SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2015-007

# THE IMPACT AND POTENTIAL OF BLOCKCHAIN ON THE SECURITIES TRANSACTION LIFECYCLE

MICHAEL MAINELLI

ALISTAIR MILNE

PUBLICATION DATE: 09 MAY 2016

# The Impact and Potential of Blockchain on the Securities Transaction Lifecycle*

*Michael Mainelli† and Alistair Milne‡*

## Abstract

This paper reports the outcome of a series of interviews and focus group meetings with professionals working in post-trade processing and the provision of mutual distributed ledger services. The objective was to elicit and document views on three research hypotheses about the potential impact of mutual distributed ledger technology ('blockchain') on post-trade processing global securities markets. These hypotheses are (a) on the appropriate access to mutual distributed ledger; (b) on whether change would be piecemeal or 'big bang'; and (c) on the extent to which applying mutual distributed ledger in securities settlement would require major changes in business processes. Our research finds that while the use of blockchain to validate operational data in mutual distributed ledgers can yield substantial reductions in both cost and risk, the concept of data sharing itself is far from new. Current interest in mutual distributed ledgers has established significant momentum, but there is a danger of building unrealistic expectations of the extent to which the technology on its own will address the underlying need for co-ordination of business processes both within and between firms. Achieving all the potential benefits from mutual distributed ledgers will require board level buy-in to a substantial commitment of time and resource, and active regulatory support for process reform, with relatively little short term payoff. (214 words)

Keywords: Open source software, databases, distributed ledgers, fintech, securities settlement, Bitcoin

JEL numbers: G29, L17, L89

---

* We are grateful for the support of the SWIFT Institute from a research grant awarded in September 2015 and for participation in interview and focus group meetings and comments on earlier drafts from a large number of individuals (see Appendix 3 for a listing of their firms or other affiliations).
† Z/Yen Group, michael_mainelli@zyen.com
‡ School of Business and Economics, Loughborough University, a.k.l.milne@lboro.ac.uk

# Table of Contents

## 1. Introduction

Mutual distributed ledgers (aka blockchains) record transactions and ownership using pervasive, persistent, and permanent data structures replicated across numerous computers.[1] The two principal technology components are public-key cryptography and 'peer-to-peer' or shared data storage. The end result is a data source that is simultaneously logically 'central' while technically 'distributed' across the computers on the network. The network of computers using the ledger can consult a single authoritative and immutable ledger of all the data transactions from the origin ('genesis') of the data structure. Everyone has the same 'view' of the same 'data', though they may be retrieving the data from different physical sources.

Nowadays the best known mutual distributed ledger is the Bitcoin 'blockchain'. This provides an indelible record of all of the cryptocurrency's transactions from when they first began on 3 January 2009, using a consensus process, known as 'proof of work' (Bitcoin mining) to ensuring that the thousands of active nodes on the Bitcoin network do indeed all have the same view of the underlying data to a very high level of cryptographic security.

The term blockchain comes from the cryptographic validation of Bitcoin transactions in blocks that combine several transactions together (the size of these blocks varies a great deal but can contain a thousand transactions or more). Once a block is validated by proof of work then the transactions it contains are permanently and irreversibly recorded in the blockchain across numerous machines with no single, or 'master', central record. Participants in the Bitcoin network can view the ledger transactions in the blockchain from thousands of different machines but always see the same history.

Mutual distributed ledgers are not new but, historically, they have suffered from two perceived disadvantages: insecurity and complexity. The robustness and relative

[1] In this paper we employ the following definitions. A **ledger** is a record of transactions; **distributed** means divided among several or many, in multiple locations; **mutual** is shared in common, or owned by a community; a **mutual distributed ledger (MDL)** is a record of transactions shared in common and stored in multiple locations; and **mutual distributed ledger technology** is a technology that provides an immutable record of transactions shared in common and stored in multiple locations. See Appendix 1 and also (Mainelli, 2016) for discussion of the terminology.

simplicity of the Bitcoin blockchain has drawn favourable comparisons with complex messaging and processes and the multiple requirements for storage used in most financial services, especially in wholesale financial markets' securities settlement messaging and processes. This, along with the substantial current regulatory and other cost pressures on capital markets firms, have focused many in the industry on the possibility of achieving substantial efficiency gains by applying mutual distributed ledgers to securities settlement. It is though as yet unclear clear to what extent the robustness and simplicity of the Bitcoin blockchain can be replicated when applied to the varied and substantial throughput of global financial market transactions, nor which of the many forms of mutual distributed ledger are best suited for post-trade processing and to what extent they should be applied.

Despite these uncertainties, strong claims are now being made about the potential of mutual distributed ledgers to reduce costs and risks. A number of initiatives applying mutual distributed ledger to securities settlement are now being pursued, attracting substantial investment from both major banks and venture capital funds. These employ a range of approaches. Some directly employ the Bitcoin blockchain, or a simulacrum thereof. Others employ other open source mutual distributed ledger software such as that offered by Ripple or Ethereum. Others are developing private, proprietary, or semi-public ledgers. The common feature – as highlighted by our preferred terminology 'mutual distributed ledger' and 'mutual distributed ledger technology' – is providing a common view of ownership and other data across many computers with no centralised record.

Understanding of the technology however lags well behind the hype, amongst practitioners, policy makers and industry commentators alike. 'Blockchain' technology seems to promise major change for capital markets and other financial services – some say it may ultimately prove to be as important an innovation as the internet itself – but few can say exactly how or why.

The objective of this paper is to offer some insight into the potential use of mutual distributed ledger for reducing costs and risks in securities settlement. The findings are based on engagement with practitioners in a series of structured interviews and two focus group meetings (supplemented by a review of extensive relevant public domain materials, much of which is described in an appendix).

Our principal contribution is investigating three 'research hypotheses', not hypotheses that can be confirmed or rejected in a statistical sense but carefully worded statements designed to elicit the fullest possible understanding from our informants of the practical detail involved in the application of blockchain to post-trade processing. Investigating these hypotheses through extensive engagement with a large number of practitioners has highlighted the many challenges that will need to be addressed if mutual distributed ledgers are to be fully adopted in securities settlement.

To provide a flavour of our findings, here are a couple of the conclusions emerging from our analysis. A view expressed in several of our interviews is that a root cause of inefficiency in post-trade processes is that the two sides to a trade each maintain their own separate records of the transaction and the resulting counterparty obligations. The consequence is the expenditure of much unnecessary resource reconciling this data with that held by the counterparty at each step of contract execution. This is one reason why mutual distributed ledgers have such appeal to established firms – holding out the possibility of storing all relevant operational information about trade executions in agreed and verified format shared by all participants to the trade.

It is important to recognise however that agreement on the sharing of trade information can be bilateral and therefore requires *neither* that the actual ownership of securities is recorded on a mutual distributed ledger *nor* any of the various consensus mechanisms employed to ensure consistency of data on a mutual distributed ledger.[2] Indeed from a technological perspective the fuss about blockchain is a little surprising since distributed databases have themselves been around for many years and in the securities market context the cryptographic advances incorporated in the Bitcoin blockchain do not add any obvious value over the established approaches to ensuring security widely used in financial services.

[2] Such a bilateral approach to sharing of data for improving the efficiency of post-trade efficiency seems to be the distinguishing feature of the 'Corda' software for financial services, announced in early April 2016 by the industry digital ledger consortium R3, but the possibility of such bilateral data sharing is far from new. It is also used for example in the 'woven broadcasting' time stamping and document retrieval systems of Z/Yen (see www.metrognomo.com for the States of Alderney as an open public service example).

A related finding is that achieving all of the potential benefits of mutual distributed ledger is likely to be afflicted by the problem of 'excess inertia', a problem highlighted in other non-financial contexts by the research literature on technological innovation. This is a market failure that arises when users are 'locked in' to existing practice and as a result private profit incentives are not strong enough for individual firms to adopt a more efficient standard or technology, even when adoption would reduce costs for the industry as a whole. In the case of mutual distributed ledgers, this problem of private incentives is reinforced because the full benefits of using mutual distributed ledger appears to involve substantial (although as yet unquantified) costs in the short to medium term while the anticipated benefits lie largely in the relatively distant future. Mutual distributed ledger may struggle to compete for funding in an environment of limited IT budgets much of which is already committed to regulation and compliance.

Our overall judgements are cautious compared to much that has been written about the application of mutual distributed ledgers in financial services.[3] While agreeing that mutual distributed ledgers have considerable potential for both cost and risk reduction, a great deal remains to be done in order for this potential to be exploited. The momentum behind a shift to recording data in mutual distributed ledgers does however appear to provide the industry with an opportunity to harmonise business processes and address many long-neglected inefficiencies in post-trade and other financial operations.

The paper is organised as follows:

- Section 2 sketches the background to our work. It considers the challenge of cost reduction in post-trade processing, explains how mutual distributed ledgers such as the Bitcoin blockchain differ from traditional centralised recording of data and why there is now such a high level of interest in their application to securities settlement.

[3] Two other recent reports also emphasise the practical challenges of employing distributed ledgers in capital market operations are (DTCC, 2016; Euroclear & Oliver Wyman, 2016). The contents of these two reports are summarised in our Appendix 1.

- Section 3 sets out the three hypotheses that we investigated and describe the methods we have used to test them. A significant test of our hypotheses was a focus group meeting of November 2015. We provide a complete transcript of this meeting in Appendix 2.
- Section 4 presents two arguments that proved useful in organising our analysis – the continuing need even in mutual distributed ledgers for third parties playing a more limited 'notary' role and the interpretation that we have found useful of distributed ledgers as a form of database technology with wider and more flexible access than conventional relational databases. It then reports findings from our main focus group and subsequent interviews.
- Section 5 provides a few additional opinions of our own drawing on our extensive experience of the industry.
- Section 6 concludes.

There are three supporting appendices. We emphasise that it is *not* necessary to read these appendices in order to understand our conclusions or how we conducted our research. These appendices do though provide key supporting material and so will be useful to a critical reader wanting more supporting evidence for our findings. Appendix 1 records the range of opinions obtained from our interviews and public domain materials. Appendix 2 documents our principal focus group meeting. Appendix 3 lists a selection of the firms with whom we have engaged during our research, without in any way implying that they agree with our conclusions.

## 2. Background

In this section we discuss why there is now such widespread interest in the application of mutual distributed ledger technologies in global capital markets. We highlight two of these: first the potential for employing distributed ledgers to substantially reduce both costs and risks; and second the perception of current the "FinTech" boom, exemplified by the cryptocurrency Bitcoin, as an opportunity for fundamental entrepreneurial-driven change in financial services

Firms participating in financial markets today devote enormous amounts of resource to obtaining data, checking data records, and reconciling that data both internally and against the records of other firms. Broadridge, utilising data from Oliver Wyman

and Morgan Stanley, report that costs in global post trade processing alone are in the range $17bn to $24bn per year.[4] These are only one part of total costs in back- and middle-office. Another major middle and back-office expenditure for capital market firms are know-your-client (KYC) and anti-money laundering (AML) compliance which come to upwards of $12bn per year for major capital markets participants.[5] According to Oliver Wyman the aggregate revenues of the firms servicing the specific activities that can directly utilise mutual distributed ledger – clearing, securities settlement, collateral management and custodian services – together amount to some $40bn to $45bn.[6] Taking account of the full range of market data, risk management, mark to market reporting and regulatory functions can support estimates of total capital markets back and middle-office costs of $100bn per year or more.[7]

In many other industries the adoption of distributed and standardised business models, of the kind familiar from online commerce and the internet, has supported simplification and efficiency improvement in the supply chain.[8] Judging by the experience of these other industries, the adoption of mutual distributed ledger technologies may help remove 50% or more of costs in capital market transactions.[9]

Mutual distributed ledgers also offer opportunities for substantial reduction in counterparty, operational and liquidity risks. The industry has to commit large amounts of collateral to the hedging of counterparty risks in security and derivative

---

[4] (Broadridge, 2015). This estimate covers core post-trade processing, reference data, reconciliations, trade expense management, client life-cycle management, corporate actions, tax and regulatory reporting

[5] See (Chan & Milne, 2013) Section 5 for more detailed discussion of these costs.

[6] (Oliver Wyman, 2015) exhibit 3.

[7] This is broadly consistent with the IDC estimate that capital market firms account for about one quarter of total 2015 global financial Services IT external expenditure of $458 billion (International Data Corporation, 2015).

[8] See (Gospel & Sako, 2010; Herbert & Seal, 2012) for studies of consumer products and accounting.

[9] This 50% is only a guesstimate. For comparison we made some effort to review the research literature on cost reduction in non-financial industries through supply chain automation (see (Yu, 2013) for a recent review article). While such automation is widely perceived as having been crucial to improving efficiency and maintaining competitiveness, the research literature does not provide any precise quantification. This in part because automation is pursued in order to achieve a range of goals - for example greater responsiveness to customer needs, more flexibility in changing product design, better ability to cope with supply disruptions – not just cost reduction. Perhaps most persuasive in the work surveyed in (Yu, 2013) are the large and sustained increases in market capitalisation of those firms – of 7% per annum or more relative to their competitors – investing most in supply chain management relative..

transactions.[10] The fragmentation of security operations is a factor behind the large spikes in 'trade fails' at times of market stress.[11] Lack of transparency about the ownership of securities and their commitment in re-hypothecation together with the comingling of client assets proved to be a major problem in the resolution of Lehman Brothers International and might have been avoided through use of mutual distributed ledgers.[12]

Reducing these costs and risks is however far from being a new challenge. What has changed recently are perceptions of the means for pursuing these efficiency gains. Mutual distributed ledgers are now seen as a major opportunity for cost and risk reduction. This new perception has led to several firms developing digital ledger solutions for financial markets. We have paid closest attention to three of these: Digital Asset Holdings which is developing mutual distributed ledger solutions for a variety of use cases;[13] R3 which operates under a membership model, at most recent count involving forty two of the world's largest global banks;[14] and SETL the London based start-up offering its own multi-asset, multi-currency institutional payment and settlements infrastructure.[15]

These and other mutual distributed ledger initiatives on which we focus are a relatively small part of a much larger wave of new financial technology (or FinTech) start-ups in the US, the UK and elsewhere which have been attracting considerable venture capital funding. Accenture report that FinTech start-ups have raised a total of

---

[10] (Singh, 2013) reports that the increased concerns with counterparty risk and central banks purchases of good collateral have contributed to shrinkage in the pledged collateral market from $10 trillion prior to Lehman crisis (end-2007) to about $6 trillion (end-2011).
[11] See (The Economist, 2011).
[12] For overview of the role of rehypothecation and commingling of assets in the Lehman failure see (Deryugina, 2009).
[13] Their website http://www.digitalasset.com/ describes applications in syndicated lending, US Treasury repo and securities settlement. Digital assets announced a $60mn first round venture capital financing on January 22nd, 2016 with investment from ABN AMRO; Accenture; ASX Limited; BNP Paribas; Broadridge Financial Solutions; Citi; CME Ventures; Deutsche Börse Group; Goldman Sachs; IBM; ICAP; J.P. Morgan; Santander InnoVentures; The Depository Trust & Clearing Corporation; and The PNC Financial Services Group, Inc (Digital Asset Holdings, 2016).
[14] See http://r3cev.com/about/ and the press release (R3, 2015) , which announced a five person team who will responsible for leading joint working groups with the 30 global banks involved in the project and facilitating a collaborative lab environment or "sandbox" to test and validate distributed ledger prototypes and protocols.
[15] See https://setl.io/. SETL have recently appointed former Bank of England Executive Director David Walker as Chairman and are now engaged in a first round of fundraising.

$12.1bn dollars globally in 2014, more than three times the $4.0bn raised in 2013 (Accenture, 2015). One part of this boom in FinTech has been the huge recent interest in cryptocurrencies triggered by the success of Bitcoin. By early April 2016, over $1.1bn in cumulative venture capital has been raised for more than 200 Bitcoin and blockchain related ventures.[16]

What exactly is new about Bitcoin and blockchain? 'Digital cash' technologies have been around for more than a quarter of a century without achieving mass adoption. They record value in digital form using digital signatures to prevent double spending and maintain privacy of the user.[17] The innovation of the Bitcoin protocol (Nakamoto, 2008) is that there is no third party issuing the currency or providing convertibility (a promise to pay on demand) into other forms of money. Bitcoin has demonstrated the practical possibility of maintaining secure records of value open mutual distributed ledger using its consensus process (the 'proof of work' described in our introduction) to maintain an agreed and irrevocable record of transactions and ownership.

This dramatic rise of investment in FinTech has persuaded some commentators that banking could be on the verge of the same kind of digital disruption that has previously affected many other industries.[18] Some go so far as to argue that Bitcoin and blockchain is a key part of a new 'sharing economy' in which all our formerly centralised economic institutions are displaced by decentralised alternatives, a fundamental innovation that will come eventually to be seen as more significant even than the internet itself.[19] Bank of England governor Mark Carney has spoken along these lines, speculating that banking could be facing an 'Uber moment' (Edwards, 2015), i.e. disrupted by the technology of the sharing economy in much the same way as Uber and other 'peer-to-peer' technologies have disrupted the booking of taxis and the provision of other services.

---

[16] (Coindesk, 2015a)
[17] (Chaum, 1992) provides an accessible summary of these methods.
[18] For overview of the experience of other industries see (Christensen & Raynor, 2013; Christensen, 1997). Often this has been triggered by online competition, e.g. in retailing (Amazon), in booking of air travel and accommodation (Expedia, AirBnB). Increasingly mobile phone apps connect customers directly with suppliers of a range of services (e.g. the Uber taxi interface).
[19] (Vigna & Casey, 2016) is one lucid statement of this point of view. (Wright & De Filippi, 2015) discuss the legal consequences of such a profound change in economic relationships.

