Government
Office for Science

Distributed Ledger Technology: beyond block chain

A report by the UK Government Chief Scientific Adviser

17%
33%
50%

Contents

Foreword 4

Executive Summary and Recommendations 5

Definitions 17

Chapter 1: Vision 21

Chapter 2: Technology 33

Case study – Research and horizon scanning 37

Chapter 3: Governance and Regulation 41

Chapter 4: Security and Privacy 47

Chapter 5: Disruptive Potential 53

Case study – Diamonds 56

Case study – Corporate actions 58

Case study – SETLing transactions 60

Chapter 6: Applications in Government 65

Chapter 7: Global Perspectives 73

Case study – European energy retail market 76

Case study – Estonian block chains transform paying, trading and signing 80

References 84

Acknowledgements 87

A short video has been made to accompany this report which can be viewed at: https://youtu.be/4sm5LNqL5j0

Foreword

The progress of mankind is marked by the rise of new technologies and the human ingenuity they unlock.

In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services. As we have seen open data revolutionise the citizen's relationship with the state, so may the visibility in these technologies reform our financial markets, supply chains, consumer and business-to-business services, and publicly-held registers.

We know there will be challenges as Distributed Ledgers mature and disrupt how we think about and store data. The UK is in a unique position to explore those challenges and help maximise the benefits to our public services and our economy. We already have world-class digital capability, innovative financial services, a strong research community and growing private sector expertise. It is vital that our key assets – including the Alan Turing Institute, Open Data Institute and the Digital Catapult – work together with the private sector and with international partners to unlock the full potential of this technology.

We are both, therefore, delighted to be jointly leading efforts in this area, and look forward to working with other departments on seizing the opportunity as well as understanding how its use can be implemented for the benefit of UK citizens and the economy.

THE RT HON MATTHEW HANCOCK MP
Minister for the Cabinet Office
and Paymaster General

THE RT HON ED VAIZEY MP
Minister of State for Culture
and The Digital Economy

Executive Summary and Recommendations

Introduction

Algorithms that enable the creation of distributed ledgers are powerful, disruptive innovations that could transform the delivery of public and private services and enhance productivity through a wide range of applications.

Ledgers have been at the heart of commerce since ancient times and are used to record many things, most commonly assets such as money and property. They have moved from being recorded on clay tablets to papyrus, vellum and paper. However, in all this time the only notable innovation has been computerisation, which initially was simply a transfer from paper to bytes. Now, for the first time algorithms enable the collaborative creation of digital distributed ledgers with properties and capabilities that go far beyond traditional paper-based ledgers.

A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network.

Underlying this technology is the 'block chain', which was invented to create the peer-to-peer digital cash Bitcoin in 2008. Block chain algorithms enable Bitcoin transactions to be aggregated in 'blocks' and these are added to a 'chain' of existing blocks using a cryptographic signature. The Bitcoin ledger is constructed in a distributed and 'permissionless' fashion, so that anyone can add a block of transactions if they can solve a new cryptographic puzzle to add each new block. The incentive for doing this is that there is currently a reward in the form of twenty five Bitcoins awarded to the solver of the puzzle for each 'block'. Anyone with access to the internet and the computing power to solve the cryptographic puzzles can add to the ledger and they are known as 'Bitcoin miners'. The mining analogy is apt because the process of mining Bitcoin is energy intensive as it requires very large computing power. It has been estimated that the energy requirements to run Bitcoin are in excess of 1GW and may be comparable to the electricity usage of Ireland.

Bitcoin is an online equivalent of cash. Cash is authenticated by its physical appearance and characteristics, and in the case of banknotes by serial numbers and other security devices. But in the case of cash there is no ledger that records transactions and there is a problem with forgeries of both coins and notes. In the case of Bitcoins, the ledger of transactions ensures their authenticity. Both coins and Bitcoins need to be stored securely in real or virtual wallets respectively — and if these are not looked after properly, both coins and Bitcoins can be stolen. A fundamental difference between conventional currency and Bitcoins is that the former are issued by central banks, and the latter are issued in agreed amounts by the global 'collaborative' endeavour that is Bitcoin. Cash as a means of exchange and commerce dates back millennia and in that respect there is a lineage that links cowrie shells, hammered pennies and Bitcoin.

But this report is not about Bitcoin. It is about the algorithmic technologies that enable Bitcoin and their power to transform ledgers as tools to record, enable and secure an enormous range of transactions. So the basic block chain approach can be modified to incorporate rules, smart contracts, digital signatures and an array of other new tools.

Distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. In the NHS, the technology offers the potential to improve health care by improving and authenticating the delivery of services and by sharing records securely according to exact rules. For the consumer of all of these services, the technology offers the potential, according to the circumstances, for individual consumers to control access to personal records and to know who has accessed them.

Existing methods of data management, especially of personal data, typically involve large legacy IT systems located within a single institution. To these are added an array of networking and messaging systems to communicate with the outside world, which adds cost and complexity. Highly centralised systems present a high cost single point of failure. They may be vulnerable to cyber-attack and the data is often out of sync, out of date or simply inaccurate.

In contrast, distributed ledgers are inherently harder to attack because instead of a single database, there are multiple shared copies of the same database, so a cyber-attack would have to attack all the copies simultaneously to be successful. The technology is also resistant to unauthorised change or malicious tampering, in that the participants in the network will immediately spot a change to one part of the ledger. Added to this, the methods by which information is secured and updated mean that participants can share data and be confident that all copies of the ledger at any one time match each other.

But this is not to say that distributed ledgers are invulnerable to cyber-attack, because in principle anyone who can find a way to 'legitimately' modify one copy will modify all copies of the ledger. So ensuring the security of distributed ledgers is an important task and part of the general challenge of ensuring the security of the digital infrastructure on which modern societies now depend.

Governments are starting to apply distributed ledger technologies to conduct their business. The Estonian government has been experimenting with distributed ledger technology for a number of years using a form of distributed ledger technology known as Keyless Signature Infrastructure (KSI), developed by an Estonian company, Guardtime.

KSI allows citizens to verify the integrity of their records on government databases. It also appears to make it impossible for privileged insiders to perform illegal acts inside the government networks. This ability to assure citizens that their data are held securely and accurately has helped Estonia to launch digital services such as e-Business Register and e-Tax. These reduce the administrative burden on the state and the citizen. Estonia is one of the 'Digital 5' or D5 group of nations, of which the other members are the UK, Israel, New Zealand and South Korea. There are opportunities for the UK to work with and learn from these and other like-minded governments in the implementation of block chain and related technologies.

The business community has been quick to appreciate the possibilities. Distributed ledgers can provide new ways of assuring ownership and provenance for goods and intellectual property. For example, Everledger provides a distributed ledger that assures the identity of diamonds, from being mined and cut to being sold and insured. In a market with a relatively high level of paper forgery, it makes attribution more efficient, and has the potential to reduce fraud and prevent 'blood diamonds' from entering the market.

An important challenge for this new set of technologies is communication of its significance to policymakers and to the public — this is one of the important purposes of this report.

The first difficulty in communication is the strong association of block chain technology with Bitcoin. Bitcoin is a type of cryptocurrency, so called because cryptography underpins the supply and tracking of the currency. Bitcoin creates suspicion amongst citizens and government policymakers because of its association with criminal transactions and 'dark web' trading sites, such as the now defunct Silk Road. But digital cryptocurrencies are of interest to central banks and government finance departments around the world which are studying them with great interest. This is because the electronic distribution of digital cash offers potential efficiencies and, unlike physical cash, it brings with it a ledger of transactions that is absent from physical cash.

The second difficulty in communication is the bewildering array of terminology. This terminology is clarified by Simon Taylor who has provided a set of definitions at the end of this summary. A particular term that can cause confusion is 'distributed', which can lead to the misconception that because something is distributed there is therefore no overall controlling authority or owner. This may or may not be the case — it depends on the design of the ledger. In practice, there is a broad spectrum of distributed ledger models, with different degrees of centralisation and different types of access control, to suit different business needs. These may be 'unpermissioned' ledgers that are open to everyone to contribute data to the ledger and cannot be owned; or 'permissioned' ledgers that may have one or many owners and only they can add records and verify the contents of the ledger.

The key message is that, by fully understanding the technology, government and the private sector can choose the design that best fits a particular purpose, balancing security and central control with the convenience and opportunity of sharing data between institutions and individuals.

As with most new technologies, the full extent of future uses and abuses is only visible dimly. And in the case of every new technology the question is not whether the technology is 'in and of itself' a good thing or a bad thing. The questions are: what application of the technology? for what purpose? and applied in what way and with what safeguards?

To help answer these questions, the Government Office of Science established a senior group of experts from business, government and academia to assess the opportunities for distributed ledgers to be used within government and the private sector, and to determine what actions government and others need to take to facilitate the beneficial use of distributed ledger technology and to avoid possible harms. The aim was to decrypt the terminology behind the technology for policy audiences and provide policymakers with the vision and evidence to help them to decide where action is necessary, and how best to deploy it.

In summary, distributed ledger technology provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector.

This executive summary now sets out the eight main recommendations from our work. These are presented in the context of a summary of the key points from the seven chapters of evidence which cover vision, technology, governance, privacy and security, disruptive potential, applications and global perspective. The chapters have been written by experts in distributed ledger technology in a style that should be accessible to non-experts. I am extremely grateful to these experts for their guidance and thoughtful contributions.

Mark Walport, Chief Scientific Adviser to HM Government, December 2015

Vision

Distributed ledgers offer a range of benefits to government and to other public and private sector organisations. As their name implies, they can be distributed extremely widely in a precisely controlled fashion. They are highly efficient because changes by any participant with the necessary permission to modify the ledger are immediately reflected in all copies of the ledger. They can be equally robust in rejecting unauthorised changes, so corrupting the ledger is extremely difficult. However, distributed ledgers should not be seen as an end in themselves. It is only when they have other applications — such as smart contracts — layered on top on them, that their full potential can be realised.

The first role for government in supporting the development of distributed ledgers is to develop a clear vision of how this technology can improve the way government does its business and is able to deliver services to citizens. This needs to be followed by government acting as an expert customer to implement the technology — procuring distributed ledger solutions where they are applicable. In doing so, government can support and influence the development of economic activity in this sector, including new and growing businesses as well as larger incumbent businesses.

The opportunity is for government to enable a future where the delivery of government services is more personal, immediate and efficient. Wherever appropriate, citizens should have the opportunity to signal their individual preferences and needs through participation in smart contracts. The implementation of distributed ledgers with embedded smart contracts should lead to substantial improvements in compliance, cost-efficiency and accountability.

The UK Government Digital Service is developing a digital platform for government to deliver its services and distributed ledgers could be at the heart of this.

Recommendation 1: *We recommend that government should:*

- *Provide ministerial leadership to ensure that government provides the vision, leadership and the platform for distributed ledger technology within government. Specifically, the Government Data Service should lead work in government as a user of distributed ledgers and the DCMS Digital Economy Unit should lead work on government as an enabler of distributed ledgers (working with the Department of Business, Innovation and Skills and with Innovate UK).*
- *The Government Digital Service and the DCMS Digital Economy Unit should develop a high-level capability road map and a supporting outline plan based on the work of this report and very early stage activity already underway in departments, and deliver this in a timely fashion; and continue to oversee the recommendations made in the rest of this report, to maintain momentum and rapid action. In undertaking this work, they should work closely with other government departments and with industry and academia and should consider setting up a time-limited expert advisory group in support.*

Technology

Distributed ledger technology is still at a very early stage of development. The development of block chain technology is but the first, though very important step towards a disruptive revolution in ledger technology that could transform the conduct of public and private sector organisations. The technology can be adopted so that ‘legitimate’ changes to ledgers can be made in principle by anyone (an ‘unpermissioned’ ledger), or by a limited number of individuals or even a single authorised person (in a ‘permissioned’ ledger). For government applications, ‘permissioned’ ledgers are likely to be more appealing than Bitcoin’s unpermissioned model, because they allow the owner, or owners, of the data to enforce rules on who is and is not allowed to use the system. Distributed ledgers have the added advantage of moving a lot of the complexity of managing security into the background, making systems easier and cheaper to use.

There are many unsolved problems to tackle before the full potential of this and related technologies can be realised, including the resolution of issues of privacy, security, performance and scalability. There is also an extraordinary array of opportunities to develop algorithms that will add sophistication to ledgers by supporting ‘smart’ contracts, signatures and other applications. These will enhance and diversify the value and range of uses of ledgers. This field is developing rapidly and many of these problems are already being investigated and, in some cases, solved. If government waits for ‘perfect’ solutions, it will miss the opportunity to shape and procure implementations of the technology that will provide maximum benefit to the public sector, and the UK may lose opportunities for economic benefit as well.

As well as ensuring that the technology is robust and scalable, we need to understand the ethical and social implications of different potential uses and the financial costs and benefits of adoption. With respect to research and development, the UK is in a good position, though we cannot take this for granted as there is interest and competition in development of distributed ledger technology around the world.

The research councils are playing an important role, led by the EPSRC and ESRC, supporting research in universities and in the newly-created Alan Turing Institute. There is also an important role for business to invest in research and development, and key opportunities for joint public and private investment to tackle generic problems around security, privacy and the development of standards — all areas where industrial advantage will be gained by co-operation rather than competition.

Existing digital investments by the government and private sector include the Digital Catapult, Future Cities Catapult and Open Data Institute. Added to this are groupings such as the Whitechapel Think Tank which can provide a focal point for discussion and sharing ideas. This means that the UK is in a good position from which to build a solid distributed ledger research and testing capability. But there is a danger that we will not get the most from this potentially fragmented activity and there is a strong case that the research and development community in the public and private sectors should ‘self-organise’ in a way that encourages co-operation where appropriate and competition where it will stimulate the most creative research.

Our next two recommendations are aimed at encouraging further research and establishing UK capability to trial and experiment with different distributed ledger solutions:

Recommendation 2: *The UK research community should invest in the research required to ensure that distributed ledgers are scalable, secure and provide proof of correctness of their contents. They need to provide high-performance, low-latency operations, appropriate to the domain within which the technology is being deployed. They need to be energy efficient. The newly-created Alan Turing Institute, working with groupings such as the Whitechapel Think Tank, could play an important role in co-ordinating and 'self-organising' the public and private research and development sector interested in this and related technologies. The private sector should consider investing in the Alan Turing Institute to support the pre-competitive research that will ultimately facilitate new commercial applications that are robust and secure. This includes work on obvious areas such as cryptography and cybersecurity but also extends to the development of new types of algorithm.*

Recommendation 3: *Government could support the creation of distributed ledger demonstrators for local government that will bring together all the elements necessary to test the technology and its application. A demonstrator at a city level could provide important opportunities for trialling and implementing distributed ledger technologies. Innovate UK could use its work with cities in the development of 'city deals' to implement the development of a city demonstrator.*

Governance

Effective governance and regulation are key to the successful implementation of distributed ledgers. Governance comprises the rules set by the owners and participants of the ledger that safeguard their private interests. This needs to be supplemented by regulation and / or legislation, which comprises the framework of rules that are set by an outside authority to protect the broader interests of society. Government legislates and creates the framework for regulation, singly or in partnership with other governments, and usually creates or enlists a regulator accountable to government to undertake the work.

In the case of the digital world, there are two sets of rules or codes that control the operation of digital technologies. The first is the classical set of rules provided by the legislative framework, the code of law and regulation. The second is the set of rules that determine the operation of the algorithms encoded by the software. This is the technical code, and there needs to be at least as much focus on ensuring the rigour of the technical code as on legislative code.

Successful implementation of a distributed ledger will require a combination of governance to protect the participants and stakeholders and regulation to ensure the system is resilient to systemic risk or criminal activity. The challenge is to strike the balance between safeguarding the interests of participants in the system and the broader interests of society whilst avoiding the stifling of innovation by excessively rigid structures.

There are also opportunities to take advantage of the potential interactions between legal and technical code. For example, public regulatory influence could be exerted through a combination of legal and technical code, rather than exclusively through legal code as at present. In essence technical code could be used to assure compliance with legal code, and, in doing so, reduce the costs of legal compliance. This could provide a ‘use case’ for the use of technology to enhance regulation, so-called RegTech, which formed one of the key recommendations of the FinTech report from the Government Office for Science[1].

Determining the optimum balance between governance and regulation, and between legal code and technical code, is going to require unusual mixes of skills, including the need for lawyers, mathematicians and computer experts to work together to resolve many of the key issues, which are outlined in Chapter 3.

Recommendation 4: *Government needs to consider how to put in place a regulatory framework for distributed ledger technology. Regulation will need to evolve in parallel with the development of new implementations and applications of the technology. As part of the consideration of regulation, government should also consider how regulatory goals could be achieved using technical code as well as legal code. The DCMS Digital Economy Unit could take ownership of this recommendation.*

Security and privacy

Criminals have moved away from cracking metal safes and bank vaults. The money is now in their digital equivalents and these are proving vulnerable to the hackers and crackers of the codes of the digital world. The cryptographic codes of the digital world are extremely hard to break, but however hard these may be, they can be vulnerable to being bypassed. Bypass mechanisms range from the human, who may give away the key accidentally or deliberately, to the presence of ‘back doors’ due to deficiencies in the software code. The hardware hosting distributed ledgers may provide additional vulnerabilities and equal attention should be paid to the resilience and security of hardware systems.

In the case of Bitcoin, the ‘wallets’ that hold the currency have proved vulnerable to theft — but the ledger itself has remained resilient, though in principle it would be vulnerable if over 50% of the computer processing power for the Bitcoin ledger fell into the hands of a single malevolent individual or organisation. Indeed, a great strength of distributed ledgers is that they should be highly resilient to attack.

However, it is not only the integrity of the ledger that matters. Privacy and confidentiality are also key issues. Depending on the nature of the ledger, it may hold personal confidential records that could range from financial to familial and health. The opportunity is for distributed ledger technologies to provide much greater security for these data than is available in current databases, but this is not a given. This is another area where much research and development is needed as part of the development of the technology.

Security and privacy are areas where Government has an important role to play, so our next recommendation is:

Recommendation 5: *Government needs to work with academia and industry to ensure that standards are set for the integrity, security and privacy of distributed ledgers and their contents. These standards need to be reflected in both regulatory and software code.*

For each particular use of the technology, government and private sector users, as appropriate, should conduct a bespoke risk assessment to identify the relevant threats. The Centre for the Protection of National Infrastructure (CPNI) and CESG should keep a watching brief on distributed ledger technology and play a central role inside and outside government in providing expert advice on ensuring the integrity, security and privacy of distributed ledgers. As suggested in recommendation 2, the newly created Alan Turing Institute, working with groupings such as the Whitechapel Think Tank and with CESG could play an important role in co-ordinating and 'self-organising' the public and private research and development sector.

It must not be overlooked that the software and hardware systems can become degraded over time, as better technology emerges and hostile agents learn 'new tricks'. So for systems intended to have a long lifetime, the initial design should make it straightforward to update hardware and software components during that lifetime. Additionally, as part of trialling new implementations of the technology, it is important to include penetration testing at both the system and user levels.

Trust and interoperability

As set out in Chapter 7 on global perspectives, trust is a risk judgement between two or more people, organisations or nations. In cyberspace, trust is based on two key requirements: prove to me that you are who you say you are (authentication); and prove to me that you have the permissions necessary to do what you ask (authorisation). In return, I will prove to you that I am trustworthy by delivering services or products to you in a secure, efficient and reliable fashion.

Authentication and identification are interlinked but they are not the same thing. Authentication does not require that I know your identity but it does require that you provide me a token that is inextricably linked to your identity, for example the pin number associated with a credit or debit card, or a fingerprint allied to a biometric passport or other document. Equally, when I provide my authentication token to you, I need assurance that I am providing it to the correct individual or organisation, ie that you are who you claim to be. So it is equally important that organisations can provide authentication to their users, be they individuals, other organisations or government.

The opportunity in the digital environment is to use and create much more powerful and robust identity management tools that provide authentication whilst protecting privacy. One such system is public key infrastructure (PKI) relying on a cryptographic standard called X.509. Organisations using PKI can federate in order to provide, share and potentially simplify the secure delivery of services or products. Another important international standard is being developed for organisational identification, known as the Register of Legal Organisations (ROLO), and this may help to underpin the authentication of organisations as opposed to individuals.

Another key enabler of secure authenticated interactions by individual users is the use of smartphones as the *de facto* trusted user device. The latest smart phones incorporate important security features such as a 'Trusted Platform Module', which secures digital certificates and cryptographic keys for authentication, encryption and signing, and a 'Trusted Execution Environment' and a 'Trusted User Interface', each of which are resistant to interference by 'malware'.

This discussion of authentication shows that, in order to maximise the power of distributed ledgers, these may need to be interoperable with other ledgers. However, maximising the potential of interoperability goes far beyond interoperability of authentication — it requires agreements about data interoperability, policy interoperability and the effective implementation of international standards.

Recommendation 6: *This recommendation is linked to Recommendation 5. Government needs to work with academia and industry to ensure that the most effective and usable identification and authentication protocols are implemented for both individuals and organisations. This work needs to go hand in hand with the development and implementation of international standards.*

A disruptive future – some potential use cases for government

Distributed ledgers have the potential to be radically disruptive. Their processing capability is real time, near tamper-proof and increasingly low-cost. They can be applied to a wide range of industries and services, such as financial services, real estate, healthcare and identity management. They can underpin other software- and hardware-based innovations such as smart contracts and the Internet of Things. Furthermore, their underlying philosophy of distributed consensus, open source, transparency and community could be highly disruptive to many of these sectors.

Like any radical innovation, as well as providing opportunities distributed ledgers create threats to those who fail or are unable to respond. In particular, through their distributed consensual nature they may be perceived as threatening the role of trusted intermediaries in positions of control within traditionally hierarchical organisations such as banks and government departments.

With its wide range of stakeholders, services and roles, the government has a multitude of different operations. Some distribute value rather than create it, and others create and maintain effective regulatory regimes. Many of these activities will be enhanced by innovations afforded by distributed ledgers, and others will be challenged.

Ultimately, the best way to develop a technology is to use it in practice. The expert group that supported the development of this report has scoped some specific examples of potential uses by the UK government, and these are set out in five use case studies in Chapter 6

- protecting critical infrastructure against cyberattacks
- reducing operational costs and tracking eligibility for welfare support, while offering greater financial inclusion
- transparency and traceability of how aid money is spent
- creating opportunities for economic growth, bolstering SMEs and increasing employment
- reducing tax fraud

Each of these case studies provides an overview of the distributed ledger proposition, its potential benefits and an assessment of the maturity level of the technology to deliver the application.

Only a tiny fraction of the possible applications are identified in this report but we believe they provide a good starting point for government to start piloting the technology within departments. So our final set of recommendations are aimed at implementing trials of distributed ledger technology and developing government capability:

Recommendation 7: *Understanding the true potential of distributed ledgers requires not only research but also using the technology for real life applications. Government should establish trials of distributed ledgers in order to assess the technology's usability within the public sector.*

We suggest that the trials should be co-ordinated in a similar fashion to the way that clinical trials are implemented, reported and assessed, in order to ensure uniformity and maximize the rigour of the process. The outcome of these trials and the lessons learnt should feed into the road-map proposed in Recommendation 1.

