

Financial institutions  
Energy  
Infrastructure, mining and commodities  
Transport  
Technology and innovation  
Life sciences and healthcare


---

 NORTON ROSE FULBRIGHT

# Unlocking the blockchain

A global legal and regulatory guide

Chapter 1: An introduction to blockchain technologies





## Contents

Overview	04
<b>An introduction to blockchain technologies</b>	<b>05</b>
Why do businesses need to understand blockchain technologies?	06
When are blockchain technologies likely to deliver significant value?	08
Which industry sectors might be affected?	09
What blockchain applications could be deployed horizontally across industry sectors?	15
What is a blockchain?	17
What are the component parts of a blockchain?	18
What is the difference between a permissioned and a permissionless blockchain?	19
How does a typical blockchain transaction work?	21
How does blockchain cryptography work?	22
What are the main performance characteristics that define blockchain technologies?	23
What is the current state of the vendor and investment market and likely adoption timelines?	24
Are there obstacles to widespread adoption?	25
What are the key legal and regulatory issues?	31
What are the implications for business?	36
Glossary	37
Contacts	40
Global resources	42

# Overview

Interest in blockchain technologies has grown dramatically over the last twelve months. This has triggered growth in investment in businesses operating in this area and marked engagement from all industry sectors (and financial institutions in particular) in blockchain technologies and their disruptive potential. Such engagement has led to the development of increasingly sophisticated proof-of-concept use cases and notable live deployments.

Against this backdrop, a number of regulators have been focusing on the benefits, challenges and risks posed by blockchain technologies and how blockchains might operate within the existing regulatory framework. Any proposed deployment will need to take into account such regulatory considerations and a range of other legal issues. In view of this, Norton Rose Fulbright's global blockchain and distributed ledgers practice group has produced a global legal and regulatory guide to blockchain technologies.

This guide will be published in a series of chapters, covering the following topics and use cases:

Topics	Use cases
an introduction to blockchain technologies	clearing and settlement
the regulatory considerations	securitisation and trade receivables finance
the IP and IT issues	identity (including data privacy issues)
litigation and dispute resolution considerations	insurance
competition/anti-trust issues	supply chain management
tax considerations	DAOs (decentralised autonomous organisations)

We hope that you will find this first chapter on 'an introduction to blockchain technologies' insightful and would welcome the opportunity to discuss any aspect of it with you in greater detail.

If you would like to register to receive the subsequent chapters, please contact [julie.frizzarin@nortonrosefulbright.com](mailto:julie.frizzarin@nortonrosefulbright.com).

**Sean Murphy**

**Global head of blockchain and distributed ledgers**

Norton Rose Fulbright LLP

July 2016

# Chapter 1:

## An introduction to blockchain technologies

## Why do businesses need to understand blockchain technologies?

---

Blockchain technologies are receiving a great deal of attention from businesses across a broad range of industry sectors, and for very good reasons.

In blockchain technologies “we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services. ... the visibility in these technologies [may] reform our financial markets, supply chains, consumer and business-to-business services, and publicly held registers.”

*UK Government Chief Scientific Adviser, Government Office for Science, Distributed Ledger Technology: Beyond Blockchain, 2016, page 4*

This chapter considers the circumstances in which the deployment of blockchain technologies is likely to deliver significant value and the potential impact of the new technologies upon various industry sectors (and horizontally across multiple sectors). It outlines the nature of blockchain technologies, surveys the current state of the vendor landscape and current investment trends, and examines potential obstacles to adoption. It also outlines the key legal and regulatory issues (many of these are dealt with in more detail in later chapters of this Guide). Finally, it considers the implications for businesses.

---

Blockchain technologies have the potential to:

**Facilitate simultaneous record-keeping and validation:** they allow record-keeping (the process of recording actions that have happened) and record validation (the process of ensuring that a new record is a valid representation of what has occurred) to be combined into one activity in an electronic and automated fashion (achieving cost savings in the process). “Two tasks that were previously time-consuming and expensive become one process”.<sup>1</sup>

**Eliminate duplication:** they can replace electronic ledgers that counterparties must keep in parallel and in sync (requiring periodic data checking and reconciliation, and periodic storage to unalterable media) with one consolidated record that constitutes a single and shared version of the truth. Such an outcome can be achieved extra-group (between different business participants) or on an intra-group basis when records are replicated across parts of a business, geographically or along functional lines.

**Implement business process re-engineering:** they make possible the re-engineering of business methods required for business transformation. It has been estimated that a blockchain “is about 80 per cent business process change and 20 per cent technology implementation”.<sup>2</sup>

**Deliver cost savings:** costs can be reduced by streamlining back-office processes.

**Authenticate transactions:** they can verify the origination of, and authentication of, a transaction conducted electronically.

**Provide permanence:** they can constitute a record of transacting history that is indelible and immutable.

**Enable direct peer-to-peer transactions:** they enable businesses who do not know each other to transact directly on a peer-to-peer basis without the need for a trusted third party to intermediate (and provide the requisite degree of trust through its involvement).

**Reduce time scales:** they shorten the time it can take to settle transactions to near real time.

**Enable automation:** in combination with smart contracts or other coded business logic (that is, software), blockchain technologies automate business processes through automatic performance (for example, the release of money on satisfaction of a condition).

“Blockchain will affect the way that individuals and organisations interact, the way that businesses collaborate with one another, the transparency of processes and data, and, ultimately, the productivity and sustainability of our economy.”

*Deloitte, Blockchain: Enigma. Paradox. Opportunity, 2016, page 13*

---

<sup>1</sup> Kwori Ltd, *Blockchains and Distributed Ledgers in 2016*.

<sup>2</sup> Deloitte, *Blockchain: Enigma. Paradox. Opportunity*, 2016, page 11.

## When are blockchain technologies likely to deliver significant value?

---

Although potentially very wide in their scope of application, blockchain technologies are more likely to deliver significant value when deployed in situations involving one or more of the following business needs:

---

**Reconciliation of data:**

such as where there are multiple market participants whose separate stores of data require periodic reconciliation.

---

**Reduction in**

**duplication:** for example, where parts of the same business maintain multiple records of the same data for use in different aspects of the lifecycle of a single transaction or for use in different transactions.