We conclude this section with a brief comment on terminology. Some more committed proponents of Bitcoin argue that Bitcoin and its blockchain with the associated proof of work through mining are indissoluble and that it is quite wrong to refer to blockchain, e.g. as in "our securities settlement is on the blockchain" if Bitcoin is not being used to trace ownership.[20] These critics have a point. If validation does not rely on tracing back transaction history through a sequential sequence of groups of authenticated transaction records then it is not using a blockchain. We therefore prefer the more general term 'mutual distributed ledger' since this covers various applications we have examined, both permissioned and unpermissioned and whether or not they trace transactions back to back to a genesis block.

Still we cannot avoid using the term 'blockchain' altogether. It has acquired a life of its own as a marketing term to communicate the excitement about the possibilities of decentralised processing akin to the buzz surrounding Bitcoin. We sometimes, notably in the title of our paper, use the term blockchain in this way, in order to acknowledge the current level of excitement about these new approaches and the belief that they may fundamentally transform financial market operational processes. Our interviews and focus groups (Section 4) and our own additional analysis (Section 5) suggest there are many substantial barriers to achieving such fundamental change, but the term 'blockchain' is still useful for communicating the excitement about what can be achieved from using mutual distributed ledgers.

# 3. Hypotheses and Research Methods

## Research hypotheses

Our review of public domain materials (Appendix 1) together with our initial interviews led us to focus our subsequent research on three hypotheses. These capture the major business questions that practitioners and commentators about the application of mutual distributed ledgers in securities settlement.

---

[20] This controversy about the term 'Blockchain' echoes an earlier terminological dispute from the early years of relational databases when firms might claim to be using the open source 'relational database' such as Ingres or MySQL when they were actually using a proprietary database such as Oracle, DBII, or Sybase.

1. *Any mutual distributed ledger settlement of securities purchases (or other transactions in public financial markets) will need to use a 'permissioned' ledger, in which only a limited number of approved network participants can propose updates of the ledger and participate in verification. This contrasts with permissionless mutual distributed ledgers (of which the 'Bitcoin Blockchain' is the leading example) where anyone can join the network and all have equal rights to propose updates to the ledger and participate in verification.*

This hypothesis reflects the widespread concern that the open nature of the Bitcoin network, which anyone can join, lacks the controls that will be necessary for obeying the regulatory and legal requirements of public securities trading. Although most practitioners expect any ledger used in public markets to be permissioned, a range of different views are still consistent with this hypothesis. For example this hypothesis leaves open the question of which institutions are given permission to participate in a mutual distributed ledger and the arrangements for granting this permission. In any first efforts at the adoption of mutual distributed ledger for settlement in public financial markets, permission to participate in recording of ownership and consensus verification seem most likely to be restricted to the major banks that already act as established intermediaries. It is possible though that permission could be extended to other new entrants in order to promote competition, especially if open distributed arrangements are developed for handling the full range of legal and regulatory processes.

2. *The initial applications of mutual distributed ledger will be based on piecemeal developments, in specific situations where there is no established centralised security depository for recording ownership. A coordinated and widespread change in operational processes across all the major public markets for equities, bonds and other financial assets will only be possible in the relatively far-off future, once technical feasibility is established in more limited contexts.*

This second hypothesis is more contentious than the first. Many proponents are envisaging mutual distributed ledger as a means of achieving complete standardisation and hence simplification of our existing post-trade processes. This is

seen as an attractive route to the long-standing goal of fully automated processing, resulting in major reductions of costs and risks. Others are putting forward much more specific practical proposals, aimed at improving post-trade processing of specific assets which are not currently held in central security depositories e.g. trading of syndicated loans, repo/ securities lending or insurance contracts.

In practice we anticipate the most pronounced difference of views on our phrase ‘relatively far-off’. Practical progress would seem to require first demonstrating application in specific limited contexts. Much less certain is how quickly these early demonstrations can be taken further and applied to post-trade processing in the major public markets. Also uncertain is the extent to which existing legacy arrangements and the challenge of coordinated processing may serve as a barrier to adoption. Firms may be reluctant to start using a mutual distributed ledger alongside existing inefficient arrangements because this will require an interim period of additional expenditure before the new replaces the old.

*3. At present current participants in the settlement cycle carry out a bundled set of functions (verification of ownership, preparation for exchange including associated borrowing of securities or cash, delivery of value against payment) using historically developed arrangements (tiered accounts, fungibility of securities ownership). Obtaining the benefits from the application of mutual distributed ledger to securities settlement will require a substantial reengineering of these arrangements in which the positioning for settlement must be carried out prior to trade.*

This third hypothesis is closely related to the second. If Hypothesis 3 is accepted as correct then so must Hypothesis 2, it will then not be possible to move rapidly to widespread use of mutual distributed ledger for settlement in the major securities markets. Conversely the rejection of Hypothesis 2 implies also rejection of Hypothesis 3.

Posing this as a third, separate hypothesis though seemed useful to us in order to distinguish two challenges to adoption of mutual distributed ledger, (a) the primarily technical challenges of reconciling information in different post-trade systems (the points raised in our discussion of hypothesis 2, which are naturally prominent to practitioners responsible for managing and developing post-trade operations), from

(b) the potentially major changes in business process which will need to be addressed once technical issues are resolved, especially if mutual distributed ledgers are used to support near-real time same day settlement.

The importance of distinguishing technical information reconciliation challenges from business process changes can be seen in considering moves towards near real-time settlement. Under current arrangements settlement for equities typically occurs at time T+2 (on the morning of the second day after trade execution).[21] This gives trade participants a full working day to position for settlement, borrowing securities or cash as necessary. Technical information reconciliation under T+2 or even T+1 can potentially be enhanced with mutual distributed ledgers. However, near real-time settlement after trade based on mutual distributed ledger (T+0) would require pre-positioning of cash or ownership prior to trade. This would be a major change to business processes.

## Research methods

The central activities were interviews and two focus group meetings held on 29 September 2015 and 25 November 2015 at the Z/Yen offices in London. Appendix 3 lists firms whose staff were either interviewed, attended a focus group, or provided comments on drafts. The purpose of the early interviews and the first focus group were to obtain information about the various proposals for using mutual distributed ledgers in securities settlement and to frame our hypotheses as clearly as possible. This involved a number of preliminary interviews, mostly conducted by telephone, together with the October focus group with 20 attendees run under the title "Ledger Legends - Mutual Distributed Ledgers versus The Blockchain".[22] This focus group addressed issues of where tokens or coins were needed and how to define mutual distributed ledgers.

Having framed our hypotheses we then tested these through a full discussion during our second focus group in November 2015. Because of the importance of this focus

[21] Actual practice is more varied than this. For example in the UK Government bonds settle on T+1 and many money market instruments on T +0. In the US equities settlement is currently T+3, but there is discussion of moving to T+2. Still in all cases a move to near time settlement will involve major changes in business process.

[22] This title – while catchy – drew a somewhat false distinction since, as explained, all blockchains, including the Bitcoin blockchain, are a type of mutual distributed ledger.

group in our research we reproduce in Appendix 2, in full, the transcript to this focus group (which was circulated to all participants for their opportunity to comment and amend). After this focus group we completed a first draft of the paper, which we circulated for comment, and conducted a number of further interviews with practitioners, going through our research and our findings and eliciting further comment.

We acknowledge two research biases that may have influenced both the framing of these hypotheses and our interpretation of the focus group discussions and our various interviews. Michael Mainelli at Z/Yen has been involved in developing mutual distributed ledger applications in various contexts, both financial and non-financial since 1995. Alistair Milne has written extensively about the industrial economics of post-trade securities clearing and settlement, arguing on many occasions that the industry is subject to 'excess inertia' with the combination of co-ordination costs and resistance by vested interests often blocking any changes that seek to improve operational efficiency. Our shared predisposition to this research was from the outset that we have seen this kind of thing before and therefore doubted whether renewed efforts to re-engineer post-trade operations based on mutual distributed ledger could differ markedly from past introductions of new technology.

What we have endeavoured to do is to ensure that our findings, stated in Section 4, are a reflection of the views on our three hypotheses obtained from our research informants, not a statement of our own opinions. Our personal judgements are contained in Section 5.

# *4.* Findings

## Two general insights

Before setting out the findings on the three hypotheses, we first discuss two general insights into the business application of mutual distributed ledgers that have emerged from interviews and focus groups. We found it difficult to interpret the material from our interviews and focus groups without taking into account these two points:

- In real world contexts distributed ledgers do not entirely remove the need for central third parties. The central third party role narrows towards confirming identity and asset existence (notary function), as well as dispute resolution and enforcement of legal obligations.

- Distributed ledgers are a form of database technology. In order to appreciate their potential, as well as the barriers to their adoption, it is worthwhile examining their similarities to and differences from the relational databases widely used in business applications since the 1970s

### The continuing need for trusted third parties

Where parties interact and need to keep track of transactions and ownership they have often found it helpful to create a centralised ledger. Centralised ledgers are found in registries (land, shipping, vehicles, tax), in securities depositories (stocks, bonds), libraries (index and borrowing records) and travel reservations (airlines, hotels and car-hire bookings) to give just a few examples.

Centralised ledgers are traditionally overseen by a "trusted third party" (or "central third parties"). Trusted third parties appear in many contexts in finance: for securities settlement, as custodians, as payment providers, and as poolers of risk. In most cases, these centralised ledgers are stored in relational database form, facilitating the extraction and comparison of the data they contain with that from other databases.

In the context of financial transactions, trusted third parties perform three functions:

- confirming – confirming (or 'validating') the existence of something to be traded or transacted, the legal and regulatory obligations involved and membership of the transaction community;
- safeguarding – preventing duplicate or fraudulent transactions, i.e. someone selling the same thing twice or 'double-spending', or having an asset taken without permission;
- preserving – holding the history of transactions to help analysis and oversight, and in the event of disputes.

Major problems arise if a third party breaks the trust placed in them.[23] There can be problems even when the trusted third party is honest. Control over access to the centralised ledger may also be a source of market power, allowing the incumbent or incumbent institutions to price at above cost and extract economic rents from users, a so-called 'natural monopoly'. Much attention is given to governance of trusted third parties and "industry mutuals". Even if market power is not exploited in this way, the arrangements for accessing the ledger may be complex and costly, especially when the ledger infrastructure has been developed piecemeal building on legacy arrangements designed around particular historical technical constraints. The employment of mutual distributed ledgers has the potential to address these substantial concerns about access to traditional centralised ledgers.

As mutual distributed ledger technology is established, it can be expected to replace two functions of the trusted third party: safeguarding against duplicate or fraudulent transactions and preserving a verifiable public record of all transactions. A distributed ledger though does not fully substitute for the first function of the trusted third party, confirming the existence of the asset (security, money or other financial or real asset) to be traded, compliance with regulations and the rights of those participating in the transaction, though it may reduce switching costs which in turn can reduce the potential for exploitation of market power.

A related issue is managing rights to access the data held in a mutual distributed ledger. To the extent that any institution creates data it creates some kind of value. An institution may wish to understand its end-to-end costs in the full cycle of settlement. To do this, it will need to reuse the data it creates in settlement processes in a meta-analysis endeavour (using data for analysis beyond the intent of its original creation). If such data is in a mutual distributed ledger, the institution must be able to extract it. If the institution can extract data on what other institutions are doing, it may gain an advantage over them. Attention will therefore need to be given to ensuring that mutual distributed ledgers are configured to allow access by an institution only to the data it creates, or in which it is a counterparty. This is

[23] While a third party may be trusted, it doesn't mean they are trustworthy. For illustration of the consequences of a corrupt third party, see the 'Ship registry skit' in (Mainelli & Smith, 2015) Box 1, page 40.

though something which the application of cryptography to a distributed ledger, applied appropriately, deals with very effectively: as we discovered from our interviews and focus groups (see further discussion below) a ‘configuration file’ can be set up to ensure that data is revealed only to those who ought to be seeing the data.

### Distributed ledgers as a database technology

Distributed ledgers offer a specific benefit: a transparent and rapidly updated shared record of one single aspect of business activities. But business activities are inherently complex. This suggests that creating mutual distributed ledgers will be only one of several steps required towards achieving the substantial potential reduction of middle and back office costs and risks in capital market firms.

A mutual distributed ledger can be understood as an evolution of the computer databases widely used from the 1970s onward. Some key differences are summarised in Table 1 below.

This table illustrates two different respects in which mutual distributed ledgers differ from conventional databases:

- First, their distributed structure means data is recorded consistently in multiple locations. This makes them robust – they are not vulnerable to failure of a central server – but also creates design trade-offs that are not present in centralised systems, especially the need to compromise between the timeliness with which consistency of records is achieved and the availability of data across the network. This may limit application in contexts where rapid updating is critical e.g. in order-driven trading.

- Second, their open architecture supports direct access of participants to the data. Instead of relying on separate specialised software (a database management system and associated messaging) for controlling access to and updating of data, a configuration file establishes the permissions for reading and writing of data.

| | *Centralised Databases* | *Distributed Databases* | *Mutual distributed ledgers (unpermissioned)* | *Mutual distributed ledgers (permissioned)* |
|---|---|---|---|---|
| *Storage* | Single master | Multiple copies | | |
| *Definition of data* | Multidimensional, typically using some approximation to the relational database design of Codd | | Specialised single dimensional for e.g. ownership, amount | |
| *Participation* | Closed | | Open. New nodes can be freely added. | New nodes added subject to agreement by core participants. |
| *Rights e.g. for updating of entries* | Governed by separate data base management system | | Built into the ledger protocol. | Configuration file determines all node rights to decrypt/ update |
| *Validation of data* | | | Uses ‘proof of work’ or some weighted voting schema such as ‘proof of stake’ | Typically based on confirmation by core participants |
| *Reconciliation of data* | Only necessary when data is moved. | Iterative, trading off consistency against availability | | |
| *Robustness* | Historically vulnerable to server failure | Resilient, continues to update even with partial node availability | | |

**Table 1: Table Comparison of Database designs**

A further practical difference is that mutual distributed ledgers such as the Bitcoin blockchain have been developed to support the recording and communication of data on a simple single relationship, that of the ownership of a token or virtual currency. Conventional databases, in contrast, incorporate multiple relations. For example a business database may have records for customers (name, address, email, telephone), for inventory (item, number), for transactions (date, customer, order description) and other items. Conventional databases therefore usually employ some form of Codd's relationship database principles with each record type associated with a primary key that can be used to relate that record to other types of record.

The relative simplicity of mutual distributed ledgers from the perspective of database design resolves one question that emerged early in our research: the issue of one, few, many, or multitudes. Will there be a single mutual distributed ledger for all securities traded in a particular market or even one global distributed securities ledger? Or will there instead be a plethora, one mutual distributed ledger for each security in each jurisdiction? Will there be further ledgers for identity, Know-Your-Customer and Anti-Money Laundering processes? The relatively narrow application of mutual distributed ledgers, at least in their most basic form tracking only one dimension the relationship of ownership, indicates that this is a false question.[25] The very simplicity and openness of the ledgers means that it should be straightforward to combine the information from different ledgers together or to ensure simultaneous and matching changes in different ledgers.[26]

It is also clear that in a practical business context the data in distributed ledgers will have to be combined with many other sources of data in a wide range of business processes such as management information and financial accounts, performance measurement, and risk and regulatory reporting. For these purposes data stored in mutual distributed ledgers will still have to be extracted and transferred to a data warehouse, integrating data from many different operational systems. This in turn creates a maintenance responsibility, ensuring that the semantic definitions in both

[25] This is not to say that a complex of further functionality e.g. 'smart contracts' cannot be built on top of the basic distributed ledger.
[26] (Mainelli and Smith, 2015) demonstrates several ledgers working together.

mutual ledgers and the various operational systems used internally by the firm are consistent and interpreted correctly during the process of data warehousing. The use of a mutual distributed database does not remove the need to confront various trade-offs in assembling and combining such data.

For an illustration of the kind of processing involved, consider the non-financial example of a distributed electoral register i.e. a mutual distributed ledger used to support voting (one of the standard use cases for a mutual distributed ledger recording the ownership of votes and in which the permission to cast a vote can only be exercised by the owner of that vote). After a round of voting the data from the ledger could then be analysed to assess the characteristics (age, education) of voters and the relationship of voter characteristics to voting choices. Extending the mutual distributed ledger to this further application requires confronting many of the same design trade-offs that arise in conventional database design. Should the voter characteristics be stored as part of the mutual distributed ledger or drawn instead from other databases? If included as part of the mutual distributed ledger then the ability to perform future relational analysis may be frozen, characteristics that were not included at the original design stage cannot be easily added. Any change in a mutual distributed ledger will be a major co-ordination challenge.

If stored as a separate database then choices must be made about the design of every database and the primary keys and other entries that are included in order to conduct relational analysis. The introduction of mutual distributed ledgers in a practical business context will involve revisiting and, if necessary, redesigning many of the processes used for aggregation and reporting of financial data.

The example of the relational analysis of a distributed electoral register is relatively simple. Businesses frequently need to combine information from many different databases. In the case of securities firms these will include for each holding inter alia characteristics of issuer, characteristics of owner, liens or claims on the asset, promised cash flows of the security, current and historical security prices and where necessary supplementary internal valuations and related derivative contracts. Routine business activity will require relational analysis on all these data items and more.

Simply moving the records of ownership of a particular security from conventional databases, such as the security accounts held with custodian banks, onto a mutual distributed ledger will not of itself fundamentally change the challenges of data management within any large financial organisations. Indeed in the short term such a change could be costly requiring reengineering of many internal systems (and given the problems of understanding poorly documented legacy systems many years after their original implementation, it might be argued that the necessary evolution in existing systems will be prohibitively expensive).

These differences between traditional databases and mutual distributed ledgers are fundamental to understanding the potential for employing mutual distributed ledgers in securities settlement or other business applications. A mutual distributed ledger tracks one specific aspect of business information, e.g. the ownership and the transfers of ownership of assets, and ensures that this information is directly available to many users. This reduces inconsistency and delays when accessing common data but it does not solve all problems of business data management. Mutual distributed ledgers are only one step towards employing standardised and open information technology architectures in order to achieve the substantial potential reduction of middle and back office costs and risks in capital market firms.

