EPS PEAKS Our Expertise. Your Knowledge.

ECONOMIC AND PRIVATE SECTOR

PROFESSIONAL EVIDENCE AND APPLIED KNOWLEDGE SERVICES

HELPDESK REQUEST

Application of Distributed Ledger Technology within Department for International Development

Dr Catherine Mulligan

Imperial College Centre for Cryptocurrency Research and Engineering

October 2016

coffey international development · ODI · University of Birmingham · Nathan · LSE Enterprise · Oxford Policy Management

EPS-PEAKS is a consortium of organisations that provides Economics and Private Sector Professional Evidence and Applied Knowledge Services to the DfID. The core services include:

1) Helpdesk
2) Document library
3) Information on training and e-learning opportunities
4) Topic guides
5) Structured professional development sessions
6) E-Bulletin

To find out more or access EPS-PEAKS services or feedback on this or other output, visit the EPS-PEAKS community on http://partnerplatform.org/eps-peaks or contact Alberto Lemma, Knowledge Manager, EPS-PEAKS core services at a.lemma@odi.org.uk.

Contents

Abbreviations

3rd Party	Third Party
AMLD	Anti Money Laundering Directives
DFID	Department for International Development
DL	Distributed Ledger
DLT	Distributed Ledger Technology
EU	European Union
H&M	Hennes and Mauritz
ICT	Information and Communication Technology
ID	Identity
JiTM	Just in Time Management
LEGEND	Land: Enhancing Governance for Economic Development'
MB	Megabyte
PoC	Proof of Concept
PSD	Payment Services Directive
QR Code	Quick Response Code
R3 or R3CEV	Consortia for banking organisations investigating the use of blockchain
UK	United Kingdom

Executive summary

This report was commissioned DFID to investigate the possible roles that Distributed Ledger Technology (DLT) within the remit of its operations.

DLT will undoubtedly assist in many areas of DFID's operations, but needs to be carefully assessed due to the complex and sensitive nature of many of the areas that DFID works. DLT are not, for example, a panacea for fixing corruption but do provide significant opportunities for the creation of just and fair governance structures within different nations, including providing better humanitarian response and also the opportunity for economic growth and sustainable job creation.

The report outlines the potential for DLT within a 5-10 year time frame, focusing on both technical and institutional barriers that need to be overcome in order to successfully deliver the promise of greater transparency, dramatically reduced costs of operations as well as the better tracking and accountability within the management systems themselves. The report discusses three main areas of applications, those with:

1. A **strong probability** of technical and institutional success, namely: **Identity Management** for Education and Healthcare and **Data Sharing** for Land management, International Aid and Disaster Response;
2. A **medium probability** of technical and institutional success, namely: **Identity Management** for Births, Marriages and Deaths and **Supply Chain Transparency** for both global and micro supply chains;
3. A **weak probability** of technical and institutional success, namely **Smart Contract**s for managing aid payments and the use of **cryptocurrencies** for large-scale aid payments.

On the whole, DLT have an extremely promising role to play within DFID's remit of operations. As with any new technology, however, there is the potential for unintended consequences due to its introduction. As a result, it is recommended that DFID take a staggered approach to the implementation of DLT in order to fully understand the technical, regulatory and institutional issues associated with applying DLT within the scope of the 28 countries that it is active within. Ideally, this would involve the development of some proofs of concept, followed by small-scale trials that run alongside existing systems and finally a staged transition to a full DLT solution.

1 Introduction

Blockchain and Distributed Ledger Technology (DLT) have gained increasing attention recently due to their potential to disrupt traditional business processes[1,2,3]. The technology has now moved far beyond its origins in Bitcoin[4] and multiple commercial organisations, industrial bodies and governments are now investigating how to apply these technologies to not just reduce costs but also to remove friction from internal and external markets.

This document outlines the role that Distributed Ledger Technology (DLT) and blockchain technology may play within the Department for International Development (DFID) scope of activities to end extreme poverty. Specifically, it investigates the role of DLT in creating jobs, increasing transparency and in humanitarian emergencies, including aid payments and disaster response. A key aspect of this document is to carefully approach this new technology cognizant of the sensitivity of the domain and its importance to saving lives and livelihoods. Many new technologies, whilst holding great promise can have many potential unintended consequences – both positive and negative. The report therefore outlines an approach that enables the use of the best parts of the current state of the art of DLT whilst providing a balanced approach to the potential risks.

[1] M. Swan, 2015, “Blockchain: Blueprint for a New Economy”.

[2] The Economist, “The trust machine: The technology behind bitcoin could transform how the economy works”, available online at http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine/, October 2015.

[3] C. Skinner, ValueWeb, 2016, “How FinTech Firms Are Using Mobile and Blockchain Technologies to Create the Internet of Value”.

[4] S. Nakamoto, 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System”, available online at https://bitcoin.org/bitcoin.pdf/.

2 Landscape of DLT applications

The current landscape of blockchain and distributed ledgers is extremely diverse and it seems each day a new application for the technology emerges. From decentralizing asset ownership and management to providing "smart" contracts and low-friction global remittances, there are a multitude of areas that DLT can be applied within. This broad range of solutions is illustrated in Figure 1 below:

Figure 1: Global DLT landscape

Source: Imperial College Centre for Cryptocurrency Research and Engineering.

There are multiple different types of distributed ledgers (DL) however ranging from ones with heavy computational and energy requirements to those which can be run on lightweight devices such as mobile phones or raspberry Pis[5]. In this section, we provide a very brief overview of the different types of DL and illustrate the main differences between them with a view to understanding how they can be applied in later sections of the document. This does not provide a detailed overview of the cryptographic techniques used to create DL; instead it provides references for interested readers.

2.1 Cryptocurrencies

"A cryptocurrency is a form of virtual currency that uses cryptography to verify that any person who attempts to spend some of the currency is the person entitled to do so" [6]. This prevents the "double-spend" problem traditional associated with digital money – namely the ability of a person to spend the same digital token twice. In order to achieve this, cryptocurrencies use a decentralised peer-to-peer network to verify transactions and to record them on a decentralised public ledger. Bitcoin, a virtual currency introduced in 2008 that is both decentralised and transparent, has dominated discussions around cryptocurrency as well as its associated distributed ledger – blockchain. This is only one in a number of virtual currencies, however, and it is computationally expensive. The creation of blockchain and associated distributed ledgers, however, holds powerful opportunities to develop applications far beyond the currency space.

[5] https://slock.it/

[6] Norton, Rose & Fulbright, 2016, "Deciphering Cryptocurrencies: A Global Legal and Regulatory Guide".

2.2 Distributed ledgers

From the simplest perspective, a distributed ledger allows untrusting parties with common interests to co-create a permanent, unchangeable and transparent record of exchange and processing. Nodes in the network providing a resilient and secure method of storing transactions verify all transactions within a DL.

The degree to which a high-throughput low-cost solution can be realised in the context of any given use case depends primarily on the openness of the system in terms of who is permitted to submit, validate and process transactions.

2.2.1 Permissionless and permissioned DLT

Within the popular media, the prototypical system used to explain DLT is the Bitcoin network. It is important to appreciate that Bitcoin and its associated **permissionless distributed ledger** - the Bitcoin blockchain - are not representative of all possible types of DLT, nor are they suitable for many DLT applications. Indeed, most commercial-grade applications are being built without using the Bitcoin blockchain. Because of its unique design goals of operating in a completely open environment without any points of centralised trust, and in which potentially malicious actors are not only allowed to submit transactions but also participate in transaction validation, Bitcoin's blockchain adds an extra component known as *proof-of-work*. This approach is computationally expensive[7], uses a significant amount of electricity, does not scale well and requires a large number of network participants in order to be able to generate the `trust' required to ensure the network works effectively. For further technical details on Bitcoin protocols readers are referred to[8] and for further discussion of the scalability limitations of the Bitcoin network, readers are referred to[9].

Permissioned DLTs, however, are based on a set of trusted transactions processors and validators who are also the only parties allowed to take part in the consensus mechanism. They are distributed in a precisely controlled fashion and can be equally robust in rejecting unauthorised transactions or changes, so corrupting the ledger is extremely difficult. More importantly, in comparison to permissionless systems like Bitcoin, they require substantially less computational capacity and energy to run. Private DLTs restrict the participants who can submit transactions and access blockchain data to an explicit whitelist of identified participants. This is suitable for regulated environments and contrasts with the public pseudonymous nature of the Bitcoin blockchain.

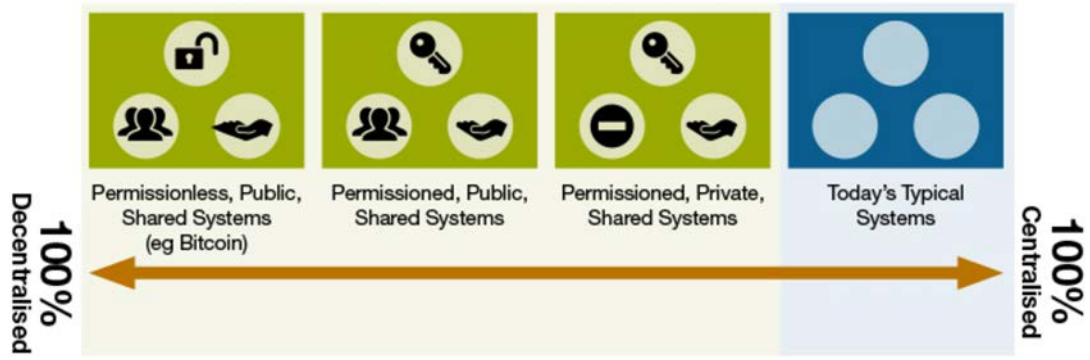
There are a wide range of DLT available to be used within different applications. Figure 2 illustrates the different types of DLT, with traditional databases on the far right hand side and the bitcoin blockchain-style solutions on the left. In the middle are the permissioned solutions – which can be either publicly available or have access controls placed on them, so only those selected are able to register transactions onto the ledger:

Figure 2: Types of DLT

[7] In computer science, the analysis of algorithms is the determination of the amount of resources (such as time and storage) necessary to execute them. For the purposes of this report, computationally expensive means that you need a large amount of both processor time and storage in order to be able to execute a transaction.

