DISTRIBUTED LEDGER TECHNOLOGIES AND FINANCIAL INCLUSION

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFS

(03/2017)

ITU-T Focus Group Digital Financial Services

Distributed Ledger Technologies and Financial Inclusion

Focus Group Technical Report

ITU-T

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFS) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Distributed Ledger Technologies and Financial Inclusion

About this report

This technical report was written by Leon Perlman, PhD.

The author would like to thank members of the International Telecommunications Union (ITU), TIC, WG, and others for their considered and constructive comments on drafts of this study. In particular, Paul Makin of Consult Hyperion UK, Prof Kevin Butler of the University of Florida, Albert Lewis of the US Federal Communications Commission, Vijay Mauree of ITU, Prof Emin Gün Sirer of Cornell University, Tim Swanson of R3, Adrian Hope-Bailie of Ripple, and Ariadne Plaitakis of Mondato.

All citation links were checked for validity in February 2017.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfs@itu.int

Table of contents

Executive summary

Distributed ledger technology (DLT) is a new type of secure database or ledger for keeping track of who owns a financial, physical, or electronic asset, but without the need for a centralized controller of this data. Instead, the data is shared in a peer-to-peer manner across multiple sites, countries, or institutions.

DLT has the potential to speed up and reduce the cost of transactions, give individuals more control over their personal data, reduce or remove the need for costly intermediaries, provide secure 'smart' legal contracts that execute without user intervention, bolster data security by providing almost real-time evidence of tampering, and revolutionize regulatory compliance.

A prime example of DLT is called blockchain technology. All blockchains operate by taking a number of records and putting them in a block and then chaining that block to the next block using a cryptographic signature. While the data (blocks) are stored one after the other in a continuous ledger, they can only be added when the participants reach a quorum (consensus) over their validity. Each record is time/date stamped and provided with a unique cryptographic signature, which is designed to ensure the authenticity and integrity of the ledger. This distributed design eliminates the need for a central authority or intermediary to process, validate, or authenticate transactions and data.

The manner in which consensus for proposed changes to the ledger is reached defines the type of blockchain. The process may be permissionless or permissioned. Some may be public or private and may allow only certain people to view all or subsets of the data on a blockchain. These ledgers are similarly designed for rapid detection of unauthorized changes to the data.

Thus, the study sets out to detail: The evolution of DLT; its numerous strengths and weaknesses; the varied commercial and public-good applications that have been identified; the implications of the disintermediation of traditional centralized controllers of data; concerns in respect of the technology designs and their consistency; issues in implementation and usage; security of DLTs; validity of the information placed on a blockchain; and the spectrum of evolving legal and regulatory challenges and uncertainties around DLT. Therefore, the use of emerging 'regulatory sandbox' tools employed by regulators to allow testing of DLTs in a controlled way, with clear consumer protection and implementation and exit windows, are also explored.

The study also investigates some applications that may be particularly useful for financial inclusion, including: remittances; developing new identity systems; interoperability between digital financial services (DFS) and banking platforms; innovative, self-executing 'smart contracts'; micro-insurance uses; clearing and settlement (C&S) in payment systems; credit provision; and property and land registration.

Approach

Because of rapid changes and the relatively large scope of issues surrounding DLT, this study does not, and cannot, cover all aspects of DLTs. Rather, it is of a landscaping nature with an additional focus on financial inclusion. It is written with primarily regulators, lawmakers, and others with a non-technical interest in DLT in mind. For ease of reading for non-technical readers, most of the technical details around DLTs are placed in the endnotes.

Readers who have a technical interest in DLTs and the nuances of the technologies, classifications, and terminology are encouraged to read the papers referenced in the endnotes.

It must also be noted that since DLT is an amalgam of emerging and evolving technologies, there appears to be limited consensus amongst academics, commentators, those in DLT development and consulting industries, and regulators on 'standard' DLT terminology and the technical and commercial use and implications of the technology. Even the term 'DLT' to describe new decentralized ledger technology has variations. However, this study settles on terminology and DLT concepts in general use at the time of writing.

List of Acronyms

AML	Anti-Money Laundering
BaaS	Blockchain-as-a-Service
BIP	Bitcoin Improvement Proposal
C&S	Clearing and Settlement
DAO	Distributed Autonomous Organization
D-CENT	Decentralised Citizens Engagement Technologies
DFS	Digital Financial Services
DLT	Distributed Ledger Technology
eKYC	Electronic Know Your Customer
FinTech	Financial Technology
ID	Identity
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MNO	Mobile Network Operator
POC	Proof of Concept
POS	Proof of Stake
POW	Proof of Work
RCL	Ripple Consensus Ledger
RegTech	Regulatory Technology
SEPA	Single Euro Payments Area
SME	Small Medium Enterprise
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPS	Transactions Per Second

1 Introduction to Distributed ledger technology (DLT)[1]

1.1 What is a DLT?

DLT is a new type of secure database or ledger that is replicated across multiple sites, countries, or institutions with no centralized controller. In essence, this is a new way of keeping track of who owns a financial, physical, or electronic asset.

The concept of DLTs emerged from the introduction of the 'blockchain' in 2008 through the launch of the cryptocurrency[2] Bitcoin.[3]

Bitcoin's decentralized transaction authentication rests on blockchain approaches: It records in a digital *ledger* every transaction made in that currency in identical copies of a ledger which are replicated – *distributed* - amongst the currency's users - *nodes* - on a chain of data blocks.[4] There are similar technologies to blockchain, but since all these definitions and concepts relating to these technologies ultimately refer to databases which are *distributed*, the term DLT is commonly used as a term of art by those in the technology development community as the generic descriptor for any distributed, encrypted database and application that is shared by an industry or private consortium, or which is open to the public.[5]

This report embraces and uses the technical term DLT to describe all distributed ledgers, no matter what underlying sharing technology or protocol is used.[6]

1.2 The concepts of blockchains and 'distributed ledgers'

DLTs generally integrate a number of innovations which include: Database (ledger) entries that cannot be reversed or otherwise modified, the ability to grant granular permissions, automated data synchronization, rigorous privacy and security capabilities, process automation, and transparency, such that any attempts at changes to entries will notify others. Its main disruptive attribute is that it is decentralized and therefore not dependent on a central controller or storer of the data.

Blockchain technology, as an example of a DLT, has as its most disruptive innovation the elimination of the need for third party intermediaries in favor of *distribution* of the data across

---

[1] Drawn from Perlman, L (2016) *Aspects of the Legal and Regulatory Issues in Blockchain Technology.* Many of the technical details around Distributed Ledger Technology can be found in the endnotes of this paper.

[2] The concept 'cryptocurrency' was first described in 1998 in an essay by Wei Dai on the Cypherpunks mailing list, suggesting the idea of a new form of money he called 'b-money.' Rather than a central authority, it would use cryptography to control its creation and transactions. See Dai, W (1998) *b-money*, available at http://www.weidai.com/bmoney.txt.

[3] Bitcoin is a consensus network that enables a new payment system and a completely digital money or 'cryptocurrency.' It is thought to be the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. The first Bitcoin specification and proof of concept (POC) was published in 2008 in a cryptography mailing list by one 'Satoshi Nakamoto.' It is not known if this is a pseudonym, The Bitcoin community has since grown exponentially, but without Nakamato. See Bitcoin (2016) *FAQs*, available at https://bitcoin.org/en/faq#what-is-bitcoin.

[4] The technology, in the words of Bitcoin's apparent creator, is: '[A] system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.' See Nakamoto, S (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System,* available at https://bitcoin.org/bitcoin.pdf.

[5] See Mills, DC *et al* (2016) *Distributed Ledger Technology in Payments, Clearing, and Settlement FEDS Working Paper No. 2016-095,* available at https://ssrn.com/abstract=2881204; and UK Government Office for Science (2016) *Distributed Ledger Technology: Beyond Block Chain*, available at https://goo.gl/bVg0Vq . The term Distributed Ledger Technology is often used interchangeably with 'Shared Ledger Technology.' DLT though will be used throughout this study. SLT was coined by Richard Brown, CTO of blockchain company R3. See thereto, https://goo.gl/gaeDRU ; and Hoskinson, C (2016) *Goodbye Mike and Some Thoughts About Bitcoin*, available at https://goo.gl/bGVN0R .

[6] There is also the Ripple DLT, which is not viewed as 'blockchain' technology. See Section 2.3 on Ripple.

participant nodes. This means that every participant – a *node* – in a blockchain can keep – *share* – a copy of the blockchain. The blockchain updates the nodes automatically every time a new 'transaction' occurs.[7] Accuracy of the information is maintained through synchronization of the nodes, so that the information on each node precisely matches each other node.[8]

Usually only those with an appropriate cryptographic key can view or add to the data on a blockchain, which may layer on permissions for different types of users where necessary.[9] Anyone can, with the right tools, create a blockchain and decide who can see the data in the blockchain, or add data to it. Banks, governments, and private entities are rapidly developing and implementing blockchain-based solutions worldwide.[10]

Exhibit 1: Differences between centralized and distributed methods.

A blockchain is shared as it does not reside in a central place. It is said then to be decentralized (distributed) across nodes.