## Detailed research findings

With this background about the role of trusted third parties and about database design, we now turn to our detailed research findings. These turn out to be fairly simple and can be summarised in a few paragraphs. The simplicity of these findings, compared to the complexity of our initial hypotheses, is a consequence of the close relationship between hypotheses two and three. These are not independent. It is clear from our workshop and interviews that ***if*** the substantial potential gains of using mutual distributed ledgers for settlement are to be fully realised ***then*** it will be necessary to have a *"A coordinated and widespread change in operational processes across all the major public markets"* (Hypothesis 2) and this will in turn *"Require a substantial reengineering of these arrangements"* (Hypothesis 3).

A core question is exactly what changes in operational processes will be adopted if and when mutual distributed ledgers are widely applied in securities settlement. Answering this question will be a central task for the various initiatives seeking to

develop the application of mutual distributed ledgers in securities settlement. A major task will be developing consensus on the required operational changes and also defining the necessary standards for widespread adoption of mutual distributed ledger in securities settlement and in other areas of application. The Hyperledger Project exemplifies the kind of cross-industry collaboration that is being encouraged by the interest in mutual distributed ledgers, but the difficulty of attaining binding industry wide agreements on business process as opposed to software solutions should not be underestimated.[27]

Determining in detail what operational changes will need to be introduced is a matter of choice for industry participants in each market and beyond the scope of our own report. We would highlight some further points about operational changes raised in our focus group meetings and interviews that might usefully inform industry discussion.

- In any given operational context (which will depend on instrument and jurisdiction) the various processes involved in a securities transaction are well understood by participants. Where not covered by shared documentation, there is detailed practitioner knowledge and documentation within individual firms. Developing a mutual distributed ledger to support transactions in a particular operational context should not therefore be so difficult, provided this is based on an assessment of all the trade information that need to be shared and accessed by various participants (for example institutional investors, asset managers, custodian banks, brokers, hedge funds, central counterparties and central securities depositories). The content of the mutual distributed ledger will however still need to be mapped to the current systems in each institution. This is problematic because the knowledge (in detail) of the processing logic and data semantics is never complete, for example the way operations staff choose to use the services and data available in the system. Thus in moving

[27] The Hyperledger Project was announced in early February 2016. It is a collaboration between thirty organisations, including R3, Digital Assets and a number of major financial institutions (see Linux Foundation, 2016). Digital Assets, the former owners of Hyperledger which won the 2015 Innotribe FinTech start-up challenge at SIBOS (see SWIFT, 2015) have donated Hyperledger to the project. This illustrates willingness to co-operate on open source code for mutual distributed ledgers in financial services, but co-operation on underlying business process may be more difficult to achieve.

to a mutual distributed ledger there will be potentially costly mapping against existing systems.

- The transfer of ownership against payment is only the final relatively straightforward step of the process of clearing and settlement of securities trades. The vast majority of resource employed in clearing and settlement is required for three other tasks: (i) for establishing trust before final settlement (ensuring that the trade is agreed accurately on both sides and that counterparties are ready and willing to settle); (ii) for ensuring the legal validity of the exchange; and (iii) in dealing with the exceptions that arise when trust and legal validity are not established automatically through the automated clearing processes carried out before final settlement. Switching the ultimate record of ownership from central securities depositories and custodians onto a mutual distributed ledger does not of itself deal with these problems of trust and legality.
- A mutual distributed ledger (or more likely two mutual distributed ledgers, one for cash, the other for securities) can be used to establish that the counterparties to a trade are positioned for final settlement; but at what point in the trade life cycle must this positioning for settlement be in place? We discuss this further below, in particular the choice between retaining current conventions, where positioning is established in several stages of post-trade operations involving central counterparties, custodians, commercial banks and central securities depositories, or a shift to near real-time settlement e.g. T+15' (final settlement after 15 minutes).

In short, a change to settlement arrangements to utilize mutual distributed ledgers or other forms of data sharing could require a substantial reengineering of operational processes. This will not be easy. The difficulties in altering established arrangements for settlement is illustrated by the time and resource required for moves from T+3 to T+2 clearing and settlement of equity trades (something only recently achieved in London and still under consideration in US markets) or the challenges of developing the T2S settlement arrangements in Europe.

With these points in mind, we can then turn to Hypotheses 2 and 3. Hypothesis 2 was that adoption would be through piecemeal development rather than ‘big-bang’ transformation. We find that the challenge of using mutual distributed ledgers in

securities settlement is not just demonstrating technical feasibility but rather achieving the necessary co-ordination in reengineering business processes across multiple firms. Some opportunities show promise as proof of concept, e.g. syndicated loans or repo, but even in these cases it is far from clear that merely shifting records of ownership onto mutual distributed ledger will result in much efficiency gain. To take the example of syndicated lending, delays in settlement (which can amount to 20 days or more) arise primarily because of the legal complications associated with transfer of loan participations. The need to deal with legal complications is not affected by the method of recording ownership data.[28]

It thus appears that virtually all applications of mutual distributed ledgers on securities transactions will involve industry-wide change, and this requires leadership. It will be essential to have widespread involvement from both sides of each market, buy side and sell side, together with regulators (this was widely agreed at our November 2015 focus group).

One question raised in the second November 2015 focus group about securities transactions and mutual distributed ledgers was, "is this going to be rounds of evangelism followed by little progress?" To provide some further insight into this discussion, Figure 1 below illustrates ten generic application areas for mutual distributed ledgers: viz. timestamping, regulatory reporting, archiving, identity, wholesale payments, shared data (e.g. LEIs), deal rooms, asset transfer, asset maintenance, and contract execution (e.g. 'smart' contracts).

The vertical axis attempts to place these generic applications in order of technical difficulty, the horizontal axis in order of process change difficulty. The securities transaction functions can go clockwise 'without leadership' for quick technology wins, or counter-clockwise 'with leadership' for big process wins, or ideally both as mutual distributed ledgers change the data ownership and access, in turn changing the processes. Securities settlement (here 'asset transfer') can be seen as one of the more challenging applications of mutual distributed ledger because it involves

[28] In this we are reaching a rather different conclusion than the recent report by Euroclear and Oliver Wyman who argue that a first priority for the industry must be to work on concrete proofs of concept (Euroclear & Oliver Wyman, 2016, pg 21).

substantial change in the business process dimension along with significant change in technology.

Past practice has typically involved an emphasis on changes in the vertical rather than horizontal dimension of Figure 1. As one participant noted, “our industry has a history of incremental improvements rather than new approaches”. Another view put forward in the focus group was that “there has been an historic focus on process, not on data”. Another similar perspective, from interview, is that unless underlying data quality problems are addressed, putting data on a mutual distributed ledger will create as many problems as it solves. So in order to use mutual distributed ledgers the industry may need to give much greater priority to data quality than in the past.

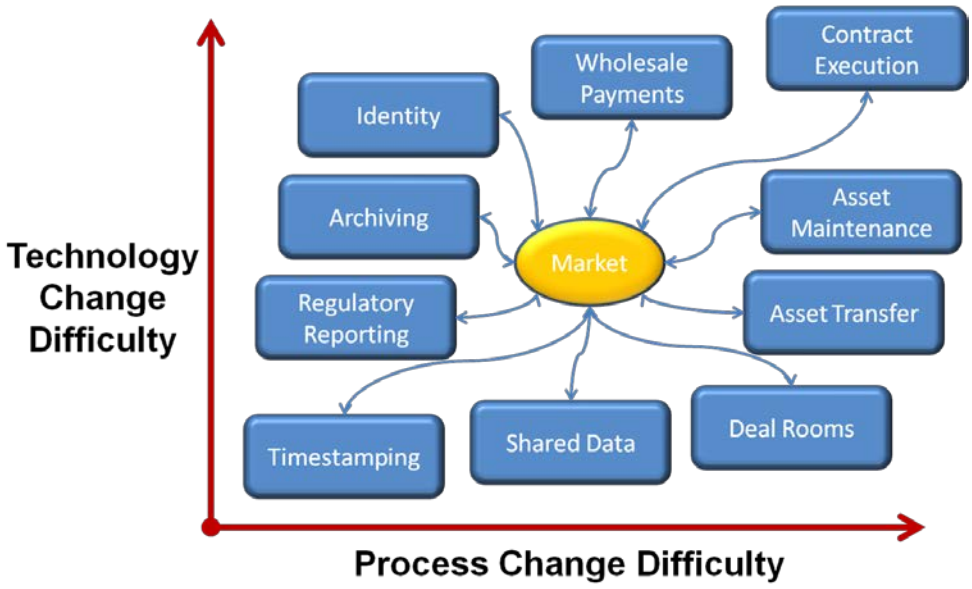


**Figure 1: Technology change and process change in ten potential applications of mutual distributed ledgers**

Our Hypothesis 3 was that the application of mutual distributed ledgers to securities clearing and settlement would require an accompanying shift in business practice to positioning for settlement prior to trade. Here it is necessary to distinguish two separate issues that are often conflated. The first issue, one that we have already discussed at some length, is that utilising mutual distributed ledger technologies to achieve efficiency gains in securities settlement (or other operational processes) requires harmonisation and development of business process. So yes, to some extent this hypothesis is confirmed, substantial accompanying shifts in business practice will indeed be required.

Some commentators have argued that near real-time settlement is one of the main commercial benefits of adopting mutual distributed ledger technologies (see for example the quotation from (Masters, 2015) transcribed in Appendix 1). These commentators seem to be unaware of the challenges involved. It is difficult to overstate the scale of change in business process required for a shift to near real-time settlement (T+15'). Under current business practice, whether executed on own account or on behalf of a client, traders do not typically have securities or cash in their position at the time of trade execution. The large scale netting under T+2 or T+3 settlement (DTCC for example is currently able to reduce the volume of trades for final settlement through netting by approximately 97%) will no longer be possible, at least not at all easily, under T+15', although central counterparties might still be employed for other reasons for example ensuring counterparty anonymity. Nor will it be possible to make use of the algorithms provided by central securities depositories to sequence settlement so as to economize on gross commitment of money and securities. Accounting and management reporting are also affected, allowing offsets of daily settlement that would likely to be unacceptable under near real-time settlement. The necessary prepositioning would also require fundamental changes in the management of market liquidity.

One informant suggested to us that it might be possible offer a choice of time frame for settlement, with some market participants electing for settlement at T+15' and others at say T+2. While placing fewer obligations on market participants to change their own business models, it is unclear that this is workable. It requires the introduction of some mechanism on trading venues ensuring that the two counterparties to every trade agree not just on the price and quantity of the security being traded but also on the settlement time frame. Given the resulting potential for operational problems it is unsurprising that market infrastructures have avoided having such an options in the past. An important part of the development of pan-European post-trade arrangements has been harmonizing on a common time frame for settlement.

Even more damning for the claim that the employment of mutual distributed ledgers will allow near real-time settlement is that decision of whether cash and securities should be positioned prior to trade turns out to be a quite separate issue from the sharing of data. The adoption of mutual distributed ledger technologies is neither

necessary nor sufficient for a move to near real-time settlement cycle. Mutual distributed ledger technology could be adopted – and yield substantial reductions in costs and risks – without any change in settlement times, e.g. from the current standard for equity trading of day T+2. Equally a shift to near real-time settlement could be achieved without the use of mutual distributed ledgers (this is already technically possible with existing centralised arrangements provided cash and securities are positioned prior to trade).

This understanding that there is no close relationship between settlement times and the adoption of mutual distributed ledgers emerged clearly from our second focus group. Delayed settlement is a design choice involving deep economic market structures, not least of which are leverage and liquidity. A shift to near real-time settlement, say a few minutes after trade will bring costs as well as benefits. Yes, it will economise on the commitment of cash and collateral but it will require a major change in business processes, with the holding of securities and cash having to be positioned prior to trade and greater exposure to liquidity risks. Moreover the costs of two day settlement are not so much the delay itself (the financial costs of tying up cash or collateral overnight for settlement are minor relative to overall costs of trade processing).[29] Where more substantial costs arise is in the uncertainty about the timing of final settlement: trades may fail because collateral or cash is not in position, especially at times when market liquidity is stressed. So a much more important gain from applying mutual distributed ledger in securities settlement is from greater certainty of final settlement time rather than contraction of the period of settlement.

Our last finding on our Hypotheses 2 and 3 is that most of our informants remain skeptical about the ability of the industry to agree on mutually coordinated solutions to operational problems. An example is the very poor track record of the industry in establishing pan-industry standards for reference data on both entities and securities. The global LEI (legal entity identifier) is now available as an industry wide standard identifier of securities market participants, but this was a regulatory initiative pushed through industry opposition (principally fearing a ‘natural monopoly’ on LEI

[29] Overall commitment of collateral in global financial markets is large (Singh, 2013) but this is largely associated with the provision of initial margin for cleared derivatives trades and the financing of leveraged positions whether long or short, not with securities transactions per se.

data).[30] Before the Financial Stability Board established the global LEI through fiat, there were many previous failed attempts to establish industry wide entity identifiers.

Even today the industry has failed to establish agreed security identifiers, firms have to handle several different incompatible schemas creating considerable and unnecessary complexity in internal data management. Absence of standardized security identifiers is not, in our view, itself an obstacle to the adoption of settlement on mutual distributed ledgers. Rather the opposite, this would seem to provide an incentive for using a mutual distributed ledger because this removes any ambiguity of understanding between the two sides to a trade about the security being transacted. But the failure to establish such standards does illustrate how difficult it has been to co-ordinate the industry in the past.

This leaves only Hypothesis 1, that mutual distributed ledgers in securities settlement will be 'permissioned' rather than 'unpermissioned' in order to meet with the unavoidable regulatory and legal requirements applied to capital market transactions. While, unsurprisingly, this first hypothesis was confirmed, the answer was rather more nuanced than we initially expected. The key insight for us was the availability of 'configuration files' for cryptographic control of access and updating rights to ledger participants. One of the advantages – arguably the principal advantage - of mutual distributed ledgers and the cryptographic methods they employ is that they provide a precisely defined but flexible control over access to shared data. This means that the choice about permissioning is not a simple yes/no or in/out decision. There are a wide range of possibilities about access and administrative privileges for a wide range of potential participants. So, while the hypothesis is essentially correct, careful thought needs to go into determining the permissioning environment and ensuring the flexibility for changing and updating when necessary.

### Further applications including smart contracts

To complete our findings, we mention some further applications of mutual distributed ledger in capital markets that came up in our interviews and focus group discussions,

[30] For description see (Chan & Milne, 2013)

even though these lie beyond the primary scope of this report. Our research has focused on the application of mutual distributed ledgers in securities settlement. But there are many other examples of potential cost reduction in capital markets resulting from employing mutual distributed ledgers to hold shared data. One is in KYC/ AML compliance. Using the global LEI as a standard identifier in a distributed KYC ledger could substantially reduce the billions of dollars required for KYC/ AML compliance. Another is using a distributed KYC ledger in OTC derivatives markets.

Our interviews and discussions briefly explored the application of so-called 'smart contracts' in mutual distributed ledgers. Mutual distributed ledgers need not just hold data, they can also contain code and this code can be used for automated processing on the ledger whenever certain pre-defined conditions are met. There is therefore much interest in the possibility of using mutual distributed ledgers to automate currently costly security processes. Examples include removing much of the cost of corporate actions for custodian banks that manage security holdings on the part of the investors, for the automation of fund portfolio allocations following trades executed on behalf of asset managers or in the context of international trade finance or domestic invoice financing.

For several interviewees and focus group participants, the most exciting business applications of distributed ledgers are from the employment of smart contracts to achieve a high degree of automation in shared inter-organisational processes and transactions with verified matching and execution of instructions. Much of the costs in the industry are associated with process incompatibilities that have to be manually reconciled. Once records and processing in data storage and business systems are consistent across firms, then the potential for considerable efficiency gains are unlocked. That said, while 'smart contracts' clearly require that firms introduce processes for sharing of data to ensure consistency, it is less clear that this sharing has to be through a mutual distributed ledger. Data sharing to support smart contracts could just as well be bilateral rather than through a mutual distributed ledger and the employment of smart contracts might actually precede the adoption of mutual distributed ledgers.

That said, most focus group participants seemed to feel that at least in the near term 'dumb short contracts' would prevail over 'smart long contracts'. There were three

primary opinions supporting this feeling. First, if an executable contract has a life of a day or so, then the mutual distributed ledger is not open to long-term sabotage or disruption. Second, most realistic smart contracts seemed to rely on the existence of persistent external data sources which means the contracts become complicated quickly, or wind up relying on human arbitration, rather defeating their purpose. Third, smart contracts that involved payments would require posting collateral to be completely automated. This locking-up of collateral would lead to a serious reduction in leverage and pull liquidity out of markets. Markets might become more stable, but the significant reduction in leverage and consequent market decline would be strongly resisted by market participants.

A final point about smart contracts is their legal status: the ideal for promoting automated execution is that the legal contracts are expressed in the same executable code of the smart contract in the mutual distributed ledger. In practice, as smart contracts are applied it is likely that a manual process of converting legal contracts into executable code will be needed. These 'automated' contracts will provide overrides for arbitration, expert determination, and mediation which will be tempting for a disadvantaged party to invoke. Over time this could become quite standardised, but in the initial stages this could create further barriers to their widespread application.[31]

## 5. The Emperor's Old Clothes?

This section records somewhat more subjective views (i.e. our own views not directly supported by our interviews and focus group meetings). These can be summarised in our section title: 'The Emperor's Old Clothes'. The potential for mutual distributed ledgers to transform securities settlement is real (in contrast to the new clothes of the Emperor in the Hans Christian Andersen's tale). Capital markets, like many other financial services, rely on operational data, and where this can be agreed and

[31] We have further evidence of this point from a February 2016 'distributed futures' meeting hosted by Z/Yen at which lawyers, arbitrators and industry specialists, explored arbitration, mediation, and expert determination for mutual distributed ledgers (the website for these meetings can be found here http://www.zyen.com/events/distributed-futures.html ). The conclusion of that meeting was that such intervention mechanisms, as well as 'legal jurisdiction' would need to be 'written into' so-called smart contracts for the foreseeable future. Completely automated contracts embedded in mutual distributed ledgers still seem some way off.

shared this can yield substantial improvements in transparency and ease of data access. We agree that the 'logically central, physically distributed' architecture of mutual distributed ledgers is probably the most powerful available means by which efficiency gains in securities transaction lifecycles can be achieved.