[8] A. M. Antonopoulos, 2014, “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”.

[9] T. McConaghy et al, 2016, “BigchainDB: a Scalable Blockchain Database, Whitepaper”, available online at https: //www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf/.



Source: Richard Brown.

2.2.2 Origins of distributed ledgers – databases

Today's typical system is a database, which is a computer system that provides a digital record of the current status of different accounts. Transactions are used to update the state of a transaction. These systems have gone through various incarnations since their introduction in the 1960s, including distribution and replication in order to increase their reliability and availability. Databases, however, are generally implemented within an enterprise or organisational boundary – so they do not allow for the sharing of data between companies or organisations quickly or effectively. Also, they provide only a snapshot of the current status of accounts or data, rather than providing a history of the transactions over time.

Databases do not protect data from censorship, malicious updates or fraud. In addition, they provide a single point of trust in the system. In order to overcome these issues, we can use a distributed ledger built on consensus protocols in order to provide transparency, protection from fraud and ease of data sharing between and across organisational boundaries.

2.2.2.1 Consensus protocols

Consensus protocols provide means by which every participant on a network reaches agreement about the state of the data stored on the distributed ledger. Every party shares updates and verifies the transactions occurring on the network and as a result, the necessity to trust third parties is removed. The easiest way to understand this concept is through the example of Bitcoin.

Traditionally, trust in banking has been created through the use of a central authority – a central bank in each nation – that through a variety of mechanisms are able to provide "trust" in that nation's currency. Bitcoin, through its distributed ledger blockchain removes the requirement for the central bank to create trust in the currency and instead creates trust through a counter-intuitive mechanism – by sharing every transaction with every participant on the network. The consensus protocol used in Bitcoin allows all the nodes to agree on the current state of the 'blockchain' – through ultra-transparency, trust is created and a third party is not required to do so.

2.2.3 Spectrum of distributed ledgers

We now turn to the different types of distributed ledgers and provide some examples of their implementation. Types of DL can be split up from the perspective of:

1. Who can participate as a transaction processor and verification of transactions, and who can submit transactions to the DL (Permissioned or Permissionless),

2. Whether the ledger is available for public inspection or not (Private or Public)

Working from left to right in Figure 2, we can see three main archetypes of distributed ledger that are emerging[10].

Type of DLT	Description	Example Application	Companies / Organisations
Permissionless, Public and Shared	• Everyone can participate as a transaction processor and verifier of transactions; • Anyone can submit transactions; • The Ledger is publicly available for inspection	Cryptocurrencies, distributed applications (e.g. smart contracts)	Ethereum, Bitcoin, altcoins
Permissioned, Public and Shared	• Transaction processors and verifiers are white listed; • Only those on the list can submit transactions; • The Ledger is publicly available for inspection	Cross supply chain, Land Registries	Provenance.org
Permissioned, Private and Shared	• Transaction processors and verifiers are white listed; • Only those on the list can submit transactions; • The Ledger is not publicly available for inspection	Internal Supply Chain management, Financial Remediation	Eris, Multi-chain, R3, Everledger

2.2.4 Beyond blockchains – smart contracts

Far beyond registering transactions onto a blockchain in a transparent manner, new initiatives are emerging that enable automated 'contract'[11] processes. In traditional enterprise architectures code is run in isolated silos with its own servers making sharing of data extremely difficult. Using a distributed ledger, the nodes on the network replicate any data for all nodes to reach an agreement. Possibly the most commonly known example of this type of service is Ethereum - which is a "decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference" [12]. Smart contracts enable application developers to perform the following without third party involvement:

1. Create markets;
2. Store registries of debts or promises;
3. Move funds in accordance with instructions given long in the past (like a will or a futures contract).

Such contracts can be established between multiple parties without requiring third-party involvement (such as a bank), and can deliver gains in efficiency – by lowering transaction costs – and in security – by introducing cryptographic principles.[13] An illustration of how smart contracts work has been created by Richard Brown and is shown below in Figure 3:

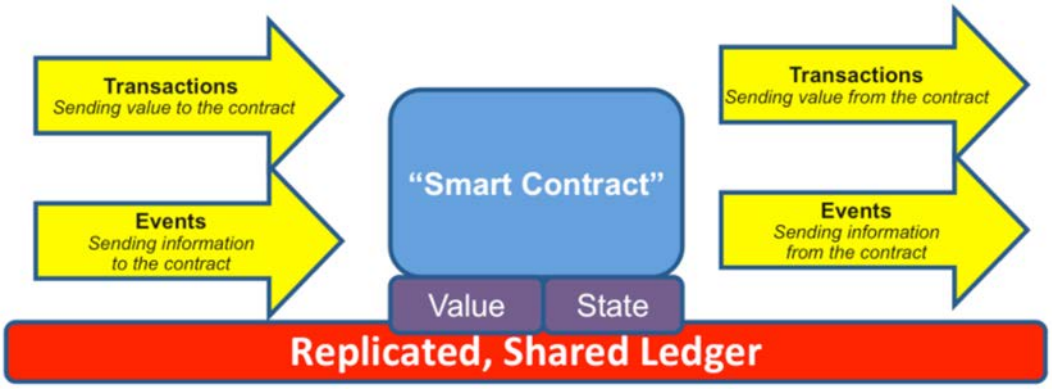
[10] The terms are currently in flux within the industry, but for these are the three main types of DLT as commonly agreed and used today.

[11] While in the common vernacular, this is referred to as a "smart contract", it may be more properly referred to as a distributed application environment rather than a contract *per se*.

[12] Ethereum.org

[13] https://ge2p2center.files.wordpress.com/2014/09/the-sentinel_-week-ending-18-july-2015.pdf/

Figure 3: Smart contracts



Source: Richard Brown

Smart contracts are therefore best viewed as aiming to provide security and algorithms for enacting distributed applications. It is unlikely that they will replace contract law – rather they will reduce the transaction costs of implementing the monitoring of contracts and execution of contracts.

It should be noted that smart contracts are in a very early stage of development. The use of Turing complete languages raises issues of stability – how should a non-deterministic real-world be captured by the technology deterministic approaches that are currently used within smart contracts? For these reasons, smart contracts are really still within the realm of the research community, rather than ready for fully-fledged pilots and trials.

2.3 Deciding when to use different types of DLT

It should be noted that despite the hype surrounding the use and application of Distributed Ledgers, the technology is not suited to every type of scenario. As with all new technologies, DLT are being proposed to solve all manner of issues – some may end up being better served by other solutions – for example, sometimes a normal database will be enough to ensure successful delivery.

Undoubtedly, there are a number of situations where distributed ledgers should not be applied. This section covers these issues from a technical perspective only. Section x.x covers other aspects of distributed ledger issues including non-technical risks.

By design, no one party can modify, delete or even append any record without consensus across the DL network in question; this makes DLs useful for ensuring the immutability of transactions. A key issue, however, is that **DLT should NOT be used to store any type of personal information** – it can be used to create a form of index that points to the information in question, but due to the immutability of the ledger, anything personal should not be stored on DL.

DL Networks also allow each participating organization in a network to create customized applications and solutions on top of the DL – this allows for a relatively cheap common base blockchain solution that can be used for innovative applications across a variety of organisations and companies.

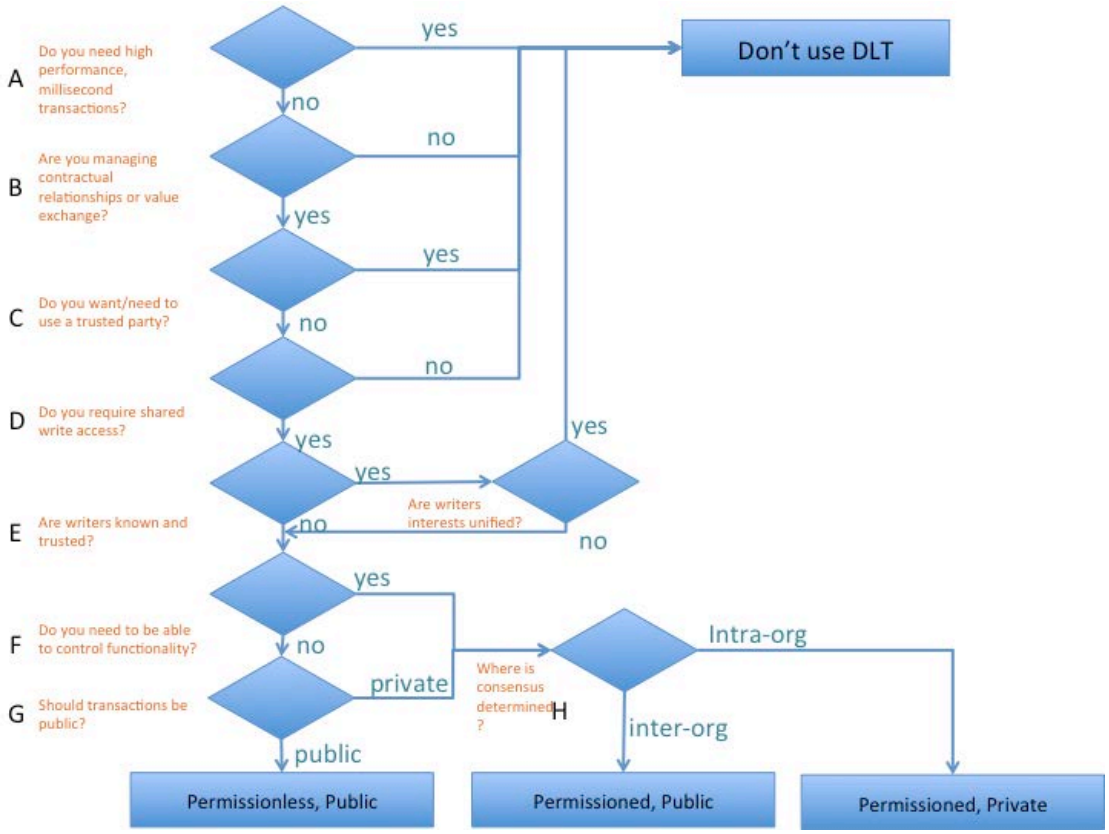
In contrast to traditional database solutions, DLs create some broader issues around the area of consensus – within some solutions; it is necessary for everyone to agree to move towards a shared system. Today, most companies run their own version of a database – while this is inefficient and comes with higher transaction costs when companies need to work together, companies are able to retain control over their data and transactions; these can often represent competitive advantage to many companies. As a result, one of the most difficult and complex aspects of implementing DLT may be ensuring that all parties

are willing to work together to achieve consensus about how the system should be implemented in the first place.

