
# Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation

# Foreword: Lord Holmes of Richmond

We have written this report to highlight the need, and significant opportunity, for government to take a leading role in the practical testing and application of distributed ledger technologies (DLT) across the public and private sectors in the service of the UK, its businesses and its citizens. That broad ambition is encouraged by advances in DLT since Sir Mark Walport's ground-breaking *Distributed Ledger Technology: Beyond Blockchain*[1]. That report identified DLT's potential to transform the delivery of public and private services and to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust.

With the right mix of leadership, collaboration and sound governance, DLT offers a step change for service delivery in both the public and private sectors. By reducing data fragmentation and enhancing traceability and accountability, DLT promises cost-savings and efficiencies on a scale sufficient to impact national finances. DLT's facilitation of common business processes, based on common and authoritative reference and transaction data, provides the means to derive improved returns and efficiencies from past and future investments, including legacy systems, through enhanced interoperability.

Sir Mark Walport's recommendations, which we endorse, focused on ministerial leadership, research, standards and the need for proof of concept trials.

Our working hypothesis is that DLT can play a valuable part in enhancing the delivery of government services to the citizens of the UK, in securing the UK's competitive position as a global leader in technology-based innovation and in protecting the security of government and citizens' data at a time when both are increasingly under threat. Testing that hypothesis depends on effective collaboration within and between the public and private sectors, recognising:

- The increasing integration of the public and private sectors in the provision of data-driven services to their citizens and customers; and
- The opportunity afforded by DLT for government organisations to rethink and transform the way in which they understand and respond to the needs of their nations' increasingly large and diverse populations.

The Walport report was well-received both within the UK and by governments around the world. However, momentum in the UK has been disrupted by the pressing need to prepare for the demands and opportunities of Brexit. Meanwhile, great progress is being made in jurisdictions such as Singapore, the Netherlands, Australia, Dubai and Oman where active and sustained government involvement has driven initiatives to understand how DLT might be leveraged to their best advantage. This report seeks to re-energise and refocus UK government attention on DLT's potential so that we can accelerate our own digital maturity, enhance the productive capacity of our businesses and benefit our citizens.

[1] *Distributed Ledger Technologies: beyond blockchain*, Government Office for Science, 2016, available at: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review


The UK has already taken a leading role in developing legislative, regulatory and institutional measures that provide a sound legal framework within which DLT development can take place. The Investigatory Powers Act 2016 sets new standards for internet-related law enforcement, while the Data Protection Bill looks beyond the EU's General Data Protection Regulation (GDPR) to create and protect rights in relation to personal data before and after Brexit. The UK is well-placed to include DLT as a key component in its digital strategy, yielding benefits for national and individual security.

DLT is shorthand for a broad set of technologies and applications. It is broader than, and certainly not synonymous with, Bitcoin and other cryptocurrencies or with novel capital raising techniques such as Initial Coin Offerings (ICOs). Those topics are properly the concern of the UK's monetary and financial regulatory authorities, and are outside the main scope of this report. Instead, we focus on the benefits to society, government and the economy that may be delivered through alternative applications of the underlying DLT technologies. Some may have a financial aspect. For example, within local government DLT may be used to provide alternative mechanisms for local currency and crowdfunding initiatives. However, as DLT technologies mature, we consider that they can be used to great effect in addressing many other forms of value, data and asset exchange. With government involvement in mind, our focus is on permissioned DLT applications[2] .

In our view, based on matching public policy delivery challenges facing government with the traceability and accountability and other capabilities offered by DLT, areas of particular opportunity for the UK include:

- Border control, customs, trade and immigration;
- National security, criminal investigations, police and public safety;
- Taxation and benefits payments;
- Health assurance, patient record management, drug safety and treatment accountability;
- Food standards and safety, traceability and accountability;
- Privacy, cybersecurity and counter-fraud; and
- Public procurement, contracting, payments, visibility of spending and asset traceability.

This report outlines the use case in each of these areas of opportunity, including their associated risks and challenges, requirements, opportunities and enablers.

While our focus is on one technology, or more correctly group of technologies, we are fully aware that others – 5G, Cloud computing, Artificial Intelligence (AI), Robotics and even Nanotechnology – are all developing as fast and may indeed compete for future time and investment. We see DLT as potentially enabling the better exploitation of those technologies, and also as a means of overcoming some of the issues associated with the existence in government as well as in many commercial entities of "legacy" systems developed piecemeal and over time using different software formats and access systems.

We do not consider that, for the moment at least, the requirement is for large-scale government funding. There is already considerable commercial interest and investment in DLT. That commercial interest brings the skills and resources and the agile and innovative style best suited to

[2] Sir Mark Walport's report includes definitions and a glossary explaining key terms relating to DLT: *Distributed Ledger Technologies: beyond blockchain*, Government Office for Science, 2016, available at: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

the development of DLT as part of an increasingly interlocked and complementary constellation of operating systems and technologies. It also means that industry already has collaborative groups ready and keen to engage with the government's digital leadership, user organisations and experts.

The opportunity is for government to bring to bear its broad interests, leadership and expertise to stimulate and shape commercial development in the public interest.

We recognise that DLT's relatively early stage of development means there is no guarantee that it will fully deliver on its promise or that it will work more efficiently at scale than other available or emerging technologies. However, we do know that DLT lies at the heart of much current development activity and investment decisions across the sectors in the UK, and globally amongst the UK's economic and technological competitors. We also know that many of the use cases being explored by businesses show potential, if fully developed and proven, to bring significant benefits to individual citizens, to commerce and to government. That development and proof can, we believe, be achieved only through significant and practical collaboration. Government has a crucial role to play as credible convenor of public sector, regulatory, commercial and academic expertise.

For ministers in each area of opportunity there is a need to take collaborative action and a real opportunity to protect, advance and secure the UK's digital leadership. This report is a call to action for all those with the interests of the UK at heart to join in that collaborative effort and the practical steps proposed so that the benefits of DLT can serve as a common good for UK businesses and citizens, public sector and Government alike.


## Our key recommendations

We call on the UK government to:

1. Create cross-departmental arrangements, with senior-level sponsorship, to improve the quality and use of information in decision-making and the delivery of public services through active, coordinated and sustained collaboration to leverage DLT and the enablers described in this report.
2. Establish and support working groups to address each area of significant opportunity identified in this report.
3. Form a neutral organisation working across government to provide objective policy, architectural and technological expertise for information management and project management linking to government priorities in the Industrial and Digital strategies.
4. Link collaboration within government with existing collaboration amongst industry partners, including the Whitechapel Think Tank and the BBFA, and with international allies.
5. Raise executive awareness across government, including at middle-management level, of opportunities to evaluate, test and pilot potentially relevant applications of DLT.
6. Provide active government support for the UK Showcase in May 2018 as a means to demonstrate the maturity of UK's digital capabilities, approaches and proposed services.
7. Deploy the UK's academic community. to provide government with support for experimentation, proofs of concept and knowledge transfer.
8. Develop a strategy to:
    a. raise citizens', consumers' and businesses' understanding of the nature of digital change, digital identity management and DLT's role in their digital future; and
    b. build on that raised awareness through targeted training and education.
9. Develop a Learn by Doing and preparedness-to-fail culture through controlled and limited-scale pilots.
10. Form a steering group/working group structure to ensure sustained collaboration, coordination, direction and momentum.


