ICAEW THOUGHT LEADERSHIP
IT FACULTY

Blockchain and the future of accountancy

About the ICAEW IT Faculty

ICAEW's IT Faculty provides products and services to help its members make the best possible use of IT.

It represents chartered accountants' IT-related interests and expertise, contributes to IT-related public affairs and helps those in business to keep up to date with IT issues and developments. The faculty also works to further the study of the application of IT to business and accountancy, including the development of thought leadership and research. As an independent body, the IT Faculty is able to take a truly objective view and get past the hype surrounding IT, leading and shaping debate, challenging common assumptions and clarifying arguments. For more information about the IT Faculty please visit icaew.com/itfac

ISBN 978-1-78363-933-5

Executive summary

Blockchain is fundamentally an accounting technology. In this paper, we describe the technology and its likely impact on business, and in particular on the accounting profession.

Blockchain has the potential to increase the efficiency of the process of accounting for transactions and assets, operating as a system of universal entry bookkeeping. This would create certainty over rights and obligations and provenance, which in turn would empower the accountancy profession to expand its scope to record more types of activity than before, and to drill down closer to the economic reality underpinning the transactions recorded.

The key features of blockchain are that:

- new transactions originate with one user but **propagate** to a network of identical ledgers, without a central controller;
- all transactions and records are **permanent**, unable to be tampered with or removed; and
- many blockchains are **programmable**, allowing for automation of new transactions and controls via 'smart contracts'.

In this paper, we explain how the technology differs from the familiar, and how these features drive the potential applications of blockchain.

While there are undoubtedly some technological and legal challenges to solve before blockchain can be fully bedded into the financial recordkeeping systems of the world, the accountancy profession's unique combination of technical and business knowledge makes it particularly well-suited to helping design the environment and solutions that blockchain will rely on. Blockchain is a combination of an economically-incentivised business model and clever supporting technology; by working with blockchain specialists, accountants can help to form the standards that will drive blockchain forward.

While some detail on the operation of blockchain is included, this paper is intended to be suitable for any reader in the financial and business sector with an interest in technology. Glossaries of specialist terms are provided throughout, and for the curious, a brief technical explanation is provided in the appendix.

Introduction

Blockchain is a foundational change in how financial records are created, kept, and updated. Rather than having one single owner, blockchain records are distributed among all their users. The genius of the blockchain approach is in using a complex system of consensus and verification to ensure that, even with no central owner and with time lags between all the users, nevertheless a single, agreed-upon version of the truth propagates to all users as part of a permanent record. This creates a kind of 'universal entry bookkeeping', where a single entry is shared identically and permanently with every participant.

KEY FEATURES OF BLOCKCHAIN

Blockchain is unusual for a hyped tech trend in that it is a back-office solution to how to transfer ownership of assets and record data online – in other words, it is a platform for accounting and business to be done on, rather than a novel application or business model. The technical details of how blockchain works and what makes it proof against attack and theft are outside of the scope of this paper; however, a brief overview is provided after the main text.

We have summarised what we believe to be the most important facets of blockchain technology, into the 'Three Ps' – three key terms that explain what makes blockchain different from the more familiar ledgers of today, which are databases owned and run by a single party. The key features are as follows.

1. **Propagation:** There are many copies of a blockchain ledger, and no 'master' copy. All participants have access to a full copy of the ledger and all copies are identical and equivalent. No one party has control of the ledger. New transactions can be posted quickly and will propagate to all participants' copies.

2. **Permanence:** With each user having their own copy of the ledger, truth is determined by consensus. Past transactions cannot be edited without the consent of the majority, meaning that blockchain records are permanent. The entire ledger is stored by each participant and can be inspected and verified.

3. **Programmability:** Some blockchains allow for program code to be stored on them, as well as ledger entries – creating automatic journal entries that execute automatically when triggered. These are the so-called 'smart contracts'.

Whether blockchain is applicable in any particular business or sector will depend on if these qualities are desirable alternatives to present methods. Good blockchain applications centre on the cost and timing advantages of removing central parties from the system, and the increased security and certainty from having a system of consensus.

