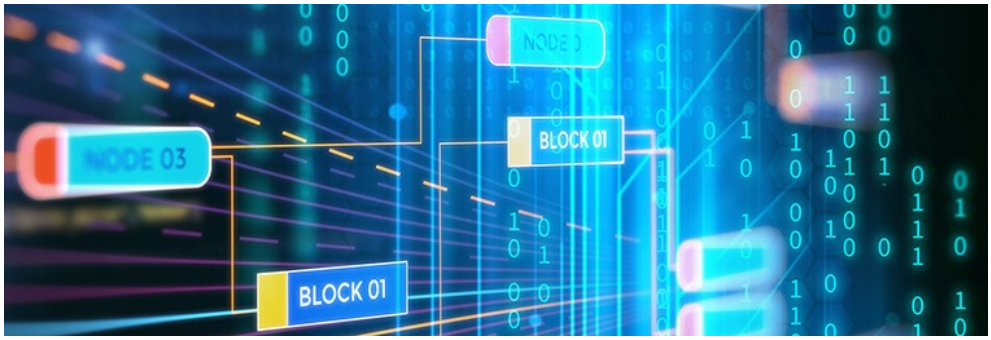
Blockchain: background, challenges and legal issues



Share this

2 FEB 2018

By: John McKinlay | Duncan Pithouse | John McGonagle | Jessica Sanders (née Turner)

Blockchain and distributed ledger technology offers significant and scalable processing power, high accuracy rates, and apparently unbreakable security at a significantly reduced cost compared to the traditional systems the technology could replace, such as settlement, trading or accounting systems. Like all new technology however, it poses challenges for suppliers and customers. So what are the key issues in relation to blockchain and distributed ledger technology?

Background

In its simplest form, blockchain is a decentralised technology or distributed ledger on which transactions are anonymously recorded. This means the transaction ledger is maintained simultaneously across a network of unrelated computers or servers called "nodes", like a spreadsheet that is duplicated thousands of times across a network of computers. The ledger contains a continuous and complete record (the chain) of all transactions performed which are grouped into blocks: a block is only added to the chain if the nodes, which are members in the blockchain network with high levels of computing power, reach consensus on the next 'valid' block to be added to the chain. A transaction can only be verified and form part of a candidate block if all the nodes on the network confirm that the transaction is valid. And in order to determine the validity of a candidate block, "miner" nodes compete to solve a highly complex algorithm to verify it (on the Bitcoin Blockchain this is known as the 'Proof of Work'). The first node to solve the algorithm and validate the block should be rewarded – on the Bitcoin Blockchain this reward takes the form of Bitcoins and this is referred to as "mining for Bitcoins." Please see the diagram on page 6 for further detail of this process.

A block generally contains four pieces of information: the 'hash' of the previous block, a summary of the included transaction, a time stamp, and the Proof of Work that went into creating the secure block. Once information is entered on the blockchain, it is extremely difficult to alter: a blockchain network lacks a centralised point of vulnerability for hackers to exploit and each block includes the previous block's 'hash' so any attempts to alter any transaction with the blockchain are easily detectable.

