HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTbrief
Number 28, August 2018

Distributed Ledger Technology

By Lorna Christie

Inside:

www.parliament.uk/post | 020 7219 2840 | POST@parliament.uk | @POST_UK

Cover page image:
Lef Apostolakis

Overview

Distributed ledger technology (DLT) is a technology that allows multiple identical copies of a record to be stored on different computers on a network and updated by multiple different users. DLT has attracted a great deal of attention in recent years as it is the technology underpinning the majority of cryptocurrencies, including Bitcoin. Most cryptocurrencies operate using a type of DLT known as 'blockchain'.

DLT is still predominantly used in cryptocurrencies. However, more recently there has been interest in the application of DLT in other areas such as financial services, supply chain traceability, taxation and benefits payments, and 'peer-to-peer' electricity trading. There are ongoing projects to pilot the use of DLT across industry and Government in the UK.

This POSTbrief provides a technical overview of the different types of DLT and how they work. It discusses some of the main applications of DLT and highlights the benefits and challenges of the technology.

*POSTbriefs are responsive policy briefings from the Parliamentary Office of Science and Technology. This POSTbrief is based on a literature review, interviews with external stakeholders and peer review.

Suggested Citation:
Parliamentary Office of Science and technology (POST). 2018. ***POSTbrief 28: Distributed Ledger Technology***. Houses of Parliament, UK

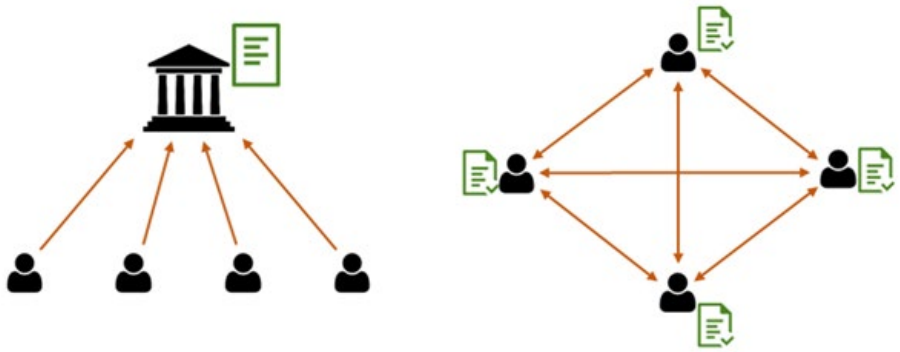
Background

A conventional ledger is simply a records system that is managed and maintained by a trusted authority. For example, a bank maintains a ledger recording its customers' financial transactions, and the Driving and Vehicle Licencing Agency maintains an up-to-date ledger recording everyone who has a driving licence. Traditionally, ledgers were paper-based; however, modern ledgers are usually kept electronically on a database. These conventional types of ledger are generally private and can only be accessed by members of the organisation in control of this ledger.

A distributed ledger is a special type of digital records system that allows multiple identical copies of a ledger to be kept on different computers on a network (such as the internet). The databases are updated and synchronised automatically each time new transactions or other data are recorded. Crucially, multiple users are allowed to update the ledger, meaning that it can be controlled by a group of participants rather than a single trusted authority (Figure 1).

Figure 1. Traditional vs distributed ledgers:

(Left) Traditional ledger, where the database is maintained by a single authority. (Right) Distributed ledger, where the database is maintained by a groupd of participants on a network



Distributed Ledger Technology (DLT) has received considerable public attention in recent years because it is the technology underpinning the majority of cryptocurrencies. Cryptocurrencies are payment systems with their own internal currency. They are designed to allow payments to be processed without any financial intermediaries such as banks, and to generate units of currency without any single issuing authority (some common cryptocurrency terms are defined in Appendix 1). The original and most widely used cryptocurrency is Bitcoin. Cryptocurrencies remain the main use of DLT, however, there are many other emerging applications of the technology.