Blockchain is not a single technology, but rather a protocol – a way of doing things – for recording transactions. Unlike the internet, in which data is shared, in a blockchain ownership can be transferred from one party to another. Blockchain is a desirable model for several reasons. For example, in a market with many transacting parties, it could remove the need to reconcile disparate ledgers. Being distributed between all users also eliminates outages and removes the cost of having to pay a central authority to maintain the accuracy of the ledger. Any participant in the ledger can trace all previous transactions, allowing for increased transparency and the blockchain to 'self-audit'.

GLOSSARY

- A **distributed ledger system** is any system that spreads the ownership of a ledger across multiple parties, each with their own copy, instead of being held centrally.
- **Blockchain** is the most successful and common implementation of a distributed ledger system. Note that there are several meanings of the term 'blockchain'.
  - The lower-case term 'blockchain' is the generic name for the protocol – the agreed rules of how to transact – used to implement a distributed ledger in one particular way.
  - 'A blockchain' is a specific distributed ledger run in this way.
  - Confusingly, the blockchain that runs bitcoin (see below) is simply called 'the blockchain', as it is the original.
  - There is also a bitcoin services company that is called Blockchain.

  The term in this paper refers only to the first two definitions.
- **Bitcoin** is an online 'cryptocurrency' – a sort of digital cash – that uses blockchain technology to operate. Blockchain was first invented for bitcoin.

GLOSSARY

- The name blockchain is inherently descriptive of how the technology works – new transactions are gathered together into a **block** and added to a **chain** of all previous transactions, by a cryptographic process that is complex to perform, but which makes it easy to confirm that the history of all transactions is genuine.
- A **hash** is a sort of digital signature or summary of a block that is used to authenticate it and its place in the chain.
- Blockchain works through a process of **consensus** – all nodes will be able to identify the longest and most up-to-date ledger and agree on what it is.

The first two of the three key features – propagation and permanence – are intrinsic to blockchain and not optional; any potential application must desire (or at least be neutral to) these key qualities. For example, a permanent record makes some activities unsuitable for blockchain solutions, such as those involving the storage of unencrypted personal data. With each participant having access to the full ledger, other applications might be constrained if a concern over opening up commercially sensitive data exists. While data on a blockchain could be encrypted, a copy of that encrypted data would still be available to all participants.

Some other constraints of blockchain, which are discussed later in this paper, could be reduced or overcome with focused development, but these qualities are fundamental parts of how blockchain is built. Distributed ledger systems beyond blockchain might forgo or reduce these qualities, but this must be for a trade-off in security or other qualities.

THE IMPACT OF BLOCKCHAIN METHODS

Conceptually, blockchain is a move from a point where the trustworthiness of a ledger derives from the central controller that maintains it, to one where it is derived from trust in the system that drives the recordkeeping. Furthermore, the potential for self-executing smart contracts allows for a programmable ledger that could fundamentally alter how all contracts operate. Assuming that all the technological barriers could be overcome, blockchain has huge potential.

If we consider just the capabilities of blockchains without smart contract functionality, a full implementation could lead to disintermediation of a large part of the financial system. Private blockchains between groups that often transact with one another could replace central authorities such as banks, clearing-houses and lawyers. With the ability to directly interact, and with only one ledger that never requires reconciliation, businesses could save on both the costs of paying the ledger owner, as well as efforts spent reconciling with their counterparties. Removing uncertainty benefits the economy by streamlining it, facilitating greater confidence in decisions.

What's more, where appropriate a tax authority, regulator, or similar oversight body could be granted view-only access to such a blockchain, and would be able to observe and monitor transactions in real time. This kind of insight could lead to a reduction in costs and increases in the efficiency of regulatory and compliance activities. The permanent record of a blockchain reduces the chances for financial crime, thus making records more trustworthy.

THE ACCOUNTING PERSPECTIVE: THE POTENTIAL OF BLOCKCHAIN

Blockchain is an accounting technology. It is concerned with the transfer of ownership of assets, and maintaining a ledger of accurate financial information. The accounting profession is broadly concerned with the measurement and communication of financial information, and the analysis of said information. Much of the profession is concerned with ascertaining or measuring rights and obligations over property, or planning how to best allocate financial resources. For accountants, using blockchain provides clarity over ownership of assets and existence of obligations, and could dramatically improve efficiency.

Blockchain has the potential to enhance the accounting profession by reducing the costs of maintaining and reconciling ledgers, and providing absolute certainty over the ownership and history of assets.