Areas where we believe work could be taken forward include the protection of national infrastructure, reducing market friction for SMEs and the distribution of funds from DWP and other government departments. During the development of this report, we found a small number of officials who are already thinking deeply about potential uses for distributed ledger technology by government. We recommend that these individuals be strongly supported and encouraged to move ahead in partnerships between government departments and GDS.

Recommendation 8: *As well as top-down leadership and coordination, there is also a need to build capability and skills within government. We recommend the establishment of a cross-government community of interest, bringing together the analytical and policy communities, to generate and develop potential 'use cases' and create a body of knowledge and expertise within the civil service. GDS and the Data Science Partnership between GDS, Office for National Statistics, Cabinet Office and the Government Office for Science could act as the convenors of this community of interest. There are important opportunities for government to stimulate the business sector by acting as a smart customer in procuring distributed ledger applications.*

Conclusion – taking a global perspective

The UK is not alone in recognising the importance of distributed ledger technologies. Other countries, large and small, are already moving quickly to adopt distributed ledgers — and the case study of Estonia shows how quickly a small country with an effective digitally-aware leadership can progress. However, there is still time for the UK to position itself within this leading group — indeed, it is essential for it to do so, given the importance of the financial and services sector to the UK economy.

Patrick Curry, Christopher Sier and Mike Halsall have considered in Chapter 7 the features of advancing digital nations and argue that the hallmarks of these include:

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

We are still at the early stages of an extraordinary post-industrial revolution driven by information technology. It is a revolution is bringing important new benefits and risks. It is already clear that, within this revolution, the advent of distributed ledger technologies is starting to disrupt many of the existing ways of doing business.

The earliest accounting records of humans date back to Babylon, Assyria and Sumer, over 5000 years ago. Many clay tablets have survived as a record of the early technological revolutions in the development of writing, counting and money. It is less clear whether digital records will have the same longevity as clay tablets. But, leaving that aside, it is clear that there is a huge opportunity for the UK to develop and use distributed ledger technology for the benefit of citizens and the economy. There are a series of ‘grand challenges’ to tackle to maximise the benefits and minimise the harms of the extraordinary developments in information technology. This report sets out some key recommendations for the government, based on expert evidence. The most important of these is the need for close partnership between the public and private sector, within the UK and between the UK and other nations.

Definitions

The terminology of this new field is still evolving, with many using the terms block chain (or blockchain), distributed ledger and shared ledger interchangeably. Formal definitions are unlikely to satisfy all parties — but for the purposes of this report, the key terms are as follows:

- A **block chain** is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a **ledger**, which can be shared and corroborated by anyone with the appropriate permissions.

  There are many ways to corroborate the accuracy of a ledger, but they are broadly known as **consensus** (the term 'mining' is used for a variant of this process in the cryptocurrency Bitcoin) — see below.

  If participants in that process are preselected, the ledger is **permissioned**. If the process is open to everyone, the ledger is **unpermissioned** — see below.

  The real novelty of block chain technology is that it is more than just a database — it can also set rules about a transaction (business logic) that are tied to the transaction itself. This contrasts with conventional databases, in which rules are often set at the entire database level, or in the application, but not in the transaction.

- **Unpermissioned ledgers** such as Bitcoin have no single owner — indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

  Unpermissioned ledgers can be used as a global record that cannot be edited: for declaring a last will and testament, for example, or assigning property ownership. But they also pose a challenge to institutional power structures and existing industries, and this may warrant a policy response.

- **Permissioned ledgers** may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. Requiring many government departments to validate a record could give a high degree of confidence in the record's security, for example, in contrast to the current situation where departments often have to share data using pieces of paper. A permissioned ledger is usually faster than an unpermissioned ledger.

- **Distributed ledgers** are a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum.

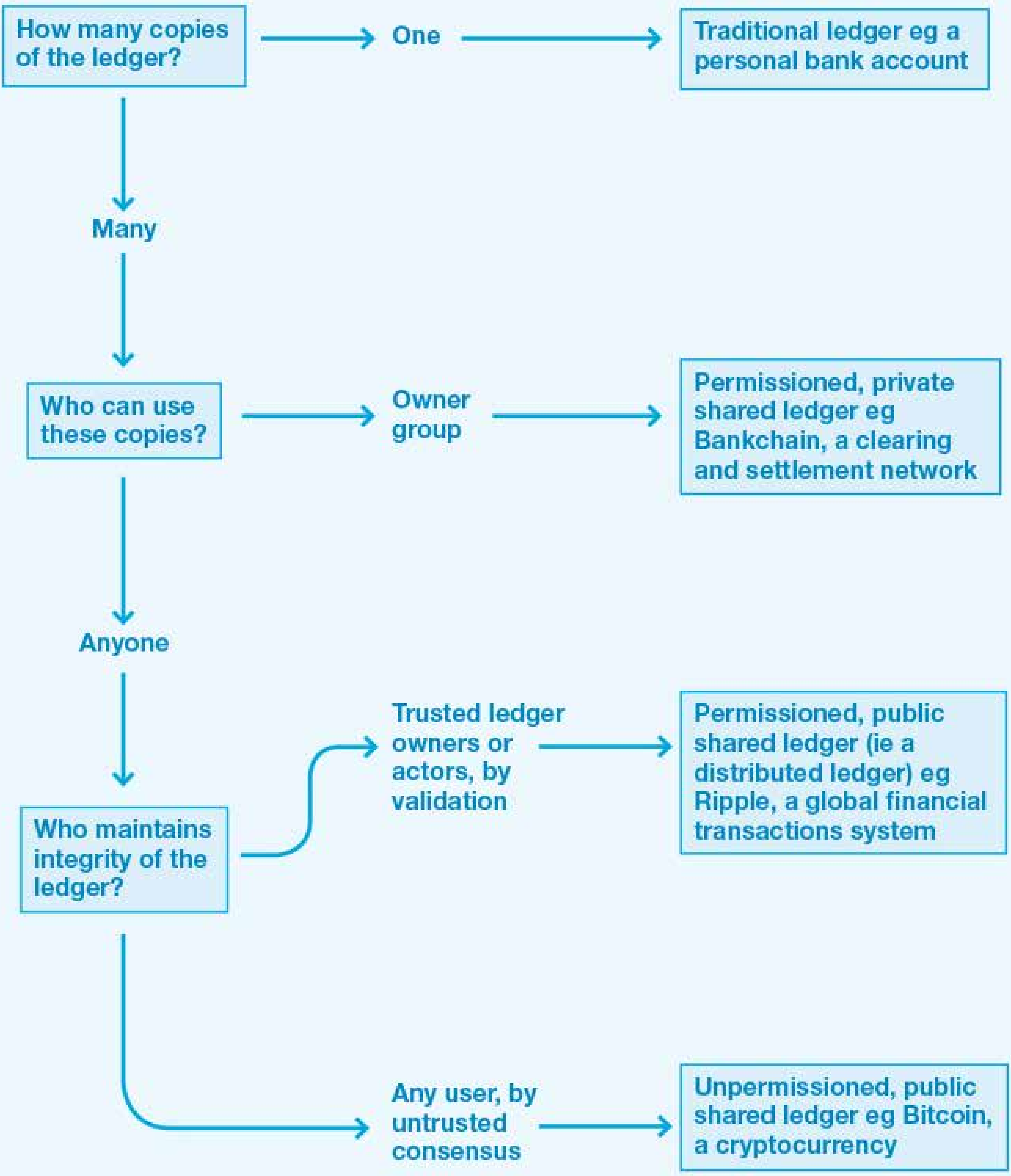
A distributed ledger requires greater trust in the validators or operators of the ledger. For example, the global financial transactions system Ripple selects a list of validators (known as Unique Node Validators) from up to 200 known, unknown or partially known validators who are trusted not to collude in defrauding the actors in a transaction. This process provides a digital signature that is considered less censorship resistant than Bitcoin's, but is significantly faster.

- A **shared ledger** is a term coined by Richard Brown, formerly of IBM and now Chief Technology Officer of the Distributed Ledger Group, which typically refers to any database and application that is shared by an industry or private consortium, or that is open to the public. It is the most generic and catch-all term for this group of technologies.

  A shared ledger may use a distributed ledger or block chain as its underlying database, but will often layer on permissions for different types of users. As such, 'shared ledger' represents a spectrum of possible ledger or database designs that are permissioned at some level. An industry's shared ledger may have a limited number of fixed validators who are trusted to maintain the ledger, which can offer significant benefits.

- **Smart contracts** are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. The potential benefits of smart contracts include low contracting, enforcement, and compliance costs; consequently it becomes economically viable to form contracts over numerous low-value transactions. The potential risks include a reliance on the computing system that executes the contract. At this stage, the risks and benefits are largely theoretical because the technology of smart contracts is still in its infancy, and some time away from widespread deployment.

Distributed Ledger Taxonomy



How many copies of the ledger?

One

Traditional ledger eg a personal bank account

Many

Who can use these copies?

Owner group

Permissioned, private shared ledger eg Bankchain, a clearing and settlement network

Anyone

Who maintains integrity of the ledger?

Trusted ledger owners or actors, by validation

Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system

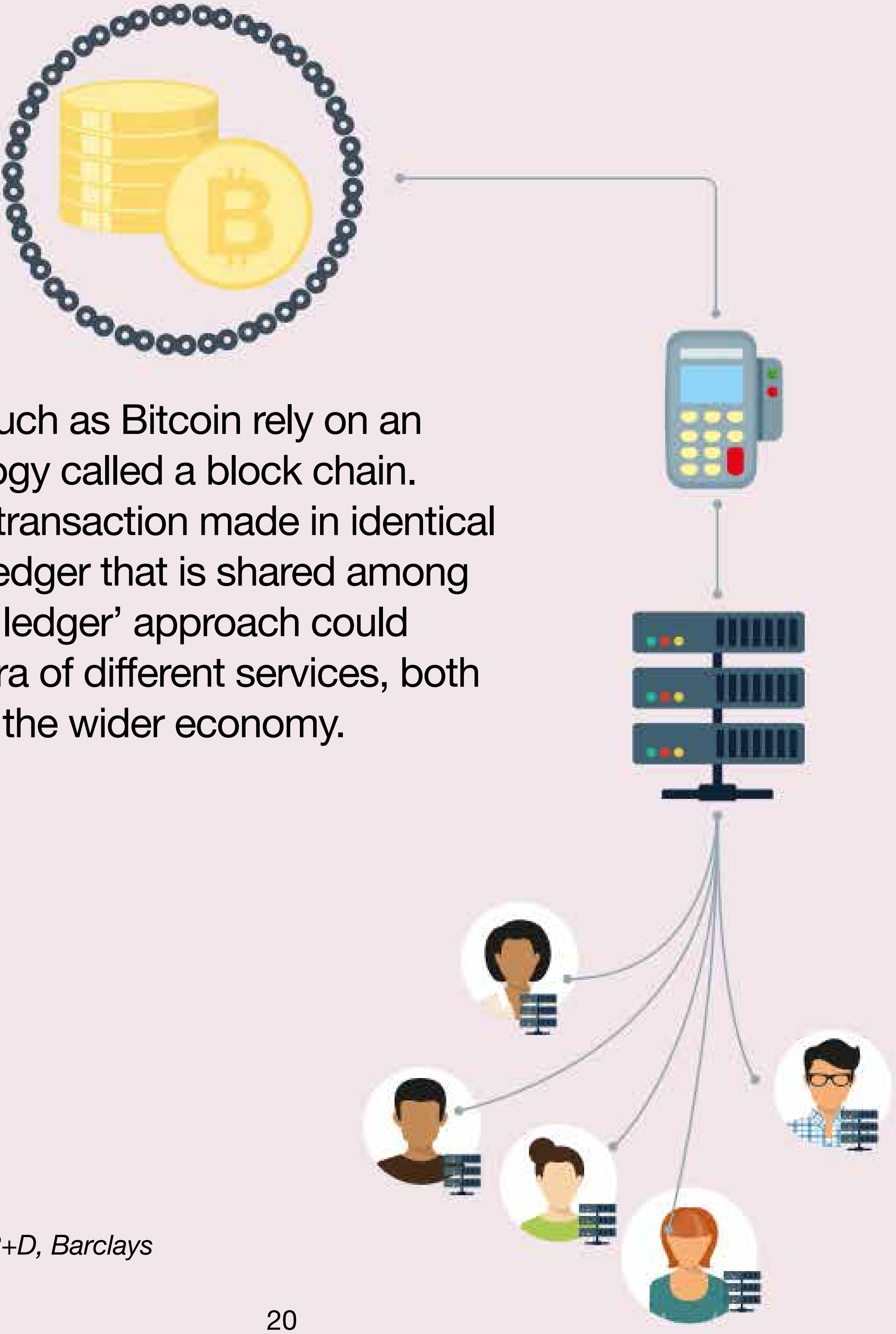
Any user, by untrusted consensus

Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency

Figure courtesy of Dave Birch (Consult Hyperion)

CHAPTER 1

Vision



Digital currencies such as Bitcoin rely on an underlying technology called a block chain. This records every transaction made in identical copies of a digital ledger that is shared among users. This ‘shared ledger’ approach could streamline a plethora of different services, both in government and the wider economy.

Author
Simon Taylor,
VP for Blockchain R+D, Barclays

Chapter 1:Vision

Introduction

Digital currencies such as Bitcoin have pioneered a new approach to tracking financial transactions. Their underlying technology — commonly called a block chain — records every transaction made in that currency in identical copies of a digital ledger that is shared among the currency's users.

Financial institutions, regulators, central banks and governments are now exploring the possibilities of using this 'shared ledger' approach to streamline a plethora of different services, both in government and the wider economy.

Many of these potential applications are medium-term prospects, but the long development cycles for government and the private sector, and the early promise that significant efficiencies could be gained, suggest that ministers and civil servants must now begin to consider how this technology could benefit them. This chapter outlines those opportunities.

What is a shared ledger?

A shared ledger is essentially a database that keeps track of who owns a financial, physical or electronic asset: a diamond, a unit of currency, or items inside a shipping container, for example. Crucially, every participant can keep a copy of the block chain, which is updated automatically every time a new transaction occurs. The security and accuracy of the information is maintained through mathematics — specifically by cryptography — to ensure that all copies of the ledger match each other. Almost anything that exists on paper today could exist on a shared ledger (see Chapter 2 for a more detailed discussion of shared ledger technology).

Since its launch in 2008, Bitcoin has relied on block chain technology. Many clichés and misconceptions have grown up around the digital currency and its underlying principles. Its associations with Silk Road, the digital black market, have left some people with the impression that Bitcoin is intrinsically linked to money laundering and terrorists. That misconception continues to affect how people think about block chain technology.

In fact, shared ledgers and databases may offer some major benefits to government and financial services, thanks to four important properties of block chain technologies.

1) **Reconciliation Through Cryptography**. Institutions such as businesses and governments currently send messages to each other to pass on details of transactions. Once the message is received, each institution then updates its own ledger. But today, there is no easy way to ensure that these copies match. Block chains can solve this in a number of ways: by simply sharing the same underlying data, for example, or by providing 'proof points' to verify the data. This approach could also be applicable to government data sets. The different actors (users) of the ledger come to a consensus about the state of the underlying data through a number of different consensus algorithms (eg Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance).

2) **Replicated to Many Institutions**. Many parties can have a copy of some

or all of the data, making it less likely that there is a single point of failure. Replication is a significant challenge for current database technologies, creating cost and complexity in industry and government IT projects. An additional benefit of this technology is that if one ledger is compromised, the remainder are not. Many parties can also confirm that those records have been added by performing the reconciliation calculations themselves.

3) **Granular Access Control.** Distributed ledgers use ‘keys’ and signatures to control who can do what inside the shared ledger. These keys can be assigned specific capabilities only under certain conditions. For example, a regulator may have a ‘view key’ that allows it to see all of an institution’s transactions, but only when a key owned by a court gives it permission (control) to do so.

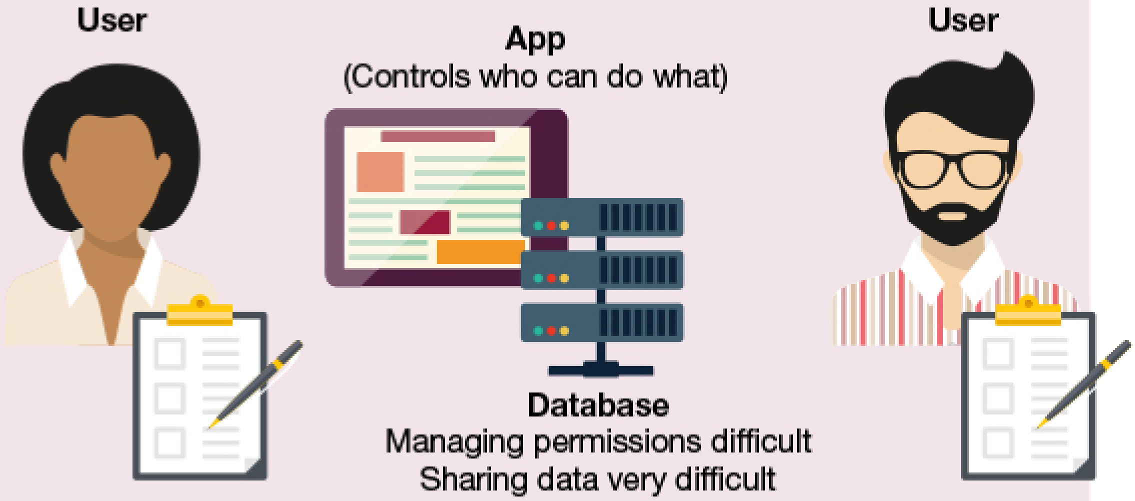
4) **Granular Transparency and Privacy.** Because many parties have a copy of the ledger (point 1), and many parties can verify every record (point 2), a shared ledger has a high degree of transparency. This allows a regulator or an independent body such as the judiciary to see with confidence that the contents of a database had not been edited or modified in any fraudulent way. Given the right conditions, it also allows them to unlock records that would otherwise be completely private and un-viewable. This could be useful for businesses (eg banks) in their regulatory reporting, fraud prevention, and could even empower citizens to hold the government to account (see Chapter 5 for a more extensive discussion). Records are added with a unique cryptographic signature that proves the right participant has added the right record according to the right rules.

When combined, these properties can solve challenges that were previously very expensive or challenging.

What is a smart contract?

If a block chain is the database, then the smart contract is the application layer that makes much of the promise of block chain technology a reality. Most conventional contracts have no direct relationship with the computer code that executes them (see Chapter 3). In many cases the paper contract is archived, and the software will execute an approximation of the contract’s terms written in computer code (see Fig. 1).

Figure 1: Conventional contracts have no direct relationship with the computer code (app) that executes them.


User
App
(Controls who can do what)
User
Database
Managing permissions difficult
Sharing data very difficult

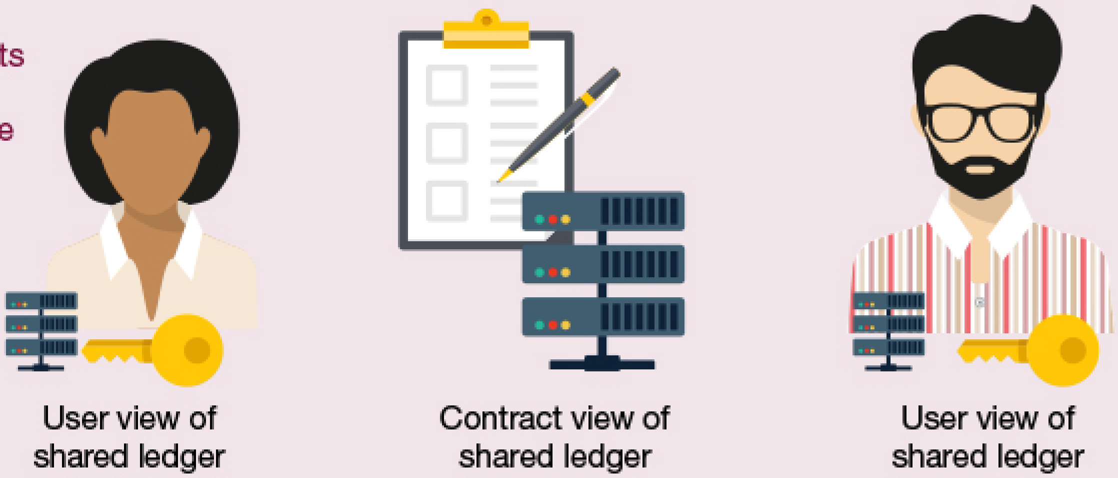

User view of shared ledger
Contract view of shared ledger
User view of shared ledger

Figure 2: Smart contracts contain the computer code that executes the contract.

This is quite effective when signing up to use a service (eg video on demand), but highly challenging when delivering multiple complex services to one user (eg updating an address in multiple government department databases). This has resulted in ever more complex data protection and data privacy legislation to manage the confidentiality and privacy of the individual in an assured way. In addition, activities like data sharing or agreeing contracts have remained in paper form, rather than being automated in the wider economy.

Combining the key attributes of a shared ledger (reconciliation through cryptography, replicated to many institutions, granular access control,

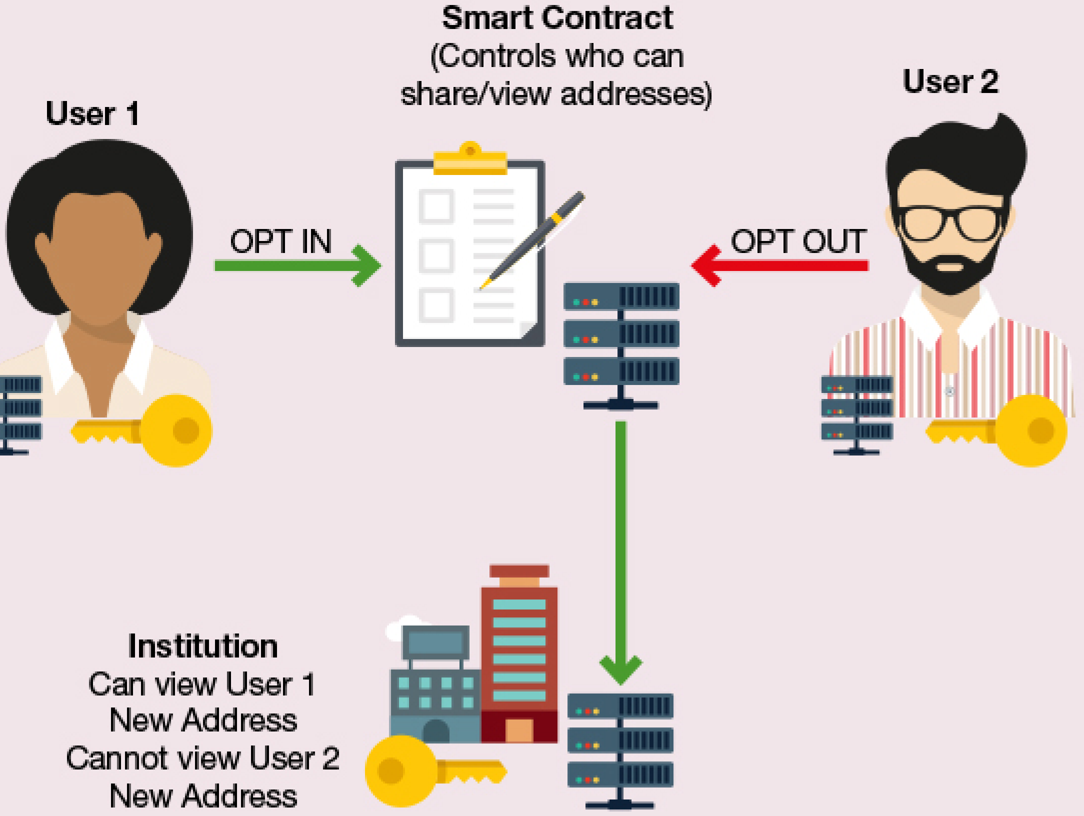

Smart Contract
(Controls who can share/view addresses)
User 1
User 2
OPT IN
OPT OUT
Institution
Can view User 1 New Address
Cannot view User 2 New Address

Figure 3: Smart contracts can control which institutions access private data.

and granular transparency and privacy) with smart contracts may create opportunities to address some of these challenges, by allowing data to either be replicated or shared under specific conditions. If two users sign a smart contract, it will then contain logic that operates on the data in all parts of the shared ledger (see Fig. 2). This could facilitate the automation or removal of manual process in government and private sector institutions, which may drive efficiencies in productivity and growth. Note there are other challenges like management of legacy databases and processes, but the "permissioning" across multiple systems is where Smart Contracts come into their own.