The finance sector has been particularly interested in using DLT for trading financial assets and making payments between banks faster and cheaper. A study by Greenwich Associates found that investment in DLT in the finance sector increased by 67% from 2016–2017.[1] Outside of the finance sector, organisations have proposed that DLT could be used to assure the provenance and authenticity of valuable assets (such as diamonds), trace goods through supply chains, and execute transactions automatically. The UK Government is also interested in DLT, and there have been a number of different projects piloting its use in government operations.[2]

The Government Office for Science published a report on distributed ledgers in 2016, which recommended eight ways that the UK Government can support the development of DLT.[2] These included: establishing trials of distributed ledgers in the public sector; considering how to put in place a regulatory framework for distributed ledger technology; and working with academia and industry to develop standards for integrity, security and privacy. Further recommendations for how the Government can support the development of DLT in the public sector were made in the 2017 Lord Holmes report.[3]

The House of Commons Treasury Committee recently launched an inquiry into digital currencies and DLT in order to examine the potential impact of the technology in the UK.[4] Furthermore, the Treasury's 2018 FinTech strategy announced plans for the Government to form a task force to explore the development of DLT in the finance sector, in collaboration with the Bank of England and Financial Conduct Authority.[5] DLT research is receiving support from UK public funding bodies.[6]

Types of Distributed Ledger

Depending on the application, DLT can be set up so that different users are given different rights to access and modify records. For example, some users may only be able to view the ledger, whereas others may be able to update and add records to it. This can enable transparency by opening up records to a defined set of people and improve privacy by controlling what is shared and with whom.[2] In general, DLT can be classified as public (viewable by anyone) or private (only viewable by those granted access). Distributed ledgers can be further classified into two main types:[2, 7, 8]

- **Permissioned ledgers** that require users to have permission to verify and add data to the ledger. The members of the network are usually known to each other or selected by an organisation that controls access to the network. For example, a group of financial institutions may want to use a permissioned ledger to track the ownership of shares.
- **Permissionless ledgers** that have no owner controlling access to the network. Anyone with the right computer software can access a permissionless ledger. However, users wishing to verify and add data to the ledger must conform to some sort of consensus mechanism, which is used to ensure new data entries are agreed by the participants. Permissionless ledgers are public, however, the identity of a user is usually unknown. The first permissionless DLT to be developed was the Bitcoin ledger. Bitcoin

(and the majority of other cryptocurrency payment systems) generally use a type of permissionless DLT known as blockchain (Box 1).

Since the technology is at an early stage of development, the terminology associated with it is still evolving, and is often inconsistent.[9, 10] Generally, DLT refers to the broad family of technologies, while the term 'blockchain' refers to a specific type of DLT. However, these terms are often used interchangeably. It should also be noted that the terms 'public and private' are frequently used synonymously with 'permissioned and permissionless' when describing the different types of distributed ledger.

Characteristics of DLT

The key characteristics that together distinguish DLT from other types of ledger are: distributed storage, mathematical security, and the use of a consensus mechanism to update the ledger.[7, 9]

Distributed storage

Identical copies of the ledger are stored across multiple computers in different physical locations and are updated simultaneously when a new data entry or transaction occurs. Depending on the type of DLT, the users may not know or trust each other, and are sometimes anonymised.

Mathematical security and verification

The use of cryptography (the encoding and decoding of information, POSTbrief 19) allows information on the database to be verified and securely recorded.[8, 11] Cryptography is also used to apply a timestamp to data entries, ensuring data are recorded in chronological order (Box 2).

Consensus mechanisms

In order for a distributed ledger to be updated, the majority of the other users on the network must verify and approve a transaction or data addition. This is done through a 'consensus mechanism'. A consensus mechanism is needed to prevent the addition of fraudulent transactions and ensure that distributed ledgers are reliable in environments where users may not know or trust each

Box 1. Blockchain

Blockchain is a type of distributed ledger technology, and was developed to create the cryptocurrency Bitcoin. Blockchain is characterised by the particular way that the data is structured within the ledger: new transactions that need to be recorded are grouped together into 'blocks' before being added onto the database.[2, 9, 12] Each of the blocks of data are secured (or chained) to each other by incorporating the hash (Box 2) of the previous block of data in the next block of data, meaning the database cannot be tampered with easily. Depending on the application, the number of transactions recorded in each block can vary. In the Bitcoin ledger, there are around 1000-2000 transactions in each data block. [13]

Cryptocurrency ledgers typically use this block-based organisation of data as it is more efficient than adding each transaction on to the ledger individually. Therefore, many people use the term blockchain as a general term to refer to permissionless DLT. However, there are cryptocurrency ledgers that do not group transactions in this way.

other. These mechanisms vary depending on the type of distributed ledger and are discussed in more detail in Appendix 2.

