Distributed Ledger Technologies in Public Services

Learnings on the application of Distributed Ledger Technologies across international digital public services and their role in *realising Scotland's full potential in a Digital World*

June 2018

Digital Scotland

Scottish Government
Riaghaltas na h-Alba
gov.scot

Preface

This report was commissioned in order to generate ideas and inform our thinking about potential applications and opportunities for Distributed Ledger Technology within Scotland.

The report's authors, Rab Campbell, Gillian Thompson, Peter Ferry and Hannah Rudman have identified international best practice and, through a series of interviews with practitioners and experts, identified the potential benefits of the technology and provided us with food for thought about the way forward. These include opportunities within the delivery of digital public services and for the further development of a vibrant digital economy in our country.

For my part, I hope that this report will challenge us all to consider the practical steps that we need—across all sectors of the economy—to take advantage of the opportunities it describes. Nobody can predict with any certainty what the most significant benefits of any technology will ultimately prove to be, but we can continue to scan the horizon, engage with experts and open ourselves up to new possibilities.

I look forward to continuing discussions about the future opportunities for Distributed Ledger Technology.

Colin Cook
Director, Digital Directorate
Scottish Government

Contents

1. Executive Summary 5
2. Key Findings and Recommendations 6
3. Digital Strategy, DLT in Context 10
4. What is Distributed Ledger Technology? 14
5. Industry Insights 24
6. HOME: Blockchain state of the nation 43
7. AWAY: International Blockchain best practice 49
8. Appendix: Public Sector Interview Methodology 61
9. Appendix: About this Report 64
10. Appendix: Netherlands Use case detail 66
11. Glossary 71
12. References 75

1. Executive Summary

This research report was commissioned by the Scottish Government Digital Directorate in September 2017. Its remit is to investigate the potential benefits of Distributed Ledger Technology (DLT), to the Scottish public sector, thus informing Scottish Government's evolving digital strategy.

Digital life relies on the exchange of information. When data is shared, it may be infinitely duplicated, modified and used in ways unintended by its originator. Identity theft, cybercrime, fake news, and misuse of intellectual property are commonplace, because we have a limited toolset to govern contemporary models of data use and exploitation.

In Scottish public services we identified many processes which continued to rely on the use of paper or web-based substitutes for paper processes. We also identified the importance of effective and appropriate information sharing in enabling cross-government collaboration to improve services for citizens.

DLT makes it possible to register and record, share and transfer value or valuable information in a secure and tamper proof way, to only the intended recipients. DLT is a superset of the technologies popularised as "blockchain". It represents a new opportunity for the creation of natively digital public services.

2. Key Findings and Recommendations

2.1 Findings

This research found an overwhelming international consensus that DLT will have a significant role in underpinning future digital government.

It uncovered a significant global innovation ecosystem focussed on building future digital public services with DLT—spanning government, policy and research, but also driven from the private sector.

Despite a popular narrative of DLT disintermediating central institutions like governments and banks, we found that its most current real-world use cases feature government actors in an extended, more effective, or efficient role.

These focus on DLT's impact on streamlined process and data governance and, in technology terms feature private (or permissioned) shared ledgers.

Beyond this we found future potential for DLT in enabling new public service delivery mechanisms, economic models, and circular economy ecosystems. We note, however, that we found limited evidence of impact to date beyond the public (permissionless) Bitcoin network.

Our research found significant scope and support for the use of DLT in Scottish digital public services. Delivery at scale will require advocacy and leadership within public sector organisations.

We also observed that those states most advanced in considering DLT are small, and that their work is sponsored from the very highest levels of government.

2.2 Recommendations

The overarching recommendation of this report is that Scotland join the international ecosystem as an active participant. This would involve developing a Scottish vision for DLT together with universities and businesses, initiating small-scale projects in the Scottish public sector, and sharing findings with the international network.

Such an approach would include Scotland in the weft and weave of DLT innovation. Scotland enjoys a foundation of research, entrepreneurialism, industry and mature government assets relevant to DLT innovation. The addition of vision, strong leadership and focussed execution could enable positive impact on digital public services, the economy, and in time deliver competitive advantage.

Broad recommendations are as follows:

2.2.1 Envision Commission an expert group representing the Scottish DLT community, and including views of SMEs, industry, public services, academia, financial services and the 3rd sector, to develop a vision for a future DLT enabled Scottish economy.

2.2.2 Plan Building on this vision, enable leadership and a plan with specific actions and measurable goals for digital transformation in Public Services. Take steps to embed deeper knowledge and skills around fundamental disruptive technologies in Scottish public services.

2.2.3 Engage Undertake proactive and co-ordinated engagement with other nations' governments on DLT. Smaller nations are forging ahead. Engagement across central, local government, companies and academia should be co-ordinated with these nations to share DLT experiences and learnings.

2.2.4 Educate Adopt a holistic approach to drive a DLT ecosystem across industrial sectors by educating leaders on DLT. Work collaboratively with Innovation Centres, local and international SMEs, to ensure that Scotland is able to maximise the benefits of this technology through innovative approaches, such as the CivTech® Programme, CodeClan and the University of Edinburgh's new AI and blockchain accelerator.

2.2.5 Deliver Appoint a group of progressive leaders from across the public sector to identify common threads of opportunity to deploy DLT to solve common problems. Provide them with a budget to invest in knowledge and undertake practical steps including proof of concept activities. They should actively scan the horizon, share their experiences in the international network, and accept that though some initiatives will fail this is better than doing nothing and being left behind.

2.3 Suggested practical steps

Based on our research with Scottish public services leaders, we gathered findings on the opportunities for DLT application which are summarised here under the themes of people, process and place:

2.3.1 People

The findings primarily focus on situations where there would be a benefit if people could have more control over their own data. Seven examples were identified:

- making transparent the way public funds are deployed in an untrusted environment
- sharing qualifications to allow people to work more flexibly
- opening existing sensitive data up to more professionals, in a secure way, to help protect vulnerable people
- allowing people to supply relevant data once, in a complex multi-agency environment, to make life easier for people from disadvantaged backgrounds
- securing the Internet of Things (IoT)
- enhancing the data available to allow people to be better cared for at home
- streamlining who has rights to make decisions on how people are cared for

2.3.2 Process

The primary finding is that similar processes are being run across the public sector but there is a need for greater collaboration in considering how they could be improved and/or unified.

There are five generic examples:

- Online voting
- The submission and management of legal evidence
- Licensing
- Asset management across organisations
- Supporting economic development with better data

2.3.3 Place

There are two generic examples:

- the urban environment
- the rural environment

These summarised themes are expanded in a 'Public Sector Interview Findings Summary' appendix which will be made available shortly.

3. Digital Strategy, DLT in Context

3.1 The Scottish Government's Digital Strategy

In March 2017, The Scottish Government published a refreshed Digital Strategy (Scottish Government, 2017) which set out a vision for Scotland as a "vibrant digital nation which could realise its full potential in a digital world".

The strategy identified a policy of continuous innovation and improvement of public services, through a collaborative approach to new technologies which delivers joint action plans across local, central government, health and the 3rd sector.

Blockchain was identified as one such new enabling technology which would be explored in this way, with a further commitment to share ideas and experiences with international governments.

In keeping with this commitment in the Digital Strategy, this report and its supporting research have been completed with cross-government collaboration.

3.2 Report Scope and Deliverables

The agreed specific deliverables and scope of this report were:

- Establishing the benefits and applicable use cases for DLT technology in Public Services generally and in Scotland specifically.
- Establishing current thinking for the use of DLT in public services across international governments.
- Engagement of Scottish Government sponsors and identification of candidate use cases for DLT implementation, and the scope of those use cases across central & local government and health.
- Identification of potential private sector industry input and collaborations.
- Recommended action plans.

This report includes a simplified view of the subset of DLT that are block-chain based trading cryptocurrencies. It presents the context in which DLT may become a useful enteprise technology for solving government and citi-zen problems, and where it presents opportunity in economic development.

It does not attempt to offer the reader a detailed understanding of the coin economy and its trading of Bitcoin, Ethereum, etc. It does not attempt to cover innovation in the Financial Services sector and related innovations in the financial regulatory environment which have come from DLT/blockchain, though it does touch on the Initial CryptoAsset Offering phenomenon.

3.3 Why DLT?

DLT is useful for digital data governance and the exchange of value, or valuable information around public networks like the internet.

In the public sector, such value resides in title deeds, records of life events, licences (to operate taxis, pubs and nurseries), childcare vouchers, parking permits, educational qualifications, and votes.

DLT can automate, reduce transaction costs, increase accountability, and enable markets for these valuable assets and data. This has the potential to transform delivery of digital public services to citizens.

The evolution of DLT can be traced over several decades, with accelerated growth in the last 10 years, and significant activity in public services since 2015. UK Government Chief Scientist, Sir Mark Walport, initiated discussion on this topic in his January 2016 report (Walport, 2015) which set out how DLT could transform the delivery of public services, boost productivity, and reduce costs:

"It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust".

More recently, the House of Lords issued a report: Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation (Richmond, 2017) with a forward by Lord Holmes of Richmond, in which he stated:

"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 offers governments a means to better empower citizens while reducing the cost and improving the quality of the state's provision of services.

A significant and growing number of governments recognise this potential and have embarked on pilot projects to demonstrate reduced cost, improved governance and online safety, and streamlined citizen experiences.

Our research shows that international governments are taking leading roles in realising this opportunity[1] and that although DLT's rapid evolution presents risks and issues still to be addressed, valuable live use cases have now emerged.

With national focus and leadership leveraging its tech, cyber and academic assets, Scotland could join the forefront of this international community[2]. The report's overwhelming recommendation is that Scotland quickly adopts international best practice by developing a vision and commissioning a

1 See section 7 "AWAY: International Blockchain best practice

2 See section 6 "HOME: Blockchain state of the nation

co-ordinated practical action-oriented plan.

In the context of the Scottish Government digital strategy, a cross-government plan for DLT is recommended to realise its full benefits for future digital public services. Specifically, public sector "pilot" activity is recommended below based on input of Scotland's Public Services and industry leaders, with evidence from global industry insights[3].

Outside focussed scope of DLT in digital public services, this report signposts to its role in the wider context of Scotland's economic development; DLT may represent the future of how citizens, consumers and industries interact in a transparent, secure and streamlined manner to form the highest performing economies.

3 See "Industry Insights" section

4. What is Distributed Ledger Technology?

4.1 How did the Distributed Ledger Technologies evolve?

In this report we examine the use and potential of Distributed Ledger technologies (DLT) in digital public services.

In the same way that the category "vehicle" covers the passenger car, the freight ship, and the space shuttle, the term DLT spans a broad set of technologies.

The foundation technologies of DLT can be traced to fundamental cryptography work over the past 50 years[4]. In 2008 a novel scheme called Bitcoin combined some existing DLT tools into an "open public network" with a "distributed trust-less consensus". In the Bitcoin network anyone can join, and can exchange value by 'spending a coin' and agree on who owns what without trusting others in the network.

In the Bitcoin scheme value exchange transactions are grouped into blocks and cryptographically linked together in a block chain.

Since then the word "blockchain" has become part of the popular dictionary, used to describe both the foundation technologies and applications of distributed ledger technologies. This is confusing; there is no clear definition of what a blockchain is, or its capabilities, and the term blockchain infers certain specific qualities present in Bitcoin[5] but not all DLTs.

4 Including the work of Merkle, Diffie and Hellman in the 1970's, and proposals of document time-stamping in the early 1990s

5 As far as the writers can discern, there is no agreement on what qualities are essential to call something a blockchain. For example, we'd note that:

- Though Bitcoin is widely viewed as the first implementation of blockchain technology, many things called blockchain today bear little resemblance to it.
- Blockchains are considered open, democratic and transparent, but in some implementations, transactions are not recorded openly.
- Blockchains are often called "decentralised" but some variants may have only a few nodes.

For this reason, we use the broader term "Distributed Ledger Technology" which is more commonly used in Public Services applications. We refer to "blockchain" only when discussing a specific technology implementation which has these characteristics.

The scope of this document does not include a summary of the many specific DLT platforms. Rather it examines the general utility of their use in Public Services scenarios.

4.2 A simple definition of Distributed Ledger Technology

The simplest description of a distributed ledger is that it is like a spreadsheet, which instead of resting with a single provider, is shared across a network. Every change is replicated, recorded and agreed by everyone.

Physically, the ledger is duplicated across many computers, so it is more difficult to subvert or destroy. Distributed Ledgers use cryptography to make them resilient to attack or unauthorised change. Usually the ledger's cryptography builds up over time so it becomes more and more difficult to hack. This makes it "immutable"—it is extremely improbable that anyone could go back and subvert the ledger's history.

The result can be a more open, transparent and verifiable shared database.

These technologies are based on research and innovation that has been going on for several decades. An important development in 2009 was Bitcoin's innovative combination of approaches (including collating transactions into blocks and cryptographically chaining these blocks together) which solved the "double-spend"[6] problem.

This use for "value transactions", i.e. sending money, enables "trust" without an intermediary.

