Distributed Ledger Technologies for Public Good – A Progress Update

Foreword by Lord Holmes of Richmond MBE

My November 2017 report, *Distributed Ledger Technologies for Public Good*, called for leadership, collaboration and innovation. Since its publication, I have witnessed excellent examples of industry and academia engaging with some parts of HMG, and other governments around the world, to promote better decision-making and greater efficiency through common access to high quality, up to date and authentic data. The initial excitement is maturing into pragmatic implementation, including early stage development of collaborative infrastructures, particularly by those industries and sectors working on pilots likely to accrue and to prove the most immediate benefit. Participants place a high priority on good legislation, compliance, security, data protection and law enforcement.

In the same period, I have welcomed signs that HMG recognises both the importance of the technology and the role for government in its development for the public good. In Parliament, the Prime Minister has stated her support for the development of DLT, the Chancellor has been active in commissioning a report from the Crypto Asset Taskforce and DCMS, through Margot James, have ensured that the UK remains in touch with European developments through her sponsorship of the UK's membership of the Blockchain Partnership. I understand that DLT was also on the agenda at a recent Cabinet Secretary's Advisory Group meeting. This all confirms my understanding that steps are being taken to ensure that the public interest is firmly captured and fed into the commercial developments in this area. I am hopeful that this senior engagement is laying the foundations for the establishment of operational cross-departmental arrangements to engage with the growing national momentum, overseen by a HMG DLT Steering Group.

The creation of cross-departmental arrangements and the formation of a steering group to ensure sustained collaboration were key recommendations from my report. Indeed, my report re-iterated the conclusions of the government's own report issued by Sir Mark Walport back in January 2016. If DLT is to be the public good that I and many others believe it can be, then there needs to be comprehensive and properly governed collaboration between public, private and academic sectors. Exemplars from other countries suggest that such collaboration works best when there is not only clear leadership and support from central government but clear alignment of the potential benefits to both public and commercial applications. I believe that such leadership and support is in prospect and I and my advisory group stand ready to assist with ministers and officials in the next stage of crystallising relevant frameworks and identifying priority use cases. We also stand ready to assist in developing executive awareness in Westminster and Whitehall so that as the case for potential applications develops senior decision makers are in a good position to be able to do so.

This update to my report highlights achievements so far and shows that, for the moment at least, the UK retains a leading place in development and use of DLT. It also builds on those achievements to indicate how the UK can secure its competitive position globally in both the development of the technology itself and the increased productivity within reach if it is applied to enhance the performance of both the economy and state administration. The response to my core message of

collaboration, coordination and **commitment**, continues to grow with participants from over 160 industry and academic organisations, 18 government organisations and 11 nations. Alongside this I must restate the compelling need for collaborative governance within government to capture and align with this momentum and contribute, to learn, leverage, apply and benefit for the public good.

Finally, I should like to recognise the support and help, in compiling this update, of all those enterprises and emerging propositions mentioned within it. In an environment still in the early stages of its development, it is not my purpose to endorse them but to acknowledge their role in assisting the progress which has been made since my initial Report. This community of participants remain ready to support the Government and to collaborate in achieving the wider economic and societal good.

Table of Contents

Introduction

This document is a progress update on activities since the publication of my report, *Distributed Ledger Technologies for Public Good*, in November 2017. This update should be read with the report, as it provides the context and baseline on which this update builds.

The purpose of this document is to:

- highlight the considerable ongoing collaborative progress made since November 2017;
- increase participation; and
- call for action inside government to address and overcome barriers to further progress.

The essential next steps are:

1. To continue growing the community-based working groups, and the number of organisations and activities, including proofs of concept, pilots and operational systems.
2. To establish a senior government Steering Group to encourage, lead, coordinate, communicate, collaborate and educate across government – and collaborate externally.
3. For the communities to document their Catalogues of Collaborative Requirements;
4. To develop the national-level collaborative capabilities for trust and interoperability required in an industry-led, government-supported, not-for-profit model, including:
    a. ROLO UK as one of many registers of authoritative data;
    b. The UK PKI bridge as one of several interoperable federated identity management capabilities;
    c. Building on the Police Identity & Access Management System to provide high assurance standards-based digital employee authentication across all HMG, interoperable with many international allies and industry partners.
    d. Enabling some 70 million British citizens to validate their passport data digitally and securely, to prove their identity for legal and other reasons at work, in society, on the Internet and travelling. To find a similar solution for those without passports.
5. To draft legal text that could enhance existing national legislation, to help UK compete internationally.
6. To establish training and education with briefings to raise executive awareness, particularly in government, and for wider awareness.
7. To enhance coordination, communication and the existing industry-led, government-supported collaborative governance.

General Situation

My November 2017 report sought to revive and build on the momentum generated by Sir Mark Walport's report "*Distributed Ledger Technologies: beyond blockchain*". That report has been translated into at least five languages and used by many governments to inform their strategic DLT developments. One of my principal objectives was to call urgent attention to the risk of the UK falling behind the rapid pace of development around the world, including:

- new legislation in several countries (including Switzerland and Malta), which is attracting interest from advanced technology and finance companies, particularly from Asia;
- new crypto currency technologies with built in trust, designed for compliance with banking regulations;

- new blockchain and non-blockchain DLT platforms designed to support accountability and traceability in and across complex supply chains and asset management systems. These are not crypto currency systems, but some do use cryptographic tokens to transfer value and ownership.
- Increasing investment, in Silicon Valley and Europe, in blockchain and DLT. In a recent meeting of the top Silicon Valley CEOs under 40, over 60% were involved in blockchains.

There are strong messages coming from government:

- The Prime Minister has affirmed the government's commitment to DLT and made positive comments in Parliament;
- The Minister for Digital has signed the EU-wide Blockchain Partnership;
- The Civil Servant Advisory Group has set a series of actions to establish current DLT activities and future requirements, and to assign initial responsibilities, in addition to putting in place mechanisms to aid communication and coordination;
- HMRC has confirmed the need for proofs of concept for future borders;
- FSA and Defra have funded proof of concepts and pilots;
- MOD, NHS, DfT, DWP and Police are considering or planning proofs of concepts or pilots;
- Organisations, including regulators, are conducting studies and assessments.
- Many local government bodies are collaborating with chambers of commerce and business bodies to explore opportunities and experiment.

Progress in relation to the recommendations and enablers set out in my report has been good but mixed inside government. The many collaborative working group activities are progressing well, but they could do more, particularly if government organisations (rather than a few individuals within those organisations), engaged more fully within a more consistently organised collaborative framework.

