Think Ahead ACCA

Divided we fall, distributed we stand

The professional accountant's guide to distributed ledgers and blockchain

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. It offers business relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **188,000** members and **480,000** students in **178** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **100** offices and centres and more than **7,110** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. It believes that accountants bring value to economies in all stages of development and seek to develop capacity in the profession and encourage the adoption of global standards. ACCA's core values are aligned to the needs of employers in all sectors and it ensures that, through its range of qualifications, it prepares accountants for business. ACCA seeks to open up the profession to people of all backgrounds and remove artificial barriers, innovating its qualifications and delivery to meet the diverse needs of trainee professionals and their employers.

In June 2016 ACCA formed a strategic alliance with Chartered Accountants Australia and New Zealand (CA ANZ). The alliance represents the voice of 788,000 members and future professional accountants around the world, who share the commitment to uphold the highest ethical, professional and technical standards.

More information is available at: **www.accaglobal.com**

This report examines distributed ledgers and blockchain. It introduces the concept and relates it to the needs of professional accountants.

ABOUT THE AUTHOR

Narayanan Vaidyanathan is head of technology insight. He has a global remit and leads research initiatives across a range of areas. He represents ACCA on various government, industry and academic forums.

Contents

Foreword

Technology has a profound impact on how we live, and a key aspect of this impact has been an increase in the level of connectedness within society. This connectedness stems from being able to share information in real-time, an ability created by the internet.

There now appears to be the possibility for another step-change in the impact of technology as a result of what has been called the 'internet of value'. The ability to track and transfer value (such as money or assets) in a secure real-time way, similar to information transfer today, could fundamentally alter the way we live and transact with one another.

The underlying technology to enable this – referred to as distributed ledgers or blockchain – is at the heart of these developments. It could change not just individual organisations, but entire industries and their supply chains. And in doing so, it offers the potential to transform existing business models and the skills relevant to delivering them. It is therefore important that professional accountants understand these developments and the nature of the impact on their roles.

ACCA is committed to developing professional accountants the world needs. This refers not just to the needs of today, but also to anticipating and planning for the profession of the future. Accordingly, our approach is to look ahead and engage pro-actively with key trends that could shape tomorrow's world. This report on distributed ledgers has been produced in this spirit.

We are delighted to add to the understanding in this area, and to complement the work of others like our strategic alliance partner, Chartered Accountants Australia and New Zealand, who are also striving to improve awareness of this important topic across our profession.

Helen Brand OBE
Chief executive
ACCA

Executive summary

This report explores the concept of distributed ledgers, also often referred to as blockchain.

This report explores the concept of distributed ledgers, also often referred to as blockchain. The primary target audience for this report is the community of professional accountants, but anyone seeking an introduction to this topic (particularly if they are not a technology professional) may find it relevant to their needs.

A distributed or shared ledger is a digital database of records. These records contain information relevant to a group of participants within a network. For example, the value of assets they hold, details of ownership, information about transactions between participants or anything else that can be represented within a digital register.

In a distributed ledger all participants are looking at a common view of the records. This is in contrast to a typical situation currently where participants (for example, in different organisations) are looking at different databases that are independently managed and updated.

When a change or update to any participant's record is confirmed, the technology ensures that the view seen by each participant in the network synchronises to reflect the latest update. This is a peer-to-peer network where the participants are themselves responsible for the validation of records – without the use of a central authority for this purpose. So if the majority of participants agree that an update has been correctly validated, that becomes the basis for the updated entry to be added to the ledger.

The network itself may be public or private. A public network offers an open permissionless invitation for anyone to join. This provides a mechanism by which complete strangers can trust the shared information they see in the ledger. On the other hand, a private or closed permissioned network enforces a membership process for participants.

Blockchain presents new areas for analysis and consideration, and the sooner professional accountants increase their awareness, the better prepared they will be to engage with it.

If the dominant requirement in the network is speed or more effective regulatory compliance, then the cost and effort of establishing trust between strangers is not relevant, and private network technologies may be preferred.

Bitcoin blockchain is a public network ledger where transactions are grouped into blocks and validated through mathematical techniques (such as encryption and hashing). The underlying governance is handled by a consensus algorithm that verifies and confirms that a block contains valid transaction information and can be added to the existing chain of blocks. A linear chain of blocks containing transactions creates a single view of the truth, capturing the details and sequence of transactions as they occur.

Distributed ledger technology (DLT) refers to technologies built primarily to suit the needs of private permissioned networks. It shares the characteristics of a digital record without a central validator, and where the ledger is replicated across different participants. These participants have been selected to enter the group and share the ledger: for example, a network of banks that have all agreed to common terms and conditions for using the shared ledger. Also, some participants may have been appointed to hold specific pre-agreed roles (such as validation) within the network. DLTs are typically designed to be faster than public network shared ledgers. The Hyperledger project is working on creating a collaborative, open source platform for DLT to support business transactions and create enterprise-relevant ledger solutions.

As DLT matures, the shared ledger's common view of records and transparency of transaction history could reduce reconciliation across different databases and drive significant efficiencies. Business processes that are characterised by inefficiencies (eg trade finance), or exist because of a lack of trust (eg Know Your Customer requirements in financial services) or poor supply chain visibility (eg for global garment supply chains) are all key areas for distributed ledger applications.

It will take time to gauge the impact of distributed ledgers on overall revenues for accountancy firms. But the most likely effects on the revenue mix may be clear sooner.

There may be a gradual move away from low-margin activities (for example, transaction checking) towards a greater emphasis on higher-margin work (for example, interpreting technical accounting policy to a given situation). Over time, this may affect the revenue model, with greater emphasis on paying for expertise and advice (outputs-based rate card) rather than for time (inputs-based, per hour billing).

Whether this evolution in revenue mix occurs or not depends on the ability of distributed ledgers to achieve large scale and mainstream adoption. Views on this vary but, one way or another, it is anticipated that over the course of the next five years the answer will become clear. If it looks likely that the revenue mix will evolve, then accountancy firms may want to evaluate their structure and organise themselves differently to prepare for the future.

This might involve providing those offerings with potential to be standardised and automated (eg data collection, records checking, bookkeeping or exceptions reporting) via a platform interface such as an accounting-as-a-service offer.

In addition, the professional accountant of the future will need a forward-looking outlook and skills and abilities that are well rounded, resilient and adaptable to changes in the business environment. For example, there may well be new areas of knowledge that need to be better understood, such as how to measure and account for value as assets transfer via a distributed ledger from one owner to another.

Blockchain presents new areas for analysis and consideration, and the sooner professional accountants increase their awareness, the better prepared they will be to engage with it.

Report structure

The aim of this report is to illuminate this area by exploring what a distributed ledger is, where it might have commercial applications and how it relates to accountancy and finance professionals.

This report comprises three main sections:

1. Introduction to concept

2. Commercial applications for distributed ledgers

3. Distributed ledgers and professional accountants

The report complements a recent report from ACCA's strategic alliance partner, Chartered Accountants Australia and New Zealand (*The Future of Blockchain: Applications and Implications of Distributed Ledger Technology*).

The aim of this report is to illuminate this area by exploring what a distributed ledger is, where it might have commercial applications and how it relates to accountancy and finance professionals.

1. Introduction to concept

Around the world, governments, technology providers and businesses are evaluating what distributed ledgers might mean for them. As part of this, the accountancy profession will also need to understand fully the implications of this technology, and many are on the journey to doing so.

New technologies are allowing us to reimagine the way we live and interact with one another. In doing so, they have brought several new ideas to the fore, each claiming to be the 'next big thing'. But some of these technologies are establishing themselves as having the ability to drive significant changes.

One of these is the distributed ledger, also commonly referred to as 'blockchain'. This has the potential to transform the way an entire 'eco-system' of organisations, such as within a particular industry, is set up. It challenges assumptions about the ways in which organisations can share information and trust each other, while still generating sustainable economic returns. And in doing so, the distributed ledger is crossing over from a topic of discussion among technologists to one that is familiar to a generalist or business audience.

Around the world, governments, technology providers and businesses are evaluating what distributed ledgers might mean for them. As part of this, the accountancy profession will also need to understand fully the implications of this technology, and many are on the journey to doing so.

1.1 THE BASICS – THE CLUE IS IN THE NAME

The headline words, namely ledger and distributed, are a good place to start.

1.1.1 Ledger

Unsurprisingly, a distributed ledger is in fact what a ledger normally is: a database of records which, in this case, is held in a digitised format. Participants can view records and contribute information to update these records.

By combining the actual transaction with the record of the transaction, distributed ledgers bring significant efficiencies.

The concept is that of a shared system of records that the participants can see, and where the technology ensures that all copies are kept updated and synchronised. In this type of ledger, doing a transaction and recording it are combined into a single view of an event.

In current systems this is not the case. When selling shares, for example, one database records the transaction details as the transaction occurs. These details are then manually re-entered into a second database that is responsible for 'settlement'. Settlement is the process by which transaction details are checked, after which shares are transferred and monies exchanged.

The above involves manually re-entering the same information, checking between multiple databases and, where there are differences due to human error or delays in updating a database, a reconciliation process. When scaled up, these factors introduce material amounts of inefficiency. In the case of shares this can mean several days of delay before transactions are settled.

By combining the actual transaction with the record of the transaction, distributed ledgers bring significant efficiencies.

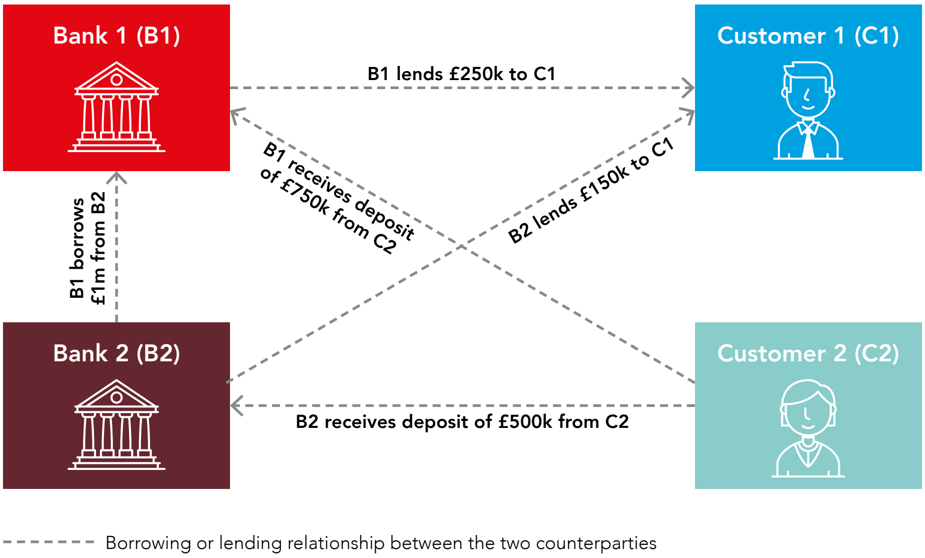
1.1.2 Distributed

'Distributed' (or 'shared') is another way of saying that all the participants in the network can see the same set of ledger records at any given time. So if thousands of people are looking at the records in a distributed ledger from their individual personal computers, they will all see exactly the same account balances and positions.

Now, if one of them makes any change to this distributed ledger, say by selling some assets to another participant in this network, that change gets updated in everyone's view of the ledger. The common view that they all see is preserved. This common view is distributed across the thousands of people sharing the ledger, ie they are looking at a localised copy of the common view on their machine.

To examine this a bit more, let's assume a simple world with only two banks and two customers, with transactions between them as shown in **Figure 1.1**.

Figure 1.1: A simple world with two banks and two customers



If a participant makes an update in a distributed ledger, the new information is validated using the technology and then added to the ledger, with everyone's localised copy of the record getting updated at that point.

The existing method for representing this system would be for each organisation to record the transactions, from its perspective, within its database as shown in **Figure 1.2**. This creates a total of 10 records across the system. The multiple records for the same transaction held in different databases need to be agreed upon, and reconciled where there are differences, before further transactions can occur.

Let's assume now that, instead of each participant using its own database, all participants use a common database. This would involve the creation of a common record that captures all the transactions within the system; a representation of this is shown in **Figure 1.3**. This would mean that a change or update for any participant's transaction would be reflected in this one common record and the view of the ledger seen by all participants would be synchronised to reflect this update.

In the current approach participants in different organisations (or, indeed, different departments in the same organisation) may use different systems, often resulting in reconciliation breaks between them. These could be due to a time lag in recording information between the systems or just human error linked to multiple data entry points.

On the other hand, if a participant makes an update in a distributed ledger, the new information is validated using the technology and then added to the ledger, with everyone's localised copy of the record getting updated at that point.