Bitcoin evolved into a global "public" network; public because anyone can download the software and join in. Speculation on this new asset class drove demand for its constrained supply, and focussed further attention and development. Five years later the Ethereum blockchain was proposed,

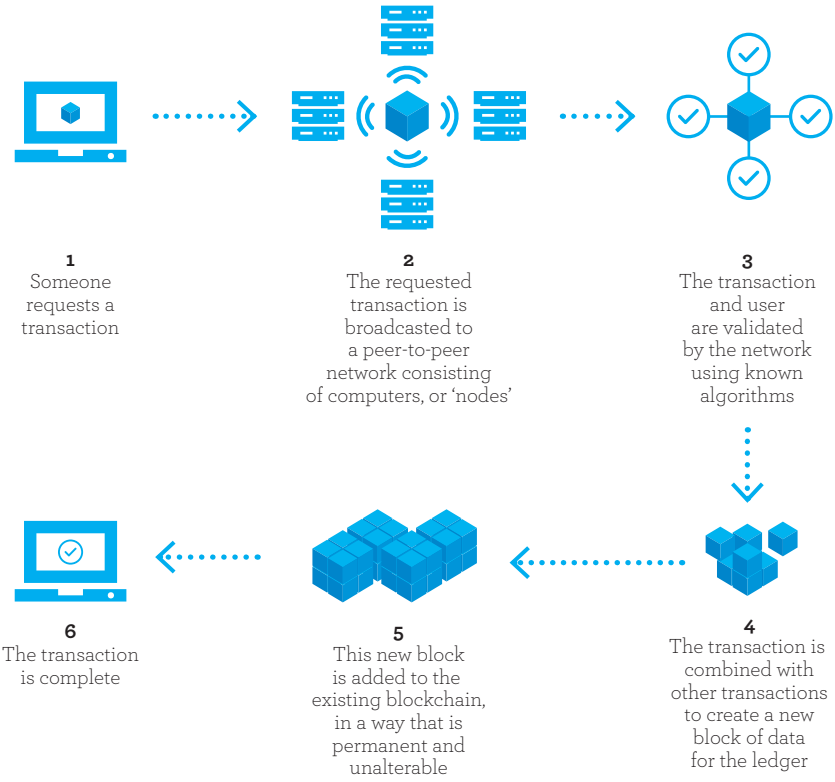
6 The risk that a digital currency can be spent twice. Double-spending is a problem unique to digital currencies because digital information can be reproduced relatively easily.

evolving the idea of autonomous or "smart contracts"; software programs which trigger when specific conditions are met to automate a process or fulfil an agreement.

Further developments have continued in the evolution of DLT technology, in both the "public" blockchain networks, and in private networks where only "permissioned" actors can play.

Likewise, in the past 5 years there has been an explosion in the application of these technology platforms to business and societal problems. "Figure 4-1 Evolution of DLT technology and applications" puts blockchain in the context of development of cryptography and Internet technology.

DLT development and application continues to influence the way we think about exchanging value and assets, enforcing contracts and sharing data.



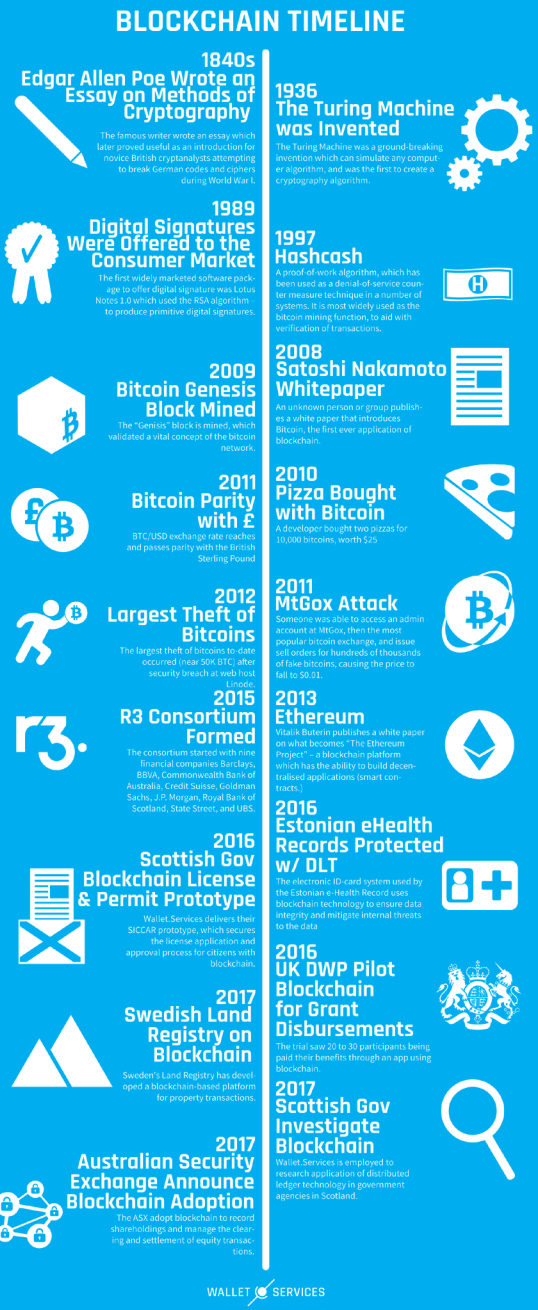


Figure 4-1 Evolution of DLT technology and applications

4.3 How can we use Distributed Ledger Technology in Digital Public Services?

Broadly speaking, Distributed Ledger technologies are tools which can engender transparency and security in transactions and make markets and systems more efficient.

This broad scope has led to a growing diversity of applications, across many vertical industries as diverse as financial services and transportation.

Some patterns of use have emerged. The following is not exhaustive, but we summarise an outline taxonomy of key DLT application themes below in "Figure 4-2 DLT Application Themes", with the specific scope of application in digital public services in mind, to inform our discussion.

Figure 4-2 DLT Application Themes

Streamlined collaboration: DLT can be applied to scenarios where multiple organisations must collaborate to achieve outcomes, but each may only act in a way that all other consent to. Examples include many legal processes such as conveyancing, or benefit and grant approvals and disbursement.

Security and Resilience: DLTs can be more "cyber-resilient" as, simplistically speaking, they deal with encryption and integrity "by default". In addition, their security compounds over time—data can be encrypted and

permissioned, and then distributed to make it more **robust** against subversion or external attack.

Privacy and Confidentiality: DLTs reduce the need to retain multiple copies of sensitive information amongst co-operating parties, so reducing risks of that information being compromised. In addition, they can support sharing and transactions on data while maintaining its confidentiality. Such techniques can be used to let a citizen or organisation enter or generate information once, yet have it shared only appropriately and with minimal exposure. Examples include identity verification and sharing of patient medical records.

Each of the three above points have a role in supporting simplified ***Citizen Experience***, for example where citizens need enter information only once and it can be securely shared across government.

Compliance and Oversight: DLT can be used to track the provenance of all data and interactions involved in completing a process, particularly in demonstrating a "chain of custody" in a regulated process. Examples include traceability in logistics and procurement supply chains, or in managing governance around the process of applying for a taxi license.

Paperless reconciliation: An obvious application of DLT is in banking, where each institution maintains its accounts and their balances. When an inter-bank transfer occurs, the sending bank adds a debit to its ledger, and the receiving bank adds a credit to its ledger. At COB, the ledgers are reconciled to update the correct balances. A shared distributed ledger makes **reconciliation** unnecessary, eliminating an administrative step and improving efficiency.

Registration and Recording: DLTs can produce a **permanent** and **irrefutable** digital record of what happened. **Unique** digital tokens can be applied to **registry of ownership** applications where assets change hands, and in **provenance** applications where it's important to track the origin and history of an asset over time. Examples include land registry and provenance of food and ingredients or precious gemstones.

4.4 Further notes and common questions on DLT

As stated above, the scope of this document does extend to a detailed description of DLT and blockchain platforms in this quickly evolving industry. This section contextualises further details on Distributed Ledger technology in the form of accessible answers to common questions and strikes a "devils advocate" tone to counterbalance any unconscious bias from the writers of this report.

4.4.1 Isn't blockchain over-hyped?

The Bitcoin blockchain became the subject of abnormal global attention as cryptocurrency investment caught the Financial Services industry off-guard and made some early investors very rich. Simultaneously blockchain's "distributed disintermediation" narrative also seemed to catch the popular mood. There has undoubtedly been a case of "blockchain fever".

Enthusiasm around the potential of any new technology must be tempered with recognition of its maturity, shortcomings and risks. Many contemporary applications of DLT are in the early stages of construction and deployment. There is a danger that it will be positioned beyond its current capabilities as a not-yet-fully-mature technology, and in some cases beyond sensible application where no benefit case can be shown above conventional simpler technologies.

However, as of June 2018 it is beyond reasonable doubt that this technology may be used to address real-world problems in industries such as Financial Services, Public Services, and Supply Chain. Academics, engineers, government leaders and business people overwhelmingly agree. Furthermore, consensus has emerged that the DLTs have an important role to play in information security and online privacy.

4.4.2 So what are the risks around deploying DLT today?

The broad category of Distributed Ledger includes some mature technologies, and some still in their infancy.

It may yet be several years before the category can fully meet enterprise

requirements of clear standards, interoperability, predictable roadmap, availability of skills, and readiness for enterprise operations. Also, as the market becomes better defined there are risks from investing in technology from early market vendors who may suffer from inevitable market consolidation.

4.4.3 What do you mean by Public and Private, and why is it important?

"A simple definition of Distributed Ledger Technology " above discusses "public" blockchains such as Bitcoin and Ethereum. In these any party can download and run its software. This joins the network by becoming a "node", validating that any change is legitimate and meets rules agreed by the whole network. Also, a subset of these nodes may serve to secure the network in exchange for the chance of rewards, by becoming a "miner".

In public blockchains miners compete with each other to solve a puzzle. The first to do so gets a reward and is able to "seal" a block of changes, and add a block to the chain. This proof of computer processing effort, or "proof-of-work" is the method by which every node in the network achieves consensus on the ledger's current state.

The Proof of Work consensus algorithm is often cited as a flaw in the Bitcoin public blockchain. Though very effective at making it computationally unfeasible to subvert the network, it also makes its transaction rate low and energy consumption high. Another criticism of Bitcoin is one of privacy—its unprecedented level of transparency means that every balance and all transactions can be viewed by everyone.

DLTs may be considered **Private** (or **Permissioned**), when the above validation and **mining** activities are more constrained to specific actors.

For example, much work in Financial Services focuses around a permissioned DLT called Corda, which requires participants to identify themselves, and uses a "Proof of Authority" consensus where only pre-approved, authorised notaries can make changes to the ledger.

DLT applications in Public Services typically leverage Permissioned DLTs, where only co-operating government actors and agencies or their delegates are authorised to "mine" changes.

4.4.5 Doesn't blockchain waste electricity?

Bitcoin uses a lot of electricity. As explained above a competition is run roughly every 10 minutes where "miners" compete to solve a mathematical puzzle first enabling them to validate and secure a block, in return for a Bitcoin reward.

Bitcoin is a global public network with many individuals and commercial "mining" businesses competing in parallel. It is estimated that each Bitcoin trade or transaction consumes 200kWh, enough to keep a small family home in electricity for a month. Clearly this seems overly energy intensive.

However, advances in public blockchain technologies seem set to address these inefficiencies. For example, the Ethereum blockchain's roadmap will have it move to a far more energy efficient "proof of stake" consensus algorithm.

Typically, "permissioned" blockchain technologies feature a restricted set of users who have the rights to validate the block transaction, meaning that energy intensive competitions are not necessary.

4.4.6 How does blockchain line up with GDPR?

A legal framework for personal data privacy known as General Data Protection Regulation (GDPR) became effective across the European Union on May 25th 2018.

The spirit of GDPR is to strengthen individual control over storage and use of their sensitive data and identity attributes. It places several obligations on organisations around their management of personal data including its access, protection, erasure, and portability.

Opinion varies on whether Distributed Ledgers are a solution to, or problem for, GDPR. On one hand their distributed nature creates many "copies" of citizen data and by design eliminates a single point of control. It is not always clear in a peer-to-peer network who is the responsible "data processor".

On the other hand, some DLT implementations are credited with enabling "privacy by design" where the "data subject" retains control over which actors have access to data, rather than surrendering control of it to another data processor.

A March 2018 report (IBM, 2018) asserted that DLT aligns closely with GDPR's goals of secured and self-sovereign data. It stated a caveat—that only cryptographic hashes of personal data (i.e. evidence of the data's existence and state) should be stored "on chain". This concern focusses on the "append only" characteristics of DLT, and supports the "right to be forgotten" (or the right of erasure).

However, many in the DLT and self-sovereign identity communities, assert the opposite view; that to show data has been "erased" is best demonstrated through cryptography, e.g. that the data has been irreversibly encrypted or that the requisite decryption keys have been put beyond use. This view is elucidated by International legal firm Hogan Lovells LLP in an explanation of blockchain's role in data protection (Hogan Lovells LLP, 2017).