These innovations also prompt a number of challenges related to their implementation, including the nascent (and often not yet properly stress-tested) nature of the technologies used; uncertain legal and regulatory status; privacy and confidentiality issues; cultural changes in requiring users to have 'trust' in often anonymous counterparties; scalability of the DLTs for mainstream use comparable to and exceeding existing non-DLTs performing similar functional tasks;[11] and the ability to link[12] different DLTs together, where required.[13]

It is important to note though that the vast majority of DLTs under development today[14] use blockchain technology. When the technically-oriented press discusses financial technology (FinTech) developments, they also use blockchain as shorthand for DLTs. Therefore, blockchain is used in this study as the primary exemplar of DLT.[15]

---

[7] Annex A demonstrates the architecture of a blockchain and how data is added and verified.
[8] See further UK Government Office for Science (2016) *ibid.*
[9] See Section 1.3.
[10] See Sections 2, 3 and 5.
[11] A common concern is that current DLTs processes are much slower than what is needed to run mainstream payment systems or financial markets. Also, the larger the blockchain grows, the larger the requirements become for storage, bandwidth, and computational power required to process blocks. This could result in only a few nodes being able to process a block. However, improvements in power and scalability are being designed to deal with these issues. See Croman, K *et al* (2015) *On Scaling Decentralized Blockchains*, available at https://goo.gl/cWpQpF ; and McConaghy, T *et al* (2016) *BigchainDB: A Scalable Blockchain Database*, available at https://goo.gl/IBcGv0 .
[12] This is also known as interoperability.
[13] There are, of course, a number of broader technical and other issues relating to DLTs and their *inter alia* advantages and disadvantages, as well as their legal, regulatory, security, privacy, and commercial implications. They are noted or discussed briefly but are generally beyond the scope of this paper and will not be detailed in depth.
[14] See Section 2 on the various other DLT designs.
[15] Ki-yis, D & Panagiotakos, K (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at https://goo.gl/Fc2jFt

An important example of the use of blockchain technology is the Bitcoin cryptocurrency, as seen in Exhibit 2.

Exhibit 2: The Bitcoin cryptocurrency, is the first use of blockchain DLT.

Bitcoin is a cryptocurrency that uses blockchain technology. Bitcoin can be difficult to define as there is no authoritative formal specification. In the original proposal, there are to be a limited number of Bitcoins that can ever be mined.[16] Through this methodology, the need for a central issuer – as an intermediary – is thus eliminated.[17]

Bitcoins are created by a process known as mining, which involves users needing to solve a cryptographic puzzle. Once the puzzle has been solved, a new Bitcoin is issued, and its presence is announced to Bitcoin users – nodes - on the Bitcoin blockchain. Spending of a Bitcoin cryptocurrency unit, or issuance of a new Bitcoin by 'miners', is sent across the nodes for verification. Thus, mining is used to validate Bitcoin transactions and the validated records are stored on a blockchain. The purpose of the blockchain is to track Bitcoin spending, specifically to prevent 'double spending' of the same Bitcoin. The system is permissionless and public.

In order to incentivize people to do the mining, and to have Bitcoin transactions validated, they pay successful miners by offering them newly-created Bitcoin when they finish validating a block of transactions and adding it to the blockchain.[18] Once there is *consensus* amongst the nodes that the data can be added, the Bitcoin blockchain is updated with the new information.[19]

1.3 Distributed ledger constructs

1.3.1 Overview

All blockchains operate by taking a number of records and putting them in a block and then chaining that block to the next block, using a cryptographic signature.[20] The method used to validate the accuracy of a distributed ledger is known as 'consensus.'[21]

The *manner* in which consensus for proposed changes to the ledger is reached defines the type of blockchain.[22]

---

[16] For an analysis of Bitcoin's components, see Bandeau, J *et al* (2015) *Soak: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,* available at https://goo.gl/o6Av8h .

[17] For the effects of Bitcoin on central banks and issuance of currency, see Rainer, B *et al* (2014) *Bitcoin: Economics, Technology, and Governance*, available at https://ssrn.com/abstract=2495572. However, there are initiatives by central banks to use digital fiat currencies. For example, see the use of eCurrency technology which powers a digital fiat currency instrument that has the same legal tender status as banknotes and coins. eCurrency and Banque Régionale de Marchés partnered to launch a digital fiat currency, the eCFA, in Senegal. See Business Wire (2016) *Currency Mint Limited and Banque Régionale De Marchés Launch New Digital Currency in Senegal*, available at https://goo.gl/baMlSZ; and World Economic Forum (2016) *The Future of Financial Infrastructure – Global Payments*, available at https://goo.gl/Wtza5r

[18] While the value of a Bitcoin can fluctuate dramatically day-to-day, this has followed a general ascent. The first Bitcoins in 2009 were traded at under US$0.01. In February 2017, a Bitcoin was trading at over US$1,000.

[19] For the Bitcoin blockchain, the updating of the blockchain across all participant nodes can take up to 10 minutes.

[20] See Annex A.

[21] Any data that is placed on the block is said to be 'on-chain' and any data that derives from the blockchain, but which for some reason must be swapped with another party not using blockchain technology is said to be 'off chain.' See also Mills *et al* (2016) *ibid.*

[22] Depending on the DLT, the consensus method may be called Proof of Stake (POS), or Proof of Work (POW). For example, with cryptocurrencies POS is a consensus mechanism used as an alternative to the POW mechanism used in Bitcoin. POS cryptocurrencies are 'minted' rather than 'mined,' so avoiding expensive computations and thus providing a lower entry barrier for block generation rewards. For a fuller discussion of these differences, see Bitfury Group (2015) *Proof of Stake Versus Proof of Work*, available at https://goo.gl/ebS2Vo.

If the process is open to everyone – such as with Bitcoin[23] – then the ledger is said to be 'permissionless', and the DLT has no owner. If participants in that process are preselected, the ledger is said to be 'permissioned.'[24] These may also be public[25] or private.

1.3.2 Permissionless shared ledgers

In permissionless (public) ledgers such as Bitcoin,[26] all participants – the nodes – maintain the integrity of the ledger by reaching a consensus about its state.[27] These public decentralized ledgers are accessible to every Internet user. This allows anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies, so that – theoretically – no one actor can prevent a transaction from being added to the ledger.[28]

The public design goal ostensibly then is to avoid censorship (by a central authority), remove counterparty exposure, and allow open, global membership. There is, however, an overarching issue of whether the correct blocks are being added to the blockchain, possibly through competing proof of work (POW) or proof of stake (POS) as the case may be. These competing blocks may arise because of fraud or because of latencies in updating the entire blockchain across all distributed nodes, such that transactions can theoretically arrive in a different order at different nodes.

This situation may then, at least for a temporary period, create what is known as a 'fork' in the blockchain. This, in turn, creates one or more 'subchains' which may (all) exist at least until the entire blockchain assesses the competing claims and decides which block addition (subchain) is correct and should be added to the blockchain. Resolving these conflicts may take time.

---

[23] Some would argue that in practice Bitcoin is basically a closed network today since the only entity that validates a transaction is effectively 1 in 20 semi-static pools. Further, the miners within those pools almost never individually generate the appropriate/winning 'hash' towards finding a block. Rather, they each generate trillions of invalid hashes each week and are rewarded with shares of a reward as the reward comes in.

[24] Distinctions between permissioned and permissionless described here reflect the current state of the art. As DLTs mature, many believe that there will be a full spectrum between permissioned and permissionless.

[25] Public blockchains are said to be fully decentralized.

[26] Bitcoin is not issued by a central authority and thus cannot be controlled, which from the reaction to Bitcoin by regulators around the world, appears to pose policy challenges.

[27] Validating nodes are different than mining nodes. Mining nodes can prevent 'double spending,' as well as what are called 'Sybil' attacks, named after the case study of a woman with multiple personality disorder. A Sybil attack then is a type of security threat when a node in a peer-to-peer network (such as a blockchain) claims multiple identities. Most networks rely on assumptions of identity, where each computer represents one identity. Fully validating nodes on a blockchain that anyone can run cannot prevent Sybil attacks or double-spending. On Sybil attacks, see Douceur, J (2002) *The Sybil Attack,* available at https://goo.gl/KG4aWY. On its effect on DLTs, see Swanson, T (2015) *Consensus-As-A-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems*, available at https://goo.gl/6tc1Y2 .

[28] The public design goal ostensibly then is to avoid censorship (by a central authority), remove counterparty exposure, and allow open, global membership. As proffered by BitFury and Wattenhofer, applying Consistency, Availability and Partition (CAP)-tolerance theorem for distributed computation systems, DLTs are available so that every request receives a response, and partition-tolerant in that the DLTs still perform, even if some nodes fail, but are not consistent. That, is a distributed system can satisfy any two of these guarantees at the same time, but not all three. While the CAP theorem is subject to some debate in between computer scientists, in all, this may create an overarching issue of whether the correct blocks are being added to the blockchain, possibly through competing POWs or POSs, as the case may be. These competing blocks then, may arise because of fraud or because latencies in updating the entire blockchain across all distributed nodes such that transactions can theoretically arrive in a different order at different nodes. This situation may then, at least for a temporary period, create what is known as a 'fork' in the blockchain. This, in turn, creates one or more 'subchains' which may (all) exist at least until the entire blockchain assesses the competing claims and decides which block addition (subchain) is correct and should be added to the blockchain. Resolving these conflicts may take time. This, in some thinking, makes blockchains, at least for the present state of the art, possibly unsuitable for real-time transactions. See Bitfury (2015) *ibid*; Roger Wattenhofer (2013) *Weak Consistency: Part 2, Chapter 3*.