---

**Auditability:** where record-keeping of immutable records is required (whether for regulatory purposes or otherwise).

---

**Authentication:** where proof of the identity of the counterparty and verification of the origination of a transaction are essential for commercial or regulatory reasons.



## Which industry sectors might be affected?

Blockchain technologies “can be applied to a wide range of industries and services, such as financial services, real estate, healthcare and identity management. ... Furthermore, their underlying philosophy of distributed consensus, open source, transparency and community could be highly disruptive to many of these industries.”

*UK Government Chief Scientific Adviser, Government Office for Science, Distributed Ledger Technology: Beyond Blockchain, 2016, page 14*

Over the next five pages we explore blockchain use cases, investment opportunities and solutions which are emerging in major industries across the globe, comprising:

.....  
Financial institutions

.....  
Property and real estate

.....  
Consumer markets

.....  
Energy

.....  
Infrastructure, mining and commodities

.....  
Transport

.....  
Technology and innovation

.....  
Life sciences and healthcare



## Financial institutions

Blockchain technologies “could reduce banks’ infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between \$15 – 20 billion per annum by 2022.”

*Santander, The Fintech 2.0 Paper: Rebooting Financial Services, 2015*

Banks, financial institutions and insurers are considering use cases for blockchain technologies across wide areas of business operations, including in relation to issuing and transferring securities, netting and clearing, settlement and other post-trade processing (in total, the global finance industry pays around \$65 billion to \$80 billion per year for post-trade costs<sup>3</sup>), collateral management, syndicated lending, trade finance, swaps, derivatives, foreign exchange and potentially anywhere where counterparty risk arises.

Other applications might include asset, know your client (KYC) and anti-money laundering (AML) registries as well as records of ownership held electronically (including, potentially, securities accounts, investment accounts and cash accounts).

Such applications are not purely hypothetical. The NASDAQ exchange has announced that an issuer (a private company) was able to use NASDAQ’s Linq blockchain ledger technology successfully to complete and record the issue of shares to a private investor. The system has potential application in many clearing and settlement contexts.

The Australian Stock Exchange (ASX Limited) has announced that it has selected US-based Digital Asset Holdings LLC to develop a new post-trade solution for the Australian equity market using blockchain technologies. According to ASX, for ASX clients “this could remove risk and reduce back-office administration and compliance costs, while investors could experience significantly faster settlement of equity transactions – potentially in near real-time.”<sup>4</sup>

Over forty of the world’s largest banks have joined the R3 consortium to design and build blockchain solutions for financial services. In early 2016 a number of these banks were reported to have run an experiment using blockchain technologies to execute and settle trades for twenty-four hours, across Asia, Europe and North America, without the need for a clearing house.

The Depository Trust & Clearing Corporation, which provides clearing and settlement services to the US financial markets, has proposed exploring its adoption of blockchain technologies for clearing and settlement services.<sup>5</sup>

Insurers are considering the potential use of smart contracts (a particular instance of blockchain deployment providing for the automation of business processes), initially for more simple policies – for example, using smart contracts for flood or crop policies where automated claims payments are linked to a weather data feed or water level monitor. For now, blockchain technologies using smart contracts are confined to simple insurance risks where pre-contractual disclosures are not required. To the underwriter’s advantage, however, automated claims linked to blockchain technologies significantly reduce the risk of fraudulent claims, with reduced administrative costs for the insurer. With data fed into such technologies, premium levels can be adjusted automatically in response to certain pre-determined events or information received.

<sup>3</sup> UK Government Chief Scientific Adviser, Government Office for Science, *Distributed Ledger Technology: Beyond Blockchain*, 2016, page 60.

<sup>4</sup> AXS Media Release, *ASX Selects Digital Asset to Develop Distributed Ledger Technology for the Australian Equity Market*, 22 January 2016.

<sup>5</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016.



## Property and real estate

---

Real estate transfers depend on centralised title registries. Blockchain technologies could decentralise them. For example, the Swedish land registry is working on a proof-of-concept collaboration to develop a digitised land title registry deploying such technologies.

Blockchain technologies deploying smart contracts could be also used for some real estate transactions (subject to important statutory formalities in relation to certain types of transactions).



## Consumer markets

---

IBM and Samsung have collaborated to develop proof-of-concept use cases in relation to smart contracts deployed on a blockchain platform.

On a B2C basis, IBM and Samsung have demonstrated the viability of a Samsung washing machine, connected to the Internet of Things, to deploy a smart contract enabled by a blockchain to order and pay for refills of detergent from a retailer, and to detect an impending parts failure, interrogate existing warranty status and order warranty service for the machine (as well as to order and pay for out-of-warranty service thereafter). It could do all this without a centralised controller mediating between the parties.



## Energy

---

On a B2C basis, IBM and Samsung have also demonstrated the viability of using a blockchain-hosted smart contract associated with a Samsung washing machine, connected to the Internet of Things, to arbitrage energy consumption with other appliances in the home.

The IBM/Samsung proof-of-concept use case also demonstrated that the technology deployment was able to reduce household overall consumption at electricity peak cost times.

In South Africa, smart metering systems have been integrated with a cryptographic payment system using blockchain technology to allow unbanked customers to prepay for electricity.<sup>6</sup>

---

<sup>6</sup> CFO South Africa, *Blockchain will revolutionise business, says Bankymoon CEO Lorien Gamaroff*, 19 February 2016.



---

## Infrastructure, mining and commodities

---

Blockchain technologies could be used as an indelible record for ownership of high value commodities. For example, Everledger is developing the technology to track transactions and ownership in relation to diamonds, with potential application for use in verification by insurers, owners, claimants and law enforcement agencies.

Industrial application of the automating power of smart contracts deployed on a blockchain may bring efficiencies to infrastructure management. For example, operating in conjunction with infrastructure connected via the Internet of Things, smart contracts deployed on a blockchain may provide opportunities to automate processes as diverse as routine and preventative maintenance, subcontractor tendering and call-off, and wider supply chain administration.



---

## Transport

---

Blockchain technologies are being considered for use in the shipment of cargo (effectively automating documentation currently provided for in bills of lading).