Such a scheme would allow the "destruction" of data in public record-keeping applications where for example in disregarding offences registered and since pardoned or disregarded[7].

We anticipate that greater clarity around the issue of erasure will emerge as regulatory rulings and relevant case law emerges over time.

7 One newsworthy example might be the Scottish Parliaments Historical Sexual Offences (Pardons and Disregards) bill.

5. Industry Insights

During the process of conducting this research, and the discovery of scenarios and priorities in Scottish public-sector agencies, we correlated these ideas with developments in the DLT/blockchain industry and technology. Several areas discussed below were felt to either illuminate, or have pertinence to the discussion of DLT in Scotland.

5.1 Identity

In November 2017 Scottish Government initiated an Online Identity Assurance programme, to develop a "common public-sector approach to online identity assurance" as part of Scottish Government Digital strategy (Scottish Government, 2017). At the time of writing, this programme has just concluded its Discovery phase. It is being conducted on the basis of Open Government principles and we suggest that the observations in this report should be considered as a contribution to its considerations:

Robust online identification is an important foundation in streamlined access to digital services for individuals, government and commerce. It is a critical component in confidence and integrity for digital public services where sensitive or valuable information pertaining to citizens is involved.

Much global DLT activity to date has focussed on digital identity. An evaluation of DLT identity solutions is beyond the scope of this report. However, an exposition of its role in the field of identity, and some context of its current application is presented below.

DLT identity application spans not only identity assurance, but also identity verification use cases such as financial services Know Your Customer (KYC) checks, and verifications of entitlement, certification and qualification. The related topic of secure sharing of personal data is discussed in section 5.2 below.

There has been recent significant capital investment in "blockchain identity" technology start-ups[8], and attention from global tech and NGO consortia such as the ID2020 project (ID 2020 Alliance, 2018):

ID2020's goal is to deliver inclusion and empowerment to 1.1 billion people unable to prove identity hence unable to access critical services and benefits. It is committed to piloting decentralised, user-owned, blockchain digital identity solutions working across national and institutional borders to address the challenge at scale. ID2020 members include the United Nations, Microsoft, Accenture, the Rockefeller Foundation and Hyperledger blockchain alliance.

8 According to global start-up investment analyst CB Insights, "Identity" has been a leading blockchain technology start-up capital investment area in 2016 and 2017 and was a target of $Millions of crowdfunded "Initial Cryptotoken Offering" (ICOs) in 2017.

This attention and investment is informed by several factors:

Firstly, in technology it has been driven by thinking and open standards since the early 1990s, spanning the evolution of decentralised OpenID protocols[9] which has resulted in the "self-sovereign identity" narrative in the 2010s. Much of the blockchain community subscribes to self-sovereign identity principles, and concepts of distributed identity. This vision for digital identity enabling trust whilst preserving individual privacy is articulated in "The Path to Self-Sovereign Identity" (Allen, 2017).

Secondly for the non-specialist it is driven by the "Equifax effect"[10]; the awareness that personal data can be vulnerable when stored in online databases, and a perception that the balance of control over personal data should shift away from institutions, to the user.

The following interviewees contributed to the research for this study:

- Christopher Allen, the architect of SSL and TLS, the protocols which underpin all off global Ecommerce;
- Bill Buchanan OBE, Professor of the Centre for Distributed Computing;
- Stuart Fraser, Founder and CEO of Wallet.Services, who has a long track record in digital identity, including as the CTO of start-up MiiCard, now the Identity Company.

5.2 Sensitive Information Sharing

Sharing information about citizens is fundamental to efficiency and effectiveness of public services. This by no means novel insight was confirmed in the public-sector leader interviews conducted during this research.

9 OpenID and its successors are open standards and decentralized authentication protocols which allows users to be authenticated by co-operating websites eliminating the need for separate login systems with a separate identity and password for each.

10 Equifax suffered a massive data breach in May 2017, losing the driving license, social security and birth dates of 143 Million Americans. 209,000 credit card numbers were exposed as were the utility bill details of 400,000 UK citizens. In the aftermath the CEO, CIO, and CSO resigned.

Sharing of sensitive information and citizen personal data is closely aligned to notions of digital identity. Industry representatives identified examples of services where some sensitive information such as the date of birth or mother's maiden name is used to verify identity through "proof of knowledge before extended sensitive information (like personal preferences, bank account records or salary information) can be accessed"[11]. To grossly oversimplify the fields of regulation, cybersecurity and civil rights, it is retention of this sensitive information that can lead to loss and misuse of the information, the concerns of citizens, and the necessity of data protection regulations.

Blockchain tools provide a means to avoid this sensitive data retention. It allows data owners (such as those agencies responsible for records and registers), to confirm and corroborate proofs of age, education, and entitlement to vote. This "attestation" approach is used by many blockchain based "identity" schemes which build up public-facing verifiable claims over time.

However, even with such shared identity schemes in place, the problems of sharing sensitive information remain. Sensitive information sharing in this context, refers to the sharing of extended personal data between government agencies to allow them to interact to fulfil other governmental service or process.

Blockchain tools fit in here by providing a means to send sensitive data and maintaining tight control over who can decrypt it, whilst in a manner publicly verifiable and regulatory auditable.

Moreover, blockchain can enable "disclosure without exposure" by supporting those cryptographic techniques which can verify certain aspects of sensitive information without giving access to it (like knowing someone is over 18 without having access to their date of birth).

This is one of the bases of much current investigation into blockchain in healthcare patient data sharing work. Professor Bill Buchanan OBE of Napier University, is engaged in preparing a "Trust Architecture for Scotland", building on some of the principles above.

11 This is how public authorities typically protect personal data with a local digital identity to allow individuals to gain access. The previous section discusses distributed identity schemes and the context of re-useable digital identity.

In the Scottish start-up ecosystem, this report's authors, Wallet.Services, are addressing such challenges with their SICCAR platform, an inter-organisation workflow and information sharing platform.

5.3 Health

In early 2017 the North of England Connected Health Cities conducted a proof of concept project with the aim of sharing patient data but with granular patient permissions.

Such projects have the potential to enable patients to give fine-grained consent around which parties can use their data and for what purpose, across the NHS, research functions and pharmaceutical companies.

The project was based on a private Ethereum blockchain used to store preferences and consent, rather than the actual patient data, and confirmed the technical feasibility of this approach.

Subsequently 2017 saw an explosion in blockchain innovation activity targeting healthcare applications. This spans such use cases as the Patient Health Record, device and pharmaceutical supply chain, care delivery, telemedicine, and into every corner of the $27Billion market for health IT solutions.

Much of this has been from start-up companies, evangelical about their technology and its disruptive and positive impact on the industry. Many such organisations have raised funding for software and solution development through Initial CryptoAsset Offerings (ICOs). This approach has driven rapid access to significant capital for idea and solution development but is criticised by many as avoiding the governance and scrutiny of more traditional investment approaches.

By the beginning of 2018 the authors have found 42 Initial CryptoAsset Offerings (ICOs) had been conducted in the health care market, raising $100 of millions across US, UK, Russia, Hong Kong, Switzerland, and Estonia.

By any measure significant investment is being expended on building blockchain use cases in health.

In Scotland one such company is Spiritus Partners, whose founders received £500,000 in Regional Selective Assistance from Scottish Enterprise to

establish the company's software development and operations in Edinburgh. Spiritus apply blockchain to multi-party service record scenarios, and are involved in a proof of concept in collaboration with NHS National Services Scotland and academic support funded by the Data Lab.

In the process of this investigation, the authors established contact with London-based MedicalChain, and Dubai based GlobalHealth. In keeping with normal start-up behaviours, many of these initiatives will fail before delivering any application capable of delivering a production service in a live environment. But the significant investment seems likely to deliver a good learning opportunity and some useful innovation.

Taking the widest possible view, the most concentrated efforts emerging in the blockchain healthcare application space are in patient health data governance, specifically in storage and integrity, record sharing and exchange, and the associated trust and permissioning of data.

One company, Guardtime, based in Tallinn Estonia, use DLT to record all updates to Estonian healthcare records. To citizens, this gives comfort that their data is being used appropriately. They can see its use through the eHealth portal, which professionals are also accessing for their personal or their children's health data, and their reasons for doing so. In this scheme, the actual data is stored in a conventional database. Guardtime's solution integrates at the database engine to create a cryptographic hash each time it is accessed or changed, to deliver a forensic-quality audit and integrity trail, based on a DLT patented by Guardtime (Keyless Signature Exchange). Guardtime are a start-up who partnered closely with the Estonian eHealth Foundation around this solution. The use of DLT in the Estonian model is specifically around audit of healthcare record access—storage, access control and any patient consent is delivered using conventional means.

The following interviewees contributed to the research for this study:

- George Crooks OBE, CEO of the Digital Health and Care Institute Scotland
- Chaloner Chute, CTO of the Digital Health and Care Institute Scotland
- Clinicians from NHS Tayside, including Mr Rodney Mountain, ENT surgeon and lead for healthcare Design and Innovation

- Artur Novek, Implementation manager and IT architect at the Estonian eHealth Foundation

Here in Scotland, the Digital Health and Care Institute (DHI) plans activity around using new technologies to give people easy access to and ownership over their health and care data through a "personal data store" or "personal health record". A 'Connectathon' was delivered in March where the DHI Demonstration and Simulation Environment was launched. We understand that this will provide a "sandbox" in which services and technology can be integrated to develop and demonstrate next generation infrastructure. The DHI has personal connections and ongoing knowledge-sharing exchanges and with Estonian Government and, in particular, its eHealth Foundation, including mutual interactions through Scotland and Estonia based Digital Health conferences, and a 2017 DHI-driven group fact-finding mission to Tallinn.

A workshop was conducted by the consultants on 27th November 2017 with a cross-disciplinary group led by Mr. Jonathan Cameron (Head of Service—Strategic Development) of NHS National Services Scotland. This group included clinicians, software professionals, and NSS Senior Management, with the objective of (a) sufficiently exploring the role, current application areas, and potential impact of DLT and (b) prioritising potential applications across Scottish NHS.

A shortlist of high-potential healthcare application areas were identified by attendees.

- Asset lifecycle and transparency (medical devices)
- Visibility of prescription across health provision
- Collaborative service provision (in crises management involving health, social care and police, and in cross-health-board scenarios)
- Linking patient data for safety and efficiency, with appropriate confidentiality

Phil Couser, Director of NSS Strategic Business Unit, identified issues of information governance, data storage and access, as fundamental issues behind these application observations. He further suggested that the establishment of a new Scottish public health body would present both a growing

challenge and opportunity in addressing these issues.

Several strands of DLT activity exist across Scotland within Health institutions which, based on the information available to the authors, could be considered as now entering the discovery phase.

Opportunities exist to better empower this discovery through:

- increased involvement of stakeholders from across the Scottish Healthcare ecosystem and interested parties from academia and the technology industry
- capitalising on the learnings from global investment in commercial and government sectors, who have moved beyond the discovery phase

5.4 Digital Currency

Digital currency is digital money.

Bitcoin is a decentralised cryptocurrency, and a form of digital money which allows payments to be sent between users without passing through a central authority, such as a bank or payment gateway. It is arguably the first cryptocurrency, which established popular participation in, and views of, digital currencies.

We consider Bitcoin here as a useful starting point to consider investigating digital currencies relevance to Scottish Government. However, we note that the scope of this report necessarily only touches on the larger topic of cryptocurrencies disruptive potential in Scotland's Financial Services industry and the monetary economy.

But Bitcoin is only one of many cryptocurrencies. Each has been devised with different purposes and is created and held electronically. Bitcoins aren't printed, like dollars or euros—they're produced by computers all around the world, using free software. Bitcoin can be considered "decentralised" as it can be created and traded without a central bank, a bank account, an intermediary financial institution, and with lower cash handling and banking transfer fees.

Bitcoin is different from traditional currencies. It is decentralised so that no

single institution controls it, and it has a limited supply, based on a set of rules baked in to its underlying algorithm. It is difficult to tie the owner of a Bitcoin to a real-world person (unlike the conventional money, where in most jurisdictions regulation dictates that people should be identified through KYC checks).

We use a "wallet" to manage the cryptographic keys used to secure access to Bitcoins. Exchanges in Bitcoin between parties, (or Bitcoin transactions), are addressed between wallets. Despite its reputation for anonymity, every Bitcoin transaction ever made can be traced back in time between wallet addresses, so it cannot be considered a confidential medium. So, although Bitcoin is often accused of being anonymous, its more strictly correct to say that it is pseudonymous.

These characteristics have made Bitcoin popular with two communities: firstly, with those who want to make financial services more transparent inclusive and accessible, and secondly with people who don't wish to be identified in criminal activities or in avoiding capital controls. The International Monetary Fund explanation of the role of Virtual Currencies (International Monetary Fund, 2016) is summarised by

"Virtual currencies and their underlying technologies can provide faster and cheaper financial services and can become a powerful tool for deepening financial inclusion in the developing world. The challenge will be how to reap all these benefits and at the same time prevent illegal uses, such as money laundering, terror financing, fraud, and even circumvention of capital controls."