This makes blockchains, at least for the present state of the art, possibly unsuitable for real-time transactions.[29]

1.3.3 Permissioned shared ledgers

There are two types of permissioned shared ledgers: private and public.

For permissioned private ledgers, only permissioned entities may read the contents of the ledger and write to the ledger, for example R3's Corda.[30] The permissioned private ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process.[31] This is carried out by trusted actors such as government departments or banks.[32] This process makes data entry and verification faster and more efficient when compared to the consensus process of permissionless ledgers. In addition, use of digital signatures by nodes on the chain also creates highly-verifiable data sets.[33]

In permissioned public ledgers, only permissioned entities may write the ledger, but anyone may view the ledger's contents, for example, Ripple.[34] A permissioned ledger may have some 'permissionless' aspects in circumstances where 'non-permissioned' entities may be given restricted access to view partial data sets. They invariably will not, however, have any editing rights on that blockchain.[35]

Permissioned (usually private) blockchains are often split into consortium blockchains, or fully private blockchains. There are benefits and drawbacks to permissioned, permissionless, public, and private approaches, and combinations thereof.[36] While these issues are beyond the scope of this paper, with permissioned blockchains there is an inherent trust as the users must be given consent by a governing body or entity to participate in that blockchain. This 'trust' reduces the amount of computational power required for that blockchain, as well as increases the speed of the blockchain.[37]

The governing body can create its own data access rules to ensure that only participants that are party to a transaction can see sensitive details. With permissionless blockchains, public keys used to assign access to blockchains are never tied to a real-world identity (ID). There is no governing authority and hence trust is measured across the nodes in the blockchain which are able to validate transactions.

---

[29] de Meijer, CRW (2016) *Blockchain, Distributed and Shared Ledger, Permissionless and Permissioned: What's in a Name!!*, available at https://goo.gl/VrhGev .
[30] See Section 2.5 on R3's Corda blockchain implementation.
[31] UK Government Office for Science (2016) *ibid.*
[32] Each transaction can also be validated by a 'notary' and a notary itself can be a 'notary pool' involving multiple nodes run by several different organizations, in effect creating a decentralized check. See Swanson (2015) *ibid.*
[33] However, note that the verification of the data on a blockchain is of its input, not the provenance or veracity of the data. The latter issues are still being developed.
[34] Ripple, while a type of DLT, does not use blockchain technology. See Section 2.3 on Ripple. Ethereum could be included here as an example of permissioned blockchain, but it also has the characteristics of a permissionless blockchain since one can program and participate in Ethereum blockchains without special permission.
[35] Although there are permissionless aspects, a security key is required for access to the blockchain. The 'owners(s)' of the permissioned blockchain will allocate access rights to the blockchain.
[36] See further, Pilkington, M (2015) *Blockchain Technology: Principles and Applications*, available at https://ssrn.com/abstract=2662660; Credit Suisse (2016). *ibid;* and Buterin, V (2015) *On Public and Private Blockchains,* available at https://goo.gl/l7ZoSk .
[37] In practice, the reason for the more or less hash rate – the measure of computational power being used on a blockchain - comes online (or goes offline) is that, for crypto currencies such as Bitcoin, it tracks the price of the cryptocurrency. Thereto, see Appendix B in Swanson (2015) *ibid.*

This however, increases not just the computational power (and cost) required to 'establish' trust (for example, a fee related to mining/buying a coin), but also increases the time (latency) for all the nodes on the blockchain to agree to what should be committed to the ledger.

2 DLT designs

2.1 Overview

As noted above, there are many different types of DLTs. While there are still significant challenges in the development and implementation of DLTs, many incorporate some or all of the following design features:

- cryptographic techniques to reach consensus on data entry and accuracy
- scalability
- transparency of data entry
- authentication of the entry of data
- disintermediation of trust
- replication of data to avoid single point of failure
- immutability of the data record
- evidence of tampering
- borderless
- quick to update
- permanent uptime
- access control & authentication through cryptographic keys
- smart, self-executing contracts.[38]

New DLTs are constantly being announced.[39] Hence, just a sample of these are enumerated below.[40]

2.2 Bitcoin

As noted earlier, Bitcoin is a cryptocurrency and is considered the first DLT.[41] It uses the public, permissionless, Bitcoin blockchain where each transaction is given a unique cryptographic number.[42] It also uses a POW consensus algorithm.

2.3 Ripple

Ripple developed the open source codebase that is used to run the Ripple Consensus Ledger (RCL). This is a distributed ledger which uses a digital currency – called XRP[43] – as its native asset. The Ripple network differentiates itself from most other DLTs in that it is designed specifically for payments and supports payments in any currency, including fiat currencies.

---

[38] Not all DLTs have smart contract capabilities. For example, Bitcoin lacks smart contract capabilities.
[39] For a sample of those announced up to November 2016, see Coindesk (2016) *State of Blockchain Q3 2016*, available at http://www.slideshare.net/CoinDesk/state-of-blockchain-q3-2016.
[40] The top 10 cryptocurrencies as of November 2016 were (in ranking order): Bitcoin, Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Steeem, Dash, NEM, and MaidSafeCoin. See Coindesk (2016) *6 Takeaways from CoinDesk's Q3 State of Blockchain*, available at https://goo.gl/JCFOSO .
[41] See Section 1.1; and Narayanan *et al (*2016) *ibid* for an extensive overview of Bitcoin technology.
[42] Blockchain technology is often incorrectly conflated with Bitcoin: although Bitcoin uses blockchain technology, other blockchains are, of course, not 'Bitcoin.'
[43] XRP was pre-mined. In other words, unlike some other virtual currencies like Bitcoin, XRP 'coins' were fully generated prior to their distribution.

The Ripple network's open payment network is underpinned by the RCL which is a simpler type of DLT, providing instant, certified, and low cost international payments targeted at banks and non-bank financial services companies.[44] Transactions on Ripple's DLT are validated by consensus rather than using a POW like Bitcoin. Participants must choose a set of validators on the network that they trust not to collude and then accept the consensus of this group of validators with regard to which transactions should be written to the ledger.

Payments across currencies are facilitated by the network's built-in order book and matching engine which will ensure that two or more trades between accounts are completed atomically. Its commercial cross-border payments solutions have evolved to predominantly make use of the Interledger Protocol[45] for cross-currency transactions, the RCL, and specifically XRP, are positioned as mechanisms for providing a frictionless, neutral digital asset that can be used as a bridge currency for cross-border payments, especially between lesser traded currencies.

2.4 Ethereum

Ethereum is an open-source, crowd-funded project, much like the Bitcoin blockchain. Ethereum has both permissionless and permissioned features: One can program and participate in Ethereum blockchains without special permission.

Ethereum allows a network of peers to administer their own smart contracts [46] via a decentralized virtual machine – the Ethereum Virtual Machine – to execute peer-to-peer contracts using a cryptocurrency called Ether and instructions which are often called EtherScript.[47] It uses a POW consensus algorithm, and is the prime DLT that uses smart contracts.[48]

2.5 Corda

Corda is a distributed ledger platform developed by R3, which includes a consortium of more than 70 of the world's major banks and insurers.[49] This DLT is designed to record, manage, and synchronize financial agreements between regulated financial institutions. It records an explicit link between human-language legal prose documents and smart contract code. Its design directly enables regulatory and supervisory Regulatory Technology (RegTech) observer nodes.

---

[44] Ripple (2014) *The Ripple Protocol Consensus Algorithm*, available at https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[45] Thomas, S and E. Schwartz (2014) *A Protocol for Interledger Payment*s, available at https://interledger.org/ .

[46] Short computer programs carried on the blockchain that execute their instructions once certain criteria have been met.

[47] Etherscripter (2016) *What Is Ethereum*, available at http://etherscripter.com/what_is_ethereum.html.

[48] See Section 4 on Smart Contracts. One example of the potential vulnerabilities in smart contracts is the effect on one employed by an Ethereum-derived investment platform investment capital called Distributed Autonomous Organization (DAO) whose financial transaction record and program rules were designed to be maintained on a blockchain. In June 2016, the DOA blockchain was found to have been exploited through a flaw in the Ethereum code, which if left unchecked, would have resulted in massive financial losses for DAO participants. After much discussion within the Ethereum community as to how to solve the issue, the community decided in July 2016 to 'hard-fork' the Ethereum blockchain. A hard fork is a backward-incompatible change in the blockchain design. The effect of this fork was to reverse the exploit and return funds to the DAO. The original Ethereum chain then adopted the name Ethereum Classic. This incident was the first time any mainstream blockchain was forked to reverse a transaction without a valid signature in order to make reparations to investors in a failed enterprise. Another hard fork was made to Ethereum in October 2016. See Coindesk (2016) *Nearly Half of All DAO Funds Withdrawn after Ethereum Hard Fork*, available at https://goo.gl/gn9Pyh .

[49] However, some banks left the consortium in 4Q2016.

Unlike Bitcoin's blockchain, which distributes the entire history of transactions among its nodes, with Corda, only verified transactions are shared in a way that only those parties with a legitimate need to know can see the data within an agreement.[50]

2.6 Microsoft Azure

Microsoft is providing 'blockchain-as-a-service' (BaaS) on their existing cloud platforms, allowing developers from any entity to deploy private or semi-public blockchains using Bitcoin, Ripple, Ethereum, R3, and other DLT protocols, and experiment with decentralized applications without incurring the capital costs associated with setting up their own networks.[51]

3 Key uses of DLTs

3.1 Overview

In the DFS ecosystem, in the financial industry, and in business networks generally, data and information usually flow through centralized, trust-based, third-party systems such as financial institutions, clearing houses, and other mediators of existing institutional arrangements.