'Emperor's Old Clothes' emphasises our view that the principal challenges involved in applying distributed ledgers to securities settlement or other financial applications are not new. Opportunities for sharing data through distributed databases have been around for years. The current interest in mutual distributed ledger technology represents a real opportunity for change. But there is a danger of building unrealistic expectations of the extent to which this technology will, on its own, address the underlying need for coordination of business processes within and between firms.

This is not at least yet how most public authorities regard mutual distributed ledgers. The principal concern for regulators when confronted with cryptocurrencies or other novel financial products and services has been ensuring that these innovations do not undermine either prudential safety or customer protection.[32] Regulators are naturally cautious: the memory is still fresh in their minds of the role played by lightly regulated US dollar 'shadow banking' in the global financial crisis of 2007-2009.

What seems to be less widely accepted by regulators is that the adoption of new technologies, especially common data standards, can help them achieve their regulatory goals.[33] We perceive a 'siloed' attitude with technology and standard setting perceived as being of relevance to a few innovative activities and to financial infrastructures – and a corresponding failure to recognise the potential benefits of widespread adoption of common technological standards for improving the cost-effectiveness of regulation as a whole. A partial exception is some of the smaller regulatory entities, for example the Channel Islands led by the states of Jersey and Alderney, who are providing positive regulatory support for distributed ledgers.[34]

---

[32] See for example (Carney, 2016) who writes "The regulatory framework must ensure that it is able to manage any systemic risks that may arise from technological change without stifling innovation."
[33] The analysis of this paragraph draws on (Houstoun, Milne, & Parboteeah, 2015).
[34] See (States of Jersey, 2015)

Why do we think that mutual distributed ledgers can be of such help to regulators? Two fundamental features of a distributed ledger, i.e. persistence and pervasiveness, make them ideal for providing a regulator with a full transaction record for both oversight and recovery in the case of a systemically important financial institution failing, and also for promoting account portability and competition. Basing regulatory reporting requirements on mutual distributed ledgers can also lead to potentially large reductions in the compliance costs of regulatory reporting. To give one example the reporting of OTC derivative transactions to trade repositories has imposed great costs on industry while yielding little useable information to regulators. While regulators are now addressing this concern by imposing standards progress remains slow and much cost could have been avoided by beginning with standardisation of data, not pursuing this as an afterthought.[35]

It also seems to us that central banks could encourage the adoption of mutual distributed ledgers, by allowing the transfer of central bank reserves used for final settlement of payments onto a distributed ledger.[36] This (significant) change would be a major step towards supporting the use of mutual distributed ledgers in settlement of securities, foreign exchange and money market transactions.[37]

We also point out that the business models of numerous institutions are potentially threatened by the introduction of shared records of ownership and transactions. These include for example, broker dealers that execute trades and provide credit and security services to clients and also custodian banks. The implications of the adoption of mutual distributed ledgers for competition and economic power structures requires more research, but we do think that full senior management buy-in to mutual distributed ledgers will only happen after taking account of the

---

[35] For more detailed discussion see (Houstoun et al., 2015)

[36] A number of central banks are looking at the possibility of the issue of their reserves on distributed ledger, and potentially going even further by allowing non-bank holdings of those reserves as a means of payment substituting for central bank notes. Such developments are mentioned in recent speeches and interviews by officials from the Bank of England, the Bank of Canada and the Peoples Bank of China (Haldane, 2015; Wilkins, 2015; Xiaochuan, 2016). See also (Milne, 2016) for analysis of the economics of central bank issuance of a cryptographic currency as the ultimate settlement media. Doing so however raises an number of concerns about security, risk and regulation (see Committee on Payment Systems and Market Infrastructures, 2015; Richards, 2016) and no immediate steps of this kind are envisaged.

[37] Some mutual distributed ledger initiatives – for example the London based start-up SETL – are focussing first on providing a distributed ledger for the gross settlement of real-time payments.

implications for their competitive positioning and may not happen at all without addressing the incentives and cultures that drive decision making in major financial institutions. Ultimately there may be a need – perhaps under regulatory and shareholder pressure – for firms to take a wider and longer term 'whole market' perspective rather than focusing on their own short term individual bottom line.

As a final point in this section we think it useful to draw an analogy between mutual distributed ledgers in securities settlement and the original adoption of computerized recording of securities ownership following the paperwork crisis in New York markets of the late 1960s and early 1970s. Then the sheer scale of practical challenge, with settlement delays of six weeks or more, forced the US industry into fully rethinking its operational processes. This led eventually to the dematerialization of securities holdings and the creation of DTCC, along with the accompanying changes to securities laws and regulations, and underpinned the subsequent remarkable explosion in speed and volume of securities trading.

The current interest in 'blockchain' is perhaps best viewed as one aspect in a much broader strategic challenge to the entire financial services industry since the global financial crises from 2007. The industry may – over the next five to ten years – need to completely re-think its infrastructure in order for more participants to distribute more products to more people, shifting from limited participation with relatively high margins to more competitive and low margin. The industry needs to build an integrated view of all transactions and business processes and the supporting data on ownership, collateral, and risk. 'Open, shared, data' might not appear to be in the immediate shareholder interest of current financial institutions, but from a longer term perspective, improving the efficiency of intermediation in global financial markets should benefit almost all investors.

While the operational costs and challenges have not yet mounted to the point where they threaten to undermine the trading processes, there is once again today an opportunity for collectively rethinking post-trade processing in global capital markets. If we were to start with a blank piece of paper and draw up the most efficient possible operational arrangements what would they be? Mutual distributed ledger technology does seem to offer the possibility of a step change in new processes, allowing the industry to move from present fragmentation and inefficiency to more

automated, safer and more efficient operations. But we believe it is a chimera to believe that this change will come through competition from technological innovators alone. Just as half a century ago DTCC required collaboration of the entire industry, so too with mutual distributed ledgers for specific process areas. There needs to be a clear-sighted focus on the necessary investments and the potential long term gains, from both senior management and senior regulators. Otherwise the much heralded 'blockchain' revolution may disappoint.

## 6. Summary and Conclusions

This paper reports the outcome of a series of interviews and focus groups, eliciting and documenting views of market professionals on the potential impact of 'blockchain' (or in our preferred terminology 'mutual distributed ledgers') on the post-trade clearing and settlement of securities trades. Many have argued that the employment of mutual distributed ledgers can substantially reduce the high costs of post-trade processing. There are no definitive figures, but these costs are in excess of $40bn per year on securities clearing and settlement alone, much of which arises in data reconciliation and in manual intervention in operational processes. After taking into account the costs of other processes – KYC, AML, corporate actions and trade allocations – it appears that mutual distributed ledger technologies could save global securities markets many tens of billions of dollars per year.

We investigated three research 'hypotheses' (carefully worded statements designed to elicit as much information as possible from our interviews and focus group meetings). The first was on whether access to distributed ledgers used in global financial markets need to be 'permissioned' with only a limited number of approved network participants (the alternative being the use of 'unpermissioned' ledgers such as the Bitcoin blockchain in which anyone is allowed to participate). While, unsurprisingly, this first hypothesis was confirmed, the answer was rather more nuanced than we initially expected. The key insight for us is the availability of 'configuration files' for cryptographic control of access and updating rights to ledger participants. One of the advantages – arguably the principal advantage – of mutual distributed ledgers and the cryptographic methods they employ is that they provide a precisely defined but flexible control over access to shared data.

The views of practitioners yielded less clear cut responses to our remaining two hypotheses. The two main issues raised in these hypotheses were: first whether the adoption of mutual distributed ledgers needed to be developed first in specific situations, establishing 'proof of concept' by apply the new technology in contexts where there is currently no centralised security depository for recording ownership; and second that the widespread adoption of mutual distributed ledgers, and full exploitation of their potential for cost reduction, will require a substantial reengineering of the arrangements for clearing and settlement.

Our principal finding on these other two hypotheses is that ***if*** the substantial potential gains of using mutual distributed ledgers in settlement are to be fully realised ***then*** it will be necessary to have a *"A coordinated and widespread change in operational processes across all the major public markets"* (Hypothesis 2) and this will in turn *"Require a substantial reengineering of these arrangements"* (Hypothesis 3).

Our interviews and focus groups proved less than supportive of the idea that progress in the adoption of mutual distributed ledgers in post-trade securities processing can be pursued simply by developing proof of concept through demonstrating application in some specific practical contexts or where for example there is not yet any centralised recording of ownership. It is not clear that there are easy wins. Wherever mutual distributed ledger is applied it has to be accompanied by substantial changes in operational arrangements, both for the completion of trades and for associated tasks such as collecting, warehousing and analysing of data for management reporting. The challenge of using mutual distributed ledger in securities settlement is not just demonstrating technical feasibility but also a co-ordinated reengineering of business processes across multiple firms.

The investigation of these hypotheses and accompanying analysis (Section 5 and Appendix 1) point to some further conclusions. Two of these have already been mentioned in our introduction. Some benefits of mutual distributed ledgers can be achieved using relatively simpler approaches e.g. reducing the substantial costs of reconciliation between the two sides to a trade by recording data at the time of trade execution in a shared *bilateral* ledger. There is also a problem of 'excess inertia', the challenge of co-ordinating change and the resistance from those market participants whose business models means that achieving the full potential of the technology will

require a concerted and co-ordinated industry wide effort. It will not come about simply by leaving the choice of technology ‘to the market’.

Some further more specific conclusions can also be drawn from our analysis.

1. Many argue for the adoption of mutual distributed ledgers in order to bring about near real-time settlement (T + 15 minutes instead of the current T+2 days for equities trades). This is fundamentally confused. Existing centralised settlement on central securities depositories already support virtually instantaneous settlement once all the preparations such as positioning of securities and cash are completed. Near real-time settlement can be achieved simply by requiring all these steps to be taken prior to trade and does not require moving settlement onto mutual distributed ledgers.
2. Our analysis in Section 4 views mutual distributed ledgers as a form of database and highlights the business requirement for ‘meta’ analysis (in e.g. management reporting, audit and risk management) using information from a number of databases. This in turn means that adoption of mutual distributed ledgers will require the updating of a range of different business processes and data sources in a coherent way. This is a further reason for believing that the scale of change to see effective and widespread adoption is large.
3. ‘Smart contracts’ i.e. embedded code can support much greater process automation (though in our opinion this will only be fully realised over the long-term). As already mentioned modern cryptography supports flexible control over rights to access and update data (rights which can be easily altered by amending configuration files). Both of these technologies support greater commonality of business process and the exploitation of economies of scale through the separation and outsourcing or sharing of process between firms, changes that can be anticipated even if the securities ownership and transactions are not all recorded on mutual distributed ledgers.

To conclude, honouring the full promise of mutual distributed ledgers will not come automatically, easily or cheaply. Agreeing the required investment will require engagement and commitment at board level across both the buy side and sell side of the industry and for regulators to play an active rather than passive role, for example requiring the adoption of shared data arrangements for regulatory reporting or

putting central bank reserves used for final settlement of cash payments onto a mutual distributed ledger. The return will then come from substantial improvements in operational efficiency that can be enjoyed for many years to come.

## References


Accenture. (2015). *The Future of FinTech and Banking: Digitally Disrupted or Reimagined?* Retrieved from http://www.fintechinnovationlablondon.net/media/730274/Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf

Belshe, M. (2016). Bitcoin Blocksize and the Future. Retrieved from www.belshe.com/2016/01/18/bitcoin-blocksize-and-the-future/

Broadridge. (2015). White Paper: Charting a Path to a Post-Trade Utility. Retrieved December 15, 2015, from http://www.broadridge.com/broadridge-insights/Charting-a-Path-to-a-Post-Trade-Utility.html

Brown, R. G. (2015a). Brief thoughts on the Bitcoin block size debate. Retrieved January 31, 2016, from http://gendal.me/2015/08/17/brief-thoughts-on-the-bitcoin-block-size-debate/

Brown, R. G. (2015b). Free advice can be valuable… but only if you take it. Retrieved January 31, 2016, from http://gendal.me/2015/08/26/free-advice-can-be-valuable-but-only-if-you-take-it/

Brown, R. G. (2016). Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services — R3. Retrieved April 10, 2016, from http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

Cantillon, E., & Yin, P.-L. (2008). *Competition between Exchanges: Lessons from the Battle of the Bund*. Centre for Economic Policy Research.

Carney, M. (2016). FSB Chair Letter To G20 Finance Ministers and Central Bank Governors. Retrieved from http://www.fsb.org/wp-content/uploads/FSB-Chair-letter-to-G20-Ministers-and-Governors-February-2016.pdf

Chan, K. K., & Milne, A. (2013). *The Global Legal Entity Identifier System: Will It Deliver?* (Economics Working Papers).

Chaum, D. (1992). Achieving electronic privacy. *Scientific American*, *267*(2), 96–101.

Christensen, C. M. (1997). *Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Harvard Business School Press. Retrieved from http://www.amazon.co.uk/Innovators-Dilemma-Technologies-Management-Innovation/dp/142219602X/ref=pd_sim_14_1?ie=UTF8&refRID=052Y5KC5AM6S5Q15FXHD

Christensen, C. M., & Raynor, M. (2013). *The Innovator's Solution: Creating and Sustaining Successful Growth* (2nd revise). Harvard Business Review Press. Retrieved from http://www.amazon.co.uk/dp/1422196577/ref=pd_lpo_sbs_dp_ss_1?pf_rd_p=569136327&pf_rd_s=lpo-top-stripe&pf_rd_t=201&pf_rd_i=1578518520&pf_rd_m=A3P5ROKL5A1OLE&pf_rd_r=072HZW6ZGCN7JQKEGZVV

Coindesk. (2015a). Bitcoin Venture Capital Funding. Retrieved December 16, 2015, from http://www.coindesk.com/bitcoin-venture-capital/

Coindesk. (2015b). KnCMiner Deploys Next-Generation 16nm Bitcoin ASIC. Retrieved April 7, 2016, from http://www.coindesk.com/kncminer-deploys-next-

generation-16nm-bitcoin-asic/

Committee on Payment Systems and Market Infrastructures. (2015). *Digital Currencies*. Retrieved from http://www.bis.org/cpmi/publ/d137.htm

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., … Gün, E. (2016). On scaling decentralized blockchains. In *Proc. 3rd Workshop on Bitcoin and Blockchain Research*. Retrieved from http://fc16.ifca.ai/bitcoin/papers/CDE+16

Das, S. (2015, December 22). Patrick Byrne Is Wary of R3's Blockchain Consortium. *Cryptocoins News*. Retrieved from https://www.cryptocoinsnews.com/patrick-byrne-is-wary-of-r3s-blockchain-consortium/

David, P. A., & Greenstein, S. (1990). The economics of compatibility standards: An introduction to recent research 1. *Economics of Innovation and New Technology*, *1*(1-2), 3–41.

David, P. A., & Steinmueller, W. E. (1994). Economics of compatibility standards and competition in telecommunication networks. *Information Economics and Policy*, *6*(3-4), 217–241. http://doi.org/10.1016/0167-6245(94)90003-5

Deryugina, M. (2009). Standardization of Securities Regulations: Rehypothecation and Securities Commingling in the United States and the United Kingdom. *Rev. Banking & Fin. L.*, *29*, 253.

Digital Asset Holdings. (2016). Digital Assets Closes Funding Round Exceeding $50 Million From Thirteen Global Financial Leaders. Retrieved from http://www.digitalasset.com/press/digital-asset-closes-funding-exceeding-50-million.html

DTCC. (2016). *Embracing Disruption*. Retrieved from www.dtcc.com/~/media/Files/PDFs/DTCC-Embracing-Disruption.pdf

Edwards, J. (2015). That $1 Billion TransferWise Deal Is Exactly Why Mark Carney Worries About "An Uber-Type Situation In Financial Services." Retrieved May 29, 2015, from http://uk.businessinsider.com/transferwise-mark-carney-and-uber-type-situation-in-banking-2015-1

Euroclear, & Oliver Wyman. (2016). *Block chain in capital markets: the prize and the journey*. Retrieved from https://www.euroclear.com/dam/Brochures/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf

Farrell, J., & Saloner, G. (1986). *Competition, Compatability and Standards: The Economics of Horses, Penguins and Lemmings*. Department of Economics, Institute for Business and Economic Research, UC Berkeley. Retrieved from http://econpapers.repec.org/RePEc:cdl:econwp:qt48v4g4q1

Gospel, H., & Sako, M. (2010). The unbundling of corporate functions: the evolution of shared services and outsourcing in human resource management. *Industrial and Corporate Change*, *19*(5), 1367–1396. http://doi.org/10.1093/icc/dtq002

Government Office for Science. (2016). *Distributed Ledger Technology: Beyond Block Chain*. London. Retrieved from https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

Hagelstrom, M. (2016). Why Bitcoin's Block Size Debate is a Proxy War. Retrieved

from http://www.coindesk.com/bitcoin-block-size-proxy-war/

Haldane, A. G. (2015). How low can you go? *Speech Delivered at the Portadown Chamber of Commerce*. Bank of England. Retrieved from http://www.bankofengland.co.uk/publications/Pages/speeches/2015/840.aspx

Harris, P. (2015). Roundup: Securities Marketplace Block Chain Projects, Startups & Technology Platforms. Retrieved from http://harris-on.typepad.com/block_chain_io/2015/09/roundup-securities-marketplace-block-chain-projects-startups-technology-platforms.html

Herbert, I. P., & Seal, W. B. (2012). Shared services as a new organisational form: Some implications for management accounting. *The British Accounting Review*, *44*(2), 83–97.

Houstoun, K., Milne, A., & Parboteeah, P. (2015). *Preliminary Report on Standards in Global Financial Markets*.