In an alternative scenario (Fig. 3), User 1 opts in to a smart contract on a shared ledger to share their address with an institution that possesses a blue key (there may be many other institutions, with many different keys). But User 2 has opted out of sharing their address, so the institution only receives a copy of the latest address from User 1. This may be useful when an individual changes their address via their local council, because the change could be reflected on their passport, drivers licence and other key department databases. Services such as Onename.io use this concept today with social networks, and it could be extended to all institutions.

Smart contracts are being considered for a wide variety of uses, particularly for regulatory compliance, product traceability and service management, and also to defeat counterfeit products and fraud in the following sectors:

- Food
- Financial Services
- Energy
- Pharmaceuticals
- Health
- Aerospace
- Aviation
- Telecommunications
- IT and communications
- Transport
- Utilities
- Agriculture
- Oil and gas

Some of these are discussed later in this chapter, and in Chapters 6 and 7.

In summary, a smart contract is useful when machines, companies or people want to create a digital agreement, with cryptographic certainty that the agreement has been honoured in the ledgers, databases or accounts of all parties to the agreement.

A vision for the future

A key role of democratic government is the appropriate distribution of resource among its citizens, both individual and corporate. This goes beyond the distribution of monetary resource and includes social intangibles such as security, democracy, the conditions for the maintenance of the rule of law; and economic conditions such as the promotion of free markets, keeping inflation low and steady, protecting the rights of private property, and guaranteeing contracts. This distribution in turn is based on an agreement between the citizen and the government on how rules are set (through voting and manifestos).

As that democratic model has developed, the machinery of government (ie the mechanism by which this distribution takes place) has become larger, more centralised and, arguably, more remote from the individual citizen.

The collection of (monetary) resource through taxation of various kinds has become hugely complex and costly, as has its distribution through welfare support, grants and pensions. This complexity may in part derive from its centralised nature.

The private sector has started to recognise that this centralised model delivers poor customer service, is no longer economic and also fails to take into account the full benefits of e-commerce and digital capability. Governments are beginning to recognise that citizens' expectations should be met in similar ways, with real time, personal and digital services offered for all government services. Application of shared ledgers and smart contracts offers the opportunity to put government in the lead in this area, ensuring that the benefits of the technology are enjoyed by those who need it most, not just those who can best afford them.

This trend is also apparent in the growth of the less-formal 'sharing economy', and in popular, social-media led phenomena such as the Arab spring and the Occupy movement. These show a shift in how society communicates and organises itself. To date, however, there has been no successful way to embrace these in a secure way while continuing to promote free markets and guarantee contracts. It is often said that the reason we have never shifted democracy online is because there is no way to be sure who is voting for what without a highly costly and arguably non-libertarian centralised identity system. Assuming this is undesirable, the properties of block chain technology (reconciliation through cryptography, replicated to many institutions, granular access control, and granular transparency and privacy) could be turned to the benefit of citizens.

In addition, the early involvement of government in the development and deployment of block chain technology offers an opportunity for reducing the complexity and cost of government. That would lead to a more personal, immediate and potentially more democratic basis for governance, with consequent increases in compliance, cost-efficiency and accountability.

Steps towards embracing block chain technology

Shared ledger technology is being actively promoted and developed in key global economies such as the United States, China, Singapore and Latin America. The UK has an opportunity to compete in this race by understanding and supporting the growth of this nascent sector.

The government's potential involvement in distributed ledger technology can be seen through three lenses:

- Government: the civil service
- Government: the legislator
- Government: the steward of the economy

Government: the civil service

The civil service has a number of key duties that could be impacted by this technology, with strong use cases focusing on the nexus of privacy, data portability and the sensory capabilities of mobile technology (see Chapter 6 for more detailed case studies).

Government: the legislator

Distributed ledger technology is still young, and likely to see several more cycles of development. As such, the government's actions can target three separate 'horizons' in the technology development process.

Horizon 1: Supporting an Emerging Ecosystem
There are already a number of digital currency exchanges, 'wallet' providers and other service providers both in the Bitcoin ecosystem and in other shared ledger systems. Recognising that the technology and businesses will continue to mature, Horizon 1 activities may include:

- Requiring exchanges to verify the identities of their customers (known as KYC, or 'Know Your Customer' regulation).
- Issuing guidance for the banking sector to demonstrate the difference between the types of companies in this space: (i) those who transfer value via block chain systems; (ii) those who provide software to industries that use block chains; (iii) those who provide block chain-based software to solve conventional business problems.
- Establish security standards for wallet providers.
- Creating challenges for academia and the start-up ecosystem to look at specific gaps in the block chain ecosystem, such as: (i) establishing the appropriate technical architectures; (ii) establishing how the technology could enhance efforts to improve customer identity verification, tackle money laundering, and prevent crime; (iii) establishing how the use of multi-signature wallets can create new government–citizen user experiences and empower citizens to control and audit their own data held by the government.
- Leveraging partners to sustain a co-ordinated conversation between the government and industry.

Horizon 2: Early Trials and Pilots
Where the government has specific opportunities it may wish to begin performing local trials of use cases. Particular questions the government may want to consider are:

- What key utilities could benefit from shared ledger / database technology?
- Where might a trial support policy (eg pension reform, welfare reform)?
- Where can a trial offer the greatest learning opportunity?

Horizon 3: Position the UK as a Leader in the Global Race
Much of the venture capital investment in distributed ledger technology has to date focused on Bitcoin, and the west coast of the United States. But the emerging opportunities for this technology lie in other applications.

- The UK should recognise this nuance and create guidance to that effect through its regulatory bodies (see Chapter 3 for more on governance and regulation).
- The UK could create a centre of excellence for these technologies and add this to the global FinTech / UK Trade and Investment agenda.

Government: the steward of the economy

To understand how the government can best promote and realise the benefit of this technology, it will be helpful to look at use cases in two different areas: financial services; and insurance and other industries.

Financial Services
Examples of where the technology could be applied to the finance sector include:

- Increased efficiency in capital markets
- Reduced fraud and increased efficiency in trade finance

1. Increased efficiency in capital markets

Capital markets still rely on paper records to reconcile a trade between counterparties. While central utilities have been created in the past, the ability to reconcile ('clear') a transaction and be sure that the counterparty has agreed is significant because today it requires reliance. Many of the fines and much of the fixed cost base of banking is based on the concept of reliance. In essence, one bank must rely on the processes of another bank and has no way to verify the behaviour of that bank. A block chain technology can help by showing the chain of transactions (reconciliation through cryptography), and the actors involved, in a way that is transparent to a regulator. In addition, auditing this data is expensive and happens after the trade has taken place. The large banks are now finding appropriate vehicles to collaborate on this technology to unlock efficiencies.

2. Reduced fraud and increased efficiency in trade finance

Trade finance still operates in much the same way as it has for thousands of years. There are often at least 5 or 6 parties involved in the buying or selling of a particular item (eg the buyer, the buyer's bank, the shipping company, the courier, the seller and the seller's bank). There have been attempts to both standardise and create central utilities in trade finance. Shared ledgers offer some unique advantages.

- A 'partially permissioned' system could enable the secure signing of a paper document (eg a bill of lading stating which products were in a container, how many, what colour etc). This could then be signed (provably and digitally) by each of the parties. (Key properties: **High Transparency; Reconciliation Through Cryptography**)
- Rather than simply storing the documents, as is done today, a shared ledger system would record proof of the state of those documents. If adopted more widely, the documents could be distributed via the shared ledger, rather than printed and signed. (Key properties: **Highly Scalable and Replicable**)

Industry and Institutions
1. Asset tracking and provenance assurance

Many items, such as fine art or consumer electronics, physically carry digital markers. There is, however, no global utility to track and trace these items that would offer control of the permissions that determine who can see which assets are being managed. Many organisations rely on paper documents to prove the origins of produce. But there is no way to verify these origins if the paper trail is forged. If parts of that supply chain used a shared ledger, and 'signed' the ledger digitally, it would be clear to all parties that the documents had not been amended or forged in any way.

For example, Provenance.org is a start-up using block chain technology to give retailers confidence in the provenance and sustainability of garments. Retailers currently rely on paper documents to confirm the provenance of garments, but there is no way to ensure that the right person completed those documents, at the right time. Using block chain technology, the appropriate person could digitally sign a contract with their private key, giving a far higher confidence that the right person signed the document at an exact date and time. The nature of block chain technology means that this would be visible to all retailers who had the appropriate privileges.

2. Confidential Use of Data with User Control

Data accuracy and confidential data sharing are key challenges for institutions. Insurance companies can create more accurate products, prices and premiums if they have additional data that is validated as accurate by one or more trusted sources (eg governments or banks). The difficulty has been to do this in a secure way while ensuring that the citizen remains in control of their data.

A block chain would provide proof of how every piece of data was accessed, perhaps using a solution such as Guardtime. Using trusted execution environments (TEEs) in mobile phones, such as ARM's TrustZone chip, any request to access data held in government would be recorded in a block chain. Unless the citizen had granted permission to the insurance company, this data would not move. If any attempt to change or access the data is made, the citizen or relevant authorities would be made aware immediately.

Shared ledger technology, when combined with simple mobile user interfaces, potentially moves a lot of the complexity of managing security into the background. The institutions that choose to adopt this way forward will need to win the confidence of the public, and early trials and implementations will be helpful in achieving this.

3. Industrial Equipment (a linked 'Internet of Things')

It can be difficult to gather accurate, real-time data about industrial equipment across many sectors, including transport, utilities and agriculture. With the advent of the Internet of Things (IoT), some of these difficulties are being addressed with low-cost commodity hardware, but this is potentially vulnerable to attack. According to a recent report[2] from the IBM Institute for Business Value:

> "The result: a proliferation of hundreds of billions of devices that will be no more expensive than their dumb counterparts, yet able to operate and act as part of complex, integrated systems."
>
> "In a network of the scale of the IoT, trust can be very hard to engineer and expensive, if not impossible, to guarantee. For widespread adoption of the ever-expanding IoT, however, privacy and anonymity must be integrated into its design by giving users control of their own privacy. Current security models based on closed source approaches (often described as "security through obscurity") are obsolete and must be replaced by a newer approach – security through transparency."
>
> "In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an "Internet of Decentralized, Autonomous Things" – and thus the democratization of the digital world"

If each device functions both as an autonomous agent, and a part of the whole, there is no central point of failure. In this use case, institutions would apply IoT devices and gain many of the benefits associated with real time data and connectivity outlined in the recent Government Office for Science report on the IoT[3]. Shared ledger and block chain technology provide new business and technology models for higher security implementation of IoT.

Example 1: A tractor that operates as an autonomous unit can authorise access to multiple farmers in an area, enabling a pay per use model. It has the ability to discover and pay for climate data, and communicate with its manufacturer for maintenance and repairs.

Example 2: Industrial equipment can be empowered to order new parts, as long as there is certainty that that device is genuine and has the authority to do so. This may also lead to new ways of financing such equipment, and new marketplaces based on the equipment's performance or efficiency.

Conclusion

It is possible to envision a future where this technology creates a form of 'glass government' that is more accountable to the citizen. There are a number of use cases, and as the technology progresses it is almost certain more will emerge. This may help to achieve policy objectives. The key points for ministers and the civil service are:

The technology is in its early stages but shows significant promise. To unlock the promise of block chain technology, it is essential to understand how the combination of:

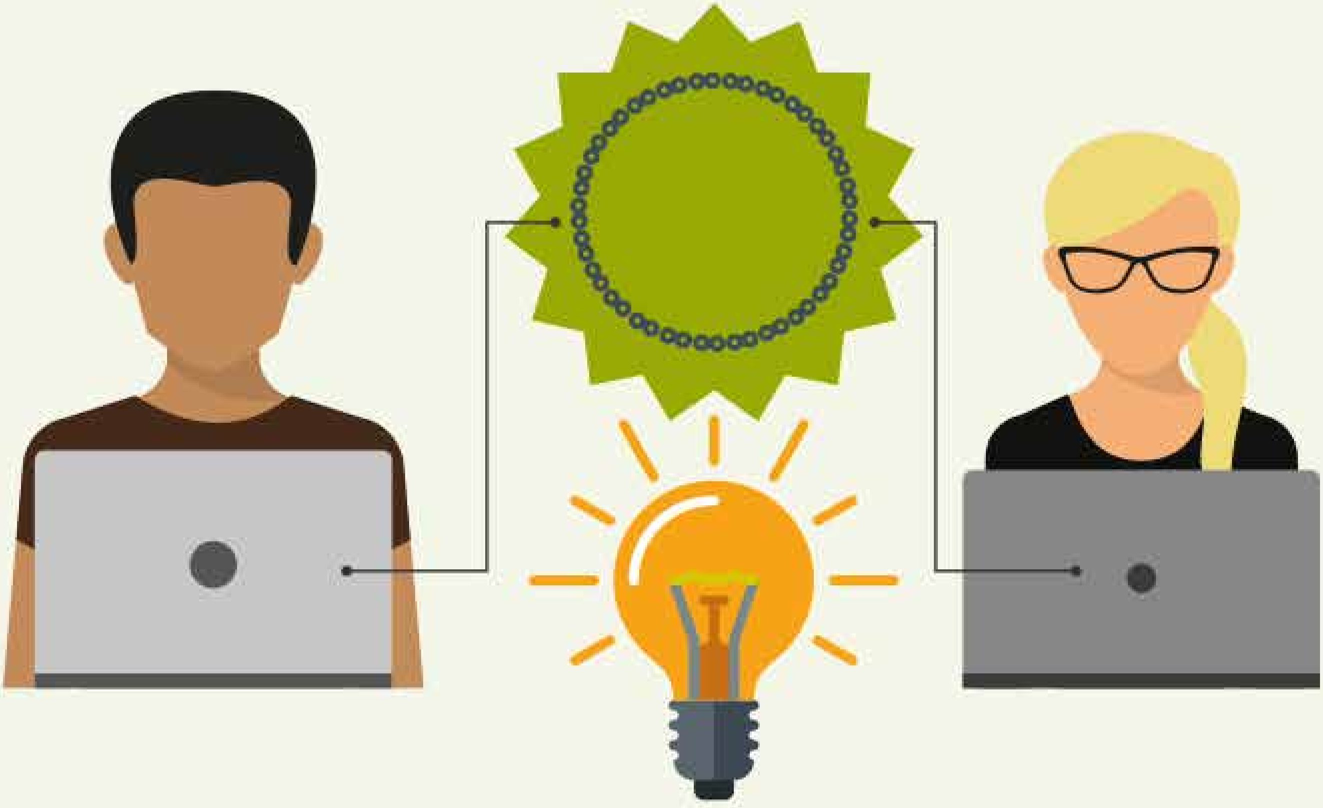
- Reconciliation through cryptography
- Large scale, secure replication of data
- Provable Transparency

can be used over three horizons:

- Supporting the emerging ecosystem
- Early trials and pilots
- Positioning the UK as a global leader

CHAPTER 2

Technology



Physical cash is unlike any other form of money. It can be transferred between two people without the involvement or permission of any third parties such as banks or governments. Bitcoin and its block chain have shown us how to perform this trick electronically. But the implications and opportunities of this digital technology are much broader.

Author
Richard G Brown,
Chief Technology Officer, R3

Chapter 2: Technology

Introduction

Bitcoin is a new form of **digital cash**. Rather than being issued by a central bank, such as the Bank of England, its issuance is controlled by a **decentralised** network of computers. This network relies on cryptography and other techniques to regulate the supply of Bitcoins and keep track of who owns them. Bitcoin is consequently known as a **cryptocurrency**.

Banks keep track of customer balances on a **ledger**. Bitcoin also uses a ledger, but it is maintained collaboratively by the decentralised network of computers, and is known as a **distributed ledger**.

As new batches of entries are added to the distributed ledger, they include a reference back to the previous batch, so that all participants can verify for themselves the true provenance of everything on the ledger. These batches are called **blocks**, and the whole collection is a **block chain**.

This chapter will explain more about these concepts, why they are important, and how they might form the basis of a much broader suite of applications.

What is money?

A £20 note is an extraordinary thing. Simply handing the note to someone instantly transfers £20 of value to them, without requiring a third party to verify the transaction. If the two people were alone, nobody else in the entire world need know it had happened, and nobody could have stopped the transfer.

But this peer-to-peer transfer only works at close distance. To transfer £20 of value to somebody in a different town or country, we need to trust other people and cede some degree of control to them: the postal worker who handles an envelope containing the cash, or the bank that carries out an electronic funds transfer. Indeed, if the bank believes that the money is connected to illegal activities, it can block the electronic transaction or seize electronic funds.

The world's financial plumbing — payments systems, the working relationships between banks, electronic communication networks such as SWIFT (the Society for Worldwide Interbank Financial Telecommunication) — are a direct consequence of the fact that physical cash really is fundamentally different to every other form of money. Only physical cash is a bearer instrument. And only physical cash can be transferred without someone else's permission — it is 'censorship resistant'.

Or so we thought until late 2008, when Bitcoin was announced. Its creator claimed that it was a system of "purely peer-to-peer electronic cash", which could be controlled outright by the holder, and sent to anybody without needing a bank's permission or running the risk of confiscation.

Every full participant in the Bitcoin system has a copy of every transaction, arranged in 'blocks', going all the way back to the start of the system. Each block is cryptographically linked to the previous block, forming a block chain that maintains a full history of transactions, and therefore acts as a distributed ledger. Users can access the ledger with a variety of different applications (such as Coinbase or Blockchain — not to be confused with the underlying technical concept), and every copy of the ledger is synchronised by algorithms set up to reach 'consensus' about the state of the ledger.

Bitcoin did not appear out of nowhere in 2008. Research into digital currency systems goes back decades, and each of the components of the system already existed. Bitcoin's breakthrough was to combine existing techniques in an innovative way, and to do so at a time when the idea of open source development on the internet was mature, and when people were receptive to the idea of alternative monetary systems.

The system is designed so that it becomes progressively harder — effectively impossible — for older blocks to be rewritten. Once a transaction is sufficiently confirmed, it can never be reversed, rendering it censorship resistant. In short, it truly is digital cash.

FAQ

What is 'the block chain'?

A block is simply a list of payments. A block chain is a list of blocks, each one referring back to the one that went before. However, when people talk about the block chain, they tend to mean the collection of technologies and techniques that underpin the Bitcoin system, which other projects have used as inspiration because they solve unrelated problems in finance and elsewhere.

Little wonder, then, that governments and regulators around the world have viewed this invention with such caution. A censorship resistant, digital bearer asset would seem to be an ideal currency for criminal networks, and Bitcoin became the primary monetary unit of Silk Road, the now-defunct digital black market.

Yet most regulators, including multiple agencies in the UK, have chosen not to ban Bitcoin, and many legitimate companies are investing heavily in this form of technology. Why?

Opportunity or threat?

Firstly, these systems are not as uncontrollable — or 'unpermissioned' — as one might expect. Contrary to public perception, the underlying architecture makes it relatively easy to track transactions and establish the identity of people who misuse the system. Regulators have also learned how to control the 'on-ramps' and 'off-ramps' where value flows in and out of the system.

Platforms like Bitcoin may sound alarming at first, but users are not guaranteed anonymity and if they want to convert their bitcoins into pounds, dollars or euros then the exchange systems are expected to enforce relevant regulations regarding identity, money laundering and terrorist financing. Furthermore, and as will be argued shortly, many of the most interesting applications of this technology enforce rules about who is and is not allowed to use the system.

The second emerging belief is that the technology underpinning Bitcoin could have valuable and benign uses, and could enable significant future innovation. Bitcoin's censorship resistance is problematic from a law-enforcement and regulation perspective, and it is therefore unlikely that major corporates or banks will engage closely with Bitcoin or related technologies in the short to medium term.

But the distributed ledger technology behind cryptocurrencies offers an openness that could be immensely valuable. Open platforms, controlled by no one firm and with a thriving community of developers, have been shown time and again to be drivers of innovation. They can enable outsiders and new entrants to offer new products and services for previously marginalised users (see Chapter 5 for more on the technology's disruptive potential).

Although distributed ledger technology was invented to satisfy one goal (digital cash), firms and other institutions are now actively exploring how it can be applied to a variety of other pressing problems. For example, businesses often find 'permissioned' block chains far more appealing than Bitcoin's unpermissioned model, because specific parties are authorised to verify transactions. This allows the businesses to create secured, private networks involving mutually trusting firms and individuals (for a more extensive discussion of permissioned and unpermissioned systems, see Chapter 3).

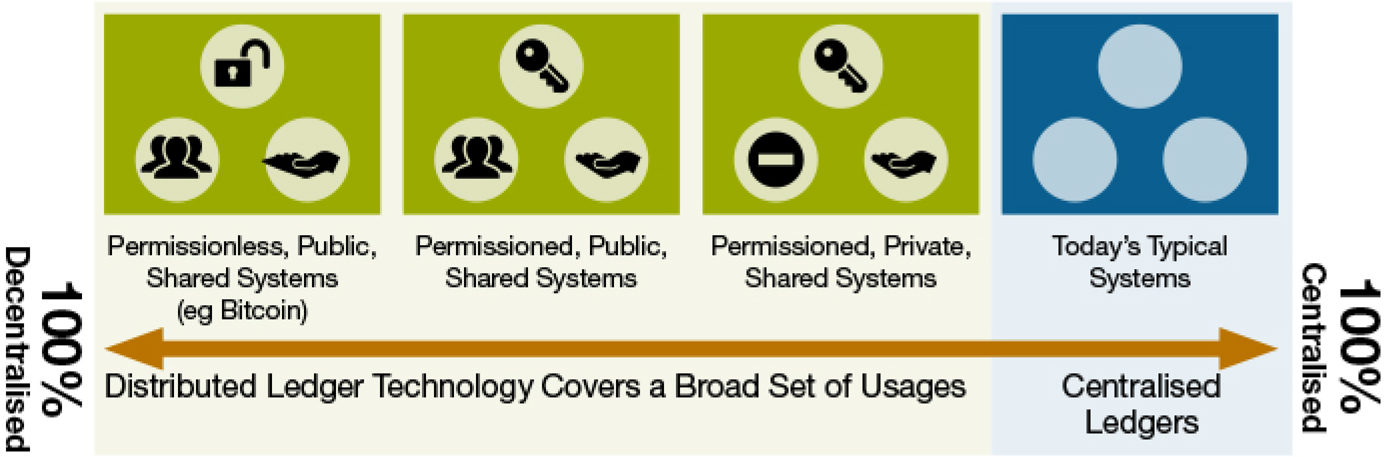
FAQ

FAQ: What fundamentally differentiates Bitcoin from previous currencies?