Use of the automating functionality of a smart contract deployed on a blockchain in relation to vehicle finance leasing products could include, for example, the ability (in combination with the Internet of Things) to deploy a “kill switch” within a leased parked car in order to make it inoperable when repayments have not been maintained. (However, complex regulatory and legal issues may need to be addressed, depending on the jurisdiction, before any such use were to be rolled out.)

UATP (a payment network privately owned by many of the world’s airlines) has announced a partnership with Bitnet that would enable airlines to accept the cryptocurrency Bitcoin using blockchain technologies.

However, blockchain technologies may have the potential for far wider application in the travel industry. They may offer a better way of administering loyalty points programmes (facilitating real-time points updating and coordinated administration of points schemes across participating businesses using a single, shared record). They may also be used for passenger identity verification and ticketing.

Smart contracts deployed on a blockchain could be linked by the Internet of Things to make vehicle road tax payments for on-road vehicles, pay parking charges and book vehicle servicing and, in the rail industry, to make season ticket payments and administer “Delay Repay” or other passenger compensation schemes using passenger identity verification.

Public authorities may be able to use blockchain technologies to maintain vehicle asset registries and to administer driving licences.

Defect reporting and authorisation of rectification work orders could be streamlined through the automating power of smart contracts deployed on a blockchain, and better data collection through the use of blockchain technologies could lead to increased asset availability and reliability.



## Technology and innovation

**“These technological changes could foretell the biggest revolution since the origin of general purpose computing and transaction processing systems”**

*IBM Institute for Business Value, Empowering the Edge: Practical Insights on a Decentralised Internet of Things, 2015*

Blockchain technologies, in combination with the Internet of Things, may lay the foundations for decentralisation of many currently centralised technology processes (the decentralised nature of blockchain technologies is described in *What is a Blockchain?*, on page 17). Decentralisation may provide improved robustness by removing single points of failure that could exist in centralised technology networks, and give impetus for technology and electronics industry suppliers to develop entirely new product and service offerings (such as data storage and management systems and order processing and management functionality).

Numerous technology vendors are now developing a range of blockchain applications across the globe. An example of a new service offering incorporating the new technology is Microsoft’s cloud-based blockchain-as-a-service (BaaS).<sup>7</sup>

Blockchain technologies could be used in combination with the Internet of Things for the purpose of “thing authentication” – that is, ensuring that devices that wish to connect to a particular network (for example, a domestic household network) actually belong to that household.<sup>8</sup> For example, IBM and Samsung have developed a device authentication framework, “ADEPT” (that is, Autonomous Decentralized Peer-to-Peer Telemetry), to enable machines to be registered on a blockchain by the manufacturer, enabling device details to be updated as the machine is bought, installed, sold or maintained.

Smart contracts deployed on blockchain technologies may enable many machine-human interactions to become machine-to-machine interactions, creating opportunities for device manufacturers.

Use of blockchain technologies to secure intellectual property and digital creative works (for example, images and music) is reportedly being considered – for example:

- Blockchain technologies are being evaluated as a mechanism by which to enforce digital rights management schemes, to help prevent illegal file sharing, to enforce licensing rights, and to collect royalty payments. Such possibilities arise by virtue of the programmable nature of code logic within a “block” on a blockchain (blocks and the programmable potential of blockchain technologies are described in *What are the Component Parts of a Blockchain?*, on page 19).
- Such technologies could prove a work’s attribution and provenance. However, there are limits to this. Moreover, in many jurisdictions, “dealings” (for example, an assignment) in certain types of intellectual property rights require compliance with legal formalities which may not be satisfied by a transaction conducted over a blockchain.
- Blockchains could be used for patent or documentation filing.

<sup>7</sup> David Schatsky and Craig Muraskin, *Beyond Bitcoin: Blockchain is Coming to Disrupt your Industry*, Deloitte University Press, 2015, page 2.

<sup>8</sup> Kwori Ltd, *Blockchains and Distributed Ledgers in 2016*.



---

## Life sciences and healthcare

---

The ability to demonstrate the provenance of component compounds of pharmaceutical drugs and parts for medical devices is of increasing regulatory focus within the life sciences and healthcare industries. Blockchain technologies could be used as an auditable record for the supply chain, from manufacturer onwards.

Factom is reportedly intending to develop blockchain technologies for use by a client to record various medical documents (such as medical procedure ordering and billing services) to add security and authenticity to the recording of the sequence of events.

While controversial, consideration is being given to whether blockchain technologies could be used to store patient clinical records (allowing them to be accessed by multiple clinicians or service providers, potentially even on a cross-border basis).<sup>9</sup>

---

<sup>9</sup> UK Government Chief Scientific Adviser, Government Office for Science, *Distributed Ledger Technology: Beyond Blockchain*, 2016, page 37.

## What blockchain applications could be deployed horizontally across industry sectors?

---

Blockchain technologies could potentially be deployed horizontally – that is, across various industries without differentiation. Typically such deployments are likely to be for infrastructure or processes that all (or most) industries have in common (such as the need to make and receive payments or to automate data processing).

Such applications may not be limited to external deployments. They could be used to reduce replication of processes and systems inside a business or group of businesses, or to link disparate parts of data infrastructure of a business together, and in either case so as to create a “single version of the truth” within a business or business group.

Horizontal applications might include:

---

**Cryptocurrencies:** there is already a well-known and fully-deployed application for blockchain technologies in the form of the cryptocurrency, Bitcoin. Various other cryptocurrency deployments typically also use blockchain technologies. It is those underlying technologies (rather than the cryptocurrencies that deploy them) that are seen by financial institutions and other industries as having transformative potential. (For information on the legal issues relating to cryptocurrencies, see Norton Rose Fulbright’s information portal, [FinTech Law and Regulation: Blockchains, Distributed Ledgers, Smart Contracts and Cryptocurrencies](#)).

**Smart contracts:** smart contracts typically rely on blockchain technologies and have the potential to automate business processes on a blockchain. (For more information on smart contracts, see our publication, [Smart Contracts: Coding the Fine Print](#)).