## Why DLT is a game changer

As digitisation connects more organisations they gain the ability to share more information, more quickly and more widely. However, managing each organisation's traditional transactional ledgers across a community or supply chain comprising hundreds, thousands or potentially millions of organisations becomes exponentially more difficult and costly. Without significantly improved levels of transparency, traceability and trust the risk of mistake and costly delay mounts.

For example, many major national and international projects have had no choice but to operate massive and centralised registers or databases, updated perhaps twice daily, in the knowledge that more accurate and up to date information would exist elsewhere in the supply chain. DLT changes this by providing all parties with the correct rights or permissions and automatically have a local copy of the register or database.

DLTs are typically (but not exclusively) enabled by blockchains. A block is a set of data records, as in a database or spreadsheet, which is cryptographically sealed and linked to the previous block. The sequence of linked blocks (the blockchain) cannot be altered without breaking the chain. Consequently, an unbroken blockchain promotes trust and provides extremely strong evidence that the data has not been altered or tampered with. This means that DLT is good for managing unique identifiers that have to be used consistently across multiple systems and organisations. It ensures data integrity and avoids data fragmentation, allowing far greater integration of new and existing systems and improved organisational effectiveness.

DLT models differ. In most, transaction data is fully replicated on each participating computer or "node" so that parties see exactly the same information at the same time. In other models data partitioning is applied so that each node contains only the transaction data relevant to or within the permissions allocated to that node. In either case risk, costs and the scope for dispute are significantly diminished through the removal of onerous reconciliation issues as each party can be confident that they have the same data.

### Strengths and opportunities

DLT is a game changer because it provides new levels of:

- Transaction data assurance as any attempt to tamper with or alter data will be evident;
- Distributed data at scale, reducing complexity and requiring minimal or no intermediation;
- Focus on outcomes and the delivery of end-user benefits enabled by a connected and assured digital infrastructure;
- Efficient management of data identifiers, enabling more systems to interoperate;
- Cross-organisational harmonisation and simplification through data re-use and the elimination of redundant manual reconciliation processes and back-office functions;
- Support for value exchange with evidential quality data providing greater resilience in relation to evidence of provenance and ownership of assets;
- Embedded use of advanced cryptography that provides built-in assurance of data origin and integrity; and
- Support for smart contracts and business automation.

## Weaknesses and threats

- DLT is a rapidly developing, though immature, technology;
- There is a small, though growing, pool of expertise;
- Inaction or too poor investment decisions;
- Business and investment cases based on financial models that focus on net present value (NPV) and free cash flows and do not recognise or put a value on broader and longer-term benefits that may accrue as a result of collaboration;
- There is a need for collaborative governance based on a community of trust;
- Initial Coin Offerings (ICOs) are controversial and risk reputational damage to DLT;
- There are several unresolved issues and unproven aspects of DLT that require further research;
- DLT depends on the preparedness of two transacting parties to share information, which may be determined by the availability and application of strong authentication of users and assets to ensure high quality, authoritative data at the point of initial input;
- Given that ledger participants may be transacting across different legal regimes dispute resolution carries legal risk;
- The interaction of DLT with data protection laws such as GDPR requires close analysis. Compliance may require "permissioned" or access-controlled DLT, which are the focus of this report, rather than the "permissionless" models which underpin Bitcoin. GDPR issues include reconciling "immutable" ledger entries with the data subject's rights to rectification and erasure and with the need to ensure that international data transfers are lawful;
- The value of "immutable" ledger entries depends in any event upon the initial quality of the data. DLT is good for maintaining quality, but cannot overcome poor data quality at the point of input; and
- The creation of DLT platforms will be heavily dependent on IT budgets which for many large organisations are continually under pressure with regulatory demand and "Business as Usual" fixes which account for an estimated 70% of typical IT budgets.

## Enablers

Clearly DLT is not a silver bullet, nor do we pre-suppose that other technologies cannot deliver similar benefits. It is, however, a new multipurpose technology in the digital information toolbox, and one that is gaining a degree of traction across industries and business processes. To realise its potential DLT requires other tools or enablers. They include:

- 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;
- Collaborative governance across sectors and organisations, focusing on shared benefits, information sharing, coordination, innovation and a facilitative approach to regulation;
- 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":
    - Authentication (prove you are who you claim to be);


    - Authorisation (prove that you have permission for what you are requesting);
    - Accountability (prove who did what, and when);
- Interoperability and assurance based on international standards;
- Data 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;
- 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;
- Training and education of citizens and others envisaged as end-users in the broader community.

In May 2018, there is an opportunity for us to put on a UK Showcase including many collaborative demonstrations of DLT in action targeted at delivery issues in both private and public sectors. We urge broad government engagement with and support for that event so that we can meet the Chancellor's stated intention that Government "be ambitious as it works to make the most of the incredible potential of the tech sector, to break down the barriers facing entrepreneurs and to drive future growth".

## What does this mean for public service?

In common with the private sector government faces the problem of how to manage an increasing quantity of data stored in a variety of databases and in different format. Government and public-sector data is of varying age and complexity and its use is subject to many legal, privacy and confidentiality restrictions. Many departments have already made good progress in improving the inevitable "legacy" problems and it is clear that sound strategies underpin the move towards "canonical registers" and the Gov.Verify programme run by the Government Digital Service.

DLT can complement and enhance that work by providing an extra layer of connectivity and capability, not only allowing identity verification and authentication to take place, but also allowing subsequent use of data to be controlled in a transparent and auditable manner. A thin operating layer enabling that connection can not only leverage the usefulness of existing data sources but also be the location in which data protection rights and obligations can be implemented, audited and assured.

Perhaps even more fundamentally, DLT presents us with an opportunity not just to consider how we might make what government currently does better, but to rethink what government can and should be doing to promote democratic engagement and the welfare of UK citizens and to stimulate and strengthen the UK economy.

The legitimacy of government and the terms of the social contract have long been predicated on the "bargain" between a central authority guaranteeing safety and property rights through the enforcement of laws in return for the citizens' agreement to obey that law, to accept the imposition of sanctions for breach and to provide government through payment of taxes with the means to meet its side of the contract.

DLT alters that traditional relationship between government and citizens. Its distributed and decentralised trust mechanisms offer the prospect of contracts being agreed, settled and audited without the need, or with diminished need, for an operational central authority. To a certain extent it


establishes transactional data about government as a public good. Trust protection and compliance monitoring are central attributes of DLT. Anyone who needs and is permitted, to know about a transaction having taken place can access that knowledge in real time, with full assurance, automatically, and with no additional processes required.

Consequently, in addition to the practical use cases set out in this report, DLT prompts a policy – and perhaps even a philosophical – debate about the role of government within a new "smart social contract" and about what "distributed democracy" might mean for the UK, its citizens and its governance. DLT provides a real opportunity to consider how technology might enable:

- A reduction in the "democratic deficit";
- Greater responsibility and accountability in our public institutions;
- Greater social and financial inclusion; and
- Greater trust between citizens and the state.

## How can Government benefit from industry experience?

Industry has been exploring DLT for several years, resulting in a large body of experience from which practical lessons can be learnt. The financial services industry has been particularly active in the DLT space, including:

- Identifying a large number of candidate use cases;
- Producing many technology prototypes; and
- Allocating appropriately-targeted funding to specific projects and to strategic investments in DLT start-ups.