Bitcoins can be owned by any individual, without permission from any bank or government. They can be sent to anybody else in the world who knows how to operate a 'Bitcoin wallet'. It is this principle of 'censorship resistance' that captures Bitcoin's essential breakthrough — and which explains early concerns by lawmakers and regulators.

Overall, it is clear that there could be a continuum of technologies in this space, which can be categorised by how 'decentralised' they are (ie to what extent are they truly permissionless) (see Fig. 1). But centralisation is just one dimension along which this domain can be analysed. Other categories under active exploration include the degree to which use of funds can be prescribed (eg funds that can only be spent by a child if a parent co-signs) and the possibility of representing assets other than money (eg securities or even title to property).

Figure 1: Different ledger technologies vary in their 'degrees of centralisation'


100% Decentralised
Permissionless, Public, Shared Systems (eg Bitcoin)
Permissioned, Public, Shared Systems
Permissioned, Private, Shared Systems
Today's Typical Systems
Distributed Ledger Technology Covers a Broad Set of Usages
Centralised Ledgers
100% Centralised

Potential applications

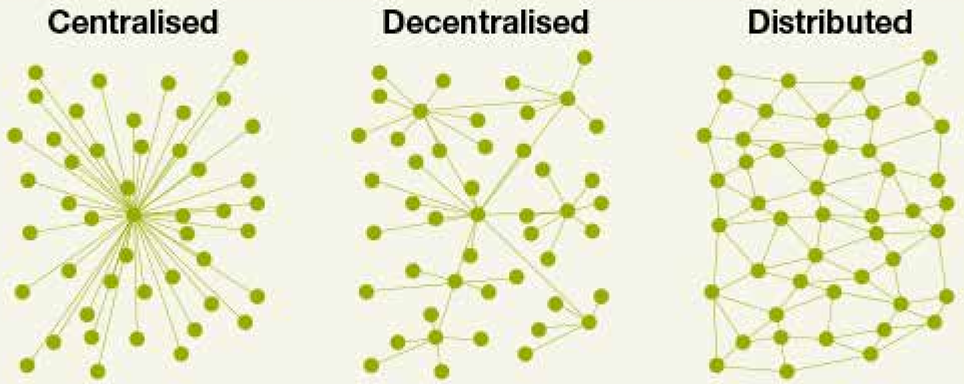
Distributed ledger technology could solve business problems that can be summed up as cost, duplication and reconciliation.

Take banking. Every bank has built or bought at least one (usually several) systems to track and manage the lifecycles of their financial transactions. Each of these systems cost money to build and even more to maintain. They must be connected to each other and synchronised, usually through a process known as reconciliation. This involves teams of people in each bank checking with their counterparts in other banks to make sure everything matches, and to deal with the problems when it does not.

A common solution involves setting up a single, centralised ledger shared by all participants. The UK has had a number of successes that rely on this approach, especially in the Faster Payments Service. But centralised utilities are typically expensive and, as their data and processing is centralised, they often must be integrated with each participant's own systems. Alternatively, many decentralised databases can sit around the edges of a network while messages move between them (see Fig. 2).

Figure 2: Distributed networks can avoid the time-consuming reconciliation processes used by centralised and decentralised databases

Tim Swinson



Bitcoin, in contrast, synchronises thousands of computers in a distributed network via the internet: if my computer thinks that I own a Bitcoin, then so does every other computer in the network. If a similar technique could be used in banking, all the banks' systems could stay in step with each other without requiring armies of people to reconcile and resolve the issues. Crucially, we do not need Bitcoin to achieve this — it is the underlying distributed ledger technology that offers a possible solution.

This could help to tackle one of the biggest problems with financial services: the costs of using paper. In recent years, there have been many different initiatives intended to remove paper documents from the economy. However, in many cases the new technology has simply recreated old processes in a new way, or continues to rely on paper in other stages of the process. For example, providing finance to exporters remains an extremely manual process: an importer's bank often issues a letter of credit, against which the exporter's bank will advance funds. Although this process is usually electronic, the subsequent verifications rely on bundles of paper documents that are manually processed around the world. A shared ledger technology could, in contrast, replace certain aspects of paper-based banking with processes that operate in a much speedier and paper-

CASE STUDY

Research and horizon scanning

John G Baird, Lead for the RCUK Digital Economy Theme, EPSRC

The Engineering and Physical Sciences Research Council (EPSRC) leads the Digital Economy (DE) Theme on behalf of Research Councils UK (RCUK). Since 2008, the DE Theme has invested over £170 million in applied multidisciplinary research, with a particular focus on societal challenges around the digitisation of the economy and its effects on social inclusion, rural economy, personal data, security, identity, trustworthiness and privacy. The DE Theme is leading on taking forward both the Digital Currencies and the Internet of Things activities announced in the March 2015 Budget. In the area of distributed ledger technologies, to date we have invested in the following activities:

1. Cryptocurrency Effects in Digital Transformations (CREDIT)[1], an 18-month £0.4 million research project that aims to investigate the phenomena of cryptocurrencies and their associated underlying technology, the block chain, grouped around 4 main themes: digital transformations, privacy, community and institutions. The main outcomes of the research will be:

- A step-by-step guide aimed at helping start-ups and incumbents understand the issues to consider for incorporating block chain technologies into their products and services
- A number of small pilot studies with companies examining the potential impacts of cryptocurrencies
- A community of academic researchers and professionals able to further develop this nascent research area

2. CREDIT builds on two previous scoping reviews that we supported: 'The disruptive role of crypto-currencies'[2] and 'ICT and the Future of Financial Services'[3]. These both reviewed the current understanding of cryptocurrencies and revealed gaps in the understanding of social, ethical, legal, regulatory impacts of crypto-currencies. As a result, we recently issued a £10 million call for research proposals on 'Trust, Identity, Privacy and Security in the Digital Economy'[4], which features "Broad applications of distributed ledger technologies" as one of its six focal areas. This focal area seeks to support research that blends and balances the technological advancement in distributed ledger systems with an understanding of the societal, ethical, legal and business frameworks needed to build confidence, trust and adoption of such systems by individuals, communities, organisations and states. Ultimately, we hope this research will pave the way towards a 'smart' economy that can support diverse scenarios of monetary and non-monetary value exchange between individuals and organisations and, in the future, 'smart' objects.

3. Finally, we have also funded a £260,000 research project, 3rd Party Dematerialisation and Rematerialisation of Capital (3DaRoC)[5], which explored how to design effective digital retail financial services based on case studies with two retail finance organisations: Zopa Limited, a peer-to-peer lender; and the Bristol Pound, a community currency. The project has produced an online toolkit to assist users and businesses interested in the key issues impacting the design and use of digital financial products[6].

less way. The Engineering and Physical Sciences Research Council (EPSRC) is already supporting exploratory research on such financial applications (see case study on research and horizon scanning, above).

But the opportunities are not limited to banking. Applications are being explored in healthcare (patient records), government (land registries and benefit disbursement— see Chapter 6), electronics (including the 'Internet of Things' —

see Chapter 1) and even the world of art and jewellery (tracking the provenance of diamonds — see Chapter 5).

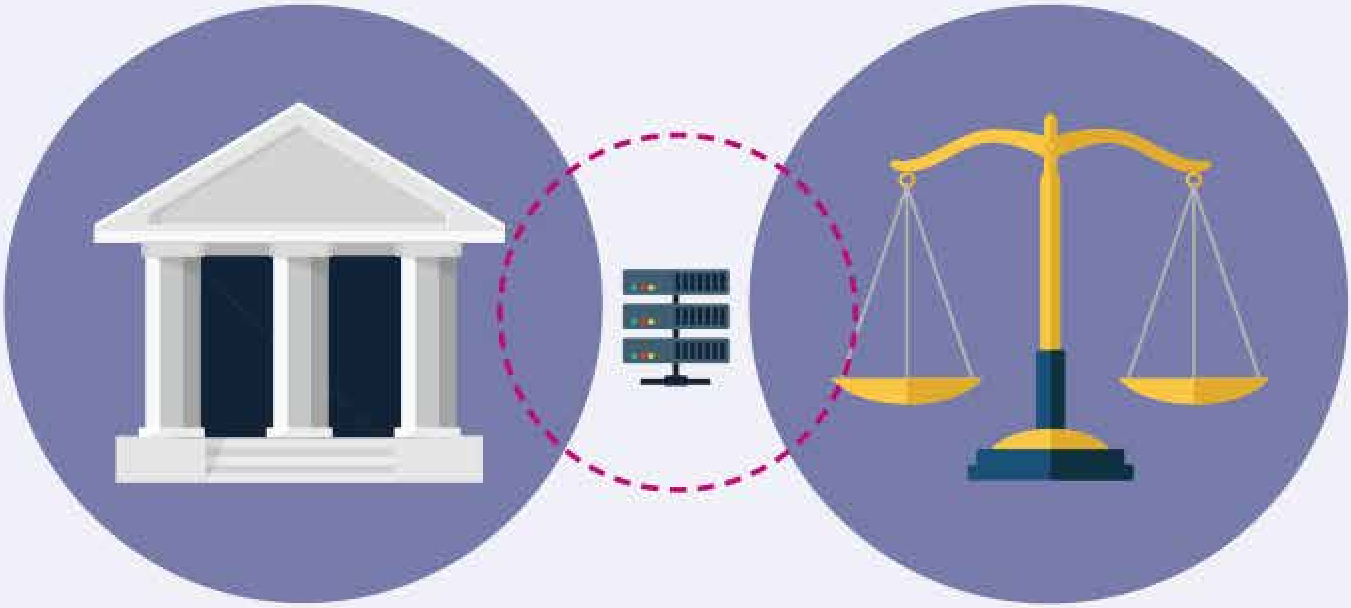
It is important to stress that these technologies are very early in their development, and there are many unsolved problems to tackle before these applications can be realised, including issues of privacy, performance, and scalability. Does the technology actually work well enough for the banks to trust? Who will build these platforms if they can't easily charge a fee when they are shared and mutualised?

But the field is developing rapidly and many of the problems are already being resolved. It is now becoming possible to distinguish between those aspects of the technology that will change over time, and those that are innate and are unlikely to change. Already, we can see that distributed ledger technology could enable firms and governments to run more efficiently, without expensive reconciliation and duplication. And it could allow both incumbents and new entrants to compete on equal terms in offering new products and services to consumers based on open access to securely shared data.

That could usher in a world-changing revolution that goes far beyond censorship-resistant digital cash.

CHAPTER 3

Governance and Regulation



Both the legal and the digital spheres are governed by rules, but the nature of these rules is different. In a digital environment, both laws (legal code) and software/hardware (technical code) regulate activity. The impact of both must be considered in setting out regulations that cover distributed ledger systems.

Author

Vili Lehdonvirta, Oxford Internet Institute, University of Oxford;
Robleh Ali, Manager – Digital Currencies, Bank of England

Chapter 3: Governance and Regulation

Introduction

This chapter deals with rules and rulemaking in distributed ledger systems. We will distinguish between **legal code** (rules consisting of legal obligations) and **technical code** (software and protocols). We will also distinguish between **governance** (rule-making by the owners or participants of a system with the purpose of safeguarding their private interests) and **regulation** (rule-making by an outside authority tasked with representing the interests of the public).

Legal code vs technical code: Two types of rules

The financial system is both a set of legal obligations between institutions and a set of digital records of these obligations. Both the legal and the digital spheres are governed by rules, but the nature of these rules is different. In a seminal text on the subject[1], Lawrence Lessig of Harvard University addressed how these legal and digital rules interact to govern activity. Lessig argued that in a digital environment both laws (legal code) and software/hardware (computer code) regulate activity, and that the impact of both needs to be considered when constructing a theory of regulation. In this chapter we refer to technical code rather than computer code. This definition covers both software and protocols, as distributed ledgers rely on both to function.

One fundamental difference between legal code and technical code is the mechanism by which each influences activity. Legal code is 'extrinsic': the rules can be broken, but consequences flow from that breach to ensure compliance. Technical code, in contrast, is 'intrinsic': if its rules are broken then an error is returned and no activity occurs, so compliance is ensured through the operation of the code itself. Another characteristic of software is that a machine will rigidly follow the rules even where that compliance produces unforeseen or undesirable outcomes. This leads to some striking differences in the operation of distributed ledger systems compared with the current financial system.

1. Current financial system: ruling via legal code

The modern financial system is already largely digital and heavily reliant on technical code. This technical code governs the creation and amendment of the digital records of the legal obligations between institutions. Financial regulation is aimed at the effects these legal obligations produce: for example, whether a bank has sufficient capital or liquidity. The financial system is already governed by this combination of technical code and legal code, but financial governance and regulation has traditionally focused on the latter.

Enforcement of the public element of the legal code falls to a specialised group of financial regulators charged with ensuring compliance by participants in the system. Participants must provide the information that their regulator needs to assess whether they are in compliance with the system's rules. If an institution is not in compliance then the regulator can take action to bring them back into line. This is not to say technical code has no influence on the existing regulatory process — all the information provided to the regulators is digital, and the product of technical code — but governance and regulatory aims are pursued by producing legal code rather than by changing the technical code.

2. Distributed ledger systems: ruling via technical code

Distributed ledger systems such as Bitcoin have shown that they can function without legal rules. Instead, the rules that each participant must follow are defined and enforced only by technical code. Each participant in the network runs the same or compatible software that defines what kinds of transactions are permissible. For example, the Bitcoin software allows participants to spend only balances that they can prove they own with cryptographic keys. The Bitcoin software also regulates how new currency is issued, and places an absolute cap on the size of the money pool. There are no bylaws or other legal documents stating these rules, and no humans to enforce them — distributed ledger systems are solely governed by their own technical code.

To prevent participants from modifying their copy of the code to issue transactions that are against the rules, each transaction needs to be verified before it enters the ledger. In an 'unpermissioned' distributed ledger system like Bitcoin, verifiers (known as miners) are chosen by lottery. The system seeks to assure their integrity through a system of economic incentives, in a process governed by the software. In a 'permissioned' distributed ledger system, verifiers are appointed by the system's proprietor, and their integrity is assured through conventional means, such as a legal contract.

In summary, distributed ledger systems differ from the conventional financial system in that they are ruled by technical code rather than legal code. One advantage of this is that compliance costs are low: participants need only use a compliant software package to issue transactions. It might seem that enforcement costs are lower, too, but this is not necessarily the case because the mining system that is used to verify transactions in all of the most popular distributed ledger systems consumes significant computational resources. That cost must eventually be borne by the system's users.

Governance vs regulation: Two types of rule-making

Because the current financial system and distributed ledgers are primarily governed by different types of rules, we must therefore ask the question: who makes the rules?

1. Current financial system: a mesh of private and public rule-making

There are many places where legal code is being produced in the current financial system, but these can be broadly divided into two categories: private rule-making (governance) and public rule-making (regulation). An example of private rule-making is the Visa Core Rules promulgated by the financial services company Visa Inc. to govern the actions of all the participants in the Visa system. Such private rule-making is done by proprietors of private financial networks like Visa, as well as by private associations of financial institutions wishing to coordinate their activities to one another's benefit. An example of public rule-making is the statutory oversight of Visa Europe's payment system by the Bank of England.

The design of the public legal code in the current financial system is the province of policymakers who have to consider the effect of regulations on the different institutions of the financial system (a 'microprudential' approach) as well as the impact on the system as a whole (a 'macroprudential' approach). As the financial system is global, international bodies such as the Basel Committee on Banking Supervision convene policymakers from around the world to reach voluntary accords that can then be translated into legislation in a specific jurisdiction.

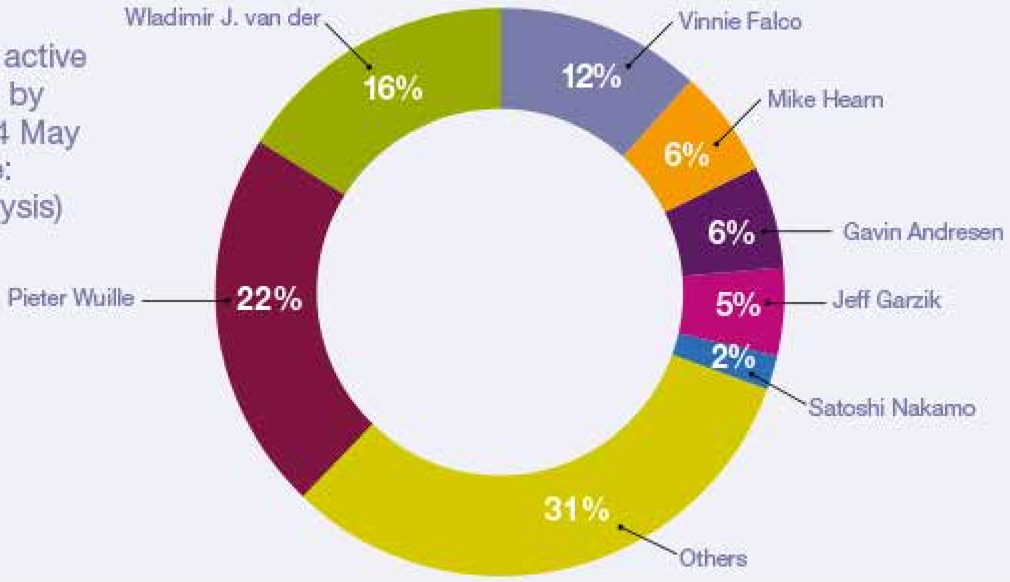
2. Distributed ledger systems: ad hoc private rule-making

Unpermissioned distributed ledger systems are sometimes thought to exist independently of human rule-making, and governed only by mathematical algorithms. This is a misconception. Just like legal code, technical code needs to be produced and maintained by humans who define the rules that the code embodies. Using Bitcoin as an example, the initial version of the software was published by Satoshi Nakamoto (a pseudonym). In 2010, Nakamoto handed control of the project to Gavin Andresen, an Australian-born programmer living in the United States. Like any software, Bitcoin needs to be regularly updated to address bugs, security issues, and changes in the operating environment. Such an update can in principle change any aspect of the software, including accounting and ownership rules. Who gets to write the software and how that process is governed is therefore critically important to all participants in a distributed ledger system.

In the case of Bitcoin, the software is governed by an ad hoc process involving a handful of informal institutions and power holders. Figure 1 shows who has written most of the current Bitcoin code. The software is open source and anyone can suggest changes to it, but technical authority to admit changes to the official version of the software is held by a team of five core developers appointed by Andresen. The core developers' power is constrained by an informal self-imposed charter, which states that significant changes to the rules require broad consensus from the community. Any update to the software must furthermore be installed by a majority of the miners (as measured by the computer processing power they contribute) for the changes to become effective. A handful of individuals who manage so-called mining pools are therefore very influential in determining whether or not miners ratify a software update in this way.

This governance process worked well when the changes to the code were uncontroversial bug fixes, but it has started to show signs of breaking down recently, because some decisions require choosing which stakeholders' interests to prioritise over others'. Andresen and others have stated that the process needs to become more formal. The community is debating what such a formal governance system should look like, but this is complicated by the fact that

Figure 1.
Bitcoin Core active lines of code by developer, 14 May 2015 (source: author's analysis)



Bitcoin was founded on an ethos of anti-institutionalism. This is an interesting conundrum, as it demonstrates the worth of legal code and shows that technical code alone does not produce an optimal outcome.

In permissioned distributed ledger systems, governance of the software is made simpler by the fact that there is usually a proprietor with clear legal and technical authority over the code. It is up to the proprietor to determine how the code is modified, and up to the users (often customers of the service) to decide whether they are comfortable with having the proprietor exercise authority over the software. Service level contracts and other conventional means can be used to establish responsibilities and enforce them. Permissioned distributed ledger systems are in this respect not very different from conventional private financial networks like Visa or software-as-a-service (SaaS) systems.

How should we regulate distributed ledger systems?

Governance in a distributed ledger system as described above is concerned with the system's stakeholders' interests, but there may also be broader social interests involved in how a distributed ledger functions. For example, regulators may wish to collect taxes, prosecute crimes, and limit the use of a distributed ledger for criminal purposes. If a system is adopted to the extent that it starts to have potential knock-on effects elsewhere in society, regulators may also wish to ensure that the system is resilient against systemic risks and market failure. This regulation can be applied through legal code or technical code.

1. Regulating distributed ledgers via legal code

Regulating a permissioned distributed ledger system is simply a matter of imposing legal obligations on its proprietor. Regulating an unpermissioned system like Bitcoin via legal code is more complicated, as there is no single legal entity in control of the system. It would be difficult to regulate what software people are allowed to install on their computers. Attempts to regulate Bitcoin via legal code have instead focused on regulating the businesses that deal with Bitcoin, such as exchanges and wallet providers. These businesses can be regulated in their own right (eg to prevent a wallet provider from disappearing with customers' money) or as a means to indirectly regulate what the ledger is used for (eg ensuring compliance with anti-money laundering regulations).

A well-known example of regulating Bitcoin via legal code is the BitLicense, issued by the New York State Department of Financial Services to businesses offering digital currency services to New York residents[2]. The deadline for businesses to obtain the license was 8 August 2015, and unlicensed service providers can be penalised.

2. Regulating distributed ledgers via technical code

The technical code for distributed ledger systems like Bitcoin is currently produced by private actors in an ad hoc process. But technical code, comprising software and protocols, can also emerge from the public sector. For example, TCP/IP and some other core internet protocols were the result of government-funded research projects and are now maintained under the auspices of the Internet Society, an international non-profit organisation with an open membership structure based on geographic location and special interests. Other parts of internet infrastructure are maintained by international multi-stakeholder processes, and some parts remain under the oversight of US public regulators.

While this patchwork is far from a perfect solution, it points to the possibility of public involvement and democratic representation in the production of technical code — public regulation via technical code as opposed to legal code.

Table 1
Examples of privately and publicly produced legal code and computer code

	Legal code	Protocol
Privately produced	Visa Core Rules Faster Payment Service Rules	Financial Information eXchange (FIX) protocol Bitcoin
Publicly produced	European Market Infrastructure Regulation BitLicense	Internet (TCP/IP) World Wide Web (HTTP)

Applied to distributed ledger systems, this could mean anything from instituting formal multi-stakeholder processes for maintaining the technical code, to developing public standards for the code. If this allowed governments or the public directly to attain legitimate regulatory goals by influencing the rules built into the computer code, it could lessen the need for a body of new legal code to regulate these systems.

Alternatively, the public sector could develop a permissioned system that allows public regulatory influence to be exerted through a combination of legal and technical code, rather than exclusively through legal code as at present. Some of the core internet technologies have shown that it is possible for governments to successfully catalyse the creation of technical code that has become foundational to private sector activity.