---

**Middleware networks:** “blockchain/distributed ledgers provide the potential efficiency of a central database and the robustness of a third-party clearing house for complex/distributed transactions without costly middleware.”<sup>10</sup> (Middleware is computer software that provides services to software applications over and above those available from the computer operating system. It is often described as “software glue”.) Database access services are often characterised as middleware. Because a blockchain is in effect a database, businesses in all industry sectors may be able to deploy blockchain technologies in a way that saves costs by replacing database-related middleware.

---

<sup>10</sup> Magister Advisors, *Blockchain & Bitcoin in 2016: A Survey of Global Leaders*, uk.businessinsider.com, December 2015, page 15.

**Record keeping:** various record-keeping activities are performed on a daily basis across a range of industries. Blockchain technologies have the potential to introduce efficiencies and cost-savings into such processes. Take, for example, financial services. Here the following important record-keeping activities could potentially be rationalised for efficiency by a blockchain deployment:

- **Identity management:** several systems (including access management systems) are typically used to link a user identity to its account or asset holdings within a bank or financial institution. Identity management requires there to be a “single source of truth” within a bank or financial institution, which is then typically integrated across the front, middle and back office applications. An internal blockchain deployment could provide that single source of truth for identity management within an organisation.
- **Master data management:** master data (such as entity information, asset information, business day and holiday information) includes information that is local to an enterprise as well as information common across an entire industry. Such information is used, for example, in securities transaction processing and can involve replicated internal and external reconciliation of such information. Such information may be “an ideal candidate for improvement using decentralised consensus, rule standardisation and auditable change history” via blockchain technologies.<sup>11</sup>

---

<sup>11</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016, page 13.

**Matching applications:** for example, enabling buy and sell orders to be matched in a marketplace. Such activities potentially lend themselves to rationalisation through the deployment of blockchain technologies.

**Issuing and servicing assets and securities:** blockchain technologies could be used to manage the issuing of securities and track ownership in a way that could greatly simplify asset servicing.<sup>12</sup>

---

<sup>12</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016, page 13.



## What is a blockchain?

“A blockchain is a digital, distributed transaction ledger, with identical copies maintained on multiple computer systems controlled by different entities.”

*David Schatsky and Craig Muraskin, Beyond Bitcoin: Blockchain is Coming to Disrupt your Industry, Deloitte University Press, 2015, page 2*

Blockchain technologies describe a group of software applications that all deploy a blockchain. Blockchains derive from technology underpinning the Bitcoin cryptocurrency, but it is widely accepted that the potential functionality and uses of blockchain technologies will extend far beyond the provision of cryptocurrencies.

### A blockchain:

**Is digital:** it is made up of software (coding including algorithms) and data. The software allows the data to be transmitted, processed, stored and represented in human readable form.

**Is a ledger:** it is a record in the form of a database of data representing transactions (or of what has occurred).

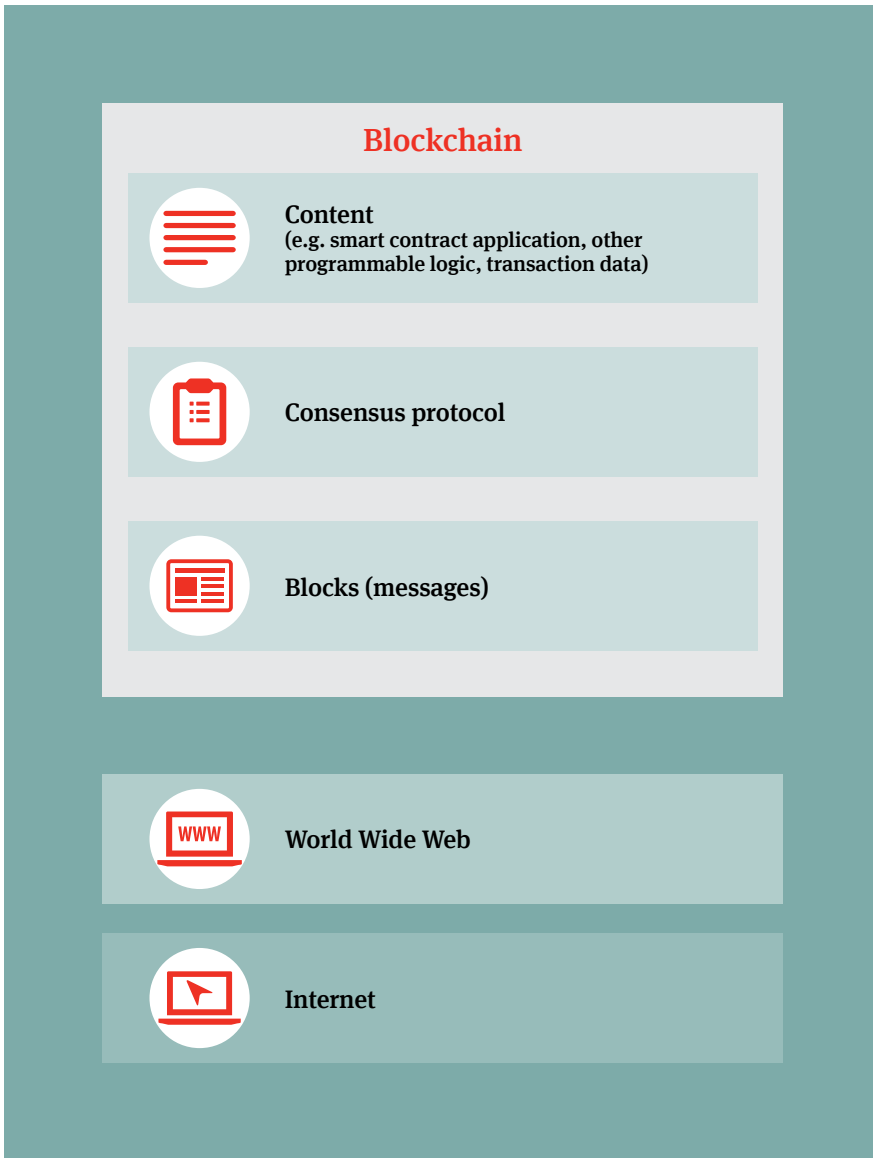
**Is distributed:** identical copies of the ledger database are downloaded from the world wide web and kept on numerous computers (known as “nodes”) spread across a site, an organisation, a country, multiple countries, or (in some cases) the entire world. For this reason a blockchain is sometimes called a “distributed” or “shared” ledger. (All blockchains are distributed ledgers, but not all distributed ledgers use blockchains).