—IMF managing director Christine Lagarde

Much innovation in the monetary cryptocurrency arena since Bitcoin has focussed on addressing issues such as identification, confidentiality and privacy of transactions. This work continues, but that blockchain-based cryptocurrencies have an important role in providing more inclusive financial services seems beyond doubt.

However, cryptocurrencies' monetary role as a store of value is more difficult to conclude. In the year to the time of writing, a Bitcoin has grown from $1,000 to $8,000 in value and was briefly as high as $20,000.

"Bitcoin is a fascinating example of how human beings create value, or estimate and judge value. You cannot tell me that you can create out of nothing a medium of exchange value. It is not a rational currency in that sense. But that does not mean it will not trade, because so long as people believe they can sell it to someone else that's all you need to create a market. Human beings buy all sorts of things that aren't worth anything but they do it anyway. People gamble in casinos when the odds are against them. It has never stopped anybody".

—Alan Greenspan, former US Federal Reserve Chairman.

Clearly popularity and speculation on Bitcoin and other cryptocurrencies has driven large swings in its value against traditional currencies, leading to

accusations of a "hype bubble" and "tulip mania"[12].

Despite this interest, Bitcoin remains of limited utility as a transaction medium. Although it is accepted within the blockchain industry, and by a tiny minority of retailers, using Bitcoin for payment is largely inconvenient and unintuitive. Other cryptocurrencies typically each have their own wallets, apps or arrangements. In terms of the consumer and business "utility banking", cryptocurrencies are challenging to manage and use, and do not yet offer the full range of services we are used to receiving from banks. Moreover, increased popularity and speculation has driven much higher transaction fees, and accusations that its consensus algorithm, running on computers around the globe, incurs excessive electricity costs and consequent emissions. These complications have so far prevented widespread popular adoption beyond the growing Bitcoin/blockchain community.

However, across governments, the third sector and thought leaders, there is enthusiasm around the role of blockchain in enabling alternative "currencies" in the wider sense (i.e. to include local currencies, time banks and token and incentive schemes, and alternative payment systems), in growing economic activity. Several have been proposed in Scotland, including proposals such as "ScotPound" and "ScotPay" (New Economics Foundation, 2015), the Glasgow Pound and People's Bank of Govanhill, citing established examples such as the Bristol Pound.

One interesting local case study which enjoys popular support is the ScotCoin project. ScotCoin originated in 2015 as an "alternative national currency" implemented as an extension of Bitcoin[13]. Today the currency trades on popular cryptocurrency exchanges and is accepted for payment at a handful of businesses. A Community Interest Company (CIC) markets ScotCoin and holds its unissued supply of cryptocurrency. We understand that the remainder is held by existing consumers and individuals or businesses involved in its developing ecosystem. In 2018 the project is revising its technology platform to address currency volatility, regulatory concerns, and transaction costs noted above.

12 Referring to the 200-fold growth in the price of tulips over a 4 year period in 17th century Holland.

13 In fact ScotCoin was originally implemented on the "Counterparty" platform, where financial transactions piggyback on the Bitcoin network.

The writers of this report have no insight into ScotCoin project governance nor current distribution of cryptocurrency ownership, but would observe that the project's leaders have articulated community benefit goals, and that the IP underpinning the ScotCoin cryptocurrency has been offered free of charge to the Scottish Government.

5.5 Tokens

Distribute Ledger Technology's utility in enabling digital currency through cryptocurrency is well known.

This utility is based on characteristics which make a digital asset or token unique, enforce rules around its ownership (e.g. the "double spend" problem in Bitcoin), and make the token programmable and able to be automated.

Beyond digital currency such tokens are useful wherever a digital asset, or phyisical asset which has been "'tokenised", moves between parties.

Figure 5-1 below summarises three overlapping forms of token:

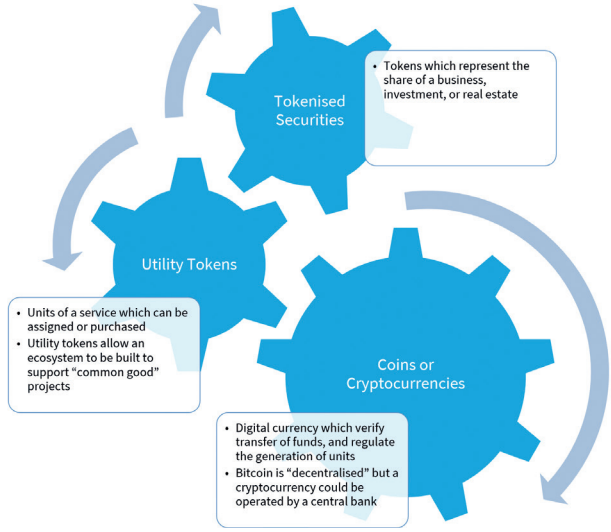


Figure 5-1 Forms of tokens

In Financial Services, organisations have undertaken much DLT innovation work around tokenised securities. In such schemes financial products, such as ownership of equities, debt and real estate, are represented as unique digital tokens.

This reduces transaction friction in the complex supply chain of these assets, reducing costs, paperwork, and improving transparency. Many feel this will bring productivity to markets. The consensus view is that increased transparency and automation will significantly change the role of intermediary actors and market makers in this financial services supply chain.

In such schemes, where a market and its transactions are represented entirely in the digital realm, Smart Contracts—or programs which trigger when conditions are met to complete a transaction—engender further automation and trust that binding agreements will be fulfilled by all parties.

A detailed exposition of the Financial Services industry use of DLT is beyond the scope of this report.

However, Utility Tokens may be more broadly relevant to the delivery of Public Services—representing services which may be granted to, or purchased by, citizens and consumers to create a liquid and efficient market for that service.

Utility tokens' objectives may be a "public good", societal change, or an open-source software project. Such schemes take advantage of peer to peer incentives and market economics to achieve their objective.

The Ethereum network, usually the No.2 crypto asset by market value, is powered by the Ether utility token. The token is required by anyone wishing to execute transactions on the Ethereum network.

Ayr-based Maidsafe is a commercial company whose objective is to create a "sharing economy" for computing storage and compute power. Their MaidsafeCoin token is granted to anyone who supplies computing power and is purchased by anyone who needs access to computing power.

Moving away from the technology and blockchain engineering space, one well-publicised scheme since 2012 is New York's Brooklyn Microgrid whose aim is to support local distributed generation and use of clean energy. Peer to peer transactions between generator and consumer are managed with a smartphone app underpinned by blockchain, to create a "virtual" microgrid.

In 2017 several global energy utilities, including Po are in trials to identify the challenges and benefits of P2P energy trading across regulated power networks.

The positive economic impact of conventional "collaborative economy" platforms such as Uber and Airbnb were noted by the *Scottish Expert Advisory Panel on the Collaborative Economy* (Scottish Government, 2017). Such platforms are run by organisations which aggregate the resources of "the crowd", to provide their service. Criticisms that such "gig economy" operators do not distribute their value equably are well documented, and the Scottish Government report noted their challenges in enabling "fair work, social value and inclusive economic growth".

Distributed Ledgers are held by some to be an enabler for such "sharing economy" or collaborative models, where the crowd can be both a contributor and shareholder. This is summarised by the *Harvard Business Review* (Filippi, 2017) which positions distributed, bottom-up co-operative crowdsourcing alternatives to eBay, Amazon, Uber and Facebook, which make use of blockchain technology to facilitate decentralised platforms which run for the benefit of their members.

As of beginning 2018 there are several such platforms operating, such as OpenBazaar (eBay, Amazon), ArcadeCity (Uber), and several Facebook alternative social platforms such as Steemit. However, their impact and user base are so far minor compared to conventional commercial collaborative platforms.

Scottish public sector collaborative models, enabled by Distributed Ledger, might contribute to improved public services by taking advantage of the best of the "gig economy" (or flexible labour) whilst delivering fair work and value to participants.

This could, for example, be considered in areas such as the provision of childcare, where this requires an effective collaboration between parents/guardians, local authorities and 3rd party providers.

5.6 A Note on ICOs

An Initial Cryptocurrency Offering, or Initial Coin Offering, is a fundraising process whereby projects sell new cryptographic tokens in exchange for established cryptocurrency like Bitcoin and Ethereum.

Most ICOs work by having investors send funds to a "smart contract" that distributes an equivalent value in a new token at a later point in time. ICOs can be considered a parallel of the Initial Public Offering (IPO) where investors purchase new shares in a company.

Though their history dates to 2013, in 2017 ICOs became a big part of the blockchain and venture capital industries. Although estimates vary, it seems that around $4Billion was raised globally in 2017, with half in Europe, and nearly $1Billion attributed to the Swiss town of Zug.

Increasingly financial regulators view ICOs as unregulated securities allowing the raising of unjustified capital. Some have started to react to the phenomenon, with the UK FCA, Germany's BaFin issuing guidance, the Japanese FSA moving to accommodate ICOs within their regulatory framework, and Chinese government administrations ruling them an illegal fundraising activity. With some evidence of fraud and bogus ICOs, Lord Holmes observed that "Initial Coin Offerings (ICOs) are controversial and risk reputational damage to DLT" (Richmond, 2017). This is because ICOs often raise money before any product or even business plan has been developed, sometimes raising $250M in a few hours, with no apparent governance.

However, many argue it is an innovative crowdfunded alternative to venture funding for start-up businesses, foundational technical projects operating at the blockchain protocol level, and non-commercial projects which enable mass investment or incentivisation in a project which has a "common good" objective.

Certainly, when viewed as an investment proposition, ICOs should be viewed as highly speculative and risky, with limited consumer protection in most jurisdictions.

5.7 Online Voting

In online voting schemes, online means are used to support those tasks involved in casting and counting votes, usually dispensing with a traditional ballot paper[14].

Both online and traditional voting systems must meet the requirements of being **secure** (so it can't be tampered with), **anonymous** (so a vote cast can't be tracked back to the individual) and **verifiable** (so it can be shown that one person cast only one vote).

Online voting, or Internet voting, or iVoting, has been proposed as means to address several issues with elections. It can increase convenience to address flagging levels of electoral participation in the smartphone age, improve the efficiency of remote voting scenarios by replacing postal ballots, and in the case of public elections reduce disruption of closure of schools and libraries for polling stations.

Many also believe that it can improve the security and transparency of voting systems which are dependent on paper ballots tipped out onto a table and counted by hand. However, others maintain a conflicting viewpoint that online voting is insecure, open to hacking and threats of voter intimidation.

This report does not attempt to argue the case for online voting systems. Rather it discusses in brief where there may be a place for DLT in an online voting scheme in Scotland, in terms of its value in the key qualities of "secure, anonymous and verifiable".

The Estonian i-Voting system is distinguished in its long-standing (since 2005) and high participation in binding elections (with 31% of the vote case online in the last national parliamentary election in 2015). In the Estonian system citizens can cast votes online using a PC or smartphone leveraging the national ID card infrastructure. This card infrastructure has already addressed issues important in the election: voter eligibility, and the distribution of signing and encryption keys. Citizens may repeatedly re-vote during the voting period with their last vote before the deadline counted. Finally, any paper ballot submitted overrides any internet vote that has been cast.

14 Online voting should be differentiated from *electronic* voting where paper ballot papers are often counted by automated electronic vote counting machines.

The Estonian system makes use of an election committee encryption key, and personal voter signing keys and, to the best of our knowledge, makes no use of DLT. This system has been criticised, specifically at 2013 municipal elections where election observers identified that officials failed to observe appropriate procedures required to protect keys PINS and passwords. We note that the company behind the current Estonian iVoting system, Cybernetica OÜ, is currently working on a next generation DLT based iVoting solution.

The Digital Strategy for Scotland (Scottish Government, 2017) committed to actions to re-design Scotland's digital Public Services. One of these is to "trial electronic voting solutions to increase democratic participation".

Throughout the research process, voting scenarios were raised as a potential DLT user case by interviewees. This included ideas relating to participatory budgeting and youth elections.

At the Scottish Government/Edinburgh University "Exploring Electronic Voting" event in November 2017, the academic attendees agreed that DLT should be a key component of future online voting solutions. Several blockchain enabled internet voting start-ups consulted with also concurred with this view.

If the Estonian system might be considered the foremost "tried and tested" internet voting scheme, what voting issues can DLT address to improve on its approach?

Firstly, before the actual casting of a vote, in the workflow of voter eligibility: an immutable and verifiable shared ledger can be used to bring benefits of improved transparency, convenience and integrity. DLT could bring increased transparency to the processes of voter and postal voter registration. This could make the registration process and checks demonstrably valid and compliant, to improve confidence in election outcomes. Further, some process steps such as change of address or death might be automated, and the identification of anomalies more obvious to maintain vigilance against electoral fraud. We note there are very few recorded instances of electoral fraud in Scotland.

The most obvious potential benefit is from the immutable characteristic of a blockchain—votes cast cannot be removed and so an individual voter can verify that his or her vote has been included in the final tally.

In the linearity of voting: In the "Exploring Online Voting" event, re-voting by casting another internet ballot, or casting a paper ballot, was seen as a desirable feature. DLT and blockchain's linear timestamping could be used to demonstrate the order in which events have taken place, preventing a possible attack vector where attackers could be retaining earlier events and replaying them closer to the election deadline.