There has been good progress in convening and growing coalitions of the willing across industry, and in some parts of government. For example, several academic institutions and business organisations have already expressed willingness to commit resources for virtual, distributed incubator and testbed facilities to develop and evaluate DLT applications with the potential to deliver public good. To support this initiative, BBFA[1] (a not-for-profit collaborative industry governance body) has established an informal Academia working group of universities and institutions to build on the work of Surrey University and UCL. This should allow a single community-based, collaborative request for government funding rather than numerous overlapping or competing bids for support. In parallel, a Blockchain Centre of Excellence is being established in London, with an accelerator and training facilities; it has begun providing executive awareness training for company boards and government officials.

However, despite the strong leadership messages, significant parts of government so far appear reluctant or unaware of the need to engage with collaborative efforts to address poor data quality within their organisations, and the consequences this brings for poor public services. Indeed, one government organisation has disbanded its data management function, which is comparable to a ship's captain switching off his navigation systems, becoming a hazard to everyone.

[1] BBFA was created following the demise of the National Identity Scheme, to enable government and industry organisations collaborate in a federated approach to digital employee identity and authentication. It has expanded into military and EU cybersecurity, internet governance, privacy, intellectual property, law enforcement, and supporting technologies including blockchains, DLT.

This uneven performance across government is somewhat at odds with the Prime Minister's firm statement of commitment to Artificial Intelligence and DLT[2]. It also risks missing opportunities that stem from the continuing efforts spearheaded by the Rt Hon Matt Hancock MP, Secretary of State, Health and Social Care, Rt Hon Jeremy Wright MP, Secretary of State DCMS, and Margot James MP, Minister for Digital at DCMS, to build a body of knowledge and understanding, which could be used across government to enable policy development and practical progress.

It is an inescapable fact that quality decision-making depends on quality data. This is equally true whether the focus is on military operations, airspace management, taxation, weather forecasting, assessment and payment of benefits, bank trading or any other policy-driven activity that depends on granular control of data about situations, resources, physical assets, people and money.

In most cases, data is distributed across many organisations, and differences in that data are very costly to resolve. DLT has the capacity to remove such differences, ensuring all parties see the same date at the same time. This dramatically reduces risk, cost and delays, creating the conditions for much faster and better decision-making, and introducing a tempo that gives significant competitive and efficiency advantages. It also provides robust and legally admissible evidence to demonstrate compliance or to prove breach. This builds trust, heightens reputations and strengthens collaboration. The UK needs this.

For these reasons, two new recommendations are:

- to explore the measurement of "information performance", based on data quality, within any government organisation, which could be used as an indicator for the quality of decision-making, and to give confidence to other organisations that use its data;
- to establish a government Chief Data Officer, whose prime role is to measure, encourage, assist and assure data quality across government systems, and to provide collaborative data governance across registers and other authoritative data sources upon which government and industry organisations depend. This echoes a similar recommendation in the report by Eddie Hughes MP [3]

Industry has already recognised the imperative of moving in this direction. As summarised below, seventeen collaborative working groups already exist or are being formed. Six more are being discussed. Most of these are supported, and in some cases led, by BBFA, which is a not-for-profit collaborative industry governance body[4]. Several of these working groups have benefited from BBFA's international connections, to include expert participants from other countries, which is vital for UK cross-border DLT activities.

The leading examples of collaborative progress are in food traceability (strongly led and supported by Defra and FSA), maritime, legal, land registration and conveyancing, identity management, health and financial management (excluding crypto currencies).

There has also been significant progress among legislators. Damien Moore MP and other MPs have formed and he co-chairs the All-Party Parliamentary Group (APPG) on Blockchain to ensure that

[2] Prime Minister's Questions, 6 June 2018: https://www.parliament.uk/business/news/2018/june/prime-ministers-questions-6-june-2018/

[3] Unlocking Blockchain: Embracing new technologies to drive efficiency and empower the citizen. Eddie Hughes MP July 2018

[4] BBFA was created following the demise of the National Identity Scheme, to enable government and industry organisations to collaborate in a federated approach to digital employee identity and authentication. It has expanded into military and EU cybersecurity, internet governance, privacy, intellectual property, law enforcement, and supporting technologies including blockchains, DLT.

industry and society benefit from the full potential blockchain and other DLT, at a Parliamentary level. The APPG secretariat and BBFA are coordinating to make visible the progress and momentum of the working group participating organisations to Parliament and senior government. Another new APPG on Digital Currencies has also formed and is linking with BBFA.

The government's strong messages are warmly welcomed, but there is an urgent need for practical, coordinated action by government from across government, industry and academic organisations. The collaborative community of many organisations and experts supporting my report is here to help with the collaborative effort needed.

Status and Progress

The UK is committed to becoming a leading digital nation, with a digital economy and a digital society. Both my and Sir Mark Walport's reports said that the hallmarks of advancing digital nations include:

- A digitally-informed leadership;
- An empowered, focused government department for all national digital transformation, which is internationally minded and collaborates closely with all industry sectors and across departments;
- A living, collaborative national plan, which is industry-led with government investment and departmental engagement;
- Technologically-aware, qualified and experienced senior officials in every government organisation; and
- Engineers and digital business leaders as elected politicians.

At this important time, our government and country need access to quality data and the digital means to use it quickly and effectively. However, the UK is well short of these hallmarks and the lack of progress and effective government action is an increasing and widespread concern.

Recommendations status

These recommendations build upon the enablers described in my report in November, which are repeated in the next section.

1. *Active support for the ISO May 2018 event and UK Showcase in terms of departmental representation, participation in the showcase event and as a means both to demonstrate and to assess the maturity of UK capabilities, approaches and proposed services.*
    a. Overall Progress. Reasonable: 50%
    b. The International ISO TC307 – Blockchain and DLT Committee Meeting in May was successfully hosted in London by BSI and UCL.
    c. The UK Showcase is being reshaped and rescheduled for mid-2019 to allow more time for government and the finance sector to prepare and participate alongside other industry sectors and allies.
    d. Next steps. For government and the financial sector to prepare.