In Figure 4 and the next page, we briefly outline a flowchart to decide:

1. When to use a distributed ledger;
2. If a distributed ledger can be used, which type should be used.

Figure 4: When to use a distributed ledger



A. **Do you need high performance, millisecond transactions?** Current distributed ledgers do not have high performance capacity and cannot process transactions at a millisecond level. If this type of performance is required, it is not currently suggested to use a DL.

B. **Are you managing contractual relationships or value exchange?** DLs work extremely well where there is a contractual relationship that needs to be managed (e.g. remittances in the banking industry) or where there is another type of value exchange. If the solutions are about managing these types of relationships, it will likely lend itself well to a DL.

C. **Do you want/need to use a trusted party?** If a trusted 3rd party is wanted or required in a solution, the use of a DL will need more investigation in order to understand why it would be needed[14].

[14] There are some well-known exceptions to this rule where having a trusted third party does not preclude the use of DLT. These examples include Everledger or Provenance.org who are using trusted third parties to certify the registration of physical objects onto a DL – namely diamonds and sustainably sourced fish. These types of solutions may fall into permissioned, public or permissioned private DLT. For those solutions where a physical object needs to be 'proven', a DLT may be used.

D. **Do you require shared write access?** Does the solution require that the organizations sharing the ledger need to all be able to write to it? If only one or two organisations need to write access, there may be more effective ways to share the data with the others (e.g. a traditional database).

E. **Are writers known and trusted?** If the writers are known and trusted, another sub question needs to be analysed;

    a. **Are the writers interests unified?** If the interests are unified, there is little need for the use of a DLT – other means will probably serve equally well. If, however, the interests are not unified, a Distributed Ledger will act well in order to ensure that the solution is running for the overall benefit of the entire community[15].

F. **Do you need to be able to control functionality?** If a solution needs to retain strict control over who can create new applications or implement business logic on top of the DL, it is advised to use a private ledger, rather than a public one. If a private one is selected, there in one final aspect remaining to be assessed in point H.

G. **Should transactions be public or private?** Finally, if transactions are able to be public, then a permissionless, public ledger should be used. If the transactions should be private, then one final aspect needs to be assessed in point H.

Where does consensus need to be determined? is the final remaining issue. If consensus is achieved between organisations, then a permissioned, public ledger is appropriate. If the consensus is achieved within an organization, then a permissioned, private ledger is appropriate.

2.4 Risks associated with distributed ledgers

As with any new technology, it is important to not just understand the benefits of Distributed Ledgers, but also to understand them within the context of the risks they bring and indeed the new type of risk *landscape* they bring to the table. This section briefly outlines the nature of the risks associated with distributed ledgers.

- It is an extremely new technology and smart contracts in particular have not yet been deployed on a large-scale in the real-world. The secondary and tertiary effects of distributed ledgers are not yet well-studied or well-understood.
- Technical robustness needs to be improved from the perspective of scalability – if many solutions start to use the blockchain network – it may be unable to cope with the levels of demand.
- Denial of service attacks – the spam attacks that we have seen in Bitcoin are really the tip of the iceberg and it is unlikely that various actors would not be interested in seeing how to attack and compromise such systems in an increasingly digitalised world.
- While today's cryptography is relatively secure from hacking attempts, there is no guarantee that this will remain that way in the future. If you put information onto the blockchain and the cryptography is compromised at some point in the future, that information becomes publicly available with no current mechanism to ensure that it is possible to be deleted.
- Information can be used nefariously if private keys are stolen or coerced from people.
- There is also an issue if people lose their private keys – they have suddenly lost the right to prove their right to their property and their right to access services

[15] It should be noted that there are many scenarios where writers' aims might be aligned (e.g. delivery of aid) but their interests may not be aligned (split of funds, speed of invoice payment). In this case, a DL will help to align interests through reduced transaction costs, reduced remittance payment times and greater transparency across the chain.

that are based on these technologies. Secure and reliable methods to retrieve and change private keys need to be developed.

- Like any system that holds potentially valuable information, people will try and deceive it. This is particularly important in areas where information about people is being stored – for example, in refugee situations, people could use it to try and track down where refugees have gone – this information can be used both for good and bad purposes.
- Immutability of data is not always compatible with human fallibility. Mechanisms are not yet in place and need to be developed in order to address errors and other special circumstances. How does the right to be forgotten align with the DL ethos?
- There is a strong issue around the contagion of risk in a new era with Bitcoin, Blockchain and Smart contracts. In today's world, it takes some time for crises to work their way through the economic system – this delay provides a level of control over the economic system that would not be available if everything moves to distributed ledgers. For example, there could be problems created by instantaneous settlements that are combined with smart contracts that have unforeseen behaviour. The technical community does not yet understand how to verify programme behaviour, especially in the context of distributed applications. Since smart contracts are effectively neither smart nor contracts, but in a fact a new form of distributed application, this can have repercussions that are as yet not understood.
- Again for smart contracts, there is a potential mismatch between the non-deterministic nature of the real world and the deterministic nature of a Turing complete language in the smart contract arena. It implies that some contracts may never get "paid out" – or executed – due to either poor code or deliberately miscoded 'contracts'.

3 Recent initiatives related to DLT

Distributed Ledger Technology and cryptocurrencies have caught the attention of many companies and governments who are now actively researching, building and piloting a broad range of DLT solutions. The tables below highlight some of these initiatives in order to illustrate that is has now moved beyond its 'cryptoanarchy' roots.

3.1 Selected national-level DLT-related initiatives

Date	Country	Initiative	Description
Feb 2015	UK	Digital Currency	The Bank of England highlights the development of a national digital currency as part of its research agenda[16]
Jan 2016	China	Digital Currency	People's Bank of China announces intention to develop and issue a state-backed national digital currency "as soon as possible"[17]
Mar 2016	Netherlands	Digital Currency	Dutch Central Bank declares an intention to develop a "concrete prototype DNBCoin based on blockchain technology"[18]
Mar 2016	Estonia	Medical Records	Estonia announces intention to secure medical records using blockchain technology[19]

[16] Bank of England, "One Bank Research Agenda": http://www.bankofengland.co.uk/research/documents/onebank/discussion.pdf/, February 2015.

[17] S. Das, "China's central bank will look to issue its own digital currency as soon as possible", available online at https://www.cryptocoinsnews.com/china-digital-currency/, January 2016.

[18] De Nederlandsche Bank, "Jaarverslag 2015", available online at http://www.dnb.nl/binaries/Jaarverslag%202015_tcm46-339389.pdf/, March 2016.

[19] I. Allison, "Guardtime secures over a million Estonian healthcare records on the blockchain", available online at http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367/, March 2016.

3.2 Selected industry-level DLT-related initiatives

Date	Organisation	Initiative	Description
May 2015	Nasdaq	Enterprise-wide blockchain initiative	Nasdaq announces its intention to leverage blockchain technology across its enterprise, beginning with Nasdaq Private Markets[20]
Dec 2015	Nasdaq/Chain.com	DLT for trading shares in private companies	Chain.com uses Nasdaq's blockchain-based Linq platform to "successfully complete and record a private securities transaction"[21]
Dec 2015	Kynetix	Commodity trading with DLT	Kynetix announces it has successfully transferred title to a single lot of pepper using a blockchain-enabled platform[22].
Jan 2016	JP Morgan	Loan trading with DLT	JP Morgan works with Digital Asset Holdings to apply blockchain technology "to address liquidity matches in its loan funds[23]."
Mar 2016	R3 consortium	Fixed Income Asset Trading with DLT	R3 consortium of 40+ financial institutions completes trials of private DLTs built by Chain, Eris Industries, Ethereum, IBM and Intel for trading of fixed income assets[24]

[20] Nasdaq, "Nasdaq launches enterprise-wide blockchain technology initiative", press release; available at http: //ir.nasdaq.com/releasedetail.cfm?releaseid=912196/, May 2015.

[21] Nasdaq, "Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology", press release; available at http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326/, December 2015.

[22] Kynetix, "Kynetix announce commodity title transfer on blockchain using Sen-Tinel:, press release; available at http://www.kynetix.com/wp-content/uploads/2015/12/; and Kynetix-announce-commodity-title-transfer-on-blockchain-using-Sentinel-1Dec2015.pdf/, December 2015.

[23] S. Das, "JPMorgan begins blockchain trials", available online at https://www.cryptocoinsnews.com/ jpmorgan-begins-blockchain-trials/, February 2016.

[24] I. Allison, "R3 completes trial of five cloud-based blockchain technologies with 40 banks", available online at http://www.ibtimes.co.uk/r3-completes-trial-five-cloud-based-blockchain-technologies-40-banks-1547260/, March 2016.