Figure 1.2: Separate records in each of the organisations

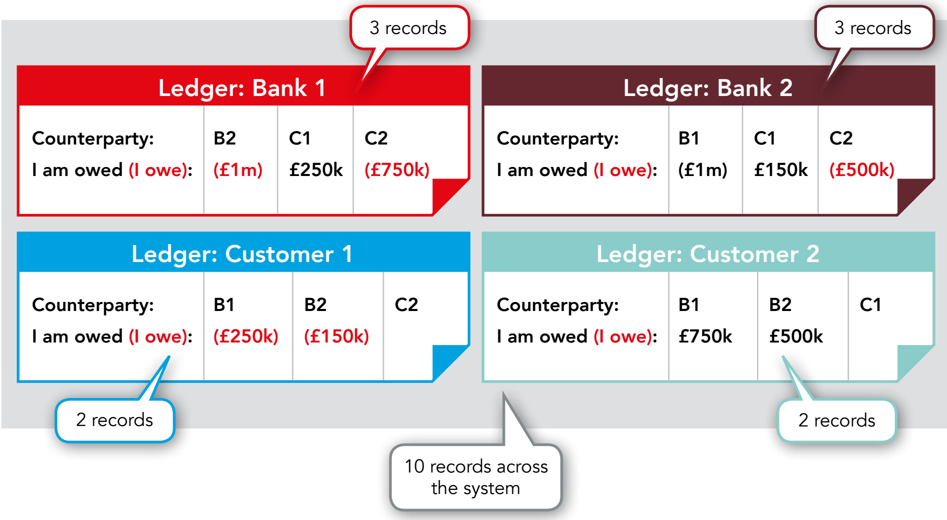
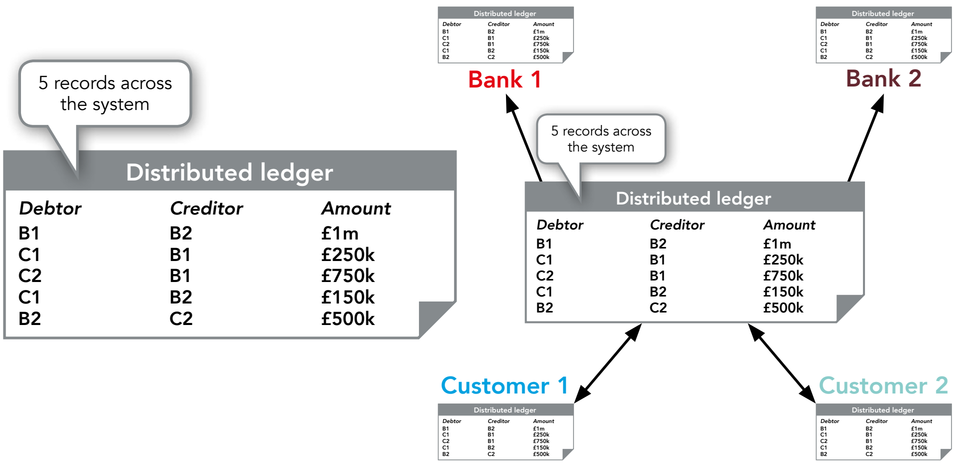


Figure 1.3: A common view of transactions



At its heart, a distributed ledger is about connecting participants, via a network, to transact more effectively.

1.2 THE NETWORK EFFECT

At its heart, a distributed ledger is about connecting participants, via a network, to transact more effectively. There are in principle, two options[1] for this network.

1.2.1 Public network

A 'public' network offers an open, permissionless invitation for anyone to join. If the dominant requirement is a trust mechanism between strangers who know nothing about each other, then a public network may be the way to go. For digital or crypto-currencies such as bitcoin this as an enabler for driving greater adoption globally, with more people being able to make purchases with these currencies.

1.2.2 Private network

A 'private' network, also sometimes called 'closed' or 'permissioned', enforces a membership process for participants. If participants are pre-selected, and the dominant requirement is speed or more effective regulatory compliance, then the cost and effort of establishing trust between strangers may not be as relevant.

For example, a group of banks that have extensive contracts in place may not need to vet each other before each transaction as if they were total strangers. But these banks may benefit from being on a network that allows them to agree balances and transact faster. They may also be governed by a common regulator, who may use a distributed ledger to monitor, for example, the concentration of risk across banks and its potential systemic impact.

1.2.3 Majority consensus

Whichever type of network is chosen, a common feature is the 'peer-to-peer' checking of records. The agreement of the majority of network participants is required before a record can be added or changed. The consensus mechanism also defines the governance, performance and security of the blockchain, replacing the role of a single designated central authority (such as the clearing houses that perform checks before shares are transferred and monies paid) for validating transactions.

A traditional double-entry system ensures internal consistency within an organisation, so that if its books balance (eg an increase in loan liabilities is matched by increase in cash assets) it has confidence in the entries. But as transactions occur it is easy for the view of the transactions across organisations to become out of sync with each other.

Distributed ledgers allow external consistency across organisations. If an entry is validated on the ledger, the view of all participants in the network synchronises to reflect this entry. So rather than just an individual organisation having confidence in the entry, all users of the distributed ledger have confidence. This is a so-called 'triple-entry' system.

1.3 QUICK REALITY CHECK

1.3.1 Data privacy

In the earlier example (Figures 1.1, 1.2 and 1.3), Bank 1 would typically face legal restrictions on allowing Customer 1 to see the bank's transactions with Customer 2, and vice-versa. The permissioned distributed ledger has mechanisms in place to ensure that users can only see data that they are authorised to see, or that transactions can be viewed without the identities of the participants being shown, providing extra assurance. So a common shared ledger doesn't necessarily mean that everyone can see every detail; controls can be put in place if needed.

1.3.2 Human error and fraud

Distributed ledgers can significantly reduce, but not completely remove, human error or fraud: the technological architecture of the ledger makes fraud and error difficult.

The consensus mechanism has safeguards to prevent either collusion between participants or the acquisition of too much influence by a single participant within the network.[2] The validation of transactions by majority consensus makes it difficult for a rogue actor to single-handedly disrupt the network.

1 Hybrids of public and private distributed ledgers are also being explored by the industry.

2 Proof of Stake consensus is based on economic investment, the consensus also limits too much economic power from building in up in one node (see section 1.5.1 below for more on nodes). Byzantine Fault Tolerance is a parallel consensus for detecting participants (nodes) misbehaving.

Bitcoin is a cryptocurrency, so unlike a traditional ('fiat') currency, its supply is not controlled by a national government

The use of encryption, a mathematical technique that allows for a secure digital signature, checks that a transaction was in fact between the stated buyer and seller and for the amounts involved.

1.3.3 Accountability

Records are shared among network participants and co-owned by them; this is similar to a model of mutual ownership. Since these mutual distributed ledgers are owned by all participants, questions can arise about accountability in the case of fraud or human error.[3]

There is a certain level of accountability inherent to the concept of a distributed ledger. For example, changes to a consensus mechanism in any ledger would need to be voted upon. Parties cannot enforce changes to the underlying source code. They cannot secretly add a new version without everyone's knowledge and agreement. Consensus is therefore a pillar that supports governance, assurance, privacy, security and performance.

Therefore any regulation from governments needs to consider the balance of priorities carefully. On the one hand is the priority of legal certainty and protection in an area where issues are not well understood by all. On the other, there is the additional regulatory burden that could affect innovation at a time when appetite for adoption is increasing.

1.4 THINGS WE WANT TO KNOW BUT DON'T ASK

1.4.1 Bitcoin, blockchain and distributed ledgers: what's the connection?

Bitcoin is a cryptocurrency, so unlike a traditional ('fiat') currency, its supply is not controlled by a national government. It operates on a digital peer-to-peer basis. Encryption tools are used to ensure that the bitcoin transfer occurs between the designated source and recipient address. Also, when bitcoin transfers occur they use balances from individual transactions, and do not net-off balances across transactions into a single balance.

Suppose A has five bitcoins (5 BTC) obtained from C in a previous transaction. A needs to send 4 BTC to B. Rather than splitting its balance obtained from C, the transaction occurs in two parts: A's balance of 5BTC is sent across the network (retaining its link to the 5 BTC obtained from C), and of this 4 BTC are credited as a transaction from A to B while 1 BTC is re-credited back to A.

The bitcoin blockchain is the underlying technology that provides a transparent view of bitcoin transactions as they pass from one network participant to another. Hence bitcoin has become a well-known example of a ledger record that provides a reliable permanent view of transactions – characteristics that are the basis of all distributed ledgers.

ENCRYPTION IN THE BITCOIN BLOCKCHAIN

This is based on an idea called public key cryptography. A user in the bitcoin network has an address with associated public and private keys. As the names suggest, the public key is visible to everyone, while the private key is known only to that user. The public key is used for encryption while the private key is used for decryption. Let's assume user 1 wishes to pay (ie transfer) bitcoins to user 2.

User 1 generates a coded message with user 2's public key and sends this to user 2 to inform them that bitcoins are to be transferred. User 2 uses their private key to decrypt this coded message. User 2 can check that it was indeed user 1 that sent the message with the help of user 1's public key. In effect, the public keys ensure that the transfer happened from the correct source and went to the correct destination. The private keys ensure that only the authorised person (user 1) associated with that source address can spend the money, and the authorised recipient (user 2) associated with that destination address can access ('receive') the money.

3 M. Mainelli and S. Mills, The Missing Links In The Chains?, November 2016.

A block contains a summary of the transactions, including time stamps showing when they occurred, a link to the block immediately preceding it and proof of the validation that was used to create the block.

This technology checks that transactions are genuine by referencing previous transactions and grouping them into 'blocks'. These blocks then get added to a 'chain' of successive events to create the single, accurate view of the full list and sequence of transactions for all network participants to date.

A block contains a summary of the transactions, including time stamps showing when they occurred, a link to the block immediately preceding it and proof of the validation that was used to create the block. This creates the 'chain of blocks' that has given rise to the term blockchain.

So, a distributed ledger is a mechanism for reliably recording and tracking transactions, assets or other information in a digitised format in a way that is shared between participants. Distributed ledger technology (DLT) generally refers to the application of this technology to suit the needs of private permissioned networks.

Blockchain is a technology used to create a distributed ledger (using chains of blocks), though the two terms are often used interchangeably in common usage. Bitcoin is a cryptocurrency that uses a distributed ledger, in this case the bitcoin blockchain, to record bitcoin transactions in an open and transparent way, using chains of blocks.

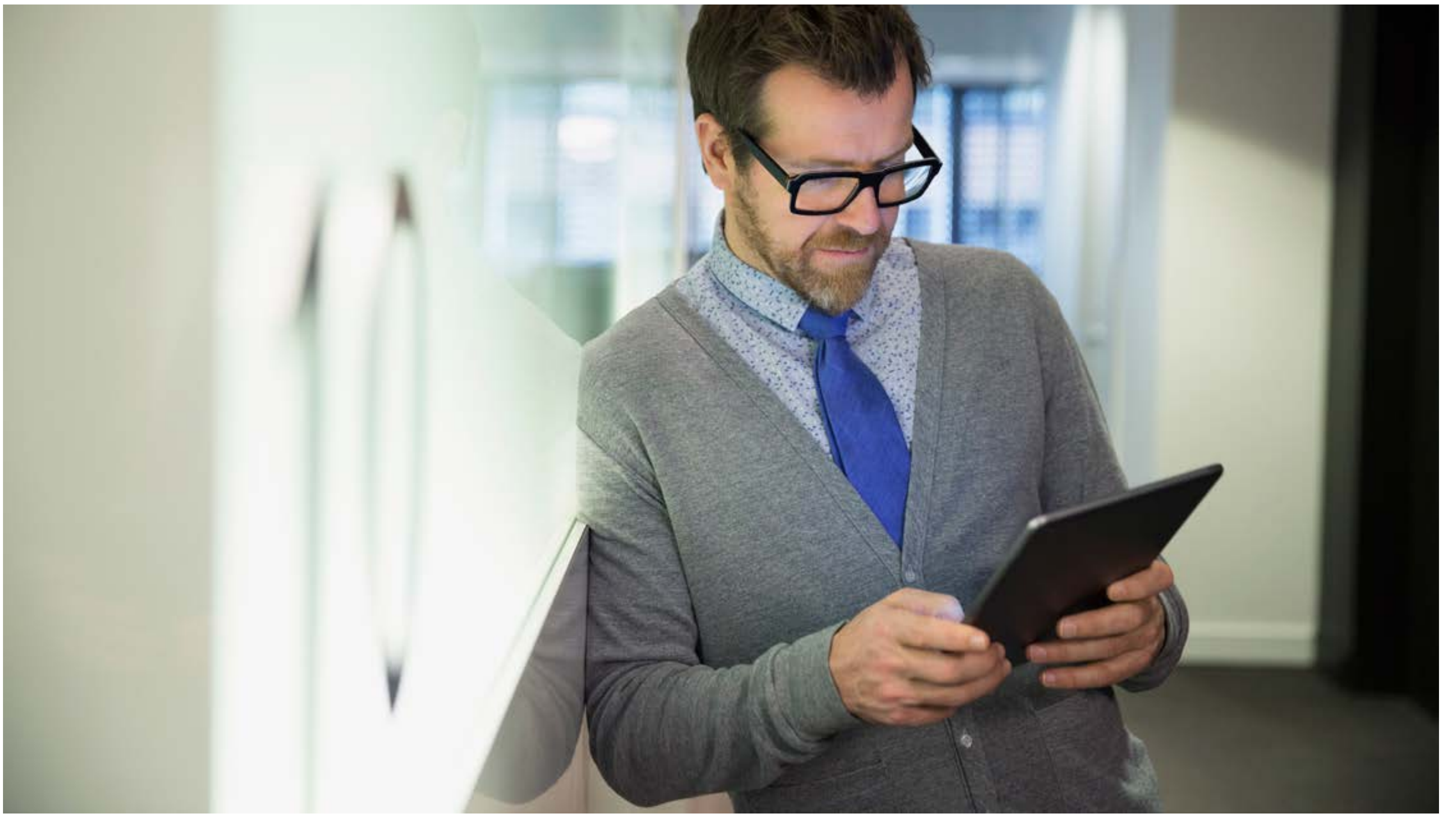
1.4.2 Do transactions stay on the blockchain for ever?