Box 2.Cryptographic techniques used in DLT

Two cryptographic techniques that are commonly used in DLT are 'hashing' and 'digital signatures'.[9]

Hashing is a process that uses an algorithm to compress a data file into a series of letters and numbers unique to that piece of data. The hash of a data file is often described as its digital 'fingerprint'. In a distributed ledger, hashing is used to verify that data entries are not tampered with; if a data file is changed, its hash will also change, and it will be evident that the data has been modified.

Digital signatures are a type of electronic signature that connect data entries to their creators. These can also be used to ensure that the person who updates the ledger has permission to do so.

Applications of DLT

DLT is most commonly used in cryptocurrencies; however many other applications have been proposed across a wide range of sectors, the majority of which make use of permissioned DLT. Some organisations are carrying out small-scale trials of DLT in order to assess the benefits of the technology for specific applications.

The following section gives an overview of some of the main applications. As the technology matures, other uses may emerge.

Financial services

Banks and financial organisations have become increasingly interested in how DLT can be used in financial operations such as making payments, transferring financial assets (e.g. shares and bonds), and creating smart contracts (Box 3).[14,15] For example, DLT could be used to streamline cross-border payments. Typically, international transfers rely on money passing through a series of commercial banks, which can be time-consuming and expensive. DLT has the potential to reduce the cost and increase the speed of international transfers by allowing banks across the world to transact with each other directly.[16] Furthermore this application of DLT has the potential to reduce fraud and increase transparency by providing an auditable trail of transactions.[8, 17]

Several UK banks, financial organisations and regulators are involved in projects and initiatives that aim to help develop DLT in the finance sector. These initiatives include:

- The Bank of England's FinTech accelerator, which helps banks and other businesses carry out proof-of-concept projects to enhance the UK's productivity in developing DLT.[18]
- The R3 DLT research and development consortium, which brings together finance companies and allows them to collaborate on DLT research

projects. The consortium includes several UK banks and financial firms.[19]

- The Financial Conduct Authority's (FCA) regulatory 'sandbox', which is a programme allowing companies to test new FinTech products and services on a small scale with live consumers in the financial market. Distributed Ledger Technology (DLT) was the most popular technology employed in the first two cohorts of the scheme.[20]

Supply chain management

Supply chains often involve a large network of different organisations, many of which still use paper-based documentation. Data about a product typically needs to be recorded at many different stages along a supply chain, particularly as it passes through different locations and organisations. [21]

DLT provides an infrastructure for registering the trade and transport of physical items by associating them with a digital profile; for example, participants can digitally record information such as the item's origin, appearance, location, price and serial number. Key updates can be added to the database as goods pass through the supply chain.[22] Some stakeholders believe DLT has the potential to reduce the losses that can arise from counterfeit goods or fraud and could also increase trust in supply chains by assuring the provenance of goods[23,24] (for example in the food industry where there have been several high-profile incidents of food fraud).[25]

DLT has already been employed by the company Everledger to track the provenance of diamonds. The Everledger system seeks to record a transparent history of a diamond's ownership in order to reduce the number of counterfeit diamonds in the market and help reduce document tampering.[26]

Government operations

The UK Government is interested in using DLT to improve its processes.[2] There are a number of trials going on in different Government departments, including:

- The Department for Environment, Food and Rural Affairs and IBM initiated a proof-of-concept project in 2017 to explore how DLT could be used for tracing the origin of food, specifically focusing on ensuring the provenance of British beef.[27]
- The Department for Work and Pensions (in collaboration with industry) carried out a proof-of-concept project in 2016 whereby benefits claimants in Tameside used a mobile phone app which recorded transactions on a distributed ledger.[28,29]
- The Department for International Development is exploring the potential of DLT technology to track humanitarian stockpiles.[30]