International Data Corporation. (2015). Financial Insights Forecast 2015. Retrieved May 30, 2015, from http://www.idc.com/getdoc.jsp?containerId=prUS25606415

Linux Foundation. (2016). Linux Foundation's Hyperledger Project Announces 30 Founding Members and Code Proposals To Advance Blockchain Technology | Hyper Ledger Foundation. Retrieved February 23, 2016, from https://www.hyperledger.org/news/announcement/2016/02/hyperledger-project-announces-30-founding-members

Lykke. (2016). *Global Marketplace on Blockchain*. Retrieved from https://wiki.lykkex.com/_media/lykke_whitepaper_march2016.pdf

Mainelli, M. (2016). Terminology Wars – I Record Therefore I Ledger; I Block Therefore I Chain? Retrieved February 23, 2016, from http://thefinanser.com/2016/02/what-is-and-what-isnt-a-blockchain.html/

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, *3*(3 Winter), 38–69. Retrieved from https://www.gfsi.ey.com/the-journal-x.php?pid=18&id=110

Malmo, C. (2015). Bitcoin Is Unsustainable. Retrieved March 14, 2016, from http://motherboard.vice.com/read/bitcoin-is-unsustainable

Masters, B. (2015). Distributed Ledgers and Blockchains: Why this new technology is important now and why you should focus on it for your business. Retrieved from https://www.sibos.com/media/news/videos?ytid=gOkBbLoPTbo

Milne, A. (2006). What is in it for us? Network effects and bank payment innovation. *Journal of Banking & Finance*, *30*(6), 1613–1630. Retrieved from http://ideas.repec.org/a/eee/jbfina/v30y2006i6p1613-1630.html

Milne, A. (2016). *Virtual gold: exploring the implications of a cryptographic monetary standards*.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, A., Bonneau, J., Felten, E., Felten, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint. In *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International*

*Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET* (pp. 280–285). IET. Retrieved from https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

Oliver Wyman. (2015). *The Capial Markets Industry: The Times They Are-A-Changin'*. Retrieved from http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2014/September/the-capital-markets-industry.pdf

Palmer, D. (2016). Scalability Debate Continues As Bitcoin XT Proposal Stalls. Retrieved from http://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls/

Prisco, G. (2015). Nasdaq, LHV Bank, Technology Startups Develop Blockchain-Based Fintech Applications in Estonia. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/nasdaq-lhv-bank-technology-startups-develop-blockchain-based-fintech-applications-in-estonia-1447870921

R3-CEV. (2015, November 19). R3 assembles expert technology team to lead distributed ledger initiative. Retrieved from http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/564dd802e4b0dff76870e198/1447942146527/PRESS+RELEASE+R3+tech+maangement+team+%2811-19-15%29.pdf

Richards, T. (2016, February 23). The Ongoing Evolution of the Australian Payments System. Reserve Bank of Australia. Retrieved from http://www.rba.gov.au/speeches/2016/sp-so-2016-02-23.html

Rizzo, P. (2015a, August 5). Overstock Unveils Blockchain Trading Platform at Nasdaq Event. *Coindesk*. Retrieved from http://www.coindesk.com/overstock-unveils-blockchain-trading-platform-to/

Rizzo, P. (2015b, August 25). Why Symbiont Believes Blockchain Securities Are Wall Street's Future. *CoinDesk*. Retrieved from http://www.coindesk.com/why-symbiont-believes-blockchain-securities-are-wall-streets-future/

Rizzo, P. (2016). IBM Director Declares "We"re All in on Blockchain'. Retrieved March 10, 2016, from http://www.coindesk.com/ibm-director-all-in-blockchain/

Singh, M. (2013). The Changing Collateral Space.

States of Jersey. (2015). *Regulation of Virtual Currency: Consultation Paper*. Retrieved from http://www.statesassembly.gov.je/AssemblyReports/2015/R.80-2015.pdf

Swann, G. M. P. (2009). *The Economics of Innovation: An Introduction*. *2009*. Edward Elgar Publishing.

Swanson, T. (2015a). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*.

Swanson, T. (2015b). *Watermarked tokens and pseudonymity on public blockchains*. Retrieved from http://www.distributedledgergroup.com/s/Watermarked-tokens-and-pseudonymity-on-public-blockchains-Swanson.pdf

SWIFT. (2015a). Hyperledger wins the 2015 Innotribe Startup Challenge. Retrieved December 16, 2015, from http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2015/PR_2015_ISC_Finale_winner.xml

SWIFT. (2015b). Innotribe@Sibos 2015 - New Kids on the Block(chain) platform. Retrieved January 31, 2016, from https://www.youtube.com/watch?v=mLWhU3f0xlc

The Economist. (2011). America's dodgy financial plumbing: Too big a fail count | The Economist. *The Economist*. Retrieved from http://www.economist.com/node/18774844?frsc=dg|a

The Economist. (2015). Special Report: International banking. *The Economist*. Retrieved from https://vpn.lboro.ac.uk/+CSCO+0h756767633A2F2F6A6A6A2E72706261627A7666672E70627A++/news/special-report/21650290-financial-technology-will-make-banks-more-vulnerable-and-less-profitable-it

Vigna, P., & Casey, M. (2016). *The Age of Crypto Currency*. New York: Picador St Martin's Press. Retrieved from https://theageofcryptocurrency.com/

von Gunten, C., & Mainelli, M. (2014). Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Retrieved June 7, 2015, from http://www.longfinance.net/lf-research.html?id=903

Wikipedia. (2015). List of Crytpocurrencies. Retrieved from https://en.wikipedia.org/wiki/List_of_cryptocurrencies

Wikipediia. (2015). List of Countries by Energy Consumption. Retrieved from https://en.wikipedia.org/wiki/List_of_countries_by_electricity_consumption

Wilkins, C. (2015). Innovation, Central-Bank Style - Bank of Canada. Retrieved from http://www.bankofcanada.ca/2015/11/innovation-central-bank-style/

World Economic Forum. (2015). *The Future of Financial Services*. Retrieved from http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

World Economic Forum. (2016). Disruptive Innovation in Financial Services. Retrieved January 31, 2016, from http://www.weforum.org/global-challenges/projects/disruptive-innovation-in-financial-services/

Wright, A., & De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Retrieved from http://papers.ssrn.com/abstract=2580664

Xiaochuan, Z. (2016). Transcript of Governor Zhou Xiaochuan's Exclusive Interview with Caixin Weekly. Retrieved March 13, 2016, from http://www.pbc.gov.cn/english/130721/3017134/index.html

Yu, M. S. W. (2013). Supply chain management and financial performance: literature review and future directionsnull. *International Journal of Operations & Production Management*, *33*(10), 1283–1317. http://doi.org/10.1108/IJOPM-03-2012-0112

## Appendix 1. Public domain materials

In this Appendix we review some of the sources we have found most useful in writing this report and take the opportunity to discuss additional issues concerning the potential application of distributed ledgers in financial services (not just in securities settlement).

### Our own previous work.

This report builds on a substantial body of our own previous research, stretching bank many years, on distributed ledgers, securities settlement and other related topics. The work of Michael Mainelli and his colleagues on mutual distributed ledgers can be accessed via the Z/Yen website, via http://www.zyen.com/what-we-do/mutual-distributed-ledgers.html. Z/Yen first did work on distributed ledgers – in a non-financial context – as long ago as 1995. Their other projects include InterchainZ (completed) and IntereXchainZ (ongoing) which have explored the application of distributed ledgers in financial services with Z/Yen's industry partners, the Distributed Futures meetings on the application of distributed ledger (http://www.zyen.com/events/distributed-futures.html) and their work on distributed ledgers in insurance (von Gunten & Mainelli, 2014 and ongoing further research).

Alistair Milne has written many research papers over the past fifteen years on financial infrastructure (retail payments, securities clearing and settlement and technology standards). His recent work on standard setting in global capital markets is at http://www.financialstandards.lboro.ac.uk/index.html Other older papers can be found via SSRN http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=148057 and https://ideas.repec.org/f/pmi529.html (there are many other papers on bank capital and financial regulation, so scroll down for work on retail payments, the global LEI, common language in financial markets and securities settlement.)

Coming as we both do from a background of industry practice and regulatory policy, is one reason why we take the position that distributed ledgers are not really so new. We believe that distributed ledgers are best viewed as just another database technology, albeit one making clever use of cryptography to provide flexible but secure distributed access. Most of the cryptography that underpins the authentication and permissioning of ledger participants and the validation of ledger

entries have been around for almost four decades. The peer-to-peer distributed architecture has been around in various forms for over two decades. The novelty is the relatively recent recognition, triggered in no small part by the publicity and debate over Bitcoin, of the potentially transformative impact of distributed ledgers providing a common and agreed record of data in many different applications, both financial and non-financial.

### Terminological disputes: what is a distributed ledger?

One problematic issue is that the many contributors to current debate about the practical application of blockchain or distributed ledger technologies have not yet settled on an agreed terminology. The same terms can be used to mean different things or different terms to mean the same thing.

Our preferred terminology (from Mainelli, 2016 and restated in footnote 1 above) is as follows. A **ledger** is a record of transactions; **distributed** means divided among several or many, in multiple locations; **mutual** is shared in common, or owned by a community; a **mutual distributed ledger (MDL)** is a record of transactions shared in common and stored in multiple locations; and a **mutual distributed ledger technology** is a technology that provides an immutable record of transactions shared in common and stored in multiple locations.

A recent UK Government Office for Science Report provides an alternative and also useful definition:

*"A distributed ledger is … an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of 'keys' and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network." (Government Office for Science, 2016, page 5)*

This same report provides some useful distinctions (ibid, page 17-18). A traditional ledger has one central or master copy (as we have discussed in Section 4, this

requires a trusted third party to maintain the ledger). A distributed ledger is a type of data base that is spread across multiple sites, countries or institutions with no single central copy. They also prefer ‘block chain’ i.e. two separate words to ‘blockchain’, we adopt the latter, more common, usage though arguably from the perspective of English language usage block is a modifier of chain and should therefore be a separate word.

A blockchain is one type of shared database that takes a number of records and combines them together in a block which is then ‘chained’ to the next block (using of course a cryptographic validation of the link). Each block of the chain needs to be validated i.e. agreed by some process of consensus amongst the network participants. Bitcoin ‘mining’ is one way of achieving this consensus, through expenditure of real resources (electricity) on searching for the cryptographic key that validates the block. A number of other consensus algorithms (many are based on some kind of voting) are possible.

There is also not yet terminological agreement on whether a blockchain is also a distributed ledger. In this report we consider blockchains as one form of distributed ledgers. The Government Office for Science report prefer to define a distributed ledger as one in which entries are added and validated one by one rather than in blocks, so in their terminology a blockchain is not a distributed ledger. They also prefer the term ‘shared ledger’ (originating with Richard Gendal Brown) as a general term to describe all ledgers with that are shared by an industry or consortium.

Figure 2, created by Consult Hyperion, provides a more detailed breakdown of different types of ledgers, highlighting the distinction between unpermissioned ledgers (anyone can use them) and permissioned ledgers, and also some of the possibilities for maintaining (in our terminology validating) ledger entries.

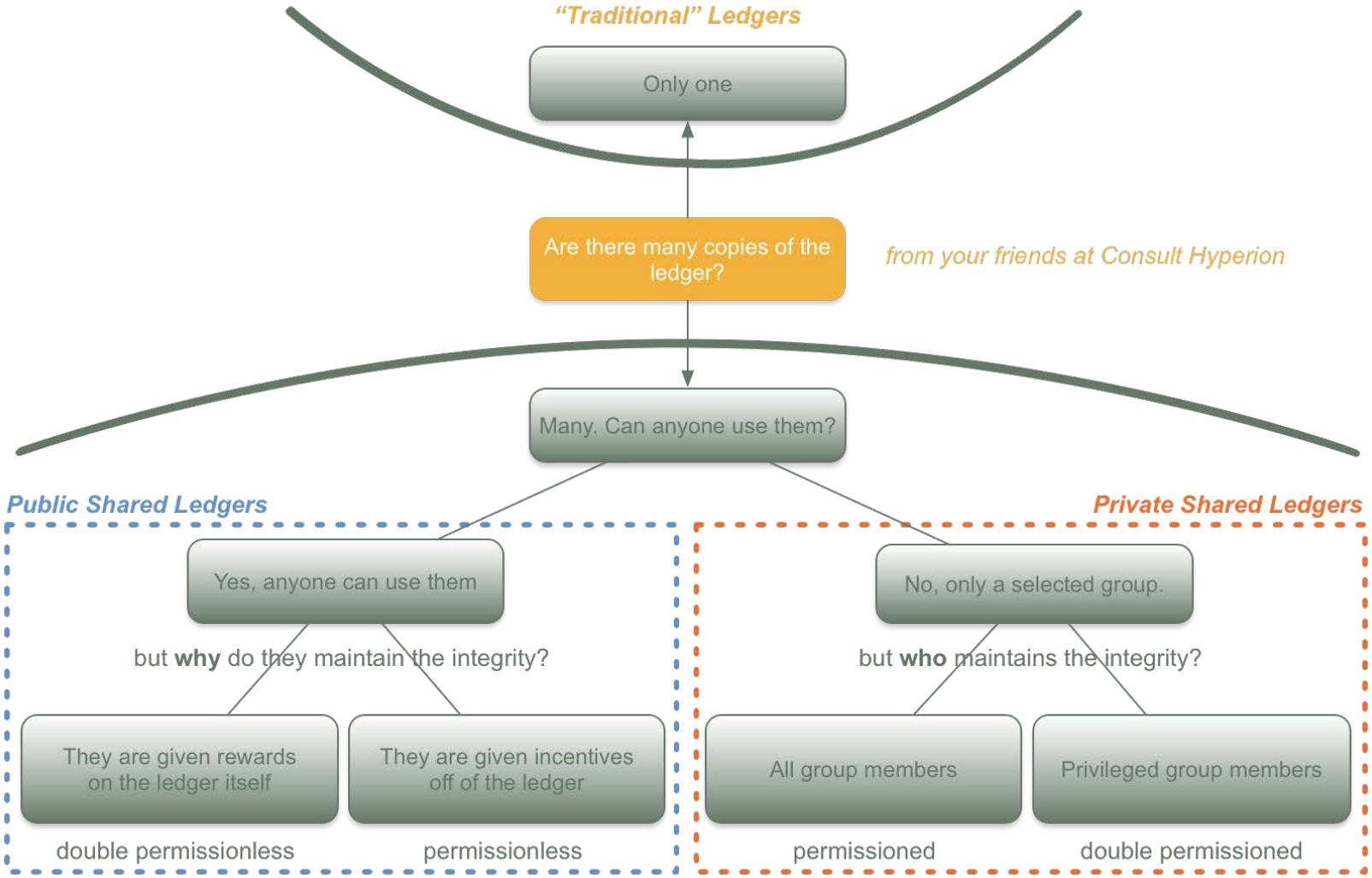


**Figure 2: a classification of different ledgers** (Consult Hyperion, https://www.flickr.com/photos/32714731@N05/24489055235/ )

Finally note that we use the additional qualifier *mutual* distributed ledgers, in order to distinguish ledgers that offer equal access and ownership to a number of firms and/or individuals from ledgers which are maintained and accessed on a distributed basis within a particular organisation. Mutual distributed ledgers may be limited to a selected group or fully public with anyone entitled to use them.

### The boom in FinTech and blockchain.

We have reported above, in Section 2, that FinTech start-ups have raised a total of $12.1bn dollars globally in 2014 and over $1.1bn in cumulative venture capital has been raised for Bitcoin and blockchain related ventures. Accenture summarise the strategic challenge: "*It is clear that the digital revolution in financial services is under way, but the impact on current banking players is not as well defined. Digital disruption has the potential to shrink the role and relevance of today's banks, and simultaneously help them create better, faster, cheaper services that make them an even more essential part of everyday life for institutions and individuals. To make the impact positive, banks are acknowledging that they need to shake themselves out of institutional complacency and recognise that merely navigating waves of regulation and waiting for interest rates to rise won't protect them from obsolescence.*" (Accenture, 2015)

These ventures have focused on five areas: payments instruments and processes; data analytics; capital markets technologies; bank credit and corporate financial information; and personal financial management.[38] Some are radical alternatives to existing financial services. Many are evolutions of existing practice and are often eventually bought out by incumbent firms.

New financial tech-based (FinTech) firms have already been successful in attracting certain lines of business away from established banks, mostly in commercial banking rather than capital markets activities. Examples include mobile and internet payments, unsecured P2P personal lending (or 'market place lending' as it is referred to in the US), retail foreign exchange and invoice financing (for a recent survey see The Economist, 2015). The major disruption to date in capital market

[38] (Accenture, 2015)

transactions has been in the front, not back, office, with a substantial share of trading now undertaken by standalone high frequency trading firms rather than humans executing client orders and the emergence of new investment strategies based on 'big data' (exploiting data from social media platforms).

There is an immense amount of online coverage of the many Bitcoin and blockchain ventures. www.coindesk.com covers most of this activity. The activities of these start-ups include Bitcoin mining, Bitcoin wallets, payments solutions build on Bitcoin as well at those using the Bitcoin blockchain as a tool for validation of other transactions i.e. this venture capital funding is being provided both to Bitcoin companies and Blockchain companies. Some seek to use the Bitcoin blockchain to support securities settlement, for example using a so called 'coloured coin' approach in which the Bitcoin blockchain is used only for recording of verified transactions and becomes a permissioned system for this particular application because it is not open to all members of the Bitcoin network.[39] Alongside this are many other announced initiatives seeking to develop some form of securities settlement application using mutual distributed ledgers but *not* the Bitcoin blockchain.

We have not attempted to review all of the announcements about the application of distributed ledger to securities settlement (there are very many as exemplified by the now quite bewildering montages of different logos presented at industry conferences and in consultancy reports).[40] Many can be characterised as 'vapourware' – announcements of a product without both a fully functioning product and an established client base. It is difficult to assess which of the many initiatives in the market place are to be taken seriously.

What we have found useful is to identify three main groups of initiatives that seem to be making a serious effort to develop solutions applicable to the settlement of securities trades and other financial transactions.