Conclusions

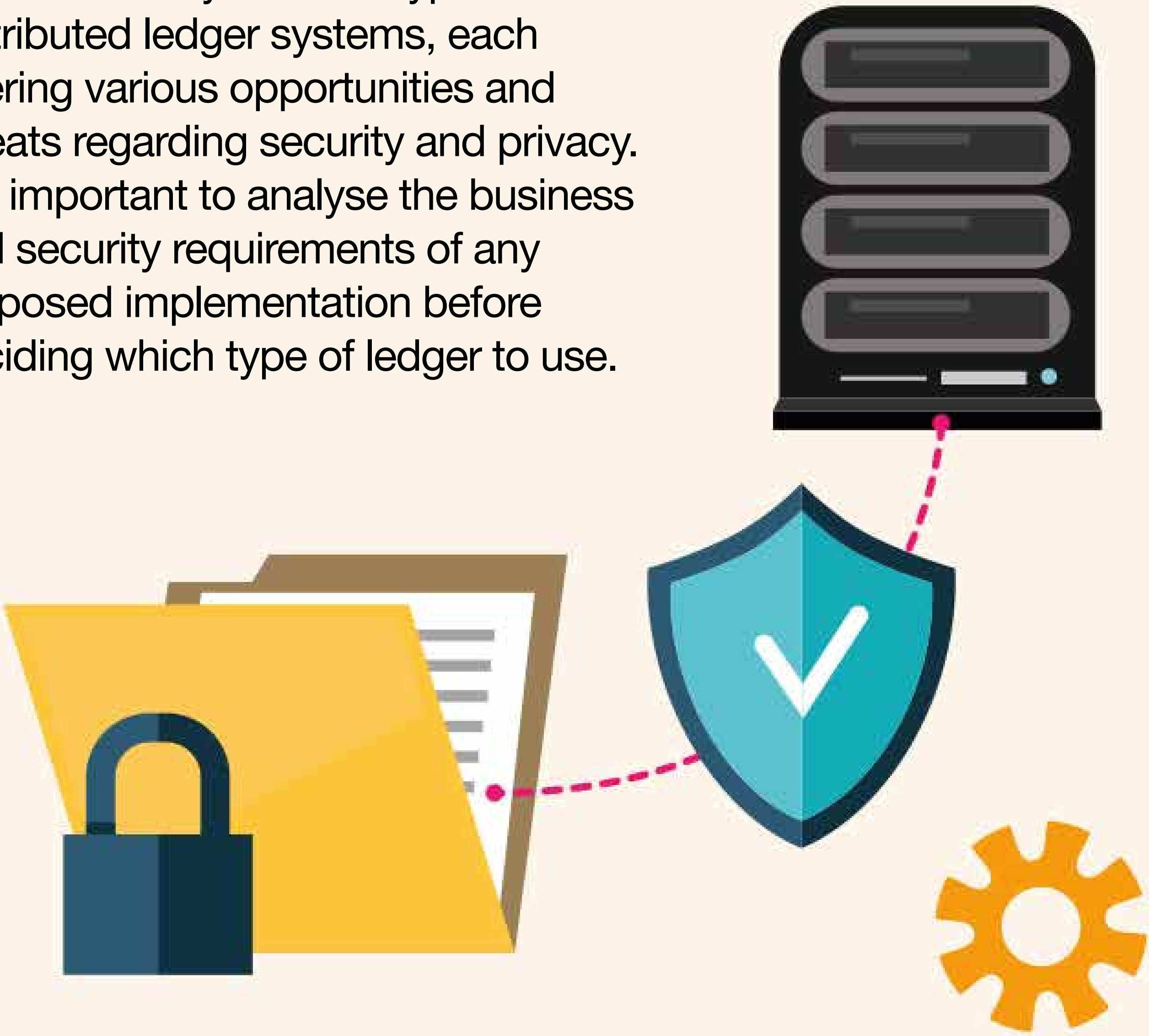
In contrast to conventional private financial networks like Visa, unpermissioned distributed ledger systems like Bitcoin lack a central legal entity with formal responsibility over the system. Instead, they are governed by ad hoc processes, usually centring on a handful of software developers who produce the system's software code. If these systems are to grow in value and influence, they will most likely need to develop more robust internal governance processes. The lack of a central legal entity also makes it more challenging for public regulators to regulate distributed ledger systems via legal code. Governments should therefore also consider ways of regulating distributed ledger systems by influencing the technical code that defines their rules. In finding the right blend, the government should consider the strengths and weaknesses of both technical code and legal code, recognising that the two interact and should be designed accordingly.

The emergence of Bitcoin and distributed ledger systems has brought the issue of technical code to the fore in the context of the current financial system as well. Distributed ledgers show that financial systems can be governed and regulated with technical code as well as legal code. Policymakers should recognise the influence of technical code on the financial system and consider how such influence could be made part of the regulatory system, with potential benefits such as lower compliance costs.

CHAPTER 4

Security and Privacy

There are many different types of distributed ledger systems, each offering various opportunities and threats regarding security and privacy. It is important to analyse the business and security requirements of any proposed implementation before deciding which type of ledger to use.



Author

M. Angela Sasse, University College London, with contributions from: George Danezis and Sarah Meiklejohn, UCL; Daniel Shiu, Government Communications Headquarters; Phil Godsiff, University of Surrey

Chapter 4: Security and Privacy

Introduction

Security can be simply defined as: “Things that should happen, do; and things that shouldn’t happen, don’t.” For any particular implementation of distributed ledger and block chain technology, the risks of desired and undesired outcomes depend on how the technology is designed, implemented and governed. Different stakeholders will face different risks.

Threats to the systems include not only attacks by external entities, but also actions by internal stakeholders and failure of components (such as software). Prior to any implementation, detailed threat models need to be developed, and specific security requirements identified, to deliver the outcomes.

Effective security provides a necessary but not sufficient foundation to deliver privacy for individual and organisational stakeholders. We must also consider how the information disclosed in a particular implementation might be combined with other available information to identify individuals or groups, or detect their activities.

Innovation advantages

One of the main security features of Bitcoin and other cryptocurrencies is the decentralised control over the network. The system is governed by a global set of peers who operate based on consensus (see Definitions, p17), so there is no central point of trust or failure. This means that any malicious actor must put in considerable effort to attack the system. For individual users, the system can also achieve a high degree of security — in order to move the bitcoins held in a wallet, an attacker must know the private key associated with a given public key (which is where the bitcoins are held). Thus, the attacker must be able to subvert the security of an established cryptographic standard (the Elliptic Curve Digital Signature Algorithm, ECDSA) in order to steal someone’s bitcoins.

Bitcoin and associated ‘altcoins’ apply a much broader computer security infrastructure — namely distributed ledgers — that provides high-integrity and view consistency. Such ledgers use cryptographic techniques to ensure that anyone can check if a particular record is within the ledger, as long as they possess a small amount of crucial information. At the same time, complex consensus protocols are employed to ensure that everyone in the system gets a consistent view of the ledger. This is key to Bitcoin’s ability to prevent double spending, but it could be equally important when using distributed ledgers for other applications, such as recording contracts or deeds. Distributed ledgers naturally lend themselves to implementing high-level services that involve notaries, time-stamping, and high-integrity archiving, and promise to lower the costs of these activities by increasing automation, enabling easy switching of service providers, and peer transactions.

One of the main problems for secure on-line communications lies in establishing that a public key belongs to a service that a user wishes to access. The prevalent mechanism used since the 1990s is known as a Public Key Infrastructure (PKI) — essentially a set of trusted third parties that provide certificates attesting the link between keys and services. But these certificate authorities have been to shown to be fallible; when compromised, they may issue invalid certificates unnoticed.

The Certificate Transparency[1] (CT) system (recently initiated by Google, and now overseen by a working group) uses distributed ledger technology to mitigate this problem. All certificates are appended to a distributed ledger, and any user or services can check that the certificate they are about to use is the one in the ledger. Consequently, rogue certificates can be detected quickly — a significant disincentive to attackers seeking to compromise and abuse the PKI system.

The problem of establishing authoritative bindings between keys and entities also exists when users want to protect personal communications. But current solutions (such as the PGP Web of Trust, or centralised solutions) are either unusable or have brittle security properties. One promising alternative is CONIKS[2], which relies on a specially crafted distributed ledger to store and retrieve user public keys that can be used to encrypt or sign emails. Unlike CT — which relies on a network of third parties to maintain and audit the distributed ledger — CONIKS uses communication providers and their existing databases of users to build a high-integrity ledger.

Security challenges

The security advantages of the decentralised systems identified above — specifically, resilience and robustness — only apply completely to unpermissioned ledgers that subscribe to a global trust theory. For permissioned ledgers, or examples with other centralised functions, there will be less resilience and robustness, but a better ability to assure central trust and/or functions.

In fact, there is a broad spectrum of options (see Chapter 2) between totally decentralised systems (as in Bitcoin) and totally permissioned system (a private, dedicated network). An example of a middle-ground solution that uses the strength of both is the proposal from George Danezis and Sarah Meiklejohn of University College London for centrally-banked cryptocurrencies[3] — relying on a centrally-controlled server to establish the block chain while using a distributed network of 'mintettes' to absorb transactions.

Given this spectrum of solutions, it is important to analyse the business and security requirements of any proposed implementation before deciding which type of ledger to use.

For example, the key priorities of a system to manage welfare support payments for the Department for Work and Pensions would include ensuring both the availability of the service and its resilience against network disruption (see Chapter 6). The greatest threats would probably come from opportunistic cyber-criminals targeting individual users for monetary gain. Therefore:

- The system should be designed to require minimum knowledge and effort from individual users ie there should only be a small number of choices and configurations, with clear feedback of consequences
- If commodity devices such as smartphones are used, ensure that credentials and keys are securely accessed and not visible to other applications
- The ledger itself should be maintained across a wide network of servers to allow for resilience against network outages

- For wider deployments, the payment authorisation service should be centralised on dedicated hardware and hardened against attack

Alternatively, a system that might be used for distributing foreign aid would need to ensure the integrity of transactions (to avoid funds being syphoned off for other purposes); and maintain the availability of the system during disaster relief situations, for example. Threats may come from nation states that could gain geopolitical advantage from disrupting transactions, or from dishonest agents within the states receiving aid. Therefore:

- The system should run on a small, hardened and dedicated network of servers that establish government copies of the ledger with offline back-ups
- Clients should be encouraged to set up their own networks of ledgers, with advice on secure design that allows regular updates or corrections from the government servers
- Allow the system to be taken offline if a serious network attack is suspected

Arguably, though, the most serious threat to any government-backed system is obsolescence. If it is too difficult to use, or does not offer the functionality required, it will not be adopted.

Another threat that has recently emerged is that of a system being hijacked because a different software implementation creates a ‘split’ within an existing system. Cryptanalysis researcher Nicolas Courtois at UCL, who has followed Bitcoin closely, reported in August 2015 that:

“There will be a possibility to mine blocks with a new version number and new rules. This is meant to make bitcoin more democratic: larger blocks, more transactions per second, lower fees, wider adoption. Current bitcoin has reached its capacity limits (not much more than 3 transactions per second) in the recent months and bitcoin developer community has FAILED to solve this problem.”

This shows that the governance of any government-backed implementation will require serious forethought of possible technical developments, and how to protect it from takeover by other entities — hostile or not.

Security recommendations

For each particular use of the technology, the government should carefully identify the relevant threats. Although no nation state actor is interested in disrupting Bitcoin, they might be interested in attacking a UK national digital currency — and if there is any financial gain to be made from fraudulent ledger entries, it is likely that organised crime will target users with low security awareness.

Given the threats identified, the government should decide on an appropriate level of security for the threat actor, and the lifetime of the proposed usage. If cyberattacks are anticipated then systems should be designed with secure usability in mind from the outset. For example, unpermissioned networks of ledgers allow actors to threaten network integrity either by adding their own servers or operating a denial-of-service attack on legitimate servers; to counter this, a long-term ledger of interest to nation states might need quantum resistant signature schemes.

It is easier to build a new secure infrastructure than to adapt existing infrastructure to a new secure application. As such, a dedicated new set of permissioned servers would be easier to configure and accredit than reusing existing internet servers. Advice on building secure systems should be sought either from the UK Government Communications Headquarters (GCHQ) or reputable industry providers.

For systems intended to have a long lifetime, the initial design should make it straightforward to update components during that lifetime (eg the ability to switch out nodes of the network with more modern hardware; the ability to upgrade cryptographic algorithms that can no longer be used securely).

In any trial of the technology, it is also important to fund penetration testing of the experiment at both the system and user levels. Real-world attackers would not be interested in a small scale proof-of-concept, but could become a threat when an application is deployed at scale.

Privacy challenges

The Bitcoin cryptocurrency was designed from the outset to provide a form of pseudonymity[5] (its designer Satoshi Nakamoto referred to this property as "anonymity", but this is a misnomer).

Users can create a number of wallets to hold bitcoins, and there is no restriction on the number of wallets they can own, nor any 'Know Your Customer' requirements to open a wallet. Coins are transferred from one wallet to another, and the obscured relationship between wallets and real-world persons provides a degree of privacy.

The decision to allow pseudonymous identities, and to not link wallets to any real-world identifiers, is a pragmatic one for Bitcoin that has contributed to its wide adoption. Most jurisdictions do not have any strong way of linking real-world identities to online transactions, and thus a reliance on the existence of such mechanism would have prevented the deployment of Bitcoin at the time, and even today. Furthermore, given the international nature of the Bitcoin network, it is unclear which jurisdiction would have been entrusted with certifying identity information, and how one could establish whether a legal jurisdiction is entitled to identify a certain user.

Finally, requiring identification as part of opening wallets potentially has an impact on the fungibility of bitcoin as a currency: if an identity provider has to be involved to authorise transactions then they may be able to block them, selectively denying the value stored in some user's bitcoins. Other parties could not be sure that value stored in bitcoins would be unconditionally available in the future. Thus Bitcoin pseudonymity allowed both rapid adoption (by avoiding dependencies on non-existent or fragmented identity infrastructures), and also preserves important aspects of Bitcoin as a currency (ie its status as an unconditional store of value).

This pseudonymous relation between users and wallets is, however, not full or perfect anonymity. Chains of transactions in and out of wallets, and from wallet to wallet, are visible to all, and can be traced and tracked in public. UCL's Sarah Meiklejohn and colleagues have shown that chains of transactions may be traced throughout the Bitcoin block chain to link, for examples, instances of bitcoin theft with specific attempts to withdraw bitcoins through exchanges[6]. This approach could be used to enforce some Know Your Customer rules, because once a particular wallet address is identified and linked with a physical person, it is possible to uncover all of their transactions.

This weak form of pseudonymity, combined with the transparency of transactions on the bitcoin block chain, actually represents a privacy challenge. Unlike traditional online payments, which are only visible to transacting parties and financial institutions, Bitcoin payments — including the wallets involved, the approximate time of the transaction, and the transaction values — are recorded in a publicly visible block chain. Anyone can process the block chain and draw inferences about, for example, the turnover of an on-line merchant, the buying profile of a particular user, or even the many transfers between private individuals — a capability that was restricted in the past to financial institutions and law enforcement.

Privacy recommendations

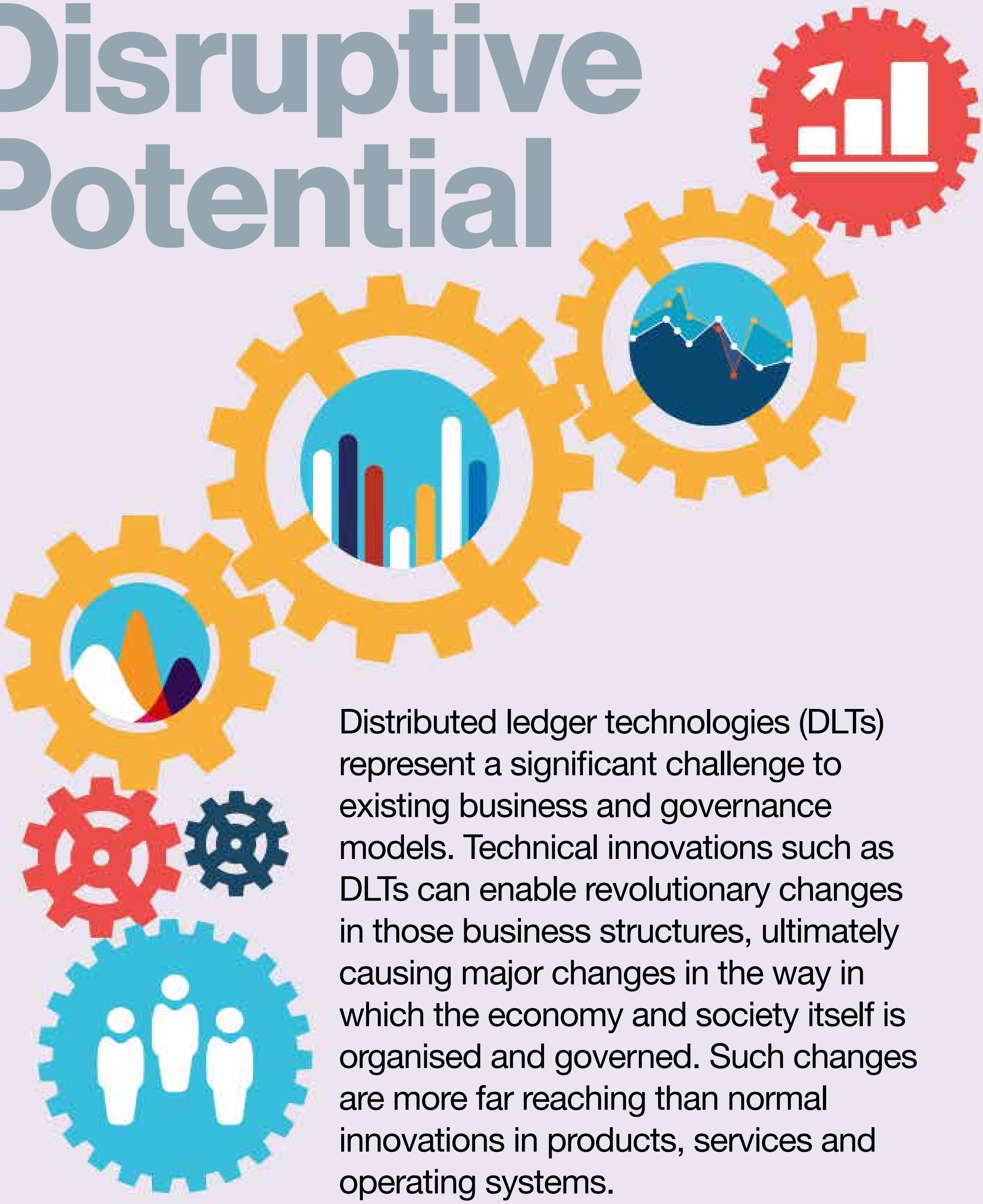
A number of techniques, and alternative cryptocurrencies, have been proposed to alleviate the privacy problems of a fully transparent block chain.

The first set of techniques involves 'mixing' systems. These take coins from a number of users, and output coins to different addresses that are not linked to the original users. By breaking the link between payer wallets and payee wallets, they provide some measure of anonymity. There are, however, two key challenges with engineering such systems. Firstly, the anonymity they provide is not perfect: although a coin may be traced to one of a number of addresses, is not perfectly hidden amongst all possible wallets in Bitcoin. This partial leakage of information allows the application of statistical attacks to de-anonymise repeated transaction through so-called Statistical Disclosure Attacks[7]. The extent to which these attacks are effective is an open question. Secondly, dishonest mixes have the potential to accept coins but never pay out, effectively stealing them. A number of bitcoin mix designs (such as Mixcoin[8]) attempt to alleviate this problem through making part of the mix operation transparent enough to ensure the integrity of its operation, without compromising its privacy.

A second family of systems radically alters the way bitcoin payments are made, and what is recorded in the block chain, to provide stronger privacy. For example, Zerocoin[9], Zerocash[10], Pinocchio Coin[11], or certain Sigma protocols[12] adapt group signature algorithms to the setting of cryptocurrency transactions. A payer provides a zero-knowledge proof that they own some coins from a list, without revealing which, while also leaking enough information to prevent double spending. This allows them to pay a coin without being fully linked to previous transactions. As with mixing systems, these techniques may only hide payees within a limited list of potential users, not all, which opens the way to de-anonymising multiple transactions. They are, however, robust in terms of integrity, and do away with mixing as a third party operation that could pose a performance or trust bottleneck.

CHAPTER 5

Disruptive Potential



Distributed ledger technologies (DLTs) represent a significant challenge to existing business and governance models. Technical innovations such as DLTs can enable revolutionary changes in those business structures, ultimately causing major changes in the way in which the economy and society itself is organised and governed. Such changes are more far reaching than normal innovations in products, services and operating systems.

Author

Phil Godsiff, Senior Research Fellow, Surrey Centre for the Digital Economy, Surrey Business School, University of Surrey

Chapter 5: Disruptive Potential

Introduction

Technological innovations can have a huge impact on how businesses operate. New technology can enable businesses to offer new products and services, capture new revenue streams, introduce lower-cost operations, and streamline their organisational structures. If existing businesses are slow to adapt, or try to create barriers to entry, new entrants can take advantage of innovations to replace these incumbents.

Sufficiently radical technical innovations can lead to revolutionary changes, not only in business models or industries, but eventually in the way in which society is organised and governed. For example, the steam engine led to the development of railways and enabled the movement of the population to urban centres.

Distributed ledger technologies (DLTs) have disruptive potential beyond innovation in products, services, revenue streams and operating systems within existing industry frameworks. They have the potential to disrupt the whole economy, and society. Understanding this can help to frame the opportunities and threats afforded by distributed ledger technologies — and how they can inform changes in the role of the government, and the services it delivers.

The role of innovation

Organisations constantly innovate to improve their competitive advantage. We tend to think of innovation in terms of new products and processes: the manufacturing industry focuses on product innovation, while the service industry develops through process innovation. Even small changes can affect the structure of an industry: many manufacturers of computer disk drives failed to adapt to the introduction of lighter and smaller drives, for example[1]. Innovation can also occur within business models, and often legitimise new relationships within an industry to create ‘cooptetion’, where firms both co-operate and compete[2].

The digital revolution has led to an increasing awareness that innovation can also occur at the level of the business model[3], and even at the level of whole industries — just think of how the Uber app, which enables customers to hire drivers in their vicinity, has disrupted the taxi industry. Changing an organisation’s viewpoint from short-term profit to long-term wealth creation can lead to radically altered activities and views of the future, for example by using open source software to create a platform that others can modify and exploit[4].

Technology innovations, such as apps, now allow customers to act as resource

FAQ

What is the disruptive potential of DLTs?

DLTs have the potential to be radically disruptive. This is partly because of the developments they have already helped to bring about (eg in cryptography and software engineering); the industries and services they could innovate (eg financial services, real estate, healthcare, identity management); and their processing capability (eg low cost, real time, immutability). But their disruptive potential also lies in their underlying philosophy of distributed consensus, open source, transparency and community.

integrators, ‘pulling’ solutions rather than having them pushed by suppliers. This can challenge existing assumptions on value creation through, for instance, ‘prosumption’ (a model where the same actors are involved in both production and consumption, used by ridesharing service BlaBlaCar and the accommodation rental service Airbnb), peer-to-peer lending and crowd sourcing. This form of innovation impacts industry structure and has the potential to create new industries; it changes “who does what”, and “who gets what”[4].

