. bank account, mobile phone contract.
- **LOA3 – User could face serious consequences from identity fraud e.g. physical harm or financial ruin.** The relying party must know beyond reasonable doubt who the user is, and that they are a real person.
- **LOA4 – User could face life threatening consequences as a result of identity fraud.** An additional biometric profile must be captured at the point of registration.

It is evident that decentralised identity solutions must support LOA1 and LOA2 as a minimum to be acceptable to regulated UK/EU financial services environments.

The UK has absolutely no mandate to create a centralised digital identity scheme such as Aadhaar in India or the WeChat ID national digital identity rollout across China. **The overall UK vision is to enable the creation and reuse of trusted, portable, flexible, open standard digital identity credentials across the public and private sectors.** In July 2019 DCMS issued an **open call for evidence,** requesting responses by mid-September 2019:

> We are committed to enabling a digital identity system fit for the UK's growing digital economy without the need for identity cards by working in partnership across government, the private and voluntary sectors, academia, and civil society. We see there are significant benefits for citizens and consumers being able to create digital identities under their own control and then to use different verified attributes to access a range of services as and when needed … In particular we're interested in evidence of the demand for individual-controlled reusable digital identities – trusted identities usable in more than one place
>
> **DCMS and Cabinet Office, Digital Identity: Call for Evidence, July 2019**
> https://www.gov.uk/government/consultations/digital-identity

The outcomes of the DCMS research may influence new digital initiatives. One potential example in UK financial services is the **Pensions Dashboard** that aims to help *"... transform retirement savings and pensions forever."*



At the heart of the proposed pensions dashboard architecture (see diagram) is the industry funded **Identity Service** that must satisfy the GPG45 rulebook for 'Identity Proofing and Verification of an Individual' while operating within the proposed digital identity guidelines. The system must use open standards with LOA2 standard assurance for the identity credentials of consumers and their professional advisers.

Source: Pensions dashboards: Working together for the consumer (April 2019)
https://www.gov.uk/government/consultations/pensions-dashboards-feasibility-report-and-consultation/pensions-dashboards-working-together-for-the-consumer#chapter-4--architecture-data-and-security

Beyond KYC / KYB there are high volume identity related processes for individuals to authorise others to make financial decisions on their behalf. The authorised persons must be able to prove to the financial institutions concerned that they have been granted authority. e.g.

- **Letters of Authority** are tripartite agreements between customers (policyholders), their financial advisers and financial institutions (providers). They are an essential, frequently paper based, onerous part of the industry processes for customers to register with and change financial advisers and also for advisers to manage their customers assets (pensions, ISAs etc) and **transfer assets** between providers;

- **Power of Attorney** is becoming increasingly important as the population ages. It is particularly vulnerable to fraud and therefore financial institutions must take special care in checking the identity credentials, level of authority and subsequent actions of attorneys that register with them to act on behalf of their donor.

In both of these cases it is easy to envisage how a portable, verifiable credential that digitally proves the authority and authenticity of individuals will streamline the processing (when it is needed) and improve data security. In the case of Power of Attorney there is more than just a financial business case, attorneys may often be trying to act during times of acute distress while the staff processing their requests must also be extra vigilant against fraud.

https://www.financial-ombudsman.org.uk/consumers/complaints-can-help/complaints/power-attorney

Decentralised identity conceptually fulfils the UK government goals for digital identity. There must be opportunities as GOV.UK Verify opens up to the private sector while at the same time decentralised identity networks and open standards are maturing and gaining traction globally.

The **Tech UK white paper on Digital Identity** published in February 2019 recommends the following steps are taken by government …

- A Government policy for the creation of a fully functioning digital identity ecosystem across public and private sectors.
- The Government release plans for the creation of a framework of digital identity standards open to all players.
- **One point of contact for digital ID within government.**
- That digital IDs be seen on an equal footing as paper-based verification.
- A lawful basis for the processing of biometric data.