There have also been important advances made by trade associations in producing foundational DLT standards for financial products. The most notable progress has been in DLT industry initiatives in capital markets where collaboration is already at the heart of their ways of working. This section identifies three example global industry DLT initiatives where banks are contributing input and guidance; it also highlights lessons learnt that could potentially also benefit government DLT initiatives.

> ***Example 1***: The International Swaps and Derivatives Association (ISDA) is a trade association which works to make the global derivatives markets safer and more efficient. This has historically included developing standardised legal documentation (such as the ISDA Master Agreement) and business information exchange standards (such as the Financial products Markup Language (FpML)). ISDA recently expanded its remit to also include establishing a common set of processing and data standards that all participants can access and deploy in order to enhance consistency and interoperability across firms and platforms. ISDA is working with its members to develop the ISDA Common Domain Model, which will provide a standard representation of data, events and actions that occur during the life of a derivatives trade. **This bold standardisation initiative will provide a common foundation for realising the full potential of new technologies, including distributed ledgers and smart contracts.**
>
> ***Example 2***: The Depository Trust & Clearing Corporation (DTCC) is a post-trade market infrastructure company that provides clearing and settlement services to the financial markets. DTCC is currently upgrading its Trade Information Warehouse (TIW) by building a

derivatives distributed ledger solution for post-trade processing based on existing TIW capabilities and interfaces with technology providers and market participants. The DLT solution should permit further streamlining, automation and cost reduction across the industry by eliminating the need for disjointed, redundant processing and associated reconciliation costs.

*Example 3*: CLS is a financial institution that provides settlement services in the foreign exchange (FX) market. CLS is currently developing a new bilateral payment netting solution, built on a distributed ledger platform. Clients can access it via their existing SWIFT systems or directly by hosting a blockchain node on CLS' network. The solution should eventually allow clients to drive operational process efficiencies and reduce risk.

The lessons learnt from these global industry DLT initiatives include:

- The key enablers of DLT include common business processes, common reference data, and common transaction data across participants. Implementation is easier where these exist – as with the examples above – though requires clear senior executive sponsorship, and a commercial and operational model that delivers value;
- Extensive collaboration is essential at all stages of the project life cycle, from gathering and articulating initial requirements to software testing and on to solution deployment and use;
- Market infrastructure incumbents can help the speed to market. This can include leveraging existing membership organisations to accelerate network effects and leveraging existing governance policies and procedures (for example, dispute resolution protocols);
- Service operators can potentially support networks where the participants are at different stages of maturity in relation to DLT. This could include hosting the technology for participants that are not yet willing or able to host their own. To maximise ease of use for particular participants, DLT may even be accessed via existing industry-standard message formats;
- Trade associations can leverage their members to both define and drive the adoption of standardised processes and data for their particular business domains. Process and data standards are foundational for smart contracts;
- Legally-enforceable smart contracts can be constructed from standardised smart contract code governed by standardised legal agreements. Such agreements can potentially include suites of counterparty agreements, network agreements, overriding rule books (such as clearing rule books);
- Key benefits of DLT include process simplification, rationalisation of infrastructure and operations and risk reduction. It is therefore relatively easy to identify many existing inefficient processes as candidate use cases that could benefit from DLT. However, it is much more difficult to construct viable business cases, particularly when taking account of the effort required to integrate with existing systems and the timeline to migrate off and decommission legacy systems.

These lessons learnt within global industry DLT initiatives could potentially benefit government DLT initiatives. They could be applied throughout project life cycles, ranging from the initial scoping and shaping of approaches to accelerating the speed to market and solution deployment.


Collaboration also brings broader economic advantage. UK industry is, for now, a significant force in relation to DLT innovation. However, the UK may soon find itself outperformed and overtaken by countries whose governments have engaged with industry to support innovation and to create an environment that attracts investment and technical talent. The UK has a significant, but time-limited, opportunity to harness and promote home-grown DLT innovation by:

- Collaborating with industry sectors to maximise the early benefit to government; and
- Supporting industry's innovative capacity and use of DLT.

## How can Government promote and realise these opportunities?

The hallmarks of advancing digital nations[3] 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.

Independent assessment of the government's digital maturity should be established as a priority, with strong participation of the National Audit Office and Office for National Statistics, reporting to the nation and Parliament. Such assessments, conducted regularly, would provide the basis for measuring tangible progress, assessing the impact of projects and comparison with the maturity of other leading nations.

The UK requires greater executive awareness of the importance of verified and high-quality information as the basis for improved decision making, and of the transformational nature of DLT, across and within government and industry organisations, to achieve a necessary change in approach.

Citizen, business and consumer engagement is also required. Citizens, businesses and consumers create, use and manage information, but with widely varying levels of safety and consistency. Government support for wider communication, training and education would promote greater understanding and personal responsibility for digital identity.

### Collaborative governance

Most organisations depend on the ability to share information under stated and agreed terms of control with customers, suppliers, partners and allies; organisations and people are simultaneously suppliers and users of controlled information. There is significant shared interest for the purpose of shared benefits (in addition to competitive benefits). However, there are also shared risks. The management of shared risks and benefits requires a collaborative governance model based on a

[3] Described in Government Office of Science report "*Distributed Ledger Technologies: beyond blockchains*".

common policy, procedures and mechanisms enabled by interoperability, trust and assurance together with the legal framework for acceptance that supports real world implementation and use.

To ensure that the UK succeeds digitally, the government should establish collaborative governance arrangements across government organisations internally, and also externally with allies and partners, with a focus on information sharing under control.

Collaborative governance is required across any community. This applies across government organisations and industry sectors, as well as across communities of communities. Effective collaboration permits the achievement of shared benefit at a shared cost. Individual organisations can attain strategic benefits at a fraction of the cost of trying to do something alone.

## DLT as a core component of the 'algorithmic government' vision

DLT provides trusted data and analytics infrastructures to maintain public records and transactions, and to manage laws and statutes. Combined with an upper AI layer DLT provides a feasible framework to redefine public services in a decentralised, lower cost, more efficient, and personalised manner. DLT underpins technologies like chatbots to engage citizen enquiries, robo-advisors to support civil servants, IoT to collect high-quality real-time data and manage the public physical infrastructure, behavioural and predictive analytics to gain enhanced insights into public sector challenges. Potential areas of opportunity include real-time monitoring of public opinion, real-time performance measurement of public services, intelligent assistance for service delivery and citizen support, modelling and forecasting of future service demands, 'smart' design/planning of the environments, and minimising the costs and redundant work in running administration and back office operations.

## Digital Trust - Authentication, Authorisation, Accountability

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, making them visible with appropriate levels of control.

Accurate and authenticated organisational identity data is a fundamental requirement, because all other forms of identity link in some way to organisational data. Fake organisations are a 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 electronically 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[4] specification, which originated in the UK, is being taken forward in some nations and is set to become an international standard; the development of ROLO UK has begun.

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

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

### Improving interoperability and data quality

As more common unique identifiers become available, so government has an increasing opportunity to use them to improve both:

- The interoperability between systems, which helps to evolve systems and improve data coherence across the community of systems; and
- The quality of information within those systems.