---

[39] For a summary of this approach see (Lykke, 2016). It is though questionable whether the transfer of such 'coloured Bitcoins' can ever be accepted as a legally final transfer of financial assets without a subsequent process of clearing and settlement outside of the blockchain (see Swanson, 2015b).
[40] One attempt at such an overview is (Harris, 2015)

1. The first are using newly developed blockchain technologies in a specific business context. This is exemplified by NASDAQ who have applied a blockchain technology to support settlement in 'pre-IPO' (or grey market) trading.[41] This particular initiative employs the 'coloured' Bitcoin approach, linking securities to small value fractions of a bitcoin which can then be settled through a transaction.
2. The second are developing radical alternatives to existing market arrangements, developing technical solutions for issuing securities in cryptographically secured digital form and trading them securely on a shared platform, with the hope of breaking down some of the barriers to entry in financial market trading. Examples include t0, the subsidiary of the online retailer Overstock and Symbiont.[42] While many of these are technologically impressive these start-ups have yet to demonstrate that any substantial adoption by established market participants.
3. The third group are working closely with established market participants. The three initiatives to which we have examined most closely Digital Asset Holdings, R3 and SETL fall into this category;[43] as does the work on mutual distributed ledgers of Z/Yen.[44]

Those working on blockchain as a radical alternative to existing financial market arrangements sometimes view with suspicion those initiatives working closely with established firms, concerned that these are protecting vested interests and protecting the privately profitable but socially damaging practices of the major financial market firms. See for example the reported criticism by Overstock CEO Patrick Byrne of R3 at a 2015 blockchain conference.[45] The view suggested by our own work is though that – due to the operational complexities of securities settlement – only initiatives that are working closely with established firms are likely to have any chance at all of achieving widespread adoption, and even these may well fail. The notion that the novel technology offered some blockchain startup can capture the

[41] (Prisco, 2015)
[42] See (Rizzo, 2015a, 2015b)
[43] See footnotes 14.-16. for more detail.
[44] See http://www.zyen.com/what-we-do/mutual-distributed-ledgers.html
[45] Reported in (Das, 2015).

bulk of global financial market settlement, becoming the Apple or Facebook of global finance, transforming post-trade operations for the social good and enjoying massive profits is simplistic. As we have argued the challenge of applying mutual distributed ledger in securities settlement is only to a small degree about the technology, it is largely about the adoption of co-ordinated and standardised business processes.

Nonetheless we believe there is a genuine concern that established firms, focused on short term returns, will not do enough to exploit the full potential for using mutual distributed ledger technologies to increase the efficiency of post-trade operations. We can draw support on this point from the substantial research literature on the economics of network innovation, especially in relation to the problem of 'excess inertia'.[46] Some industries, for example mobile telephony or internet commerce, are characterised by rapid and sometimes disruptive technical change. In others though– and this applies to most financial services – technological innovation adopted in isolation does not provide firms with a competitive advantage, and instead a co-ordinated and agreed adoption of a new technology is required. In this situation the private incentives for adoption are weak.[47] This is a form of market failure and public policy intervention may be required to promote technological innovation.

We also comment on one more radical view, ably documented for example by (Vigna & Casey, 2016), that cryptocurrencies and blockchain will prove to be as economically and socially important as the internet ushering in a new era of decentralised exchange without the need for large institutions and minimal central oversight. This seems to us somewhat oversimplified. A quotation from their book will give an idea of this perspective on blockchain

> "*Is a clash building between these two movements, the corporate world's concentration of wealth and power, and Silicon Valley's reempowerment of*

[46] Many references can be provided, for example (David & Greenstein, 1990; David & Steinmueller, 1994; Farrell & Saloner, 1986; Swann, 2009). (Milne, 2006) makes the excess inertia argument for the retail payments industry.

[47] An alternative outcome for such a 'co-ordination game' is that there is first slow adoption of innovation, and then a tipping point, after which adoption is very rapid. There are examples of such tipping points in financial services, the most well known the capture of the trading in the Bund futures contract from LIFEE by the Eurex exchange described in (Cantillon & Yin, 2008), but this is an unusual case. Our judgement is that this cannot happen in securities settlement because it is so difficult for alternative technologies to co-exist.

> *the individual? Perhaps these trends can continue to exist if the decentralising movement remains limited to areas of the economy don't bleed into the larger areas that Big Business dominates. But that's not what the proponents of this technology foresee – especially those in the cryptocurrency sector. They believe that decentralisation is just getting started and that the centralised economic and political establishments – even governments and nation-states, those ultimate centralized loci of power – will be disrupted by it. If so, cryptocurrencies and blockchain technology could ride that wave triumphantly.*" (Vigna & Casey, 2016 pp 277-278)

Yes, a shift to greater decentralisation in financial exchange may be possible and could yield substantial economic benefits in terms of much reduced costs and efficiency also wider access to financial services. But – paradoxically – to overcome the vested interest of many existing institutions that stand to lose market position and margin from such developments, such a decentralisation will require a focused and vigorous centralised action by regulators and other public authorities to remove barriers to the adoption of the new technology. The full potential of mutual distributed ledgers in securities settlement and other financial services will not come about through the free play of market forces alone.

An illustration of this point is that the major disruption that has so far affected global capital markets – the fragmentation of exchange venues and the associated rise of high frequency trading and of proprietary dark pools – was in fact the product of regulatory intervention. The transformation of equity trading – which has done a great deal to reduce transaction costs although also exposed the market to that new forms of computer driven instability the 'flash crash' and introduced new concerns about some market participants having advantages of speed and location that allow them to exploit others – would not have taken place without Reg-NMS in the United States and MIFID in Europe creating the possibility of competition between trading venues.

Without such policy intervention the most likely outcome is that the new providers of mutual distributed ledger services such as Digital Assets, R3, SETL and others, following the path of least resistance, will focus on services for which there is a clear

interest from established firms. This may mean for example that the challenge of lack of co-ordination of data between firms is tackled on a bilateral basis, through something similar in the post-trading context of the ISDA master agreements used for OTC derivative trading. An early indication of this is the recent release of information about the R3 platform "Corda" in (Brown, 2016) who notes amongst other attributes that "*Corda has no unnecessary global sharing of data: only those parties with a legitimate need to know can see the data within an agreement. Corda choreographs workflow between firms without a central controller. Corda achieves consensus between firms at the level of individual deals, not the level of the system. Corda's design directly enables regulatory and supervisory observer nodes. Corda transactions are validated by parties to the transaction rather than a broader pool of unrelated validators. Corda supports a variety of consensus mechanisms…* "

Corda is thus *not* a mutual distributed ledger; rather it rather supports bilateral data sharing. It also appears from this announcement that the development of Corda is putting a lot of emphasis on support for smart contracts, illustrating a further point that smart contracts and mutual distributed ledgers are two independent innovations, not facets of the same technology. The adoption of Corda remains yet to be proven, but even if it is and so delivers substantial reduction in the costs of manual reconciliation of transaction data between firms, this does not sound like the transformation of post-trade processes in global capital markets that many involved in the discussion of blockchain and settlement envisage.

Much of the initial interest in Bitcoin has indeed been inspired by a libertarian vision of peer-to-peer systems of exchange in which transactions take place without the need for either financial intermediaries or government regulation. As we have discussed the Bitcoin network is completely open or 'unpermissioned'. Anyone with access to the internet can join the network and acquire coins either by purchase using conventional money or by devoting resources to the 'mining' used to validate transactions. Another way of viewing this is that over 7 billion people on the planet *are* 'permissioned' to participate at any time. This is in stark contrast to conventional arrangements where financial institutions make final exchange that settles bank payments or the exchange of securities and where detailed checks of identity under KYC, AML and other regulations are required in order to open accounts.

While a libertarian perspective continues have powerful appeal to many proponents of Bitcoin and other cryptocurrencies, almost all financial market participants believe that unpermissioned ledgers such as the Bitcoin blockchain can have only limited application in capital market transactions. This is for two reasons: regulation and efficiency (speed-of-execution and volume constraints).

Virtually all wholesale financial services are regulated. The availability of Bitcoin protocol and related technologies does not relieve firms of the responsibility to comply with all relevant laws and regulations and to properly manage the risks arising in their business relationships. It is not possible to allow anyone completely free access to the networks that support capital market transactions. Clients and their transactions must be subject to KYC and AML scrutiny. Counterparty risk must be monitored and managed either bilaterally or through central counterparties.

Another barrier to applying unpermissioned ledgers employed in Bitcoin and many other cryptocurrencies is inefficiency of validation. 'Unpermissioned' cryptocurrencies must handle participants globally who are not known and for whom there are no legal or other institutional arrangements to ensure honest and trustworthy behaviour. This in turn requires validation methods, for example the Bitcoin 'mining', which are typically slow (varying unpredictably from several seconds to minutes) and resource intensive.[48] In a permissioned environment, such as a regulated financial market in which all participants are subject to approval in order to trade, such inefficient validation seems unnecessary.[49]

Some form of validation is however absolutely at the heart of financial clearing and settlement. The reliable functioning of securities, foreign exchange and derivative markets and also domestic payments, rest on minimising uncertainty about the completion of transactions. Participants need predictable finality. If trades are delayed, then participants need to be fully informed about the revised time of finality.

---

[48] The expense, high level of energy consumption and variable time to confirmation of Bitcoin validation by 'proof of work' are subjects of considerable controversy. We need not go into fully into these controversies here (though Appendix 1 provides some further discussion). Even if 'proof of work' like that used in Bitcoin was quick and resource efficient, and it seems fairly clear it is not, established financial institutions will still prefer a permissioned environment in which 'proof of work' is unnecessary.

[49] (Swanson, 2015a) discusses permissioned v. permissionless distributed ledgers further.

This means that even if using a permissioned mutual distributed ledger there still needs to be some process for ensuring that the different copies of the ledger held on all the network nodes are consistent. If it turns out different copies are not consistent, then there needs to be a process (a 'consensus algorithm') for eliminating inconsistencies over a predictable time frame.

We should mention the rather sterile debate about whether the mutual distributed ledgers being developed by firms such as Digital Asset Holdings, R3 or SETL are really true blockchains. The origin of the term blockchain is associated with Satoshi Nakamoto's original paper of 2008 which uses the term block and describes the chaining of validated blocks, although not the actual phrase 'blockchain'.[50] The term 'blockchain' has since become standard for describing the arrangements used by Bitcoin, in which digitally signed Bitcoin transactions are collected into blocks before being subsequently verified as authentic by so called 'miners' through a resource intensive process known as 'proof of work' i.e. mechanically searching to find a digital key (a 'nonce') which is uniquely associated with the information digitally recorded in the block.[51] These verified blocks are time ordered, so that each bitcoin can be demonstrated as genuine by tracing it's transaction history back, block by block, until locating its genesis block, i.e. the block in which it was first created as a reward for Bitcoin mining.[52]

---

[50] *"The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it."* (Nakamoto, 2008, pg 2)

[51] We oversimplify somewhat. We understand that a nonce is added but it is not the sole mechanism, miners. Miners will rearrange several attributes (including a nonce) to create entropy such that the resulting value is beneath the target difficulty value.

[52] The reason for the mining is to rule out the possibility of malicious network participants collaborating to rewrite the transaction history. To do this they would need to find a nonce for an alternative false block containing including transactions that are 'double spends' and hence divert bitcoins from their true owners. This possibility of this 'forking' is all but ruled out by the requirement that when there are competing chains of blocks, the longest chain takes priority. Thus the probability of a small number of miners establishing a false record as definitive and hence be able to double spend their bitcoins is small because they will not have enough computing power to do this. A fuller description can be found from many sources, e.g. (Narayanan, Bonneau, Felten, Felten, & Goldfeder, 2016) . However there are concerns that skilled attackers could still find a way around the security of a public blockchain such as Bitcoin – one reason for preferring the additional protection of a permissioned distributed ledger.

Because of their permissioned structure, the mutual distributed ledgers being developed for application in securities settlement do not need to use exactly this block structure for verification. While there must still be some mechanism for ensuring agreement on the record of transactions in the ledger, this need not require a sequential record that can be traced back in time to the point at which securities are first entered on the ledger. Even if they are ordered sequentially they do not require proof-of-work of the kind employed in the Bitcoin block chain for validation because other network participants are trusted.

### A digression on the efficiency of the Bitcoin 'proof of work'.

While not directly relevant to our research – since it is clear that any application of mutual distributed ledger in financial services will be in a permissioned environment that need not use anything similar to the Bitcoin 'proof of work' to validate transactions – we briefly here summarise two controversies about the resource efficiency and reliability of Bitcoin approach to validation (i.e. the mining to find the hashes that validate each block in the Bitcoin blockchain).

The first controversy is about the energy consumption of cryptocurrencies. (Malmo, 2015) highlighted a widely circulated but difficult to verify figure that the Bitcoin network consumes around 250MW to 500MW around the clock. From this he worked out that each Bitcoin transaction uses about the same amount of electricity for validation as is required to power the average American home for 1.57 days. Previously (O'Dwyer & Malone, 2014) concluded that "currently the entire Bitcoin mining network is on par with Ireland for electricity consumption".

If true, these figures pose significant questions about long-term transaction costs using Bitcoin, and also question its long-term sustainability in environmental terms. There are many 'clones' of Bitcoin as well (Wikipedia, 2015 reports that eight of these have a market capitalisation of over $10mn – up-to-date capitalisation and energy consumption can be found here - http://www.coinwarz.com/cryptocurrency) and a variety of other competing approaches to cryptocurrency transactions such as Ethereum and Ripple using other validation methods. Comparative energy consumption is an important criterion in deciding how, where, when and which cryptocurrency to use.

Others dispute the claim that electricity consumption and per transaction dollar costs of the Bitcoin network are anything like this high. One consideration is that measured in watts/gigahash-second (W/Gh-S) mining efficiency has dramatically improved with the introduction of ASICs (application specific integrated circuits) for mining.[53] The home PCs that were first used for BitCoin mining when the Network launched in 2009 ran at 650 W/Gh-S, first generation ASICs at 10 W/Gh-S. Today rates of 0.7 W/Gh-S or even more are achievable from machines sold retail for individuals who want to try Bitcoin mining.[54] At the same time successful mining is increasingly being undertaken by a small number of industrial scale miners, financed by substantial venture capital, who are reportedly able to achieve efficiencies of 0.025 W/Gh-S or better.[55]

These dramatic gains in processing efficiency are not however the whole story. The problem is that as the efficiency of legitimate mining improves, so does the efficiency of any 'rogue' miners using the latest generation ASIC machines to try and validate a false transaction block e.g. one in which Bitcoins are used for a second time and diverted away from their true owners, the very problem that validation through mining is meant to prevent. To counter rogue mining the Bitcoin network adjusts the difficulty of the hash rate to ensure that the average time for the validation of a new block remains at around 10 minutes. As mining efficiency improves so does the difficulty of finding a number that validates a block with no net saving in electricity. The integrity of Bitcoin depends on validation being expensive, in order to ensure that the resource required by a rogue miner to validate a false block costs more than the benefit form misdirected Bitcoin.

The resulting 'arms race' has resulted in an extraordinary increase in the hash rate for the entire Bitcoin network.[56] Whereas in January 2011 the entirety of mining

---

[53] A hash is an attempt by a miner using trial and error to find a nonce that solves the required cryptographic puzzle and hence validates a transaction block. A giga-hash is $10^9$ hashes. So an mining efficiency of 1 watt/gigahash-second means a miner will need to consume electricity at a rate of 1 W/sec or 3.6KW/hr in order to make $10^9$ attempts every second at finding a nonce or key that validates the transaction block.
[54] Based on the highest performance machines advertised on Ebay e.g. http://www.ebay.com/gds/Best-ASIC-Miners-/10000000205733242/g.html
[55] See (Coindesk, 2015b) for discussion of one such industrial scale miner.
[56] Blockchain.info https://blockchain.info/charts/hash-rate Blockchain.info https://blockchain.info/charts/hash-rate

operations in the Bitcoin network were conducted at a rate of around 1,000 gigahashes per sec (Gh-s); by January 2012 this had risen to around 10,000 Gh-s; by January 2015 to around 5,000,000 Gh-s and by March 2016 to over 1,200,000,000 Gh-s, i.e. each second there were more than $10^{18}$ trial and error attempts to find a nonce that validates a Bitcoin block. At 1 watt per Gh/s this works out to a power consumption for the Bitcoin network of around 1,200 MW. This is 28,800 MWh each day, or about 10,500 GWh per year. This is a bit less than half of Ireland's 26,100 GWh per year.[57] Note, this focuses only on the mining and ignores other energy consumption in networks and routers. The most efficient miners though are probably already operating at closer to 0.1. If the entire network achieved this efficiency total electricity consumption will be 120 MW about 1,050 GWh per year, or a little less than the annual electricity consumption of Swaziland.

Actual consumption is probably somewhere between these extremes, since some inefficient miners still make sufficient profit to keep mining. Suppose the Bitcoin network uses the intermediate consumption rate of 200MW around the clock which works out at 4,800 MWh per day or approximately 1.7 GWh per year.[58] This is about one fiftieth of the annual electricity consumption of Belgium in 2008 and close to the 2008 annual electricity consumption of Senegal. The electricity consumption of BitCoin mining is therefore high, even if not quite as high as some have suggested.

The same assumptions can also be used to generate an electricity cost per-transaction. Thus 4,800 MW hours per day in the Bitcoin network applied to 100,000 daily transactions implies that each transaction requires approximately 50 KW hours of electricity for validation. At the cheap wholesale electricity rate available to the biggest and most efficient China based miners of 5¢ per KW hour that works out at $2.50 per transaction.

---

[57] All individual country electricity consumption figures are from the CIA as reported in (Wikipediia, 2015)

[58] (Croman et al., 2016) using a slightly more detailed analysis arrive at a similar estimate of 200MW electricity consumption for the entire Bitcoin network and an electricity cost of $3.6 per transaction. They also estimate hardware costs arriving at a total per transaction cost of $6.1. These estimates are though upper bounds, depending on the efficiency of throughput. Lower bound including hardware is as low as $1.4 per transaction. See their Table 1.