'Immutability' refers to the inability to remove or amend transactions once they've gone through the process of validation, achieved majority consensus, and been added to a block that is part of the chain of blocks that constitute the shared ledger.

Once an entry has been created in the ledger, it cannot be removed or changed in any way. This means that the ledger provides an uncorrupted view of all entries recorded by participants from when the ledger was first created – a perfect audit trail.

As a corollary, if a transaction is incorrect, it cannot be amended; instead a new reversing transaction in the opposite direction must be entered to cancel it out.

Immutability is indispensable in the public network environment, where the lack of trust means it is highly valuable for records to be absolutely unchangeable. Trust is achieved in an environment where participants have separate economic interests yet want to ensure that the value and integrity of the blockchain is protected. Against this, it does bring into question the practicality of storing infinitely increasing amounts of data that cannot be removed. In the bitcoin blockchain, for example, there is a 1MB block size that can house about 1500



For a block of transactions to be successfully added to the chain it needs to be validated by solving a computationally intensive mathematical puzzle.

transactions, with signatures taking a large amount of space. Therefore distributed archiving solutions are being developed which may mean that all the data doesn't need to be held in the primary storage area.

While the above storage issues relate more to public networks, some question whether, within private permissioned networks, there are some circumstances where immutability may need to be suspended. This might occur in regulated industries such as banking, where there may be a need to amend transaction errors rather than leaving them permanently on the network. This may involve a mechanism for amending records, albeit one that leaves permanent evidence (a record) of this action. Like many things in this area, these are ideas being tested and refined, and in time the situation will become clearer.

1.4.3 What's the barrier to tampering with transactions on the blockchain?

The answer depends to some extent on the architecture of a given distributed ledger. For the sake of specificity, the account below is based on the bitcoin blockchain, though other ledgers will have similar protections.

For a block of transactions to be successfully added to the chain it needs to be validated by solving a computationally intensive mathematical puzzle (hashing algorithm). The level of processing power needed makes it an investment in time and considerable amounts of electricity to power the computers needed for the task. Also the answer to the puzzle changes if the contents of the block are altered. The difficulty of the hashing process serves as an effective deterrence to tampering.

After the puzzle is solved,[4] the participant who achieved this presents evidence of this to the network, and the majority of participants must agree through a process of network voting that it was correctly solved. At this point, the block joins as a validated part of the chain.

Now, suppose someone wanted to go back and change the transactions inside one of the blocks in the chain. Since the contents of the block have changed, the answer to the puzzle has also changed. So they need to expend computation power to solve the puzzle all over again. There are mechanisms[5] for detecting suspect behaviour and warning the network.

Furthermore, as mentioned earlier (1.4.1), each block contains a reference to the previous block. This means that the next block following the tampered block contains a reference to the tampered block. This in turn means that the contents of this next block have also now changed.

VALIDATING BLOCKS IN THE BITCOIN BLOCKCHAIN

The process, called proof-of-work, is based on a 'hash', which is an algorithm (ie a computer program) that can convert any sequence of characters (bitcoin transactions, land title, share certificates, or indeed anything else) into a string of 64 letters or numbers. Any change, however small, in the details of any of the inputs will cause the algorithm to create a completely different string after hashing.

The hash of previously validated blocks is publicly visible on the blockchain. The hashing algorithm is now applied to a sequence of characters comprising three elements: the hash of the immediately previous block in the chain, the transactions in the current block and a randomly chosen number. This results in a string that is the hash of the current block and which is then visible to the network. Validation happens when a participant in the network called a 'miner' solves the puzzle of guessing what that random number is.

Strange as this process may seem, there is a rationale for it. The probability of guessing the correct random number is very low owing to the large number of permutations. The only way is to use brute computing power, to repeatedly try numbers through trial and error. This need for computing power forces the miner to do some 'work' before they are allowed to validate a block; and it acts as a deterrent for those wanting to interfere with the network.

4 Referred to as 'Proof-of-Work'.

5 Known as 'Byzantine Fault Tolerance'.

To tamper with blocks, the amount of computing power required to change a block and all blocks following it is a barrier for an individual rogue actor.

Therefore the puzzle solution used for validating the next block has changed – and the rogue actor must expend more computing power to also re-solve the puzzle for the next block.

In fact this logic applies for all blocks following the tampered block. So to tamper with a block a rogue actor would need enough computing power not just to resolve the puzzle for the tampered block, but for all blocks that followed it as well.

1.4.4 If it is like a database, am I viewing the underlying data?

It was mentioned (section 1.3) that controls can be put in place so that one can view a record only if one is authorised to do so. But what does 'viewing a record' actually refer to?

The blockchain technology might allow participants to record and track the movement of assets, for example the title deed for a property as it gets bought and sold. But the deed itself is not held on the blockchain. Rather, the ledger holds a string of characters.

This string is a mix of alphabets and numbers that is created by applying a piece of code to a set of information that includes the contents of the deed. This string is now linked to that particular title deed as of that point in time.

At a future point in time, one might check the authenticity of a deed by presenting it to the ledger and checking that the generated string is the same as the original string associated with the title deed when it was added to the ledger.

The Swedish land registry has been working towards putting all its real estate transactions on a distributed ledger. Once a contract is made between buyer and seller, it could be put in a shared ledger and viewed by all concerned parties, such as the buyer, seller, government and estate agents, depending on their level of access.

It is important to note here that there is nothing in the code creation process to allow access to the contents of the title deed itself. This validation occurs independently of being able to look at the underlying document. This is valuable in business scenarios where third parties need to assess risk without breaching data privacy.

1.4.5 Is it possible to mount a cyberattack on a blockchain?

Yes, as mentioned (1.3.2) fraud is possible; in addition, a cyberattack cannot be ruled out. Like any technology, distributed ledgers have a design – and that design will have points of weakness which unscrupulous attackers could try to exploit. Sybil attacks (identity theft) and distributed denial of service (DDoS), which can overwhelm a network and disrupt genuine transactions, are all threats to be considered.

The precise way in which this happens will depend on the design, and to build on observations to prevent tampering (1.4.3) let's look further at the example of the bitcoin blockchain.

Block validation depends on expending computing power to solve a puzzle, an exercise carried out by participants in the network called 'miners'. To tamper with blocks, the amount of computing power required to change a block and all blocks following it is a barrier for an individual rogue actor. But what if lots of actors join together to pool their computing power? There are safeguards in the system to make this difficult, with the consensus mechanism that sits on the nodes (see 1.5.1 below) being designed to prevent this, by detecting nodes that may collude or work against the wider interests

Historically this was not a great a risk but, as bitcoin has increased in use, it has become financially viable for participants to pool together and invest in large data centres to increase their joint computation power.

A smart contract automatically fulfils obligations from one party to another when trigger conditions are met, using a piece of self-executing code.

The impact of this has been to subvert the decentralised ethos of the bitcoin network. The system involved an implicit assumption that the majority of participants corresponded to the majority of computing power. But with pooling, a numerical minority acting in concert could control the majority of computing power, and hence control which blocks get added to the blockchain.

As shown in **Figure 1.4**, four such groups controlled over half of the computation power in the bitcoin blockchain in January 2017. They could collude to introduce fake transactions into the blockchain since their joint computing power means they could overwhelm any opposition. It remains to be seen whether this would be economically attractive to them in the longer term as it could erode value from the network – most miners hold large values of bitcoins themselves so it may not be in their best interests. In any event, so far this risk has not materialised, but it is theoretically feasible.

1.4.6 What is a smart contract and is it code or 'contract'?

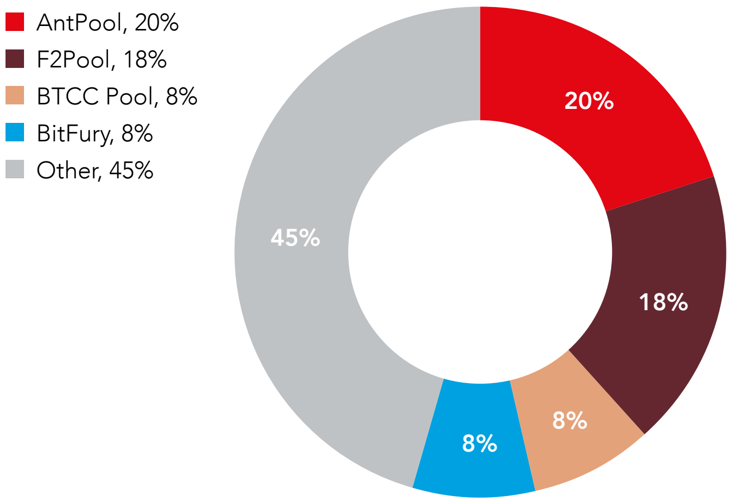
A smart contract automatically fulfils obligations from one party to another when trigger conditions are met, using a piece of self-executing code. If both concerned parties are to trust this code, it must be accessible to both of them in a transparent way, with changes made through procedures agreed between them. Clearly, this will not be possible if the two parties hold the information in their respective databases, each under its owner's sole control. This is why smart contracts have come into prominence now that the option of a shared ledger view exists. Generally, different DLTs have their own version of smart contracts.

The obvious question that arises is: in what situation would this be useful?

A typical scenario is when there is a trigger to set off a particular set of actions as part of a pre-agreed obligation. In the title deed example previously mentioned, the distributed ledger allows the authenticity of the title to be validated, while enabling access to underlying title documents only to authorised persons.

This provides a snapshot view, ie who owns the title to which property as at a given point in time. Naturally, transactions occur, and titles change hands. This is where smart contracts come in. They can use the distributed ledger infrastructure to assess veracity of the title, buyer and seller. Subject to a list of pre-agreed trigger conditions (eg buyer funds approved, identification checks), such a contract can effect a transfer of title from seller to buyer.[6]

Figure 1.4: Market share of largest mining pools



Source: Blockchain (2017) accessed 25/01/2017. Percentage in the pie chart refers to the proportion of total computation power that is controlled by a given mining pool.

6 Referred to as 'Proof-of-Work'.

> The entire concept of this technology rests on transforming an eco-system, rather than just an individual organisation.

Smart contracts are still at a relatively early stage, and are being explored across a spectrum of possibilities. This ranges from using a piece of code within a contract purely for effecting payments at appropriate times, to writing a full contract entirely in code.

The latter would be what is commonly understood as a 'contract' backed by law. There are questions to be answered about the legal enforceability of these proposed contracts, and this is a tricky aspect that may take time to be resolved.

In the near-term it may be more feasible to envisage a situation where the contract exists within traditional legal jurisdictional frameworks, with the 'smart' element being restricted to providing payment triggers for fulfilling the contract at a pre-agreed time.

Therefore as things stand, it may be more accurate to think of 'smart contracts' as self-executing code rather than contracts in the legal sense of the word.

1.5 COOPERATING TO DRIVE WIN-WIN OUTCOMES

Traditional management thinking over most of the second half of the last century has focused on what is needed for organisations to compete effectively in their markets. Ideas such as garnering market share and out-performing the competition, through lower prices or greater product differentiation, focus on how an organisation can increase the percentage of the market that it can capture for itself.

Technology has shifted this mindset by increasing the emphasis on enlarging the market, rather than fighting for a bigger share of static, or in some industries declining, sales. Nowhere is this mindset more in evidence than in the area of distributed ledgers. The entire concept of this technology rests on transforming an eco-system, rather than just an individual organisation.

This is the network effect discussed in section 1.2 above. A distributed ledger can be effective for serving the needs of an individual organisation (if it is large and complex enough). But it is likely to be truly transformative if that organisation also transacts with other stakeholders – such as suppliers, customers or maybe even competitors – on the same shared ledger. Some take an extreme view: the whole world could, in theory, be on one blockchain!

In practice the more likely scenario is that pools of participants will join together to form their own distributed ledger on the basis of shared or complementary interests. This leads to a world with multiple distributed ledgers covering different industries or parties that are linked by a common set of transactional activities.

Various technologies are being developed and tested that allow for participants in one blockchain to be able to transact or obtain information from participants in a different one.[7] This may be an important requirement for scalable use, with ideas such as 'sidechains' being developed to explore this.

Also, to collaborate in a world with multiple distributed ledgers, it will be important to establish some level of interoperability, ie a way of ensuring that these ledgers are based on common principles so that developers can build functionality using the same set of ground rules to enable scalability. Some examples include Z/Yen's software suite, ChainZy, which provides the base architecture for a range of applications, and the Hyperledger project (discussed below).

1.5.1 The Hyperledger project

The Hyperledger project brings together experts from different organisations and is attempting to establish a framework for interoperability and thereby bring a degree of standardisation to the underlying architecture of distributed ledgers.[8]

7 Transaction format, block size and token values are different between different chains – all part of the challenge in this area.

8 The standardisation of the underlying architecture will help in the case of permissioned DLTs. Integration of various permissioned and public blockchains will need meta-chains, for example as suggested by Kwan and Buchman in their paper on Cosmos (2017) and Wood in his paper on Polkadot, 2016 or 2017.

Hyperledger is also developing a 'blockchain-as-a-service' approach which can help customers create, deploy and manage blockchain networks, all enabled through a cloud-based system.

Founded from the open source Linux community, Hyperledger offers blockchain options with an integrated tool set called 'Hyperledger Fabric' to connect with the legacy world and create and build a business network.

As a membership based permissioned blockchain, the emphasis on the Hyperledger implementation is the business transaction, delivering a hierarchy of roles and actors that support ledger updates, consensus, events, systems management, wallet integration and smart contracts. Tokens can be added or used.