In Estonia, a government-led digital ID scheme uses features of DLT to provide access to private and public sector services online, such as electronic health records (POSTnote 519), tax declaration and banking.[31]

Energy

DLT has been proposed as a way to help manage the future UK electricity system. Transactions between multiple parties such as power producers, suppliers and consumers could be recorded using DLT. This would facilitate 'peer-to-peer' electricity trading, helping to manage supply and demand at a local level without the need for a central intermediary.[32] DLT could also provide a consistent register for different kinds of assets such as smart meters, network infrastructure and battery storage, which could increase the system's efficiency and reduce costs.[33]

There are several companies worldwide that are trialling DLT in the electricity sector. US company LO3 Energy are running a DLT-enabled peer-to-peer trial in Brooklyn, where up to 50 homes that are connected to a network via smart meters can buy or sell electricity (for example, from rooftop solar panels) to or from each other.[34] UK energy company Centrica have announced the launch of a similar DLT trial in Cornwall.[35]

Box 3. Smart contracts

There is a lack of consensus on the definition of the term 'smart contract'; however, it is commonly used to describe a set of executable instructions written using computer code. Unlike a traditional contract, a smart contract can process information that it receives and carry out tasks automatically (e.g. payments) if certain conditions are met.[36] For example, a smart contract could be programmed to pay a refund if a customer's flight is delayed, or sell a set number of shares when they reach a certain price.

Smart contracts are commonly recorded in the databases of distributed ledgers. This ensures that all the participants in the agreement have identical copies of the contract and allows each member to see when resulting actions have been carried out.[37] In some cases, smart contracts may also be linked with cryptocurrencies, which are used to make payments.

Smart contracts do not have a clear legal status and many experts agree that they cannot be classified as contracts by the legal definition.[37] The unclear legal status of smart contracts has raised questions over who would be liable if there was a problem, such as a flaw in the code leading to financial loss.[38]

Benefits and challenges of DLT

Benefits

There are several advantages that a distributed ledger can have over a traditional centralised system:[3]

- It is very difficult to tamper with the database because all computers on the network agree on its contents and possess a copy of the transaction history.
- It can allow transactions between participants who may not trust each other, without an intermediate authority (such as a bank).
- It is not possible for an individual user to update the ledger: data entries must be validated by the other network participants (see Appendix 2). This can improve transparency between multiple organisations.

- If a database at one location is corrupted or stops working, there are multiple other copies of the ledger in existence, meaning there is no single point of failure (this also applies to some other database types).
- In the finance sector, DLT has the potential to reduce the costs associated with certain transactions.[39]

Challenges

DLT is likely to change significantly as technological advances occur over the next few years. Since the technology is relatively immature, the challenges associated with it are also likely to evolve, and may differ depending on whether the distributed ledger is permissionless or permissioned.[9, 10] The following section gives an overview of some of the main challenges highlighted in this field.

Lack of maturity and understanding

Since DLT is a relatively new technology, there is a lack of clarity on the terminology and a general lack of understanding of what DLT can do. This creates a barrier for organisations that may want to trial DLT.[10] In the majority of sectors, it is currently unclear whether DLT will offer benefits over traditional systems. However, as discussed in the previous section, work is ongoing in several sectors to establish where DLT could be beneficial.

Regulation

There is no UK regulation specific to the use of DLT, and it is unclear whether new regulation will be needed as specific applications of DLT emerge.[40] In 2017, the FCA published a paper to stimulate discussion around the implications of DLT for the financial sector.[41] Based on responses to this paper, the FCA concluded that current regulation is sufficient for companies using or planning to use DLT, and that no regulatory amendments are needed in this sector at the moment.[42]

There are ongoing discussions worldwide about the regulation of cryptocurrencies, cryptocurrency exchanges, cryptocurrency wallets and Initial Coin Offerings (ICOs, Appendix 1). Cryptocurrencies are currently not regulated in the UK (provided they are not part of other regulated products or services). However, the recently published EU 5th Anti-Money Laundering Directive requires that anti-money laundering obligations apply to some cryptocurrency exchanges and wallets. This will require them to be registered in each member state and to take steps to identify and report suspicious activity.[43] Member states have 18 months to transpose the directive into national law. It is unclear how this will be affected in the UK by Brexit.