The case for digital IDs, A techUK white paper, February 2019
https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf

The **Bank for International Settlements (BIS)** issued their **Annual Economic Report** in June 2019 and their analysis of **big tech in finance** highlights how challenges faced by three different national authorities that must work together are not entirely compatible – competition authorities, financial regulators and data protection authorities. Financial regulators must apply specific standards for the financial sector, whereas competition and data privacy laws must apply general standards to a very wide range of businesses.

These conflicts are exposed as big tech avances deeper into the provision of financial services with the temptation to take full advantage of their great stores of personal data and histories of transactions with analytics around buying patterns and interpersonal relationships. The use of such powerful data tools by regulated financial institutions are generally restricted. The BIS proposes a 'regulatory compass' in an attempt to illustrate the situation and provide a tool to help policymakers, big tech firms and financial institutions to navigate a safe path.

https://www.bis.org/publ/arpdf/ar2019e3.htm

The next section attempts to pull the strands of this discussion together to propose a broad roadmap for decentralised identity to deliver the potential it brings to real-world systems, processes and environments, focussing on UK financial services.

Six Phase Roadmap for Adoption

This section outlines a roadmap for financial institutions to consider when planning their assessment and adoption of decentralised identity. It favours an approach of continuously enhancing existing frameworks and systems, rather than rip & replace.

1. **Issue reusable Digital KYC Verifiable Credentials for one Service within an Organisation**

   Phase 1 will need a project defined to deliver clear benefits to both customers of the service and the organisation providing the service. It must identify and tackle the challenges to be overcome to lay down strong foundations for the later phases.

Phase 1: Reusable Digital KYC
✓ Streamline customer experience: easy onboarding, no passwords, one-tap verify
✓ Reduce customer support costs
✓ Reduce the risk of identity theft and fraud
⚙ Assess suitability of decentralised identity technology, select trusted partners
⚙ Implement new KYC issuance, authentication and verification processes
⚙ Deliver Decentralised Identity app, decide whether to partner or build
⚙ Future proof by adopting decentralised identity open standards from the outset

2. **Extend reusable Digital KYC Credential to work across Services within the Organisation**

   Phase 2 is initiated once the benefits of Phase 1 have been quantified and a clear business case agreed to deliver a project to rollout across the organisation.

Phase 2: Extend use of Reusable Digital KYC across Organisation
✓ Further streamline customer experience: one-tap verification
✓ Further reduce customer support costs across multiple services
✓ Further reduce the risk of identity theft and fraud
⚙ Implement a broad rollout of authentication and verification processes
⚙ Engage with the financial services identity community, prepare for sector rollout

3. **Extend the reusable Digital KYC Credential to relying Organisations across the Financial Services Sector, operating at scale within the same legal and regulatory jurisdiction.**

   The Decentralised Financial Passport concept is fully realised in this phase. A digital identity consortium of regulated financial institutions that operate within the same jurisdiction will be required, supported by legal and compliance experts to implement a suitable decentralised governance framework. Relying parties may pay credential issuers each time customers use their KYC / KYB Credential to access a service. Trusted issuers may in turn rely on the creation of identity insurance products to safeguard them against their own risks and liabilities. Government support will be required from this phase forwards.

▶ Phase 3: Digital KYC reusable across Financial Services Sector
✓ Streamlined KYC processes across the financial services sector
✓ Reduced customer support and onboarding costs across the sector
✓ Reduced risk of identity theft and fraud across the sector
⚙ Implement authentication and verification processes that rely on external issuers
⚙ Create legal framework for liability and protection of issuing and relying parties
⚙ Setup suitable governance structure for decentralised identity consortium
⚙ Agree economic model for credential issuing and relying parties

4. **Broaden the use of Verifiable Credentials within the Financial Services Sector.**

   This phase moves beyond KYC/KYB to verifiable credentials for improving other processes that rely heavily on secure identity checks e.g. Letters of Authority, Asset Transfers and Power of Attorney processes can be greatly improved with digital verification.

▶ Phase 4: Multiple Verifiable Credentials across Financial Services Sector
✓ Streamlining of multiple identity processes across the financial services sector
✓ Further reduced customer support and onboarding costs across the sector
✓ Further reduced risk of identity theft and fraud across the sector
⚙ Improve processes for letters of authority, asset transfers, power of attorney etc.
⚙ Extend legal framework for liability and protection of issuing and relying parties

5. **The principles proven by the Decentralised Financial Passport can now be extended to other sectors and perhaps even drive the creation of a general "Digital Passport".**

   This ambitious phase must align with government strategy at policy level, combined with opening secure access to state digital services to create a broad digital identity ecosystem.