Developments in mobile payment systems introduced by new entrants are opening up new customer bases (eg by allowing small merchants to turn their phone into a bank card reader); previously unused data are being delivered to new stakeholders to create new revenue streams to capture value; and there is growing use of digital wallets and value transfer through different operating systems such as mobile phone providers (eg M-Pesa) rather than banks. But in many of these cases, the underlying transactions are still processed through established players using legacy systems (eg clearing banks and competing card schemes such as Visa and Mastercard). M-Pesa challenged the notion that value transfer for exchange transactions had to be done through banks, and leapfrogged several developmental stages. But these innovations still rely on an existing hierarchical structure, using proprietary technology and trusted intermediaries. Though the change improves customer convenience, and significantly reduces costs to users and customers, this is evolution rather than revolution.

Technological revolutions

Innovation generally proceeds incrementally, but is punctuated by radical episodes, described by economist Joseph Schumpeter as “creative destruction”, and by Carlota Perez as “technological revolutions”[5]. These innovations exist in a complex dynamic between technology, the economy and society, and sometimes an innovation can fundamentally alter the way in which a particular society or economy is organised.

The past few centuries have seen a handful of these technological revolutions: the original Industrial Revolution, the Railway Revolution, and the Oil Revolution, for example. Each one changed industrial structure, brought new forms of energy, and impacted the way society could organise (see Table 1). Now we are in the Information and Telecommunications Revolution, typified by information intensity, connectivity, specialisation, and globalisation.

There are typically three pillars to these revolutions: significantly lower costs, new communication methods, and changed infrastructure and logistics. Lowering the costs of pervasive inputs generates market tensions — and, often, financial bubbles and crashes — that ultimately lead to demands for an overhaul of existing institutions. According to Perez, the revolutionary innovations are characterised by a “set of inter-related radical breakthroughs, forming a constellation of interdependent technologies” and the “strong interconnectedness of the participating systems in their technologies and markets, and their capacity to profoundly transform the rest of the economy (and eventually society)”[5].

	Description	Year (approx)	New Technologies and Industries	New Infrastructure	'Common Sense Principles'
1st	Industrial Revolution	1770	Mechanised industry	Canals and water power	**Factory production, productivity, local networks**
2nd	Steam and Railways	1830	Steam engines, iron machinery	Railways, telegraph, ports	**Economies of agglomeration, standardised parts, urbanisation**
3rd	Steel, Electricity, Heavy Engineering	1875	Cheap steel, heavy chemistry	Electrical networks, global shipping	**Economies of scale and vertical integration, science as productive force, efficiency**
4th	Oil, Automobile, Mass production	1910	Cars, cheap oil, petrochemicals, home appliances	Road networks, universal electricity	**Mass production, horizontal integration standardised products, energy intensity, suburbanisation**
5th	Information and Telecommunications	1970	Cheap microelectronics, computers, mobile telephony	Worldwide digital communications	**Information intensity, decentralised networks, knowledge as capital, economies of specialisation, globalisation**

Table 1: the five technological revolutions (adapted from Perez[5])

Each technological revolution brings a different set of 'common sense principles' that change how businesses and society operate. These moved from mechanisation in factories; through economies of scale and vertical integration, mass production and standardisation; to functional specialisation, hierarchical pyramids and bureaucracy; and on to today's information intensity and decentralised networks, marked by "heterogeneity, diversity, adaptability and co-operation"[5]. These revolutions ultimately lead to a new techno-economic paradigm, with different cost structures, different opportunities for innovation, and organisations built on markedly different principles. In each paradigm, organisations develop along an 'S' curve, from disruptive innovation, through use and exploitation (and resistance), to maturity and eventual replacement[5]. Changing these existing mind sets and replacing them with a new one requires a transformational shift that requires new skills, abilities and knowledge, which fundamentally change the way business operates.

Previous technological revolutions had little or no impact on pyramidal, hierarchical systems of organisation and governance. But some suggest that our new technological era enables a potentially emergent 'Collaborative Commons', in which society is motivated by collaborative interests rather than individual gain[6]. This could imply distributed, consensual community structures that do not depend on intermediaries organised in hierarchies (such as banks and governments). DLTs represent a challenge in precisely this way.

Distributed ledger technology

DLTs are involved in potentially revolutionary innovations in a number of related areas: virtual currencies, distributed open and transparent record keeping, non-hierarchical networked systems, cryptography, and software engineering. DLTs represent an innovation towards the radical end of the change spectrum because of their potential to impact a broad extent of areas in the business model: from new products and services, through operating systems and organisational structures, to the sheer number of potential industries that could be affected. As such they form part of the interconnected and inter-related breakthroughs that form a technological revolution.

DLTs offer significant benefits to operational costs. Not only are they intrinsically low-cost, they can also avoid duplication and inefficiencies in control and co-ordination by enabling a common, open ledger that could operate at an industry

CASE STUDY 1

Diamonds

Leanne Kemp, Founder and CEO, Everledger

The diamond industry is highly susceptible to criminal activity. Gems are small and easy to transport in a covert manner, transactions tend to be confidential, and diamonds retain their value for many years. As such, diamonds are involved in money laundering and terrorist financing on a global scale.

Efforts to stem this illicit activity have included tracking diamonds with paper documents to certify their provenance. But document tampering is widespread — indeed, documents are sometimes created to cover up illegal transactions — and several countries with a major diamond trade still have insufficient legislation to guard against these crimes.

To combat this, the diamond industry is beginning to implement a system called Everledger, based on block chain technology, which establishes a digital ‘passport’ for each diamond. This records its provenance, travel, and transactions with a unique cryptographic ‘fingerprint’.

This system has three stages:

- Establish an e-ID (electronic identity) for each diamond, by digitising its attributes and a laser-inscribed serial number onto an authoritative block chain ledger
- Assign a digital passport to the diamond to record its travel, transaction history and provenance
- Detect and guard against illegal activities or fraudulent behaviour

By using an immutable block chain to hold this data, the ledger could provide transparency around all diamonds, revealing their origin, trail of ownership, and the processes they might have undergone. This ledger can act as a single version of verifiable truth about diamonds for the industry, governments, consumer markets, border control and law enforcement agencies.

The system also enables the use of smart contracts — terms and conditions relating to the sale and transport of the diamonds that can be carried out automatically. By using a block chain to create a distributed ledger, smart contracts can be tracked and used to verify business relationships and agreements. The block chain’s transparency offers a way to enforce the contract, whether it is related to changes in ownership of the diamond, financing of the diamond, its insurance policy, registered rights title and so on. Authenticating the transaction, along with documentary proof of authenticity, provides a vital evidentiary trail for government and law enforcement.

level, thus reducing the systemic costs involved in processes such as cross checking between individually held ledgers and databases. The ability to digitise and securely store information on practically any asset, from diamonds to bags of rice, allows organisations to identify and track their ownership and location (see case study on diamond authentication, p56). New methods of recording obligations and transfer of value using programmable contracts are being developed using DLT: Ethereum, for example, is a decentralised platform for 'smart contracts' (see Chapter 1). Their potential for disruption may even extend to a new landscape in which trusted or necessary intermediaries operating in a hierarchical monopoly — a 'hub and spoke' model — are joined or replaced by a more open, flatter community-based consensual structure (see case study on corporate actions, p58).

The development of DLTs and associated technologies also offers the possibility of real time recording of transactions and access, making transactions quicker and cheaper (see SETL case study, p60). For example, motor insurance could be based on the state of both the car and its driver, with insurance provision changing between suppliers depending on behaviour, price and appetite for risk. This could lead to a 'programmable economy' involving smart contracts, relying on decentralised networks and agents that require less human involvement, and operating as distributed autonomous organisations that deliver a wide variety of products and services.

The best example of an operating DLT is the cryptocurrency Bitcoin, and the most obvious place for a new currency to innovate is in financial services. DLTs offer a lower cost of operation within existing structures and governance, but they also provide the chance to reduce system-wide costs and complexity. They could do this by removing the duplication and cost of many separate, proprietary systems, and by challenging those systems' centralised architectures. Money creation no longer becomes the sole responsibility or prerogative of national governments, for example. Instead, new forms of currency could emerge where identity, and connections between people, becomes the means of endorsing and underwriting transactions within a community[7].

FAQ

What are the threats arising from DLT?

Like any radical innovation, DLTs provide opportunities to incumbents, and also threats to those who are unable or fail to respond. Through their distributed consensual nature they also threaten the role of trusted intermediaries in positions of control within a hierarchy. Block chains that explicitly create a new currency, such as Bitcoin, challenge the current supremacy of governments in managing the national and international economic and monetary system.

A further development enabled by the technological advances is the possibility of adding specific attribute information (eg physical assets or contracts) to the basic bitcoin to produce 'coloured coins'. This opens up the possibility of money with more than just value: it could carry attributes such as necessary purpose, expiry date, or location of allowed use. For example, money may have restrictions on the kind of goods and service it can be used to purchase (see Chapter 6); or someone renting a flat through Airbnb may have their electronic access key revoked if they fail to pay on time, or if their contract has expired.

Considerations for government

With its wide range of stakeholders, services and roles, the government obviously has a multitude of different operations. Some distribute value rather than create it, and others create and maintain effective regulatory regimes. Many of these activities will be enhanced by the innovations afforded by DLT, and others will be challenged. Change is possible at the product and service level, and at the operational and organisational level.

CASE STUDY 2

Corporate actions

Dominic Hobson, Founder, COOConnect

Listed companies must provide their annual accounts in a structured format, but any company announcements that may require action by investors or their representatives — known as corporate actions — are typically published as unstructured text, or in PDF format. Those relying on the information have to read and interpret the data manually before taking action.

Over 90 per cent of corporate actions are distributed by data vendors, and then processed on behalf of investors by an agent such as a custodian or fund manager. Information is manually extracted from the original, interpreted and re-keyed by vendors. Levels of automation are low, errors frequent, and the process highly inefficient. One estimate puts the global cost of corporate actions processing at up to $10 billion per year1. Custodians frequently reimburse clients for missed or incorrect execution of instructions.

Block chain technology could make this process more efficient. Corporate actions represent contractual information and value, which can in principle be transferred directly between payers and payees without the need for intermediaries, provided the parties can trust the source data and have the necessary experience to act upon the information they receive.

If a block chain was coupled to an application that captures and stores corporate action announcements in a structured format, it could be used to ensure that the data is from a verified source, and prove the time-stamped date that it was issued. This could be done in reverse for the execution of instructions. A distributed ledger based on such a block chain would reassure parties at every point in the process that their information is accurate, up-to-date, and unchanged since it was published by the issuer. In theory, it could eliminate all intermediaries between the issuer and the fund manager, guaranteeing the accuracy and timeliness of the information.

The important question is whether this can be organised in a fully-decentralised manner. Corporate action information differs from simpler contractual information (such as money changing hands) because investors and shareholders often need to use intermediaries with specialist knowledge to act on their behalf.

These intermediaries may need to be able to modify or augment the data before passing it on, and the original corporate action itself may change, through follow-up announcements that supersede earlier ones. This modified data could quickly lose its provenance as data vendors share it with clients or package it with other data, making the process difficult to automate.

On its own, block chain technology is currently too slow to cope with these constantly shifting packages of data. Bitcoin's block chain can handle about 20,000 transactions per hour, with up to an hour's latency before a transaction can be trusted. That would be very inconvenient in a corporate action process, which is subject to a final deadline that fund managers prefer to keep open as long as possible.

For instance, the process of ensuring that financial transfers such as welfare payments go to the right person at the right time could be improved in a number of ways (see Chapter 6). A single ledger carrying the identity and entitlements of potential claimants, updated in real time, could be a radical innovation that is much more efficient, reducing both operating and development costs. Adding attributes to a particular payment could mean that as well as the amount, the purpose and timeline of expenditure could be both specified and tracked. This would, of course, involve extensive negotiations with stakeholders, and may require some management of this form of currency to ensure any desired parity with sterling.

There are innovative possibilities in replacing hierarchical organisations with more distributed systems. The government and its agencies tend to have tiers of authority, both internally and within their respective systems: for instance, citizens are represented by elected officials in local, national and supranational institutions; financial matters involve clearing banks, clearing houses, central banks and governments. Rather than relying on periodic ballots based largely on paper records, democracy could be achieved through a voting block chain, with electors given a digital wallet and a 'vote-coin'. This has the potential to reduce fraud (because each voter can check that their vote was counted), but also to introduce a real-time democracy with a vote on any issue. This raises significant questions of social responsibility and willingness to partake, but could create more distributed forms of democracy.

The Monmouth-based company Codel, which handles corporate actions data, has overcome these limitations by combining a block chain system with its digital notary software. This system creates an immutable audit trail that parties along the chain can refer to in order to establish authenticity, offering valuable reassurance about the provenance of data.

These run alongside Instant Actions, a new searchable central registry of corporate action information that is a collaborative venture between industry participants and Codel. The registry's data is stored in the ISO 15022 and ISO 20022 formats, which provide guidance for the distillation of financial information into machine-readable formats. This means the registry can be updated as corporate action information is modified or superseded. This guarantees the integrity and accuracy of the information, which can then be made available to all parties in the corporate actions chain via the SWIFT secure network. This overcomes the verification delays of using a block chain alone, and the information — effectively shared as a distributed ledger — can be updated, distributed and modified in real-time, guaranteeing that it is accurate and up to date.

The government could help such systems to flourish by altering regulations to require companies to issue corporate actions information using a distributed ledger approach.

Threats

The innovations enabled by DLTs may be attractive, but they are not without significant threats, including those involving the nature of money and the role of hierarchies and trust.

CASE STUDY 3

SETLing transactions

Dominic Hobson, Founder, COOConnect

Clearing, settlement, custody and registration services all add a significant cost burden to issuing, trading and holding securities. There are a plethora of specialist agents and counterparties involved in moving securities and cash between investors. Not only are there specific charges for these services, there are also ancillary costs related to dealing with the myriad of different systems that need to be interfaced and integrated with business processes. In total, the global finance industry pays around $65 billion to $80 billion per year in post-trade costs.

Block chain technology offers a means of significantly reducing the complexity and cost of these post-trade services, enabling participants to operate a shared ledger that is stored on a large number of servers acting as nodes. The authority to execute transactions is conferred by public-private key cryptography.

Transactions are added to the database in blocks, and each block is reviewed by the nodes. The block is only added to the database if the node reaches a consensus that the block only contains valid transactions. Apart from setting up and maintaining the nodes, this block chain network should be completely autonomous, and does not require a controlling or regulating entity.

The SETL solution

A privately funded venture called SETL intends to develop and deploy a specialist block chain that will allow financial market participants to settle securities transactions on a peer-to-peer basis, and to maintain a distributed ‘golden’ ledger of securities and cash balances. In particular, SETL aims to have central bank money available on the block chain. Its block chain will run on an autonomous basis, and will integrate with the current financial markets, payments and exchange infrastructure.

SETL will be able to handle both the security and cash side of each transaction and will also allow for one-sided transfers of securities and cash, either as simple payments or to settle bespoke contracts, corporate actions, dividends and coupons.

SETL will be designed to collapse the costly and risky clearing and settlement process into a real-time settlement process between counterparties. In addition, by establishing a golden ledger of ownership, SETL will substantially reduce the overhead of securities registration and custody.

The SETL block chain will have the following characteristics:

- Public keys used in the SETL block chain will need to be signed by a certifying authority, making it apparent to users of the block chain who has certified each key. Certifying authorities will maintain details of the real-world identities of public key users, and complete anti-money laundering and Know Your Customer checks. SETL anticipates that the certifying authority will disclose that information when legally required to do so.
- It will have sufficient capacity to process thousands of transactions per second, commensurate with normal volumes in the financial markets.
- It will be able to handle multiple asset classes, including cash and securities of all types.
- It will allow multi-signature transactions, enabling authorization by a designated subset of users.
- It will allow ‘atomic transactions’ (ie either all transactions occur, or none do), so that

DLTs could disrupt conventional financial services, whose core business is money and value transfer. But money itself is already being disrupted in all its forms and uses through cryptocurrencies such as Bitcoin, an invented money with no government backing; and ‘colored coins’, which allow units of currency to carry different types of value. The management of money, and through that the economy, is seen by many to be a key role of government, so alternative currency systems may pose a threat to that role.

transactions will only be processed if all stages have been submitted and properly authorized.

- It will contain specific functionality designed to facilitate the management of liquidity by the participants.
- It will maintain a complete record of transactions and balances historically for the purpose of simplifying regulatory record keeping, transaction reporting and audit.

Wider benefits

Balances of cash and other assets currently tend to be maintained on specific systems and can only be deployed for particular purposes: in other words, they are ‘system specific.’ Cash and assets held on a block chain are, in contrast, available to be deployed for any purpose. This will both reduce the amount that banks have to deploy in liquidity reserves, and will simplify their management of liquidity.

SETL expects to be able to provide a solution that will run alongside the existing Bank of England Real Time Gross Settlement (RTGS) system, providing a safe and viable alternative should RTGS be unavailable at any time. SETL will be available at all times, reducing the inter-bank risk that currently accumulates when RTGS is not running eg overnight and at weekends.

The SETL payment and settlement system will be simple, unified and immediate. If the UK is the first to deploy such a system, it will promote London and sterling as the location and currency of choice for financial services. It is likely that once established in London, the system would be adopted more widely, further consolidating London’s position as the global leader in international finance.

DLTs pose a threat to any hierarchical structure through an ability to connect and operate in a distributed network, without trusted or necessary intermediaries, by replacing top-down control with consensus. Hierarchies can have serious disadvantages: duplication, added cost, potential abuse of power, and opportunities for financial mismanagement. But hierarchies do offer advantages whenever a neutral broker is needed; and, for example, in representative democracy.

Representative democracy provides stability and an ongoing process of civil government that could be threatened by wider use of DLTs. Nation states are already facing threats caused by globalisation and increasingly fluid borders, yet some of the original developers and adherents of Bitcoin espouse extreme anti-government views. The challenge will be to ensure that DLT and its associated innovations are directed towards a connected, productive society, within a supportive infrastructure.

Conclusions

The convergence of creativity and technology can lead to radical changes in existing business models and the organisational structures they sit within. DLT is presently as much a series of challenges and questions to existing structures, as opposed to a set of answers and practical possibilities. But it appears to have at least some qualities, and to be in the appropriate context, to produce change at the more revolutionary end of the spectrum.

DLTs offer significant challenges to established orthodoxy and assumptions of best practice, far beyond the recording of transactions and ledgers. These potentially revolutionary organisational structures and practices should be experimentally trialled — perhaps in the form of technical and non-technical demonstrator projects — so that practical, legal and policy implications can be explored.

Radical innovation in business models, particularly in structures and operating systems, can occur through experimentation within a relaxed but effective regulatory environment. The government should consider how regulatory regimes can best encourage and exploit an environment in which these low-cost operating models and organisational structures could be explored, with new entrants able to participate freely.

More research is needed, at a system-wide level, on the financial costs and benefits of adopting distributed ledger technology. This would enable the government to identify what existing frictional costs could be avoided, and where remaining cost savings and opportunities could be found.

CHAPTER 6

Applications in Government

Distributed ledger technology is already having a profound impact on how private companies manage data and interact with customers and suppliers. If applied within government it could reduce costs, increase transparency, improve citizens' financial inclusion and promote innovation and economic growth. This chapter considers five case studies that illustrate those benefits.

Author

Catherine Mulligan, Research Fellow, Imperial College London and Head of Digital Strategy and Economics, Future Cities Catapult. Additional contributions from Simon Taylor, VP for Blockchain R+D, Barclays; and Mike Halsall, Global Grand Challenges, Singularity University, NASA Research Park, California

Chapter 6: Applications in Government

Introduction

Distributed ledger technologies (DLTs) can do far more than simply manage digital currencies such as Bitcoin. The concepts and structures developed for distributed ledgers and the block chains they use are extremely portable and extensible to other areas of economic and social activity. As such, they have a profound potential for application within government operations — indeed, the eventual impact of DLTs on British society may be as significant as foundational events such as the creation of Magna Carta[1].

If applied properly — and issues of privacy, security, identity and trust are addressed thoroughly (see Chapter 4) — distributed ledgers create genuine opportunities for the government and other local and regional authorities in the following ways:

- Reduced cost of operations, including reducing fraud and error in payments
- Greater transparency of transactions between government agencies and citizens
- Greater financial inclusion of people currently on the fringes of the financial system
- Reduced costs of protecting citizens' data while creating the possibility to share data between different entities, allowing for the creation of information marketplaces
- Protection of critical infrastructure such as bridges, tunnels etc
- Reduced market friction, making it easier for small and medium-sized enterprises (SMEs) to interact with local and national authorities
- Promotion of innovation and economic growth possibilities for SMEs

This very broad range of possible benefits are delivered through the application of DLTs in three different ways:

- Within currency applications
- To manage contracts and create new forms of contracts
- To prompt new applications by third parties, and provide more efficient ways of structuring and carrying out activities

Within this chapter, we illustrate each of these opportunities and its application to the different technical implementations through five separate case studies:

- Protecting critical infrastructure against cyberattacks
- Reducing operational costs and tracking eligibility for welfare support, while offering greater financial inclusion
- Transparency and traceability of how aid money is spent
- Creating opportunities for economic growth, bolstering SMEs and increasing employment
- Reducing tax fraud

Case 1: Protecting Critical Infrastructure

Overview
DLTs can enable the UK and its government to better protect critical civil infrastructure against cyberattacks.

Background
Digital technologies are increasingly embedded in countries' critical infrastructures, and many of these systems are also connected via the internet. This exposes them to the possibility of attacks from hackers or other nations that are able to go undetected by existing cybersecurity defences. It is, for example, possible to seize control of critical routers, allowing them to be monitored and manipulated. This would allow the data from all the companies and government organisations behind the routers to be captured. Moreover, as various other embedded technologies are adopted in civil infrastructure — including bridges, railways, tunnels, flood barriers and energy installations — the chance that such attacks could cause damage to property and human life increases.

DLT proposition
DLT may be applied to ensure that the operating system and firmware used in a piece of critical infrastructure has not been tampered with. A distributed ledger could monitor the state and integrity of the software for illicit changes, and assure that data transmitted from systems that apply Internet of Things (IoT) technologies has not been tampered with.

Outcomes

- Efficiency and effectiveness improvements to large-scale infrastructure, ensuring better protection to human life
- Data integrity can be assured for transmissions to and from critical infrastructure

Maturity level
Ready

Case 2: Department for Work and Pensions

Overview
Novel payment models will enable HM Treasury (HMT) and the Department for Work and Pensions (DWP) to distribute welfare support more efficiently and improve policy delivery. By applying DLTs in the registration and payment processes for government grants and benefits, DWP will be better equipped to:

- Prevent financial losses through fraud and error
- Support the most vulnerable citizens by offering them the benefits of full financial inclusion
- Support the achievement of the government's wider policy objectives, especially getting people out of poverty in a sustainable way
- Offer good value for money and place public expenditure on a sustainable footing

Background

The DWP pays out roughly £166 billion of taxpayer's money in welfare support per year. Some £3.5 billion of that sum is overpaid through fraud (£1.2 billion), claimant error (£1.5 billion) and official error (£0.7 billion)[2] of which £930 million is recovered. Adding in the fraud and error that exists in the current tax credit system, which will be moving to DWP over the next few years as an element of the new Universal Credit regime, there is a total baseline of over £5 billion per year in gross overpayments.