This can be compared with an estimate of revenues per transaction Total ‘mining’ revenues are currently about 3,600 newly created Bitcoins per day – which at current market price of Bitcoin of close to $400 are worth approximately $400 x 3,600 = $1.44mn for 100,000 daily transactions. Thus the mining revenues across the entire network work from creation of new Bitcoins work out at $14 per transaction (this ignores any additional revenues from transaction fees paid by Bitcoin users). Thus the most efficient miners (whose electricity costs are even lower, but who are spending a lot on hardware) are making substantial per transaction profits (but face the problem that their expensive hardware is rapidly falls behind the efficiency frontier as even more powerful ASIC machines are developed and employed on industrial scale).

Note though that the reward for a successful proof of work is set to keep halving as the number of Bitcoins increases, from 25 Bitcoins per block to 12.5 (this is dues to take place in mid-2016) and then from 12.5 to 6.25 per block (this is projected to happen in about 3 years from now).

The second and more recent controversy – one on which we have spent relatively little time – surrounds governance problems that have emerged over the past few months in the Bitcoin network. Our summary draws mainly on (Belshe, 2016; Hagelstrom, 2016; Palmer, 2016).

These governance problems have emerged because of a technical problem with Bitcoin. A block size limit of 1MB hardcoded into the original Bitcoin software has in recent months started to cause transaction delays. We understand that the 1MB limit places a theoretical maximum of around 300,000 Bitcoin transactions per day, but that delays emerge at lower transaction rates because they are not evenly spaced around the 24 hours of the day. Since the launch of Bitcoin it has taken approximately 10 minutes for payments to be initially validated (the average time for block validation, although for complete finality it is necessary to wait until six blocks have been successively validated i.e. one hour, in order to avoid the possibility of the most recent blocks in the chain being replaced by a longer fork). Now however as transactions volumes have risen they are instead often being queued for up to 10 hours at busy times because miners are already tackling the maximum block size and must put additional transactions on hold.

One interim solution has been prioritisation of payments that are willing to pay a ‘transaction fee’ to miners and hence incentivising miners to place them earlier in queues for inclusion in blocks. But even those paying such transaction fees are suffering delays.

The reason this is a governance problem is that the decentralised nature of Bitcoin makes it difficult to agree and co-ordinate a change in software for the entire network, in this case for example replacing the old version with the lower 1MB block size limit with a newer version with a higher limit. There is disagreement about whether there should be a maximum block size at all, what that maximum should be and whether an increase in block size is indeed the best way to resolve the current problem of transaction delays. A key concern is excessive centralisation. Larger block sizes could favour a small number of large miners, although in practice such centralisation is already happening anyway. There are also concerns about computational efficiency with large block sizes. As a result not all Bitcoin network participants agree on how to deal with this technical problem.

Bitcoin does allow the software to evolve. It is possible for two versions to run alongside each other, compatibly (a so called ‘soft fork’) and once 75% of nodes adopt this then becomes the new software that is used by all. A first attempt at a new version, Bitcoin-XT incorporating an eventual increase in the block size limit to 8MB, failed because it did not attract sufficient uptake. A more recently released coding Bitcoin Classic, which increases the blocksize to only 2MB looks to have a better chance of acceptance. There are though other proposed solutions not involving an increase in block size, notably ‘Segregated Witness’ (which reduces the information that needs to be incorporated in each transaction thus allowing more transactions within a given maximum block size) and ‘Lightening Fork’ (which seeks to provide a ‘side chain’ that takes smaller Bitcoin payments off the Bitcoin network).

The debate on which solution should be adopted to deal with this technical problem has become acrimonious and sometimes personal (for example with accusations of serving certain vested interests). A lot of emotion has been expressed about the possibility of a ‘hard fork’ that Bitcoin might split into two incompatible systems. Likely that one solution will eventually win out, without such a hard fork, but this does not guarantee that similar governance problems do not emerge in the future.

## Why is there considered to be so much potential value from the application of distributed ledgers in financial services?

We here mention a few of the sources that have shaped our perceptions and the framing of our hypotheses. Much valuable and technical practical insight can be gained from Richard Gendal Brown's blog http://gendal.me/ (Gendal Brown is now chief technology officer at R3). One contrast he draws (in Brown, 2015a of 15th Aug and Brown, 2015b of 26th Aug)(in Brown, 2015a of 15th Aug and Brown, 2015b of 26th Aug) is between two contrasting cultures in the debates about blockchain and finance. One is a security engineering perspective, driven by fear of technical failure and prioritising the need to ensure cryptographic security and immunity from external attack. The other, typical of the operational functions in large organisations such as banks, takes a different engineering perspective driven instead by fear of practical failure. As he writes:

"*I often argue for the importance of blockchain and distributed ledger technology by using the following chain of logic:*

*Bitcoin's architecture solved the problem of censorship-resistant digital cash*

*But few, if any, financial firms are interested in censorship-resistant digital cash. So why are they looking at this technology?*

*Because some principles underpinning Bitcoin's architecture – shared ledgers, for example – could be relevant to problems that banks face.*

*Sure, a blockchain or a replicated shared ledger could indeed be useful to banks. Perhaps it could reduce the need for reconciliation between firms if they all ran off a single ledger, for example. But this says nothing about whether blockchains are the optimal solution to any particular problem in banking. That still has to be argued, of course.*"

This distinction is well worth keeping in mind in the debates about blockchain and its applications in finance. The original Bitcoin blockchain is an elegant solution to a particular problem, the exchange of digital claims on value in an environment with no institutional constraints on the behaviour of network participants and where strong cryptographic protection is required against the possibility of malicious behaviour.

While there is agreement across the industry that many current processes are unnecessarily inefficient and these inefficiencies could be substantially reduced by adopting some form of shared ledgers, there is a huge amount still to be done to agree on the details. We have further argued in this paper that integration with existing business processes and legacy systems will be a crucial challenge for the effective adoption of distributed ledger in securities.

A persuasive statement about the potential benefits of applying distributed ledger to security settlement is provided in an online talk from the 2015 SIBOS conference by Blythe Masters, the chief executive of Digital Asset Holdings. She says:

*"What exactly is a distributed ledger? Simply put these are shared, replicated and decentralised transaction networks based on open-source internet protocol that draw on cryptographic techniques to secure the information that is recorded on those ledgers; a technology that has grown out of innovations in internet bandwidth, computing power and the science of cryptography. What does a shared distributed ledger really mean especially in the financial services context? Well what it means is that instead of each independent party to financial transactions keeping their own independent and private record of transaction information independently, instead there can be one master prime record or if you will golden record of the truth relating to a transaction history that acts as a single source of information to multiple different and independent parties as opposed to the status quo today where everyone essentially maintains their own ledger of activity.*

*When different parties record the same transaction information inevitably this leads to inconsistencies and enormous amounts of effort, time and cost are put into subsequent reconciliation of these different sources of what should ultimately be the same data, being reconciled and addressing the errors and inconsistencies that result. … In the event that parties are able with confidence to share the same transactions record, and can share that transaction record and agree its validity at the inception of that transactions record then there is an enormous opportunity to reduce errors, reduce the time spent addressing and resolving those errors and it means that that same data can be accessed in real time and in a secure fashion at different locations, in different time zone and by different entities. The opportunity for efficiency gain here is truly quite breath-taking.*

*This also means the entire life cycle of a transaction including its execution subsequent netting, reconciliation of facts by the different parties that need to know, the buyer, the seller, their agents, the custodian, the central securities depository, a regulator for example, all those entities can rely on the same single source of information and agree on the validity of that transaction at the point when it is submitted for settlement rather than later in the process and after the fact….*

*The opportunities that we are talking are themselves significant because the markets that we are talking about are themselves gigantic, they are measured typically in the billions and trillions of dollars notional with the consequence that the benefit of reducing inefficiencies results in very large dollar cost savings measured well into the billions of dollars per annum and perhaps more important than the cost saving is the reduction of risk associated with being able to complete transactions in near real time after they have been agreed rather than allowing for lengthy delays during which time errors and inconsistencies in transaction records have to be addressed." (Masters, 2015, our transcription)*

While agreeing with Masters about the huge potential for reducing both costs and risks from using mutual distributed ledgers, our research findings highlight the substantial challenges involved in adapting existing business processes and integrating them with these new technologies.

Another valuable resource from the 2015 SIBOS conference is the Innotribe debate "New Kids on the Block(chain) platform" (available on YouTube (SWIFT, 2015b)). This hour long session presents a wide range of views on the potential applications of blockchain in finance, with contributions ranging from providers of cryptographic distributed ledger solutions, through start-up firms seeking to employ these new methods (in microfinance and securities settlement) to major banks. Perhaps the biggest point of agreement is that practical application is still some way off, one contributor for example arguing that we are looking still at 12-18 months of exploration, seeking to define practical needs, before crystallising on particular solutions. There is also a degree of scepticism about whether securities settlement presents the most obvious use case, that first application may well be in other financial applications.

A further useful document, amongst the many we have reviewed, is the World Economic Forum report on how disruptive innovations are reshaping financial services (World Economic Forum, 2015). This report – the fruit of 15 months of work based on interviews with around two hundred industry leaders and technical experts and fifty or so workshops – provides both overview and detail about the prospects for technical change in global financial services. While commenting on the near real-time settlement of payments achieved by decentralised digital payment and transfer solutions – they highlight Bitcoin, Ripple, Litecoin and Namecoin – they devote relatively little space to the discussion of distributed ledger or securities settlement.

What they do is identify six areas of financial activity where substantial technology driven change is occurring (Payments including decentralised digital payments and transfers, Insurance, Deposits and Lending, Capital raising including crowdfunding, Investment Management, and finally Capital Markets). The World Economic Forum is following up this project with a stream of work on distributed ledger technologies (see World Economic Forum, 2016), with some initial meetings around the January 2016 Davos forum, indicating their awareness of the substantial potential impact of this technology on financial services. Still there is no obvious reason from their work to date for thinking that the first successful financial applications of distributed ledger technologies will be to the settlement of securities in the major financial markets. i.e. our Hypothesis 2 about piecemeal development for establishing proof of concept could mean that securities settlement is far from being the first use case.

### More cautious perspectives and the case for co-ordinated and collaborative change

Two other recent reports seem to us to provide sensible and cautious appraisals of the new technology and challenge of practical business implementation in global financial markets. (Euroclear & Oliver Wyman, 2016) pose the question of what 'utopia' would look like if we were starting with a blank sheet of paper and designing processes in capital markets without any of the constraints of legacy systems or existing business practice. They summarise this utopia as follows (pg. 9):

"*The record of each security would be held on a flat accounting basis - that is, with multiple levels of beneficial ownership in a single ledger. There would be no need to operate data normalisation, reconcile internal systems, or agree exposures and*

*obligations. We would have standardised processes and services, shared reference data, standardised processing capabilities (such as reconciliations), near real time data and improved understanding of counterparty worthiness. For privileged participants such as regulators, we would have transparent data on holdings, among many other improvements.*"

They also consider how such a utopia might be implemented suggesting that this could be achieved with a relatively small number of mutual distributed ledgers, one for cash, on for securities, one for derivatives, plus one for funds and one for collateral pledged for margining (their Figure 3).

(Euroclear & Oliver Wyman, 2016) go on to consider the practical hurdles to adoption (pgs. 14-15). In their view while there are some technological challenges still to be met, in order to demonstrate the scalability that will be needed to support global capital market transactions, most of these hurdles are business and institutional. Law and regulation will need to accommodate and this will in some cases require new primary legislation, for example in the definition of the finality of settlement or regulations on the physical location of data. In their view a 'multiple skeleton key' approach may be also needed, allowing courts, regulators and others to view data and where appropriate enforce change of ownership without compliance by the existing owner, and also to securely managing anonymity and identity reliably, according to clearly stated and agreed rules. The industry will also have to develop effective common standards and governance for the mutual distributed ledgers and carefully manage the operational and business risks associated with migration.

The rest of their report considers the pathways to adoption, identifying a number of specific applications where this might take place first (they suggest pre-IPO securities trades, syndicated loans, depository receipts, KYC data sharing, collateral ledgers for margining, book running and fund portfolio management) with subsequent application to holding pricing data, market surveillance, securities servicing and regulatory reporting (Euroclear & Oliver Wyman, 2016 Figure 5) and suggesting that adoption will come about through a combination of displacement by start-up challengers (though many will fail), accommodation by incumbents (In their phrasing 'collaboration') and finally mandated uptake by regulators and law makers. Overall they believe that some initial proof of concept in limited test cases can be

expected over the next 24 months, that disruptive uptake in some areas of application (substantial in small less development markets, narrow in larger markets) taking 2-5 years and then broadening adoption and widespread agreement on standards and replacement of legacy systems taking  from 5 to 10 years out, and mass adoption in 10+ years (Euroclear & Oliver Wyman, 2016 Figure 7).

An even more cautiously realistic view is provided by a recent DTCC white paper on the adoption of mutual distributed ledgers in global capital markets (DTCC, 2016). They emphasise the long and substantial effort involved in developing the current system of securities transactions (pg. 2), which while certainly complex and arguably inefficient "…*provides the necessary stability, reliability and certainty that ensure global markets are efficient, transparent and cost effective.*"  Like us they argue (pg. 3) that "…*modernizing current practices and laws to enable real-time settlement are not dependent on the use of blockchain technologies."* i.e. reducing settlement time is a business process not a technology challenge.

As suggested by their title 'Embracing Disruption' (DTCC, 2016) see a lot of potential value in mutual distributed ledgers, in addressing particular problems such as: reconciliation (multiple versions of the truth in siloed layers of the financial system); technological vulnerabilities (such as exposure to cyber-attacks); unnecessary complexity requiring frequent manual intervention in business processes; and better suited to 24 hour, 7 days a week, 365days a year trading. But like us they also note limitations to distributed ledger technologies, including lack of integration with existing systems for data management and retrieval, the technical trade-offs in moving from centralised to decentralised processing (notably latency, as well as challenges of making these systems conform with national data privacy laws) and in a useful terminology the continued need for third parties to manage the 'trust boundary', for example ensuring that any off ledger assets (represented on the ledger but with physical of legal presence off ledger) are properly secured and the proper onboarding of ledger participants.

In sharp contrast to (Euroclear & Oliver Wyman, 2016), (DTCC, 2016) are sceptical about whether any significant uptake of distributed ledger will come through challenger initiatives. They rather take the view (pg. 11) that *"…this is a generational opportunity to reimagine the financial industry infrastructure, and this can only be*

*accomplished from a well-considered, collaborative, design approach*." and emphasise (pg. 10) the need for co-ordination *"Achieving this goal will require a collaborative rearchitecture of core industry processes and practices that were built over many decades, each somewhat differently and all requiring reconciliation with previous and subsequent systems. A collaborative industry modernization program that includes distributed ledger technology could reduce the process steps required for financial transactions and improve the security and resiliency of the remaining processing systems, thereby reducing costs and risks of transaction failure."*

Another dose of realism was provided by the January 2016 Blockchain Conference in San Francisco by IBM Global Blockchain Offering Director John Wolpert (we here rely on the report of this speech by Rizzo, 2016). Wolpert argued that many early blockchain implementations are 'first generation' implementations that suffer from deficiencies that will hold back their appeal to businesses. He emphasised the need for further development which he anticipates taking place through open-source development, most importantly the recently launched Hyperledger project of the Linux Foundation in which IBM but also R3, Digital Assets, SWIFT, ABN Amro, the CME Group and several others are participating (a later annouuncement after the Wolpert speech confirmed the participation of 30 founding members and code-sharing arrangements to promote the development of blockchain technology came after the Wolpert speech, see Linux Foundation, 2016).

An indication of the appeal of blockchain, revealed by Wolpert, is that when the Hyperledger project was first announced in December 2015, some 2,300 companies enquire about being part of the project. As reported by (Rizzo, 2016), Wolpert argues that *"You need a fabric that allows for lots of competition on platforms and huge competition on solutions. We need to evolve the Internet to become economically aware and this Internet is not going to be an application, it will be a fabric."* and concluded that *"It's either going to be a holy mess or it's going to change the world."*

To conclude, our reading of the current state of industry debate is that – while there is huge interest in distributed ledger technologies in a wide range of financial services and other applications – the practical ways forward are as yet far from clear.

To quote again from Richard Gendal-Brown:

"…*don't assume that today's blockchain platforms (permissioned or permissionless) are the (whole) answer, then surely we're back in the land of engineering, architecture and hard work? Perhaps this means that the combination of persistence, data models, APIs, consensus, identity and other components that we need won't all come from one firm. So a common language, some common vision and an ability to collaborate may become critical. Where is your distinct differentiation? Where would you fit in an overall stack?*" (Brown, 2015b)

## Appendix 2. Record of Focus Group Meeting of 25th Nov, 2015

This meeting was held under the Chatham House rule, i.e. all views are reportable but not attributable without permission.

### Initial discussion

Before addressing the three hypotheses there was a lively discussion about the factors driving interest in mutual distributed ledgers. As one participant put it: what would arrangements for settlement look like if we started with a 'blank piece of paper? We certainly would not have them as they are. But there needs to be a push for change. The switch out of paper-based processing forty years ago came about because existing ways of doing things "just became too painful". That's why it was ended. Are we reaching a similar situation today?

A central point is the level of costs that are passed on to customers. A recent study by Oliver Wyman suggests that the global industry devotes around $65-$80bn cost to post trade processing (although not everyone in the room accepted that the costs are quite so high). But it is not just about cost, it is also about security and certainty.

What is the underlying challenge? There is multiple mirroring of information. The problem is structural. Huge effort is devoted to reconciliation. There is recognition of how much information is there and could be made available and used, but is locked and has to be released. We need to substitute the complex with the simple. Technology allows new approaches. The global LEI is one example of success, but only one step.