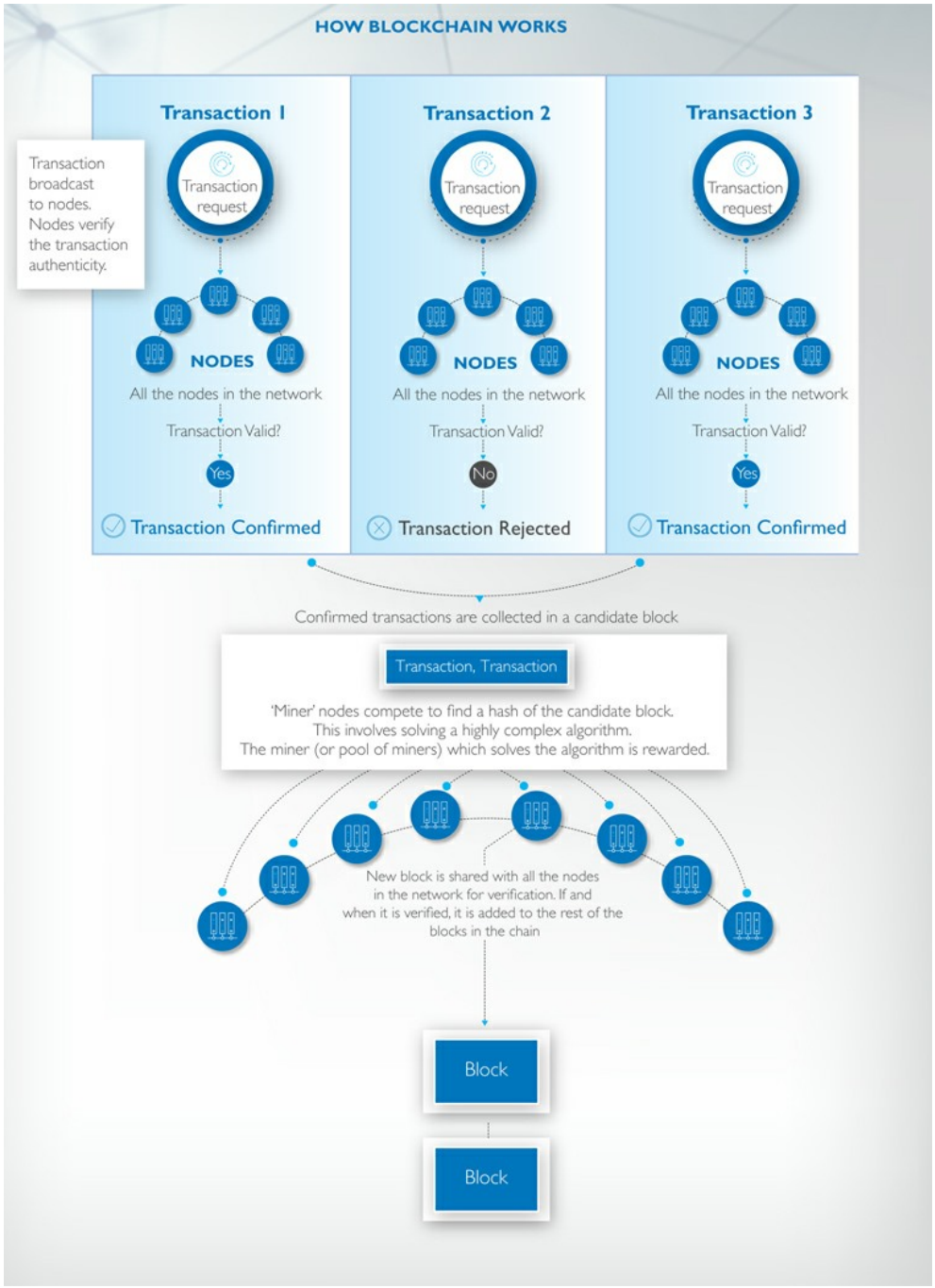
In other words, blockchain is a self-maintaining database which typically has a "functionality wrapper", or app development platform, on top. Blockchain can be thought of as an operating systems for which useful applications or "smart contracts" can be written. Assets and information about transactions can be stored and tracked without the involvement of a typical intermediary, such as a bank, or a central authority or some other trusted third party.

A blockchain network may be public and open (permissionless) like the internet or structured within a private group like an intranet (permissioned). The blockchains that have captured the imaginations of many financial institutions are known as "private" or "permissioned" blockchains because only certain preapproved participants may join them. These blockchains use a variety of means to ensure the identity of parties to a transaction and to achieve consensus as to the validity of transactions. The entities creating the "private" blockchain agree on rules that govern how entries are recorded and under what circumstances they can be modified. Only specific authorised participants are given access and are known within the network.

RELATED SERVICES
Intellectual Property and Technology

RELATED SECTORS
Technology

RELATED SITES
Technology's Legal Edge



Challenges

Security comes (only) with simplicity

One of the key attributes of blockchain is that it is said to be virtually unhackable due to the complex cryptography and the distributed nature of the ledger: it is understood that a hacker intent on corruption or malpractice would need more computing power than at least half the nodes in the blockchain. This is in stark contrast to the weakness of so many existing highly centralised systems with a single point of failure.

However, as soon as additional coding complexity is added to meet later specific requirements, this can introduce vulnerabilities to the blockchain and so reduce the effectiveness of the ledger's security.

As a consequence, in order to avoid defeating the very purpose and attraction of the blockchain, customers may need to resist the temptation to require bespoke developments and modifications (or at least understand the potential consequences of doing so), whilst vendors will be required to design both the solution, and any necessary back-up protocols, to avoid introducing security vulnerabilities in the first place and to provide safeguards in the event this is not completely successful.

Performance challenges

Blockchain databases grow rapidly in size as new transactions are written, and there is a concern that the size of database required, and the consequent speed of access, may make it unsuitable for certain forms of transactions where speed is of the essence. In this regard, the scalability and resilience of a blockchain solution is clearly of the utmost criticality, particularly where the service is used as part of a financial institution's ability to fulfil trading obligations, customer interactions or regulatory requirements.

Early adoption

At the moment, many blockchain solutions are in a development or low adoption phase and, as a consequence, the technology and policies offered are relatively untrusted. Many organisations will therefore be uncertain of using services in relation to business critical activities without a high degree of confidence in the quality and stability of services it will receive. Vendors will need to be prepared to provide a level of protection to customers via not just the solution but the contractual terms themselves. In this regard, we suspect that, in the same way that cloud providers have had to, Vendors will need to make concessions to accommodate regulated customers. The extent of such movement will depend, as ever, on finding an appropriate balance of risk for the parties. Given blockchain in its purest form is predicated on multiple users contributing to the chain, so the on-going success and viability of blockchain as a market initiative will depend on the confidence placed in it by the various market users.