2. *The creation and sponsorship of inter-departmental collaboration and coordination arrangements to identify and exploit opportunities for improving the quality and use of information in decision making and delivery of public services, and as a priority to act to leverage the enablers described.*
    a. Overall progress. None to Poor: <10%

b. Following my discussions in early 2018 with Sir Jeremy Heywood, Cabinet Secretary and Head of the Civil Service, several departmental Permanent Secretaries and agency executives, an intention and commitment emerged to establish a collaborative steering group and initial governance structure inside HMG, which would facilitate both internal and external collaborative activities and accelerate progress. Other government priorities have since intervened, but many of these priorities, particularly involving cross-border traceability and Customs, are dependent on accelerating the use of these technologies. Therefore, the case for establishing this steering group and getting behind industry-led initiatives already begun is even more compelling and imperative.
c. Following my subsequent discussions with the Secretary of State, DCMS is considering how and where it can most effectively engage to assist leading government organisations to collaborate more effectively, internally and with industry. It is clear that industry is at the forefront of developments because of market forces, and it needs joined-up government to increase its support and participation. This would give industry tangible confidence that the government is ready, able and willing to be a reliable partner in a rapidly expanding situation, measured in weeks and months, not years.
d. The participation of several government departments, agencies, NHS and police are essential because they are each sources of authoritative data on which other government organisations, industry and society depend.
e. Of note, there is a significant focus on legislation, compliance, cybersecurity, counter-fraud, identity, privacy, data protection and law enforcement. Risk management and mitigation are central themes for all working groups.
f. Next steps.
    i. Grow DCMS capacity and capability, with help from industry and other collaborative groupings, thereby to strengthen DCMS' engagement and support.
    ii. Establish a HMG Steering Group, with Perm Sec participation and leadership, with supporting HMG working groups. The CSAG recognises this need and it is hoped that this can be achieved soon. These should coordinate and collaborate with existing industry/academic working groups. It would help significantly to have a small expert secretariat to support these internal interactions and to provide a focus externally.

3. *To extend this collaboration with industry partners and international allies*.
    a. Overall Progress. Poor 10% to Medium 40% in specific working groups.
    b. The level of collaboration within government is not yet sufficient for it to be extended with others, but this will happen. However, there are a growing number of government organisations whose experts seek to collaborate on a case-by-case basis. From an industry point of view, this can be confusing as cases have occurred where government organisations have had similar initiatives competing with each other. As of yet, there is no focus or forum within government where clarity can be sought, and confusion positively addressed.
    c. Internationally, there are many points of connection, with companies, governments, parliaments, law enforcement and NGOs. All these connections would welcome the opportunity to engage with the HMG Steering Group.

d. Discussions on international collaboration with the US Congressional Blockchain Caucus and the Australian Parliament's Friends of Blockchain are ongoing. Links with other parliaments are being established.
e. Next Steps. Once HMG establishes a Steering Group, or similar body, it would be a simple task to connect with the collaborative working groups operated by BBFA and others. This secretariat would be a major enabler.

4. *To raise executive awareness and learn by doing – proofs of concept and business pilots.*
    a. Overall Progress: Executive awareness. None to Poor: <10%. Learn by doing – Medium: 30%
    b. As far as we are aware, there is no acknowledged need to raise executive awareness about new technologies, even those that change the way we live and work. This is despite recent experience. As long ago as 2013[5], the Cabinet Office formed a joint-venture with Capita, called Axelos, with a focus on HMG intellectual property and cybersecurity (amongst others). Soon after, BIS launched the Cyber Essentials cybersecurity baseline for UK organisations, and the Band of England's Prudential Regulatory Authority (PRA) launched CBest vulnerability assessment of financial institutions. All required executive sign-off, which presumed adequate executive awareness. This helped to raise executive awareness on cyber security in industry. However, the retraction of several CESG cyber security standards had an opposite effect in government, where different organisations vary in their executive awareness of the changing digital landscape and cyber security threats to their organisations. This asymmetry needs to be avoided. A more inclusive and collaborative approach is needed for DLT.
    c. Learning by doing – proof of concepts and business pilots. A few government organisations are active, seeing benefits and building on their collaborative progress. See below.
    d. Next Steps.
        i. Executive Awareness. BBFA is working with academia and an emerging blockchain centre of excellence to provide options for executive awareness, education and training. One action is to provide a briefing session in November/December for the potential HMG Steering Group, and the chairs of its working groups, in the Palace of Westminster, which could include samples from the existing educational material.
        ii. Learning by doing. Existing communities will continue to expand. Slowly, these will be linked to the UKRI, Innovate UK and other sources of government funding, until a Steering Group can provide further support.

5. *Raising departmental and policy engagement through asking for evidence of plans and raising questions within individual departments, in Select Committees, and for nominated senior departmental advisers to be a focus for identifying and realising opportunities for DLT-enabled public service improvements.*
    a. Overall Progress. Nil: 0%
    b. Next Steps.
        i. Awaiting the existence of focal points within government organisations with whom to engage and a structured, easy means to engage.

[5] https://www.axelos.com/about-axelos

Enablers

The recommendations reflected the enablers, below.

1. Increased executive awareness within government of its capacity to make more effective use of fragmented data sources to deliver faster and better decisions. Work already done as part of the government's digital strategy could be harnessed to reduce data fragmentation, to improve data authentication and to develop a data-driven communication strategy for government, business and society;
2. Collaborative governance across sectors and organisations, focusing on shared benefits, information sharing, coordination, innovation and a facilitative approach to regulation;
3. Digital trust based on validation of organisational and entity data for all UK organisations doing business on the internet to a high level of assurance, coupled with "AAA":
    a. Authentication (prove you are who you claim to be);
    b. Authorisation (prove that you have permission for what you are requesting);
    c. Accountability (prove who did what, and when);
4. Interoperability and assurance based on international standards;
5. Data linking and analytics to link entities and events where appropriate (for example, linking a payment to a particular asset and its user) to provide shared benefit and shared risk management;
6. Secure electronic communications (including mobile phones) to give users greater ownership and control over their digital identity and privacy, and promoting greater financial and social inclusion;
7. Training and education of citizens and others envisaged as end-users in the broader community.

	Industry	**Government**	**Peer nations**
Executive awareness	★★☆☆☆	★☆☆☆☆	★★☆☆☆
Collaborative governance	★★★☆☆	★☆☆☆	★★☆☆☆
Authoritative organisational data	★★☆☆☆	★★☆☆☆	★★★☆☆
Interoperability and assurance	★★★☆☆	★★☆☆☆	★★★☆☆
Data linking and analytics	★★★☆☆	★★★☆☆	★★★☆☆
Secure digital identity	★☆☆☆☆	★☆☆☆☆	★★★☆☆
Training & education	★★☆☆☆	★☆☆☆☆	★★☆☆☆

Working Groups Overview

There are currently 17 collaborative working groups, either operational or forming now, involving experts from more than 160 industry and academic organisations, 18 UK government organisations and 11 nations. More WGs are being planned. The purpose of each WG is to generate collaborative requirements (not competitive) and to 'learn by doing' in proof of concepts (de-risk technology) and pilots (de-risk business case). The collaborative governance model can take forward these requirements into policies, procedures and mechanisms for operation.

Of these, the largest and most advanced involves Food traceability. Its TORs include cross-border traceability for land, sea and air, including the Northern Ireland border.