Members have different levels of participation, but all have access to their own transactions and keep a copy that is synchronised by the network, ensuring that privacy is maintained and identity (which can remain private) assured. It is a community-based collaborative environment that provides industries with an effective way of working together to solve industry issues, with certain aspects of governance exercised through a centralised authority that certificates actions, decisions and transaction types.

Hyperledger is a shared system of records that helps member organisations to integrate their legacy operations with the blockchain and start using it; the various participants may have different roles, known as nodes, on the blockchain. For example, a peer node monitors ledger state, an endorsing peer verifies and validates transactions and an ordering peer organises transactions into blocks for entry to the ledger and communicates with other nodes. Unlike many other blockchains, Hyperledger can handle transactions and messages through different channels, so improving overall performance.

Hyperledger is also developing a 'blockchain-as-a-service' approach which can help customers create, deploy and manage blockchain networks, all enabled through a cloud-based system. This may over time make blockchain a much more accessible proposition for a range of organisations that would find it difficult to create a blockchain on their own.

2. Commercial applications for distributed ledgers

When considering commercial applications, the starting point is a critical, unbiased analysis of what the problem is that needs to be solved and why distributed ledgers might help.

2.1 SOLVING THE RIGHT PROBLEM

When considering commercial applications, the starting point is a critical, unbiased analysis of what the problem is that needs to be solved and why distributed ledgers might help. This is essential to avoid the risk of meddling with a business process that is already 'good enough' for what is required.

To manage this risk, it is worth considering the following concerns.

- **Fear of missing out:** are distributed ledgers being experimented with because they are a shiny new tool that needs to be tried out?
- **Fitting the question to the answer:** are distributed ledgers intended to solve this sort of problem or are they being force-fitted to do something for which they were not designed?
- **Using a sledgehammer to kill an ant:** it's the right type of problem but does it involve enough complexity or scale to justify use of distributed ledgers or would a traditional database do the job?

Many potential commercial applications have been suggested and, in general, three problem areas are consistently emerging as the most suitable, as shown in **Figure 2.1**: those where there is a deficit in efficiency, visibility and/or trust, which we will consider in more detail in section 2.2 below. These areas are not mutually exclusive, of course, and, in reality, a given use will overlap across multiple or all problem areas, even if it is primarily targeted on one.

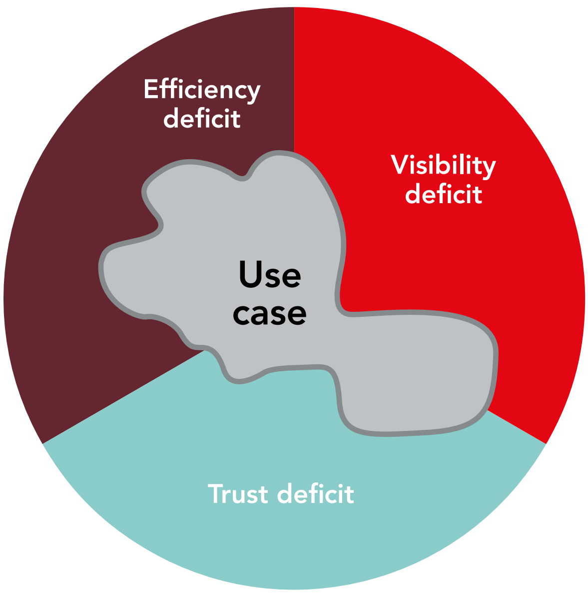
2.2 DISTRIBUTED LEDGERS IN ACTION

2.2.1 Efficiency deficit

Industries that involve a large amount of manual processing, 'legacy' systems or have heavy reliance on outdated and/or offline modes of working could benefit. One example is in dealing with trade finance transactions, as shown in **Figure 2.2**.

This is a mature area with long-standing practices. These practices have evolved so that importers and exporters do not have to deal with banks in a foreign country and can therefore avoid the complications of foreign regulations and of establishing credit worthiness overseas. The process is

Figure 2.1: What problem are we trying to solve?



Distributed ledgers allow banks to improve efficiency levels without compromising trust.

paper heavy with original documents, even in today's digital world, often sent as hard copy by courier and needing a manual counter-signature.

It can take one to three weeks for a transaction to be completed. When scaling this to the many thousands of importers and exporters operating in hundreds of jurisdictions around the world, the result is a trade finance industry that is incredibly inefficient for banks.

The industry has evolved in this way to solve a trust deficit problem between importers, exporters and overseas banks. In solving this problem, however, a massive efficiency deficit problem has been created.

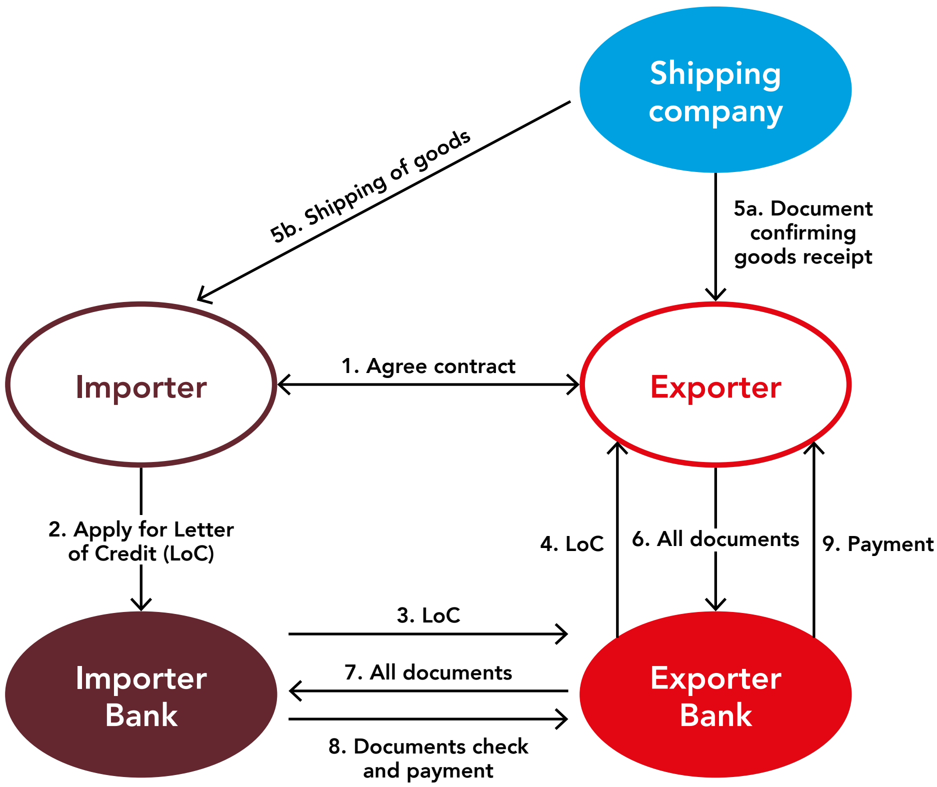
Distributed ledgers allow banks to improve efficiency levels without compromising trust. The ledger would contain the contract between importer and exporter, letter of credit, shipping receipt and a range of more detailed paperwork not mentioned in the simplified example above, such as regulatory documentation (eg for customs) and insurance. Multiple parties, such as the importer, exporter, their banks, shipping company, regulatory bodies, shipping/port authorities and other relevant stakeholders, would be able to access the ledger.

Encryption restricts access to authorised parties for relevant parts or 'events' of the transaction. For example the event between the importer and their bank in creating the letter of credit would not be visible to the exporter. The latter's view would be restricted to the events pertaining to its receipt of the letter of credit from its own (ie the exporter's) bank.

Parties on the ledger achieve consensus on the digital record of a transaction event before it gets legitimately added to the ledger. At the end, in order to fulfil the transaction (ie make payment to exporter) a smart contract would trigger the instructions once certain pre-conditions, such as receipt of goods by importer, had been met.

Ultimately, banks deal with documents rather than the underlying goods, and trustworthy digitised copies of these documents provide them with the material they need to establish trust via shared ledgers.

Figure 2.2: Simplified outline of a trade finance transaction



Supply chain visibility refers to the ability to track goods as they transit through the various stages of their creation, distribution and sale.

2.2.2 Visibility deficit

Supply chain visibility refers to the ability to track goods as they transit through the various stages of their creation, distribution and sale. The increasingly global nature of supply chains means that seeing who is involved is not always straightforward, particularly if the supply chain is in a foreign jurisdiction. Also, with frequent use of outsourcing and many processes now handled outside the systems and processes of a company, it difficult to have clear evidence of the product's journey through the supply chain.

The garment supply chain is a typical example. In general terms a supply chain can be expected to involve certain common actors, namely producers, suppliers, manufacturers, wholesalers, retailers and end customers. Taking the example of a shirt, this could translate to: the farmer growing the cotton, the cotton mill that converts raw cotton into thread, the weaving factory that makes the fabric, the shirt-making factory that stiches the fabric into shirts, the garment warehouse that buys shirts in bulk and the shop that sells shirts to the general public. It is very possible, indeed likely, that these stakeholders will be in different parts of the world, often with the factory in a low-cost location, but retailers elsewhere.

A typical mechanism may involve the integration of shared ledgers with other technologies such as mobile systems and the Internet of Things (IoT) in order to achieve a solution that is user friendly and practical. As a starting point, in the above example, cotton farmers might have been certified by an independent body to confirm their credentials. This provides the starting point for involving mobile technology.

Mobile phones are accessible to users in many parts of the world, including in low-income[9] countries where penetration is 60 mobile subscriptions per 100 people. So farmers could use mobile devices to send a text message, which would be used to generate an entry in the shared ledger. This could confirm, for example, that a given numbered consignment of cotton bales was produced on a given date and sent to an identified mill for further processing.

These consignments, now logged in the ledger, would be sent to the cotton mill. As is always the case with distributed ledgers, these transaction events are also logged so there is a record of which mills received which consignments on which dates.

There is also the potential for an interface with IoT technology, for example in the form of smart tags that can be attached to consignments. As a result, when the cloth was made from the cotton, it would remain possible to see which consignments and farmers it originated from, and where it had travelled when it left the factory.

Smartphone applications can be used to scan these smart tags; this gives visibility of the full supply chain history as stored in the distributed ledger. This aspect becomes particularly important as one goes further down the chain, with various consignments being sent to different manufacturing units for the production of shirts. It is likely that a given shirt will have cotton contributed from various originating sources and the smart tag offers a window into a robust distributed ledger record of all the events leading up that point.

This immutable record is a valuable resource and its utility spans the full range of involved stakeholders, who may value it for differing reasons. The end customers may want comfort that the shirt they purchase is ethically sourced without the use of child labour. Or a regulatory authority may want data tracking the cross-border movement of materials so as to check taxes or customs payment schedules.

Provenance is a key benefit here. For perishables, the visibility of supply chain – sometimes called 'field to fork' or 'field to shelf' – is evidence not just of shipping but also of freedom from tampering. One global issue concerns counterfeit products, where governments lose tax revenue and brands are damaged by faking, and people are dying because of dangerous products. Distributed ledgers may be a useful part of the solution.

9 World Bank, Mobile Cellular Subscriptions (per 100 People), 2015.

If all the participants could look at a secure encrypted common view via a distributed ledger, it could potentially reduce the duplication significantly, reduce costs and free time for other activities.

2.2.3 Trust deficit

This goes to the heart of distributed ledgers as a 'trust engine' that can allow network participants to have confidence in the information contained in the ledger.

Another example concerns know-your-customer (KYC) documentation, required by many regulators. The KYC process exists because one doesn't know enough about the counterparty one is transacting with and requires further information to establish trust that it is safe to proceed.

Let's consider how this works in a simplified situation within the insurance industry. To ensure that customers can get advice about a range of options available in the market, the industry structure is based on broker intermediation. So the broker would request documentation from the customer to cover the information required (ID checks, for example) for the KYC process.

The broker then proposes the case to the underwriter. Because it is the latter that will take the risk onto its books, it will conduct its own KYC on same customer. This will be based on the same information already obtained by the broker for the same purpose. In addition, underwriters often use a reinsurer to transfer risk, and the reinsurer will then redo the whole KYC process.

Essentially brokers, insurers, and reinsurers all have to perform KYC on all their counterparties, both legal entities and individuals, including third parties who are due payments under claims.[10]

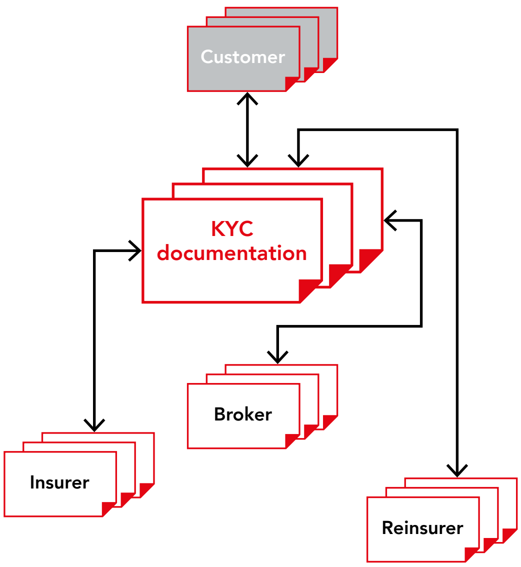
This means their each re-doing the same process, on the same source information, for the same reason. Clearly, this creates an inefficient cycle of repeats – all linked to a regulatory requirement to obtain the same information. This is a source of costs and delays, for no real additional insight into the customer or reduction in their risk profile.

If all the participants could look at a secure encrypted common view via a distributed ledger, as shown in **Figure 2.3**, it could potentially reduce the duplication significantly, reduce costs and free time for other activities.