As more regulations are created, so there are increasing requirements for legally-compliant and authoritative sources of data attributes (including unique identifiers), which any regulated organisation can easily access with confidence. Some of these authoritative sources will be in government, and they must have very high data quality. Examples include NHS NINO (person), HMPO (passport), Ordnance Survey (address) and Companies House (company). Authoritative sources could be underpinned by the tamper-resistant and tamper-evident attributes of DLT.

### Data analytics

Data analytics technologies are advancing rapidly and offer huge potential as an enabler. However, their ability to become a significant enabler depends on overcoming two major challenges:

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


- No amount of analytics can compensate for a lack of accurate, timely and authoritative data at the point of input. Bad data cannot be made good, just through analytics; and
- Complying with privacy regulations, notably GDPR and the UK's Data Protection Bill. Although enablers exist to anonymise, pseudonymise or encrypt data and also to manage consent where required, there is a pressing need to understand and address the interaction between distributed data and the protection of data subject rights, such as the right to rectification of inaccurate data, or the "right to be forgotten" once the specified basis for lawful data processing no longer applies. DLT applications also require careful assessment to ensure that replication across DLT does not amount to an unlawful international transfer of data.

Another enabler would be to link payments data to non-payment business processes, particularly for tracking purchased assets. The linking can be done on a privacy-friendly DLT. Law enforcement and public safety rely increasingly upon data analytics to manage risks and to understand threats. Trusted data is essential to these purposes, and DLT can improve the trustworthiness of shared data.

### Connected world

People are increasingly using personal mobile technology to manage their lives and day-to-day interactions. The point has been reached where these devices are becoming a person's digital proxy in cyberspace through which they carry out complex and often highly-regulated business transactions as well as social interactions. The smartphone and future personal devices must be secure and safe - able to encrypt and protect data, and to authenticate users. DLT is a major enabler for supporting authentication, authorisation and accountability in a mobile environment, working right down to the smartphone and its user, particularly if it is applied consistently across the range of government, social, financial and other services that most directly affect or support daily life.

## From collaboration to implementation

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.

### Organise for collaborative action

Organising for collaborative action requires a small core group of influential organisations to create the beginnings of a community that can grow through attraction. Organisations should want to join in order to achieve shared benefits with minimum shared costs. Government can assist by establishing an internal collaborative working group that is also able to collaborate with industry groups for strategic, national benefit. Industry has proven collaborative governance models that government can re-use. Government and other public sector contracting bodies also have access to flexible


procurement structures, such as innovation partnerships which allow carefully phased and structured collaboration to develop solutions not readily available in the market.

We ask government to establish its internal governance working group as soon as possible, and to engage with industry, including the Whitechapel Think Tank and BBFA, before 4 January 2018, to support preparations for the UK Showcase on DLT taking place in May 2018. This is to support:

- The creation or further development of working groups in each of the areas of significant opportunity. In each case, these working groups are expected to have sub-groups to cover:
    - Collaborative requirements;
    - Interoperability – policies, procedures and data;
    - Trust – policies, procedures and mechanisms for accountability and traceability; and
    - Technical and implementation activities;
- The engagement of these working groups with industry partners and allies in ongoing and future activities;
- Preparation for the UK showcase on DLT taking place in May 2018;
- The development of a growing community-of-communities for innovation, to promote a more collaborative strategic approach, providing guidance, coordination, awareness and communication and developing and embedding collaborative capabilities.

In addition, the government should continue to consult with industry players to explore how each department could be quickly up-skilled or provided with resources to conduct experiments or proofs of concept, within an overarching government strategy to improve efficiency and transparency through DLT.

One of the challenges for information-centric collaboration is cross-organisational corporate memory, which requires a pool of senior, experienced technological and policy experts. The UK government currently has no such entity but instead relies on hiring external expertise and consultancy services. Consequently, it experiences difficulty in retaining the benefit of experience and learning outcomes from particular projects and in applying those lessons to good effect elsewhere.

The government of the Netherlands has recognised that such a fragmented approach results in a steady drain of hard won knowledge. To address that threat they have formed a highly-respected, capable and neutral organisation called Interim Rijk, which works across government to provide objective policy, architectural and technological expertise for information management and project management.

Interim Rijk's professionals work across the full-width of the government organisations to support complex projects and programs, especially in the functions of a project or program management and in-depth expertise in information management and innovative use of digital technologies. Clients can thus temporarily and quickly have the right information-centric expertise at senior level. One consequence of Interim Rijk has been a significant rise in cross-organisational collaboration and capability re-use, reducing costs, risks and time. We recommend that government should consider the establishment of a similar body for the UK.


## Cross-sector knowledge transfer consortium

UK universities should also be more visible in the conversation since they can provide a major support in embracing latest developments in data science to improve public decision-making and service delivery mechanisms as a whole.

The UK academic community can provide government with major support for experimentation, proofs of concept and knowledge transfer. A potential knowledge transformation consortium could provide the essential thought leadership in the field by creating an eco-system for co-creation and testing of ideas, involving researchers, policy-makers, and the GovTech companies. The activities of the consortium might include bi-monthly seminars, innovation sandboxes, GovTech TechSprint 'hackathons', and international meetings.

UCL's recently-developed proposal along these lines in collaboration with the Universities of Cambridge and Oxford received considerable interest from government departments including Cabinet Office, DCMS and BEIS; and also the industry partners including Meganexus/Interserve, GlassAI, Adarga, Oculus Defence, Neoncentury, Thomson Reuters, PWC, and Microsoft. If supported by senior political leadership, we believe this might be a good kick-start to expand the conversation.

## Communication and executive awareness

Executive awareness, including at middle-management level, is an important success factor. It is essential for setting the strategic direction and organisational tone, and to guide the investment and operational decisions essential for rapidly evolving digital capabilities internally and externally. It underpins government leadership.

General communication is essential to raise citizens', consumers' and businesses' understanding of the nature of digital change and DLT's role in our digital future. Within organisations, this should be backed by training and education.

## Implement and use collaborative capabilities

Collaborative capabilities are those capabilities that need to be available for use by everyone or every organisation in a community, typically for national, government and global industry supply chain uses.

Existing collaborative capabilities provide the basis for further development. They include:

- Trust. High assurance PKI federation, based on international standards, to allow organisations to collaborate and share sensitive information under control. The police IAM (Identity Access Management) is compliant and has the potential to meet this requirement across all the public sector organisations, as well as to federate with industry partner communities and a number of international allies;
- Authoritative company data. Develop ROLO UK for the UK, based on the existing specification. Access legally admissible and authoritative company data in other countries via commercial providers; and
- Authoritative location data, building on existing examples of best practice such as the Unique Property Reference Number (UPRN) in Ordnance Survey's AddressBase.