Legal Issues

Jurisdiction

Blockchain has the ability to cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues which require careful consideration in relation to the relevant contractual relationships.

The principles of contract and title differ across jurisdictions and therefore identifying the appropriate governing law is essential. In a conventional banking transaction, for example, if the bank is at fault then irrespective of the transacting mechanism or location, the bank can be sued and the applicable jurisdiction will most likely be contractually governed. However, in a decentralised environment, it may be difficult to identify the appropriate set of rules to apply.

At its simplest level, every transaction could potentially fall under the jurisdiction(s) of the location of each and every node in the network. Clearly, this could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes. In the event a fraudulent or erroneous transaction is made, pinpointing its location within the blockchain could be challenging.

The inclusion of an exclusive governing law and jurisdiction clause is therefore essential and should ensure that a customer has legal certainty as to the law to be applied to determine the rights and obligations of the parties to the agreement and which courts will handle any disputes.

Service levels and performance

The willingness of vendors to commit to performance assurances is likely to depend on three considerations: (i) their risk/reward profile; (ii) the service delivery model and (iii) the "multiplication factor" of accepting significant liability for multiple customers – on a "one to many" approach – at the same time. This is likely to mean vendors preferring to offer the technology and service on an almost "as is" basis, with a limited availability service level, and excluding warranties regarding performance of the services, leaving customers without any assurance that the technology will function as described or the service be reliable and available. However for users who are utilising the service as part of their business, this is unlikely to be an acceptable proposal. The balance of performance risk will therefore be a key issue.

Liability

The risk to customers of a systemic issue with trading related infrastructure such as blockchain could be material if trades are not settled or are settled incorrectly. Likewise the risk relating to security and confidentiality will be towards the top of the risk issues of any prospective customer.

Blockchain poses different risks as a consequence of the technology and manner of operations: one of the main issues affecting public blockchain is the inability to control and stop its functioning. In case of a private blockchain, the lack of control on the functioning of the platform does not apply but whether or not this would be sufficient to trigger a liability of the company managing the platform has not yet been tested.

So the allocation and attribution of risk and liability in relation to a malfunctioning blockchain service must be thought through carefully, not just at the vendorcustomer level, but as between all relevant participants, in particular the parties (perhaps counter-parties for a trade) affected by the issues.

Intellectual property

There is inevitably value in the blockchain, and ownership of the IP in it will likely form an important consideration albeit that the limitations on the patentability of software and business processes (in the UK at least will erode some of the relevant issues). However, given the amount of investment and the potential financial returns of blockchain technology, blockchain vendors will have to determine their IP strategy: vendors will likely want to capitalize on any other commercial benefits to be generated from the Blockchain, including commercialization of the underlying data set. To the extent the data set relates to the users, this is likely to be a carefully negotiated area.

Likewise, what of specific developments or solutions which overlay the core, developed to meet a customer's specific requirements? Possible IP options are no different to any other software development agreement and are likely to hinge on whether those specific requirements could give a customer a

competitive edge and/or can be used by the blockchain vendor with another customer or by the customer with another blockchain vendor. Depending on the answer to these questions, a customer may insist on ownership of such developments, may be willing to 'merely' license them for the term of the agreement (or perpetually if usable with other networks) or restrict the vendor's ability to use such developments in some way, whether time, use or recipient based or a combination of all three.

An "open innovation" approach is prevalent throughout fintech. Financial organisations are working towards a viable blockchain proof of concept and are developing a lot of code in-house. Traditionally financial organisations have expected to own the IP in any software that they develop. However there appears to be a realisation that technology will have to be shared in order for value to be gained.

Data privacy

As one of the key USPs of the blockchain is that once data is stored it cannot be altered (at least, not easily), this clearly has implications for data privacy, particularly where the relevant data is personal data or metadata sufficient to reveal someone's personal details. Equally the unique transparency of transactions on the blockchain is not easily compatible with the privacy needs of the banking sector: the use of crypto-addresses for identity is problematic as no bank likes providing its competitors with precise information about its transactions and the banking secrecy must be kept by law.

In order to prevent this becoming a barrier to take-up, technology-based solutions will need to be found to design privacy-protecting blockchains. This might include limiting who can join the blockchain network to "trusted" nodes and encrypting the data on the blockchain, although this is not without its challenges, and it remains to be seen how vendors, particularly those targeting the financial services industry, tackle the balance of privacy versus transparency.