Blockchain could help accountants gain clarity over the available resources and obligations of their organisations, and also free up resources to concentrate on planning and valuation, rather than recordkeeping.

Alongside other automation trends such as machine learning, blockchain will lead to more and more transactional-level accounting being done – but not by accountants. Instead, successful accountants will be those that work on assessing the real economic interpretation of blockchain records, marrying the record to economic reality and valuation. For example, blockchain might make the existence of a debtor certain, but its recoverable value and economic worth are still debateable. And an asset's ownership might be verifiable by blockchain records, but its condition, location and true worth will still need to be assured.

By eliminating reconciliations and providing certainty over transaction history, blockchain could also allow for increases in the scope of accounting, bringing more areas into consideration that are presently deemed too difficult or unreliable to measure, such as the value of the data that a company holds.

Blockchain is a replacement for bookkeeping and reconciliation work. This could threaten the work of accountants in those areas, while adding strength to those focused on providing value elsewhere. For example, in due diligence in mergers and acquisitions, distributed consensus over key figures allows more time to be spent on judgemental areas and advice, and an overall faster process.

Blockchains also allow for a greater degree of transparency than traditional ledgers. This is appealing in cases where corruption or misappropriation of assets are at risk. For example, aid spending could be provided in a blockchain-based asset; from there the end recipient of the funding could be readily identified.

Presently, transactions between companies lead to a sort of 'quadruple entry bookkeeping', where each company does their own double-entry, and in theory the two sets of entries are equal in value. This model could be substantially altered by blockchain. By lowering the walls around each company's internal accounting and making entries directly on the blockchain, the bookkeeping allows for the transaction to be recorded faithfully, verifiably and identically by each party. This might start as something for intra-group trading, but with time could grow to cross multiple entities, creating a kind of 'universal entry bookkeeping'.

Fundamentally, any kind of asset ledger will have to be designed around the limitations of privacy that a blockchain creates. While the data in each transaction can be encrypted, if the provenance or ownership of assets is at stake, then prior transactions must be public to verify this. Finding a way to balance the competing priorities of decentralisation, privacy, and security is a current area of research among blockchain specialists.

There are more areas still which blockchain could affect. When coupled to a robust digital ID system, an identity blockchain could store credentials for individuals, simplifying 'Know Your Client' and other identity processes by allowing organisations to share identification work. Similarly, a database of intellectual property rights could be distributed to simplify the process of identifying IP owners, requesting and paying for rights.

Blockchain case studies

GLOSSARY

- A **node** is a computer that is participating in a blockchain, by posting transactions and maintaining a copy of the ledger. Nodes may or may not be miners.
- A **miner** is a particular node that not only participates in the blockchain, but helps to keep it operating by running computations that allow new transactions to be verified and posted.
  - In bitcoin, miners are rewarded automatically with a transaction fee and with some newly-minted bitcoins. This is a very computation-intensive – and lucrative – business.
  - Other systems have been proposed for computing and maintaining new transactions that are more sustainable, cheaper, and more efficient, but none of them has yet risen to prominence.

Blockchain applications divide into several categories depending on the element of the technology that they are most focused on. Some applications are built around the automatic synchronicity of the ledger and the ability to simplify the reconciliation processed around these activities while also gaining additional transactional certainty. Others are more interested in the ability to remove middleman institutions from the system, reducing cost and bias while opening up access to more participants. And still others are interested in using blockchain as a platform to host smart contracts, automating and adding certainty to contractual arrangements and transactions.

A few case studies are illustrative in understanding how blockchain could form a part of a range of implementations.

BITCOIN – CRYPTOCURRENCY

Bitcoin is an online cash currency, which was created by an unknown person or persons under the pseudonym Satoshi Nakamoto. Posting their seminal white paper in late 2008 and launching the initial code in early 2009, Nakamoto created bitcoin to be a form of electronic cash that could be sent peer-to-peer without the need for a central bank or other authority to operate and maintain the ledger, much as how physical cash is used. While it wasn't the first online currency to be proposed, the bitcoin proposal solved several problems in the field and has been by far the most successful version, now accounting for a market capitalisation of around US$69bn in issued bitcoins, according to figures taken from coinmarketcap.com in September 2017.