4 Humanitarian response

'Given the heavy strains on the humanitarian system, there is an urgent need to invest more in making sure that the system as a whole works better to meet current and future humanitarian needs'
Humanitarian Response Index 2008

The world is currently facing a humanitarian capacities challenge as we move into an era of increasing economic, environmental and even social/geopolitical uncertainty. There is a high likelihood that the number and nature of crises that DFID need to respond to will rise in the face of the increasing potential for [i] systems collapse, [ii] simultaneous crises and [iii] sequential crises[25]. The interactive nature of the world's economic and environmental systems will require investigating new means by which to approach humanitarian crises and the institutional structures that are used to respond to them. The use of DLT may assist in some areas; in particular, those that require a new approach to delivering aid, increasing transparency and developing local capacity[26]. This sections outlines these principles from two perspectives:

1. International Aid Payments;
2. Disaster Response.

4.1 International aid payments

One of the most commonly mentioned use cases for cryptocurrencies in international aid is for delivering payments directly to those that need them, bypassing middlemen and often even the recipient governments themselves where corruption is an issue. The use of cryptocurrencies for large-scale aid payments – while initially attractive – may prove a difficult option to execute in reality. **Firstly**, the global regulatory environment for cryptocurrencies in extremely uncertain and it is not necessarily the case that recipient nations will have a favourable view of such currencies, even in the case of aid. We cover the current regulatory environment in more detail in the next section. **Secondly**, it necessitates some form of exchanges to be available locally so that recipients are able to use it effectively to pay for goods/services – this is not a simple infrastructure to set up and requires the creation of an exchange rate. For example, would such a cryptocurrency have the same value in every nation, or every aid situation? The alternative to establishing exchanges in every country is that a local economy would emerge based around the cryptocurrency concurrently to the local currency, but this may lead to the creation of a black market for the cryptocurrency, negating any real benefits. **Thirdly**, if cryptocurrencies were used within aid scenarios, it would still require institutions that are able to execute on the aims of the aid in the first place, ensuring the delivery of the expected results. Cryptocurrencies, therefore, do not negate the necessity of well-established and functioning institutions within a nation – ironically a cryptocurrency works best in nations with well-established central banks exactly because there are other institutions in place. **Fourthly**, as much as possible, any international aid should be delivered with respect for the sovereignty of the affected governments in order to allow them to rebuild effectively. For these reasons, we think the use of cryptocurrencies for delivery of aid payments would have to be implemented as part of a long-term strategy and involve building of institutions, rather than providing a panacea for corruption.

[25] Kent, Armstrong, & Obrecht, "The Future of Non-Governmental Organisations in the Humanitarian Sector: Global Transformations and Their Consequences, Humanitarian Futures Programme Discussion Paper for the Start Network".
[26] Ibid.

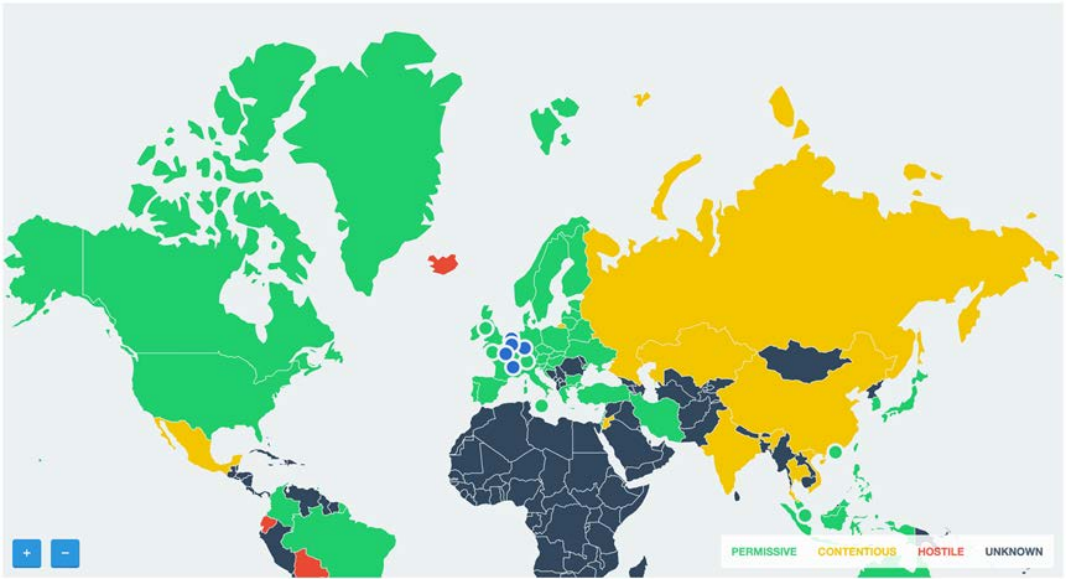
4.1.1 Regulatory environment for cryptocurrencies

A key issue in delivering aid payments via a cryptocurrency is that there is actually no universal legal definition of either “currency" or even “money". This means that the global regulatory environment for cryptocurrencies is varied across the globe and in many cases is still being reviewed. In South Africa, for example, as crypto- and digital currencies are not considered to be `legal tender' (only the government can issue legal tender) these types of transactions do not fall within the jurisdiction of their Financial Surveillance Department[27]. In the UK, meanwhile, a digital currency has no legal status and it does not have the same protection or regulation as the pound sterling. The United States has taken another perspective - that digital and virtual currencies are treated as commodities, rather than currency. This means that cryptocurrencies are under the jurisdiction of the Commodity Futures Trading Commission whose authority extends to futures and swaps contracts in any commodity[28].

The EU, meanwhile, have no regulation regarding cryptocurrencies, but have recently announced an initiative to investigate some areas of regulation (esp. around exchanges) to ensure that they are not able to be used for funding terrorism: “As a first step the Commission will propose to bring anonymous currency exchanges under the control of competent authorities by extending the scope of the AMLD to include virtual currency exchange platforms and have them supervised under Anti-Money Laundering/ countering terrorist financing legislation at national level. In addition, applying the licensing and supervision rules of the Payment Services Directive (PSD) to virtual currency exchange platforms would promote a better control and understanding of the market. The Commission will also examine whether to include virtual currency wallet providers[29].

The map in Figure 5 below illustrates the broad range of regulatory ‘positions' across the world with respect to Bitcoin. As will be noted, many of the 28 countries within which DFID is operational, the regulatory status of cryptocurrencies is unknown or contentious.

Figure 5: Global overview of Bitcoin regulatory landscape



[27] South African Reserve Bank, “User alert: monitoring of virtual currencies”, http://www.treasury.gov.za/comm_media/press/2014/2014091801%20-%20User%20Alert%20Virtual%20currencies.pdf/.

[28] Bloomberg, “Bitcoin is socially a commodity, according to U.S. regulator: The Commodity Futures Trading Commission makes its mark”, http://www.bloomberg.com/news/articles/2015-09-17/bitcoin-is-officially-a-commodity-according-to-u-s-regulator.

[29] EU Commission, Communication from the Commission to the European Parliament and the Council: On an Action Plan for Strengthening the Fight against Terrorist Financing, http://ec.europa.eu/justice/criminal/files/com_2016_50_en.pdf/.

4.2 Disaster response

The increasing occurrences of natural and man-made disasters require a transformative approach to disaster response. The growing frequency, unpredictability and complexity[30] of emergencies means that centralized operations are inefficient and ineffective tools for disaster response. Much research in the space calls for a significant increase in local capacity in order to be able to handle issues locally. On the other hand, completely decentralized operations are unwieldy and lack the scale of activities required in order to respond to disasters appropriately. DLT may provide some mechanisms through which DFID can achieve a balance of local, regional and global activities in order to respond to the increasing requirements for disaster response.

DLT can help provide a number of simplifications to the management and tracking systems that are currently barriers to ensuring local capacity is available and able to respond appropriately when required. Moreover, it builds resilience into and between the local and global actions, allowing for a more agile approach to disaster response that is appropriate across a range of cultural and geopolitical contexts.

Many of the current management practices within the disaster response industry are based on traditional industrial structure, with narrowly defined products and 'markets'[31]. As with many other industries, economies of scale and scope have been applied in order to achieve efficiencies, however, emerging digital technologies mean that these traditional delivery models may no longer be the most effective and are potentially ripe for 'digital disruption'.

Within disaster response, for example, a number of issues create delays in payment across the 'chain' of actors. These management/overhead and coordination costs can be overly burdensome in some cases, in particular where there is a consortium of actors working together who do not necessarily trust one another or cannot share data easily between one another, creating lag times in delivery response to those who need it. DLT can in these cases, assist in reducing the management overheads and therefore reduce the complexity of many actors working together in response to an emergency. Through applying DLT effectively, it is possible to develop approaches that provide the gains from partnership with an equivalent or lower unit cost than traditional centralized approaches. In fact, DLT can be used to create distribution that works on a global scale.

4.3 Use of distributed ledgers in humanitarian response

One of the main ways that DLT can be applied in humanitarian response is assisting in the creation of distributed capacity connected together at global scale – through capturing and providing an immutable record of the activities and transactions that have occurred within a particular programme or response area. These scenarios, however, mainly relate to private permissioned DLT, rather than permissionless cryptocurrencies per se. This section outlines a few areas where DLT may be used to create a more effective internal structure for managing the aid system and its responses in various scenarios, rather than creating a new currency. We focus on the following areas:

- Increasing the speed of remittances between aid organisations;
- Transparency of payments and traceability of how the aid is being used;
- Tracking and tracing of activities for better targeted response;

[30] http://www.start-network.org/news/leveraging-blockchain-technology-improve-financial-mechanisms-humanitarian-sector/#.Vv1YbHAkcnN/

[31] Wallace, Bornstein and Chapman, 2007, "The Aid Chain: Coercion and Commitment in Development NGOs".