The distributed ledger could be used to record all the customer's personal documents and evidence of validation held by the organisation or by an outsource service provider. All documents on the ledger would be encrypted, with only the customer having the keys, thus resolving a set of regulatory issues around privacy and data protection.

The customer could then present the ledger with an appropriate subset of keys to the next institution with which they want to do business. This institution would then be able to rely on the validation done initially, eliminating delays, reducing costs and time spent on KYC procedures overall.

Figure 2.3: Placing KYC documents in a secure distributed ledger



10 Michael Mainelli and Bernard Manson, *Chain Reaction: How Blockchain Might Transform Wholesale Insurance*, July 2016.

3. Distributed ledgers and professional accountants

There is an inherently futuristic element to any discussion about distributed ledgers. There is, however, also a reality that defines the current working life of professional accountants and will be used here as a starting point when assessing what distributed ledgers could 'mean' to them.

3.1 STARTING WITH THE PRESENT

There is an inherently futuristic element to any discussion about distributed ledgers. There is, however, also a reality that defines the current working life of professional accountants and will be used here as a starting point when assessing what distributed ledgers could 'mean' to them. This situation is fast changing and evolving. So rather than final answers, the aim of the account below is to provide food for thought and a more granular understanding.

3.1.1 The auditor[11]

Completeness The distributed ledger removes multiple, disjointed internal and external databases of records that need reconciling – and should reduce the risk of inadvertently missing transactions through timing mismatches or booking errors.

Auditors conduct testing on the basis that the organisation may not always have the best intentions. Could a rogue employee intentionally leave certain entries outside the ledger to understate liabilities? How would a distributed ledger remove the need for the auditor to exercise judgement in knowing what to look for and how to test for it, such as by examining related accounts?

Occurrence Use of public and private encryption keys in the shared ledger validates both source and destination in a transaction. Also, new transactions may only be added if validated by the majority of users, which may neutralise a rogue actor.

It appears to be relatively difficult, expensive or otherwise impractical to unilaterally introduce false transactions into the network.

Valuation Asset valuations may depend on a variety of factors, including business and operating conditions, future expectations and technology. Valuation is not an exact science and distributed ledgers do not appear to be designed to help the auditor with this sort of analysis. It is not the sort of calculation that can be trivially derived from the ledger record of transactions.

Classification and understandability
It may be helpful – from an understandability point of view – for transaction information or account balances to be aggregated (to avoid missing the bigger picture) or dis-aggregated (to see major risks that might otherwise get netted off). It is difficult to specify a way in the code that allows for this flexibility.

Accuracy Transactions booked in a transparent manner and without involving intermediaries could help maintain accuracy, although human error remains a factor. But the transparency safeguards should ensure that everyone can see when there has been an inaccuracy, and if immutability is respected the audit trail will be preserved; a correcting entry is added rather than removing or changing historical entries.

Nonetheless, the auditor needs to combine the ledger information with

Table 3.1: Using distributed ledgers to test audit assertions

	AUDIT ASSERTION	DESCRIPTION	POTENTIAL FOR DIRECT BENEFIT FROM DISTRIBUTED LEDGERS (INDICATIVE VIEW)*
1	**Completeness**	All transactions are recorded in the financial statements	√√
2	**Occurrence**	The transactions in the financial statements actually happened	√√√
3	**Valuation**	Items in the financial statements have been included at appropriate amounts	√
4	**Classification and understandability**	Financial information is correctly categorised and disclosures are clearly communicated	√
5	**Accuracy**	Data is recorded at the correct amounts, which are verifiable in source documents	√√
6	**Rights and obligations**	Correctly establishing right to use or dispose of assets as well as obligations to pay off liabilities	√
7	**Cut-off**	Recording of transactions for the correct accounting period	√√√

* More √ indicates greater potential for direct benefit. Excludes indirect benefit where DL might improve data quality in general terms which creates knock-on benefits

11 Refers to the external auditor in the context of conducting a statutory audit.

Nonetheless, the auditor needs to combine the ledger information with policies and generally accepted accounting principles, such as when testing accuracy of depreciation amounts.

policies and generally accepted accounting principles, such as when testing accuracy of depreciation amounts.

Rights and obligations The distributed ledger provides a robust view of ownership, but it may be less straightforward to establish the rights and obligations linked to it.

With third-party warehousing, the inventory may be flagged as owned, but the organisation may not have unimpeded access to the warehouse where it is stored. On the other hand, with consignment inventory, the assets may be available for use by the retailer, but the ownership may still be with the supplier. Distributed ledgers do not seem suited for capturing this type of nuance and interpretation.

Cut-off In the distributed ledger, the digital record of the transaction is firmly linked to the transaction itself. In other words, the record of the transaction and transaction event itself are triggered simultaneously. This makes it difficult to envisage a situation where a transaction that does not belong to one accounting period can be included within the records for that period.

3.1.2 The accountant working within the organisation

Management accounting Distributed ledgers help transaction-level data to be compiled, checked or reconciled but their role in non-financial information (as required for integrated reporting) or qualitative commentary on performance is less clear.

Finance business partnering This requires the auditor to be the gatekeeper who views the business from a risk perspective, but also a business unit staff member who can contribute insights to help increase divisional revenues. Building trust in this context requires superior communication skills and a high emotional quotient. These skills are not connected with the type of transaction management that distributed ledgers improve.

Regulatory compliance The emerging area of 'RegTech', combining regulation and technology, may change the current operating environment, since proof of compliance requires data from transactions to be readily available and trustworthy. Distributed ledgers may give the regulator a more transparent view of an organisation's ability to meet requirements.

Strategy and performance This work is unlikely to be directly affected but those involved in it will need to understand distributed ledgers as they could affect the business case for certain activities conducted by the finance function. Technologies like this, in combination with others – such as robotic process automation – may have a significant impact on the return on investment of the finance function.

3.1.3 The picture so far

These initial explorations suggest that distributed ledgers increase trust in transaction data, but that the accountant's role involves certain aspects of financial and organisational performance that are not solely linked to superior transaction management and therefore will not be directly affected by this technology.

Table 3.2: Distributed ledgers and the roles of accountants working within an organisation

	EXAMPLE ROLE	DESCRIPTION	POTENTIAL FOR DIRECT BENEFIT FROM DISTRIBUTED LEDGERS (INDICATIVE VIEW)*
1	**Management accounting**	Preparation and use of financial and non-financial information	√√
2	**Finance business partnering**	Supporting divisions or business units to deliver organisational outcomes	√
3	**Regulatory compliance**	Policy and implementation level adherence to regulations relevant to the organisation's activities	√√√
4	**Strategy and performance**	Direction setting, and driving organisational performance to deliver strategy	√

* More √ indicates greater potential for direct benefit. Excludes indirect benefit where DL might improve data quality in general terms which creates knock-on benefits

With a distributed ledger it is possible to generate an exceptions report that reviews all transactions rather than just a selected sample of them.

3.2 LOOKING AHEAD

3.2.1 Why might things be any different?

Volume of data In a world of big data and the Internet of Things (IoT), the volume of data that is expected to be generated in the years ahead is enormous. It represents a step-change rather than a steady increase, as is evident from the fivefold increase in the number of devices forecasted to be transmitting data in the 10 years from 2015 to 2025 (**Figure 3.1**).

This increased data will translate into quadrillions of transactions creating greater complexity and volume for systems and databases to handle. This level of scaling also has the effect of magnifying inefficiencies. Inefficient processes or reconciliation requirements are painful even at current levels of volume – at this future level of scale it is unclear if current ways of doing things (even adjusting for steady improvements in processing power) would be practical.

Tokenisation A token is a digital representation of an underlying entity, such as an asset. It may be used to establish one's claim to that asset, and to transfer ownership of the asset, via the distributed ledger, to a new owner. Smart contracts could determine the conditions for the transfer to occur.

Tokens can also be used to associate fractional ownership of assets such as art, commodities, financial instruments, copyright, profit sharing and dividends and work with several decimal places,[12] allowing value to be syndicated in new ways, and creating new tradable instruments.

3.2.2. Can distributed ledgers help with audit?

Immutability Key to audit is the immutable record of the full list of transactions from the time they first entered the ledger. The potential for a comprehensive audit trail that cannot be tampered with by malicious actors is appealing. This may reduce the costs of fraud detection if there is no, or significantly reduced, need for further checks on the transaction data.

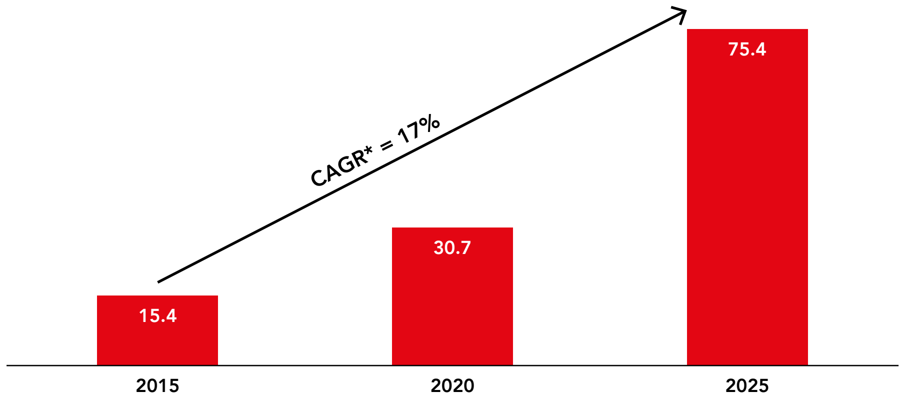
Sampling This immutable record is likely to have implications for sampling. The current process of selecting a representative sample from within the population of transactions is necessitated by human limitations on the time and cost of reviewing transactions.

With a distributed ledger it is possible to generate an exceptions report that reviews all transactions rather than just a selected sample of them. From a probabilistic point of view, this is more robust and results in less uncertainty about the audit conclusions.

Timing In addition, the current audit process, again because of the time and effort invested in it, is typically an annual exercise. Distributed ledgers may make it possible to conduct more frequent audits on a quarterly or monthly basis. Taken to its logical extreme, even a real-time audit is conceivable.

This could make it practically impossible for transactions to be adjusted in advance of audit scrutiny and could present auditors with exceptions reporting on a continuous

Figure 3.1: Internet of Things (IoT) installed number of devices, in billions



Source: IHS

*Compounded Average Growth Rate

12 Bitcoin has eight decimal places, others vary.

The aim is to reduce risks from unknown-unknowns within the transaction data.

year-round basis. This improves the auditor's understanding of the business, as the engagement is no longer based on a snapshot at a given time of the year. This can facilitate the ability to spot trends or future risks proactively.

True and fair view This greater contextual understanding will increase confidence that auditors are getting a true and fair picture. It will also provide time to deepen understanding of the overall business model, rather than reducing the audit to a tick-box compliance exercise. Initiatives such as the extended audit report are already laying emphasis on developing this deeper understanding of the business, and distributed ledgers might have arrived at the right time to advance this priority.

3.2.3 Considerations for the accountancy firm

Any possible future model for the accountancy firm will depend, at a minimum, on the business model for generating revenues, and on the operating model that determines the processes and people to realise the business model.

The current business model Audit revenues are linked to the hours required, with charge-out rates being calibrated to reflect experience and skills. This is so because an audit job involves an identifiable volume of work based on a well-defined set of tasks, usually linked to statutory requirements. This rigorous and defined set of input activities, as captured in the audit work papers for that engagement, is designed to build trust in the output – which is the view expressed in the audit report.

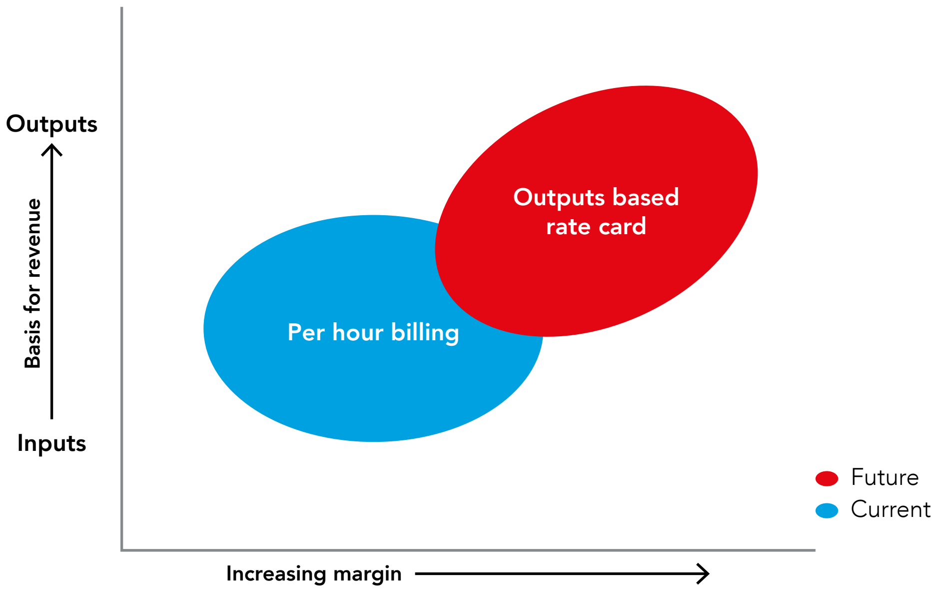
Since the fee is linked closely to input activities it has historically made sense to charge on a time basis with a per-hour billing rate.