The engine that runs the bitcoin ledger was named blockchain, a name which is now used to refer to all similar distributed ledger technologies. The original and largest blockchain is the one that still orchestrates bitcoin transactions today. Others run the several hundred 'altcoins' – other similar currency projects with different rules – as well as truly different applications such as Ethereum or Ripple. The system has several features that have caught the attention of investors and disruptors across the financial services systems and it is thought that blockchain, the underlying technology, has the potential to be a disruptive technology and perhaps grow to be a bedrock of the worldwide recordkeeping systems.

Bitcoin works by paying miners – those that do the computational legwork of posting new transactions – with newly-minted bitcoins. As long as the currency is desirable, it is self-sustaining. The system also automatically adjusts the difficulty of posting transactions and the reward for doing so in order to control inflation.

Blockchain leverages economic incentives originally designed for bitcoin. Only adding to the longest existing chain is rewarded, so that miners are incentivised to take on new transactions rather than forking off into differing subgroups. But standardisation is a challenge, as new updates to the bitcoin client are effective only when an overwhelming majority of participants agree to install them.

Bitcoin is attractive to users for several reasons:

- payer-borne transaction costs are low;
- the valuation of the currency has generally been growing strongly since its creation; and
- the system is much less restricted than traditional banking.

Bitcoin has no 'Know Your Client' or identity requirements – anyone with a working internet connection can join and start receiving and sending bitcoins. While this does make the system cheap and easy to access, it has also made it attractive to criminals in much the same way as paper cash, with the Silk Road 'dark net' black market site having mostly used bitcoin before being shut down by the FBI in October 2013.

As an internet-based currency, bitcoin also observes no international borders, meaning that transfer between territories is no different from any other payment. There are other blockchain projects that are looking to capitalise on this for international payments applications in central bank issued fiat currencies, such as Ripple.

R3 – INTERBANK RECONCILIATION

Blockchains are designed to be useful in systems that require reconciliation between parties. Many of the major players in banking are backing the R3 consortium, which is researching the use of a blockchain-like distributed ledger for interbank reconciliations and other financial applications. Currently, millions per year are spent reconciling ledgers between banks; however, if a distributed ledger solution could be created that is able to handle the volume of transactions between the banks, then this could be greatly reduced.

This kind of application would be a private ledger – one where only invited parties can view the records or participate in creating new entries. However, it would allow for interbank transactions to form a single, authoritative record that all parties could verify. This could reduce the considerable efforts currently spent reconciling books with counterparties, and allow for a more efficient banking system.

A solution of this kind is not feasible with the present implementations of blockchain, either in volume or in speed, and indeed the R3 project has now morphed into other distributed ledger applications for the financial sector. However, assuming that these significant challenges could be overcome, this is potentially a very impactful area of application for blockchain. Others are looking at supply chain integration for similar reasons.

THE ACCOUNTING PERSPECTIVE: IMPLICATIONS FOR AUDITORS

Blockchain has applications in external audit. Performing confirmations of a company's financial status would be less necessary if some or all of the transactions that underlie that status are visible on blockchains. This proposal would mean a profound change in the way that audits work.

A blockchain solution, when combined with appropriate data analytics, could help with the transactional level assertions involved in an audit, and the auditor's skills would be better spent considering higher-level questions.

For example, auditing is not just checking the detail of whom a transaction was between and the monetary amount, but also how it is recorded and classified. If a transaction credits cash, is this outflow due to cost of sales or expenses, or is it paying a creditor, or creating an asset?

These judgemental elements often require context that is not available to the general public, but instead require knowledge of the business, and with blockchain in place, the auditor will have more time to focus on these questions.

GLOSSARY

Some blockchains, such as Ethereum, can also contain executable computer code on them.

- A **smart contract** is code that is set to add certain transactions automatically upon certain trigger events taking place; it works something like a self-operating escrow account. The code that makes up the smart contract is examinable, so that the parties can confirm how it will operate ahead of time.