	DLT Working Group	Meetings	Participating Organisations	Government	Pilots, POCs[6]	Progress
1	Red Meat Traceability	4	58	Defra, FSA	6	★★★★★
2	Plant Traceability	Oct	10+	FSA	TBC	★★☆☆☆
3	Food Data Policy Management Authority	Oct	10+	Defra, FSA, *GDS*	TBC	★★☆☆☆
4	Legal	4	10 incl AU, CH, MT and Africa Legal Network	MoJ, Law Commission[7]		★★★★☆
5	Legal Text	Oct	5+	TBC		★★★☆☆
6	KYC & AML	Oct	10+	*FCA,* police*, MOJ, HO*	TBC	★★☆☆☆
7	Charities	2	9	Charities Commission	*1	★☆☆☆☆
8	Token	1	8	Nil	5+	★★★☆☆
9	Police	TBC	TBC	Police, NCA	*2+	TBC
10	Register of Legal Organisations UK (ROLO UK)	2	12, inc. NL, JP	Police, NCA, HMRC, CO, NAO, Co House, *DWP*	1	★★★☆☆
11	Academia	4	8	Nil	TBC	★★☆☆☆
12	Maritime	Oct	10 inc. NL	*DfT*	3+	★★★★☆
13	Aviation	Nov	3	TBC	1	★☆☆☆☆
14	Health	3	25+	NHS	2	★★★☆☆
15	Prescription Drug Addiction	Oct	TBC	NHS, MHRA, CQC, GMC	1	★★☆☆☆
16	Identity Provision	1	8	*MOD, HO, CO, DCMS, DVLA*	TBC	★★★☆☆
17	Authentication	1	10	*MOD, CO, DCMS*	TBC	★★★☆☆
18	Entitlement	1	8	*DCMS, MOD*	TBC	★☆☆☆☆
19	Land Registers and Conveyancing	Oct	TBC	Land Registries, *OS, OSNI*	1+	★★☆☆☆
20	Assurance	Oct	6+	TBC	-	★☆☆☆☆
21	Master Data Management	Nov	TBC	*NAO, ONS, GDS*	-	-
22	Finance	New	In collaboration with another organisation			
23	Insurance	New	TBC	TBC		-
24	Gambling/gaming	New	TBC	TBC	TBC	

Invited organisations in discussion, but not yet participated are shown in italics.

[6] * = Identified Requirements

[7] The Law Commission is currently investigating and preparing to report on "smart" contracts.

Demonstrators

The following collaborative demonstrators have been identified as candidates for the UK Showcase due in 2019. More candidates are emerging. Their status varies from planning through proof of concept, pilot, preproduction and production/operational.

	DLT Demonstrator	Status	Government	Potential reuse
1	Personal KYC Validation	Preproduction	TBC	★★★★☆
2	Defra red meat	Proof of concept	Defra	★★★★☆
3	FSA red meat abattoir data	Pilot	FSA	★★★★★
4	Pork traceability retail	Operational	China	★★★★☆
5	Whisky & beer traceability retail	Preproduction	Scotland	★★★★☆
6	Meat traceability retail	Pilot	UK	★★★★☆
7	Flight Chain - aviation	Pilot, now closed	DfT	★★★★☆
8	Maersk & Rotterdam container tracking	Preproduction	NL, Rotterdam	★★★★☆
9	MTI Container tracking	Preproduction	DfT, NL	★★★★★
10	Doctors medical credentials register	Pilot	NHS	★★★☆☆
11	Medicines management	Proof of concept	NHS, H2020 partners	★★★☆☆
12	DISC Mobile Benefits Payments	Pilot	DWP	★★★☆☆
13	3M traceability	Preproduction		★★★☆☆
14	Estonia patient records	Operational		★★★★☆
15	Estonia privacy records	Operational		★★★★☆
16	Company data validation evidence	Preproduction	Companies House	★★★★★
17	Football imagery exchange	Pilot		★★★☆☆
18	Malta e-gaming	Proof of Concept		★★☆☆☆
19	Islamic charity payment tracking	Planning		★★★☆☆
20	Property exchange	Preproduction	Land Registry	★★★★☆
21	NL - UK: Dutch Blockchain Coalition	Planning		TBC
22	Token management	Preproduction		TBC
23	Whitechapel Think Tank: UK Finance	Planning		TBC
24	Police Digital Witness	Planning	Police, NCA, Borders	★★★☆☆
25	Legal	Planning		TBC
26	Pharmaceuticals	Proof of concept		TBC

Government Virtual Ideas Incubator

Together with the Digital Minister, Margot James MP, I led a meeting on 23 May to seek a collaborative commitment from industry and academic organisations to participate in, and contribute resources to, a virtual incubator for government ideas. A plan is slowly emerging, which

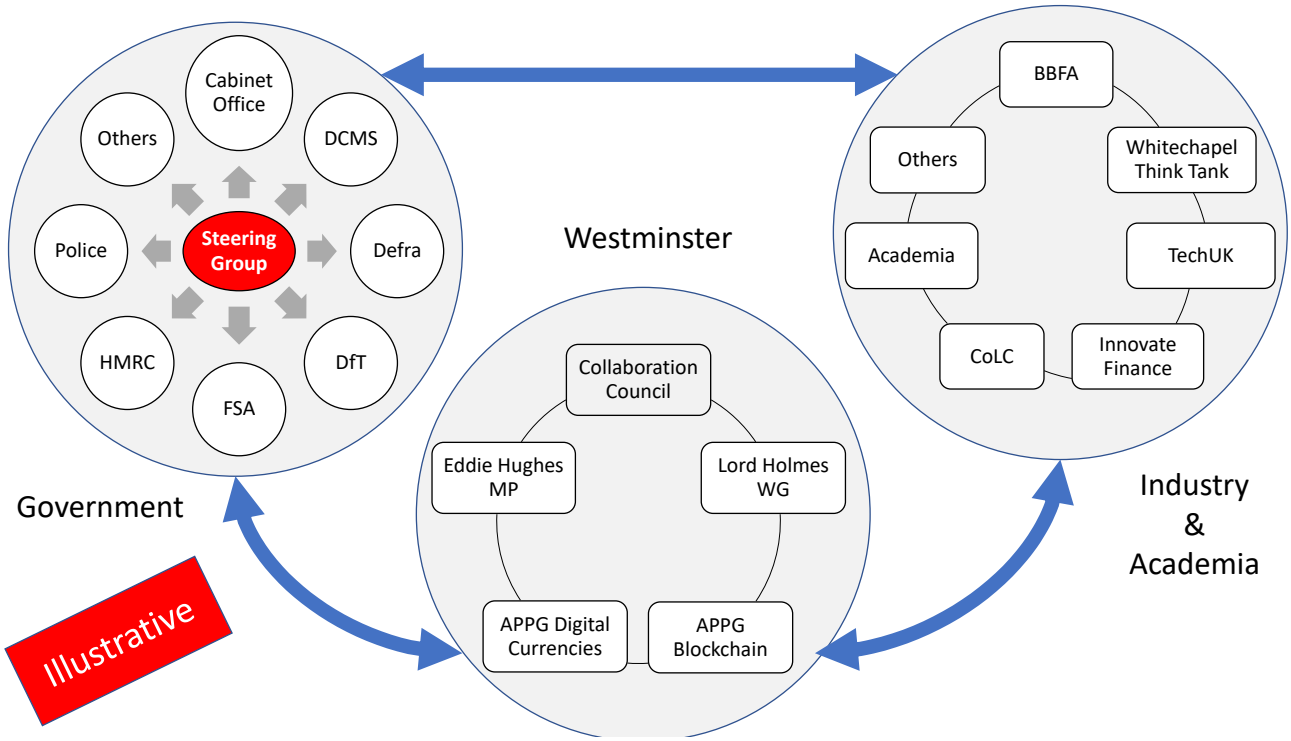
will require some form of collaborative governance, the shape of which will depend on the operating and funding models.