These transfers can be inefficient, slow, costly, and vulnerable to manipulation, fraud and misuse.[52] Bilateral and multilateral agreements are needed,[53] which are typically recorded by the parties to the agreements in different systems (ledgers).[54]

As indicated above, a number of blockchains and DLTs have emerged in recent years that aim to address these issues. Each may have its own different use cases, offering benefits such as larger data capacities, transparency of and access to the data on the blockchain, or different consensus methods.

3.2 Application of DLTs

Some of the applications using DLTs could include the following:

- remittances
- identity (ID) Systems
- electronic know your customer (eKYC)[55]
- small medium enterprise (SME) finance
- digital rights management
- insurance contracts
- interoperability between banking and payment platforms
- clearing and settlement (C&S)[56]

---

[50] Bloomberg (2016) *Bitcoin and the Blockchain*, available at https://www.bloomberg.com/quicktake/bitcoins.
[51] Gray, M (2015) *Ethereum Blockchain as a Service Now on Azure*, available at https://goo.gl/2NttVV .
[52] Lack of transparency, as well as susceptibility to corruption and fraud, can lead to disputes.
[53] As transactions occur and data is transferred, the agreements and the data they individually control need to be synchronized. Often though, the data will not match up because of duplication and discrepancies between ledger transactions, which results in disputes, disagreements, increased settlement times, and the need for intermediaries (along with their associated overhead costs).
[54] See also IBM (2016) *Blockchain Basics: Introduction to Business Ledgers*, available at https://goo.gl/dajHbh .
[55] This would, with current developments, be more applicable to identity systems rather than national identity systems. It can be applied then to digital identity, with notes that certain attributes have been attested by certain authorities. The keys associated with the identity, and the details of the attributes and the associated attestations, would be held in a separate secure identity store, under the control of the individual. One of the attributes might be name – attested to by the national identity service. The identity on the blockchain would be derived from that.
[56] See Mills *et al* (2016) *ibid.*

- shareholder voting[57]
- credit provision
- trade finance
- clearing houses[58]
- share registries
- property registration
- notarization of data[59]
- supply chains
- correspondent banking.[60]

Further applications of DLTs to financial inclusion and DFS are explored in Section **Error! Reference source not found.**.

4 Smart contracts

4.1 Overview

Some[61] DLT implementations have built-in intelligence, setting (business logic) rules about a transaction as part of what is called a 'smart contract.[62] The smart contract can execute in minutes.

4.2 Nature of smart contracts

Smart contracts are contracts whose terms are recorded in blockchain code and which can be automatically executed. The instructions embedded within blocks – such as 'if' this 'then' do that 'else' do this – allow transactions or other actions to be carried out only if certain conditions are met. Smart contracts are – and must be – executed independently by (user) every node on a chain.

Smart contracts are tied to the blockchain-driven transaction itself. For example, in the Ethereum blockchain, its EtherScript programming language allows the use of natural language 'notes' in an EtherScript that helps improve human readability in smart contracts. These notes are analogous to the wording in a separate (physical) legal contract. The physical contract signature is replaced by the use of cryptographic keys that indicate assent by participant nodes to the 'legal' terms embedded in the blockchain by the EtherScript.

In all then, a legal contract is replaced by computer code, and consequently the need for lawyers to be involved in the chain of execution of the smart contract is mistakenly thought by some to

---

[57] ZDNET (2016) *Why Ripples from this Estonian Blockchain Experiment may be Felt around the World*, available at https://goo.gl/eaLf3G .

[58] The Depository Trust and Clearing Corporation, the company that serves as the back end for much Wall Street trading and which records information about every credit default swap trade, is replacing its central databases as used by the largest banks in the world with blockchain technology from IBM. See NY Times (2017) *Wall Street Clearinghouse to Adopt Bitcoin Technology*, available at http://nyti.ms/2iac0iM.

[59] Bitcoin Magazine (2015) *Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents*, available at https://goo.gl/YdoYKq .

[60] See, for example, US Bank Wells Fargo and Australia's ANZ who have built a shared distributed ledger platform prototype for correspondent banking payment reconciliation and settlement. Wells Fargo (2016) *Distributed Ledger Technology and Opportunities in Correspondent Banking*, available form https://goo.gl/X0gmS6 .

[61] Not all DLTs support smart contracts. Bitcoin, for example, does not support smart contracts. The Ethereum DLT is the prime exemplar of the use of smart contracts.

[62] Smart contracts were first described in 1997, relating to vending machines. See Szabo, N (1997) *Smart Contracts: Building Blocks for Digital Markets.*

be redundant.[63] However, compliance rules with one or more of the counterparties – or through peremptory regulations such as those dealing with anti-money laundering (AML) rules or the implication of tax laws – would probably require proper legal counsel.

4.3 Opportunities and challenges with smart contracts

The potential benefits of smart contracts include low contracting, enforcement, and compliance costs. They consequently make it economically viable to form contracts for numerous low-value transactions. Smart contracts then could be successfully applied in e-commerce, where they can significantly facilitate trade by reducing counterparty risk and the costs of transacting by minimizing the human factor in the process.

In a practical use case example, where a contract between parties to purchase a property asset is written into a blockchain and a set triggering event, such as a lowering of interest rates to a certain level is reached, the contract will execute itself according to the coded terms and without any human intervention. This could in turn trigger payment between parties and the purchase and registration of a property in the new owner's name.

The smart contract may also make the need for escrow redundant. The legal impact is established through the smart contract execution, without additional intervention. This methodology contrasts with the conventional, centralized ID database in which rules are set at the entire database level, or in the application, but not in the transaction.

In another example, national IDs could be placed on a specific blockchain, and the identifiable person could embed (smart contract) rules into their unique ID entry, allowing only specific entities to access their ID for specific purposes and for a certain time. The person can, through the blockchain, monitor this use.

Potential risks to smart contract technology include: A reliance on the computing system itself that executes the contract; flaws in the smart contract code; or the reliance on an external 'off chain' event or person – to integrate with and execute – the embedded terms of the smart contract.[64]

Although 'digital events' may seamlessly trigger a smart contract, initiation of a digital event from the physical (external) world could be problematic. For example, if a smart contract retrieves some information from an external source, this retrieval must be performed repeatedly and separately by each user node. But, because this source is outside of the blockchain – known as 'offchain,' there is no guarantee that every node will receive the same answer, and at the same time.[65] Or, as has been suggested,[66] perhaps the source will change its response in the time between requests from different nodes, or perhaps it will become temporarily unavailable.

---

[63] PWC (2016) *Blockchain and smart contract Automation: How smart contracts Automate Digital Business*, available at http://www.pwc.com/us/en/technology-forecast/blockchain/digital-business.html Etherscripter (2016) *What is Ethereum*, available at http://etherscripter.com/what_is_ethereum.html.

[64] See further, Kakavand, H (2016) *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, available at https://ssrn.com/abstract=2849251.

[65] This may be particularly pronounced with DLTs with high latencies, whereby the nodes all need to be communicated with, and their responses obtained.

[66] See Olickel, H (2016) *Why Smart Contracts Fail: Undiscovered Bugs and What We Can Do About Them*, available at https://goo.gl/0PTBIm .

In either of these scenarios, the consensus necessary for the blockchain to be in sync may be broken. Three possible solutions have been proposed – multi-signature transactions,[67] prediction markets,[68] and oracles[69] – but all require the intervention of humans, in a group or individually.[70] This need does undermine the DLT goal of a decentralized automated system. Automated performance also does not guarantee that parties will always, or even often, be capable of determining all eventualities, as what happens after parties strike a deal is often unpredictable.[71]

There are also reportedly flaws prevalent in smart contract blockchain codes:[72] while there have been important academic studies of vulnerabilities in blockchain,[73] automated software applications that may detect these flaws before they are exploited and lead to loss are only now being developed.[74]

5 Challenges in implementation of DLTs

5.1 Overview

DLT provides opportunities to innovators and may challenge the current role of trusted intermediaries that have positions of control within a centralized hierarchy.[75] But while the technology matures and the 'tires are kicked', there are current and evolving concerns that will need to be addressed in both developed and developing world contexts. These range from confidentiality of data, user privacy, security of blockchains, legal and regulatory issues, and fragmentation of the technology, as well as the veracity of the data placed on a blockchain.[76]

5.2 Privacy and confidentiality of data

Current methods of data storage on centralized systems have always been vexed by attempted and successful intrusions.[77] Database controllers attempt to harden these systems against data compromise and leak of private and confidential information through *inter alia* tightly

[67] Multi-signature transactions require a trust agent to be involved to ensure that the conditions for triggering the contract between the parties have been met and the contract can be executed. LTP (2016) *Blockchain-Enabled Smart Contracts: Applications and Challenges,* available at https://goo.gl/fzwLSR .

[68] The accuracy of prediction markets rests in the idea that the average prediction made by a group is superior to that made by any of the individuals in that group. The economic incentive can be built in a way so that it rewards the most accurate prediction. For an example of implementation of predictive market technology built on the Ethereum blockchain, see www.augur.net. See also LTP (2016) *ibid*; and Needham (2015) *ibid*.