**Uses consensus:** a computer protocol in the form of an algorithm constituting a set of rules for how each participant (say, separate counterparties or businesses) in a blockchain should process “messages” (that is, a transaction of some sort) and how those participants should accept as correct (or reject) the processing done by other participants. The following applies in respect of consensus protocols:

- The purpose of a consensus protocol is to achieve consensus between all the participants in a blockchain as to what a blockchain should contain at a given time (including by the addition of new records of new transactions, known as “blocks”).
- Consensus generally occurs when more than fifty per cent of nodes conclude that a message is authenticated and verified, so that the message can be added as a block to a blockchain. (Authentication and verification are described in *How Does a Typical Blockchain Transaction Work?*, on page 21).
- In certain blockchain applications (for example, some “permissioned” blockchains, described in *What is the Difference Between a Permissioned and a Permissionless Blockchain?*, on page 20), consensus is not used as the basis for determining what a blockchain should contain at a given time. Instead a particular person or entity (for example, an administrator) may be empowered to undertake such determination on behalf of all participants.

**Uses cryptography:** blockchains deploy public key infrastructure in the form of public and private encryption keys to verify that a message comes from who it purports to come from and to authenticate the contents of that message. (The process of encryption is described in more detail in *How Does a Typical Blockchain Transaction Work?*, on page 21).

The communications medium between participants to a blockchain is typically the world wide web. It is from the world wide web that participants' nodes (their computers) download and maintain the then current form of a blockchain. The "technology stack" for a blockchain can therefore be represented like this:



## What are the component parts of a blockchain?

Blockchains are made up of component parts that are generated and hosted by software. The following are key components:

**Messages:** a message is a submission of data (typically a transaction) for processing by nodes (participants' computers) with the object of having the message authenticated and verified by cryptography and consensus reached on it (so that it becomes a transaction record). Messages may:

- Act as inputs or outputs of computer programs, and may themselves contain or point to computer code.
- Contain content that is encrypted or they may refer to encrypted content stored elsewhere.

**Blocks:** a message or messages relating to a transaction (or the change in status of something) are bundled together by the software in a software-generated container known as a block and given a title known as a block header. Blocks can be entirely public (all their contents can be viewed by any participant) or merely semi-public (in that other participants can see the container and its label, but they may not be able to see the contents without a cryptographic key).

**Block headers:** the block header:

- Is dependent on the combination of messages in the block.
- Lists the transaction(s), the time at which the list was made, and a reference back to the hash (described below) of the most recent block.

**Time stamp:** a number representing a point in time at which the list of contents (for example, messages) within a block header was created.

**Hashing:** software causes the block header to be "hashed". Hashing is the process by which a grouping of digital data is converted into a single number, called a hash. The number is unique (effectively a "digital fingerprint" of the source data) and the source data cannot be reverse engineered and recovered from it.

**Chaining:** the block header for a new block contains a reference to the hash for the previous block in the chain. When a later block is added, it too will include a reference to the hash for the immediately preceding block. In this way there is a continuous chain of blocks (that is, a blockchain) back in time.

In order to change one block in the chain, it would be necessary to change every single block that came after it. If any data in any block in the chain are later altered, this is immediately apparent to all participants of that blockchain, as that block's hash (and that of any subsequent block) will no longer correspond to the later block's record of that hash.

The result is an indelible record. That factor, in combination with the comfort to be had from correspondence between the respective copies of the blockchain achieved through consensus, provides the requisite trust between participants, even if they are strangers. It is therefore the system itself, rather than a central authority or third party with whom the participants interact, that is the basis of that trust.

## What is the difference between a permissioned and a permissionless blockchain?

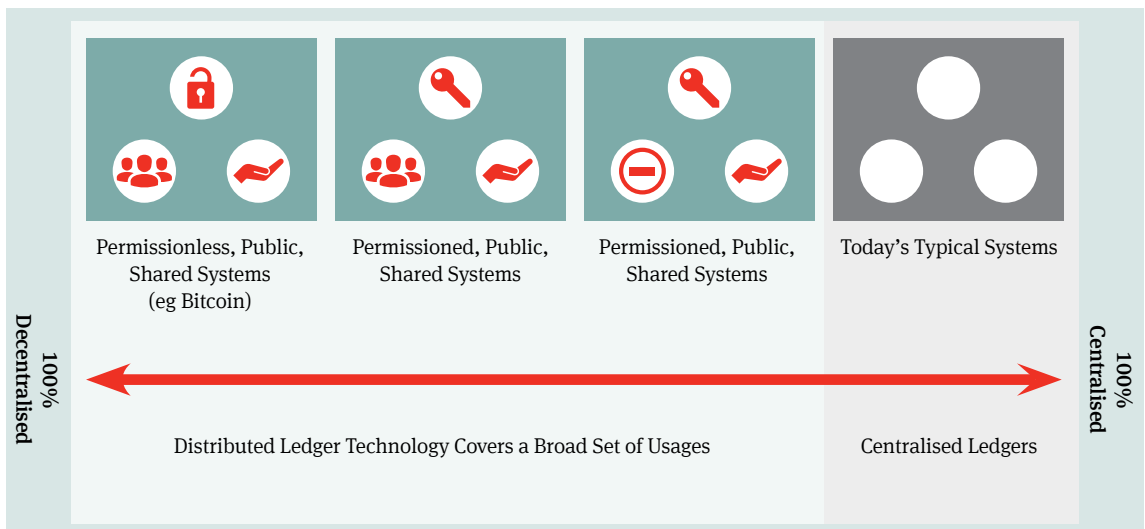
A blockchain deployment can be permissionless or permissioned. There are also hybrid models:

**Permissionless (public):** a blockchain is permissionless when anyone is free to download the software, submit messages for processing and/or be involved in the process of authentication, verification and reaching consensus. While a permissionless blockchain will typically use a consensus protocol for determining what the current state of a blockchain should be, it could also use some other process (such as using an administrator or sub-group of participants) to determine that state. Such systems are typically controlled by no-one and the participants are usually pseudonymous.