Apart from the direct financial cost of overpaying money to those not entitled to it, the taxpayer also bears the cost of post-payment intervention (debt collection, investigation and prosecution, claimant queries and dispute resolution).

A further, as yet unquantified, proportion of welfare support spending will fail to meet policy objectives in less identifiable ways. For example, it may effectively fund expenditure by claimants that arises from the way that welfare support is distributed, ultimately servicing non-bank debt and paying the 'poverty premium'[3].

DLT proposition

A large number of welfare claimants are un- or under-banked[4] and face barriers to greater financial inclusion such as credit checks, access to traditional financial products, and the costs of unauthorised transactions. DLTs offer a cheap and supportive means of getting these claimants into the benefits system.

Digital identities could be confirmed through distributed ledgers running on securely-encoded devices — or even through software on a mobile device — which would allow end-users to receive benefits directly, at reduced transaction costs to banks or local authorities. This may allow them to become more fully included in the financial system through a secure distribution point that is more reliable than a bank account. Such a solution could also be linked with other systems to reduce the level of fraud and official error in the delivery of benefits, as identities would be more difficult to forge.

Such activities may help to achieve one of the DWP's principal policy objectives: to lift people sustainably out of the cycle of poverty and state dependence. Through the innovative application of such technologies, it would be possible — with agreement from the benefit claimant in question — to set rules at both the recipient and merchant ends of welfare transactions. This may present the opportunity for ministers to consider options for achieving better policy outcomes from the distribution of welfare support by agreeing or setting rules around the use of benefits.

Outcomes

- Reduction of losses due to fraud and official error
- Enable ministers to assure taxpayers that public funds are being used more effectively for the purposes of meeting genuine need

Maturity level

- Requires a lot of education for the recipients
- Requires some integration of sterling onto a distributed ledger for benefits
- May create a subset of the economy with a stigma attached to 'benefit coins'

Case 3: Stregthening International Aid Systems

Overview

DLT could enable the government to better control the distribution of foreign aid, and to ensure that the funds reach the intended recipients. This will also help ministers help improve transparency and encourage effective financial management. The use of DLT could therefore help in honouring the UK's international commitments to achieve the Global Goals.

Background

In order to meet global obligations, countries must support Global Goal action plans that incorporate transparency, accountability and integrity measures[5]. International aid donors place significant emphasis on helping to develop more transparent and robust aid systems. Activities preventing fraud, theft and mis-appropriation of funds can be expensive. Technological advancements that could help strengthen prevention efforts would be beneficial for the wider aid system

Fraud and corruption reduces opportunities for poverty alleviation, reduces inward investment, and is strongly linked to lower educational achievement. There is, therefore, a great opportunity to apply DLT in international aid in order to provide transparency and traceability of funds. Proving that money is being well spent could encourage nations to give more, and also all funders to target key outcomes more effectively.

DLT proposition

The key aspect of this proposition would be to use three main aspects of DLT. Firstly, it would allow international donors to issue coins that have a sterling value, without encountering many of the bureaucratic hurdles of traditional banking. Distributed ledgers achieve this through their lack of geographic boundaries — they operate in the same way in any jurisdiction in the world. There is an opportunity, therefore, to reduce the foreign exchange fees for international aid significantly below standard transaction costs. Moreover, it is possible to create smart contracts that can be used "to create self-enforcing contracts between strangers, offering citizens a framework for transactions independent of the domestic judicial and executive branch"[6].

Secondly, international donors could take advantage of DLT's ability to reduce the fungibility of cash, offering the possibility of reliable and irreversible transfers of digital goods — in this case aid funding. In addition, digital ledgers solve the double-spending problem: where digital currencies may allow end-users to spend the same unit of currency twice, digital ledgers prevent this because each 'coin' is unique. This makes payment without intermediation possible[6]. In cases where aid is meant to directly support end-users, it is possible to bypass the limitations and restrictions placed on currencies and banking services in some countries through peer-to-peer transfer of funds.

Thirdly, the use of unique sterling-linked coins could prevent them from being spent on items not deemed appropriate within the international aid context. For example, money sent to build infrastructure intended to reduce poverty could not be appropriated for other purposes. This stems from DLT's ability to trace exactly where the currency has been spent and by whom.

Outcomes

- Increased transparency of international aid spending targeted specifically at the Global Goals to reduce corruption to better achieve desired development objectives.

Maturity level

- Unpredictability of donor demands may create bigger problems than fraud and corruption, and would therefore need to be carefully aligned to project outcomes to ensure effectiveness.
- In every case of international aid, international donors needs to maintain a relationship with the host government. Where issues of corruption are linked to individuals within specific ministries or embedded within the systems of host governments, it is crucial to get buy-in from the recipient nations for this type of system.
- Converting distributed ledgers into usable services of this nature requires the creation of a whole range of complementary capabilities

Case 4: Reducing Market Friction and Enabling Innovation

Overview

One of the greatest potential benefits of DLT is its ability to remove barriers and friction in the market and enable the creation of new forms of information marketplaces[7]. As discussed in Chapter 1, the sharing of information between economic entities through distributed ledgers would enable new forms of innovation to emerge. This would allow ministers to achieve policy outcomes centred on assisting SMEs achieve economic growth through effective use of technological innovation.

Background

Reducing transaction costs for SMEs when dealing with local and national government would enable these businesses to move more freely within the market and face lower overall operating costs. At the same time, enabling these companies to register their intellectual property (IP) within a distributed ledger, rather than through traditional patent applications, may reduce the overall number of contract disputes. Contract disputes make up 57% of all litigation in the UK, more than any other category of legal action.

DLT proposition

DLTs could be applied in a broad variety of areas, particularly in smart contracts and asset registration. By registering assets on a distributed ledger, all property could effectively become ‘smart assets’, providing a robust and trustworthy proof of record for a broad variety of services that currently cost SMEs time and money. Examples include registering IP and patents, wills, notary services, NHS health data and SIPPs/Pensions. Distributed ledgers offer a new way to co-ordinate these types of services, in a truly digitally-enabled manner, with scale and efficiency.

Distributed ledgers have the ability to handle micropayments, decentralised exchange, token earning and spending, and transfers in a way that the web currently does not[8]. As a result, DLT has the potential to re-invent the operating costs of local jurisdictions and businesses through[9]:

- Business licencing
- Registration
- Insurance
- Taxation management at many municipal and regulatory levels
- Pension data

It is possible that DLTs could help to completely remove some functions, as companies are able to register identities not just for their businesses, but also for their assets. More importantly, citizens can also have more control over their data assets (such as health data), which are traditionally held by government. This would enable citizens to check whether their data has been accessed and used in the correct manner for the correct reasons.

In addition, the use of distributed ledgers allows for sharing of data across new forms of information marketplaces — or possibly even data utilities — allowing for the sharing of pension data.

Outcomes

- Reduced transaction costs for SMEs and streamlined cost of operations for local and national government. Additionally, having a trustworthy proof of ownership for digital assets such as IP will reduce the options for litigation, providing an overall social benefit for UK society.

Maturity level

- Requires local and national authorities to adopt DLTs

Case 5: European VAT

Overview

The economy can be categorised in many ways, including (i) the tax-compliant economy, (ii) the tax quasi-compliant economy and (iii) the tax non-compliant (or ‘black market’) economy. VAT shortfalls occur in all three for a variety of reasons that may include business insolvency; creative use of international laws to structure companies in such a way as to circumvent tax liability; or the more straightforward ‘no paperwork, cash only’ scenarios. The annual shortfall in the EU’s value added tax (VAT) revenue is estimated to be between €151 billion and €193 billion[10].

DLT has both the exponential growth characteristics and the potential to make transactions significantly more transparent. The UK could play a pivotal role in supporting the development of technology, process protocol and implementation solutions for DLT in order to reduce the EU’s VAT shortfall.

Background

Moore’s Law correctly forecasted the exponential growth in digital computational processing density several decades ago. In fact, information technology has been growing exponentially since the late 1800s, with current predictions indicating this should continue throughout the 21st century.

Information technologies are self-generating because they help to navigate the unknowns of nature through scientific discovery. This in turn enables us to develop faster and more cost effective technologies, thus uncovering more of nature’s secrets, which ultimately leads to a compounding of technological capacity.

There are numerous information technologies available to help significantly reduce VAT shortfalls, including machine learning, super digital computers, quantum analogue computing, and distributed ledger technology. The key challenge is for governments to implement and leverage these technologies faster than organised crime groups can deploy them.

DLT proposition

The development of an EU-wide series of VAT standards and protocols would enable DLT to be deployed across Europe, with unilateral alignment of all VAT accounting transactions, from invoices to bank receipts. The system could include smart contracts designed to outsmart the tax quasi-compliant economy, which would also help to address the various threshold differences in VAT applicability across EU member states.

With machine-learning devices reading the EU’s VAT transactions in real time, erroneous transactions (including so-called carousel fraud) are far more likely to be spotted than by the current methods of auditing. Increasing traceability and transparency — including payment providers, banks and other financial institutions — would make the black-market economy more difficult to conceal.

Outcomes

- Reduce the administrative burden imposed on companies and other organisations to collect and pay VAT
- Increase transparency of real-time transactions throughout the economy
- Create opportunities to assess credit risk more accurately, reducing losses caused by insolvency
- Provide data to lenders that offer finance to SMEs, including credit factoring
- Enable smart contracts between treasuries and commerce

Maturity level

- Technologically ready
- Important to bring payment organisations into the conversation early on, as their data inputs are also required to ensure visibility over payment settlements
- Government agencies need to be able to handle DLT for tax
- End-users and small business owners need to understand how to use DLT for effective tax management

Conclusion

Distributed ledgers undoubtedly hold value for government, offering new ways of operating that reduce fraud, error and the costs of delivering services to underserved users. At the same time, these technologies offer new forms of innovation and the ability to reduce transaction costs for SMEs in the UK. This chapter has highlighted only some of the possible use cases. As distributed ledgers are adopted more widely, it is likely that a new form of operating government services will emerge.

CHAPTER 7

Global Perspectives

Organisations that do digital business in cyberspace must be able to trust — and be trusted by — their partners. They also need to be interoperable with large and growing communities of other organisations around the world. Block chains have the potential to contribute to both.

Author

Patrick Curry, Director of the British Business Federation Authority; Christopher Sier, Director, FiNexus; and Mike Halsall, Global Grand Challenges, Singularity University, NASA Research Park, California

Chapter 7: Global Perspectives

Introduction

The rate of global change — both good and bad — is accelerating, driven by internet-enabled globalisation, societal expectations, and increasing competition for resources. Unlike the developing world, developed nations and their citizens have a consumerist ethos and privacy expectations that can conflict with traditional, resilient community values and personal norms of behaviour. This has left the state, rather than the community, responsible for helping those in distress and hard times. Governments struggle to satisfy these growing demands of consumer expectation and seemingly bottomless social assistance. US President John F. Kennedy's call — "ask not what your country can do for you, ask what you can do for your country" — has increasing relevance today: most citizens want to help their country but they lack the means to engage in the digital age. They want to be part of the herd, not a vulnerable outlier.

One consequence of this lack of community behaviour is a polarisation in attitudes, an emergence of differing perceptions and an increasing tendency to oversimplify complex changes into a series of binary disconnected issues. The global reality is a complex mesh of physical, virtual, legal, historical, geographical, societal, behavioural, economic, informational and technological factors. The rate of change and the speed of introduction of new, disruptive technologies add to this complexity. Scale, speed and complexity have to be considered together. This makes it increasingly difficult for industry leaders and national governments to understand this mesh, and to plan, implement and realise benefits using their traditional non-collaborative organisational structures. The initiative lies with those who are more agile, such as the financial markets and organised crime. Increasingly, developing nations such as Kenya and Rwanda are leaping to new technologies, unencumbered by this legacy. In the developed world, some smaller and more homogeneous nations are making significant advances that are transcending borders to provide international benefits, particularly in Europe (see case studies on European energy markets, p76, and on Estonia, p80).

The hallmarks of advancing digital nations include:

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

The UK has much to do in each of these areas if it is to become one of the leading digital nations. Yet the world increasingly relies on digital economies. This requires us to do more than apply computer technology to existing economic models; instead, we must reassess our understanding of what a digital economy is becoming, as well as its constituent actors and activities. This is similar to the transition from cash-based to asset-based accounting, which requires every organisation to have a much wider understanding of the complexity of supply chains, services and markets, and demands a different approach to collaborative risk management, decision making, gainsharing and shared liability. To do digital business in cyberspace, an organisation has to be able to trust, and be trustworthy. It also has to be interoperable with large and increasing communities of other organisations. Trust and interoperability are foundational in cyberspace, much more so than in the physical world. Block chains have the potential to contribute to both, but the magic is not in the technology — it is in how we use it nationally.

Trust and interoperability

Trust is a risk judgement between two or more people, organisations or nations. In cyberspace, trust is based on two key requirements:

- Prove to me that you are who you say you are (**authentication**)
- Prove to me that you have the permissions necessary to do what you ask (**authorisation**)

If I am not satisfied with the response, I can still choose to allow you to proceed, but I am incurring risk. However, there is no viable relationship unless others trust me too. In this sense, being trustworthy is analogous to being creditworthy.

Interoperability involves several factors:

- Data interoperability. We need to understand each other in order to work together, so our data has to have the same syntactic and semantic foundations
- Policy interoperability. Our policies need to be aligned or based on agreed common policy, so that I can be confident that you will treat my information in the way that I expect (and vice versa)
- The effective, collaborative implementation and use of international standards

Information protection is about access control, which requires authentication, authorisation and more. Authentication requires identity management of all entities involved (usually people, organisations, devices and software), to a given, internationally-defined level of assurance (LoA). Authentication across communities of multiple authorities or organisations requires federated identity management (FIM).

At an international scale, such FIM currently exists only at ‘low assurance’, designated LoA 1 in international standards[1]. It is primarily applied in social networking where multi-jurisdictionality is not a significant issue. Google, GakuNin (the Japanese universities network), Microsoft, Ping Identity, The Nikkei newspaper, Tokyu Corporation, mixi, Yahoo! Japan and SoftBank have also deployed FIM systems; and there are more mature deployments underway by other organisations, such as Deutsche Telecom, AOL, and Salesforce.com.

Medium assurance (LoA 2) requires evidence of identity during enrolment to meet Know Your Customer (KYC) requirements, which financial institutions require of consumers and businesses in financial transactions. There is some federation at LoA 2, mostly in banking systems.

Several industries use security systems based on Public Key Infrastructure (PKI) federations that rely on a cryptographic standard called X.509. These offer high and very high assurance levels (LoA 3 and 4) for employee authentication, notably in aviation, the pharmaceutical industry, defence, banking and, increasingly, e-health. The US and China have the largest deployments of international-standard PKI federations, closely followed by South Korea (where it is mandated for all companies by regulation), Estonia, Netherlands and many others. At LoA 3+, it is possible to link a user's identity to other trust functions, such as legally-robust digital signatures, identity-linked encryption and physical access control in buildings. PKI federation isn't the only option for high assurance supply chain collaboration and sharing sensitive information at scale, but it is the de facto norm today. Block chains offer a potential alternative, but a combination of PKI federation and block chain federation offers even more attractive opportunities for greater digital accountability, assurance and trust in business processes, coupled with exploiting new technologies.

In the UK, only the police service operates a large-scale PKI federation in accordance with international standards, albeit in a basic form. With best-practice collaborative governance, this could be expanded to support many UK government services, including the emergency services; and international collaborations in areas as broad as trade, border controls or migrants and refugees, with other allies who have similar PKI federations today. The strategy for the government's Public Services Network to use PKI federation for employee authentication has yet to be implemented, however, so there is no high assurance identity management of employees or collaborative trust across government organisations, based on international standards, that could federate with industry partners and international allies eg US, France and the Netherlands. In combination with block chains, PKI federation could provide enhanced services extending to the privacy-friendly handling of identity data and greater traceability of payments.

The NHS has a very large PKI, but it does not comply with international standards and cannot (yet) federate. The MOD has international obligations to establish PKIs with the US-centric defence supply chains, and similar obligations under the NATO Cyber Defence Action Plan, but has no published implementation plans. Industry is considering other potential areas for PKI federation eg for countering food fraud, described in the 2014 Elliott Review into the integrity and assurance of food supply networks. It is also developing a memorandum of understanding with a South Korean government agency that would enable British companies to have PKI credentials that could be used in the supply chains of Korean businesses eg Samsung, Kia, Hyundai and Daewoo (which is currently the manufacturer of the largest container ships in the world). The UN's International Maritime Organisation is developing international guidelines for maritime cybersecurity, and has the potential to leverage the UK-Korea PKI federation initiative. There are more examples in other areas, and all would benefit from a forum where these discussions can come together in a collaborative manner.

The EU Parliament approved the Electronic Identification, Authentication and Trust Services Regulation (eIDAS) in September 2014, giving nations three years to comply. Under eIDAS, if any nation 'notifies' an e-ID scheme for its citizens, the e-IDs are legally required to be accepted by every other member state for electronic public purposes. Much work has yet to be done, but eIDAS is forcing governments and industry to consider their overall plans to exploit FIM for societal and commercial benefit. In the UK, the government has introduced a federated, standards-based approach to identity assurance: GOV.UK Verify. GOV.UK Verify has been built to respond to the latest developments in the market by having competing providers of identity services and allowing users to choose which one to use. Enhancing and linking Verify to block chains and PKI federations could add value to Verify itself. Block chain and high assurance PKI federation solutions could benefit from Verify's privacy-friendly inputs. Together, in their different ways, they would contribute significantly to the UK's digital economy, border control and its efforts to combat cybercrime.

CASE STUDY 1

European energy retail market

Igor Nai Fovino and Jean-Pierre Nordvik, Joint Research Centre, European Commission

The European Commission Energy Union Framework Strategy[1] sets out the vision of an 'Energy Union' "with citizens at its core, where citizens take ownership of the energy transition, benefit from new technologies to reduce their bills, participate actively in the market, and where vulnerable consumers are protected". However, while the development of energy smart-grids is progressing steadily, the retail energy market is still waiting for modernisation. The Commission's policy initiative 'New Energy Market Design' will have to face several crucial points:

- how to deliver appropriate information on costs and consumption to consumers so that they can identify new opportunities in a fully-integrated continental energy market
- how to reward for active participation, facilitate switching of contracts and manage demand-response to dynamic prices
- how to ensure interoperability in the market for residential energy services, expanding consumers' choices, and enable a real gain from self-generation and self-consumption, and local micro-generation.

In this context, distributed ledgers can act as a new driver to enhance the level of integration and development of the energy retail market. The Joint Research Centre[2] of the European Commission is currently investigating their practical applications, such as the following cases.

1. Micro-Generation energy market. Micro-generation is the capacity for consumers to produce energy in-house or in a local community. The concept of 'market' indicates the possibility of trading energy that has been micro-generated among consumers and 'prosumers'. Traditionally, however, this market has been served by pre-defined bilateral agreements between prosumers and retail energy suppliers. Until now, electricity-generating prosumers have not had real access to the energy market, which remains a privileged playing field for the institutionalised energy suppliers. This has greatly limited the economic advantages of micro-generation for end-users. Distributed ledgers, in combination with smart-metering systems and next-generation batteries (to accumulate energy locally), have the potential to open the energy-market to prosumer production. Smart meters could be used to account and register the micro-generated energy on a distributed ledger (becoming the equivalent of an 'energy-coin' system).

Self-generated electricity could normally be either consumed within the house, or accumulated in next-generation batteries for later use, or simply given back to the grid. Alternatively, thanks to the distributed and pervasive nature of the ledger, In cyberspace, every entity and transaction binds or links to an organisation. Establishing the validity of an organisation to the desired LoA, and information about it in real or near-real time, is a fundamental digital requirement. Increasing use of block chains will considerably increase this requirement to avoid any records in the chain becoming tainted. A new international standard is being developed for digital organisational identification, known as the Register of Legal Organisations (ROLO). Several nations, including the US, are already considering adapting the ROLO specification to meet their needs. Today, globalisation and the lack of digitally-suitable business registers is resulting in a situation, particularly in the EU, where the majority of financially active organisations in a country are not registered in that country or at all, but it is not possible to tell the difference. UK industry and government organisations, including law enforcement and cybersecurity organisations, urgently need ROLO UK as a digital trust anchor. Industry is starting to develop ROLO UK, which would benefit from greater participation by government user organisations.

the produced energy could also be redeemed elsewhere, for example when charging an electric vehicle abroad; or sold through the ledger to the best buyer, according a mechanism similar to that of a stock-exchange market.

2. Energy Contracts Ledger. A consumer who intends to change energy supplier currently needs to close their contract with their current supplier, then open a new contract with a new supplier, and revisit the contractual conditions of all complementary energy services provided by third parties. Managing the administrative complexity of these operations is a real barrier to developing a competitive energy retail market, and is a source of cost for energy suppliers and distributors. Using distributed ledgers to record energy contracts online would greatly simplify these operations. It would allow consumers to finalise the transition from one supplier to another with just a few clicks on a computer or mobile device. Likewise, energy suppliers and energy service-providers would save resources otherwise devoted to these administrative operations.

There are still questions about the scalability, security and stability of such applications. However, the benefits are so promising that they certainly merit further investigation.

Digital Economies

Digital economies seek to harness speed, reach and efficiency. Federated trust enables confidence and risk reduction. Interoperability enables efficiency and re-use of capabilities. In a mature supply chain, each time a company competes in a new programme or sector, re-use gives it agility and a competitive advantage: a view held by aerospace and defence companies and voiced publicly by Airbus, Boeing, BAE Systems, Lockheed Martin, Northrop Grumman, Raytheon[2] and others.

In February 2014, Neelie Kroes, then a vice-president of the European Commission and its digital agenda commissioner, stated that “democracy must talk to technology[3]”. She argued that we are making a transition to a data-driven world in which trust is key, and that “without security there is no privacy”. She pointed out that strong cybersecurity is important to Europe’s Single Digital Market, and that the EU Cyber Security Strategy is providing the right building blocks. Without such initiatives, she concluded, democracy would “fail to manage technology”.

The dialogues on these topics involving the EU, US and the Association of Southeast Asian Nations (ASEAN) are gradually converging in banking, electronics, pharmaceuticals, food, maritime, aerospace, cyberspace and law enforcement. Through the UN and organisations like the Council of Europe, there is a growing push for developed nations to help developing nations as they become part of the global digital economy. But a lack of digital governance hampers developing nations, creating major opportunities for cybercrime and terrorism that ultimately target developed nations. The Commonwealth could play a significant role in tackling this situation. Collaboration is key.

The potential of decentralised ledgers and block chains

Economies rely on collaborative governance to provide trust in the financial markets, ensuring that all play by agreed rules. Digital economies are the same. The primary reason that block chains are associated with cybercrime is an absence of strategic governance to establish agreed rules and ensure compliance. Once such governance (with policies, procedures and mechanisms) and enforcement exist, the true societal benefits of block chains can be realised. Governmental concerns about the instabilities and vulnerabilities associated with cryptocurrencies and their trading exchanges have made governments cautious regarding the use of block chains, and, generally, they would prefer industry to lead in the development of a better situation.