The aim is to reduce risks from unknown-unknowns within the transaction data. If auditors know of a risk, they can test for it and decide whether it is material or not. If they do not know of it, there is nothing they can do about it. The rigorous set of input activities governing the audit process acts as a mechanism for sweeping up all possible areas that need to be considered, and reducing the likelihood of an unknown-unknown.

The future business model If a distributed ledger can give a definitive view of the entire transaction data set rather than a selected sample, it might be possible to reduce the risk from unknown-unknowns.

The auditor role may pivot towards non transaction-management elements requiring human judgement, business context and knowledge of technical accounting policy and of the outputs created by the application of these elements to specific questions within the audit, for example the fair value of assets (**Figure 3.2**).

Figure 3.2: Business model for accountancy firms: possible direction of travel?



The auditor's role may now be less standardised and prescriptive across assignments, and pivot away from checking transaction data.

For the auditor, revenues generated may be increasingly tied to providing a view in response to specific questions, which may vary from assignment to assignment. The auditor's role may now be less standardised and prescriptive across assignments, and pivot away from checking transaction data.

The auditor may still need to be able to interrogate or provide some form of assurance that the outputs of the technology can be trusted. While the details will differ, this may not be hugely different in approach to systems assurance as currently conducted.

The revenue generated by audit firms may become increasingly de-linked from a standardised prescriptive list of input activities and the time and effort they take. And move towards a more outputs based approach.

Over time, this might increase the proportion of revenues linked to an outputs rate card, rather than a per-hour billing rate.

The outputs might be achieved in a range of situations – anything from a technical accounting policy opinion, an audit view on materiality for a difficult-to-quantify value, mergers and acquisitions implications, to forensic accounting, etc. But they are all likely to share the common attribute of not being a standardised and repeatable answer to a generic question.

It will take time to gauge the impact of this shift on overall revenues for audit. But what could become clear sooner is a likely change in the revenue mix. The catalyst for this may be a gradual move away from low margin activities, towards a greater emphasis on paying for expertise and advice rather than for time required.

The Operating model – platform-based operations? If the revenue mix does evolve, some firms might choose to explore the role of platform-based operating models for certain services, such as data collection, records checking, bookkeeping or exceptions reporting. These might be performed through platforms jointly held by a firm and its platform partner, with the client getting an 'accounting-as-a-service' offer for certain standardised tasks.

It is useful to examine what is already being explored at present. Accounting software providers are a group to be understood more closely in this context and they may play a key role in future events.

The professional accountant of the future will benefit hugely from an outlook that is well rounded, resilient and adaptable to changes in the business environment.

One cloud accounting application is exploring the sharing of API[13] keys between customers and suppliers. This enables the direct passing of transaction data to ledgers on each side of a transaction without the need for verification and manual rekeying of data.

If both parties use the software provided for all messages, they are fully synchronised. This creates a channel between the two trading entities that can speed up administrative processes, improve transaction efficiency and enhance accuracy of reporting.

This seems to be moving in the direction of triple entry bookkeeping. Next steps might be increasing scalability in a network environment, with a large number of simultaneous transactions and delivery of encrypted receipts.[14]

The compliance sector is also exploring the 'as-a-service' model, with platforms emerging to provide risk and compliance reports. While many of these relate to bitcoins and public blockchains, it is not inconceivable that bespoke platforms for the needs of specific sectors will emerge in due course.

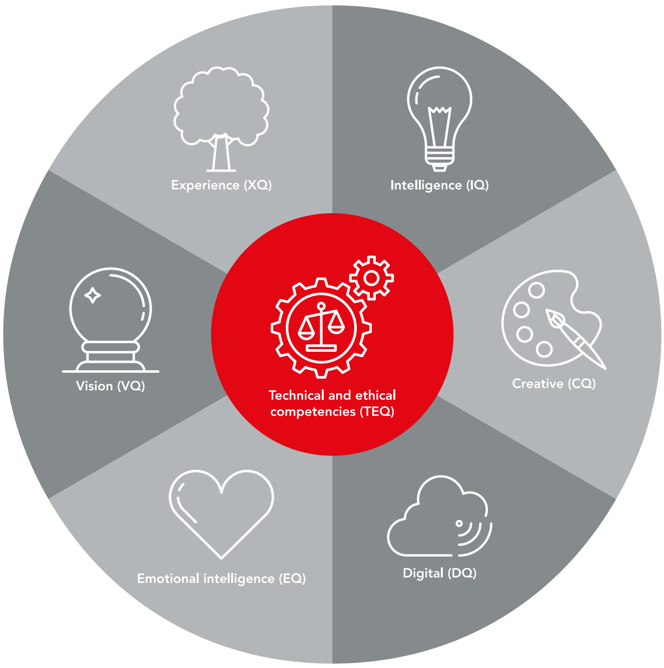
The operating model – the skills outlook

Assuming the critical caveat that distributed ledgers achieve significant mainstream adoption, they could cause the form and content of services to evolve. And so the skills needed to deliver these services may have to evolve as well.

The professional accountant of the future will benefit hugely from an outlook that is well rounded, resilient and adaptable to changes in the business environment. There may well be new areas of knowledge that need to be better understood, such as the emergence of new ways of syndicating and transferring value, ownership and rights using token-based cryptocurrencies. This may require new ways of measuring and accounting for value, as tokens pass from one owner to another or indeed from one blockchain to another. Implicit in all this, before even getting to this level of detail, is an assumed, at least high-level, knowledge of how these mechanisms work.

But alongside acquiring this knowledge, there is the need to recognise that learning must be continuous and lifelong. The professional accountant of the future must be able to incorporate this and embody the skills quotients[15] outlined in **Figure 3.3**.

Figure 3.3: Professional quotients for success



13 Application Programming Interface: building blocks for creating application software.

14 Other industries are also exploring new ways of working via shared ledgers, eg legal services.

15 ACCA, *Professional Accountants – the Future: Drivers of Change and Future Skills*, 2016.

Accounting firms that stay abreast of developments may find they are better prepared for future client retention and increasing market share.

Bringing it all together A big part of achieving success, when there are really big changes involved, is effective leadership. While all can be leaders at their own level, some have a particular responsibility. Whether they are chief financial officers (CFOs) in an organisation or partners in an accountancy practice working with client organisations, the leadership skills of senior practitioners will often be the single biggest determinant in arriving at the right response strategy. It is for them to take the first step and, as Table 3.3 outlines, this can be kept fairly simple to begin with and gradually built up as more information emerges.

Accounting firms that stay abreast of developments may find they are better prepared for future client retention and increasing market share. Firms that can drive the client relationship towards a more output-based proposition, and keep the door open for possible service platform models if required, may be well placed for future developments and resilient against future threats.

3.2.4 Legal and regulatory framework

It seems less likely at this stage that the fundamental regulation of business form (partnership law, company formation law, etc.) will change significantly in the short term.

Statutes change slowly, and legislators will take time to understand the features of any new model before creating blockchain-specific corporate bodies. Some are making a start, with the European Union (EU) considering inclusion of cryptocurrencies as part of upgrading the Anti-Money Laundering Directive – though this may take some time to be fully analysed.

Time will show whether smart contracts can replace a traditional natural language contract, with all the complexity and subtlety that contracts used in a court of law involve. Investors will want to see a defined and explicit linkage or alignment to an established legal system before engaging with such tools in any meaningful way. There will also need to be evidence of effective dispute resolution where these smart contracts are involved, so that confidence builds.

Table 3.3: Taking the first step

STAGE	KEY CONSIDERATIONS
Establish baseline	What is the current level of understanding in my organisation? Do we need a designated lead to coordinate work in this area? Is there a case for organising basic training or knowledge building?
Evaluate landscape	Which of my organisation's partners, clients or suppliers might be considering a proof of concept application? Which of my organisation's clients are in an industry that is actively exploring this (such as financial services)? Are there lessons to be learned from industries or sectors other than my own? What is the regulator or government saying about this in our jurisdictions? Which of our existing competitors is starting to explore this area? What new types of organisation could become future competitors?
Estimate impact	Can we identify any possible role for distributed ledgers in our main revenue generating activities? On the basis of the above, roughly how much of our revenue could be 'at risk' in 3 years? If 'at risk' revenue seems nil at present, when should the next check-point be to re-assess this?

> In practice, the ability of the government machinery to understand and engage will be a big part of incorporating distributed ledgers and cryptocurrency arrangements into the mainstream.

RegTech is an area that is fast emerging as a case example of what a partnership between nimble start-ups and regulatory bodies might look like. Regulatory 'sand-boxes' provide start-ups with the opportunity to test their ideas. This gives regulators early visibility of potential financial products/services and may enable them to respond effectively.

It allows the regulator to think ahead about the best regime for balancing innovation and risk. This is much more powerful than trying to retro-fit existing clunky regulation to new areas that have quickly grown and caught regulators unawares.

3.2.5 Implications for taxation

For some areas, such as value added tax (VAT) and customs duties, the implementation of Fiscal Till programmes might prove helpful. Fiscal Tills are secure transaction recording tools that retain a tamper-proof record of cash transactions to form the basis of a business's tax records, typically VAT/GST (goods and services tax), but potentially profits-based income taxes as well.

Currently, systems have a number of potential cost and security shortcomings, such as being based on specific hardware that needs system-specific software. Distributed ledgers based on software rather than hardware may offer the benefits of instant refund payments where due, reduce scope for fraudulent transactions and facilitate low-cost instant transmission of verified tax information to facilitate prompt repayments.

In practice, the ability of the government machinery to understand and engage will be a big part of incorporating distributed ledgers and cryptocurrency arrangements into the mainstream. There is no regulatory framework for bitcoin. It isn't owned by anyone, and crosses borders and jurisdictions. Like the transmission control protocol/internet protocol (TCP/IP) on which internet communication depends, it cannot be controlled or regulated. The network is independent, an 'eco-system' of anonymous 'miners'. This therefore will require a different mindset from traditional government approaches.

3.2.6 Future risks

Managing scale As distributed ledgers move beyond proof-of-concept, and projects such as Hyperledger become more mature, it will become clearer whether the architecture has sufficient control and governance to ensure that all actors work in the best interests of the community and that the safeguards are adequate to prevent collusion.[16]

A FINE BALANCE

Achieving the right balance between innovation and regulation is crucial to financial regulators from the perspective of risk management and industry development.

The approach used by the Monetary Authority of Singapore (MAS) stresses that regulation must not run ahead of innovation. Introducing regulation prematurely may stifle innovation and potentially disrupt the adoption of useful technology. Further, as technologies mitigate existing risks but may create new ones, MAS also seeks to focus on the balance of risks and minimise these new risks.

To achieve this, two basic tests are applied to regulating blockchain and emerging technologies more generally: materiality and proportionality.

Materiality refers to bringing in the regulation only when the risk posed by the new technology becomes material or crosses a threshold. Once this has been established, the weight of regulation must be proportionate to the risk posed. The regulatory approach must encourage risk mitigation while restraining the new risks.

In other words, the regulator must run alongside innovation, rather than ahead of it, if it is to promote safety, soundness and long-term sustainability in the provision of financial services.

16 Particularly for Proof of Stake and permission chains, with owners. Users may be concerned the owners are not neutral and have adapted the code for gain.

Cryptocurrencies are based on libertarian views, offering a permissionless, trusted, 'level playing field', particularly to the unbanked in emerging markets.

Sovereign intervention Fiat currencies may be open to manipulation by governments; often the basis for an argument that the current system of Fractional Reserve Banking[17] isn't working. Cryptocurrencies are based on libertarian views, offering a permissionless, trusted, 'level playing field', particularly to the unbanked in emerging markets. New options may arise for issuing sovereign debt using cryptocurrencies to create stability, fungibility and liquidity.

But on the other hand, sovereign states that have had a tough time economically or a political agenda that is disruptive might be attracted to cryptocurrencies for the wrong reasons. This is, after all, programmable money that an unscrupulous government might try to manipulate, exploiting the perception of an open, fair and transparent distributed ledger.

The big hack As any new technology matures it will be under constant attack from cybercriminals and hackers testing and probing for vulnerability. For a long time, decentralised and distributed computers were thought to be more vulnerable than a centralised approach. Whether it is a Sybil or distributed denial of service (DDoS) attack,[18] the blockchain has so far proved especially resilient and has not been successfully attacked.

Recent hacks have found vulnerabilities in electronic wallets held on mobile phones and desktops where the owners have not kept their private keys safe. There is also the example of the DAO[19] hack where flaws in the smart contracts code allowed USD50m in value to be moved.[20] In addition, quantum computing may present a key challenge to the ability to use current encryption techniques to safeguard data. It can complete operations while using less computing power and with greater speed. This may make it easier to perform more intensive calculations and hack systems.

3.3 SO WHERE DOES ALL THIS LEAVE THE ACCOUNTANT?

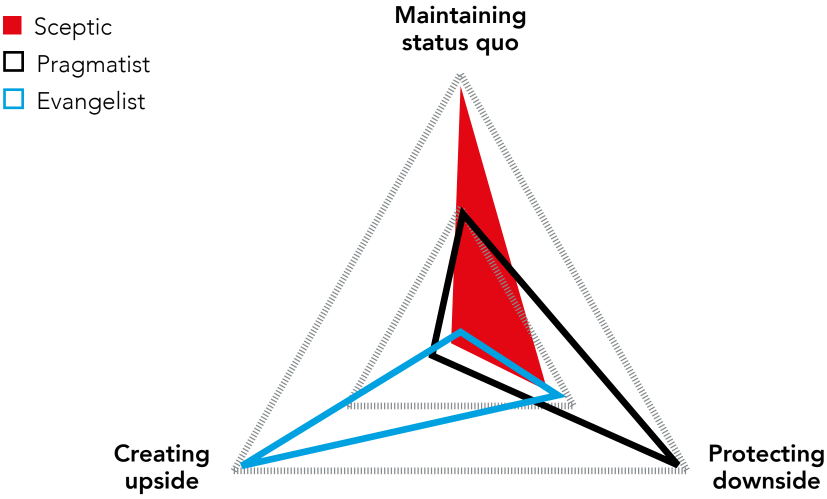
The importance of leadership skills in formulating the organisational response has been discussed. But there is also the individual response. Individuals working across an organisation have their own views that might or might not agree with that of their organisation.