LAND REGISTRY

Perhaps the clearest case for where blockchain could be advantageous is provenance and transfer of ownership of assets, and land registry is a particularly good case. There have been several pilot studies and proofs-of-concept made, but none have reached full operational maturity as of yet. One proof-of-concept in this field was for land registry in Honduras, which has no current public land ownership registry and experiences difficulties with corruption and misappropriation; other projects have been proposed or developed in Georgia and Sweden, but none have yet reached large-scale testing. Creating a clear and permanent record of ownership and transfers of ownership would help create additional liquidity in the economy by increasing security, and fight corruption by distributing the maintenance of records to all parties rather than just to some.

As a public register, the open visibility of the blockchain is not an obstruction for land registry. It is acceptable for participants to see who owns, sells, and divides land; furthermore, the verifiability aspect can help to add transparency where needed.

A land registry blockchain would have to start by tokenising the land assets in question – that is, creating a representation of each section of land as a legally-equivalent digital asset, stored on the blockchain. This would be followed by making sure that the present owners had the ownership of the appropriate tokens assigned to them. This is no small undertaking as existing systems are already very complex, and there is a need to be flexible in future if existing land deeds are altered or split. What's more, if corruption in state officials is a concern, then getting approval from those same officials for a project that would reduce that corruption is challenging – and indeed this is what stalled the Honduras pilot scheme.

FURTHER READING

Distributed Ledger Technology – beyond the block chain

Government Office for Science. Available at http://bit.ly/1KoEw50 [accessed 19 September 2017]

An excellent introduction to the potential government applications of distributed ledger systems such as blockchain.

There is a larger lesson for blockchain in this example – bitcoin works because it is a wholly online system, with all participants agreeing to the ownership and provenance records of bitcoin due to how blockchain works. But many other areas are more complex – ownership still needs to be registered, but also be tied to the real world. This causes problems in both directions: the register must reliably reflect real-world existence and condition of assets, and there must also be legal mechanisms for enforcing ownership rights when blockchain records indicate these are held, even against parties who are not part of the blockchain, or do not recognise it as legitimate.

Assuming that these challenges could be overcome, then a land registry blockchain could thereafter record sales of land (or other similar transactions), creating a verifiable and permanent record. Furthermore, the distributed nature of the ledger would mean that neither downtime nor server failure would ever affect the availability of the service. While the costs of transacting on a blockchain can be relatively high, for a low-volume, high-value channel such as purchases and sales of land, they would likely be competitive.

SMART CONTRACTS

There are already many examples of automated contracts in place in the present-day financial system – from the mechanical simplicity of a vending machine, to a bank-operated standing order or direct debit. The idea of a smart contract is to allow for all kinds of transactions to be made automatically and simply, in the same way as a vending machine purchase – and without the need to rely on (or pay) a central party to adjudicate the operation of the contract terms.

Blockchain technology offers opportunities in this arena, because smart contract code can be written directly onto a blockchain and is examinable by the contracting parties ahead of time, just like a traditional legal contract. If it is agreed to, then the smart contract – armed with appropriate rights – will automatically execute its own terms. This could mean releasing a payment following a certain trigger, running a software escrow account, making an investment, or anything else.

Other than disintermediation, one potential advantage of smart contracts over traditional law is that they reduce counterparty risk. With a traditional legal contract, the courts act as a cure to breach – if the contract is broken, they can enforce the terms after the fact. However, smart contracts can be preventative – they operate on the stated terms regardless, which binds its parties without the ability to choose to default. What's more, smart contracts are unambiguous – the contract will carry out the one and only meaning of its code.

To reach this world of smart contracts, there are some challenges that must first be resolved. While the process of executing a smart contract might be disintermediated, there may still be a need for a trusted professional – in this case, a programmer to create the smart contract. If institutional trust (and cost) moves from the lawyers drawing up the contract to the programmers encoding it, there is no real advantage to be gained.

There are some projects out there, such as Legalese, which are seeking to build a computer language for legal contracts that can easily be translated into natural language. However, we are currently a fair way away from this reality. Courts would have to recognise that the operations of smart contracts are legitimate ways to transfer ownership and value between parties, and that the terms of smart contracts are enforceable in case a breach somehow does occur. What's more, an answer would have to be found to the question: What redress is available if the smart contract is exploited in a way not expected by one of the parties? Could intent override the letter of the code?