To best support anonymity, cryptographic tools might be used as part of a DLT based voting scheme such that cast votes could be counted, without any privileged party having access to an individual's vote, i.e. the votes could be processed without election officials ever seeing the data. Such tools are recent innovations, and are the subject of much academic research and commercial innovation, but have thus far found few "engineered", tried and tested real world applications.

However, there is not yet consensus on how such a system should be designed and implemented. Blockchain voting technology start-ups use many different approaches and platforms. With public blockchain platforms questions remain of their ultimate control in terms of individual core developers and mining consortia, and how this might be leveraged to impact elections.

In common with commercial (non-DLT) iVoting solutions, not all of the technology involved is open to inspection and scrutiny—and citizens and election authorities may not be comfortable with a "trust us we're secure" approach.

Discussing the use of DLT in voting inspired considerable passion in the academic, blockchain, and political/policy sectors. Certain policy groups maintain deeply held views that technology has no role whatsoever in voting. Other political groups see it as a route to achieve a specific political objective. Members of the global blockchain community see it as the route to "fluid democracy", libertarianism and maximum representation. Clearly it is important that any steps towards iVoting in Scotland should be carried out in an open and verifiable manner. DLT could underpin a collaborative and transparent approach which could satisfy or mitigate the resistance of highly vocal groups.

It is possible to use DLT to better support secure, transparent electoral process, whilst preserving voter privacy. Such systems seem likely to form the

basis of the next generation of iVoting systems to deliver improved secure, anonymous and verifiable qualities compared to the current generation of commercial iVoting solutions.

A specific international discovery of DLT use in iVoting, could be explored in less critical scenarios such as community engagement.

For this study:

- Election Unit representatives were interviewed.
- The Scottish Government "Exploring Electronic Voting" event was participated in, which included academic, returning officer, and e-voting supplier communities.
- Matthew Rice, Scotland Director of the Open Rights Group was interviewed.
- The international landscape of blockchain technology as applied to voting was reviewed, including Switzerland's Boulé, Australia's MiVote, and US's FollowMyVote platforms.
- Publicly available information on the Estonian internet voting system was examined.

6. HOME: Blockchain state of the nation

6.1 UK

An important function of government is to maintain trusted information about individuals, organizations, assets, and activities. A November 2017 report by Reform (the independent non-party think tank) states that only "13 per cent of people trust government to use their data appropriately, while 46 per cent do not". The report asserts that current models of "identity" cause duplication and friction and suggests that blockchain could simplify the management of trusted information, making it easier for government agencies to access and use critical public-sector data while maintaining the security of this information. Some records exist only in paper form, and if changes need to be made in official registries, citizens often must appear in person to do so. Individual agencies tend to build their own silos of data and information-management protocols, which preclude other parts of the government from using them. The Reform report suggests that blockchain could enable a shift ownership of personal data from the government to the citizen and proposes a new identity management model powered by block-chain (Maisie Borrows, 2017).

The House of Lords report Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation was written 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. With government leadership, the report suggests, DLT can enhance government services, protect government and citizen data, and act as a platform to advance innovation in technology, such as IoT and robotics. 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, includ-ing legacy systems, through enhanced interoperability. The report underpins

Sir Mark Walport's recommendations, and it endorses a focus on ministerial leadership, research, standards and supporting proof of concept trials. It identifies blockchain's potential in the specific scenarios of border security, taxation and benefit, health, and privacy/cybersecurity.

Government and its arms-length bodies in the UK are evaluating blockchain: HM Land Registry's Digital Street Initiative is aiming to speed up the conveyancing process. So far, a proof of concept has created a digital register for a small selection of properties, as a first step towards having a register that is fully machine-readable and able to be updated instantly by multiple parties across different organisations (Abbott, 2018).

HMRC has built a blockchain proof of concept to coordinate interventions at the border (Evenstad, 2017): Mike Potter, Director of Future Borders at HMRC stated:

"We have now built a proof of concept based on blockchain that demonstrates that you can actually get all of the 28 organisations that act at the border to coordinate all of their risk and intervention, so we only do it once and we do it well."

HM Treasury recently invited responses using fintech to their Rent Recognition Challenge (Gov.uk, 2017). A Scottish consortium including private and social sector landlords, a Scottish Credit Union and Wallet.Services proposed a blockchain solution.

6.2 Scottish Community

Scotland holds several assets in establishing a cluster of DLT skills and innovation. The nation's banking background led to the creation of several security operations centres (SOCs) and Cyber Security expertise, fed by the Cyber Academy and others. The academic sector has strong cryptography representation with specific focus in Edinburgh, Napier and Stirling Universities. Edinburgh's position as a financial centre drove many to take an early interest in Bitcoin and other cryptocurrencies.

This has helped establish the growing community of computing scientists, cryptographer mathematicians, and cyber professionals with skills which can be brought to bear on DLT engineering and in applying these tools to vertical industries.

The Edinburgh Bitcoin Meetup, established in Jan 2014, has evolved to be the Scottish Blockchain Meetup with around 400 members. This event regularly attracts over 200 attendees, and world leading expert speakers. The Meetup and the annual ScotChain conference are supported by MBN Solutions of Glasgow.

Several Scottish SMEs have established capability in this field and are working on industry applications.

Wallet.Services develop solutions which streamline, simplify and secure digital life by harnessing the benefits of blockchain. As of March 2018, Wallet.Services' 12-person team includes engineering and business specialists. In 2017 Wallet.Services' work for Scottish Government during the CivTech® cybersecurity challenge was recognised with the global Citibank Technology for Integrity award, and the Scottish Cyber Awards "Best Cyber Breakthrough". Together with a consortium from the Oil and Gas sector, Wallet.Services has built a proof of concept of chain of custody/verification across the supply chain (see 7.4, below). In the rented property sector Wallet.Services has just completed a project using blockchain to collate multiple letting agent rental zone data to provide aggregated insight into the overall rental marketplace. In early 2018, Wallet.Services raised £425K in equity investment to fund development of their SICCAR secure information sharing product first prototyped with Scottish Government CivTech®.

Joining Wallet.Services in CodeBase, Edinburgh, Blockchain Technology Partners is committed to both consuming and contributing to open source (Blockchain Technology Partners, 2018). Founded by cloud pioneer Duncan Johnston-Watt, BTP provides a production ready blockchain platform and partner with businesses to deliver blockchain-based solutions which they then operate on their behalf. Their first customer is The ScotCoin Project which is the community interest company behind ScotCoin—Scotland's digital currency.

Spiritus Partners, also based in Edinburgh is building next generation service records applications for critical assets and infrastructure. In sectors such as healthcare, life sciences, energy, and power, they provide assurance that safety, security and compliance measures have been taken across the operating life of their assets through blockchain solutions (Spiritus, 2018).

Kippitech are an Aberdeen-based start-up, part of the Hyperledger project—an open source collaborative effort. They are building supply chain software for the food, energy and transportation sectors (Kippitech, 2018).

Blockchain Development Services are based in Glasgow and have a focus on developing socially and environmentally impacting services. With projects focussing on encouraging engagement with recycling and reducing waste, BDS are using blockchain for good to make a positive impact on the world (BCDC.Online, 2018).

APPII, are a Scottish-based online verification and career management platform which uses a public blockchain to store 3rd party verifications of assertions on candidate CVs.

6.3 Other Projects of Interest

Maidsafe are a Troon based company whose project dates back to 2006. Maidsafe's SAFE is a distributed storage network with improved security and privacy. SAFE has evolved to embrace cryptocurrency in a circular economy where storage consumers pay those who offer storage with Safecoin. Maidsafe have a community of over 7,000 engaged supporters around the world (Safe Network Forum, 2018). Maidsafe ran a global developer conference in April 2018 as part of their move towards launch of the full public autonomous Network.

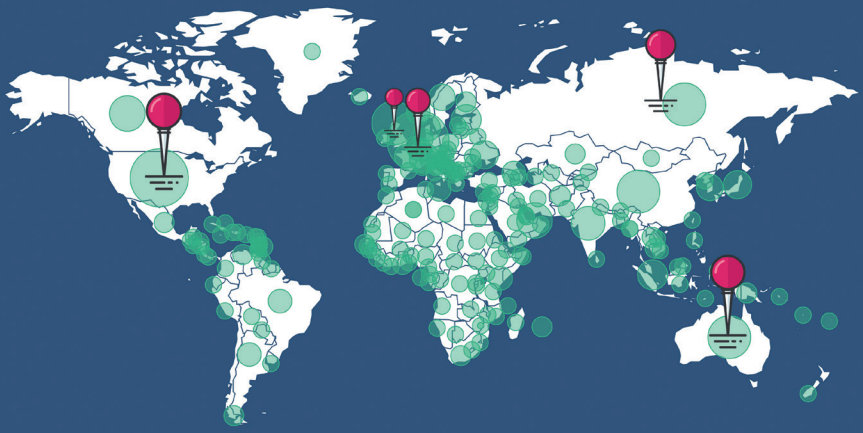
6.4 Academia

Napier University will build on the world class reputation of the Cyber Academy to set up ABIL (Advanced Blockchain Identity Lab), based at the Edinburgh Merchiston campus and funded for three years at £600,000.

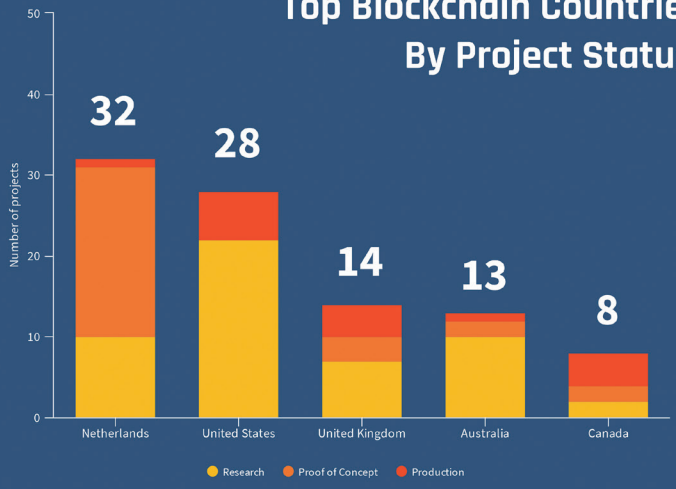
Led by Professor Bill Buchanan OBE, a key focus of the lab will be to create world-leading knowledge and innovation around areas which focus on the rights of the citizen to privacy, while enabling new methods to provide citizen-focused system. The funding includes research staff and PhD studentships.

Edinburgh University School of Informatics in February 2017 established

Global Public Sector Blockchain Activity



Top Blockchain Countries By Project Status



Source: Blockchain in Government Tracker 2018 - https://airtable.com/shrelXQjzluCxam37/tbl7qVDFKKiEcFFrc (accessed March 29, 2018)

WALLET SERVICES

a Blockchain Technology Laboratory (UoE, 2018). The lab brings together students and academics to focus on industry-inspired problems. Led by Professor Aggelos Kiayas, Chair in Cyber Security and Privacy at the University of Edinburgh, the Lab's multidisciplinary research scope will encompass economics, business and law. The lab is funded in partnership with IOHK (Input Output Hong Kong) a company founded to address practical issues of security resilience and performance. The Laboratory launched the EU's first blockchains and Distributed Ledgers course, and attracted £1.2m for a research project for Oxfam focussed on Smart Contracts for Donations ("Ox-chain").

The Advanced Forming Research Centre (AFRC), part of the High Value Manufacturing Catapult hosted at the University of Strathclyde, is currently developing a blockchain pilot around digitally managing supply chains in the Oil and Gas sector, in a consortium of sector organisations together with Wallet.Services.

7. AWAY: International Blockchain best practice

In researching international governments' activity in DLT we made use of published information and attendance at industry conferences. In the months since this report was commissioned many more nations, regions and cities have come forward with initiatives specifically or implicitly targeting DLT.

These initiatives are recent, and in most cases start with research then proceed to action via practical "proof of concept" projects, typically in co-operation with local commercial enterprises who are concerned with developing their own solutions. In some cases, the initiatives seek to support inward investment by running challenges and competitions to attract funded international start-ups.

In 2018 many of these projects are moving into pilot phase. To our knowledge the Republic of Estonia is alone in having a production service established for several years.

Where more detailed investigation has been undertaken, and where we have made contact with the appropriate government personnel, we include detail.

7.1 Estonia

Estonia is a small nation of just over a million people with a reputation as a global leader in e-government. Citizens of Estonia enjoy a streamlined experience across their digital interactions with the state. The "e-Estonia" narrative has driven Europe's most efficient and effective digital public service, putting it in the driving seat of the European Commission's digital single market, and sustaining Estonia's tech start-ups at home, and its international growth aspirations.

"Even though there are only a little over a million of us, thanks to Estonia's capabilities, we can make ten million payments, perform ten million requests and sign ten million contracts in just ten minutes. Even ten times larger states cannot beat us."