Collaborative Governance

Collaborative governance recognises the importance of competition but excludes it from collaborative activities. Importantly, any collaboration involving government, industry and academic institutions must recognise that any party is normally and simultaneously a customer and supplier of data. This is a radical departure from the traditional approach within government, which misleadingly views government organisations only as customers and industry only as suppliers.

In any digital economy, government organisations are (or should be) not only consumers or recipients but also important providers of fundamental, quality data. This dual role is recognised in some parts of government, such as NHS and GDS Registers, but there is at present no sustained government focus or mechanism to grow or disseminate a culture to provide and consume shared data simultaneously, and to be mutually dependent on quality data.

The conceptual collaborative governance model that has been articulated since publication of my report is illustrated in the diagram below. The elements relating to Westminster and to Industry and academia now exist or are coming together. The elements relating to government – in particular a central steering group or coordinating body – have yet to be formed. Without them, there is a risk that the substantial progress made since November 2017 will stall. The willingness of industry and academia to collaborate with government, and to contribute time and resource for that purpose, depends on reciprocal engagement and collaboration from government.



BBFA is a neutral, not-for-profit, membership-based governance body tasked to enable secure collaboration across industry and with government organisations. It has a background in identity management, secure collaboration & information sharing, cybersecurity, surveillance, privacy, Internet governance and DLT. It is a registered EU H2020 research programme partner. Its members include government, industry and, soon, academic organisations. It is continuing to grow

in terms of national and international participation, industry sectors and use of emerging technologies.

BBFA

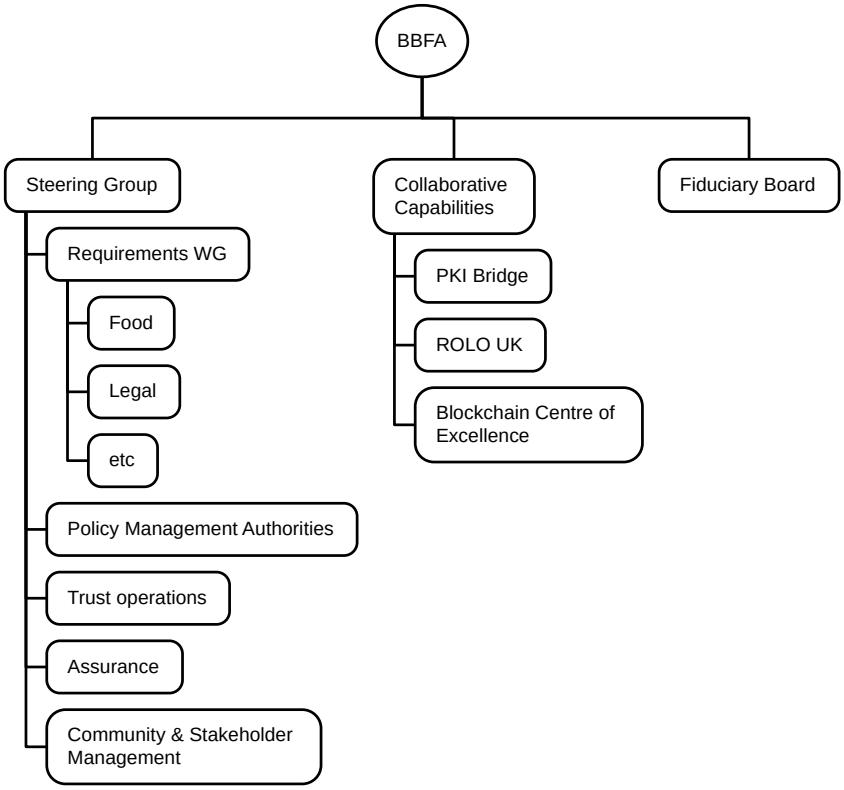
Its collaborative governance is based on:

- Communities of trust with transparency
- Shared objectives, shared risks, shared liability and shared benefits
- The ability to develop and operate collaborative capabilities, used by all, in a not-for-profit model, avoiding many constraints of competition law and government procurement rules.

Its organisation comprises:

- A fiduciary board of directors
- A Steering Group of members, who act like trustees for members' interests and own the collaborative requirements, and which oversees:
    - Requirements working groups, which generate collaborative requirements
    - Collaborative Policy Management Authorities and Technical Design Authorities.
    - Trust Operations for specific collaborative capabilities
    - Assurance, enforcement and trust repair
    - Community and stakeholder management
- Collaborative capabilities, each operating in a not-for-profit model to meet the community requirements in accordance with Common Policies and standards. Three capabilities are in development:
    - The UK Public Key Infrastructure (PKI) Bridge to support the federation of existing PKI certificate authorities in UK and internationally, so that high assurance PKI identity credentials can be accepted across borders and organisations.
    - The UK Register of Legal Organisations (ROLO UK) to provide a register of all UK organisations doing business on the Internet with comprehensive, authoritative data sufficient for legal and business purposes.

- The Blockchain Centre of Excellence, in which BBFA is potential partner, to provide business-centric education, training and executive awareness, and a blockchain accelerator programme.



International Collaboration and Agreements

BBFA has MOUs with Republic of Korea's largest PKI certificate authority, to enable British companies to operate digitally in RoK supply chains under Korean law, and with Switzerland's Crypto Valley Association (CVA) for British cryptocurrency and DLT operators. It is working towards similar arrangements with organisations in leading blockchain and DLT nations, including Malta, NL, Singapore and USA.

BBFA is facilitating the engagement of APPGs with similar bodies in other nations, including the US Congressional Blockchain Caucus and the Australian Parliament's Friends of Blockchain.

BBFA has informal links with organisations in AT, AU, BE, BU, CA, CN, DE, EE, ES, FI, FR, GI, HR, IE, IL, IN, IT, JE, JP, LT, MT, MY, NL, NO, NZ, PK, PO, PT, RO, SE, SG, TR, US.