**Permissioned (private):** a blockchain is permissioned where its participants are pre-selected or subject to gated entry on satisfaction of certain requirements (this could include, for example, a requirement that a participant must first satisfy KYC and AML requirements) or on approval by an administrator of the blockchain. A permissioned blockchain may use a consensus protocol for determining what the current state of a blockchain should be, or it may use an administrator or sub-group of participants to do so.

**Hybrid systems:** there are a number of different variables that could apply to make a permissionless or permissioned system into some form of hybrid. Such variables typically relate to the degree of centralisation that those responsible for setting up a blockchain wish to achieve. For example, as already mentioned, an otherwise permissionless system may nonetheless use encryption of blocks, so that, while anyone downloading the requisite software could inspect a blockchain, no-one except those with the required cryptographic key could inspect individual messages or transactions. The same restrictions could equally apply to a permissioned system.

## Different ledger technologies vary in their 'degrees of centralisation'



UK Government Chief Scientific Adviser, Government Office for Science, Distributed Ledger Technology: Beyond Blockchain, 2016

## How does a typical blockchain transaction work?

---

Blockchain technologies use public key encryption infrastructure (PKI).

Someone wishing to participate in, say, a permissionless blockchain (the initiator participant) can:

- Download the software from publicly available sources (from the world wide web)
- Using an address (an alphanumeric number uniquely allocated to it by the software), generate a public key
- Publish the public key on the system publicly, via the world wide web.

At the same time, the software will also generate a corresponding private key for the initiator participant's address, to be held securely by it.

If the initiator participant wishes to initiate a transaction on the relevant blockchain, it uses its address to send an initiating message, encrypted with its private key, to the other participants via the world wide web. The message is picked up by the participants' nodes.

Messages purporting to be from the initiator participant's address can only be signed off by a person in possession of the initiator participant's private key. Participants with access to the public key (which they get from the software via the world wide web) can use it to verify that the transaction was initiated by the initiator participant in possession of the private key and to authenticate the message contents.

When sufficient nodes reach the same conclusion (more than fifty per cent), the applicable consensus protocol determines that the message should be written into a block and added to the blockchain.

PKI used by blockchain technologies deploys an asymmetric algorithm. This means that participants do not (in contrast to systems using a symmetric algorithm) share a secret key. This makes it extremely difficult to reverse engineer back from the public key to the private one. It also means that the participants do not need to know each other or to share anything secret in order for them to trust each other.

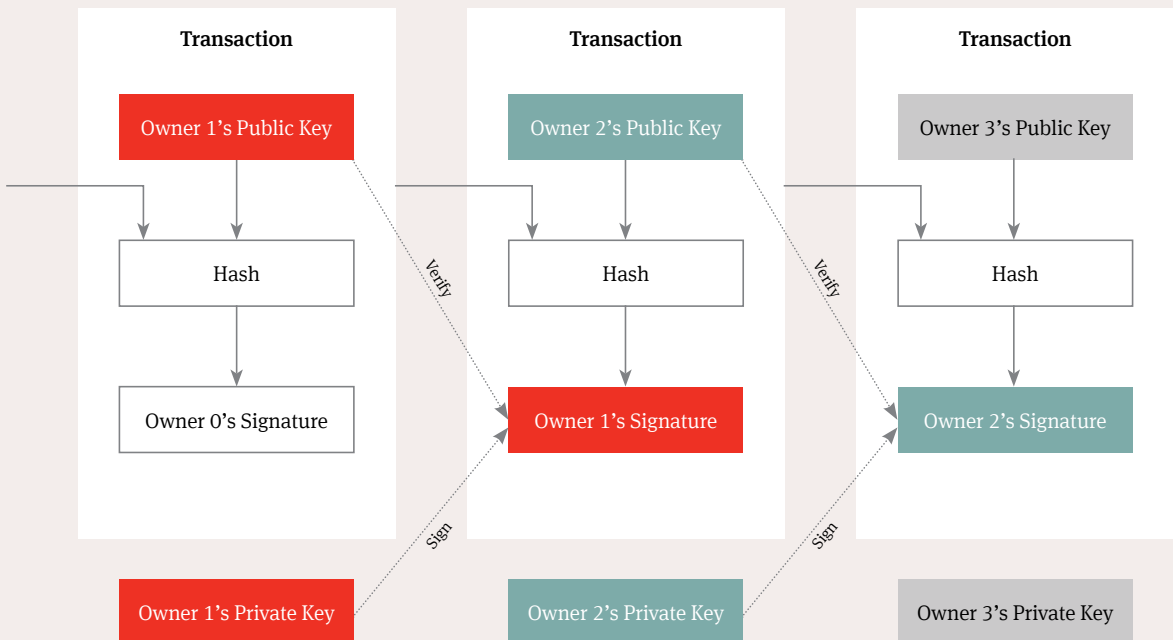
## How does blockchain cryptography work?

Owner 1 wishes to initiate a blockchain transaction via a message that Owner 1 wants all participants to know emanates from Owner 1.

Owner 1 signs the message with its private key. A digital signature unique to the message data and the private key is created by combining the message and the private key.

Owner 2 wishes to check the authenticity of the message. Owner 2 downloads Owner 1's public key from the system, and using it and the message, Owner 2 can verify that the message was sent from the holder of the private key (Owner 1).

Owner 2 is able to make such verification as no-one other than Owner 1 would be able to generate the signature. This is because the two keys are mathematically related.



Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, [www.bitcoin.org](http://www.bitcoin.org)

## What are the main performance characteristics that define blockchain technologies?

---

The performance characteristics of blockchain technologies are determined by the technology architecture and coding functionality. Some of these are relevant to any legal or regulatory analysis relating to proposed use of blockchain technologies.

Typically a blockchain has the following key performance characteristics:

**Transparency:** in a fully permissionless blockchain, all messages (including – when consensus has been reached – when they have been included on a blockchain as blocks) sent by participants are visible to all other participants. Accordingly blockchains are highly transparent, because each participant has a complete, traceable record of every transaction recorded on a blockchain. However, as already mentioned, while the blocks themselves might be visible, in some blockchain deployments (typically a permissioned blockchain) the contents of the blocks might still be encrypted. The level of transparency may determine the kind of uses made of a blockchain, and will be relevant when considering the legal and regulatory issues relating to that use.