3.3.1 The sceptic

Distributed ledgers are seen by sceptics as a 'solution looking for a problem'.

As with many other fads that came and went before them, the belief is that they will generate a lot of discussion but that ultimately the status quo is unlikely to be materially altered.

Figure 3.4: Professional accountants – view on distributed ledgers



17 Bank reserves are a fraction of deposits.

18 Sybil and Denial of Services attacks relate to decentralised computing where individual nodes can be probed for vulnerability and where nodes could collude and work together for commercial gain. The Byzantine Fault Tolerance algorithm was specifically designed to identify actors operating against the interests of the network.

19 Decentralised Autonomous Organisation.

20 Source: O. Kharif, 'A $50 million Heist Unleashes High-Stakes Showdown in Blockchain', *Bloomberg Technology*, 23 June 2016.

A detailed understanding of how the data was generated may become more important than checking the data itself.

Whether this represents Luddite zeal or foresight is of course something that time will reveal. As has often been noted with new technologies, there is the possibility of over-estimating impact in the short-term but under-estimating it in the long-term. Sceptics will no doubt focus on the first part of that claim.

There are, however, a few factors for them to consider.

Firstly, in a digital age, it is easier to 'fail fast'. The time it takes to concept test ideas, launch them, fail, refine/change and try again, may not be as much of a barrier as in previous waves of technology. This raises the likelihood of eventually getting a solution that works.

In addition, there appears to be no shortage of capital to fund innovation in this area, whether it is from commercial banks forming consortiums, central banks willing to test blockchain solutions, or the range of venture capital financiers seeking the next successful technology. Again, this raises the likelihood of eventually getting a solution that works.

Finally, because these ledgers have impact across the whole economy, even if one works in an organisation that doesn't have much time for all this, the suppliers or customers might use it and, in order to transact cost-effectively with them, it may become necessary to use this technology in order to operate.

None of this guarantees large-scale mainstream adoption, of course, as sceptics will point out. But the bottom line is that five years is viewed as a reasonable time frame for the technology and its use to mature – so one way or another it won't take for ever to find out.

3.3.2 The pragmatist

The pragmatist doesn't have a particularly strong view on distributed ledgers, but would like to be prepared for any change – just in case. The emphasis is on protecting against the downside and is generally accompanied by a relatively neutral emotional response to these ledgers; the pragmatist is neither dismissive of the technology nor a cheerleader for it.

In many ways, this approach ensures that there is a connection with underlying skills requirements despite evolving business and operating models. As an analogy, being a cab driver in the 19th century involved the skill of controlling a horse. The same job in the 20th century involved the skill of driving a car. Looking ahead, with the prospect of driverless cars, the job of a cab driver in the 21st century may well involve understanding the software that controls the car.

Similarly, the auditor may no longer need to understand sampling techniques or query individual transactions. But in its place the job of an audit may place a much greater emphasis on the skill of querying the technology, and knowing where and how to look for potential issues in the system or the use of data. A detailed understanding of how the data was generated may become more important than checking the data itself.

So the pragmatist is likely to prioritise an understanding of new skills requirements that might stem from this technology as an insurance policy covering unforeseen events.

3.3.3 The evangelist

These are the people who genuinely believe in distributed ledgers, and who see them as an opportunity rather than a distraction, inconvenience or threat.

The mindset of these early adopters is often shaped by the view that the upside opportunity is exciting and important. It allows professional accountants to increase their value to the organisation, and spend less time on tasks that the technology can handle faster, with fewer errors and on a much larger scale.

As the use of distributed ledgers, and indeed of FinTech more generally, starts to grow, the evangelists see a whole new sector in which to get involved. Some accountancy practices, for example, now offer FinTech services within their sectorial offerings, specifically with an eye to increasing their size and their revenues from this new base of clients.

Evangelists would argue that this is just the start and a whole new set of possibilities lie ahead.

4. Conclusion

Whatever one's opinion about distributed ledgers, they look likely to be the focus of sustained attention over the coming years.

Whatever one's opinion about distributed ledgers, they look likely to be the focus of sustained attention over the coming years. Innovation, where it concerns new technologies in particular, tends to be a constant iterative process of improvement by trial and error. And this distributed ledger technology is very much in the early to middle stages of that development.

Its attractiveness is as an idea that creates more than a technology process improvement. It aspires to create a business model and eco-system-level transformation. That's a bold aspiration, the evolution of which will be closely watched in coming years.

And the answer as to whether it ultimately succeeds or not might not be binary. Just as online learning did not eliminate the classroom teaching model, distributed ledgers may prove to be at their best when used alongside human experience and judgement.

Appendix 1

Organisations involved in blockchain development

- The first blockchain company to offer triple entry bookkeeping was Balanc3 (part of the Consensys spoke model): **http://balanc3.net/**
- Consensys is a leading Ethereum platform and valuable blockchain vendor business creating solutions for accounting, music, asset management and content management; it was founded by Joe Lubin, also an Ethereum founder: **https://consensys.net/ventures/spokes/**
- Chain Inc. is a blockchain business that supports the digitisation of currency as tokens: **https://chain.com/**
- Abra is a next generation payments and remittance provider using blockchain: **https://www.goabra.com/**
- Microsoft has committed to blockchain and offers a fully integrated 'blockchain as a service' option linking to its enterprise software called Bletchley: **https://azure.microsoft.com/en-gb/solutions/blockchain/**
- cashaa is a blockchain remittance and payment company working with unbanked people in Africa and using bitcoin financial systems: **https://cashaa.com/**
- Cryptocompare is a blockchain comparison website offering crypto economics/currencies comparisons: **https://www.cryptocompare.com/coins/#/btc**
- Ethereum Live transaction dashboard is the home of Ethereum markets: **https://ethstats.net/**
- Assembly is a blockchain business that allows collaborative value creation and profit sharing using APPCoins: **www.assembly.com**
- Ambisafe is a blockchain asset-management platform that allows the tokenisation of any assets: **www.ambisafe.com**
- Nxt and Ardour is an alternative to bitcoin and Ethereum; it provides a decentralised asset exchange: **www.nxt.org**
- Exscudo is a new blockchain exchange, four years in production, providing the gateway between capital markets and the cryptocurrency market 2.0 Platform: **http://exscudo.com/**
- Banking 4.0 is the next generation of banking for the previously unbanked, using BIO Identity software: **www.humaniq.co**
- Ethereum Foundation is a decentralised autonomous organisation or DAO: **https://www.ethereum.org/dao**
- Tokenmarket exists for creating tokens, distribution, and crowd-sale hosting for initial coin offerings: **https://tokenmarket.net/ico-calendar**

Appendix 2

Key data sources, references and further reading

ACCA (2015), *The Data Revolution.* <http://www.futuretoday.com/content/dam/IMA/pdf/Technology/Data/data-revolution-report.pdf>, accessed 5 April 2017.

ACCA (2016), *Professional Accountants – the Future: Drivers of Change and Future Skills.* <http://www.accaglobal.com/content/dam/members-beta/images/campaigns/pa-tf/pi-professional-accountants-the-future.pdf>, accessed 5 April 2017.

Ace Cloud Hosting (n.d.) 'Blockchain: All that it Has to Do with Your Accounting'. <http://www.acecloudhosting.com/blog/3581_blockchain-technology-with-your-accounting/>, accessed 5 April 2017.

Ali, R., Barrdear, J. et al. (2014), 'Innovations in Payment Technologies and the Emergence of Digital Currencies', Bank of England *Quarterly Bulletin* Q3. <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf>, accessed 5 April 2017.

Allen & Overy, *Decentralized Autonomous Organizations.* <http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralized%20Autonomous%20Organizations.pdf>, accessed 5 April 2017.

Blockchain (n.d.), 'A view of global blockchain mining and transaction activity'. <https://blockchain.info/blocks> accessed 5 April 2017.

Blockchain (2017), 'Hashrate Distribution'. <https://blockchain.info/pools>, accessed 5 April 2017.

Brown, R.G. <https://gendal.me/2015/04/27/how-to-explain-the-value-of-replicated-shared-ledgers-from-first-principles/>.

BTC.com (live), 'A bitcoin trading dashboard bitcoin network'. <https://btc.com>, accessed 5 April 2017.

Del Castillo, M. (2016), '"Big Four" Accounting Firms Meet to Consider Blockchain Consortium', Coindesk, August. <http://www.coindesk.com/big-four-accounting-firms-meet-to-weigh-benefits-of-blockchain-consortium/>, accessed 5 April 2017.

EtherScan a Blockchain web explorer Ethereum Market Stats and Views. <https://etherscan.io/>

Financial Reporting Council (2016), *Key Facts and Trends in the Accountancy Profession.* <https://www.frc.org.uk/Our-Work/Publications/Professional-Oversight/Key-Facts-and-Trends-2016.pdf>, accessed 5 April 2017.

Grigg, I. (2005), 'Triple Entry Accounting'. <http://iang.org/papers/triple_entry.html>, accessed 5 April 2017.

Hyperledger.org (2017), 'About the Hyperledger project'. <https://www.hyperledger.org/about>, accessed 4 April 2017.

IBS World (2017), 'Accounting & Auditing in the UK: Market Research Report'. <https://www.ibisworld.co.uk/market-research/accounting-auditing.html>, accessed 5 April 2017.

Kharif, O. (2016), 'A $50 million Heist Unleashes High-Stakes Showdown in Blockchain', *Bloomsberg Technology,* 23 June. <https://www.bloomberg.com/news/articles/2016-06-23/a-50-million-heist-unleashes-high-stakes-showdown-in-blockchain>, accessed 5 April 2017.

Kwan, J. and Buchman, E. (2017) , 'Cosmos: A Network of Distributed Ledgers'. <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md> accessed 5 April 2017.

Mainelli, M. and Manson, B. (2016), *Chain Reaction: How Blockchain Might Transform Wholesale Insurance.* <http://www.zyen.com/Publications/LongFinance_How_Blockchain_Technology_Might_Transform_Wholesale_Insurance_July2016.pdf>, accessed 6 April 2017.

Mainelli, M. and Mills, S. (2016), *The Missing Links In The Chains?* <http://www.zyen.com/PDF/The_Missing_Links_In_The_Chain_Mutual_Distributed_Ledger_(aka_blockchain)_Standards_2016.11_v2.4.pdf>, accessed 4 April 2017.

Myers, R. (2017), 'Betting on Blockchain', *CFO Magazine*, March. <http://ww2.cfo.com/technology/2017/03/betting-blockchain/?utm_content=bufferd5232&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>, accessed 5 April 2017.

Smith & Crown, 'ICOs, Token Sales, Crowd Sales'. <https://www.smithandcrown.com/icos/>, accessed 5 April 2017.

The Shared Ledger (n.d.), 'Blockchain for Auditing'. <https://sharetheledger.com/reading-list/blockchain-for-auditing/>, accessed 5 April 2017.

Wikipedia (n.d.), 'Satoshi Nakamoto'. <https://en.wikipedia.org/wiki/Satoshi_Nakamoto>, accessed 5 April 2017.

Willis, R. (2015), 'Distributed Accounting Ledgers', Medium.com, 20 January. <https://medium.com/@3ntry/distributed-accounting-ledgers-d527d31870fe#.51i0qb611>, accessed 5 April 2017.

Wood, G. (2016 or 2017), 'Polkadot: Vision for a Heterogeneous Multi-Chain Framework'. <http://www.the-blockchain.com/docs/Gavin%20Wood%20-%20Polkadot%20-%20%20Vision%20For%20A%20Heterogeneous%20Multi-chain%20Framework.pdf>, accessed 5 April

World Bank (2015), 'Mobile Cellular Subscriptions (per 100 People). <http://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=XM&name_desc=true>, accessed 6 April 2017

xBRL (), 'An Introduction to XBRL'. <https://www.xbrl.org/the-standard/what/an-introduction-to-xbrl/>, accessed 5 April 2017.

Xero Business Help Centre (2014), 'Send a Sales Invoice from Xero to Xero'. <https://help.xero.com/uk/SalesInvoiceX2X>

Glossary

Blockchain
A blockchain is a type of technology used to create a distributed ledger. A blockchain records data blocks with each block cryptographically 'chained' to the next in a linear chain of blocks, each containing transactions that create an historic immutable, tamper- and censorship-resistant record of historic truth that cannot be changed or altered. Bitcoin, Ethereum, and NXT are open permissionless architectures that anyone can use.

Cryptocurrency
A form of digital currency based on mathematical representations of value (of trade) between one or more parties in a network, the nodes of which create the digital currency as a reward for processing transactions. Cryptocurrencies are a digital representation of money or value and there are more than 900 in circulation. Not all cryptocurrencies are used as money, some are used for rewards and others are used to tokenise things/assets so they can be traded across a peer-to-peer network.