This last issue is not theoretical – when the DAO (a smart contract-driven investment vehicle created for the Ethereum blockchain) had much of its funding hijacked through a loophole in a poorly-written smart contract, there was a fierce debate over how to resolve the issue that eventually lead to a fork, with most participants agreeing to roll back the loss of funds. But some kept the status quo and became a separate blockchain, which now exists under the name Ethereum Classic. This rollback was only possible because more than half of the participants agreed to implement it.

FURTHER READING

Smart Contract Templates: foundations, design landscape and research directions

Christopher D. Clack, Vikram A. Bakshi, Lee Braine. Available at http://bit.ly/2yrgEQ8 [accessed 19 September 2017]

Highly technical paper, but a good covering of possible directions for integrating smart contracts with legal systems.

Constraints and challenges

FURTHER READING

Avoiding the pointless blockchain project

Multichain. Available at http://bit.ly/2gdRJHn [accessed 19 September 2017]

Detailed and technical explanation of when blockchain is or is not appropriate.

GLOSSARY

- An **unpermissioned** ledger is one that allows anyone at all to view or add transactions (bitcoin is one example).
- A **permissioned** ledger is one that has some rules about which parties can add transactions, but may still be open to public examination.
- A **private** ledger is a permissioned ledger shared only between certain nodes by invitation, and in many ways is simply a shared database with a multiplicity of copies instead of a single one.
- These terms affect how **centralised** the ledger is – to what extent control of the ledger is held by a central party or small group, versus being an open standard.

There are some key guidelines for assessing whether a particular project should use blockchain. Virtually any activity that would otherwise run on a database could be on a blockchain platform, but whether this is actually beneficial will depend on the circumstances. Many proposed blockchain applications could use a shared traditional database hosted by a trusted central party and would provide nearly identical results.

A problem where blockchain might be an appropriate solution is one that has:

- a number of participants who don't have institutional trust in one another;
- a desire to work without an intermediary (either because of cost or because one isn't available); and
- a need for a complete definitive log of transactions.

With present technology, there are some barriers to blockchain becoming a central element of the financial system. Taking bitcoin, as the most developed and widespread example, here are some key statistics, based on calculations and information taken from blockchain.info in September 2017.

1. The fee per transaction posted has historically averaged US$5 to US$8 (currently over US$40 due to the strong BTC); most of this cost is met with new bitcoins and not passed on to those transacting.
2. Latency – the time between a transaction being initiated and officially recorded – averages at four to five minutes but can be considerably more in times of peak demand.
3. The maximum capacity for transactions is around seven transactions per second for the smallest possible transactions, or around three transactions per second for the average actual transaction size (compared to thousands or tens of thousands of transactions per second for Visa).

These qualities derive from the way that bitcoin is designed and how blockchain works. Much of the work involved in Nakamoto's design of blockchain was in setting up economic incentives to make the system self-sustaining without a central manager or organisation to run it. The design of the system requires enormous computing power to verify the transactions made: in total several hundred times the world's top supercomputers' power across the network. For the moment, that means that the system relies on minting new bitcoins as the primary way of rewarding those that contribute computing resources to the network, and can handle only so much throughput.

Additionally, blockchain requires each participant to be furnished with a full copy of the ledger to operate. If the ledger is commercially sensitive, this would require the data to be encrypted. Furthermore, for a large or active ledger, there could be a barrier for new participants, who would need to download very large historic data files before being able to join in.

While these statistics for bitcoin are currently nowhere approaching the levels needed to compete as a major player in the payments sector, many of these are held back by the fact that bitcoin allows transactions from anyone and hence requires additional security. Private blockchains between trusted collaborators could forgo this security and consequently run more efficiently.

HOW COULD BLOCKCHAIN OVERCOME THE BARRIERS?

The answer is two-fold. First, the more immediate applications will be in areas where these figures are better than existing alternatives, and blockchain can be of use in its current state. Second, the transformational applications of blockchain to areas such as payments or inter-bank reconciliation, will come only after R&D and innovation are applied to reach a point where the technology's limitations have been greatly reduced.

While bitcoin's key metrics compare unfavourably with payment architecture such as Visa, it is ahead of the game in some fields. For example, clearing and settlement in capital markets takes days and the costs are high. The suggestion above to use blockchain for land registry is common because transactions are relatively infrequent and in a situation where higher fees would be acceptable. Likewise, blockchain company Everledger has created a digital asset register for diamond trading, using a large collection of physical and chemical measurements to uniquely identify stones and track their provenance and ownership. Everledger also benefits from having a restricted base of users, with identity requirements to join, meaning that less verification needs to occur within the actual system.