Most ICOs are not regulated in the UK and many are based overseas. Some ICOs have features similar to Initial Public Offerings (IPOs), private placement of securities, crowdfunding or collective investment schemes. Therefore, depending on how an ICO is set up, some aspects of it may fall under existing regulation. This is determined case by case and depends on the characteristics of the ICO.[44] Concerns have been raised recently after several ICOs and

cryptocurrency exchanges were uncovered as scams, leading to financial loses for investors. This prompted regulators in China and South Korea to ban them completely. The FCA has warned consumers about the risks of investing in ICOs, and is currently investigating whether there is a need for them to be regulated in the UK.[44]

Scalability and speed

Most permissionless DLTs (predominantly cryptocurrency ledgers) face issues with scalability and speed of transactions. These limitations arise from the computationally-intensive consensus mechanism they require. For example, the way the Bitcoin network is set up means it can only process 4–7 transactions per second, whereas Visa is capable of processing up to 56,000 transactions per second.[9, 45] As the number of transactions being carried out on the Bitcoin network increases, an increasing amount of computing power is required to run the ledger and maintain a steady transaction rate (see Appendix 2). It has been estimated that the annual electricity consumption of the Bitcoin network is currently comparable to that of Austria.[46]

Permissioned ledgers are easier to scale and are faster at processing transactions since they do not have the same consensus mechanisms.

Security

DLT, like any software, is vulnerable when weaknesses in software design or implementation are found and exploited by malicious users. In a permissionless network, malicious users could theoretically take control of more than 50% of the computing power in the network to manipulate the consensus of a ledger (known as consensus hijacking). Some distributed ledger networks have been targeted by cyber-attacks such as Distributed Denial of Service (DDoS) attacks, whereby an attacker overwhelms a network with large numbers of spam transactions. This type of attack is unlikely to completely bring down a network, however it can slow it down.[47]

One of the key features of DLT is the storing of information across multiple computers in a network. Some groups have expressed concerns that this is a less secure way of recording information than a centralised database as it provides multiple points through which an attacker could attempt to access the database.[10, 48]

Privacy

One of the key challenges in distributed ledger technology is ensuring certain transactions are kept private and sensitive data are protected. Furthermore, the design of DLT means that it is not possible to change data on the ledger once it has been entered (although it is possible to post an amendment as an additional transaction).

Depending on the type of distributed ledger, data stored on the ledger may qualify as personal data. Distributed ledgers that store personal data are subject to data protection law, including the recently introduced European Union General Data Protection Regulation[49] (GDPR, more information can be

found in the Commons Library Briefing CBP-8214, Data Protection Bill [HL]). It is currently unclear how some permissionless distributed ledger systems will comply with GDPR, since the data are not controlled by one single organisation, but rather by many participants who remain anonymous.[50] Furthermore, GDPR requires companies to erase the personal data of any EU citizen who requests that they do so, which might not be possible for some networks. As a possible solution to this challenge, some groups have suggested that permissionless DLT should not be used for storing personal information.[51, 52]

Implementation and interoperability

To gain maximum benefits from DLT systems, they will need to be compatible with the other computer systems that an organisation has. Additionally, separate DLT systems may need to interact with each other.[53] Replacing existing infrastructure may be costly and would require collaboration between the participating organisations. The exact cost of implementing DLT is currently unknown.)

Appendix 1

Glossary of common cryptocurrency terms

Mining is a process by which users compete to add a set of a valid transactions to a distributed ledger by competing to solve a complex mathematical problem. Miners are only allowed to add a block of transactions to the ledger if they are successful in solving the problem, and cryptocurrency is issued as a reward for doing this.

Mining pools are groups of miners that pool together computing resource to verify and add cryptocurrency transactions to their ledgers. The cryptocurrency reward is split according to the amount of computing power a user contributed.