—Kersti Kaljulaid, President of Estonia

In 2007 Estonia suffered a nationwide cyberattack. Government websites and digital services were defaced or unavailable. Following the attack, there were worries that sensitive citizen data may have been compromised. By this point Estonia's public services were already in an evolved state of "digitalisation" to meet the cost and efficiency imperatives of the small nation. Services such as tax and voting were already online. Unlike its peers which could rely on disconnected nature of paper process, Estonia needed solutions to assure continuity and integrity of citizen data.

In the aftermath of the attack steps were taken—NATO established the Cooperative Cyber Defence Centre of Excellence in Tallinn. In 2008 Estonian government took steps to secure and guarantee authenticity of transactions in some Government databases, building on indigenous cryptography work

(Ahto Buldas, 2004). This was the genesis of the scheme which today uses "linked timestamping" to audit changes in several Estonian Government databases and assure that they have not been tampered with. Such technologies are commercialised by Guardtime AS and others, and are today considered Distributed Ledger Technologies (DLT)s[15].

Much has been written by Digital Transformation commentators about the reasons for e-Estonia's success, but the following systems play an essential role:

1. A uniform digital identity system implemented across public services, banking, and some private service providers[16].
2. A cross-government data interchange system (the X-road system lets government agencies look up information in other government databases).
3. Availability to citizens of systems to monitor how and when their personal information is being used by government officials (mostly implemented by Guardtime's DLT audit).

These foundations are mortared together with strong technical leadership, political commitment to remove legal and regulatory impediments to the deployment of technology solutions, and a populace with a higher than average degree of trust in digital government solutions.

Estonia and neighbouring countries have an active blockchain and cryptocurrency community. In 2017 there were two major conferences which attracted speakers from Silicon Valley and rivalled London-based events in size. The active tech start-up scene in Estonia has given rise to a significant share of Europe's more established blockchain start-ups, notably Funderbeam (financial services), Healthureum (Healthcare), and a healthy pool of smaller

15 A distributed ledger which does not feature the block-batching-hashing-and-chaining characteristics which gave blockchain its name following Bitcoin.

16 The state eID system is based on a Public Key Infrastructure, with 2 factor authentications based on an identity smartcard or mobile device. In early 2018 a vulnerability was discovered in a code library utilised on the proprietary smartcard hardware used in some Estonian cards, which allowed private key material to be compromised. The vulnerability was addressed before any encryption and signing could be circumvented, but several lessons were learned, including reinforcement of the dangers of closed source implementations which hinder the process of testing for flaws.

bootstrapping and seed funded companies already with customers such as WePower (Energy).

Estonia has a record of technology entrepreneurialism which belies its size. It enjoys a healthy angel and institutional investment environment for technology ideas. That the 2011 sale of Skype to Microsoft created many Tallinn-based developer $Millionaires undoubtedly helped.

In 2014 Estonia's digital identity scheme was extended through the E-Residency programme[17] to foreigners. This "government start-up" scheme seems to have created an elite group of Global Estonians including well-known operators in Silicon Valley's Venture Capital scene, further increasing access to capital. It also provided an easy infrastructure for location independent businesses to establish head office operations, tax, employment and business banking within the EU. At the time of writing E-residents were responsible for the creation of 5,000 businesses (mostly in the technology industry) based in Estonia. At the end of 2017 this has generated €15Million in net income according to independent auditors.

Building on the e-Estonia narrative, the Estonian government is reinventing its mission:

"Estonia is now a blockchain nation. Our digital society is underpinned by blockchain technology and our secure digital identities provide a significant advantage to blockchain companies that need to verify online identities"

—former President Toomas Hendrik Ilves

What does this mean in practical terms? Firstly, blockchain companies (both

17 E-residency is operated within the economic and entrepreneurial development organisation, Enterprise Estonia, the peer organisation of Scottish Enterprise.

physically based in Estonia, and registered in Estonia by E-residents) are using the E-residency identity verification process to satisfy KYC checks as they raise funding through ICOs. In late 2017 Estonian Government issued proposals for the establishment of an E-residency cryptocurrency[18], under the working title of "EstCoin" with goals of enabling a fluid marketplace and incentivising growth in the E-residency community.

7.2 Dubai and Malta

Wallet.Services attended the UNLOCK blockchain forum, which brought together international Governments and blockchain entrepreneurs in Dubai, UAE, in January 2018.

The event attracted public servants from UAE, South Korea, Malta, China, and the USA, keen to understand how distributed ledger tech could improve delivery of basic government services and play a role their regional economic development. It also attracted a global cross-section of representatives from blockchain tech companies, public services, health, genomics, utilities, electric vehicles, cybersecurity, and education sectors.

Several representatives of smaller jurisdictions who were investigating the role of DLT in government services were met, underlining the notion that smaller nation-states are at the forefront of DLT innovation, and often have ambitious goals to advance its deployment and its capacity for business transformation[19]. These nations shared a view that collaboration around learning and commissioning of DLT pilots was desirable.

The following people were interviewed for this study:

- Abdalla Kablan, Malta Stock Exchange Blockchain Committee
- Andrea Tinianow, Founder and Director Global Delaware
- Dr Aisha Bin Bishr, Director General at Smart Dubai Office

18 Subsequently a blunt response to this announcement was issued by the Mario Draghi, President of the European Central Bank who stated that "No member state can introduce its own currency; the currency of the eurozone is the euro."

19 The small nation phenomenon could be attributed to sample bias, in that our research was opportunistic in its access to Government technology leaders, and we were limited only to shareable information.

In 2016 Dubai set a city blockchain strategy to "deliver more seamless, safe, efficient, and impactful public services". It set the goal of eliminating bureaucracy by replacing 100 million documents with natively digital transactions, underpinned by distributed ledgers, by 2021.

Dr Aisha Bin Bishr discussed Dubai's 20 planned blockchain pilots, spanning applications across permits & licenses, transportation, energy, health and education. This strategy is a co-ordinated cross-government multi-agency effort with defined results and deadlines.

"Adopting blockchain technology Dubai stands to unlock [£1 billion] in savings annually in document processing alone"

—Dr Aisha Bin Bishr, Smart Dubai

One example is the Dubai Land Department which is building a real estate register system to record transactions with improved transparency, timestamping and credibility in a city state which is a hotspot of foreign inbound property investment. This department deals with the Land and Property Register, and also deals in the extended services of property financing, letting, brokering, and disputes. Currently in pilot, the project will be delivered in 2019 and involves a broad ecosystem including real estate companies, IKEA and Emirates Bank.

Dubai's hope is to establish itself as a destination for the most innovative start-ups to help diversify away from oil revenues. It sees blockchain start-ups as attracting the best talent and investment.

At the UNLOCK blockchain event, the city energy utility DEWA issued a challenge to the start-up companies present around a blockchain platform for Electric Vehicle registration, charging and billing. Later in 2018 it will repeat the Smart Dubai Office Blockchain Challenge—targeting international start-ups under three years old. Its goal is to drive solutions for government efficiency, thought leadership, and to support creation of a blockchain industry in Dubai.

Malta was represented by Dr Abdalla Kablan who explained that Maltese government attention had focussed on the role of cryptocurrency in its position as Europe's "online gambling hub", and DLT in Malta's role as a financial centre.

US State Delaware is small with 1M residents, but its sympathetic state laws mean that 60% of US Corporations are based in the state. Delaware aims to address use cases in share ownership, record keeping, transaction and settlement.

Malta and Delaware's blockchain initiatives are directly sponsored by their Prime Minister and Governor respectively. In Dubai the nation's Ruler is on record saying all applicable transactions will be on the blockchain by 2020.

It is further noted that the city government of Zug in Switzerland is currently in pilot of a "self-sovereign" identity utilising blockchain technology from Blockstack.

7.3 Netherlands

Since 2016, the Dutch Public Service has delivered eleven blockchain pilots focusing on processes and services it wanted to modernise in different government organisations. The Netherlands seems to have implemented the best example of co-ordinated cross-government activity and it is represented in detail in "Appendix: Netherlands Use Case detail", below.

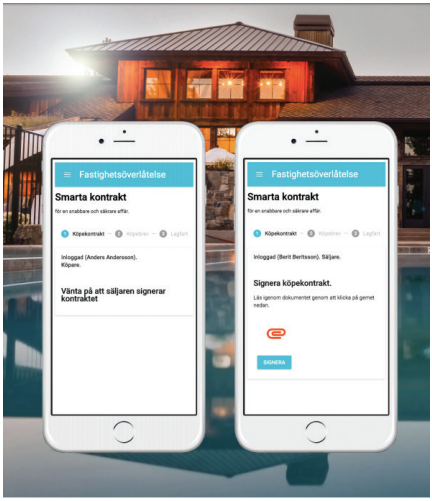
The results of the pilots were that participating organisations gathered valuable knowledge about blockchain and its potential impact. A specific use case was developed for each organisation, and an informal blockchain network was set up by participants to share best practice and projects emerging from Dutch academic institutions and businesses. Additionally, a government-business network was set-up to collectively develop blockchain applications building on the learnings and outputs from pilots. This network includes large corporations, IT companies, universities, and start-ups.

The Dutch government has defined clear policies with regards to digital identity, value registration and critical personal data management; started a series of small projects in partnership with blockchain businesses of which the failures and successes are transparently shared; and established rules and standards for blockchain code (if it is created with government funding, code

should be completely open source (Hartog)).

7.4 Sweden

Since 2016, Sweden's land-ownership, mapping and cadastre authority, the Lantmäteriet, has been piloting and testing its own blockchain based platform for property transactions. At March 2018, they are seeking volunteers to participate in buying and selling property who are interested in reducing the time from signing a contract to registering a sale which can take between three to six months.



Framtidens husköp i blockkedjan

The National Land Survey of Sweden has developed a full digital property transfer process with blockchain. It means sellers and buyers, and those who accept the transfer of the property's registry, such as the Land Survey Property Registration department can create the right content in the Land Registry and witnessing in principle can be done by everyone. The Land Registry is a publicly held ledger of real estate transactions, with inbuilt transparency and crypto security, so that no one can tamper with records without detection (Lantmäteriet, Landshypotek Bank, SBAB, Telia company, Chroma-Way, Kairos Future, 2017). With the blockchain system, the entire transaction could be completed in hours.

There are still obstacles to overcome in Sweden before blockchain can be adopted on a wider scale for real estate dealings, namely that digital signatures for registering or purchasing properties are currently illegal under Swedish law (Zuckerman, 2018).

Swedish bank SEB is also trialing a blockchain platform for the trading

of mutual funds, together with Nasdaq. The current Swedish mutual fund market does not have a centralized tracking mechanism in place (unlike equities markets), and so tracking and maintaining a ledger of transactions is a radically complex process involving a host of players, some aspect of which are still recorded with pen and paper. The platform intends to make it possible for all fund managers, distributors and other mutual fund participants to make trades directly onto the blockchain technology ledger. This would increase efficiency, tracking and auditability and make trading of funds faster, smoother and easier for all parties (Buck, 2017).

7.5 European Commission

Under the auspices of the European Commission there are several significant streams of work in Distributed ledger Technology, spanning policy, research, economic development and implementation.

This culminated in the signing of the Declaration on the establishment of a European Blockchain Partnership (European Commission, 2018) with the express goal of preparing for the launch of EU-wide blockchain applications across the Digital Single Market. The UK Government was included as a signatory.

Shortly afterwards the EU DG Joint Research Centre policy unit released the final report of a project started in early 2017 #BlockChain4EU: Blockchain for Industrial Transformations[20]. This project's aim was to identify and communicate blockchain use cases from an EU industrial and business context. At the time of writing its final report is available only in printed form.

The Commission launched the EU Blockchain Observatory and Forum in February 2018 with support of the European Parliament. This will highlight key developments of the blockchain technology, promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities. The European Commission wants to build on existing initiatives, ensure work across borders, consolidate expertise and address the challenges created by the new paradigms enabled by blockchain (such as disintermediation, trust, security and traceability by design). The EU Blockchain

20 https://blogs.ec.europa.eu/eupolicylab/portfolios/blockchain4eu/

Observatory and Forum will actively help Europe to seize new opportunities offered by blockchain, build expertise and show leadership in the field. It will gather information, monitor and analyse trends, address challenges and explore blockchain's socioeconomic potential (European Commission, 2018). The Observatory and Forum will review the five innovations emerging from the €5m blockchains for Social Good competition closing later this year.

7.6 United States

The US government have been evaluating blockchain via several US government agencies to improve transparency, efficiency and trust in information sharing in:

- Financial management
- Procurement
- IT asset and supply chain management
- Smart contracts
- Patents, Trademarks Copyrights, Royalties
- Government-issued credentials like visas, passports, SSN and birth certificates
- Federal personnel workforce data
- Appropriated funds
- Federal assistance and foreign aid delivery

7.7 Israel

The Israeli Government funds and collaborates with businesses and academic institutions via the Iraeli Blockchain Association. With a policy of open government, Israel has commissioned an interactive political platform that promotes the policies of an open government and eliminates the communication gap between the elector and the elected a utilizes smart contracts for enforcing campaign commitments made by politicians—such as budgets proposals and policies (Ozelli, 2018).