## Learn by doing – pilots

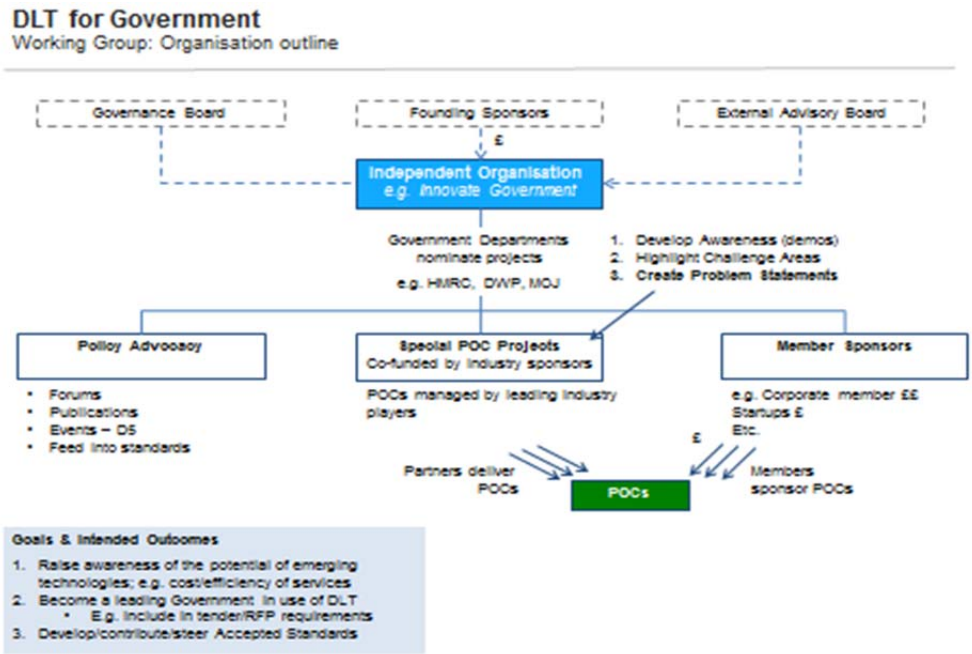
The nature of digital disruption means that organisations have to "learn by doing". Proofs of concept and collaborative pilots will be essential to de-risk and optimise ongoing development and innovation, and to give credibility to business cases and financial forecasts. Another benefit is to develop the relationships that underpin the collaboration and community.

## Governance

There is a clear role for "the entrepreneurial state" to brigade together the work that is going on in the UK in individual large corporates, in collective bodies and in small Tech start-ups. It can provide a safe place in which public policy delivery problems can be matched with the wide range of potential solutions that are under development or actually in implementation.

Based on an open, collaborative and scientific methodology solutions can be tested in "sandbox" conditions in short sharp experiments and learning generated regardless of success or failure. A sensible steering group/working group structure would ensure that the necessary coordination is enabled and forward direction maintained.

An outline of the proposed structure would be:



# SPECIFIC USE CASES AND AREAS OF OPPORTUNITY

## Border control, customs and immigration

26 different government organisations have an interest in the operation of the border. The Cross-Whitehall Border Planning Committee beings together 31 bodies to consider the interdependencies applicable to cross-border trade and traffic, ranging from customs declarations and regulatory compliance checks to food standards and immigration control.

Brexit requires stronger but frictionless land, sea and air border controls based on access to trusted and authoritative data about travellers, employees, vehicles, ships, aircraft and their cargoes. The UK shares those needs with major allies and industry partners including the Netherlands for Rotterdam (Europe's largest port), the Republic of Ireland for our only land border and the US, European and Commonwealth nations for aviation.

### Risks and challenges

- Lack of traceability and accountability in supply chains;
- Airports suffer from passport check volumes, fake identity documents and inability to check documents;
- Aviation freight cannot see further back than two or three steps into the freight-handling chain;
- Maritime problems with bulk freight, manifest manipulation, port security and 'box in a box' visibility;
- Maritime difficulties with checking crew and passenger identity documents;
- Land borders and ports lack the physical capacity to cope with volume, speed and cargo visibility; and
- Customs checks are a gating operation and lack early digital visibility of end-to-end transportation.

### Requirements

- Traceability of people based on source data, communications data, device identifiers and better facial matching;
- Transparency as to the source and/or the method through which data has been verified;
- Access to authoritative source data;
- Better use of privacy-friendly technologies that support traceability and user consent, but without disclosing personal data unnecessarily;


- Linking of asset traceability data, backed by authoritative data on organisations, ships, aircraft, vehicles and payments. It should be possible to match a licensed driver to a registered vehicle to an owning organisation (where relevant) to the cargo items to the transportation companies and manufacturers. These should match to customs, export control and safety licences and documents;
- The ability to identify counterfeit products and establish the provenance of valid products; and
- The ability to identify counterfeit documents by validating securely against authoritative data from authoritative sources.

### Opportunities and enablers

- Communication infrastructure and interoperability are reasonably good;
- Data standards exist that can support interoperability and information sharing. They could be more widely used;
- Standards and capabilities for trusted mobile driving licences and passports exist;
- HMPO has authoritative data for some 70M 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]. This would reduce the level of risk stemming from fake UK passports, directly reducing identity fraud and cybercrime; and
- UN, EU and partner nations have programmes for identifying refugees and immigrants, that could be used to increase their traceability in the UK.

## National security, criminal investigation, police and public safety

National security, including our economic resilience, depends on strong physical and digital borders and protection against identity fraud. Improvements in risk detection and prevention could significantly reduce the costs and damage of rising criminal and terrorist activities.

Identity fraud is recognised as the greatest enabler of crime in Europe. In response, major new international banking regulations (derived from the Payment Services Directive, PSD2) set high standards for strong customer authentication (SCA) and for legally-admissible evidence of identity-related events. SCA means authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is). These elements must be independent so that breach of one element does not compromise the reliability of the others. The SCA as a whole must be designed in such a way as to protect the confidentiality of the authentication data. Although PSD2 adopts a "technology-neutral approach", technologies such as DLT are widely recognised as a credible way to meet the exacting standards required for SCA.

### Risks and Challenges

- A general lack of connected and authoritative data to support public safety operations and investigations, about locations, occupancy, vehicles, persons and other entities;
- Rising identity fraud and theft. The ability of criminals to be anonymous;


- Lack of ability to prevent digital evidence from being destroyed and also to access digital evidence in mobile phones and social media, particularly across borders;
- The lack of ability to share sensitive information under control with partner police and non-police organisations, nationally and internationally; and
- Privacy enhancing technologies increasingly conflict with public safety requirements.

### Requirements

- Access to location and occupancy data for emergency services;
- Privacy preserving alerts about victims, suspects and injured persons, particularly regarding mental health issues such as post-traumatic stress disorder and violent tendencies, that could help the emergency services prevent harm to the individuals themselves, the emergency services and others; and
- Greater ability for law enforcement agencies to access personal data in support of criminal investigations.

### Opportunities and enablers

- In the UK, only the police service operates a large-scale PKI federation in accordance with international standards, albeit in a basic form. With best-practice collaborative governance, this could be expanded to support many UK government services, including the emergency services; and international collaborations in areas as broad as trade, defence, policing, border controls or tracking and managing migrants and refugees, with other allies who have similar PKI federations today;
- Link a mobile trusted identity to a ticket purchase for public events, and use it to access the event. Use the identity picture to rule out 'safe citizens' to enable law enforcement agency surveillance to detect anomalies and threats, faster and more accurately. This could be very advantageous in the emerging 5G, IoT and high-density sensor environments in places such as smart cities; and
- Build upon existing relationships with telecommunications built within OSCT, banks and internet companies to enable citizens to use their identity more effectively to be visibly trusted in society as they wish. Being trusted has value, societally and commercially.

## Taxation and benefit payments

The digital financial landscape is becoming more complex and global. Transactional volumes and speeds are increasing and their costs are reducing. However, the levels of risk are increasing, particularly around reckless speculation and cyber-crime. DLT technologies create opportunities to link payment transactions to asset traceability, user accountability and the use of taxpayers' money.