[69] Oracle services are third-parties that are verifying the outcome of the events and feed the data to smart contracts data services. However, the issue of trust of these oracles has been raised. LTP (2016) *ibid.*

[70] See Shabab, H (2014) *What are Smart Contracts, and What Can We do with Them?*, available at https://goo.gl/xpG0FS ; and Wright, A and De Filippi, P (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, available at https://ssrn.com/abstract=2580664.

[71] Shabab (2014) *ibid*

[72] See in relation to issues discovered with the Ethereum blockchain; Buterin, V (2016) *Thinking About Smart Contract Security*, available at https://goo.gl/iH78GN ; and Daian, P (2016) *Chasing the DAO Attacker's Wake*, available at https://goo.gl/DxgOHD.

[73] See Cornell Sun (2016) *Cornell Prof Uncovers Bugs in Smart Contract System, Urges More Safety in Program Design*, available at https://goo.gl/d6d4F2 .

[74] See Olickel (2016) *ibid*

[75] They also offer authorities a new, and almost real-time, access to data for compliance (RegTech) purposes, while blockchains such as Bitcoin that create new decentralized currencies may challenge the current supremacy of governments in managing the national and international economic and monetary systems. On the disruptive possibilities of DLTs and the implications, see Mills *et al* (2016) *ibid;* UK Government Office for Science (2016) *ibid*; Credit Suisse (2016) *Blockchain*, available at https://goo.gl/1YT6Ci; IBM (2016) *ibid*; Accenture (2016) *Blockchain Technology: How Banks Are Building a Real-Time Global Payment Network,* available at https://goo.gl/5bHSd4 .

[76] There are other challenges, but as noted earlier, these are beyond the scope of this paper.

[77] See for example, BI (2016) *1 Billion Yahoo Accounts Have Been Stolen in the Biggest Hack Ever — Here's What You Should do*, available at https://goo.gl/lnKf4j .

controlling access through just one or more trusted (central) parties and by encrypting databases.[78]

With the distributed node motif embedded in the DNA of most DLTs, they have a different perspective to the storage of data and access thereto. That is, data on blockchains in large measure should be visible to everyone – the nodes[79] – on that blockchain.[80] The ostensible reason for this is that to validate additions of data to the chain, nodes must have visibility over the data they are validating.[81] In theory then, everyone could see everyone else's data, at all times.

And, although access to a blockchain requires a private key, not all of the information on a blockchain is encrypted.[82] For example, on the Bitcoin permissionless, public blockchain, data is pseudo-anonymous: The user's ID is self-asserted and encrypted, but transactional data is not.

For financial institutions using permissioned, private blockchains, the visibility of commercially sensitive information – customers, transactions etc. – to everyone may be a serious barrier to adoption.[83] So, although a blockchain could potentially replace Society for Worldwide Interbank Financial Telecommunication (SWIFT)[84] for value transfer or a bank for settlement, it also means that *everyone* could see the transaction flows, since they are on the nodes and – intrinsically to the distributed nature of blockchain – would have to verify any transactions for that transaction to be placed on the block.[85]

There is thus a tension between shared *control* of data on a ledger – the core of the DLT motif – and *sharing* of the data on a ledger.[86]

Solutions to these issues are being developed, but not yet mainstream. For example, 'zero-knowledge proofs'[87] are emerging, potentially enabling validation of data without visibility over the underlying data itself. This is being applied in the crypto currency realm with Zcash,

[78] Of course, these characteristics have their advantages and disadvantages. That is, centralized access through trusted parties, but a potential single point of failure where an intrusion could expose data.
[79] These nodes may be trustless.
[80] As noted below, some newer blockchains design solutions so that some parties can only read the blockchain, while others can also sign to add blocks to the chain
[81] Even so, there have been instances where identities of blockchain users have been discovered using transaction graph analysis. This uses the transparency of the transaction ledger to reveal spending patterns in the blockchain that allow bitcoin addresses – using IP addresses and IP address de-anonymization techniques - to be bundled by user. Ludwin, A (2015) *How Anonymous is Bitcoin? A Backgrounder for Policymakers,* available at https://goo.gl/DJnIvP .
[82] This also depends on the blockchain design. A blockchain can have all of its data encrypted, but signing/creating the blockchain wouldn't necessarily be dependent on being able to read the data. An example may be a digital identity blockchain.
[83] For discussions of these potential tradeoffs and concerns, see Kosba, A *et al* (2016) *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, available at https://eprint.iacr.org/2015/675.pdf; Greenspan, G (2016a) *Blockchains vs Centralized Databases*, available at https://goo.gl/gKfoym ; and R3 (2016) *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services,* available at https://goo.gl/IgD1uO ; and Deloitte (2016) *Blockchain: Enigma. Paradox*, *Opportunity*, available at https://goo.gl/yNjtFE ; and Irrera, A (2016) *Blockchain Users Cite Confidentiality As Top Concern*, available at https://goo.gl/IIuuua .
[84] Society for Worldwide Interbank Financial Telecommunication (SWIFT) - supplies secure messaging services and interface software to wholesale financial entities.
[85] See further Greenspan, G (2016b) *Understanding Zero Knowledge Blockchains,* available at https://goo.gl/r9P4jZ . Greenspan is founder and CEO of Coin Sciences, a company developing the MultiChain platform for private blockchains.
[86] Lewis, A (2017) *Distributed Ledgers: Shared Control, Not Shared Data*, available at https://goo.gl/KieCHG .
[87] In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. Quisquater, J-J, (2016) *How to Explain Zero-Knowledge Protocols to Your Children*, available at http://pages.cs.wisc.edu/~mkowalcz/628.pdf.

an emerging decentralized and open-source cryptocurrency that competes with Bitcoin and which purports to offer privacy and selective transparency of transactions.[88]

There is also R3's Corda blockchain technology – supported by over 70 banks and insurance companies worldwide – that shuns, in its design, global sharing of data such that only those parties with a legitimate need to know can see the data placed within an agreement on the blockchain.[89]

Digital Asset Holdings has also announced a 'fingerprinting' model to address privacy concerns: Though these fingerprints with blockchain data are shared amongst all users of a given blockchain, only trusted parties will be able to decipher them.[90]

And, for smart contracts, Hawk has been announced: It is a decentralized smart contract system that does not store financial transactions in the clear on the blockchain, retaining transactional privacy from the public's view.[91]

5.3 Security of DLTs

There have been very high-profile intrusions into the 'vaults' that store Bitcoins, resulting in huge loses for Bitcoin holders.[92] But while Bitcoin storage facilities have been compromised, there are no reports to date of the Bitcoin blockchain *itself* being compromised.[93]

Nonetheless, the underlying code in any blockchain may be a security issue: The exploitation of a flaw in the Ethereum blockchain led to the immutability paradigm of blockchain being necessarily violated by its creators to restore (potentially) lost funds.[94]

Despite the use of strong cryptography, DLTs are not necessarily a panacea for security concerns people may have.[95] Indeed, there is a tradeoff between replacing costly – and often risky – intermediaries with cryptographic key-only access distributed across nodes.[96] For example, for permissioned ledgers replacing centralized intermediaries, the cost-benefit in using blockchain is somewhat ameliorated by the need to trust permissioned authors rather than relying solely on the nodes who offer the guarantee of ledger integrity.[97]

---

[88] Zcash payments are published on a public blockchain, but the sender, recipient, and amount of a transaction remain private. Zcash uses different encryption approaches to keep both transactions and identities private. See https://z.cash/about.html?page=0a.

[89] R3 (2016) *ibid*

[90] Leising, M (2016) *Blythe Masters Unveils Fix for Blockchain Privacy Concerns*, available at https://goo.gl/KblSLm.

[91] Kosba *et al* (2016) *ibid*

[92] Reuters (2016) *Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong*, available at http://reut.rs/2atByqe.

[93] Compromised in the sense that data on the blockchain was altered without consensus of all the user nodes in the blockchain.

[94] Hertig, A (2016) *The Blockchain Created by Ethereum's Fork is Forking Now*, available at http://www.coindesk.com/ethereum-classic-blockchain-fork-ddos-attacks/.

[95] For public, permissionless (trustless) blockchains like Bitcoin where the use of nodes on the blockchain are publicly used to verify transactions is a core feature, security of its blockchain – and not the vaults bitcoins are stored in - is ensured by syntactic rules and computational barriers to mining. See also Greenspan (2016b) *ibid.*

[96] There is arguably also a trade-off in DLTs between security and transaction processing speeds. For a technical discussion thereof, see Kiayias, A and Panagiotakos, G (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at https://goo.gl/bgsTR8.

[97] The counterargument could be that a properly designed 'permissioned' network would be designed so that there is no single-point of failure or central administrator who can unilaterally change the state. See Swanson (2015) *ibid.*

The issues are said to be thus: The more trusted parties per node that are needed, so too does the compromisable 'surface area' of a distributed network increase.[98] Also, requiring a third party private key management function is contradictory – and possibly even nugatory – to the core 'disintermediation' principles of DLTs. In all, these tradeoffs may arguably reduce the utility of DLTs.