- Creating new organisational structures that balance global organisations with local capacity;
- Empowering local citizens.

4.3.1 Increasing the speed of remittances between aid organisations

Through the implementation of a private, permissioned DLT, the remittances between organisations across the chain of actors can be increased dramatically by enabling much faster transfer times. This will enable actors at the local level to received funding immediately, rather than needing to wait for a series of transactions to occur between organisations' banks. This can help overcome the perceived lack of responsiveness in disaster relief situations. This private ledger would be available only to the participating organisations, rather than being publicly available for everyone to read.

4.3.2 Transparency of payments and traceability of how payments are being used

DLT can also be useful in creating transparency in how aid money is being applied and used. A DLT can be implemented that tracks the flow of money across a broad range of actors – who may not necessarily trust one another or be able to easily share data between one another due to legacy systems. The use of a DLT has the added benefit that it does not need to replace the legacy systems themselves, but can be used as an added extra.

4.3.3 Tracking and tracing of activities

A key area that DLT can help reduce the management burden of humanitarian assistance is in the monitoring and the testing of prevention and preparedness mechanisms. It can also help to reduce the management burden of tracking and tracing metrics that need to be reported back to a centralized authority, freeing local actors up to focus more on capacity building and the development of a sustainable processes and mechanisms for prevention.

4.3.4 Creating new organisational structures

As the number and severity of humanitarian crises increases, DLT can help create dynamic networks that form and dissolve as and when required through providing a rapid mechanism to identify which actors, organisations and government agencies are responding and in what manner. This can enable a new type of organizational structure for disaster response – one that is able to create mission-focused networks, characterised by defined, time-bound objectives and peer-to-peer interaction between the consortia. A key aspect of such DLT will be to empower both local citizens and the diasporas to provide verified and immutable information about the real situation on the ground. Such DLT solutions can help to better target activities by being able to trace and provide more granular information about the results of different actions.

5 Creating sustainable jobs and economic growth

> Firms operating in the informal economy are often small and face barriers to growth, preventing them from offering high-quality goods and services … Addressing informality is, therefore, not only a matter of concern in terms of social equity. It also helps to improve a country's dynamic efficiency
> **WTO, 2009**

DLT can be used to create new forms of innovation within markets – opening up data to be shared in a trusted and controlled fashion via a DLT will create new forms of 'data markets'. These data markets will allow companies, individuals and other actors to share and monetise data in new ways. For example, many end-users of health and fitness wearables could store their data in a DLT and permit for it to be shared with different economic actors in exchange for monetary or other forms of value, e.g. insurance companies in exchange for reduced insurance premiums.

Within the scope of DFID's activities, however, there are simpler means to apply DLT compared to the "data value chain" approach that will help create sustainable jobs and more equitable distribution of wealth across nations and the globe. Properly implemented, DLT will provide some of the mechanisms required to overcome extreme poverty. While, there are many applications, in the next section we focus on three main ones:

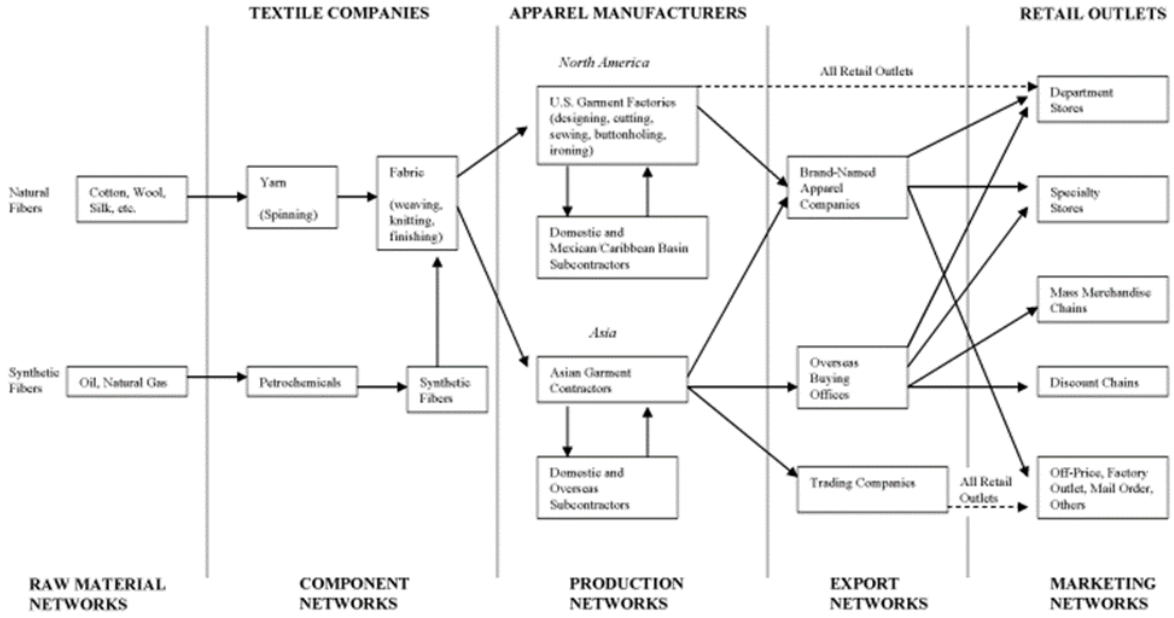
1. Creating sustainable global supply chains;
2. Creating local micro supply chains;
3. Providing security of ownership of land and assets.

5.1 Creating sustainable global supply chains

Globalised supply chains are extremely complex and are now generally built on a 'cascade' of contracts[32] – developing at the same time a cascading risk of exploitation of vulnerable and disadvantaged people. Within this section, we present an example based on clothing supply chains, but the principles are equally applicable in a variety of other industries, including food production or the globalised flower market. In particular, women and children are often exploited in e.g. clothing supply chains – producing clothing items for small payments for larger middlemen who then sell them on to clothing retailers across the globe[33]. One example of the global commodity chains that have developed in the clothing arena is illustrated below in Figure 6.

[32] Nolan, Zhang & Liu, "The Global Business Revolution, the Cascade Effect and the Challenge for Firms from Developing Countries", Cambridge Journal of Economics, (2008) 32 (1): 29-47.
[33] https://www.gov.uk/government/case-studies/helping-women-open-up-for-business-in-pakistan/

Figure 6: The apparel commodity chain



Source: Appelbaum and Gereffi, 1994[34]

There are many examples of how these supply chains house a great deal of opaqueness to both the Marketing Networks (on the far right side of the diagram), as well as the consumers. Quite often, consumers are unaware of the fact that child labour has been part of the supply chain that produced their clothes. At the same time, large scale retailers, e.g. H&M or Primark, do not have clarity over the supply chain once a contract has been signed with a Producer (in the middle of the diagram). Quite often, even large-scale manufacturers outsource to smaller middlemen in order to meet delivery schedules. This cascade of contracts does not just create opaqueness in the supply chain – it also transfers the economic burden *down* the supply chain, rather than *up* it. As a result, many small producers end up being exploited, producing many garments for a low per piece rate.

DLT can be efficiently applied with the cascade of contracts in order to provide transparency over the supply chain as it really stands[35]. For example, if retailers and Marketing Networks started requesting that all orders are placed within a private permissioned DLT and the Producers sourcing of garments were stored there as well, it would be possible to get clarity over the 'cascade' of contracts that forms the entire supply chain, rather than just the point of entry. Supply chains would gain significantly more fine grained detail over the origin of inputs (e.g. cotton or polyester) and the process by which they were produced. Retailers would then be able to provide customers with much more detail about the manner in which clothing or other products have been produced. More importantly, they will be able to enforce the contracts they have established with suppliers in more detail.

A Proof of Concept has been included in the Appendix 1 of this report built by students at Imperial College.

---

[34] Appelbaum, Richard P. and Gary Gereffi, "Power and Profits in the Apparel Commodity Chain", in Edna Bonacich, Lucie Cheng, Norma Chinchilla, Norma Hamilton, and Paul Ong (eds.), 1994, "Global Production: The Apparel Industry in the Pacific Rim. Philadelphia".

[35] Please note that this does not necessarily require the use of smart contracts within the solution, rather that the agreement is registered onto the DL.

5.2 Creating micro supply chains

Another option for ensuring sustainable livelihoods is to empower the local end-users. A slightly more complex application of DLT, therefore, is to develop and encourage new forms of localised supply chains to operate at a much larger scale.

Within many of the countries that DFID are active within, there are a number of initiatives that help empower local communities through e.g. providing microfinance loans[36]. These enable the borrowers to increase their earning capacity and to create new jobs for the wider community, assisting people "to escape poverty, invest more in their children's health and education and, as well as better participate in the wider community."[37]

Many such enterprises are micro enterprises – often created by one person growing to a few people hired locally. A key issue for micro enterprises is the ability to deliver large-scale orders – often they will not have the capacity and as a result have difficulty in meeting supply. Through using DLT, it is possible for micro enterprises to work together in order to smooth supply chain issues and successfully deliver larger orders than necessary.

Managing supply requires co-ordination of efforts – which can nowadays be effectively managed via mobile phones, much like microfinancing can. Through using DLT, micro suppliers would be able to inform one another reliably what products and services they are able to deliver in that particular time period – allowing them to co-ordinate larger orders between them to ensure supply for larger orders. This can enable micro enterprises to achieve scale economies, while ensuring they are able to maintain a good price for their products.

An example organisational structure has been included in the Appendix 2 of this report, funded through EPSRC grant: EP/J000604/2.