Estonia points the way. In 2016 60% of personal taxes were collected in 3 days and, as a result, Estonia is considering dispensing with personal tax returns because the relevant data is already available to its government. The Estonian ID card, used with Estonia's efficient pan-government information services, has reportedly enabled savings of up to 2% of GDP.

## Risks and challenges

- Company and organisational tax and payments fraud, enabled by cybercrime and identity fraud;
- Increasing international requirements for taxation traceability and accountability of organisations, Persons of Significant Control and Ultimate Beneficial Owners;
- 18 major regulations impacting the financial sector, requiring greater traceability and accountability. Payments Service Directive 2 requires Strong Customer Authentication for consumers, while the Wire Transfer Regulation requires banks to check, as a counter-terrorism measure, that certain information is on a payment message. DLT could check that the correct information flows all the way through the payment chain;
- Poor data quality and unlinked processes that impede the digitisation of benefits, taxation and payments, impacting companies and citizens;
- Siloed behaviours across organisations; lack of collaboration;
- Digital distribution of public money in benefits hampered by financial exclusion;
- Welfare claimants often forced to use cash and therefore pay more for accessing their welfare money, for utilities and goods and for borrowing; and
- Significant resources being devoted to tax collection.

## Requirements

- Greater traceability and accountability. More accurate data and more authoritative data sources;
- Better use of unique data identifiers across government systems and organisations to link sets of data, increase operational effectiveness, and reduce risks and costs;
- Access to electronic means of transacting that do not rely on traditional identity assurance methods or CRA ratings; and
- Faster and more efficient methods of tax collection.

## Opportunities and enablers

- HMRC data rationalisation programme. DWP mobile payments pilot;
- Linking benefits payments to purchase data has shown poor food purchasing decisions that indicate a propensity for obesity and diabetes 2. Helping beneficiaries to make better food choices could improve their health and quality of life, and significantly reduce NHS costs from obesity, diabetes 2 and depression, which at some point is likely to affect more than 30% of the nation's population;
- Offering claimants the choice of electronic settlement through a distributed ledger controlled from their mobile phones could lead to reduced costs, better cashflow management and reduced risk of indebtedness, thus providing better policy delivery outcomes for DWP including supporting claimants into financial independence and providing better value for


money for taxpayers. Beneficiaries could be equipped to make wiser spending decisions helping to improve their mental health, wellbeing and quality of life and social inclusion; and

- Ability to stop payments "in-flight" in case of fraud or a change of benefit status (e.g. the death of a claimant).

Characteristics of this scheme would be:

- Welfare money from legacy benefit claimants is paid into a holding account, though to the unequivocal credit of the claimant. Access to that credit is then enabled by a distributed ledger such that credit can be exchanged with merchants in the "ecosystem" without the need for an actual payment to pass. The cost to the merchant of such transactions would be reduced as they no longer have to incur card interchange fees and the cost to the claimant is similarly reduced as they can access tariffs otherwise only available to those with a credit history;
- Essential suppliers to claimants, such as Housing Associations and utility companies could be included in the ecosystem, guaranteeing their share of welfare monies in return for providing services to welfare recipients and allowing them to provide appropriate discounts and credit terms; and
- Details of transactions would be available to claimants on their mobile phones providing real-time information about sums that remain available to spend. Claimants would also be able to budget for advance and repeating payments, helping them to plan their finances and enabling their welfare money to go further.

Currently this is only available to those in receipt of legacy benefits such as Jobseekers' Allowance. In view of the importance to future welfare provision of the Universal Credit system, and the well-publicised problems, such as rent arrears, that some recipients experienced in the early stages of their Universal Credit claim, further exploration of the extension of DLT to this flagship transformation of the welfare system is desirable.

- Building stamp duty collection into an end-to-end process. Distributed ledger technology can facilitate the creation of an end-to-end platform for registering the purchase of land, equities and other stampable assets which incorporates taxation as an integral part of the process. By providing a ‘golden source’ of ownership that is directly linked to transactions, the technology could negate the need for manual reconciliation by reducing the multitude of systems and processes involved, improving efficiency and transparency. This can enable a number of tangible benefits:
    - Direct customer access to real-time records and balances;
    - Permissioned and controlled access of specific data points to a wider group of stakeholders, for example other government departments;
    - Simplification of transaction processing to encourage improved reporting behaviours across customers; and
    - Reduced fraud due to enhanced control and authentication methods.

DLT can, by using established and recognised standards, work alongside and interface with government systems to provide integrated information and automation.

## Health assurance - patient record management, drug safety

Health services reach every person in the UK, and are responsible for the initial identification at birth. Health data could contribute enormously to other parts of the public sector and to the delivery of public services to citizens. However, opportunities are currently lost because of data duplication and fragmentation within the NHS.

Data duplication and fragmentation adversely affects existing physical care and cost management, and creates further challenges as the need for access to available data for mental and social health care rises.

Technology can help to contribute to the efficiency and savings needed in already strained healthcare system while providing the high-level trust required in this highly-regulated field. For example, DLT could be used to streamline the pre-employment and identity checks mandated by NHS employers. The current time consuming and repetitive manual processes could be done in a fraction of the time with a higher level of trust. In addition it would provide a fully auditable record, facilitating GDPR compliance by putting the end user (in this case the healthcare worker) in control of their own data.

A conservative estimate of 25,000 doctor days a year are currently spent on identity and pre-employment checks with 50,000 junior doctors rotating through positions every three, four, six or twelve months. Creating a federated and trusted digital identity using DLT for doctors would cut the time for this process from thousands to tens of days a year, freeing up doctors to care for patients.

This is not just relevant to doctors but across the one million clinical and non-clinical staff across the entire NHS.

A trusted digital identity for healthcare workers could create extensive possibilities for innovative workforce management solutions such as skill-set matching platforms which could reduce the reliance on agencies. They could also increase the trust and use of remote medicine tools such as tele-health, and play a role in accessing patient data in future where patient health records and data stores will become more common.

In line with the cross-cutting approach recommended by this report, such a digital identity could be re-used for purposes including management of patient records, prescription automation, treatment traceability and for a trusted referee in the community such as a witness for a will or firearm certificate application. It could also be used for paying authenticated VAT and personal taxes.

### Risks and challenges

- Increasing management pressures and societal expectations upon primary care staff resulting in an increasing staff exodus and diminished recruiting;
- Frequent inability to find or access patient records, resulting in additional records being created;
- Lack of visibility of a rising population with mental health issues that impact physical and societal health, leading to family breakdowns and more mental health issues. Trauma related mental health issues are also increasing;
- Difficulty in locating or prescribing drugs in primary care. Problems with drug traceability in the supply chain and in distribution and consumption; drug fraud is increasing;


- Lack of an employee identity management capability that could be recognised for authentication by the emergency services and others; and
- Lack of a patient identity management and authentication capability, including for power of attorney or delegated proxy.

### Requirements

- Ability to give more personal accountability back to patients to family/self-manage expectations and use community support;
- Ability to access authoritative patient record data for physical and mental health according to clinical need, including providing privacy friendly alerts to GPs and from GPs to other professionals;
- Ability to generate quality data as a by-product of normal working, reducing management administration and error; and
- Ability to procure support services collaboratively for primary care, to achieve economy of scale and re-use of capabilities and information.