The main areas for development today are:

- Ungoverned block chains are used for unregulated and criminal activities, particularly where parties seek to be anonymous and unaccountable
- Startup companies are working with leading banks to develop trusted cryptocurrencies and block chains eg a ‘trusted Bitcoin’. This could offer significant benefit to major online consumer companies
- Private block chains are being used in closed commercial communities to support digital trust mechanisms, under their own rules. These are non-interoperable and cannot scale to support supply chains

Only recently have governments started to work with industry to explore the strategic potential of block chains. But implementation will accelerate, driven by four major enablers:

- To provide a basis for cryptographic trust in a similar way to PKI. This means that block chains could federate with each other and also with existing PKI federations. Block chains could leverage PKI’s deployed scale and governance, while PKIs could leverage block chain’s payment and ledger functions. These synergies would open up new opportunities that smart, collaborative governance could accelerate.
- Permissioned ledgers contain a data field of unlimited size. Information about a transaction, including the contract, licence or copyright, could be included,

providing a strong additional factor for trust. This enables 'smart contracts' (ie the binding of the contract to the transaction — see Chapter 1 for more), offering efficiency and non-repudiation.

- Leveraging new protocols, such as the new Uniform Economic Transfer Protocol (UETP) that links the producer to the carrier, the customer, the product, the payment and the banks, and also to the smart contract. The Netherlands is leading on this, with UK industry and possible police participation. US involvement is beginning and will accelerate due to their emerging regulations for cyberassurance across all supply chains. Other nations, such as South Korea and Japan, are expected to be involved soon.
- Smartphones are becoming the de facto trusted user device. The latest smart phones include important new security features, including: Trusted Platform Module, which secures digital certificates and cryptographic keys for authentication, encryption and signing; Trusted Execution Environment, where secure processing occurs without the operating system that could be vulnerable to malware; and Trusted User Interface, which prevents a malware attack between the user and the device. Using near-field communication, the smart phone could interact securely with some national e-ID cards and electronic passports, so that a user could interact securely online with an authority eg at a border or with the police. Consumers and employees now have a secure, trusted device for the first time ever, with which they can sign transactions (eg using a block chain) and payments (eg using a 'trusted Bitcoin'). Samsung, HTC, and LG have been selling tens of millions of such advanced security-enabled smartphones, ready for the software to be deployed in early-mid 2016. Apple and others are expected to follow suit.

Strong collaborative and pervasive governance is required to ensure that these capabilities are not abused or misused. These four enablers are encouraging greater use of block chains and distributed ledgers for financial purposes, and for a growing range of other digital, data-centric purposes across supply chains and with governments. As such systems mature, and their capabilities expand, these four enablers could help to solve a number of difficult social and global challenges. Examples include:

- **Transparent and honest government**. Trust among citizens in developing countries is lower than in countries where stable and accountable legal and regulatory structures engender better community and societal behaviours. It takes a long time for people living in regions devastated by wars and autocratic regimes to trust their governments and to be relatively free of corruption. Accountability and assurance mechanisms (using block chains, FIM and related capabilities), embedded in business processes, are vital to ensure effective implementation and enforcement of laws, policies and organisational structures.
- **Tax evasion and money laundering**. When the distribution curve of a country's wealth steepens excessively, money and asset ownership seeks off-shore domiciles to conceal wealth, reducing financial liquidity in home markets and thereby diminishing economic opportunity for those further down the wealth distribution curve. Eventually, capital starvation can start to unseat economies, followed by wide-scale youth unemployment that can scar lost

generations with a long-standing distrust in their leadership. This undermines democracy, creating conditions for societal fracture, failed states, terrorism and human misery. Again, accountability and assurance are required to tackle these problems.

- **Illegal trade and environmental vandalism**. About 50% of marine species have become extinct in the past 30 years, and the situation is similar on land. Despite international efforts under the *Convention on International Trade in Endangered Species* of Wild Fauna and Flora (CITES), the evidence suggests we are heading towards the Earth's sixth mass extinction. If we are to have any hope of rescuing the global situation, we have to implement much stronger detection and asset tracking mechanisms, with the same accountability and assurance.
- **Food fraud and supply chain disruption**. The UK is more dependent on food imports than ever before, and more vulnerable to national food denial than in 1917 or 1942. The food supply chain can be difficult to track — witness the meat adulteration saga of 2013 (widely known as the 'horsemeat scandal'),

CASE STUDY 2

Estonian block chains transform paying, trading and signing

Alastair Brockbank, British Embassy Tallinn

Experimenting with block chain technology was a logical step for Estonia. By providing a distributed and unalterable ledger of information, it has ideal qualities for the storage and management of public keys. These are a form of encryption key, provided by a designated authority, which can be combined with a private key to effectively encrypt messages and authenticate digital signatures. Estonia now has the most regularly used national Public Key Infrastructure (PKI) in the world.

Moreover, as a decentralised solution, a block chain is inherently more portable and scalable. It is capable of computing vast amounts of data every second and seamlessly working across borders. For companies in a country of just 1.3 million people, block chains thus offer a way for national solutions to more easily become global solutions. Their computational power also makes them faster, and in certain cases the technology has the disruptive power to make existing intermediaries redundant.

The three case studies below — profiling a bank, a start-up and a cybersecurity provider — show the transformative power of block chains for a wide range of transactions. All three examples underline that block chains must be made user-friendly. The customer need not know that they are trading in coloured coins, nor that their ID card login uses hash-function cryptography. In this sense, a block chain acts as a silent, more efficient workhorse behind a solution that looks familiar: a mobile payments app, an online crowdfunding and trading platform, or a login portal.

As in the UK, the need for and extent of regulation is a key issue for the Estonian authorities. They understand that hesitation and indecision can be as damaging to innovation as strictness. The risks of innovators moving to new and less tightly regulated jurisdictions — specifically, the loss of revenue from failing to capitalise on commercial opportunities, and the potential for criminal activity — are patently clear.

for example — and there are many opportunities for fraud. The international and UK food supply chains have no choice but to follow best-in-class supply-chain assurance from other sectors, in order to implement accountability and granular traceability.

- **Supply chain threats**. As cybercrime and international intellectual property theft increase (involving sums of more than $7 trillion globally), supply chains are coming under increasing regulatory, market and societal pressures for stronger assurance based on collaborative risk management, including accountability and federated identity management.

Along with other advanced nations and international experts, the UK could influence the Council of Europe, the World Bank, G20 and the UN to implement block chains with strong authentication, to provide and enforce accountability and assurance. The UK government cannot do this alone. Industry wants the government to be part of an energetic national approach to achieve national capability and first-mover advantage, collaborating with industry to ensure UK is amongst global leaders.

A pioneering bank issues cryptocurrency securities

Earlier this year, LHV Pank — the largest independent Estonian bank — became the first bank in the world to experiment with programmable money when it issued €100,000 worth of cryptographically-protected certificates of deposits. The experiment followed the establishment of a new LHV subsidiary, Cuber Technology, focused exclusively on Bitcoin-based digital securities. Cuber's work comprises two strands: CUBER securities and the Cuber Wallet.

CUBER (Cryptographic Universal Blockchain Entered Receivable) securities are simply bank certificates of deposits recorded in the Bitcoin block chain. They are denominated in euros, may pay interest and are suitable for various purposes — as a store of value, medium of exchange, trust and escrow services, and even for machine-to-machine transactions, opening potential applicability in the Internet of Things (IoT). LHV views CUBER securities as the Lego building block for their future financial innovation.

The Cuber Wallet is the first demonstration of CUBER usability. It is a piece of software for mobile phones, enabling instant and free peer-to-peer euro transactions, and low cost instant payments for merchants and consumers, using underlying CUBER securities.

Users store their private keys on their smartphone to enhance security and mobility. To protect against server compromises, Cuber Wallet decentralises trust from the server and makes the users themselves the Bitcoin clients. The app uses SPV (Simplified Payment Verification) — a type of 'thin client' security — which means the user never has a complete copy of every block in the chain. Instead they download a smaller amount of data, the 'blockheaders', which link transactions to a place in the chain. This allows them to see that a network node has accepted the transaction, while blocks added after it further confirm that the network has accepted it.

The wallet uses bitcoins as a data carrier, which they 'paint' by adding unique markers to them. This then represents a claim in fiat currency against LHV Bank, as the entry into a database represents a claim against the traditional bank system. By using fiat currency, the wallet can be used not just for personal transfers, but also for retail payments — the merchant has to approve this payment method just as they have to approve credit cards. LHV is currently testing it in a few physical locations, but anticipate wider utility in online business, particularly for smaller payments.

The use of fiat currency undoubtedly makes the app more user friendly. LHV asserts that the underlying technology is the bank's concern: the user and merchant do not and should not need to

CASE STUDY 2 (continued)

see, nor know, that Cuber uses Bitcoin.

Cuber's open source code and application program interface are available to third parties online, inviting other cryptocurrency exchanges and developers to tap into the technology. Both LHV and its development partner, ChromaWay, prefer to drive usable innovation with smaller software developers and start-ups, rather than large banks.

When pressed on their challenges, LHV is clear: regulatory uncertainty risks killing Cuber's transformative power by severely limiting its reach. The bank urges regulators to embrace block chain technology and adapt, rather than run scared from it.

On the face of it, being backed by a bank affords Cuber huge advantages, because transferring money from a conventional bank account to a digital wallet (and back again) is simplified. CUBER is technically still a security — the foundation of bank trading — albeit with decentralised record keeping. But in reality, being a bank remains a regulatory obstacle, because they are typically subject to more legal arbitrage than new innovators. Similarly, EU Know Your Customer (KYC) rules that require a face-to-face meeting to create a bank account disadvantage Cuber when other online payment services such as TransferWise and Holvi only need a quick online sign-up. If banks are to compete effectively in this market, regulation will need to impose no additional barriers to banks, nor reduce their mobility to reach and recruit new users.

Admittedly, LHV is in an unusual position: an 'innovation-friendly' bank doing it themselves, but whose forward progress is currently restricted by regulatory uncertainty. With no positive movement, Cuber will either have to be distanced from LHV's license and the advantages that being tied to a bank bring, or look at moving outside Europe to another jurisdiction.

Developing a simple, secure and legally compliant bridge between crypto and traditional banking continues to prove exceptionally challenging for all players. But none are closer than LHV.

A liquid aftermarket for start-up investments

The illiquidity of start-up investment is a common complaint from angel investors and founders alike. Backers typically need to part with at least €10,000, and must often wait 5 or more years to exit.

Funderbeam — a reputed business intelligence platform for investors — may well have found a solution to this problem: a block chain-based investment marketplace, to buy and sell coloured coin stakes in start-up syndicates.

Investors will soon be able to use Funderbeam's online platform to create an investment syndicate for one or several start-ups. Investment can be in any configuration, and there is no limit to the size of a syndicate. A £100,000 stake could comprise one lead investor and 99 backers investing £1,000; a lead investor on £75,000 and five backers on £5,000; or any other combination. Similar to crowdfunding, this diminishes the threshold to invest in start-ups.

What differentiates Funderbeam from the crowdfunding alternatives is the issuance of 'coloured coins' representing syndicate members' stakes, which can be instantly bought, sold, or traded with other investors. This enables more fluid management of investment portfolios, and expedites financing for start-ups. The Bitcoin block chain underpins the aftermarket, allowing for fast, effective and transparent asset ownership tracking.

Every syndicate is paired with a microfund. Once a syndicate is complete, and the start-up is funded, Funderbeam's aftermarket uses coloured coins to give all members of a syndicate a digital representation of their share in that microfund, which is immediately tradable. Backers can thus sell their whole share, or a proportion of it, once they have made a decent return or want to cut their losses.

Flexibility for investors is not the only benefit the block chain solution affords. Kaidi Ruusalepp, CEO of Funderbeam, also points to the efficiencies that a distributed ledger offers through bypassing bureaucracy. “We don’t need a business registry, central depository, or another formal authority to confirm the integrity of a transaction,” he says. “With the block chain, every investment, every ownership change has a secure, distributed audit trail.”

Jaan Tallinn, co-founder of Skype and an investor in Funderbeam, lauds the additional layer of security and verification it offers for online transactions. By being decentralised and unalterable, block chains can create more transparency in the equity market, without compromising anyone’s privacy.

Funderbeam’s offering — providing flexibility, speed, security and transparency — shows how distributed ledgers can provide an alternative but wholly viable basis for small and medium-sized enterprise (SME) financing to expand in the 21st century.

The next generation of public-key infrastructure

Since 2013, Estonian government registers — including those hosting all citizen and business-related information — have used Guardtime to authenticate the data in its databases. Their Keyless Signature Infrastructure (KSI) pairs cryptographic ‘hash functions’ (see below) with a distributed ledger, allowing the Estonian government to guarantee a record of the state of any component within the network and data stores.

This is no small undertaking. Estonia has the most regularly used national PKI in the world. Using their ID card, citizens order prescriptions, vote, bank online, review their children’s school records, apply for state benefits, file their tax return, submit planning applications, upload their will, apply to serve in the armed forces, and fulfil around 3000 other functions. Entrepreneurs use the ID card to file their annual reports, issue shareholder documents, apply for licenses, and so on. Government officials use the ID card to encrypt documents for secure communication, review and approve permits, contracts and applications, and submit information requests to law enforcement agencies. Ministers even use their ID cards to prepare for and conduct cabinet meetings, allowing them to review agendas, submit positions and objections, and review minutes.

Digital authentication is thus critical to government, business and public services alike, from drafting policy and legislation, to declaring finances and registering property and inheritance rights. Over 200 million digital signatures have been made using the ID card: some 39 per capita per year and rising. It is thus imperative for the government to know its records are the right records, and that they have not been altered from the inside, or by a cyber attack.

So how does a block chain help? It helps because every alteration of a piece of data is recorded. By providing proof of time, identity and authenticity, KSI signatures offer data integrity, backdating protection and verifiable guarantees that data has not been tampered with. It is transparent and works to the user’s benefit too: citizens can see who reviewed their data, why, and when; and any alterations to their personal data must be authorised. Moreover, through using hash functions, as opposed to asymmetric cryptography used in most PKI, KSI cannot be broken by quantum algorithms. It is also so scalable that it can sign an exabyte of data per second using negligible computational and network overhead. It removes the need for a trusted authority, its signed data can be verified across geographies, and it never compromises privacy because it does not ingest customer data. It is clear that the system marks a major advancement in PKI.

Ultimately, the KSI block chain means that while the Estonian ID Card may never be immune to a breach (although there have been none so far), the government is assured that rogue alterations to public data will be 100% detectable.

References

Executive Summary

1 Government Office for Science ‘FinTech Futures: The UK as a World Leader in Financial Technologies’ 2015. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

Chapter 1

1 Government Office for Science ‘FinTech Futures: The UK as a World Leader in Financial Technologies’ 2015. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

2 IBM Institute for Business Value ‘Device democracy: Saving the future of the Internet of Things’ 2015. Available at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF

3 Government Office for Science ‘The Internet of Things: making the most of the Second Digital Revolution’ 2014. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

Chapter 2 Case Study: Research and horizon scanning

1 ‘CREDIT: Cryptocurrency Effects in Digital Transformations’ EPSRC reference EP/N015525/1 (2015). Available at http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/N015525/1

2 ‘2015 ITaaU Community Conference’. Available at http://www.itutility.ac.uk/event/2015-itaau-community-conference/

3 Networked Society Lab, Ericsson ‘ICT and the Future of Financial Services’ (2014). Available at http://www.slideshare.net/Ericsson/horizon-scan-ict-and-the-future-of-financial-services

4 EPSRC ‘Trust, Identity, Privacy and Security in the Digital Economy’ (2015). Available at https://www.epsrc.ac.uk/funding/calls/trustidentityprivacysecurity/

5 Perry M and others ‘The currency of digital money’ (2015). Available at https://www.youtube.com/watch?v=PCa3pTCegE8

6 3DaRoC ‘Digital Intermediary Exchange Toolkit’ (2015). Available at https://digitalintermediaries.wordpress.com/toolkit/

Chapter 3

1 Lessig L ‘Code and other laws of cyberspace, Version 2.0’, New York: Basic Books 2006.

2 New York Department of Financial Services ‘BitLicense Regulatory Framework’. Available at http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework.htm

Chapter 4

1 Internet Engineering Task Force ‘Certificate Transparency’ 2013. Available at https://tools.ietf.org/html/rfc6962. Also see http://www.certificate-transparency.org/

2 Melara MS and others ‘CONIKS: Bringing Key Transparency to End Users’ Cryptology ePrint Archive: Report 2014/1004. Available at http://eprint.iacr.org/2014/1004.pdf

3 Danezis G and Meiklejohn S ‘Centrally banked cryptocurrencies’ Cryptology ePrint Archive: Report 2015/502. Available at https://eprint.iacr.org/2015/502.pdf

4 Courtois N ‘Is Bitcoin Going to Split in Two?’ 2015. Available at http://blog.bettercrypto.com/?p=1811

5 Nakamoto S ‘Bitcoin P2P e-cash paper’ 2008. Available at http://satoshi.nakamotoinstitute.org/emails/cryptography/1/

6 Meiklejohn S and others ‘A fistful of bitcoins: characterizing payments among men with no names’ Internet Measurement Conference 2013 pages 127-140

7 Danezis G and others ‘Statistical Disclosure or Intersection Attacks on Anonymity Systems’ Information Hiding 2004 pages 293-308

8 Bonneau J and others ‘Mixcoin: Anonymity for Bitcoin with Accountable Mixes’ Financial Cryptography 2014 pages 486-504

9 Garman C and others ‘Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity’ Financial Cryptography Workshops 2014 pages 140-155

10 Miers I and others ‘Zerocoin: Anonymous Distributed E-Cash from Bitcoin’ IEEE Symposium on Security and Privacy 2013 pages 397-411

11 Danezis G and others ‘Pinocchio coin: building zerocoin from a succinct pairing-based proof system’ PETShop@CCS 2013 pages 27-30

12 Groth J and Kohlweiss M ‘One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin’ EUROCRYPT 2015 pages 253-280

Chapter 5

1 Christensen CM and others ‘Strategies for Survival in Fast-Changing Industries’ Management Science 1998: volume 44, pages S207-S220

2 Jacobides MG and others ‘Benefiting from innovation: Value creation, value appropriation and the role of industry architectures’ Research Policy 2006: volume 35, pages 1200-1221

3 Baden-Fuller C and others ‘Business Models & Technological Innovation’ Long Range Planning 2013: volume 46, pages 419-426

4 Jacobides MG and others ‘Who does what and who gets what: capturing the value from innovation’ Advanced Institute of Management Research Briefing 2006. Available at http://faculty.london.edu/mjacobides/assets/documents/whodoeswhat.pdf

5 Perez C ‘Technological Revolutions and techno-economic paradigms’ Working Papers in Technology Governance and Economic Dynamics 2009: Tallinn University of Technology, Tallinn, Norway

6 Rifkin J ‘The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism’ 2014. New York, Palgrave Macmillan

7 Birch D ‘Identity is the New Money’ 2014. London Publishing Partnership

Chapter 5 Case Study: Corporate actions

1 Oxera. ‘Corporate action processing: what are the risks?’ May 2004. http://www.oxera.com/Oxera/media/Oxera/downloads/reports/Corporate-action-processing.pdf?ext=.pdf

Chapter 6

1 Swan M ‘Blockchain: Blueprint for a New Economy’ O’Reilly Media Inc 2015

2 Department for Work and Pensions ‘Fraud and Error in the Benefit System 2013/14’ 2014. Available at https://www.gov.uk/government/collections/fraud-and-error-in-the-benefit-system

3 Financial Inclusion Commission ‘Financial Inclusion: Improving the financial health of the nation’ 2015. Available at http://www.financialinclusioncommission.org.uk/report

4 Rowlingson K and McKay S ‘Financial Inclusion: Annual Monitoring Report 2014’.

Available at http://www.birmingham.ac.uk/Documents/college-social-sciences/social-policy/CHASM/annual-reports/chasm-annual-monitoring-report-2014.pdf

5 United Nations ‘The Millennium Development Goals Report’ 2010. Available at http://www.un.org/millenniumgoals/pdf/MDG%20Report%202010%20En%20r15%20-low%20res%2020100615%20-.pdf

6 Ammous S ‘Economics beyond Financial Intermediation; Digital Currencies’ possibility for growth, poverty alleviation and international development’ Columbia University Working Paper No. 82 November 2013

7 Mulligan CEA ‘The Communications Industries in the Era of Convergence’ Routledge 2011

8 Swan M ‘Blockchain: Blueprint for a New Economy” O’Reilly Media Inc 2015

9 A more extensive list is available at ‘Bitcoin Series 24: The Mega-Master Blockchain List’. Available at http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list (accessed 13 August 2015)

10 EU Taxation Commissioner Algirdas Semeta, quoted in 2013 at http://www.eureporter.co/economy/2013/09/20/fight-against-fraud-study-confirms-billions-lost-in-vat-gap/ (accessed 18 September 2015)

Chapter 7

1 ISO/IEC 29115 – Entity Authentication Assurance Framework

2 Including Boeing, Northrop Grumman and Raytheon joint video.

3 EU Cybersecurity Strategy High Level Review – 28 Feb 14.

Chapter 7 Case Study: European Energy Retail Market

1 European Commission ‘A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy’ 25 February 2015: COM(2015) 80 final. Available from http://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0001.03/DOC_1&format=PDF

2 Joint Research Centre. Available from https://ec.europa.eu/jrc/

Acknowledgements

I would like to thank the many contributors for the support they have provided to this review – Sir Mark Walport, Government Chief Scientific Adviser.

The expert panel for their guidance and drafting of the evidence papers:

Robleh Ali	Bank of England
Richard Brown	R3
Patrick Curry	British Business Federation Authority
Richard Copland	CGI Group
Dr Phil Godsiff	University of Surrey
Mike Halsall	Singularity University/ Almanis
Derwen Hinds	CESG
Matthew Johnson	Guardtime
Dominic Hobson	COOConnect
Dr Vili Lehdonvirta	Oxford University
Jonathan Levin	Chainalysis
Dr Catherine Mulligan	Imperial College London / Future Cities Catapult
Professor M. Angela Sasse	University College London
Dr Chris Sier	FiNexus
Daniel Shiu	GCHQ
Simon Taylor	Barclays

Additional contributions and advice from

Hadley Beeman	GDS
Dr John Baird	EPSRC
Alastair Brockbank	British Embassy Tallinn, Estonia
Dr George Danezis	University College London
Shaul David	UKTI
Nick Davies	DWP
Igor Nai Fovino	Joint Research Centre, European Commission
Leanne Kemp	Everledger
Dr Sarah Meiklejohn	University College London
Jean-Pierre Nordvik	Joint Research Centre, European Commission
Tom Price	BIS
Thomas Wilkinson	Home Office
Naomi Wright	HMRC

The review team for their support and synthesis of the evidence papers

Dr Claire Craig	GO-Science
Martin Glasspool	GO-Science
Emma Griffiths	GO-Science
Elizabeth Surkovic	GO-Science

Editor

Dr Mark Peplow

This publication available from www.gov.uk/go-science

Contacts us if you have any enquiries about this publication, including requests for alternative formats, at:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
Email: contact@go-science.gsi.gov.uk

GS/16/1

Design and Production: WordLink