5.3 Providing security of ownership of land and assets

As discussed in DFID's LEGEND project describes: "Land and property rights is a complex and politically sensitive issue to address. Weak land governance puts a brake on economic development. It deters responsible investors, threatens food security, increases the likelihood of conflicts, and puts the livelihoods of millions at risk, particularly women and girls. Changing the way in which we deal with land is critically important for growth and poverty eradication."[38]

Land management is also critical with regards to environmental protection – for example in Indonesia, more than 7m hectares of land has had licences for the same concessions allocated to four different palm, pulpwood, logging and coal mining operations at the same time[39]. This creates problems for corporations and – as has been seen recently – environmental devastation through the lighting of multiple forest fires. Indonesia's lack of a centralised land registry is one of the main causes of this issue, as well as possible corruption. Many countries across the world lack proper means to register land or other assets.

The lack of registries and effective means by which to prevent fraud are costly for corporations, nations as well and individuals, in particular women.[40] The use of DLT for

[36] https://www.gov.uk/government/case-studies/helping-women-open-up-for-business-in-pakistan/
[37] Ibid.
[38] DFID Land Policy Bulletin, Issue 1, June 2015.
[39] http://landportal.info/news/2016/04/greenpeace-reveals-indonesias-forests-risk-multiple-companies-claim-rights-same-land%E2%80%8B/
[40] DFID Land Policy Bulletin, Issue 1 June 2015.

the registration of property, land and other assets is probably one of the simplest examples of DLT outside of currency applications that have been well publicised through various announcements, e.g. in Honduras[41].

As outlined in Deloitte's Blockchain report[42], DLT can be used to associate a piece of land with a particular private key and any sale or transfer of ownership of the land is recorded as an immutable transaction, in a similar manner to how coins are exchanged in the bitcoin network. Through the unchangeable nature of the distributed ledgers, it is possible to trace the entire history of the exchange of a piece of land or other property.

[41] http://www.coindesk.com/debate-factom-land-title-honduras/

[42] https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-public-sector.pdf/

6 Identity management with DLT

One of the main areas that DLT may assist in DFID's areas of operation is that of identity management. An inability to prove your identity within society can lead to serious issues regarding access to basic services, lead to potential "unnecessary harassment from officials … restrict rights to vote, open a bank account, or register to obtain any other services"[43]. Essentially, effective identity management can help citizens engage better within society and create opportunities for economic growth and sustainable job creation. This is a critical area that will underpin many of DFID activities as "over 2 billion people lack an official ID. The problem disproportionately affects children and women, from poor rural areas in Africa and Asia."[44]

Far beyond just proving rights of ownership of land and other assets, identity management on a DL can help to manage many areas of a person's life and provide an immutable record of their 'journey' from birth to death covering areas that are critical to provide records of for employment or further education. In particular, such a system may prove useful in areas experiencing unrest or conflict. Use of DLT may dramatically reduce the time required to register and provide services to displaced people. It should be noted, however, that research is required in order to ensure that any such solution does not create unintended consequences regarding the privacy and long-term security of individuals. A key aspect of any ID management system is the requirement to establish a standardised integration approach in order to reduce costs, ensure interoperability and avoid duplication.

Within this section, we focus on three main areas:

- Births, Marriages and Deaths;
- Education; and
- Healthcare.

6.1 Births, marriages and deaths

Within the significant majority of nations birth, death and marriage certificates are required to prove identity of a person, when they change their name or marital status. When a person dies, a death certificate is often required to prove next of kin's right to inheritance. There is a significant of fraud in these areas globally, not just those nations in DFID's remit.

Through using DLT to register these events, it provides an immutable record of them and the person they are associated with. From a technical perspective, this could be done relatively easily, but there are possible significant issues with some aspects of the process. **Firstly,** the use of DLT is complex in the case of lost or misplaced private keys. What are the mechanisms that would need to be put in place in order to enable people to retrieve them?

Secondly, irrespective of the technology selected to prove identity, the process of recording everyone's birth, marriage and death is inherently an institutional issue, rather than a technical one. DLT can be used to overcome the differing levels of infrastructure maturity in different nations, but a robust strategy and roadmap would still need to be

[43] http://www.undp.org/content/undp/en/home/ourwork/ourstories/in-sri-lanka--providing-access-to-justice-through-mobile-clinics.html/

[44] World Bank, 2015, "ID4D-Integration Approach Study Complete".

developed in order to ensure that the necessary training and education was put in place to assist people to use it effectively.

6.2 Education

Proving that a person has the education that they state they have is not just a problem in developing nations – it is an international problem[45] and is costly to:

- Employers who need to pay to have them checked; and
- Institutions, who need to pay someone to confirm/deny a student's affiliation, degree and grades when requested.

DLT provides an excellent means by which to track someone's progress through their educational career. As a student graduates from different institutions, this fact and their grades can be registered onto a DL. Both the student and the awarding institution would be provided with keys that permit the records to be unlocked. Upon request from e.g. an employer, the student would be able to provide them with access to those records seamlessly.

Beyond proving educational qualifications, DLT may also be used within the educational process itself – allowing the tracking and tracing of standardised exam results across regions and schools more effectively and robustly. These results could be anonymous and allow for targeting of educational initiatives in areas where certain capabilities seem to be lacking. It may also allow the tracking of attendance by students.

A Proof of Concept has been included in the Appendix 2 of this report built by students at Imperial College.

6.3 Healthcare

An area where DLT can help make critical improvements for nations in DFID's remit is healthcare. Through registering patients' journeys through the healthcare system, the provision of healthcare services can be significantly improved and better tailored to the patient's needs. For example, it may help to better provide antenatal and postnatal care to mothers and children ensuring they turn up for appointments and to better track development.

Healthcare provides a rich opportunity for the better management of the process by which information is gathered and stored about patients – it can streamline processes and reduce errors within hospitals by reducing the necessity to transfer information between parties. More importantly, using a DLT will allow patients to understand their own overall health history better and to know when someone has accessed or read their files[46].

A key aspect of such a solution requires the handling of patient consent – how does a patient give consent for actions if they are unable to do so e.g. after having been in an accident? The solutions will need to be developed to allow consent to be permitted in such cases, but to be retrieved as well. For nations tracking information in this manner on a DLT, they will be better able to identify possible emerging health issues or emergencies and also analyse the healthcare data of the nation more effectively.

A Proof of Concept is currently being developed at Imperial College.

---

[45] See e.g. http://www.fakediploma.co.uk/.

[46] http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367/

DLT can also be used to track pharmaceuticals[47] in developing nations, in order to ensure that fake medicines are not sold, reducing the risk of populations developing resistance to medication and the risk of patients not recovering from illnesses.

[47] GO Science, 2015, "Forensic Science and Beyond: Authenticity, Provenance and Assurance".

7 Barriers to DLT use within DFID operations

It is still early days for the application of DLT in a variety of industries. Within DFID, DLT hold significant promise but must be assessed properly before replacing existing solutions. There are a number of barriers that need to be addressed prior to a full-scale implementation. In this section, we focus on the two main ones:

- Technical feasibility;
- Institutional Barriers.

7.1 Technical limitations

Blockchain has progressed significantly since the first paper released by Satoshi Nakomoto in 2008[48] . As people have realised the power of the distributed ledger approach, these techniques are now moving out of cyberlibertarian roots into both the corporate and public services domains. There do, however, remain some technical issues that need to be addressed for any use case by DFID.

7.1.1 Cryptocurrency transactions speeds and scalability

Because of its unique design goals of operating in a completely open environment without any points of centralised trust, and in which potentially malicious actors are not only allowed to submit transactions but also participate in transaction validation, Bitcoin's blockchain adds an extra component known as proof-of-work. This approach is computationally expensive, uses a significant amount of electricity, does not scale well and requires a large number of network participants in order to be able to generate the `trust' required to ensure the network works effectively. For further technical details on Bitcoin protocols readers are referred to[49] and for further discussion of the scalability limitations of the Bitcoin network, readers are referred to[50].

Due to the protocol restricting blocksizes to 1MB, Bitcoin has a peak capacity of around 7 transactions per second compared to approximately 56,000 for Visa's network[51]. This provides an inherent scalability problem that would prevent it being used for large-scale aid payments and may make it unsuitable for processing smaller payments as well. For this reason, the use of a cryptocurrency solution is not recommended unless it is implemented without the proof of work mechanism.

7.1.2 Remittances

The application of DLT within remittances requires the development of a new back-end system between multiple parties, which will need a lot of effort to put together. This system will likely have a large impact on transaction costs and also the reduction in response times aid money transfers. It could therefore be one of the most positive prospects for early-stage application of DLT within DFID. As it relies heavily on the agreement, participation and training of multiple actors across the chain of organisations active within consortia, it may take a long time to develop the appropriate technical solution.

7.1.3 Smart contracts

Smart contracts, as discussed are self-executing contractual states, stored on the blockchain, which nobody controls and in theory everyone can therefore trust[52]. These are relatively new, however, and there are few real-world examples of smart contracts – most

[48] https://bitcoin.org/bitcoin.pdf/

[49] A. M. Antonopoulos, 2014, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies".

[50] T. McConaghy et al., 2016, "BigchainDB: a Scalable Blockchain Database, Whitepaper", https://www.bigchaindb.com/whitepaper/bigchaindbwhitepaper.pdf/, March 2016.

[51] https://en.bitcoin.it/wiki/Scalability/

[52] https://smartcontract.com/

are proofs of concept. Moreover, the status of smart contracts has not yet been tested in any legal setting and many legal firms are currently struggling to understand the impact of this type of technology. Within the scope of DFID's work, the use of smart contracts may prove difficult due to lack of understanding about jurisdictional status for different contracts.

In addition, smart contracts are often coded with Turing Complete programming languages. This means that there can be some issues with poor or malicious coding that cause contracts to fail to execute. Prior to full-scale implementation within DFID, therefore, this would need full investigation and also the development of policies and regulations that could be enacted algorithmically by programmers.

A further complexity associated with smart contracts would be the ensuring that there were sufficient auditors able to investigate and read the code developed for auditing purposes.