7.8 Columbia

Centre for Digital Public Innovation (CDPI) of the Colombian Government is looking into the potential of blockchain after the blockchain-powered voting platform Plebiscito Digital (Digital Plebiscite) and worked with several civil society organizations to allow expat Colombians abroad and not allowed to vote to cast symbolic votes on a peace treaty through the platform (Case Study: Blockchain Voting for Peace—Colombia).

7.9 Africa

Africa still has an unbanked majority, and so cryptocurrencies have offered opportunities to those with no access to traditional financial services. DLT are now disrupting Africa's business arena at a time where governments and industries are still rife with corrupt deals, poor record-keeping and untraceable transactions.

Last year, the Rwandan government developed the first phase of an initiative to digitise Rwanda's Land Registry onto blockchain to aid authenticity.

South Africa's newly-appointed president Cyril Ramaphosa made an announcement in February 2018, stating that a 'digital industrial revolution commission' would be set up in partnership with the private sector and encompass new technologies, such as blockchain.

The same month, Kenya's Ministry of ICT appointed a team to produce a blockchain roadmap. Led by Dr. Bitange Ndemo, the eleven-member team will spend three months researching artificial intelligence and the potential use of distributed ledger technology in Kenya.

Also announced in February was a blockchain-based information portal for crime control in Nigeria. The citizen-focused platform, named interPort, will allow Interpol to access information and manage stakeholder engagements and crime reporting.

A pilot scheme, set to launch in Q3 2018, will use blockchain to monitor cobalt mining in the Democratic Republic of Congo. The scheme aims to ensure that cobalt used in lithium-ion batteries (found in everything from cell phones to electric cars) hasn't been mined by children. Companies are under increasing pressure from consumers and investors to show that cobalt has come through supply chains free of rights abuses, similar to other minerals

such as tantalum, tin, tungsten and gold (Top 5 African Blockchain Applications, 2018).

7.10 Asia

7.10.1 Australia

In 2017 an Australian stock exchange (ASX Ltd) announced that it would replace its legacy clearing house system (CHESS) with a blockchain based post-trade settlement system. This decision is widely credited with accelerating the Australian blockchain ecosystem, and its implementation timetable requires external trading participants to be ready in late 2020.

7.10.2 Singapore

The city-state of Singapore has a blockchain ecosystem populated by many well-funded start-ups and supported by a strong academic research environment. At the time of writing, the Financial Services regulator in Singapore (Monetary Authority of Singapore) is in consultation around regulatory changes to ease market entry for blockchain-based decentralised exchanges.

7.10.3 China

In 2017 Chinese state moved to address perceived fraud and money laundering issues. Despite China being a global hotspot for Bitcoin "mining" operations, the financial regulator moved to force Bitcoin miners to exit from China, and to ban developers and entrepreneurs from launching coin offerings.

However, in a May 2018 speech Chinese President Xi Jinping endorsed blockchain technology and seemed to suggest that a national research and development lab would be established.

8. Appendix: Public Sector Interview Methodology

The research for this report followed a four-stage process:

1

At the suggestion of the consultants, the Director of the Scottish Government Digital Directorate wrote to a number of public sector bodies saying:

"....We have recently commissioned research to look at how DLT is being applied in other jurisdictions and to assess whether and/or how it might be applied in Scotland. This will, amongst other things, seek to identify any viable business cases for investing in the technology across the public sector and will, in particular, look at the opportunities it offers for improving services (Process) in particular geographic locations (Place) and improving life for individuals, families and communities (People)....."

2

Interviews and workshops were conducted with CXO level staff across Scotland's public sector. These sessions tended to fall into two halves. During the first a short slide deck was used to explain to interviewees the types of business issues that DLT was best suited to resolve. During the second we focused on their business issues in that context.

Interviewees were provided with the following three questions in advance to stimulate discussion in the second part of the meeting:

Q1 *Are there any data-related aspects to your business that cause you a concern and that might result in a serious degradation to your service? This is sometimes known in the commercial sector as an 'extinction level' event.*

Q2 *Looking forward, over the next 3-5 years do you envision digital*

enabling better performance, outcomes and inclusion for your agency/ department? What are the 3 or 4 blockers holding you back from achieving that vision?

Q3 *Thinking about your interaction with, and dependency on, external organisations and people—with you as both a recipient and a provider of data, are there situations where there are delays, efficiencies, inaccuracies and additional costs? E.g. elapsed times, reverting to paper or e-mail, a requirement for 'wet' signatures, re-entry of existing data etc.*

3

Sixteen interviews were conducted between October 2017 and March 2018. The interviews, and in some cases workshops, lasted between one and three hours.

4

Desk based research into trends and comparative use cases of DLT within the public sector from across the globe, and an in-depth review of the Scottish DLT ecosystems were conducted. This involved meeting with Universities, SMEs, larger companies such as IBM, Sopra Steria, Exception and the Scottish blockchain meet-up community.

The figure below shows the project shape focused around the themes of People, Place and Process.

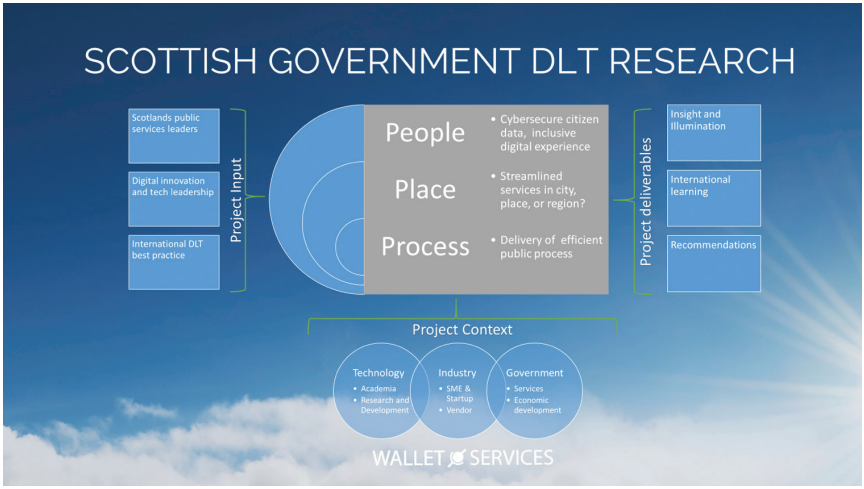


Figure 8-1 Scott Government DLT Research Methodology

The full findings around the opportunities outlined by the interviewed organisations are currently being reviewed by the Digital Directorate. These will be published shortly in an updated version of this report.

9. Appendix: About this Report

9.1 The Report's Authors

Wallet.Services develops solutions which streamline, simplify and secure digital life by harnessing the benefits of blockchain. The team that undertook the research and consultation was:

Local Research

Rab Campbell

Rab is an experienced business professional who spent ten years working for a global System Integration company as Account Director for Scottish Government. He was also Chair of the Digital Industry trade body, ScotlandIS from 2012 – 2014. He was involved in establishing CodeClan, ensuring its financial viability by implementing an innovative commercial scheme to ensure employers make an appropriate financial contribution. Rab has an MBA from Edinburgh University (2003) and recently completed the Common Purpose Meridian Programme. He was appointed Executive Chair of Wallet.Services in June 2017.

Gillian Thompson OBE

Gillian has deep experience in delivering the policies of the Scottish Government including development of devolved and reserved policies, leading legislative and organisational change, project and programme management, corporate and financial accountability, influencing and negotiation. She has full working knowledge and experience of Scottish political scene and has a well-regarded reputation for delivering organisational strategy and expertise, working at Board level as chair and member and as the responsible person for a national service. Currently Gillian is Chair, Management Advisory Board, Scottish Public Pensions Agency. She has an active interest in provision of high quality services to citizens by central and local government and third sector.

International Research

Peter Ferry

Peter is Commercial Director of Wallet.Services and focuses on establishing business strategy, customer and partner growth strategy, and company communications. Previously, Peter built a subsidiary with revenues of $120M as part of the founding team of Microsoft Corp in Scotland. He was architect of Microsoft Scotland's partner program. Building on his background as a software developer, Peter's experience in Microsoft spanned Technology Consulting across Scotland's larger enterprises in Financial and Public services, establishment of an award-winning SME business partner program, and P&L responsibility for Microsoft Ltd Solutions and Partner group in Scotland. He served on the board of ScotlandIS from 2013 to 2015, is on the National Cyber Resilience Leaders Board—Economic Opportunity working group, and was appointed the Honorary Consul for the Estonian Republic in July 2017.

Dr Hannah Rudman FBCS FRSA

Hannah is Director of Strategic Transformation at Wallet.Services. She is a highly experienced IT, Digital, and Organisational Transformation Professional. Previously, Hannah led £multi-million publicly funded, national digital transformation and innovation programmes, creating digital transformation in over 250 enterprises. Hannah advises governments on how to empower sectors to change and transform to maximise digital opportunities. She has made keynote addresses at international conferences in Mexico and Australia and is a persuasive communicator, as a speaker, writer, academic, interviewer and presenter of filmed case study documentaries. During '16 – '17, she worked with global science and technology solutions company Leidos as Associate Principal Consultant, developing their Digital Transformation practice, and over '17 – '18 worked as Associate Director for international firm BOP Consulting.

10. Appendix: Netherlands Use case detail

Focus of pilot	Government Organisation	Brief description of pilot	Current status
Digital Identity	Ministry of Internal Affairs	Sharing specific information only in a specific context. Each citizen would have control over which data s/he would share with whom.	Building a prototype for age control while purchasing specific goods, such as cigarettes or alcohol
Execution of a judicial decision of juvenile court	Ministry of Justice	Use blockchain for the registration of labour that has been completed by minors against sentence for minor crimes.	Building a prototype
Changing role because of blockchain	Court of Audit	Considering how the Court's role would change if it had real-time access to the data and intervention happened at an earlier stage. Compliance could be built into the financial rules via blockchain.	To be determined

Focus of pilot	Government Organisation	Brief description of pilot	Current status
Information sharing during a criminal trial	Ministry of Justice	Blockchain would become a security/truth layer 'on top' of the existing systems through creating a log of what information was shared with whom at what time. This could prevent proceedings from being paused as a result of the claim of one of the parties involved not to have received a piece of information.	Involving multiple stakeholders to determine viability of developing a prototype
Authorisations in the healthcare process	Healthcare Institute	Blockchain is being used to create a clear overview of authorisations in the healthcare process. The pilot has developed a prototype on Ethereum, which allows involved healthcare providers to get real time information on a need to know basis about their client/ patient. The client/ patient has more control over his data and can determine—via an application—which professional can get access to additional information.	Testing phase with prototype
Optimising the subsidy process	Province of Noord-Brabant	Using blockchain technology and smart contracts, exploring whether it would be possible to reduce the time to get through the administrative and financial processes for applying a subsidy for the disposal of drug waste from 13 weeks to 13 minutes.	Completing additional research into the judicial applications of a blockchain driven subsidy process

Focus of pilot	Government Organisation	Brief description of pilot	Current status
FlashCompany	Chamber of Commerce	The Chamber looked into the possible benefits of establishing a temporary organisation (a FlashCompany) on the blockchain in order to collect money for a good cause. It found that for the registration process (online), opening a bank account (can be linked automatically) and selecting conditions for establishing and ending the temporary organisation, blockchain was a viable solution. Using smart contracts for donations ("If this video has 1000 views, I will donate 100 Euro") was identified as a further benefit.	Developing a prototype of a FlashCompany
Registering a ship	Cadastre, Land Registry and Mapping Agency	Blockchain-based registration of ships. The system is more user-friendly for the owner of a ship that only needs to fill in a registration form. Upon registration, a "file" on the blockchain is created which triggers requests to, e.g. the builder of the ship, who then adds information to this file. The Cadastre doesn't have to manually check each set of documents but gets a notification when data of the parties involved in the registration of a ship don't match.	Developing this concept with TU Delft

Focus of pilot	Government Organisation	Brief description of pilot	Current status
Improving Request for Legal Aid	Legal Aid Board	The Legal Aid Board wanted to verify whether blockchain could create a faster, more secure automated process for the attribution of legal support focusing on requests for legal support. The added value of blockchain was an error free log of available lawyers, however third-party information sources (e.g. Tax Agency) was an outstanding challenge.	Next steps to be determined
Smarter Tax Revenues	Tax and Customs Administration	The Tax Agency created a use case that makes it possible to redistribute tax money as soon as it gets deducted from an employee's income. The most fundamental shift was that entire data was combined into one dossier that was managed by the citizen involved. That citizen would have better understanding about who has (or wants) access to his/her data.	Further research by the Tax Agency, mapping legal implications of a blockchain based Income Tax System

Focus of pilot	Government Organisation	Brief description of pilot	Current status
Transport of toxic waste	Human Environment and Transport Inspectorate	The HETI rethought the entire paper intensive process of transporting toxic waste from the Netherlands to another EU State in order for it to get disposed. The complex process involves multiple stakeholders: the Human Environment and Transport Inspectorate (HETI), its foreign counterpart, the company that wants to dispose waste, a transport company and the company that will take care of the disposal. All notifications during this logistical process could now go through different applications; approval for a transport could be automated based on a smart contract on the blockchain.	HETI involving all stakeholders to build first prototype i.e. the smart contract on the blockchain, including smartphone applications

11. Glossary

Bitcoin

A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Bitcoin can be used for online transactions between individuals, and addressed the "Double spend" problem to prevent the same account balance being spent more than once.