Authorized access is also an issue: Nodes on the blockchain are – using current protocols – said to be unable to distinguish between a transaction by an authorized, actual user and a fake transaction by someone who somehow has gained access to the blockchain trusted party's private key.[99] This means that if a bad actor gains access to a comprehensive banking blockchain that itself accesses all or of part of a core banking network blockchain – or a real-time gross settlement system – then this breach would in effect be compromising all banks' databases simultaneously.[100]

Risk for loss of funds where credentials are controlled by a single entity was demonstrated in the recent compromise of the credentials used in the transfer of funds through the (non-DLT) SWIFT network from the Federal Reserve Bank of New York[101] to the central bank of Bangladesh, Bangladesh Bank.[102] To circumvent or mitigate this type of risk, private key management functions or biometric linked private keys have been suggested.[103]

The issue of longevity of the security of blockchain-based data may also be an issue. For example, the possibility of 'old' transactions on a particular blockchain may be vulnerable to advances in cryptography over a period of years or decades such that 'old' transactions can be undetectably changed.

A type of equivalence to this issue would be security compromises of the circa-1980s GSM – and later generations of – mobile communications encryption specifications affecting feature (non-smart) phones whose firmware cannot easily be updated with a fix for any vulnerabilities. The ability then to upgrade the cryptographic techniques used for 'old' transactions should be considered in DLT designs.

5.4 Fragmentation in DLTs

DLT-based solutions intrinsically rely upon multiple users for achieving critical mass: Nodes need more nodes to distribute the data, to do the validations of the blocks in the process of being added, and to do the processing itself.[104] Widespread adoption then is essential for the positive network effect of DLTs to be truly harnessed as a single entity using blockchain could be seen as analogous to a centralized database.[105] Although good and important work is being

[98] Credit Suisse (2016) *ibid;* and Kaminska, I (2016) *How I Learned to Stop Blockchain Obsessing and Love the Barry Manilow*, available at https://goo.gl/mv3Lcy.
[99] Vermont (2016) *ibid*
[100] Greenspan (2016a) *ibid*
[101] The Federal Reserve Bank of New York is one of the 12 Federal Reserve Banks of the United States.
[102] Reuters (2016) *Exclusive: New York Fed Asks Philippines to Recover Bangladesh Money*, available at https://goo.gl/yqaJh7 .
[103] Vermont (2016) *ibid*
[104] Metcalfe's Law says that the value of a network is proportional to the number of connections in the network squared. Shapiro, C and Varian, HR (1999) *Information Rules*. Similarly, per Paul Makin, the more people who have an identity on blockchain where nodes can attest to the authenticity of the correct people being identified, the more entities will take the trouble to be part of the acceptance network for that blockchain; that is, entities will join that blockchain to make use of the identity functionality it provides.
[105] Credit Suisse (2016) *ibid*

done by the various DLT consortia, this may yet lead to silo'ed – and incompatible – blockchain initiatives.[106]

So-called 'forking' of existing DLTs may also introduce fragmentation and slow down transaction processing speeds.[107] There are a number of classifications of 'forks,' which include forks, hard forks, soft forks, software forks, or git forks.[108]

Although the various DLT initiatives may address different market sectors and thus require nuanced design and implementation, some level of consistency between at least similar implementations is desirable to avoid unnecessary fragmentation that would delay the emergence of industry 'standards' for a sector. Besides, interoperability required to connect these silos may introduce security and efficiency risks to the respective blockchain operations.

5.5 Validity of records

Although the data on a blockchain is said to be secure, and any data input authenticated, the DLT does not address the reliability or accuracy of the data itself. Blockchain thus only addresses a record's authenticity by confirming the party or parties submitting a record, the time and date of its submission, and the contents of the record at the time of submission,[109] and not the *reliability* or *accuracy* of the records contained in the blockchain.

If a document containing false information is hashed – added to the blockchain – as part of a properly formatted transaction, the network will and must validate it.[110] That is, as long as the correct protocols are utilized, the data inputted will be accepted by the nodes on a blockchain. This is the DLT incarnation of the unfortunate mantra of 'garbage data in, garbage data out' which is usually characteristic of some databases in the non-DLT world.

The possibility has also been raised[111] of an individual participant on a blockchain showing their users an altered version of their data whilst simultaneously showing the unedited (genuine) version to the other participant nodes on the blockchain network.

Others may only be able to trust the data on the blockchain if they can cross-validate data across multiple user nodes.

---

[106] On the other hand, concentration of use in just one blockchain type could also possibly trigger competition-related issues.
[107] See Section 5.6 below. Upgrading of a blockchain may require multiple consensus steps. For example, to upgrade the blockchain which Bitcoin uses requires a Bitcoin Improvement Proposal (BIP) design document for introducing new features since Bitcoin has no formal structure. See Anceaume, E *et al* (2016) *Safety Analysis of Bitcoin Improvement Proposals,* available at https://goo.gl/MO3JBb .
[108] Although there is no consensus on terminology, the various types of 'forks' that are generally possible have been classified by the Bitcoin community into forks, hard forks, soft forks, software fork or git fork. A hard fork, classified as a permanent divergence in the blockchain, commonly occurs when non-upgraded nodes can't validate blocks created by upgraded nodes that follow newer consensus rules. A fork is a regular fork where all nodes follow the same consensus rules, so the fork is resolved once one chain has more proof of work than another. A soft fork is a temporary divergence in the blockchain caused by non-upgraded nodes not following new consensus rules. A software fork is when one or more developers permanently develops a codebase – a collection of source code – separately from other developers. A git fork is when one or more developers temporarily develop a codebase separately from other developers. See Bitcoin (2016) *Hard Fork, Hard-Forking Change*, available at https://bitcoin.org/en/glossary/hard-fork. However, other definitions may be used to describe the type of forks. For alternative classifications, and solutions to the identified forks, see Blockchain (2016) *A Brief History of Bitcoin Forks,* available at https://goo.gl/o3XDmk .
[109] These records may in fact be encrypted.
[110] Vermont (2016) *ibid*
[111] Lewis (2017) *ibid*

5.6 Speed of processing

Speed of transactions is still an issue though: Some DLTs currently have substantially slower transaction speeds due to POW or POS or other requirements.[112] Even so, for DLTs to scale to compete with, for example, existing payment processing platforms, changes to processing techniques must be implemented.[113]

This may also involve implementing systems providing short-term 'float' insurance for (slow) transactions.

6 Policy, regulatory, and legal issues relating to DLTs

6.1 Overview

Just as the emergence of the Internet upended laws, regulations, policies, and internal rules of the time, DLTs may provide an impetus for new sets of laws, regulations, policies, and internal rules.

As was shown with the emergence of the Bitcoin cryptocurrency, regulators were unable to quickly respond to the Bitcoin phenomenon as it gained traction in many markets. As such, in a more visceral reaction than a considered policy approach, some countries placed restrictions or bans on the use of Bitcoin and/or the trading thereof.

Of course, DLTs are not Bitcoin, and although innovation and application of new technologies continues generally and use of DLTs continues unabated, there is still concern within enterprises as to the impact DLTs may have on general compliance. A 2016 survey by consulting group Accenture indicated that regulatory and compliance concerns are delaying application of DLTs by many entities.[114]

Besides the policy issues – that is, how far (if at all) can DLTs be implemented in specific sectors – there are also open legal issues to consider.[115]

6.2 Regulatory and policy responses to DLT

DLTs have prompted varying responses by regulators. Bitcoin, the first DLT, was met with a mixed response by many regulators.[116] This speaks to the fact that many regulators are still attempting to develop the capacity to understand DLTs so as to develop proper responses to the multitude of legal, regulatory, policy, financial, and security issues DLTs precipitate.[117]

---

[112] In comparative processing statistics quoted by Kiayias & Panagiotakos, the current rate for Bitcoin processing is seven transactions per second (tps), compared to payment service provider Paypal which handles an average of 115 tps. The VISA network has a peak capacity of 47,000 tps. See Kiayias & Panagiotakos (2015) *ibid*. SafeCash claims though to handle up to 25,000 tps. See Market Wired (2016) *Safe Cash Speeds up Blockchain to 25,000 Transactions Per Second,* available at https://goo.gl/yEJVjm .

[113] As with legacy systems, DLT-based systems may also be slowed due regulations and compliance requirements. Although high latencies due to technology design may also cause slowdowns, there are initiatives trying to improve DLT transaction speeds.

[114] Accenture (2016) *ibid*

[115] Some of these issues are described below in Section 6.

[116] See IMF (2016) *Virtual Currencies and Beyond: Initial Considerations*, available at https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

[117] For example, see China's central bank, which is hiring blockchain experts. QZ (2016) *China's Central Bank Is Hiring Blockchain Experts to Help It Kill off Cash*, available at https://goo.gl/QTaOyt.

Responses thus far have been more strategic,[118] with some financial regulators embracing the concept of a 'regulatory sandbox' that may allow beta testing of DLTs – and other FinTech – applications.

These 'sandboxes' have been created or are in the process of being created in the US, Singapore, UK, Australia, and Abu Dhabi.[119] The UK Financial Conduct Authority, for example, has started a FinTech sandbox program, which allows a limited launch of FinTech applications, products, and services. In the US, a bill has been proposed to mandate federal support for FinTech sandboxes.[120] In Singapore, the Monetary Authority of Singapore (MAS) recently published its FinTech regulatory sandbox guidelines.[121]

Beyond creating the necessary regulatory framework to consider DLTs and other innovative technology/processes, regulators have also been specifically looking at DLTs and how to embrace their positive attributes. The European Commission plans to set up a FinTech task force that will look at all emerging technologies including those linked to blockchain virtual currencies.[122] In the UK, the Government Office for Sciences published a generally positive report and recommended embracing DLT for specific purposes, describing developments as potentially catalyzing 'exceptional levels of innovation.'[123]

Over and above policy support for DLT development, certain regulators and governments are embracing DLT themselves. In Singapore, the MAS is fully embracing DLT in partnering with R3 and a consortium of financial institutions on a proof of concept (POC) project to conduct inter-bank payments using blockchain.[124] The project will develop a pilot system in which blockchain infrastructure is used to issue and transfer funds among participants.