Decentralised Autonomous Organisations (dAOs)

DAOs are essentially online, digital entities that operate through the implementation of pre-coded rules. These entities often need minimal to zero input into their operation and they are used to execute smart contracts, recording activity on the blockchain.

Modern legal systems are designed to allow organisations, as well as actual people, to participate. Most legal systems do this by giving organisations some of the legal powers that real people have – e.g. the power to enter into legal contracts, to sue, and to be sued. But what legal status will attach to a DAO? Are they simple corporations, partnerships, legal entities, legal contracts or something else?

Since the DAOs "management" is conducted automatically, legal systems would have to decide who is responsible if laws are broken. What, if, any, is the liability of DAOs and their creators? Who or what is claimed against in the case of a legal dispute?

Courts and regulators are unlikely to allow the wholesale adoption of technology which bypasses established oversight.

The enforceability of smart contracts

Blockchain makes possible the use of so-called "smart contracts". Smart contracts are blockchain based contracts which are automatically executed upon certain specified criteria coded into the contract being met. Execution over the blockchain network eliminates the need for intermediary parties to confirm the transaction, leading to self-executing contractual provisions. In addition to the cost and efficiency gains it is hoped this will achieve, this also raises significant legal questions in relation to applicable regulation, leaving a sense of uncertainty as to the legal enforceability of smart contracts.

Since smart contracts are prewritten computer codes, their use may present enforceability questions if attempting to analyse them within the traditional 'contract' definition. This is particularly true where smart contracts are built on permissionless blockchains, which do not allow for a central controlling authority. Since the point of such blockchains is to decentralize authority, they might not provision for an arbitrator to resolve any disputes that arise over a contract that is executed automatically. It remains unclear whether the elements of capacity, including the ability to rely on apparent or ostensible authority would apply and the questions of offer and acceptance, certainty and consideration would also need to be considered. However, there have been advances in many countries regarding the level of acceptability of electronic contracts so it is realistic to hope this is carried over to smart contracts. In the meantime, customers should ensure that smart contracts include a dispute resolution provision to reduce uncertainty and provide for a mechanism in the event of a dispute.

Compliance with financial services regulation

Many sourcing arrangements, including the use of certain technology solutions, require regulated entities to include in the relevant contracts a series of provisions enabling them to exert control, and seek to achieve operational continuity in relation to the services to which the contracts relate. With blockchain (as has been the case with cloud and certain FinTech agreements) this may well be more of a challenge. The contracts and overall arrangement will need to be carefully reviewed to ensure compliance, as required. For in-depth analysis of the current state of the regulatory landscape, please see our publication "The Blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies."

Exit

The need for exit assistance will be determined in large part by the specific solution and the extent to which the blockchain vendor holds the customer's data. If the customer does not have its own copy of the data, it will require data migration assistance to ensure the vendor is obliged to hand over all such data on expiry or termination of the agreement and a complete record of all transactions stored on the blockchain.

Is data on a blockchain "property"?

At common law as a general principle there is no property right in information itself, but that while individual items of information do not attract property rights, compilations of data – for example in a database – may be protected by intellectual property rights. Where a database of personal information is sold, if a buyer wants to use the personal information for a new purpose, in order to comply with the Data Protection Act they will have to get consent for this from the individuals concerned.

Due diligence on blockchain

Public companies and private investors have already begun to make significant capital investments in blockchain technology startups. This trend is likely to accelerate as commercial deployments of blockchain technology become a reality. Transactional lawyers who are tasked with performing due diligence on the buy and/or sell side in connection with these investments need to understand blockchain technology and the emerging business models based on the technology. Traditional due diligence approaches may need to be adapted. For example, there will be unique issues concerning ownership of data residing on decentralised ledgers and intellectual property ownership of blockchain-as-a-service offerings operating on open source blockchain technology platforms. These issues will need to be considered in the context of the business value proposition and competitive barriers to entry.

Conclusion

Blockchain does have the potential to become an integral part of the operation of many businesses, offering scalability, security and computing power at a lower CAPEX and OPEX. But, of course, as is the case with most new technology service offerings, there are a number of risk based issues that need to be carefully considered before business, particularly heavily-regulated ones, can start to fully realise the potential benefit.

If you would like to discuss the issues arising out of this publication, please get in touch with your usual DLA Piper contact, or email Jessica Sanders or John D. McGonagle (Senior Associates in DLA Piper's UK Intellectual Property and Technology practice).

DOWNLOADS

Read the article as a pdf

AUTHORS

Jessica Sanders (née Turner)
Senior Associate

London
T: +44 20 7153 7699
Email Jessica
Full biography

Duncan Pithouse
Partner

London
T: +44 (0)20 7153 7264
Email Duncan
Full biography

John McKinlay
Partner

Edinburgh
T: +44 (0)131 242 5593
Email John
Full biography