Phase 5: Digital Identity Credentials reusable across multiple Sectors
✓ Sectors could include Financial Services, Healthcare, Education, State etc.
✓ Streamlined access to services and reduced costs across multiple sectors
✓ Reduction in risk of identity theft and fraud across multiple sectors
✓ Wide reduction in GDPR liability, citizens control their own data and consent
✓ Accelerated innovation opportunities, such as aggregated personal services
✓ Economic benefit estimated at £27.8bn increase in UK GDP See page 4 of https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl Shift_Data_mobility_report_full.pdf
⚙ Establishment of a single adaptive UK regulatory entity for digital identity
⚙ Regulator opens "golden issuer" API access to private sector identity verifiers

6. **A successful National Digital Passport sets a model for International Digital Passports**

   This final phase tackles serious global challenges faced today, including humanitarian causes. It relies on a degree of global political alignment and may face opposition from corporations whose business models are based on monetising their silos of personal data.

Phase 6: Digital Identity Credentials reusable across Borders
✓ Fast, regulated, low cost, cross border remittances and payments
✓ Financial inclusion enabled through "thin file" portable digital identities
✓ Humanitarian causes supported by refugee & aid worker digital passports
✓ Innovation opportunities are now opened up on a global scale
⚙ Resistance encountered from organisations built to sell personal data
⚙ Challenges of supporting regulatory requirements across multiple jurisdictions

Calls to Action

The digital identity landscape is evolving rapidly with the shift towards decentralised identity strengthening daily. Identity, payments and asset tokenisation technologies are advancing hand-in-hand with the prevailing direction of data privacy laws and financial regulation.

- The W3C open standards for Verifiable Credentials are expected to advance to "proposed recommendation" in Q3 2019. This is the final stage before becoming a W3C recommendation and effectively become **an identity standard for the web;**
- The **Sovrin decentralised identity network and the ecosystem** being created by the **Decentralised Identity Foundation** community of Microsoft, Mastercard, IBM, Evernym, Deloitte, Barclaycard and many others are maturing rapidly around these standards;
- These points can address the problem of the "missing identity layer for the internet";
- The **Facebook Libra** assertion that "decentralized and portable digital identity is a prerequisite to financial inclusion and competition" is a powerful pointer to how big tech firms plan to tackle their trust issues with financial regulators and central banks;
- The **GOV.UK Verify** federated identity scheme for citizen identity is being **opened up to the private sector by April 2020** when public funding is withdrawn. **DCMS issued their Call for Evidence** on digital identity in a paper that explicitly favours portable digital identity credentials for citizens created "under their own control";
- Of the 29 projects accepted into **FCA Regulatory Sandbox Cohort 5**, four are directly related to portable digital identity and KYC, while eight others have strong associations.

UK financial institutions should engage with decentralised identity as there are opportunities to be seized and missed in this fast maturing new landscape. Some actions to consider are:

1. **To focus your thinking around digital identity**, review the forthcoming responses to the DCMS Call for Evidence that completed on 15th September 2019. https://www.gov.uk/government/consultations/digital-identity
2. **Conduct business case research around issuing and relying on portable digital identity credentials** to quantity the cost savings, understand the benefits, opportunities, risks and threats specific to your organisation. The costs of KYC / CDD vary wildly between firms - surveys from Thomson Reuters and others typically put them in the £ millions p.a. depending on the scale and functions involved. The scope for cost saving is huge.
3. **For specialist help**, look at partnerships such as Evernym, Sovrin and Microsoft: https://www.evernym.com/plans/early-access/ https://sovrin.org/join-the-sovrin-alliance/ https://www.microsoft.com/en/security/technology/own-your-identity
4. **For the global technical perspective**, engage with the W3C, DIF and Sovrin communities
5. **For the national policy perspective**, look at the FCA Sandbox, engage with Digital Identity groups at techUK, TISA and THINK Digital who operate close to government. Consider the need for a consortium of members focussed on the distribution, wealth management and financial advice end of the of the financial services stack.