The Republic of Georgia is using DLTs for property registries,[125] a common approach by other governments looking for public-good uses of DLT. In a discordant note on the limits of DLTs, the US state of Vermont undertook a feasibility study for use of DLTs for public records but decided against its use primarily because of cost and the need to adapt existing state record-keeping structures.[126]

The Dubai government announced that it plans to use blockchain technology for all government documents by 2020,[127] while in South Africa, the South African Reserve Bank is part of the new Blockchain Working Group along with its central securities depository and several of the

[118] For example, see the US Securities and Exchange Commission, which has created a DLT Working Group to consider the uses, effects and regulations of DLTs. Coindesk (2016) *Blockchain Won't Just Change Regulation, it Could Reshape the SEC*, available at http://bit.ly/2eWQQQv.
[119] See Mondato (2016) *The Regulatory Sandbox*, available at http://blog.mondato.com/the-regulatory-sandbox/.
[120] Finance Two Zero (2016) *U.S. Government Sandbox Program to keep FinTech Applications in Play*, available at https://goo.gl/660pjU .
[121] Crowdfunding Insider (2016) *Monetary Authority of Singapore Issues FinTech Sandbox Guidelines,* available at https://goo.gl/L4OcWW .
[122] Arstechnica (2016) *European Parliament Votes for Hands-Off Approach to Blockchain Tech Regulation*, available at https://goo.gl/P4FW75. There is also D-CENT (Decentralised Citizens Engagement Technologies), an EU project that has proposed the creation of a social blockchain toolset that will allow adopters to generate their own alternative currency. See http://dcentproject.eu.
[123] UK Government Office for Science (2016) *ibid.*
[124] MAS (2016) *MAS, R3 and Financial Institutions experimenting with Blockchain Technology*, available at https://goo.gl/zCu8C1 . See Section 4.3 .
[125] See Section 7 below.
[126] Vermont (2016) *Blockchain Technology: Opportunities and Risks,* available at https://goo.gl/6SA2Hf
[127] Gulf Business (2016) D*ubai to Use Blockchain Technology for All Government Documents By 2020*, available at https://goo.gl/76vICG .

country's largest banks, aiming to chart a course toward large-scale blockchain implementation.[128]

And in France, the Banque de France has tested blockchain technology for hypothetical use in the management of Single Euro Payments Area (SEPA) credit identifiers.[129]

Similarly, many technology companies and financial institutions have been working on the adoption of voluntary guidelines and self-regulation to promote best practice.[130]

6.3 Legal and regulatory issues with the use of DLTs

DLT and the possibilities of its use in multiple economic sectors – from property registration, to remittances, trade finance, identity management, to share trading and certificates – pose bigger sets of legal and regulatory challenges.

At a regulatory level, some of the questions that have been raised[131] include how to apply consumer protection measures, how to apply AML measures, and use of identities registered in one jurisdiction in others.

At a legal level, the issues relate to how specific DLTs would interact with current laws and regulations governing (these) specific sectors, and common law rules (where used) that are needed where regulations are silent.[132]

That said, the legal issues that would appear to be most pertinent to DLTs include: The legality of smart contracts; place of contracting using a blockchain; chain of legal liabilities; and time of contracting using a blockchain.

All these open (and evolving) legal issues suggest that embracing of DLT for mainstream commercial and public use requires both doctrinal and legislative shifts.

7 Application of blockchain/DLT technology to financial inclusion

7.1 Overview

Currently, the foundational layer and infrastructure necessary to support a rich ecosystem of DLT-based applications and services is being established. The robustness of the technology has piqued the interest of financial institutions, regulators, central banks, and governments who are now exploring the possibilities of using DLTs to streamline a plethora of different public services.

Billions of dollars are being spent on applications of DLTs, from new national ID systems where a person can be provided with a unique ID that they can share; to tracking of assets; to

[128] CoinDesk (2017) *South Africa's Financial Power Players Are Going All-In on Blockchain*, available at http://bit.ly/2khelqQ .
[129] These are identification markers used to establish the identity of creditors within the Single Euro Payments Area. See CoinDesk (2016) *France's Central Bank Details its First Blockchain Test*, available at https://goo.gl/F9EZks .
[130] Norton Rose Fulbright (2016*) Financial Institutions and Blockchain Technology*, available at https://goo.gl/e5ffsM .
[131] *ibid*
[132] A simple example would relate to which laws and regulations would be applicable when placing property registration on a public blockchain: conventional approach would be through property registration laws, and laws relating to electronic records and evidence.

settlement of financial transactions; to digital rights management; and to the development of cryptocurrencies such as Bitcoin.[133]

Trials using DLTs for international settlement have shown great promise and may find application to remittances, S&C, cross-border currency exchanges, and interbank transfers. A survey by Accenture showed that the current state of financial institution interest or adoption of DLTs is in the POC phase.[134]

7.2 C&S

Financial services firms can minimize operational complexity with the use of DLTs. Systems that rely on trusted intermediaries to support and/or guarantee the authenticity of a transaction today could instead be efficiently conducted using DLTs.[135]

Currently, C&S between parties may take up to two to three days to achieve, leading to credit and liquidity risks. C&S time can be reduced to minutes with DLTs. Private, permissioned blockchains between banks – such as R3's Corda, described above[136] – could potentially authenticate transactions and undertake C&S considerably faster.[137]

This may help to reduce counterparty credit risk, which in turn may reduce an institution's capital requirements, collateral, or insurance where required by regulation to prevent settlement default.

Permissioned, private blockchains achieve this savings by removing the need for trusted intermediaries and granting the counterparties real-time visibility to their respective liquidity positions whilst undertaking netting. Similarly, this real-time liquidity visibility allows DFS providers to use DLTs to remove the need for prefunding in bilateral interoperability designs.[138]

7.3 Remittances

Current business models for remittances are relatively centralized: Payments sent and received between entities are costly, time consuming, error prone, and subject to widespread fraud and potential money laundering.

As a result, the time and cost efficiencies could support large amounts of small transactions or micro transactions, which are essential for bringing underbanked and unbanked individuals into the formal economy. DLTs aim to reduce the cost of a cross-border transfer by reducing the costs of C&S time and finding better exchange prices.

Two companies, Stellar, which operates as a decentralized protocol for fund transfers, and Oradian, a cloud-based software provider for microfinance institutions, have partnered to bring

[133] Needham, C (2015) *The Blockchain Report: Welcome to the Internet of Value,* available at https://goo.gl/fje2p3 .
[134] Accenture (2016) *ibid*
[135] According to Santander Bank, blockchain could reduce banks' infrastructure costs attributable to cross-border payments, securities trading, and regulatory compliance by between US$15-20 billion per annum by 2022. CoinDesk (2016) *Santander: Blockchain Tech Can Save Banks $20 Billion a Year*, available at https://goo.gl/QHWN7Y ,
[136] See Section 2.3 on R3.
[137] However, transaction processing times, as noted above in Section 5.6, would need to improve.
[138] DFS providers in Tanzania use this bilateral interoperability mechanism.

instant money transfers to Nigeria using DLTs.[139] The National Bank of Abu Dhabi is introducing real-time cross-border payments using Ripple technology.[140]

It is important to note that, despite the great potential for DLTs in the area of payments, there are significant hurdles that remain for large-scale implementation, chief amongst them an uncertain and un-harmonized legal regulatory environment relating to the sending and receiving jurisdictions.[141]

For example, Kenyan-based remittance provider Bitpesa – which transfers value internationally via Bitcoin[142] – lost its court bid for an order that would have forced Kenyan mobile network operator (MNO) Safaricom to provide Bitpesa access to Safaricom's M-PESA DFS platform as a payment option for Kenyan Bitcoin buyers.[143] Safaricom had cited the uncertain regulatory environment in Kenya around Bitcoin as the reason for blocking Bitpesa from its platform.

7.4 Digital identities

Many unbanked individuals do not have access to traditional financial services because they lack verifiable ID or any identification at all. By using DLTs, individuals can receive a digital identity verified with biometrics which is securely stored and managed for transacting value nationally and internationally. Essentially, the identity manifests as a cryptographic key that the user can provide, using a specified biometric marker to verify and authenticate themselves when needed.[144]

As well as being seamlessly able to prove identity for access to government and commercial services, these enhanced privacy protections prevent use of that identity beyond what the individuals have authorized. BanQu,[145] Bitnation, and Onename are examples of companies using blockchain to help solve the identity problem.[146] By allowing this type of authentication – if done by a mobile device and seen as an acceptable ID for DFS know your customer (KYC) – this could be used to fulfill KYC remotely, which would allow for remote opening of DFS accounts, and thus the propagation of those accounts in rural areas with little access to banking branches or even MNO agents.

However, there are many challenges to introduction of these systems, most notably, the fact that much of the developing world is without any form of government-issued identification or even traditional documentation such as birth certificates. Proving actual birth identity *a priori* for inclusion on an ID blockchain is thus very challenging.