Blockchain

Specifically, blockchains are distributed ledgers in which records are linked and secured in a growing chain using cryptography, making it ever more difficult to modify retroactively.

This immutability makes blockchains useful for record keeping applications.

Consensus

In a distributed ledger each peer must follow consensus rules to ensure every copy is correct and identical.

Such consensus strategies are designed to make distributed ledgers robust against faulty or rogue peers.

Digital identity

A digital identity is a set of claims made by one digital subject (a person, an organisation, or a device) about itself.

The subject is unique and enhanced with specific attributes which provide information and validity. Digital identity is how we present digital subjects and demonstrate they have the required attributes, as proven by the owner or custodian of those attributes, to confirm the subject's validity.

Distributed ledger

A shared database spread across multiple sites and operators. Often such ledgers have no single central administrator, but are instead owned, updated and monitored by every operator, or "peer", with each maintaining a copy.

Distributed ledgers are useful for applications where no single central authority, or intermediary is available or desirable.

Encryption

Encryption refers to the operation of disguising plain text information so that it is concealed. The set of rules to encrypt the text is called the encryption algorithm. The operation of an algorithm depends on the encryption key, or an input to the algorithm with the message. For a user to obtain a message from the output of an algorithm, there must be a corresponding decryption algorithm which, when used with a decryption key, reproduces the plain text.

Identity

Identity is real world information about a person which describes them. We are given a legal identity at birth, with our birth certificate, which is used to demonstrate our legal rights to participate in society. We also have other contexts, disconnected from our personal being, such as when we act as an agent or delegate for someone else, or for an organisation e.g. as company director or government inspector.

Identity attributes

Our Identity attributes are pieces of information about us and that we build upon and extend over our lifetime. These are sometimes permanent, and sometimes temporary during tenure of position, or receipt of a benefit. Attributes are often sensitive personal data items such as date of birth, social security, medical or social condition. Often, they extend to biometrics or authority to perform or restrict a function. These attributes may only be valid in a given context or with a particular authority.

Many attributes are retained by public authorities and commercial third

parties. These copies are used to verify identity through 'proof of knowledge' exchange. Often this leads to data inconsistency and loss. This lets attackers impersonate an individual by having a more complete set of answers to 'proof of knowledge'.

Permissioned Ledger

Private or permissioned ledgers are only open to authorised operators and provide the same core ledger facility as Public Ledgers. They do however have different operational properties such that they can scale and provide throughput not achievable on Public Ledgers. This provides inherent security as access is by invitation, adding layers of lifecycle management and centralised control. Processing is shared by the consortium who can agree data and processing characteristics appropriate to requirements of their application.

Personal data

Personal data includes basic data such as name, address, date of birth, phone number, email address and bank details from which a living person could be identified, as well as additional special category data like health records, ethnicity, sexual orientation, religion, race and political views. Public authorities and commercial companies typically protect personal data with a local digital identity. This lets us interact with local services and functions but rarely allows re-use of that proof in other contexts.

Usually the data is about you but does not belong to you. You may own your house but the record that you own your house belongs to the land register. Medical data is about you but maintained and held in trust by the health service.

Public Ledger

Public Ledger DLTs are fully open to any participant assuming they play within the rules. It is not just the ledger data that is shared but the workload of verifying the transaction is distributed in order to maintain a balanced and trusted ledger. It is the distribution of this verification that ensures no single party can enforce invalid transactions into the permanent records. This verification workload can lead to constraints in scalability and throughputs in public ledger systems.

Smart Contract

Software that allows users to create invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level. Smart Contracts can provide a distributed execution environment to automate transactions according to pre-agreed rules without any human interaction. Smart Contracts can be built on to hold funds, support Initial Coin Offerings, and even Decentralised Autonomous Organisations. Popularised in the Ethereum public blockchain's solidity programming language, they have received popular attention and have been exploited by entrepreneurs—but nevertheless human error has allowed their autonomy to be exploited in real-world scenarios.

12. References

Abbott, J. (2018, February 7). Flexible digital services, fit for the future. Retrieved March 29, 2018, from HM Land Registry: https://hmlandregistry.blog.gov.uk/2018/02/07/flexible-digital-services/

Ahto Buldas, M. S. (2004). On provably secure time-stamping schemes. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.65.8638

Allen, C. (2017, March 1). The Path to Self-Sovereign Identity. Retrieved from https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

BCDC.Online. (2018). Retrieved March 29, 2018, from https://www.bcdc.online/

bitcoinwiki. (n.d.). Retrieved March 12, 2018, from https://en.bitcoin.it/wiki/Category:History#2009

Blockchain in Government Tracker. (2018). Retrieved March 29, 2018, from https://airtable.com/shreIXQjzluCxam37/tbl7qVDFKKiEcFFrc

Blockchain Programs. (2018). Retrieved March 29, 2018, from U.S. Emerging Citizen Technology Atlas: https://emerging.digital.gov/blockchain-programs/

Blockchain Technology Partners. (2018). Retrieved March 29, 2018, from https://blockchaintp.com/

Blockchains and Distributed Ledgers. (n.d.). Retrieved March 29, 2018, from http://course.inf.ed.ac.uk/bdl/

Buck, J. (2017, September 28). Blockchain for Mutual Funds? Nasdaq and Swedish Bank Start Testing. Retrieved March 2018, 2018, from Coin Telegraph: https://cointelegraph.com/news/blockchain-for-mutual-funds-nasdaq-and-swedish-bank-start-testing

Case Study: Blockchain Voting for Peace—Colombia. (n.d.). Retrieved March 29, 2018, from OECD: https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-colombia.pdf

European Commission. (2018, February 1). European Commission launches the EU Blockchain Observatory and Forum. Retrieved March 29, 2018, from European Commission: http://europa.eu/rapid/press-release_IP-18-521_en.htm

Evenstad, L. (2017, September 15). HMRC builds blockchain proof of concept for UK border. Retrieved March 29, 2018, from ComputerWeekly.com: http://www.computerweekly.com/news/450426393/HMRC-builds-blockchain-proof-of-concept-for-UK-border

Filippi, P. d. (2017, March). What BlockChain means for the Sharing Economy. Harvard Business Review. Retrieved from https://hbr.org/2017/03/what-blockchain-means-for-the-sharing-economy

Finney, H. (2004, August 15). Satoshi Nakamoto Institute. Retrieved March 29, 2018, from http://nakamotoinstitute.org/rpow/#selection-53.161-53.254

Frequently Asked Questions: Estonian blockchain technology. (n.d.). Retrieved March 12, 2018, from https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf

Gov.uk. (2017, December 6). Rent Recognition Challenge: Using FinTech to help renters. Retrieved March 29, 2018, from Gov.uk: https://www.gov.uk/government/publications/rent-recognition-challenge-using-fintech-to-help-renters

Hartog, K. L. (n.d.). Blockchain Pilots: A Brief Summary. Retrieved March 29, 2018, from https://docs.wixstatic.com/ugd/df1122_3de6de424d3b-4f618af9e768e12d0ca0.pdf

Hashcash. (2003, November). Retrieved March 12, 2018, from http://www.hashcash.org/.

Hill, R. (2017, March 28). DWP minister: Government 'carefully considering' wider blockchain benefits trial. Retrieved March 29, 2018, from Public Technology.net: http://www.publictechnology.net/articles/news/dwp-minister-government-'carefully-considering'-wider-blockchain-benefits-trial

IBM. (2017, January 30). Four Ways BlockChain could Aid Governments. Retrieved from IBM THINK Blog: https://www.ibm.com/blogs/think/2017/01/four-ways-for-blockchain/

IBM Institute for Business Value. (2017). Building Trust in Government—Exploring the potential of blockchains. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN&

ID 2020 Alliance. (2018, January). ID2020 Alliance. Retrieved from https://static1.squarespace.com/static/578015396a4963f7d4413498/t/5a5f92bc-c8302548e722dff3/1519157409748/ID2020+Alliance+Doc+-+Jan+2018.pdf

International Monetary Fund. (2016). Virtual Currencies and Beyond—Initial Considerations.

ISO. (2018). Blockchain and distributed ledger technologies standards catalogue. Retrieved from https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

Jeremy Wilson, V. C. (2017, Feb 8th). Barclays Bank Vice Chairman commentary on impact of BlockChain technology. Retrieved from Barclays Bank: https://www.home.barclays/news/2017/02/blockchain-could-be-new-operating-system-for-the-planet.html

Kippitech. (2018). Retrieved March 29, 2018, from http://kippitech.com/

Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay, Kairos Future. (2017, March). The Land Registry in the blockchain—testbed. Retrieved March 29, 2018, from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia Company, Chromaway, Kairos Future. (n.d.). Future house purchases in the blockchain. Retrieved March 29, 2018, from https://www.lantmateriet.se/contentassets/6874bc3048ab42d6955e0f5dd9a84dcf/blockkedjan-framtidens-huskop.pdf

Maisie Borrows, E. H. (2017). The future of public service identity: blockchain. Reform UK.

Meyer, D. (2017). The Australian Securities Exchange just made blockchain history. Retrieved March 29, 2018, from Fortune: http://fortune.com/2017/12/07/blockchain-technology-australian-securities-exchange-asx/

New Economics Foundation. (2015, November). ScotPound: digital money for the common good. Retrieved from http://b.3cdn.net/nefoundation/3a512ad0ef4458b28b_ntm6bwk42.pdf

News, B. (n.d.). Scottish Government Owned Energy firm. Retrieved from http://www.bbc.co.uk/news/uk-scotland-scotland-business-43692159

Ozelli, S. (2018, March 2018). Blockchain Technology Takes Hold in Israel: Expert Take. Retrieved March 29, 2018, from Coin Telegraph: https://cointelegraph.com/news/blockchain-technology-takes-hold-in-israel-expert-take

Price, R. (2017, May 22). Someone in 2010 bought 2 pizzas with 10,000 bitcoins — which today would be worth $20 million. Retrieved March 12, 2018, from Business Insider UK: http://uk.businessinsider.com/bitcoin-pizza-day-passes-2000-20-million-2017-5

R3 (Company). (n.d.). Retrieved March 12, 2018, from Wikipedia: https://en.wikipedia.org/wiki/R3_(company)

Richmond, L. H. (2017). Distributed Ledger Technologies for Public Good: leadership, collaboration and innovatio. House of Lords.

Safe Network Forum. (2018). Retrieved March 29, 2018, from http://www.safenetforum.org

Scientific American. (2016, June 23). Top 10 Emerging Technologies of 2016. Retrieved from BlockChain enhances Privacy, Security and Conveyance of Data: https://www.scientificamerican.com/article/blockchain-enhances-privacy-security-and-conveyance-of-data/

Scottish Government. (2017, March 22). Realising Scotland's full potential in a digital world: A Digital Strategy for Scotland. Retrieved from http://www.gov.scot/Publications/2017/03/7843

Scottish Government. (2017, January). Scottish expert advisory panel on the collaborative economy: report. Retrieved from https://beta.gov.scot/publications/scottish-expert-advisory-panel-collaborative-economy-report/pages/3/

Spiritus. (2018). Retrieved March 29, 2018, from https://www.spirituspartners.com

Stornetta, H. &. (1991). How to Time-stamp a Digital Document.

Top 5 African Blockchain Applications. (2018, March). Retrieved March 29, 2018, from Trend Watching: http://trendwatching.com/trends/

top-5-african-blockchain-applications/

UoE. (2018, February 14). Beyond Bitcoin—IOHK and University of Edinburgh establish Blockchain Technology Laboratory. Retrieved March 29, 2018, from University of Edinburgh: https://www.ed.ac.uk/informatics/news-events/stories/2017/beyond-bitcoiniohk-and-university-of-edinburgh

Walport, M. (2015). Distributed Ledger Technology: beyond Bitcoin. Retrieved from gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Wikipedia—Digital Signature. (n.d.). Retrieved March 29, 2018, from https://en.wikipedia.org/wiki/Digital_signature#History

Wikipedia—History of Cryptography. (n.d.). Retrieved March 29, 2018, from https://en.wikipedia.org/wiki/History_of_cryptography

World Economic Foundation. (2016, August). The Future of Financial Infrastructire. Retrieved from World Economic Forum: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

Zuckerman, M. J. (2018, March 7). Swedish Government Land Registry Soon To Conduct First Blockchain Property Transaction. Retrieved March 29, 2018, from Coin Telegraph: https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction

Scottish Government
Riaghaltas na h-Alba
gov.scot

ISBN: 978-1-78781-123-2

This document is also available on The Scottish Government website: **www.gov.scot**

Produced for The Scottish Government by
APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA

PPDAS450446 (08/18)

w w w . g o v . s c o t