Cryptocurrency exchanges are businesses which allow customers to exchange cryptocurrencies for other financial assets such as alternative cryptocurrencies or legal tender. Concerns have been raised recently over the security of cryptocurrency exchanges; in 2018, Tokyo-based cryptocurrency exchange Coincheck lost $530 million of cryptocurrency after a breach by hackers.[54]

Cryptocurrency wallets are software programs that are needed in order for cryptocurrency users to send and receive funds, and monitor their cryptocurrency balances. Most cryptocurrency payment systems provide wallets for their users, and many can be accessed through smart-phone apps.[55]

Initial coin offerings (ICOs) are a method of raising funds from the public for start-up projects. ICOs are often used to start new cryptocurrencies. Investors are pre-allocated some of the cryptocurrency before it is established in exchange for other, well-established cryptocurrencies or legal tender. The funds generated are then used to launch the project.[56] ICOs have caused controversy recently as some have been used to commit fraud (see Challenges section).

Appendix 2

Consensus mechanisms

Consensus mechanism design varies depending on whether the ledger is permissioned or permissionless. The types of consensus mechanisms used in permissioned and permissionless systems are described below:

Permissionless consensus mechanisms

When a transaction is initiated, it is broadcast to all the users in the network. The network users check the new transaction against a copy of the ledger to ensure it is valid. This includes checking the sender has sufficient funds to carry out the transaction, and checking the transaction's digital signature. Verified transactions enter a 'pool' of transactions which have not yet been recorded on the ledger.

A user then gathers together a block of transactions from the pool of transactions, and organises them in chronological order before adding them to the ledger. Consensus mechanisms in permissionless ledgers make it resource dependent to add data to the ledger, which deters users from adding fraudulent transactions to the database. The system is designed so that it is more profitable for a user to maintain the ledger than attack it.[57] There are many different ways in which a user can add a group of valid transactions to the ledger. The most common method of doing this known as Proof-of-Work (PoW), which uses a process often referred to as 'mining'.[12]

PoW is deliberately designed to make adding data to the ledger expensive, requiring significant computing power. To update the ledger, users compete to solve a computationally intensive mathematical problem (based on cryptography).[58] The user successful in solving the problem is rewarded by receiving a certain amount of newly generated cryptocurrency, hence this part of the consensus mechanism is referred to as 'mining'.[9] The ability to earn currency provides an incentive for people to provide computing resource and participate in updating the ledger. A disadvantage of this type of consensus mechanism is that it is extremely energy intensive due to the amount of computing power required for it to operate. In order to regulate the rate at which data is added to the ledger, the complexity of the mathematic puzzle that 'miners' need to solve is automatically increased as more transactions are carried out on the network, meaning as the network grows, an increasing amount of computing power is needed to run it.

Other consensus mechanisms have been developed which are less energy-intensive and faster than PoW, however these have not been as widely implemented.[59] An example is the Proof-of-Stake (PoS) mechanism, where users are required to pay a security deposit if they wish to update the ledger.

Permissioned consensus mechanisms

In a permissioned ledger, only pre-approved participants can be part of the network. Generally, the users trust each other to add legitimate data and

transactions to the database, and a financial incentive to maintain the ledger is not required. A variety of consensus mechanisms are possible for permissioned distributed ledgers, and generally these are faster, cheaper and not as resource intensive as permissionless systems. In some cases, an algorithm is used to select a user to add a data entry to the ledger.