### Opportunities and enablers

- Across government, health reaches more people in the UK than any other and it is the originator of the National Identification Number (NINO). For person identification and traceability purposes, health data is a key authoritative source, providing the opportunity to improve data quality across the public sector as a whole;
- Health data can provide privacy-friendly alerts to other government organisations, such as emergency services, and the private sector; and
- Health data and the lives of patients could be improved by linking it to other data e.g. benefits payments and food safety. This could significantly increase citizens' wellbeing and reduce NHS costs in areas such as mental health, diabetes 2 and obesity.

## Food standards and safety, traceability and accountability

Food fraud is a global issue, but public awareness is low. As evidenced by the Elliott Review, the UK is at the forefront of countering food fraud in collaboration with US, EU and Chinese experts. However, unlike other highly regulated sectors, the food supply chain is fragmented and there is an urgent need to establish the data-centric means for accountability and traceability across the supply chain to establish a food sector community of trust through which the supply of high quality British food can be assured.

DLT is already making a positive contribution. Local DLTs are being used in some areas, and the Food Standards Agency is seeking to establish distributed ledgers for the UK. Establishing DLT for food traceability across the Northern Ireland/Republic of Ireland border could provide a model for customs and border control in general, which could contribute significantly towards meeting the land border control challenges presented by Brexit.


### Risks and challenges

- The risks of a major food fraud or contamination incident;
- Rising international food fraud;
- Lack of traceability and accountability to assure the safety of all food consumed in Britain;
- Lack of traceability and accountability to assure the quality and of food products for export; and
- Long term damage to the agricultural industry and its regional economic impact;

### Requirements

- To establish strong food traceability and accountability, nationally and internationally, from farm to fork, including animal feed and animal ancestry; and
- To link food traceability to international transportation, logistics and payments, particularly with Rotterdam and other major European ports.

### Opportunities and enablers

- Leverage the national and international progress since the Elliott Review;
- Leverage fishery collaboration with leading individual EU states; and
- Leverage food traceability developments and the agricultural community in the Republic of Ireland and Northern Ireland; this would also link to intelligence-related developments in relation to cybersecurity and cybercrime.

## Privacy, cybersecurity and counter fraud

GDPR comes into operation in May 2018 and includes fines of up €20 million or (if greater) 4% of global annual turnover for serious data protection breaches. However, practical protection depends on the availability of high-quality and interoperable data, shared under strict control and with data flows carefully mapped within and across organisations. Privacy, like cybersecurity and counter-fraud, is greatly facilitated by authentication. DLT provides a degree of transparency that aids accurate data mapping and privacy impact assessment, and so could be a major enabler for managing and sharing data with the required degree of protection and control.

### Risks and challenges

- Identity fraud and theft (persons, organisations, devices, things) are the top enablers of crime. Internationally, there has been an estimated 300% increase in cyber-enabled crime since 2011. Cyber-crime now accounts for approximately 50% of UK crime according to the British Crime Survey;
- The Internet itself is vulnerable to identity fraud and fake technology in many forms;
- Fake companies, domain names and untrusted digital certificates can most effectively be defeated by greater traceability and accountability in registration processes and their use;


- Government security organisations cannot protect the nation as a whole. Our economy and society are at risk. Without greater national collaboration to reinforce government effort, the UK is at risk; and
- The use of digital evidence based upon internet events needs to be assured as increasing amounts enter the criminal justice system.

### Requirements

- Greater authoritative traceability and accountability of persons, devices, organisations;
- Greater ability to detect and track anomalies;
- Greater ability to share sensitive information under control across law enforcement;
- Greater ability to assist citizens in the management of their privacy and protection of their personal data, and to recover from an incident; and
- Ability to assure digital evidence, to access it and adduce it into evidence.

### Opportunities and enablers

- Re-use existing information sharing capabilities, such as NCSC CISP, and its technologies; and
- Use leading company validation capabilities for authoritative data to provide a trust anchor for all company related data and the identification of company Persons of Significant Control, Ultimate Beneficial Owners, Politically Exposed Persons and those on international sanctions lists.

## Public procurement, contracting, payments, visibility of spending and asset traceability

DLT increases transparency, traceability and trust and therefore has the ability to effect radical change in public buying by:

- Improving government and public-sector performance as a buyer by providing greater visibility into and understanding of the entire supply market; and, as a result,
- Potentially enabling moves towards a more distributed model for government and public-sector buying, improving access for SMEs, promoting local growth and supporting regional policies.

Efficient and effective procurement decisions depend on the contracting authority's ability to trust in bidders' identity, experience, eligibility and reputation. DLT provides powerful support, enabling high quality digital identity management, together with a verified record of previous transactions.

Major public-sector departments and agencies have always had difficulty in establishing the identity of contractors and their extended supply chains. Globalisation, outsourcing, offshoring and cost pressures have exacerbated this difficulty, significantly reducing government's ability to see into supply and distribution chains for purposes such as the enforcement of export controls or the assessment and collection of customs duties. Government also experiences difficulties in reconciling electronic payments with assets and services. This makes it difficult to identify, understand and address major financial, informational and cybersecurity risks within those supply chains.


With DLT the provenance of a particular supplier could be verified, allowing contracting authorities to check, for example, that a supplier meets minimum requirements of financial standing, compliance status in relation to tax and experience, or to validate references and prices. Tracking of assets or products also support broader compliance and regulatory enquiries, for example providing assurance in relation to a supplier's working practices in relation to child or forced labour and of its directors, officers or staff in relation to Anti-Bribery issues or compliance with international sanctions.

DLT as a core capability could enable the linking procurement and finance platforms to existing and legacy databases creating a transparent view of government spending. The outcome of this would be the ability to identify greater efficiencies through demand aggregation, price amortisation, specification of requirements etc. It could then have an instrumental impact on payments and the efficiency with which government pays its supply base, notwithstanding the clear benefit of creating full traceability in government contractors' supply chains.

While there are multiple benefits, the potential to improve efficiency in the appropriation of government funds is arguably the greatest. Furthermore, increasing transparency through DLT could also champion the long-sought achievement of policy objectives such as increased SME engagement and success in public procurements. It reduces or eliminates factors that have tended to aggregate spend towards a limited number of suppliers and to favour incumbents rather than supporting procedures and contract sizes that allow SMEs credibly to compete.

This dis-aggregation of government spending, however, should not erode the fiscal benefits seen through aggregation of demand. Instead it should deliver further fiscal benefits through the amortisation of pricing and service delivery reducing waste across the public sector. Finally, the impact of this potential greater distribution is increased competition and therefore increased innovation. This connected chain of impacts is something the UK will require to build a strong economy going forward.

With regards to contracting, DLT and blockchain provide the foundation for "smart" contracts, allowing government to develop an approach to dynamic procurement similar to that underpinning recent innovation in the shipping and manufacturing sectors.

DLT is emerging as a foundational layer in private sector procurement. It is also being explored and embraced by forward-looking governments. In March 2017 Estonia and Finland established the Nordic Institute for Interoperability Solutions, with a remit that includes the development of Estonia's X-Road technology to enhance the ability of organisations freely and security to exchange and reuse data between their respective systems. The projected advantages for procurement are clear. Interoperability minimises the time and costs incurred in populating and managing procurement documents, connecting them with official publications or registries and with contracting authorities' and (potentially) bidders' internal documents and financial management systems.