It is worth noting that the latency aspect – the time between transactions – cannot be improved without knock-on effects. A problem with distributed ledger systems such as blockchain is making sure that all the participants remain synchronised, even when communications take time to reach each participant; this is important to prevent the ledgers falling out of synch with one another and opening the door to double-spending the same resource. Blockchain solves this by gathering new transactions together into blocks and posting them at once, roughly every 10 minutes in the case of bitcoin. Shorter time delays can be done (Ethereum uses a ~17 second delay, for example), but this means that mining is less cost-efficient and the short-term potential for differences or abuse is higher. While other alternative methods have been proposed, there is no simple solution to decrease block times.

FURTHER READING

The Distributed Ledger Technology Applied to Securities Markets

European Securities and Markets Authority. Available at http://bit.ly/1srBHgZ [Accessed 19 September 2017]

Provides a balanced assessment of the possibility of implementing blockchain solutions in clearing and settlement and other securities applications, alongside the risks and constraints.

THE ACCOUNTING PERSPECTIVE: HOW THE PROFESSION CAN LEAD

The move to a financial system with a significant blockchain element offers many opportunities for the accountancy profession. Accountants are seen as experts in record keeping, application of complex rules, business logic and standards setting. They have the opportunity to guide and influence how blockchain is embedded and used in the future, and to develop blockchain-led solutions and services.

To become truly an integral part of the financial system, blockchain must be developed, standardised and optimised. This process is likely to take many years – it has already been nine years since bitcoin began operating and there is much work still to be done. There are many blockchain applications and start-ups in this field, but there are very few that are beyond the proof of concept or pilot study stage. Accountants are already participating in the research, but there is more for the profession to do. Crafting regulation and standards to cover blockchain will be no small challenge, and leading accountancy firms and bodies can bring their expertise to that work.

Accountants can also work as advisers to companies considering joining blockchains themselves, providing advice on weighing the costs and advantages of the new system. Accountants' mix of business and financial nous will position them as key advisers to companies approaching these new technologies looking for opportunity.

FURTHER READING

The Future of Blockchain: Applications and Implications of Distributed Ledger Technology

CA ANZ and Deloitte Access Technologies. Available at http://bit.ly/2gJAQ87 [Accessed 19 September 2017]

Good discussion of how blockchain and accounting might interact; also has a useful list of blockchain companies and projects.

A final area of challenge is getting an appropriate legal framework into place. An entry created on a blockchain ledger has to gain full legal recognition as a proper transfer of value between parties, with courts having the ability to enforce this if appropriate. With no central location, it is unclear which jurisdiction(s) even would have to rule on such matters. The legalisation of blockchain is a substantial challenge. It is unlikely that specific legislation will be written for blockchain while there are so many competing approaches and standards in the marketplace. Standardisation on both the technological elements of blockchain and the use standards for areas such as asset ownership and transfer will need significant development. Only after this can the legal problem be truly tackled.

Legal recognition will also have to deal with smart contracts, which differ significantly from the form of traditional legal contracts. Not only do smart contracts self-execute, they are autonomous, and thus restrict the control that parties have once the contract is initiated. This could be particularly difficult if a smart contract does not operate as a party in good faith believed it would. There are also issues with recourse – due to the records propagating across many users, it could be impossible to enact a court's judgment to remove a transaction or take down data stored on a blockchain.

THE ACCOUNTING PERSPECTIVE: SKILLS FOR THE FUTURE

The parts of accounting concerned with transactional assurance and carrying out transfer of property rights will be transformed by blockchain and smart contract approaches.

The reduction in the need for reconciliation and dispute management, combined with the increased certainty around rights and obligations, will allow greater focus on how to account for and consider the transactions, and enable an expansion in what areas can be accounted for. Many current-day accounting department processes can be optimised through blockchain and other modern technologies, such as data analytics or machine learning; this will increase the efficiency and value of the accounting function.

As a result of the above, the spectrum of skills represented in accounting will change. Some work such as reconciliations and provenance assurance will be reduced or eliminated, while other areas such as technology, advisory, and other value-adding activities will expand.