Further Information and About the Author

On Digital Identity Standards and Frameworks

- https://www.w3.org/TR/vc-data-model/
- https://w3c-ccg.github.io/did-primer/
- https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720963/good_practice_guide_45_identity_proofing_version_3_february_2017.pdf
- https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/
- https://www.gov.uk/servicemanual/identity-assurance
- https://www.verify.service.gov.uk/understand-levels-of-assurance/
- https://www.comsoc.org/publications/magazines/ieee-communications-standards-magazine/cfp/dawn-internet-identity-layer-and

On Digital Identity and Regulatory Landscape

- https://www.bis.org/publ/arpdf/ar2019e3.htm
- https://www.techuk.org/insights/reports/item/14707-techuk-publishes-digital-identity-white-paper
- https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf
- http://financial-risk-solutions.thomsonreuters.info/Cost-of-Compliance-2019
- https://www.paymentsjournal.com/uh-oh-is-apple-expanding-the-restriction-on-nfc-to-include-mobile-identity/
- https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Why-Govuk-Verify-faces-a-critical-few-months-again
- https://www.civilserviceworld.com/articles/opinion/opinion-think-britain-beats-world-digital-services-think-again-china-rules-digital
- https://www.ft.com/content/3e1f00e2-eac8-11e7-bd17-521324c81e23
- https://thefinanser.com/2019/08/chris-skinners-tedx-talk.html/
- https://media.consensys.net/the-state-of-stablecoins-2019-40c3eca990f4
- https://vitalik.ca/general/2019/05/09/control_as_liability.html

On Digital Identity News and Initiatives

- https://newsroom.mastercard.com/press-releases/mastercard-introduces-consumer-centric-model-for-digital-identity/
- https://www.moneyobserver.com/opinion/financial-futures-digging-digital-passport
- https://moneyweek.com/388096/the-digital-passport-that-could-revolutionise-british-savings-culture/
- https://www.computerweekly.com/news/252451663/UK-Post-Office-looks-to-enable-reusable-digital-ID
- https://vonx.io/
- https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html
- https://www.theguardian.com/business/2019/aug/23/mark-carney-dollar-dominant-replaced-digital-currency

On Decentralised Identity Implementation

- https://identity.foundation
- https://www.evernym.com/ebook-decentralized-identity-for-banks/
- https://sovrin.org/the-sovrin-alliance/
- https://www.hyperledger.org/projects/hyperledger-indy
- https://www.hyperledger.org/projects/aries
- https://www.devteam.space/blog/how-to-build-a-self-sovereign-identity-wallet/

About the Author

Many thanks for reading this paper. Please get in touch if you're interested in exploring further...

Al Sherriff
alan.sherriff@cboxx.com
www.linkedin.com/in/alsherriff
www.twitter.com/CBoxxLtd
www.cboxx.com

Over 25 years of experience working in UK financial services technology as a developer, business analyst, architect, agile project manager and innovation consultant. Notable clients include The Exchange, Standard Life, Time4Advice at St. James's Place and Mattioli Woods, Profile Pensions, AXA Wealth, Winterthur Life, Association of Professional Financial Advisers, Chase de Vere, Skipton FS, Pillar Project / 2030, Origo and Criterion.

On blockchain technology and decentralised identity - research, consulting, writing, pitching and presenting since 2015 – specifically for Hult Business School, Calastone, Digital Identity for the Identityless (DI4I, led by University of the West of England), Blockchain 4 Good (at techUK), The Investment Network, Hub of all Things (HAT) at Oxfam, Money Marketing, the Institute for Chartered Accountants in England & Wales (ICAEW), Team Blockchain, Frontiers In Blockchain, Pillar Project / 2030 and Criterion.

With special thanks to David Taylor of OCP for his invaluable feedback and review ...
david.taylor@ocp.co.uk
https://twitter.com/rdavidtaylor
http://www.ocp.co.uk/who-we-are