BBFA is active in international standards, providing experts and editors to:

- ISO JTC1 SC27 – Information Security Technologies; for cybersecurity, identity & privacy
- ISO JTC1 SC17 – Machine readable documents; for passports and driving licences
- ISO TC307 – Blockchain and DLT

UK DLT Showcase

The UK DLT Showcase originally planned for 3-4 December 2018 in London has been rescheduled to mid-2019. This will allow more time for government and the financial sector to participate and

demonstrate blockchains and DLT in collaborative use. The current list of candidate demonstrators is above and will change. I am pleased to support it, together with the Lord Mayor. The collaborative organising committee includes City of London Corporation and BBFA.

Upcoming Opportunities

Borders

Supply chains cross borders. Many sectors and organisations have significant legal and market-driven requirements to improve accountability and traceability from end to end (production to consumption), and to link the item or product to the logistics (pallet/container) and transport (vehicle/plane/ship). These are significant complex tasks, requiring volumes of detailed data, mostly in real time. As increasing numbers of sensors are deployed in packaging and transport systems, so the volume and speed of data is growing. Data velocity is key to the future. This data has value and needs to be strongly protected against increasing criminal data theft and corruption.

However, the reality is that there are big differences between industries. Paper systems dominate in many industries, including in UK, which inhibit data velocity. Today, most abattoirs in UK rely on paper records and most international airline cargo systems can only see one or two steps into the chain because of its paper-based documentation, so they cannot guarantee what is in a cargo.

Prior to Brexit, the UK was much the same as everyone else. Post-Brexit, the UK will have an increased burden of proof to satisfy to its new partners and allies. The UK must find a way to be at the forefront of digital accountability and traceability, from end to end, across borders. If UK is to avoid BSE-type risks for food exports and imports, then HMG must get organised to help relevant government and food industry organisations collaborate to share quality digital data.

Examples where UK could benefit from taking a collaborative leading role in using DLT include:

- NL Rotterdam and KR are moving ahead with maritime container tracking. The top eight UK port authorities are engaging, but they need stronger UK government support, linking to the supply chain data. Transport for the North starting to engage with this process, as is the Greater Manchester Chamber of Commerce.
- IATA is looking for ways to improve cargo handling and logistics visibility in aviation. Greater UK participation and practical innovation would be welcomed.
- Informal discussions between industry, law enforcement and the Irish Government have recognised that goods movements across the NI border are mainly agricultural and food products. They also recognise that food traceability best practice technologies and data could be a leading contributor to any new cross-border Customs processes, starting with the end-points in the chain and securing both the physical (items) and logical (data) together, and automating points in the chain.
- Many major airports are struggling with passport controls and airline passenger screening, due to the increasing demands of passenger movement and the inadequacy of existing paper-centric gating systems. Standards are being developed, but they are taking too long. So new collaborative innovations are taking place, such as the DLT-based World Economic Forum Known Traveller Digital Identity (KTDI), where NL and CA will be the first nations to pilot immigration for some of their citizens without using passport documents at the border. A second pilot with Asian nations is being organised. Discussion on a third pilot involving the US and UK has begun, but it has not yet been possible to find a suitable point of contact inside the UK government. This contrasts with recent letters from Heathrow executives to ministers, highlighting a wide-scale underperformance of border controls, and expressing concern at potentially increasing harm post Brexit.

- Airspace management and drones. The use of drones, nationally and internationally is increasing, including across borders. The potential benefits are huge, for logistics, farming, marketing, emergency services, traffic management, environmental monitoring, pylon maintenance, fisheries, immigration, airport protection and more. Drone sensors will provide more and richer data. However, the cases of misuse and criminality will also grow, if left unchecked. Dynamic drone airspace and flight safety management will become a reality, requiring drone identification and data in mission. A dynamic authoritative register of drones and their capabilities, their licensed operators and qualifications, and their purpose for use, plus their flight plans in controlled airspace, would significantly enhance the beneficial use of drones and reduce misuse. Most of the underlying technology exists already. This could be underpinned by a blockchain to provide legally admissible authoritative evidence of drone movements and authorisations, and provide a basis for the airspace management and enforcement.

Economy

The Industrial Strategy states "Governments in successful economies have recognised their strategic power and leadership role, allowing them to coordinate and convene efforts to develop and disseminate new technologies and industries" and for commerce "We know that the earliest adopters of new technologies are able to reap the greatest rewards in terms of additional jobs and increased revenue" HMT, Bank of England and others are exploring the current economic value and future potential for UK financial services. However, the economic value of collaborative data deriving from trade, business (all other sectors), data driven efficiencies and particularly second order societal benefits remains relatively unexplored. Examples include:

- Applying within government organisations, leading industry practice in increasing end to end visibility of products and services in supply chains, each tailored to individual consumer requirements, cutting out waste, speeding delivery and increasing customer convenience.
- Providing feedback data in the supply chain. There are many examples. E.g. The FSA DLT pilot instantly feeding back the private medical data of an individual cow at slaughter to the farmer, so they can better manage their cattle and costs.
- Reducing health costs and improving peoples' lives. Reducing instances of obesity would considerably reduce diabetes 2, improve an individual's mental, social and financial health. Empirical evidence indicates that poor food choices (particularly by DWP beneficiaries and low-income families) are likely to increase obesity resulting in physical and mental health issues. 23%[8] of the UK population is likely to be referred to the NHS for mental health during their lifetime and this figure is worsening, partly because any reduction in an individual's wellbeing[9] impacts the wellbeing of those closely connected, particularly a spouse and children. Other regions in UK see potential in the DWP benefits payment pilot in Manchester, which uses DLT. Academia and health organisations see significant savings in rising health treatment costs by investing more in nutrition and food buying choices. Two second order benefits include encouraging the citizen to be an asset to the nation, not a dependent, and giving people a real quality of life. These are huge benefits.
- Exploiting Building Information Management (BIM). Many countries seek to reduce costs and waste in infrastructure projects. Lord Maude of Horsham, as the Cabinet Office Minister, championed Building Information Management (BIM) where a building's design is

[8] NHS GP working data.

[9] Combination of physical, mental, societal and financial health, all of which are interconnected and depend on a sense of belonging within a community.

created in software and linked to the real component parts. However, projects still suffer implementation problems because there is no single source of truth during the implementation to which all contractors and constructors can refer. Linking BIM with DLT, the DLT provides that single dynamic view, resulting in significant savings in cost and time – as has been proven in NL. Construction companies in Greater Manchester have expressed interest, through its Chamber of Commerce.