To properly audit a company with significant blockchain-based transactions, the focus of the auditor will shift. There is little need to confirm the accuracy or existence of blockchain transactions with external sources, but there is still plenty of attention to pay to how those transactions are recorded and recognised in the financial statements, and how judgemental elements such as valuations are decided. In the long term, more and more records could move onto blockchains, and auditors and regulators with access would be able to check transactions in real time and with certainty over the provenance of those transactions.

Accountants will not need to be engineers with detailed knowledge of how blockchain works. But they will need to know how to advise on blockchain adoption and consider the impact of blockchain on their businesses and clients. They also need to be able to act as the bridge, having informed conversations with both technologists and business stakeholders. Accountants' skills will need to expand to include an understanding of the principle features and functions of blockchain – for example, blockchain already appears on the syllabus for ICAEW's ACA qualification.

Ultimately, blockchain is likely to be a foundational technology. It will take years – perhaps even decades – for it to be fully developed, standardised and embedded in the architecture of the internet and the financial system. It will also need to work quicker, more efficiently and have lower operating costs. But the rewards are trustworthy records and reduced reconciliations. So we can expect that if not blockchain, then some implementation of distributed ledger systems will emerge as a key business technology. Accounting will be more efficient due to the increased trust in the information available and the reduced time spent in reconciling and disputing records with other parties. This will lead to greater focus on the ultimate aims of accountancy – interpreting the economic meaning of transactions, and providing information to support better decisions.

Appendix: How blockchain works

A detailed operational understanding of blockchain is not necessary to follow the work in this paper, but an overview is provided here.

Each participant in a blockchain (each node) keeps a copy of all the historical transactions that have been added to the ledger, and by comparing to the other nodes' copies, each is kept synchronised through a consensus process. Unlike in a traditional ledger system, there is no node with special rights to edit or delete transactions – in fact there is no central party at all, which is one of the reasons that blockchains can be useful when a trusted central party is either unavailable or too expensive.

The idea of having a ledger that propagates to all its participants has been around for some time, but there were some serious barriers to overcome. The most important of these was the ordering of transactions and the 'double spend problem'. In a large network, transactions are broadcast constantly from different nodes, and those transactions will take varying amounts of time to reach different points of the network. Hence, it is difficult to have a definitive order of transactions – especially important if two transactions attempt to credit the same resource, leading to double-spending and two parties disagreeing on who has the right to a given asset.

Blockchain solves this problem by having newly broadcast transactions go, not directly onto the ledger, but into a holding space. These transactions are periodically bundled together into a block, which is then officially considered to have posted with a simultaneous timestamp, thereby **propagating** the transaction to all users. In order to prevent blocks from clashing, and to avoid the need for a central authority to do the block-making process, blockchains use various methods to impede the process of making ('mining') new blocks. The process for bitcoin, for example, automatically adjusts the difficulty of the process (which involves complex mathematics), so that on average a new block is formed every 10 minutes. Different nodes compete to solve these mathematical problems, so no central party controls the process. Successful mining is rewarded with new bitcoins and a transaction fee. A system that only included trusted parties of known identity can simplify this by reducing the amount of verification that is needed for each transaction.

So that's the 'block' part covered – what about the chain? Well, new blocks don't just contain the list of approved transactions, they also contain the timestamp of the block, and the hash – a unique cryptographic signature – of the previous block. Because the block references the immediately preceding block, its order in the chain is unambiguous. What's more, an attempt to change a previous block would be immediately obvious, as the hash signature would change and no longer match the backward reference in the following block. Consequently, changing something in a blockchain after the fact is not viable and blockchain records are **permanent**.

Some blockchains are set up to contain, not only details of transactions and ownership, but also executable programming code. Parties can agree to add code to a blockchain in the form of a smart contract, that is, code that will carry out agreed transactions when triggered. This allows for automation of new transactions, and allows some blockchains to be **programmable**.

There are over 1.7m chartered accountants and students around the world – talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 150,000 of these are ICAEW Chartered Accountants. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

ICAEW
Information Technology Faculty
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA
UK

T +44 (0)20 7920 8481
E itfac@icaew.com
icaew.com/itfac

Chartered Accountants Worldwide
Member

GAA
Global Accounting Alliance