Endnotes

1. Greenwich Associates, Blockchain Adoption in Capital Markets – 2018, 2018
2. Government Office for Science, Distributed Ledger Technology: beyond block chain, 2016
3. Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation, Lord Holmes report, 2017
4. House of Commons Treasury Committee, Digital currencies inquiry, 2018
5. HM Treasury, FinTech Sector Strategy, 2018
6. https://epsrc.ukri.org/newsevents/news/distributedledgertechnologytransformenergybanking-healthcare/
7. Bank of England, The economics of distributed ledger technology for securities settlement, 2017
8. ASTRI, Whitepaper On Distributed Ledger Technology, 2016
9. World Bank Group, Distributed ledger Technology (DLT) and Blockchain, 2017
10. British Standards Institution, Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards, 2018
11. Bank for International Settlements, Distributed ledger technology in payment, clearing and settlement, 2017
12. Bank of England, Innovations in payment technologies and the emergence of digital currencies, 2014
13. Blockchain, Average number of transactions per block, accessed 11/06/18
14. IMF, Virtual currencies and beyond: initial considerations, 2016
15. IBM, Banking on blockchain: charting the progress of distributed ledger technology in financial services, 2016
16. R3 Reports, Blockchain KYC/ AML Utilities for International Payments, 2017
17. Deloitte, Blockchain Enigma. Paradox. Opportunity, 2016
18. Bank of England, Bank of England FinTech Accelerator: latest proofs of concept announced; and results so far reviewed, 2017
19. R3, The R3 story, accessed 20/08/18
20. Financial Conduct Authority, Regulatory sandbox lessons learned report, 2017
21. European Parliamentary Research Service, How blockchain technology can change our lives, 2017
22. HICL, Blockchain in Logistics and Supply Chain: Trick or Treat?, 2017
23. Deloitte, Using blockchain to drive supply chain innovation, 2017
24. DHL, Blockchain in logistics, 2018
25. European Parliamentary research service, Fighting Food fraud, 2014.
26. Everledger, Do you know your diamond?, accessed 20/08/18
27. CIO, John Seglias Defra, accessed 11/06/18
28. Public Technology, DWP minister: Government 'carefully considering' wider blockchain benefits trial, accessed 12/06/18
29. Written question to the Department for Work and Pensions by Eddie Hughes MP, 20th February 2018
30. Medium, Blockchain for humanitarian supply chains—project launch!, accessed 14/06/18
31. Guardtime, Our Technology, accessed 11/06/18
32. PwC, Blockchain – an opportunity for energy producers and consumers?, 2016
33. Electron, About Us, accessed 20.08.18
34. Siemens, A Microgrid Grows in Brooklyn, accessed 20/08/18
35. Centrica Business Solutions, Blockchain trial starts at Centrica's Cornwall Local Energy Market, accessed 20/08/18
36. M. Alharby and A. van Moorsel, Blockchain-based smart contracts: a systematic mapping study, 2017
37. Clyde and Co., Smart contracts, blockchain and distributed ledger technologies, 2017
38. R3 and Norton Rose Fulbright White Paper, Can smart contracts be legally binding contracts?, 2017.
39. European Parliament, Distributed ledger technology and financial markets, 2016
40. SWIFT, SWIFT on Distributed ledger Technologies, 2017
41. Financial Conduct Authority, Discussion Paper on Distributed Ledger Technology, 2017
42. Financial Conduct Authority, Distributed Ledger Technology Feedback Statement on Discussion Paper 17/03, 2017
43. Directive (EU) 2018/843 of the European Parliament
44. Financial Conduct Authority, Statement on ICOs, accessed 20/08/18
45. Visa, Visa Inc at a Glance, 2015

46. At time of writing: Digiconomist, Bitcoin Energy Consumption Index, accessed 20/08/18
47. European Union Agency For Network And Information Security, Distributed Ledger Technology & Cybersecurity, 2016
48. Federal Reserve Bank of Chicago, Blockchain and financial market innovation, 2017
49. Regulation (EU) 2016/679
50. Hogan Lovells, A guide to blockchain and data protection, 2017
51. Grant Thornton, GDPR & blockchain, 2017
52. Chainfrog, Blockchain and GDPR, 2017
53. ESMA, Discussion Paper The Distributed Ledger Technology Applied to Securities Markets, 2016
54. Reuters, Coincheck hit by lawsuit as investors seek restart of cryptocurrency withdrawals, accessed 30/08/18
55. Stansberry Churchouse, The Crypto Capital Wallet Guide, 2018
56. Institute of International Finance, Initial Coin Offerings, 2018
57. R. Chitchyan, R. Murkin, Review of Blockchain Technology and its Expectations: Case of the Energy Sector, 2018
58. M. Pilkington, Blockchain Technology: Principles and Applications, 2015
59. S. Bano, et. al., SoK: Consensus in the Age of Blockchain, 2017