Myths and Misconceptions

DLT is an emerging and rapidly evolving family of technologies. Through efficient management of data identifiers, it has the potential to deliver substantial benefits. It enables legacy and new systems to interoperate, promoting simplification through data re-use and the elimination of redundant manual reconciliation processes and back-office functions. It supports value exchange, with evidential quality data providing greater resilience in relation to evidence of provenance and ownership of assets, and it provides a sound basis for smart contracts and business automation.

However, realising those benefits requires collaboration, and that in turn depends on participants having sufficient confidence in the technology to commit to proofs of concept, pilots or scaled up applications.

There is a material risk of confidence in blockchain and DLT being impaired by commentary and concerns that tend falsely to equate DLT with Bitcoin and other cryptocurrencies. Equally, there is a risk that the practical application of blockchain and DLT might be undermined by the inaccurate, though widespread, use (including in legislative text and definitions[10]) of terms such as "immutable" which lead to the identification of intractable legal risks that can, in fact, be overcome by technical means or through properly informed decision-making. Consequently, a key element in the terms of reference of the working groups established since publication of the report has been to identify, analyse and address such myths and misconceptions.

Energy and Environmental Cost

In January 2018 Alex Hern of the *Guardian* reported on a Credit Suisse briefing note[11] which focused on the energy-intensive nature of Bitcoin mining, commenting:

> Burning huge amounts of electricity isn't incidental to bitcoin: instead, it's embedded into the innermost core of the currency, as the operation known as "mining". In simplified terms, bitcoin mining is a competition to waste the most electricity possible by doing pointless arithmetic quintillions of times a second.

The article acknowledged the possibility of switching from the essentially competitive "proof of work" approach that earns miners the right to validate the next batch of Bitcoin transactions, but observed that while competitors were talking about a move to "proof of stake", that shift had yet to occur. As regulated sectors invest increasingly in DLT, so they require greater legal certainty and non-repudiation in transactions, which is resulting in a shift from "proof of stake" to "proof of authority" based on a strong identity management capability, which is far away from the anonymity built in to Bitcoin and many cryptocurrencies. The advent of proof of authority significantly reduces risks and costs to all parties, including government services.

---

[10] https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/

[11] Alex Hern, "Bitcoin's energy usage is huge – we can't afford to ignore it" (*The Guardian*, Wed 17 January 2018) https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

The concerns expressed in Alex Hern's article related solely to Bitcoin and other cryptocurrencies. However, the perception that blockchain and DLT is inherently and inevitably associated with heavy demand for electricity and computing power tends to inform more general discussion of the technologies, feeding scepticism about their viability.

That conflation of concerns was evident in relation a DWP trial project, which was carried out pro bono by a company GovCoin - now called Disc - during 2016. That project saw 20 to 30 participants being paid their benefits through an app using DLT. In a June 2018 response to a written question, DWP Minister Kit Malthouse reported that the application was "not viable due to limited take up potential and the expenses it would incur". That written response was reported[12] as a statement that blockchain *per se* was regarded by the UK government as "nonviable" for welfare and benefits. Observations on the DWP pilot were then directly (but erroneously) associated with Dutch Central Bank experiments relating to its "Dukaton" prototypes[13] for financial market infrastructure, and with concerns about high energy consumption. In reality, the pro bono Disc pilot in Manchester has grown to more than 150 beneficiaries, with more user take-up, and attracted the interest of other local government bodies who recognise tangible benefits, such as instant payments (vs 3 days through the banking system), voluntary user spending controls and reduced operating costs. The technology is undergoing significant technological and user control enhancements and could potentially link to other initiatives to provide further synergistic benefits.

GDPR and DLT

The General Data Protection Regulation (GDPR) came into full operation on 25 May 2018. Commentary on the new law[14] included the observation that there is an inherent tension between the operation of distributed ledgers and the protections afforded to personal data by GDPR.

There is a clear concern in relation to "permissionless" DLT, where the replication of data to each new node would constitute a transfer of any personal data held on the blockchain. Transfers outside the EU/EEA would immediately run into the prohibition set out in GDPR Article 44, requiring either an adequacy decision, the use of model clauses or binding corporate rules or reliance on an Article 49 derogation. Transfers within the EU/EEA might also encounter legal problems in the absence of GDPR-compliant controller-to-processor clauses.

From a legal perspective, those GDPR issues may be intractable in relation to personal data held on "permissionless" blockchains. However, that does not mean that there is a wholly intractable problem if viewed from a technical, rather than a legal, perspective. Firstly, the issue is far less acute in relation to "permissioned" and geographically controlled blockchains. Secondly, in any case it is possible to avoid the occurrence of GDPR problems by ensuring that no personal data is stored on, and distributed from, the blockchain. That position may be attained either through careful differentiation between "on-chain" and "off-chain" data, or through technological solutions such as "zero knowledge proof".

The key practical point is that identifying a potential problem (whether legal, environmental or cost-based) does not necessarily mean that the problem is insoluble, or of such magnitude that it undermines the value and potential of a proof of concept, pilot or larger project. In many of the cases we have encountered since publication of the report, collaborative and cross-disciplinary

[12] https://financefeeds.com/uk-sees-use-blockchain-nonviable-welfare-benefits-system/
[13] https://www.dnb.nl/en/news/news-and-archive/DNBulletin2018/dnb376502.jsp
[14] https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/

discussions have allowed accurate assessment of issues, identification of viable workarounds, and management of risk – separating myths and misconceptions from practical reality.

That experience has underlined the point that concerns relating to particular architectures and applications do not necessarily apply to others. Consequently, we consider it a key role of the collaborative working groups formed since publication of the report to inform discussions relating to potential proofs of concept and pilots within government, helping to identify and accurately evaluate risk factors and points of potential concern that might dissuade government from engaging with such projects. For that to work, we reiterate a key point made in the report:

> *DLT works across multiple organisations, so collaboration is essential. For the UK to be more digitally mature and able to leverage the opportunities of DLT, industry experience highlights four major next steps:*
>
> - *Organising for collaborative action;*
> - *Communicating to raise executive awareness;*
> - *Implementing and using collaborative or shared capabilities; and*
> - *Learning by doing.*

Industry and academia have already committed to collaboration and await the establishment by government of an effective internal collaborative Steering Group and working groups that are also able to collaborate with industry groups for strategic, national benefit.

Identity and Security

Economies are increasingly interdependent. Increasing legal, regulatory and commercial requirements exist for accountability and information protection. Information protection requires access control, which, in turn, requires:

- Authentication. Prove to me that you are who you say you are;
- Authorisation. Prove to me that you have the permissions necessary to do what you ask;
- Accountability. Can your organisation prove this to me?

These provide the basis of trust and for an organisation to be considered trustworthy. However, authentication is not just about a person, it can also be about an organisation, a device, a component, a piece software or a piece of data. Often, it can be a combination of a person (employee), an organisation (employer), device (mobile) and component (SIM). DLT is able to track all these identifiers, and the valid or invalid relationships between them, making them visible with appropriate levels of control.