### Risks and challenges

- Lack of information quality management within information systems;
- Lack of interoperability between information systems within and across government organisations;
- Lack of interoperability and trust mechanisms between industry and government procurement systems, sufficient to support procurement efficiency and effectiveness;


- Lack of ability to manage information quality to make more timely and effective decisions at all levels in an organisation;
- Lack of adequate traceability between the through-life management of assets and services, and the payments for them;
- Lack of good management information, based on accurate data, to inform buying decisions; and
- The desire to iterate solutions to meet existing business needs rather than understanding the root cause of issues with government buying and how DLT could create wholescale change to mitigate them.

### Requirements

- A standard set of unique identifiers for all cross-organisational activities involving public procurement, payments and asset traceability;
- An authoritative source for those unique identifiers;
- A collaborative governance regime, with stakeholder members, to assure and manage those identifiers; and
- An information quality management capability that could embed information quality management in government organisations.

### Opportunities and enablers

- Experience from industry;
- Experience of the US Federal government on the management and mandatory use of unique identifiers, information quality and digital identity management to ensure:
    - Interoperability;
    - Information quality;
    - Asset and electronic payments traceability and trust across thousands of systems.
- Experience of the Estonian government in the development and use of X-Roads to ensure the provision and use of quality information across government; the use of its Estonian identity card and e-Residency card for government and business; and for its use of blockchains for patient records, government procurement, citizen privacy management and value exchange (using Estcoin).

# Sources of further information

## Websites and useful contacts

AddressBase products, Ordnance Survey: https://www.ordnancesurvey.co.uk/business-and-government/products/addressbase-products.html

BBFA: www.bbfa.info

Data for Policy, http://dataforpolicy.org/

Gov.Tech, https://www.pwc.co.uk/industries/government-public-sector/govtech.html

Wall Street Blockchain Alliance: https://www.wsba.co/

Whitechapel Think Tank LinkedIn page: https://www.linkedin.com/company/10001556/

## Articles and reports

*Adopting Blockchain for enterprise asset management*, IBM March 17, 2017: https://www.ibm.com/developerworks/cloud/library/cl-adopting-blockchain-for-enterprise-asset-management-eam/index.html

*Beginner's Guide to Traceability and Trackability*, Food Quality & Safety, September 7, 2017: http://www.foodqualityandsafety.com/article/beginners-guide-traceability-trackability/

*Blockchain for fraud prevention: Industry use cases*, IBM, July 12, 2017: https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/

*Blockchain Technology A game-changer in accounting?* Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft, 2017: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjTz4-J18rXAhWECewKHR4aAvAQFgg5MAM&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fde%2FDocuments%2FInnovation%2FBlockchain_A%2520game-changer%2520in%2520accounting.pdf&usg=AOvVaw0OK3Xavc4oPEgh-oPXAL0Y

*Blockchain: what are the opportunities for Procurement?*, Procurement Tidbits, July 17, 2017: https://medium.com/procurement-tidbits/blockchain-what-are-the-opportunities-for-procurement-d38cfd5446fa

*Bridging the divide: How CLS and IBM moved to blockchain*, CLS: https://www.cls-group.com/document-downloads/bridging-the-divide-how-cls-and-ibm-moved-to-blockchain/

*Close Encounters: the power of collaborative innovation,* Womble Bond Dickinson: *https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/claiming-advantage-collaboration-startups*

*COP23 explores the role of blockchain in climate action*, Daily Planet, November 2017: https://dailyplanet.climate-kic.org/attention-role-blockchain-implementing-paris-agreement/


*Distributed Ledger Technologies: beyond blockchain*, Government Office for Science, 2016: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

*Dubai to use blockchain technology for all government documents by 2020*, Gulf Business: http://gulfbusiness.com/dubai-use-bitcoin-database-technology-government-documents-2020/

*Food You Trust: How Blockchain Will Reinvent the Supply Chain*, Hackernoon, November 1, 2017: https://hackernoon.com/food-you-trust-how-blockchain-will-reinvent-the-supply-chain-1d6ae601ae53

*Gov.Tech - The power to transform public services in the UK*, PWC, September, 2016: https://www.pwc.com/gx/en/psrc/united-kingdom/assets/govtech-report.pdf

*How blockchain technology could improve the tax system*, PWC: https://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html

*Identity and access management (IDAM)*, Defence Information and Systems Agency: http://www.disa.mil/initiatives/identity-access-mgmt

*Innovation and the Application of Knowledge for More Effective Policing*, N8 Policing Research Partnership Catalyst Project, Policing Research Partnership: http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf

*Ksi blockchain*, Security and safety, e-Estonia: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

*Made Smarter*, Review 2017, Department for Business, Energy & Industrial Strategy, October 30, 2017, Gov.UK: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655570/20171027_MadeSmarter_FINAL_DIGITAL.pdf

*Managing the HMRC estate*, HM Revenue & Customs, National Audit Office, January 10, 2017: https://www.nao.org.uk/wp-content/uploads/2017/01/Managing-the-HMRC-Estates-Summary.pdf

*Registers: authoritative lists you can trust*, Government Digital Service, Gov.UK, September 1, 2015: https://gds.blog.gov.uk/2015/09/01/registers-authoritative-lists-you-can-trust/

*Regulatory Technical Standards on strong customer authentication and secure communication under PSD2*, European Banking Authority: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/press-release

*Reshaping U.K.'s National Health Service With the Blockchain*, Nasdaq, March 23, 2017: http://www.nasdaq.com/article/reshaping-uks-national-health-service-with-the-blockchain-cm765582

*Roadmap for a Leading Global Financial Centre in Asi*a, Monetary Authority of Singapore: http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/Roadmap-for-a-Leading-Global-Financial-Centre-in-Asia.aspx

*The characteristics of a register*, Government Digital Service, Gov.UK, October 13, 2015: https://gds.blog.gov.uk/2015/10/13/the-characteristics-of-a-register/

*The power of the UPRN*, Geo Place, available on: https://www.geoplace.co.uk/addresses/uprn


*300% Increase in Cyber Attacks Across the EU*, Novitnite.com, September 3, 2017: http://www.novinite.com/articles/182944/Maria+Gabriel%3A+There+is+a+300+Increase+in+Cyber+Attacks+Across+the+EU

*Using Cognitive and Blockchain to drive innovation at the border*, IBM, November 29, 2016: https://www.ibm.com/blogs/insights-on-business/government/cognitive-blockchain-drive-innovation-at-border/

*What is e-Residency?*, Join the new digital nation, e-Estonia: https://e-resident.gov.ee/

*Whitepaper Smart Contracts and Distributed Ledger – A Legal Perspective*, International Swaps and Derivatives Association, 2017, available on: https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

*X-road*, Interoperability services, e-Estonia, available on: https://e-estonia.com/solutions/interoperability-services/x-road/

I would like to thank those in the UK government, public and private sectors and academia who have supported me in producing this report. They include members of the Whitechapel Think Tank, the British Business Federation Authority and UK Finance. I look forward to their continued collaborative support as the report's recommendations are taken forward. I am also grateful to Barclays Bank PLC and Womble Bond Dickinson LLP for their contribution towards the preparation and launch of this report on 28 November 2017.