**Time-stamped:** as a time stamp is associated with each block, this allows all participants to know when a transaction recorded by a block occurred. This is likely to be particularly useful when it is necessary to prove transacting history (for example, for legal or regulatory reasons).

**Immutable:** current thinking on blockchain technologies suggests that, based on present computing power, it may be nearly impossible to alter existing data illicitly (including, for example, a time stamp) on a blockchain without detection (a theoretical exception is a so-called “51% attack” described in *Are there Obstacles to Widespread Adoption?*, on page 25). Data on existing (non-blockchain) systems are not immune from alteration as things stand, and accordingly business cases evaluating risk associated with blockchain technologies could legitimately compare relative data security as between blockchain deployments and existing systems (rather than attempt to prescribe the exclusion of all such risk, theoretical or otherwise).

**No single point of failure:** because identical copies of a blockchain are downloaded from the world wide web onto multiple nodes (that is, the computers of all participants), if any node fails (perhaps for technical reasons affecting a particular computer, or because that participant ceases to operate), the other nodes will continue to make the information available to all other participants. This characteristic is something that can be taken into account when evaluating matters such as business continuity, disaster recovery and (in IT terms) system “redundancy” (redundancy is discussed in more detail in *Are There Obstacles to Widespread Adoption?*, on page 25).

**Irrevocable:** transactions recorded on a blockchain can be made to be irrevocable and irreversible. This can be both a strength (for example, an irrevocable commitment) and a weakness (for example, in some types of trading, the ability to reverse or cancel a placed trade is standard practice). (For discussion of some of the legal issues concerning the irrevocable nature of a blockchain in the context of smart contracts, see our publication, *Smart Contracts: Coding the Fine Print*).

**Programmable:** instructions can be included in code embedded within a block on a blockchain. They can, for example, perform actions when, say, particular conditions are satisfied. An example of such programmable logic is a smart contract implementation on a blockchain. (For more information on the legal implications of the programmable logic of blockchain technologies in the context of smart contracts, see our publication, *Smart Contracts: Coding the Fine Print*).

## What is the current state of the vendor and investment market and likely adoption timelines?

“Blockchain has evolved from zero to the cusp of being a multi-billion dollar market in less than 24 months”

“2016 marks a ‘race to production’ as innovators seek to push beyond the prototype stage. This is particularly important for vendors looking to establish market position”

*Magister Advisors, Blockchain & Bitcoin in 2016: A Survey of Global Leaders, uk.businessinsider.com, December 2015, pages 18 and 9*

It has been estimated by Magister Advisors that over \$1 billion will be spent by large financial institutions on blockchain projects over the next twenty-four months. Many large financial institutions have reportedly already identified portfolios of ten to twenty potential blockchain projects to evaluate.

### Vendor market

The vendor market is now characterised by a split between:

#### Industry-specific (or “domain”) application and solution providers:

- They seek to provide specific functionality (often specific to a particular industry).
- Their solutions typically will need to integrate with existing (legacy) platforms.
- Their solutions can be deployed to re-engineer existing business processes.
- Examples include digital wallets, loyalty programmes, identity verification, and inter-bank settlement solutions. While the market is still very much at the “proof-of-concept” phase in technology development, a recent survey by Magister Advisors suggests that the largest technology providers have twenty to thirty client projects already underway.

#### Platform vendors of middleware and services:

that is, those providing the underlying technology upon which particular blockchain applications and solutions can run. Platform vendors seek to provide platforms that:

- Provide flexibility to tailor applications to individual requirements.
- Are general purpose infrastructure.
- Are akin to relational databases for enterprise applications within a business.

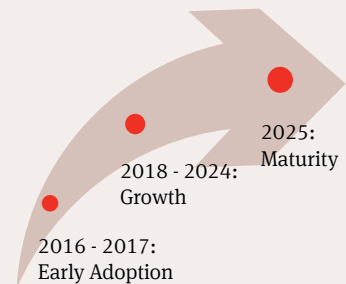
#### Infrastructure and protocols:

that is, vendors who look to develop cryptographically secure consensus mechanisms for use as part of blockchain technologies.

### Investment opportunities and adoption timelines

Recent predictions suggest that the focus for investment in 2017 could well be middleware and infrastructure providers who provide the backbone technology and infrastructure necessary for the development of a wider ubiquitous blockchain ecosystem.<sup>13</sup>

Accenture predicts that the likely adoption timeline will be:



Early adoption, so the argument goes, will be driven for external uses by regulatory certainty. As adoption enters the growth phase, regulatory guidance will become clearer, there will be widespread network adoption and incumbent processes and services will be discarded. By 2025 blockchain technology will be considered mainstream.<sup>14</sup>

<sup>13</sup> David Schatsky and Craig Muraskin, *Beyond Bitcoin: Blockchain is Coming to Disrupt Your Industry*, Deloitte University Press, 2015, page 6.

<sup>14</sup> Accenture, *Blockchain-enabled Distributed Ledgers: Are Investment Banks Ready?*, 2016, page 7.



## Are there obstacles to widespread adoption?

There are a number of technical and functional factors that could impede uptake of blockchain technologies generally, or that need to be taken into account by a business proposing to deploy or participate in a blockchain.



### Confidentiality

In a permissionless blockchain, unless message content itself is encrypted, all transactions, including the flow of money and pricing, are exposed for inspection by anyone. There will be many instances in which participants will wish to keep such information private (in relation to the public generally, and perhaps in relation to other participants to a blockchain who are not counterparties to the relevant transaction). For example, a financial institution would not wish to make its trading exposure public.

Participants may prefer to use a permissioned blockchain so that its content cannot be viewed by non-participants. However, as already described (see *What is the Difference Between a Permissioned and a Permissionless Blockchain?*, on page 20), the distinction between a permissioned and permissionless blockchain is a question of degree. Hybrid models exist on the spectrum between one and the other, and it is perfectly possible, for example, to have a permissionless blockchain whose message content is nonetheless encrypted.