Unfortunately, the UK is now in a position where its needs for digital identities of many kinds are increasingly important, and most citizens, consumers, employees and employers recognise the urgency of this, yet historic myths, misconceptions and incompetence have tainted the UK political and government landscape regarding identity, frustrating the possibility of an open dialogue and collaborative action. Companies are looking for alternatives, such as the Estonian e-Residency card. The only practical way ahead for the nation, in which industry can have any confidence, is through industry-led collaboration with specific government organisations, backed by the government, resulting in a unified approach for the nation as a whole. To that end, four collaborative working groups are now working on different aspects of identity and have agreed to develop both a strategy and an outline plan leveraging existing capability. GDS has supported the participation of the Verify programme providers.

My report highlighted that HMPO has authoritative data for some 70 million British citizens, which could be used to validate citizens at high assurance using secure mobile applications [and gain an

industry-estimated £500 million in revenue for HMG]. This would reduce the level of risk stemming from fake UK passports, directly reducing identity fraud and cybercrime, benefitting police in Action Fraud, AMBERHILL, GENESIUS and operations such as FALCON. Progressing this is an essential pre-requisite for the national exploitation of DLT and a top priority for many industry sectors. However, despite high level discussions and a Home Office ministerial call[15] for greater collaboration through its Assured Identities initiative, the Home Office has so far proved reluctant to collaborate in any discussion or working group when there is an abundance of compelling evidence and urgent need to validate passport data, with privacy and user consent, throughout most of the economy and society.

Not everyone has a passport. The government should start to look at suitable solutions for citizens without a passport, particularly those that receive government payments and benefits, and those that are unbanked or digitally excluded. Industry is exploring better and more interoperable collaborative solutions.

ROLO UK

Accurate and authenticated organisational identity data is a second fundamental requirement, because everything digital links in some way to an organisation. So that organisation needs to be trusted. Fake organisations are a significant problem. For an increasing number of business and cybersecurity reasons, there is a need to establish one or more interoperable registers for organisational information to which other organisations can refer digitally for efficient, affordable and safe operations in the Internet Age.

Entry in such registers would not necessarily be a legal requirement. Voluntary adoption may be driven by factors such as:

- Competitive advantage;
- Contractual requirements; and
- Regulatory risk and cost management.

DLT is well-suited for such registers and is already being considered or adopted in countries around the world. The ROLO[16] specification, which originated in the UK, is being taken forward in some nations and is intended to become an international standard. ROLO UK is key to the UK's digital future. The development of ROLO UK has begun, with the participation of selected government organisations, banks and law firms, plus NL government and JP industry organisations who have similar goals. Discussions in several other countries and Interpol are ongoing.

The ROLO UK WG is about to expand to include more organisations that understand the fundamental importance of authoritative organisational data for a digital economy, including GDS Registers in the Cabinet Office. Discussions with the NAO are ongoing to find a way in which the NAO could assess the potential benefits of ROLO UK to public sector organisations. This is a good example where either the HMG DLT Steering Group or the Collaboration Council (if they existed) could assist the NAO in making this happen.

PKI Federation

Trust across a community of multiple organisations requires federation, based on common policy and collaborative governance by the community's stakeholders. The opportunity exists in the digital environment to use and create much more powerful and robust identity management tools that provide authentication whilst protecting privacy. At high levels of assurance, the foundational

[15] Assured Identities initiative, 28 February 2017.

[16] Register of Legal Organisations, for all organisations in a country doing business on the Internet.

cryptographic technology is public key infrastructure (PKI). Organisations using PKI can federate to provide, share and potentially simplify the secure delivery of services or products.

As mentioned in my report, in the UK, only the police service currently operates a large-scale PKI federation for authentication in accordance with international standards. With best-practice collaborative governance, this could be re-used to support many UK government services, including the emergency services. It could federate nationally with industry and internationally in areas as broad as trade, border controls or migrants and refugees, with other allies who have similar PKI federations today. Examples include the USA, France, Korea and the Netherlands. The potential exists to support more secure overseas trade, international aid and trade finance.

In combination with blockchains, PKI federation could provide enhanced services extending to the privacy-friendly handling of identity data.

Conclusions

Quality data has huge value. Nearly every organisation in industry and government is both a customer and a supplier of data, and needs to behave accordingly and responsibly, or their reputation and competitiveness will suffer. The quality of decision-making depends directly on the quality of available data and information. Newer DLT helps bring a big step improvement in the management of data quality within and across organisations, removing costly mistakes and disputes, eliminating costly intermediaries and introducing order of magnitude improvements in speed and scale.

The message of Collaboration, Communication and Commitment for DLT is translating well into action, participation and initial investment. There is a realisation of the vital importance of quality data and the potential of DLT to improve significantly our national situation, resulting in a growing willingness to collaborate. This industry-led growth continues, with pockets of good collaboration by parts of some government organisations, which needs to grow too.

Actions by the CSAG to progress collaboration and DLT are warmly welcomed, however there is an urgency to establish and encourage practical, working collaboration. A HMG DLT Steering Group is needed to engender commitment and momentum, supported by a small collaborative secretariat for day-to-day focus and coordination, internally and externally. Underlying barriers include a lack of executive awareness and informed digital leadership within and across organisations. Establishing such collaborative governance internally and collaborating externally with industry partners and international allies would accelerate progress.

Industry also has much to do as it holds and processes orders of magnitude more data than government. It can do more to encourage and implement assured interoperable mechanisms for accountability and traceability, based on detailed, automated quality data. Government can use and benefit from such industry efforts.

Further progress updates will be provided.

The essential next steps are:

1. To continue growing the community-based working groups, and the number of organisations and activities, including proofs of concept, pilots and operational systems.
2. To establish a senior government Steering Group to encourage, lead, coordinate, communicate, collaborate and educate across government – and collaborate externally.
3. For the communities to document their Catalogues of Collaborative Requirements;
4. To develop the national-level collaborative capabilities for trust and interoperability required in an industry-led, government-supported, not-for-profit model, including:
    a. ROLO UK as one of many registers of authoritative data;
    b. The UK PKI bridge as one of several interoperable federated identity management capabilities;
    c. Building on the Police Identity & Access Management System to provide high assurance standards-based digital employee authentication across all HMG, interoperable with many international allies and industry partners.
    d. Enabling some 70 million British citizens to validate their passport data digitally and securely, to prove their identity for legal and other reasons at work, in society, on the Internet and travelling. To find a similar solution for those without passports.
5. To draft legal text that could enhance existing national legislation, to help UK compete internationally.
6. To establish training and education with briefings to raise executive awareness, particularly in government, and for wider awareness.
7. To enhance coordination, communication and the existing industry-led, government-supported collaborative governance.