Incremental change may not work, what is required is a whole new approach. How can we collectively change? Any proposed evolutionary path must be seen in this context. One major interest group is those who are really bearing the costs, i.e. fund administrators and behind them final investors, so we need to get them to influence the decisions of the intermediaries. Many of the data and operational costs are not in settlement *per se* but in corporate actions and fund management. Complicated but a key opportunity.

While agreed that there are ‘multiple versions of the truth’ we have to recognise that with such a huge problem this also means that there is a great deal to change. Executing such major change is far from straightforward. Two examples: T2S in Europe, took several years to execute, and the switch from T+3 to T+2 in the UK took a huge effort over more than a year. It is the management of change in business process around the technology, not the technology itself. What is needed is leadership.

The case for change will not be based just on short term commercial benefit. Someone needs to be wearing the diplomat’s hat. We need discussion and negotiation and a lot of challenging of ourselves. The appetite for change is real but far from easily achieved.

## Discussion of Hypotheses

*Hypothesis 1. Any mutual distributed ledger settlement of securities purchases (or other transactions in public financial markets) will need to use a ‘permissioned’ ledger, in which only a limited number of approved network participants can propose updates of the ledger and participate in verification. This contrasts with permissionless mutual distributed ledgers (of which the ‘Bitcoin Blockchain’ is the leading example) where anyone can join the network and all have equal rights to propose updates to the ledger and participate in verification.*

Discussion then moved to this first hypothesis. One observations on hypothesis 1 is that the issue is not “either/ or” there are several degrees of participation. Similarly we need to distinguish our concepts carefully. Do we mean ‘permissioned’ or ‘authenticated’? Are we using a network simply for transfer of value, authenticated and validated, or is it supporting other functions?

There are many long standing examples of shared networks without central storage. In this respect mutual distributed ledgers are far from new. The internet is based on https and certification i.e. it is ‘authenticated’. This is content independent, whatever it is can be wrapped using public/ private key PKI. Another example is SWIFT, also a shared backbone. There are many commonalities (for example open v. closed i.e. who can *read* it but not *action* it.)

The novelty in modern mutual distributed ledger is the added value of the supporting cryptography. It offers completely secure differentiation of administrative privileges and participation. All of this can be included in a configuration file. This allows great flexibility: two man days not person years to reorganize the arrangement of a system. But this needs getting policies clear from the outset in order to allow cryptography to do the heavy lifting.

This prominence now given to cryptography is closely related to the huge changes in data storage and data access. 15 years ago hardware was in its own datacenter. Now we are using the cloud and configuring data access and verification. One possibility for example is having regulators as nodes on the network, with appropriate permissioning to ensure compliance with confidentiality and other legal requirements.

Several raised concerns about responsibility and accountability. It must be crystal clear who 'owns' failure and this creates the need for permissioning. Are we dealing with nodes that we trust? One possibility is a small group with common interest and approaches such as clearing members of a CCP. Or are we dealing with a much more diverse community. What is the role of verification?

While most agreed with the basic premise of Hypothesis 1, i.e. the need limitation on participation, one participant emphasized the need to balance technical innovation against what is tightly controlled and regulated. A key is getting this balance right. In wholesale transactions, agreed there will always be a relatively small group of participants but retail is much more diverse. In both contexts we should expect 'bifurcation', with relatively novel activities operating in a lighter regime with less control.

One participant notes the confusion that arises when we conflate 'nodes' of the network with businesses. There are groups within businesses. This is of course an opportunity, to use common services and unify data. But what is the form of verification that ensures proper and appropriate access?

This is also a regulatory dimension. What will make the regulators comfortable? There are different units of regulation within the firm? There are 'Chinese' walls

within firms. Custody business is separate from the broker-dealer. And legal entities matter, we should set this up so that failure or divestment can be handled in an orderly. In short there are a whole series of implications and uses that need to be taken into account.

Another participant recounted experience of international payments networks which suggests that the simplest challenge is the technology. The bigger and more complicated challenge is incorporating the business and legal aspects. You have got to keep these people happy. They have to be comfortable. This will require a permissioned environment (legal will always insist on this). But it is also a business issue, for example does the ledger allow corporate clients to be nodes as well? If so am I allowing my clients to disintermediate me?

Conclusion we are looking at something highly structured that needs to be carefully and clearly thought through. The choice about permissioning is not a simple yes/no or in/out decision. There are a wide range of possibilities about access and administrative privileges for a wide range of potential participants. So while the hypothesis is essentially correct a great deal of careful thought needs to go into determining the permissioning environment and ensuring the flexibility for changing and updating when necessary.

*Hypothesis 2. The initial applications of mutual distributed ledger will be based on piecemeal developments, in specific situations where there is no established centralised security depository for recording ownership. A coordinated and widespread change in operational processes across all the major public markets for equities, bonds and other financial assets will only be possible in the relatively far-off future, once technical feasibility is established in more limited contexts.*

Hypothesis 1 (subject to clarification of the detail) was broadly accepted by participants. In contrast on Hypotheses 2 there were fundamental disagreements.

The huge amount of attention now being paid to blockchain, and the money being put into this by major institutions (for example the 42 banks that have now invested in R3CEV), indicates that many are expecting more than just piecemeal change. At stake are big issues, about a new operational model across assets and markets.

One suggested homely market comparison was between shopping trolleys v. checkout. There can be considerable freedom around the shopping trolley, anyone can fill it with whatever they like, but there must be complete certainty and a standardised process for checkout. It is always about pay, exchange and record. This though raises questions. Are there many containers (trolleys) or different types of container? Are we using a single asset register or multiple asset registers?

Another issue is that today the challenges are different from a couple of decades ago. There are now almost no lags in the ‘stove pipe’. But we have ended up with a lot of fragmentation. Different products like commodities or structured products are treated quite differently from other products such as securities.

Piecemeal sounds of course more practical but initial applications must be sustainable. For this first adopters need to recommend and to reuse. Another major use case, far from piecemeal, is adoption by firms to harmonise data and systems across their entire group. Lehman’s failure was a critical moment, the realisation that Lehman had hundreds of subsidiaries and so did their counterparties and no-one could work out their exposure. Global LEI is a start but does not get anywhere near to complete the challenge of fully monitoring exposures.

There is a key role for standards. Without standardisation widespread adoption of piecemeal initiatives will be a challenge. Financial standards can be either descriptive or prescriptive. Financial Services are good on descriptive standard i.e. ‘this is what we do’. But they have not succeeded in agreeing on product standards. We need the equivalent for a ‘container’ for a security, so that settlement becomes a totally streamlined process. We need agreement in this key area of development.

In reality the application of blockchain in financial markets will be at the same time both piecemeal and co-ordinated. We need examples, piecemeal development that gets around constraints and demonstrates ‘proof of concept’. Where there is the biggest pain is where we will find the fastest adoption, because it is solving a problem. But we also need broad co-ordinated change to enable adoption.

Agreed, but we should understand and learn from history. FIX provides some insightful examples. As a successful trade messaging standard (FIX) required a few key firms, a core group to get together and pioneer. Otherwise development was

supported by clear benefits e.g. an example is the development of FIX 4.1J for Japan to provide a solution to the millennium bug.

There was a short discussion of the technical constraints in applying mutual distributed ledger across the board. Clear that the basic function of exchange of value and ownership across a mutual distributed ledger can be handled extremely rapidly. The discussion of hypothesis 1 suggests that with an appropriate configuration of authorisation and permissioning, this can be done consistent with required legal, regulatory and security requirements. The bigger technical question is around the development of mutual distributed ledgers that do more than just record value and ownership, but incorporate further algorithmic processing (e.g. the virtual machines incorporated into Ethereum). The interest here surrounds 'smart contracts' that might automate the execution of legal obligations. But there are many potential pitfalls e.g. the possibility of malware, the challenge of demonstrating legal compliance, the possibility of indeterminate outcomes. We still need to establish whether the future will be more limited capability in order to support speed and certainty.

One major practical challenge where mutual distributed ledger may offer big payoffs is with KYC, who are these persons we are dealing with? Ideally this should be shared information. Indeed digital identity is at the heart of these discussions. The 'distributed' nature of the ledger is not the key issue.

An order book is a mutual distributed ledger. We have been doing distributed data piecemeal in financial services for 20 years. Security and trust are the central issues and really nothing else. Becomes centrally important when we as a community using a resource together.

This in turn implies a redefinition of shared services including in AML, KYC. This though takes us back to ensuring that there is compliance with the required by law and regulation. A key requirement is being able to say who is accountable?

But there are different views about how far this sharing can go. One example is 'standard settlement instructions' (SSIs). The key is trust. Is the distributed information community shareable? KYC/AML are the basics that can be shared, but not so easy to share what is commercially value added.  The application of mutual

distributed ledger is in opportunities for offering the most trusted shared service which provides value to all.

Back to fragmentation. We need to focus on data. There are lots of costs in duplication and in reconciliation. First we need leading firms, e.g. SWIFT, to define the size and coverage of the container. Second we need reference data. We still don't have an agreed security identifier, firms need to stitch together at least five different schema, nothing connects.

This is a co-ordination issue. 10-15 firms working together can solve a problem. Take one step at a time, but not just SSIs, there is a lot there.

KYC and AML is a relatively simple action. We need to look at *activity* (trade settlement, corporate actions) and the data needed to support that. This is not easy. The 'Single stock record' failed. A good deal of time and money wasted.

Could you use mutual distributed ledger across a firm? Again the challenge here is that we are not just discussing transfers of tokens between accounts. The Bitcoin blockchain does not incorporate any semantic definitions. At least potentially other more flexible ledgers, incorporating virtual machines, can capture a lot more.

R3 are a natural group to look to, but are they really ready to address this co-ordination challenge? They do not yet seem to be defining standards or indeed wanting to take that role.

There is a tension here between piecemeal and co-ordinated. Is it worth the effort to define requirements and then ensure they are met across the piece? An example is the goal of shifting from T+2 to T+0. But there is always an element of liquidity risk, maybe we can move to T+ 15 minutes but we still need a process of verification to confirm that settlement is possible.

Structural issue not just about 'arrangements'. To raise one issue, what is a CSD and what do they do? The CSD can check the trade and link participants and run delivery vs. payment. But we need a lot around all of that, a whole lot of stuff to make users comfortable. Technically settlement is very easy, once stock and credit lines are in place, the discussion around SSIs etc. is ensuring that.

One participant noted that the investment management association (IMA) is beginning to look at blockchain. This could be very important since up until now the buyside has not yet taken as much interest as the sell side firms, but this could change in the months to come.

Overall conclusion: Applying mutual distributed ledger in financial markets is far from being just a technology challenge or a technology fix. To make this work will require wide ranging adjustment in business process, ensuring that firms adopt common approaches and where necessary changing the way things are done. This is moreover not limited to the post-trade clearing and settlement. It will affect the whole range of back and middle office functions in buy-side and sell-side institutions. So while, absolutely, there has to proof of concept through successful demonstration in specific areas of applications, the issue is not just demonstrating technical feasibility but rather achieving the necessary co-ordination in the adaption of business processes. This is an industry wide challenge that will require leadership, not just piecemeal effort. And it will be essential to involve both sides of the market, buy side as well as sell side, together with regulators.

*Hypothesis 3. At present current participants in the settlement cycle carry out a bundled set of functions (verification of ownership, preparation for exchange including associated borrowing of securities or cash, delivery of value against payment) using historically developed arrangements (tiered accounts, fungibility of securities ownership). Obtaining the benefits from the application of mutual distributed ledger to securities settlement will require a substantial reengineering of these arrangements in which the positioning for settlement must be carried out prior to trade.*

This third hypothesis turns out to be much more closely related to Hypotheses 2 than we had originally envisaged. Since co-ordination of business processes is key, the issue of whether business process also needs substantial reengineering must be addressed upfront not as an afterthought.

There were again a wide range of views in the room. This part of the meeting also included a fairly lengthy discussion of smart contract, going some way beyond Hypothesis 3.

One view is that that we cannot drop the absolute requirement of needing someone to point to when things go wrong. Technology is not so difficult. What needs clarity is the business end, middle and back office, custodians, the communication of trade and allocation details to fund administrators, there is a whole range of market participants and who is responsible for what.

In terms of improving business process, a major problem has been lack of engagement. Achieving “t+X” (whatever X should be), depends on obtaining agreement between the buyer and seller. We also have to recognise that various asset markets differ, additional or variations in process are often required.

A further challenge is that “turkeys do not vote for Christmas”. So it may be important to be able to offer greenfield alongside existing arrangement. Buyers and sellers need to be able to choose between current arrangements for settlement and new arrangements based on shared information through mutual distributed ledgers. The market can then vote with its feet.

Over 30 years we will see a new approach. With transactions time, day and event stamped. But that is not all. At present what people care about is default. So are we to work with no possibility of default i.e. with complete pre-positioning for trade and simultaneous settlement? That seems unlikely so there will still be a huge amount of detail involved and several potential problems that must be allowed for. What this comes down to is the virtually everyone involved in post-trade processing are information providers. Then the question of who is accessing the ledger and seeing this information and to what extent this information provides them with certainty.

A particularly interesting application where change in process may make a big difference is the collateral bit. For example it can be residing in one jurisdiction but not legally movable. Today this problem is dealt with through collateral insurance but an additional expense. The business can be substantially more efficient by moving things better and faster. Here though the issue is what this really requires, does this distributed shared ledger or something else for example greater flexibility in law and regulation?

Business process affects everyone in the market. Even addressing Hypothesis 1, deciding the configuration of permissions for access, authentication and verification

requires trust. And, as we have discussed in relation to Hypothesis 2, effort is needed to harmonise and deal with potential failure. So a vision and master plan is needed of how mutual distributed ledger is to be applied and this must be developed product by product. Again this a major co-ordination challenge.

What is the role of R3? This has been discussed at board level in many firms. The positive view is that it offers a community, the forty-two institutions involved, so this is a powerful and unique selling point. At the same time definitely an 'out of the money call option'. So could be the venue for addressing the issues of business process.

But not everyone is persuaded that R3 will be the driver of change. Governance is critical. The history of alternative trading venues in Europe provides an example. Turquoise had most of the major firms on board, but as a result was a tortoise, could not do anything without endless discussion. Chi-X with small group of core institutions closely involved could move much more quickly and was as result much more successful in responding to the needs of the market. Will the same logic not apply to the implementation of mutual distributed ledger in financial markets?

Conclusion: the harmonisation and development of business process cannot be separated from the application of shared mutual distributed ledger. To what extent this requires fundamental change, e.g. in management of liquidity and collateral, and how this will be developed at market level remains to be seen.

### Additional discussion of smart contracts

The focus group concluded with some additional discussion of smart contracts. These are a means of implementing business logic. But it is still at the very earliest stages of development, similar to where databases were in in 1974. A number of entities are now using Ethereum virtual machine or the related Eris permissioned application which can support embedded code (but these do not integrate with the Bitcoin block chain, they may use an alternative consensus mechanism e.g. Tendermint implementation of byzantine fault tolerance). There are technical issues with these initiatives. Ethereum has not got IF-then etc. no infinite loops. This means we can predict definitely what will happen and we believe security cannot be broken by malware. But while a start has been made it could take a decade to build this out.

Smart contracts do seem to have a natural application in securities settlement. They offer the possibility of transparent technical implementation of what has previous been signed up to. This is far from all. Another potential application of smart contracts is data recording, internally or in trade repositories. This is not just about trade execution and settlement.

It is tempting to think that all issues of contract and default can be incorporated into smart contracts. But this does not seem realistic. Smart contracts are not themselves legal contracts. The business works on the basis that we first agree and then later we execute, but execution is still conditional. Smart contracts can be used to execute the terms of a trade, but they are not themselves a legal contract. For this we need to compile code and establish exactly what it implies. Extremely challenging to provide a legal audit to be sure that the smart contract is going to execute what is legal. Yes we need code to implement obligations, but we will not be able to see on the ledger all the legal commitments which are inevitably context dependent.

This tells us we must be careful. In some contexts e.g. ISDA master agreements less of a problem. In other situations, involving collateral and cash and hence DVP we use a range of different contracts in place. There no effective standardisation and few reporting requirements except registration. There are other challenges as well, e.g. high frequency trading that will not easily slot into any mutual distributed ledger based settlement. Scary to think about some cases where smart contracts could be applied e.g. to CDOs. More philosophically, financial markets built on “mistrust and leverage”, seems difficult to capture such intangibles in code.

## Appendix 3. List of Informants' Affiliations

We list here the affiliations of individuals we have engaged with or who have commented on a preliminary draft. In several firms there were multiple individuals. Many of the firms with whom our contributors were affiliated do not have an agreed view. Some of our contributors were candid that the prevailing view in their firm was sometimes at odds with their own thinking. A few of those whom we interviewed or attended our focus groups wish their organisations to remain anonymous.

Allianz
Askget.com
Association of Foreign Banks
Axa
Bank of America Merrill Lynch
Bank of England
Bank of New York Mellon
Banking Technology
Barclays
BNP Paribas
British Bankers Association
BT
Cambridge Blockchain
Central Bank of Barbados
Central Bank of Ireland
Centre for the Study of Financial Innovation
Chartered Institute for Securities & Investment
Citi
City of London Corporation
Complymatic
Consensys
Deloitte
Deutsche Bank
Deutsche Börse
DSTL (Defence Science & Technology Laboratory)
DTCC
ESMA
Ethereum
Eurex
Euroclear
EY
Financial Conduct Authority
Freshfields
Fujitsu
HSBC
IBM
ICAP
Imperial College
ING
Interxion
Investment Association
ISDX
Isle of Man
Jefferies
JP Morgan
KPMG
LCH Clearnet
Lloyd's of London
Lloyds Bank
London Stock Exchange
Lykkex
Mizuho
Nasdaq NLX
Nomura
Northern Trust
Norton Rose Fulbright
NYSE
Oriel Securities
Ovum
PRMIA
PwC
R3
Rivast Consulting
Santander
SETL
State Street
States of Alderney
States of Jersey
Sullivan & Cromwell
SWIFT
Swiss Re
Thomas Murray
Turquoise
UBS
UCL
UK Office of the Government Scientist
Vocalink
Wedlake BellWorld Economic Forum