7.1.4 Use of DLT in computationally poor areas

A DLT is not much use without the ability to access it and use it effectively in local and regional areas. For this reason, cryptocurrencies or DL that rely on proof of work mechanisms are not recommended for areas with low technical capacities. DLT built without proof of work mechanisms can realistically be implemented on devices with significantly lower computational capacity – a mobile phone will often be enough to store and access private keys effectively.

7.1.5 Technical recommendations

For all of the early-stage prototypes, proofs of concept and small-scale trials, it is therefore recommended that DFID use a private, permissioned DLT that permits it to control access, know who and when someone has accessed the DL. These trials should be used to gain knowledge and know-how about how the organisation might work with DLT effectively on a larger scale. These DLT solutions should be run in parallel with existing legacy systems initially in order to provide a back-up system in critical situations, but also to provide baselines for further technical improvements based on end-user feedback.

7.2 Institutions

The largest barrier to the application of DLT within DFID's scope of operations is not actually technical – it is institutional. As with any new technology, the success of any project relies not just on provision of hardware, software and connectivity - it requires process re-engineering, training, education, and change management processes[53].

Numerous case studies exist about the role of technology in assisting people to:

- Access financing and banking, through e.g. microfinance solutions;
- More effectively access services through e.g. e-government approaches;
- Provide better healthcare for rural areas and disadvantaged people;
- Improve access to education; and
- Improve economic prospects through access to market information.

The role of DLT and cryptocurrencies play within society, however, is far more complex than a traditional ICT solution. These technologies demand not just that people are trained in a new means of completing an existing process, but rather that the entire manner in which society is organised is re-assessed and re-defined. Distributed ledgers dramatically adjust the manner in which society "believes" and "trusts" certain types of information.

[53] https://india.gov.in/e-governance/national-e-governance-plan/

7.2.1 Redefining trust and the role of intermediaries

Traditionally, intermediaries have created the generation of trust in societies. For example, a nation's central bank is responsible for generating trust in the national currency – a 5-pound note is considered legal tender in Britain precisely because it comes with the backing of the Bank of England. People therefore 'trust' that this currency is usable. Similarly, people trust the land registries of many countries as the most accurate record of land ownership. Births, marriages, deaths, educational track records are all stored in centralised databases or filing storage by authorities that are trusted to ensure the contents are as accurate as possible. The 'trust' in these records is generated by the fact that a central authority keeps them.

DLT changes the functioning of these intermediaries dramatically – and in some cases removes the need for them whatsoever. This is not necessarily and trivial thing for people using DLT to fully understand and as a result people may take time to trust the new method of operation for the creation of trust. For example, bitcoin requires people to grasp that the 'trust' in the network is generated by the very fact that no-one trusts one another. By storing all of the transactions on a public ledger, trust is generated, as it is impossible to change the records without a level of computational capacity that currently does not exist on planet earth. Through providing this notion of "shared untrustworthiness to create trust", the necessity to have a central bank to provide trust in a currency is removed. This example holds for land registries as well – by publishing every transaction onto a public DL, it removes the necessity for a central trusted authority to provide the trust in land records. Similarly, for education, healthcare and all manner of other components of a stable and just governance system within a nation. These are not simple concepts to grasp and ensuring that other parties within the ecosystem are comfortable and fully understand the new method of operation is critical to the success of any effort.

It is critical to understand that technology does not solve problems, but rather that it is a tool that effectively applied can help countries establish functioning governance systems that assist in creating stability and economic growth prospects. The use of DLT needs to be carefully balanced against the development pathways that a nation is on – each pathway is of course different and within each nation, the use of DLT will need to be assessed separately.

There are, however, ample opportunities for DFID to assist countries to apply DLT in nations where there is currently little order or technology in governance of the nation. The relative low cost and accessibility of DLT compared to legacy systems built for the enterprise era of ICT can assist them in radically improving governance without massive cost.

7.2.2 Institutional governance of humanitarian activities

Within DFID itself, however, the role of DLT can be relatively successfully implemented in e.g. delivery of aid solutions where DFID is working together in a consortium. This is because many within the aid community are already investigating how DLT can be applied and because as discussed in the previous section, the system itself is in desperate need of reform with regards to management and organisational structures for a new era of humanitarian response.

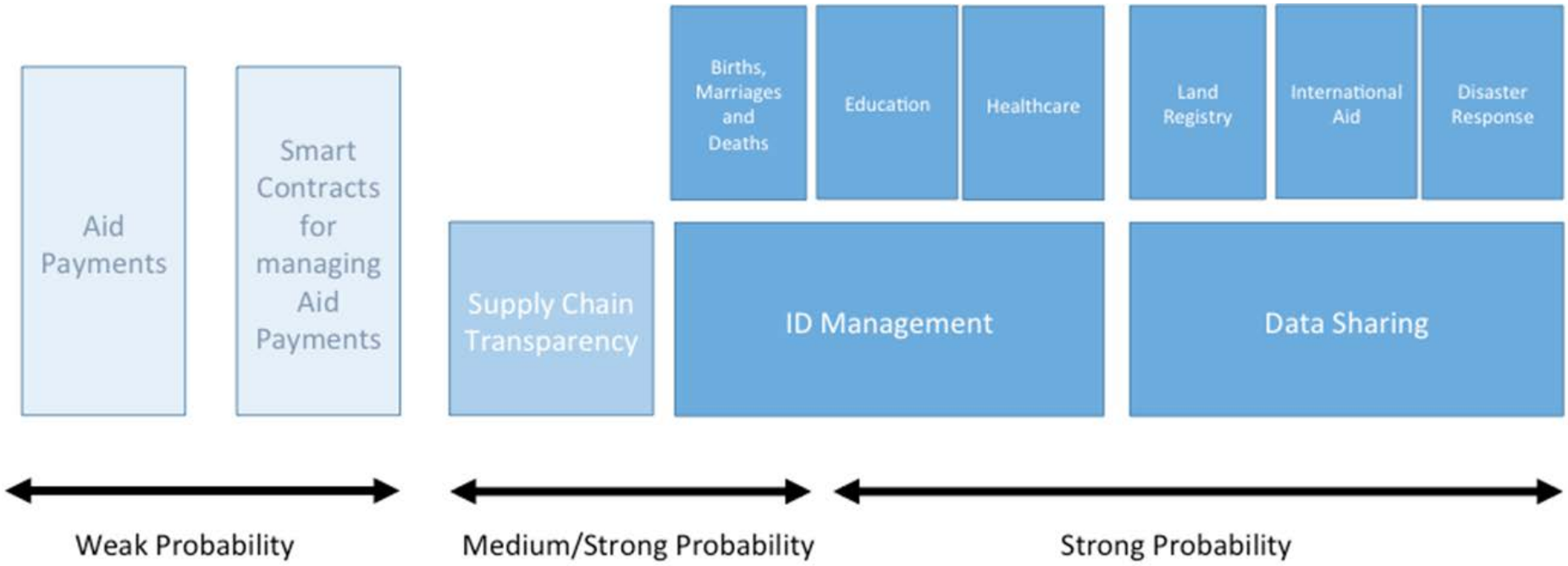
The approaches taken to managing a DLT within humanitarian response can be likened to a more traditional change management strategy across a supply chain – where all actors need to understand how to interface the new system. The potential for dramatic reduction both in transaction costs across the overall aid landscape and the amount of time required to get activities working on the ground in affected areas will likely prove enough of an incentive to all the actors involved.

A critical institutional aspect, however, will be the manner in which standardised activities on top of the DLT will be managed and need to be carefully addressed during implementation. For example, achieving agreement on an international level about what

an ID looks like will likely prove critical for the successful implementation of identity management and remittances.

8 Summary of DLT landscape within DFID's operations

Figure 7: Spectrum of DLT applications within DFID in 5-10 year time frame



References

- Appelbaum, R., Gereffi, G., 1994, *"Power and Profits in the Apparel Commodity Chain"*, in Edna Bonacich, Lucie Cheng, Norma Chinchilla, Norma Hamilton, and Paul Ong (eds.), 1994, "Global Production: The Apparel Industry in the Pacific Rim. Philadelphia".

- Allison, I., March 2016 "*R3 completes trial of five cloud-based blockchain technologies with 40 banks"*, available online athttp://www.ibtimes.co.uk/r3-completes-trial-five-cloud-based-blockchain-technologies-40-banks-1547260/,

- Allison, I., March 2016, IBI Times, *"Guardtime secures over a million Estonian healthcare records on the blockchain"*, available online at http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367/,

- Antonopoulos, A.M., 2014, *"Mastering Bitcoin: Unlocking Digital Cryptocurrencies"*, O'Reilly 204

- Bank of England, 2015, *"One Bank Research Agenda"*: http://www.bankofengland.co.uk/research/documents/onebank/discussion.pdf/, February 2015.

- Bloomberg, 2016, *"Bitcoin is socially a commodity, according to U.S. regulator: The Commodity Futures Trading Commission makes its mark"*, http://www.bloomberg.com/news/articles/2015-09-17/bitcoin-is-officially-a-commodity-according-to-u-s-regulator.

- Coindesk, 2016, *"Blockchain Land Title Project 'Stalls' in Honduras"*, available online at: http://www.coindesk.com/debate-factom-land-title-honduras/

- Das, S., 2016, Cryptocoin News, *"JPMorgan begins blockchain trials"*, available online at https://www.cryptocoinsnews.com/ jpmorgan-begins-blockchain-trials/, February 2016.

- Das, S., January 2016, Cryptocoin News, *"China's central bank will look to issue its own digital currency as soon as possible"*, available online at https://www.cryptocoinsnews.com/china-digital-currency/, January 2016.