---

[139] It indicates that it allows 300,000 Nigerians to cheaply transfer money between microfinance institutions over the Stellar network. See TechCrunch (2016) *Stellar Partners with Oradian to Bring Instant Money Transfer to Nigeria*, available at https://goo.gl/mI0DLH . See also Abra, which uses a blockchain backend for cross-country remittances. It has operations in the Philippines and the US. www.goabra.com.

[140] Coindesk (2017) *Blockchain as a Geopolitical Tool*, available at http://bit.ly/2lf8B1K .

[141] See also Baruri, P (2016) *Blockchain Powered Financial Inclusion*, available at https://goo.gl/c2nIWr .

[142] Bitpesa enables the exchange of bitcoin for Kenyan Shillings, and allows users in Kenya, Nigeria, Uganda and Tanzania to send fiat funds to popular DFS wallets. It also has a corridor to China. See www.bitpesa.co

[143] CoinDesk (2015) *Kenyan Court Upholds Bid to Keep Bitcoin Startup off M-Pesa*, available from https://goo.gl/0tkjir .

[144] As noted earlier, an issue is whether identities registered in one jurisdiction can be seamlessly used for authentication purposes in another jurisdiction if dissimilar enrollment techniques are used.

[145] Private ID provider BanQu uses proprietary DLT to create unique, usable identity by creating a mash-up of a 'selfie' plus other key human characteristics for people with no access to technology or banking. That profile is recognized and accepted by financial institutions as legitimate identification information. See Banqu (2016) *Identity Process Flows*, available at http://www.banquapp.com/identity-process-flows.

[146] Inside Bitcoins (2016) *Blockchain Identity: Solving the Global Identification Crisis*, available at https://goo.gl/M7JoXu .

The issue of an ID that was enrolled at one institution for KYC purposes being fully accepted for KYC purposes at another institution is also an open question and may require legislative intervention.[147]

7.5 Property registers

Similar to identity, property, or land registry formalization, can be another hindrance for those financially excluded to enter or participate in a formal economy. Although people may own small plots of land, dwellings, vehicles, and equipment, they are not able to monetize these assets as collateral due to the lack of formal legal title to those assets.[148] The causes of this are said to be from poorly resourced and often corrupt bureaucracies.[149]

DLTs can help solve these encumbrances by lowering the cost of land titling and formalization through databases that work with the local governments to record and track land title transactions, allowing unbanked individuals to enter and benefit to some extent from the formal financial system.[150] Property titles could then be effected and verified without a centralized third party. In the Republic of Georgia, the National Agency of Public Registry plans to utilize a permissioned blockchain to develop a permanent and secure land title record system to track all land title transactions across the country.[151] Similar pilots in Ghana and Sweden use DLT as a decentralized land registry.[152]

However, high initial capital costs could, as with the adoption of any new technology, be a deterrent to the implementation of these systems, especially when there is no existing map of planned roads, land plots, or zones that indicate proper location or boundaries of the property. Barriers to reliable electronic land records are typically not in the data structure used to store them but in the acquisition of reliable source data.

7.6 Smart contracts

As noted earlier,[153] smart contracts that are self-executing and embedded into a blockchain can enforce legal contracts containing multiple assets and enforcement or performance triggers. This could relate, for example, a smart contract that provides insurance for crop failure whereby small farmers are automatically paid out by insurance companies based on externally-derived micro-climate pattern data linked to the smart contract that over a period, signals drought conditions.

[147] See ITU Focus Group Digital Financial Services Report *Identity and Authentication* (2017).
[148] De Soto, H. (2000) *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere.* Basic Books.
[149] Consumer's Research (2015) *The Promise of Bitcoin and the Blockchain* available at https://goo.gl/MzCGyh .
[150] This formalization of property provides a great many additional benefits, such as establishing the basis for legal protections for land ownership in the country, greater transparency within the economy, and the ability of landowners to participate further in the formal economy by using their land as collateral for financial products such as loans. Consumers Research (2015) *ibid*
[151] Coindesk (2016) *Republic of Georgia to Develop Blockchain Land Registry*, available at https://goo.gl/vZgGSi .
[152] Bitcoin (2016) *Bitland: Blockchain Land Registry Against Corrupt Governmen*t, available at https://goo.gl/gAVjGK; Coindesk (2016) *Sweden Tests Blockchain Smart Contracts for Land Registry*, available at https://goo.gl/YhNDSZ .
[153] See Section 3.

8 Conclusions

- DLT – exemplified by blockchain technology – potentially ushers in a scalable, robust, and smart next generation of applications for the registry and exchange of physical, virtual, tangible, and intangible assets and information, shared across the world between actors that do not trust – or even know – one another. The decentralized, transparent, immutable, and trustless nature of the DLTs may eliminate the need for some intermediaries, and theoretically could reduce settlement time, cost, and fraud in financial transactions.
- DLT is likely to be disruptive in terms of disintermediation of guarantors, authenticators, and trusted third parties, and could replace current procedures that process, record, reconcile, and audit transactions within a system where participants trade directly.
- For enterprises, compliance costs could be lowered through application of DLT-powered RegTech. Moreover, the KYC process could be streamlined as identities can be stored on the blockchain establishing trust and authenticity, and AML monitoring can be done in real-time based upon predefined conditions via the use of self-executing smart contracts.
- DLT is also likely to be beneficial to a number of important components that relate to financial inclusion, especially DFS and its adjacencies. On the horizon – if and when DLTs are applied correctly – are improved ID management through provision of DLT-powered IDs and thus facilitation of remote DFS account opening; seamless interoperability between DFS providers and banks without the need for providing costly collateral; the ability to secure property records, and then for citizens to use their property as collateral for loans, and similarly, the ability to source more readily available trade finance.
- For large-scale implementations of DLTs in financial processing, transaction speeds need to improve from current levels.
- From a privacy perspective, there is thus a tension between shared control of data on a ledger, and sharing of the data on a ledger.
- Undefined and un-harmonized regulatory environments and lack of a formal legal framework both on the national/regional and international level need to be resolved by financial institutions, governments, regulators, and other relevant participants for large scale implementation of DLT. Where possible, functional (and not institutional) approaches to any changes to applicable laws and regulations should be embraced. Regulatory (and legal) capacity to understand the technology, engage with industry, design policy around DLTs, and properly regulate as needed is critical to its use for financial inclusion.
- It may not always be possible to fit the use of DLT into existing financial laws and regulations. As a result, changes to laws or regulations, no-action relief, or interpretive guidance from regulators may be necessary.
- Regulatory sandboxes that allow DLTs to be tested in markets are emerging and should be embraced by regulators in a familiar form to that of the 'test and learn' regulatory philosophy of forbearance that bootstrapped the emergence – and global success – of DFS transactional platforms.

9 Recommendations

- Regulators who may be impacted by the emergence of DLTs should undertake capacity-building exercises with other regulators, government departments, academia, and the FinTech industry to build understanding of DLTs.
- Any changes to laws and regulations should use a functional approach to ensure that there are no technology-specific constraints to implementation of new technologies.
- As it may not always be possible to use existing financial laws and regulations for DLT, changes to laws or regulations, no-action relief, or interpretive guidance from regulators may be necessary.
- DLTs should be tested though regulatory sandboxes, in similar form to that of the 'test and learn' regulatory philosophy used for the first DFS implementations.

Annex A
How a blockchain operates

Data in a blockchain is stored in fixed structures called 'blocks,' which consist of a header and the blockchain's content. The block header includes metadata, such as a unique block reference number, the time the block was created, and a link back to the previous block.

The block data – its content – is usually a validated list of digital assets and instruction statements, such as transactions made, their amounts, and the addresses of the parties to those transactions. The blocks are stored one after the other in a continuous ledger, but they can only be added when the participants – nodes in a distributed network – reach a quorum (*consensus*). The nodes on the blockchain independently verify transactions before agreeing on those that are valid.[154]

As shown below,[155] the chain is *only* appended, *never* retrospectively edited – the key design feature of blockchains that facilitates immutability of the data placed on the blockchain.[156] DLTs then are tamper evident. Such that any edits will be obvious to others in ways that will prevent their broad uptake on the chain.

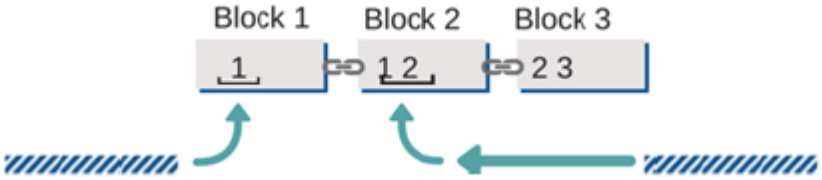

Exhibit 3: How blocks are added to a blockchain

The link that ties individual blocks together is the timestamp. Recording the timing of the transaction is essential to the nature of the blockchain. Each record is time/date stamped and provided with a unique cryptographic signature, which is designed to ensure the authenticity and integrity of the ledger.[157]

Using the latest block, it is possible to access all previous blocks linked together in the chain, so a blockchain database retains the complete history of all assets and instructions executed since the very first one.

This makes the data in a blockchain verifiable and independently auditable. Once placed on the blockchain, data on the blockchain is said to be 'hashed.'

---

[154] Vermont (2016) *ibid*
[155] Image from Vermont (2016) *ibid*
[156] Deloitte (2016*) ibid*
[157] McLean, S and Deane-Johns S (2016), D*emystifying Blockchain and Distributed Ledger Technology – Hype or Hero?*, available at https://media2.mofo.com/documents/160405blockchain.pdf ; de Meijer, CRW (2016) *ibid*