Permissionless
Permissionless networks are open to any participant, and transactions are verified against the consensus algorithm that defines the underlying rules of the network. All participants can view transactions on the blockchain ledger. Bitcoin, NXT and Ethereum are examples of permissionless networks.

Permissioned
Permissioned networks nominate certain participants within what is normally a 'permission distributed ledger'. Participants are allowed to see only the transactions relevant to them. The Hyperledger Project is founded to support the development of permissioned blockchains and is a successful example of this approach.

Consensus
Consensus is the pillar of any blockchain or distributed ledger; it defines the governance of a blockchain and sets the underlying parameters of performance, privacy, authentication, reward, fault tolerance and structure. There an several types of consensus: Proof of Work, Proof of Stake, Byzantine Fault Tolerance, Proof of Elapsed Time, Stellar, DPoS, Paxos, Raft, Distributed Concurrence and Practical Byzantine FT.

Distributed ledger technology (DLT)
DLT refers to shared, replicated databases that are synchronised across geographies, locations and companies, and that generally operate in a closed or permissioned network. They may not use a token (cryptocoin) and are deployed within an industry or large organisation as a community. Permissioned ledgers are generally faster and perform better than permissionless ones. They can be more energy efficient than bitcoin-style blockchains and therefore more economically viable for large-scale enterprise applications.

Smart Contract
Smart contract is software code that executes terms of an agreement, better known as a smart transaction or object that operates autonomously. Technically neither a contract nor very smart, the software code is a reliable way of making sure terms of an agreement are executed, monitored and completed without human intervention. Different distributed ledgers have versions of this – Hyperledger uses a concept called ChainCode and other DLs have their own version of a smart contract that are great for automating payments, moving title or ownership, and monitoring and ensuring terms are complied with.

Acknowledgments

Alasdair Blackwell

Alasdair is head of technology at Everledger. Everledger is a permanent, global, digital ledger that tracks and protects diamonds, fine art and other valuable items as they are traded over time. Using the technology database network behind Bitcoin, Everledger provides traders, insurance companies, financiers, consumers, claimants and law enforcers with an immutable history of an item's authenticity, existence and ownership.

In 2011 Alasdair co-founded Decoded with the goal of teaching the world to code. He helped oversee Decoded's growth, scaling the company to a team of over 100 people across London and New York, and up-skilling teams from Google, Talk Talk, British Gas, and the Cabinet Office (UK). He has also worked on The Good Jobs Campaign, developing technology-focused learning pathways for young people.

David Gorman

David has worked in IT for 28 years; he is currently part of the IBM CTO Europe team, specialising in blockchain, and is based at the IBM Hursley Laboratory in Hampshire. The team is the centre of blockchain client enablement worldwide for IBM.

David works with customers across a broad spectrum of industries, enabling their understanding of blockchain and of making best use of the technology within their respective industries.

Dave Treat

Dave is a managing director and the global head of Accenture's Capital Markets Blockchain practice.

He has 18 years of experience in financial services, split between consulting and industry roles, with the last decade being focused on capital markets. Dave has expertise in running strategy functions, innovation, strategic cost management, large-scale restructuring, customer relationship management, M&A, outsourcing and offshoring and process excellence.

Dr Garrick Hileman

Garrick is a senior research associate at the Cambridge Centre for Alternative Finance and a researcher at the Centre for Macroeconomics. He was recently ranked as one of the 100 most influential economists in the UK and Ireland and he is regularly asked to share his research and perspective with the FT, BBC, CNBC, WSJ, Sky News, and other media.

Garrick has been invited to present his research on monetary and financial innovation to government organisations, including central banks and military colleges, as well as private firms such as Visa, BlackRock, and UBS. Garrick has 20 years' private sector experience with both start-ups and established companies such as Visa, Lloyd's of London, Bank of America, The Home Depot, and Allianz.

Garrick's technology experience includes co-founding a San Francisco-based tech incubator, IT strategy consulting for multinationals, and founding MacroDigest, which employs a proprietary algorithm to cluster trending economic analysis and perspectives.

George Osborne

George is innovation director for the financial institutions business within Barclays' global transaction banking. He is charged with ensuring that the best of Barclays' innovation work is brought to bear for clients and works closely with the innovation functions across Barclays' businesses. He has been a mentor on the accelerator programme, and is leading on a number of areas in Barclays' positioning for new sectors within FinTech.

Previously he managed banking relationships in FinTech at Barclays, developing his interest in Strategic Innovation. Before joining Barclays he served as an British Army Officer in various roles, leading soldiers in the UK, Northern Ireland, Germany, Cyprus, Kenya and Iraq. He holds an Executive MBA from London Business School.

Greg Unsworth

Greg is PwC's Digital Business Leader, based in Singapore, and also leads the risk assurance practice. He has significant experience advising clients in the technology, media and telecommunications sectors on the impacts of technology, disruption and risk. Greg has broad overseas and regional experience, having been based previously in the London, Sydney and Tokyo offices. While in Tokyo, he was responsible for the coordination and provision of services for IBM throughout the Asia-Pacific region, as well as advising a number of leading Japanese and multi-national telcoms companies on a range of key business, risk and governance issues.

He has significant US GAAP and SEC reporting experience and has worked with both large and emerging media companies. He has also recently served as the technology and research and development working committee for the Singapore Government's 2025 Infocomm Media Masterplan.

Greg is a member of a number of PwC's global advisory and editorial committees involved in the development of our industry thought leadership around risk, digital disruption and emerging technology, and regularly works with global and regional industry networks and specialists.

Leon J. Perlman

Leon is a specialist consultant on digital financial services, emerging payments, mHealth, mAgriculture, big data, and cryptocurrencies, concentrating on commercial, technical and regulatory aspects of these ecosystems.

He is currently an affiliate research fellow at CITI at Columbia University Business School in New York, exploring the regulatory, disruptive and commercial aspects of DFS, emerging payments, big data, and the crypto-economy.

Dr Mathias Bucher

Mathias is the founder and CEO of Diamond Digital Inc., and of the consulting company Blockchain-Innovation.com. Diamond Digital is the company behind Diamond Coin, the first digital currency globally to be fully collateralised by high-grade diamonds.

He is the project Coordinator of 'OTC Swiss Blockchain', globally one of the first OTC clearing and settlement platforms on the blockchain that is currently being implemented by a large Swiss consortium.

Mathias holds a PhD in finance from the University of Zurich, and a Master in Economics from HEC Lausanne and Universidad Carlos III Madrid. He lectures on blockchain technology at the Lucerne University of Applied Sciences and Arts.

Professor Michael Mainelli FCCA FCSI FBCS

Michael co-founded Z/Yen, the City of London's leading commercial think-tank and venture firm, in 1994 to promote societal advance through better finance and technology. A qualified accountant, securities professional, computer specialist and management consultant, educated at Harvard University and Trinity College Dublin, Michael gained his PhD at London School of Economics where he was also a visiting professor.

He has led Z/Yen from creating mutual distributed ledgers (aka blockchain technology) through Taskforce 2000, the Financial Laboratory, Long Finance, the Global Financial Centres Index and the Global Intellectual Property Index.

Paul Warrunthorn Kittiwongsunthorn

Paul is the co-founder of OnePay and chief operating officer of TenX (its parent organisation). TenX is working on a cross-blockchain interoperability technology allowing any blockchain to send assets securely and instantly across blockchains. The network enables any blockchain to link to another, whether they are open-blockchains such as bitcoin or Ethereum or a bank's private blockchain, with near-zero cost.

Paul has a background in design thinking and innovation and has been trained at the Kyoto Institute of Technology and Stanford University. He is fascinated with the world of finance and technology, and views blockchain as the perfect intersection of these fields.

He is currently focused on making the future of money as free and easy as sending text messages; with the help of blockchain technology.

Dr Rajan Chadha

Rajan is director of IBN, where he patented a disruptive digital infrastructure that assists organisations to improve their processes for risk, audit and compliance, as well as facilitation of tools for accounting and reporting, and to manage supply chains automatically using blockchain technologies.

He has served in the United Nations, Barclays Bank/SWIFT (inter-banking community), BP, Thames Water, Ford, and the fuel and power industries, and attained a high level of expertise in strategic planning, executing complex projects, and bridging innovative technologies with business requirements. As a special adviser to Barclays Bank/SWIFT (UK, Brussels, US) he managed regulatory affairs, focusing on networks for digital banking and payments, including mobile payments.

He holds a doctorate in physics from Imperial College, London.

Robert (Bob) Hayward

Bob is a digital business leader, advising senior executives on technology innovation, trends and their impact, strategic opportunities, and driving transformation. In recent years, he has focused primarily on distributed ledgers/ blockchain, intelligent automation (robotic process automation (RPA), cognitive computing, machine learning), FinTech, RegTech, IoT, Smart City, cloud transition, platform/eco-system strategies, cloud transformation, digital operating models and other emerging technology-related strategic concepts.

Bob works closely with IT leaders in business to implement IT operation model change and with the challenges of IT governance, architecture, organisation, culture, skills, cyber-risk, vendor management and other challenges that make up the chief information officer's agenda.

He has worked as an entrepreneur (co-founder of Qualix, Omniscien Technology and inQbator); as a business leader within Asia Pacific (vice president of the region for Gartner, Candle Corporation and KPMG IT Services) and independent board member (AIIA, Strategic Publishing Group, NSW Government IT Advisory Board).

Roger Willis

Roger is the developer relations lead at R3, a financial innovation firm that leads a consortium partnership with over 75 of the world's leading financial institutions. R3 aims to design and deliver advanced distributed ledger technologies to the global financial markets.

As someone with formal computer science and accountancy training, Roger is interested in the applications of distributed ledger technology to automate audit and accounting. At R3, he supports developers using Corda, R3's distributed ledger platform.

He has previously worked at Ernst & Young in audit and data analytics, in bitcoin companies, as well as in his own start-up.

Dr Shantanu Godbole

Shantanu is a senior technical staff member at IBM Research and a member of the IBM Academy of Technology. He leads the newly launched IBM Center for Blockchain Innovation (ICBI) in Singapore. He has been with IBM Research for over 10 years and has worked in research and in development for global analytics offerings. He is currently interested in topics at the intersection of technology and business, such as blockchain and cognitive computing.

Shue Heng Yip

Shue Heng is director of services of the Sectoral Innovation Group within Infocomm Media Development Authority of Singapore (IMDA). In his current role, he has helped shape numerous trade finance innovation initiatives together with the banking industry and the regulator. One of the initiatives for an irrevocable distributable ledger, which he forged together with Standard Chartered Bank and DBS Bank, garnered the 2016 Global Finance award for product innovation and process innovation.

Before joining IMDA, he was the regional chief architect of Citi Transaction Services before assuming the role of regional technology head of channels, information, client delivery, liquidity management and the Innovation Lab at Citibank. Before Citibank, he spent 10 years with Microsoft, where he assumed various roles across technical consulting and solution sales.

As part of sectoral transformation within the services sector, Shue Heng plans to co-create new business models for implementation with industry partners in the accounting and legal sectors, leveraging technologies in distributed ledgers and cognitive computing.

Siân Jones

Siân is the founder of EDCAB European Digital Currency & Blockchain Technology Forum, an independent Brussels-based public policy platform. Siân heads COINsult, a regulatory compliance consultancy focusing on digital currencies and consensus-based technologies. She also heads EDCAB, where she helps EU policymakers and legislators shape sound policy and regulation relating to virtual currencies and distributed ledger technology.

Siân is a founder member of the UK Digital Currency Association and co-led its Regulation and Banking Group from 2014 to 2016. She is an ambassador for the Emerging Payments Association and also works with Credits, the first and only blockchain platform provider awarded a UK government G-Cloud framework agreement.

Dr Simon Rice

Simon is the group manager (technology) at the Information Commissioner's Office (ICO) in the UK government. The technology team advises on the technical aspects of complaints received and data breach investigations. They also monitor the technology environment to identify the developments that may have an impact on information rights.

Between 2005 and 2011, Simon was a database and software developer at the Health and Safety Laboratory, the principal source of scientific support for the Health and Safety Executive. Before joining the Health and Safety Laboratory, Simon studied for his PhD at the University of Manchester in the field of data mining. His research used a range of machine-learning techniques to extract information from large collections of numeric and textual data.

Sopnendu Mohanty

Sopnendu is chief FinTech officer at the Monetary Authority of Singapore. He is responsible for creating development strategies and regulatory policies for technology innovation to improve risk management, enhance efficiency and strengthen competitiveness in the financial sector.

Before joining MAS, Mohanty was global head of the Consumer Lab Network and Programs at Citibank, where he drove innovation programmes and managed innovation labs globally. He played a significant role as a subject matter expert in driving Citibank's global smart banking programme, to transform the bank's physical network to a digital first, smart and innovative, client-centric and highly effective customer engagement centre.

Mohanty is co-author of various patented works in area of retail distribution in the financial sector. He is based in Singapore, loves travelling, reads history and pursues culinary innovation as a hobby. He was in the Institutional Investor list of Fintech's Most Powerful Dealmakers of 2016.

William Gee

William is a partner in the Risk Assurance (RA) Practice at PricewaterhouseCoopers China. William is one of the partners responsible for FinTech in China, and is a member of the PwC Think-tank on Innovations and Disruptions, with responsibilities over innovations for RA at a national level.

He is a chartered accountant, and has over 30 years' experience in providing a wide range of assurance and advisory services relating to the assessment of, and response to, business and technology risks, as well as the design, review and enhancement of business and technology processes and controls.

PI-DISTRIBUTED-LEDGERS-BLOCKCHAIN

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / www.accaglobal.com