- De Nederlandsche Bank, 2015, *"Jaarverslag 2015"*, available online at http://www.dnb.nl/binaries/Jaarverslag%

- Deloitte, 2016, *"Blockchain applications in the public sector"*, available online at: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-

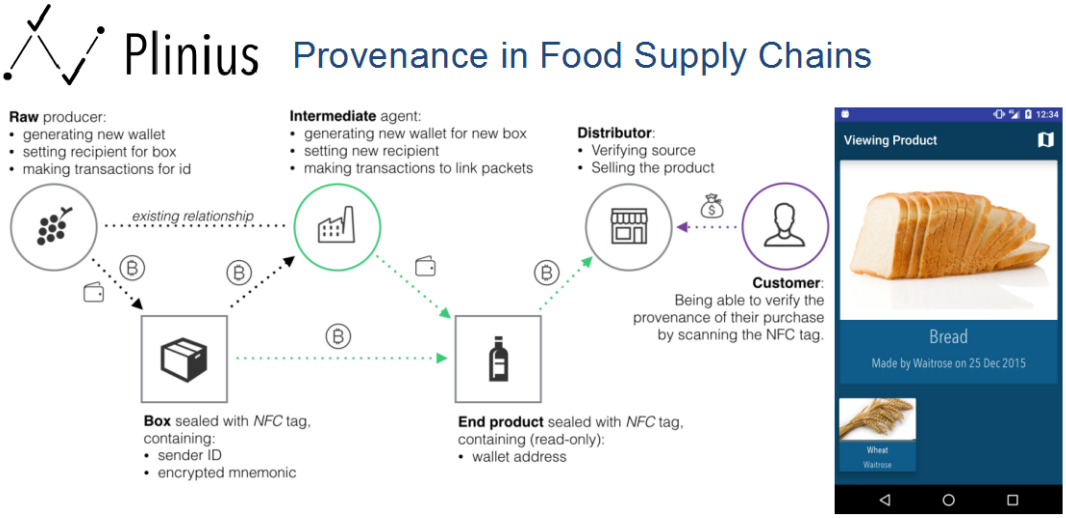
en-innovation-deloitte-blockchain-app-in-public-sector.pdf/

- DFID Case Study, 2015, *"Helping Women Open up for Business in Pakistan"*, available online at: https://www.gov.uk/government/case-studies/helping-women-open-up-for-business-in-pakistan/
- DFID Land Policy Bulletin, June 2015, Issue 1
- EU Commission, *Communication from the Commission to the European Parliament and the Council: On an Action Plan for Strengthening the Fight against Terrorist* Financing, http://ec.europa.eu/justice/criminal/files/com_2016_50_en.pdf/.
- GO Science, 2015, *"Forensic Science and Beyond: Authenticity, Provenance and Assurance"*.
- Kent, Armstrong, & Obrecht, 2015, Smart Network White Paper, *"The Future of Non-Governmental Organisations in the Humanitarian Sector: Global Transformations and* Their Consequences, Humanitarian Futures Programme Discussion Paper for the Start Network", available online at: [1] http://www.start-network.org/news/leveraging-blockchain-technology-improve-financial-mechanisms-humanitarian-sector/#.Vv1YbHAkcnN/
- Kynetix, 2015 *"Kynetix announce commodity title transfer on blockchain using SenTinel*:, press release; available at http://www.kynetix.com/wp-content/uploads/2015/12/; andTinel:, press release; available at http://www.kynetix.com/wp-content/uploads/2015/12/; and
- Landportal, 2015, *"Greenpeace reveals Indonesia's forests at risk as multiple companies claim rights to same land"*, available online at: http://landportal.info/news/2016/04/greenpeace-reveals-indonesias-forests-risk-multiple-companies-claim-rights-same-land%E2%80%8B
- McConaghy, T., et al, 2016, *"BigchainDB: a Scalable Blockchain Database, Whitepaper"*, available online at https: //www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf/.
- Nakamoto, S., 2008, *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, available online at https://bitcoin.org/bitcoin.pdf/.
- Nasdaq, 2015 *"Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology"*, press release; available at http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326/, December 2015.

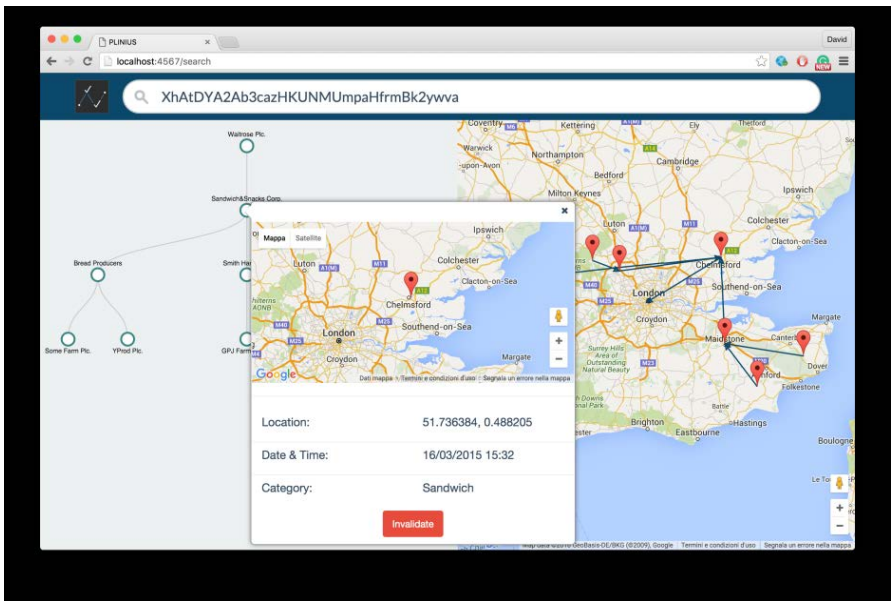
- Nasdaq, 2015, *"Nasdaq launches enterprise-wide blockchain technology initiative"*, press release; available at http: //ir.nasdaq.com/releasedetail.cfm?releaseid=912196/, May 2015.
- Nolan, Zhang & Liu, 2009, *"The Global Business Revolution, the Cascade Effect and the Challenge for Firms from Developing Countries"*, Cambridge Journal of Economics, (2008) 32 (1): 29-47.
- Norton, Rose & Fulbright, 2016, *"Deciphering Cryptocurrencies: A Global Legal and Regulatory Guide"* White paper
- Skinner, C., ValueWeb, 2016, *"How FinTech Firms Are Using Mobile and Blockchain Technologies to Create the Internet of Value"*, available online at: http://thefinanser.com/2016/03/valueweb-how-fintech-firms-are-using-bitcoin-blockchain-and-mobile-technologies-to-create-the-internet-of-value.html/
- South African Reserve Bank, 2015 *"User alert: monitoring of virtual currencies"*, http://www.treasury.gov.za/comm_media/press/2014/2014091801%20-%20User%20Alert%20Virtual%20currencies.pdf/.
- Swan, M., 2015, *"Blockchain: Blueprint for a New Economy"*, O'Reilly 2016
- The Economist, April 2016, *"The trust machine: The technology behind bitcoin could transform how the economy works"*, available online at http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine/, October 2015.
- UNDP, 2014, *"Sri Lankans get access to justice through mobile clinics"*, available online at: http://www.undp.org/content/undp/en/home/ourwork/ourstories/in-sri-lanka--providing-access-to-justice-through-mobile-clinics.html/
- Wallace, Bornstein and Chapman, 2007, *"The Aid Chain: Coercion and Commitment in Development NGOs"*, Practical Action Publishers, 2007
- World Bank, 2015, *"ID4D-Integration Approach Study Complete"*.

Annex 1 – Provenance in supply chains

Plinius was a proof of concept developed by students at Imperial College Centre of Cryptocurrency Research and Engineering. Through using a DL, the students illustrated the ability of DLT to track and trace the transfer of goods between different parts of the supply chain. The PoC focussed on the use case of wine and food. It illustrates the usefulness for the supply chain, the consumers and also regulators.



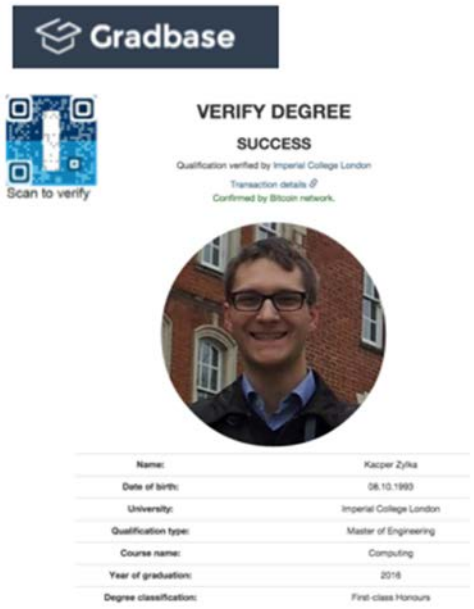
Imperial College Centre for Cryptocurrency Research and Engineering



Annex 2 - Organisational Structures for Micro Supply Chains

A micro supplier – a single person enterprise based in London – used lightweight digital technology (mobile phone and twitter) to build a supply chain management system that helped manage her ability to deliver products and services to large customers. Working with edible flowers, she was able to connect supplier across the UK (Scotland and England) to deliver high quality edible flowers to Michelin star restaurants in London and develop and build edible wedding bouquets.

Annex 3 – Education records using DLT



- **Universities** upload degree data to blockchain
- **Students** are given link to their degree data (QR)
- **Employers** can confirm that degree is valid using Gradbase
- Degree information cannot be changed and can be shown to have come from relevant institution

Imperial College Centre for Cryptocurrency Research and Engineering

Annex 4 - Blockchain- verified contracts

EXPRESS AGREEMENT

- **Contracts** are agreed and signed by all parties
- **Encrypted** contract is uploaded to the blockchain
- At any time, any party may check the terms of the agreement
- **Blockchain** ensures the agreement remains unchanged