**78% of those recently polled said that, in relation to financial services, permissioned systems would ultimately become the preferred governance model used in that sector**

*DTCC Blockchain Symposium 2016*



### Identifiable participants

Blockchain transactions can be pseudonymous. While the system itself is intended to create the requisite trust between the participants, in legal, regulatory or commercial contexts the identity of the counterparty may be of fundamental importance to the other participant(s). For example, it may be necessary for regulatory reasons to satisfy KYC and AML requirements before transacting with a participant.

For these reasons a business may prefer to operate within a permissioned blockchain, where an administrator can control the membership and prescribe the conditions (including, potentially, legal terms and conditions) upon which participation is permitted.



---

## Persistence of the community

---

Confidence in the long term nature of a blockchain depends upon confidence in the fact that the participants whose nodes host it (and who therefore ensure its survival) will themselves persist as a community.

That means having confidence that those who maintain a blockchain will continue to do so. If they do not, the record of data and transactions may be put at risk. For example, proponents of blockchain technology acknowledge that there is a theoretical risk that a blockchain could be “overwhelmed” by an attacker with control of 51% (a so-called “51% attack”) or more of the network’s total hashing power (at least in the context of Bitcoin’s deployment of blockchain).

That risk arises where consensus is the basis chosen for determining the current state of a blockchain, because to reach consensus (under a typical consensus protocol) requires more than fifty per cent of participants to agree on the current state of a blockchain.

The risk of a 51% attack might increase if the participants in a consensus-driven blockchain begin to ebb away. This is because it will take fewer nodes to control more than fifty per cent of the system.

To deal with that concern, the participants may look to a third party who is willing to host the blockchain as a document of record for as long as it is needed. There is already a model for this type of arrangement in the e-mortgages industry in the US, where Bank of New York Mellon is used for certification and custody of eNotes.



## Latency, bandwidth and storage constraints

“A decentralised design requires significant computing and storage resources because all nodes perform the computations and store the ledger data, which can also result in significantly increased network bandwidth requirements depending on the number of network nodes and the size of each transaction.”

*DTCC, Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape, January 2016, page 9*

Because transactions on a blockchain using a typical consensus protocol require a majority of participants to reach consensus, it means that each node involved in reaching that consensus performs the same tasks as the other nodes in verifying its copy of the data. This results in an inherent inefficiency where this kind of consensus is used, and may result in more work for individual nodes as the number of participants or the blockchain itself increases in size.

There have been latency and bandwidth issues in some existing blockchain solutions. In IT terms:

- “Latency” is the time delay between the cause and the effect of some change in the system being observed. In the context of a blockchain, a latency issue can mean a delay in updating it to reflect new transactions.
- “Bandwidth” is the capacity of a network. As more and more transactions are added to a blockchain, it may become increasingly unmanageable in size, making it more difficult to add new transactions.

As a blockchain gets larger and larger, it takes longer to download and requires more storage capacity to store. It may be impractical for, say, consumers to store blockchains on domestic computers.

However, technical solutions are already being developed to address these problems. For example:

- Storage of large amounts of data can be dealt with by deploying a pointer hash in a blockchain which directs the participant to access the stored data from an “off-chain” database. In this way a blockchain may not need to store all the data relating to a particular transaction (or for all transactions). Nevertheless, some businesses may still wish to store their own complete copy for added reassurance.
- Technology architecture is being developed to store separately different kinds of data otherwise held on a blockchain (for example, identity and content), perhaps with a trusted third party storage provider.
- Ethereum has been working on a process, known as “sharding”, to address bandwidth issues with the object of reducing computing power required per node.

Moreover, there are aspects of the technical architecture of a blockchain that are potentially an advantage over, say, traditional database architecture, particularly in the context of redundancy. In IT terms, “redundancy” is the duplication of critical components or functions of a system with the intention of increasing the reliability of the system (usually in the form of a back-up or fail-safe). “Because messages and blocks [in a blockchain] are held by multiple participants, the system has high redundancy, and is robust to the failure of individual participants.”<sup>15</sup>

<sup>15</sup> Kwori Ltd, *Blockchains and Distributed Ledgers in 2016*.



---

## Compatibility and standards

It will be “very important to have networks with nodes that can process both the [blockchain] environment and the legacy environment, and to have smooth APIs (application program interfaces) between both.”

*Fabian Vandenreydt, Global Head of Securities, Immotribe and the Swift Institute, quoted in Mike Scotti, Panelists Discuss the Hype and Reality of Blockchain, DTCC Connection, 19 April 2016*

---

Where a business uses a blockchain, it is unlikely that all the data it needs in relation to a particular transaction, customer or other matter will be stored there. Blockchains will therefore need to inter-operate (that is, they will need to integrate) with a business’s legacy systems in order to exchange data between them. For example, inter-operability would be essential where a business trades assets in both on and off-chain environments, as here asset reconciliation would be needed between the two sets of data.

For data itself to be exchanged between participants to a blockchain, or between a blockchain and a business’s legacy systems, that data will need to be standardised so as to avoid the inefficiencies of data conversion.

“Everybody correctly cites lack of standardisation, or the challenge of reaching standards, as an obstacle.”

*Blythe Masters, CEO, Digital Asset, quoted in Jim Binder, Bodson and Masters Discuss Roadmap of Blockchain, DTCC Connection, 19 April 2016*

---

The development within a single sector of many different blockchain solutions that use different technical standards could result in less efficiency rather than more, as multiple data silos are created. In IT terms, a “technical standard” prescribes requirements to achieve compatibility and interoperability between software, systems, platforms and devices.

Technical standards are less likely to be problematic for permissioned blockchains, which are more likely to be set up by participants with a common vision of what standards ought to apply. Moreover:

- As a condition of participation in any blockchain, it may be possible to prescribe (as part of the governance or terms and conditions of use) the technical standards that a participant must adhere to in participating; and
- Adoption of new technology such as a blockchain could be an opportunity for industry in general to adopt common standards where none had previously existed.

---

While these technical issues present challenges, if addressed appropriately they also offer the potential to eliminate manual interactions, electronic exchanges of data, data format conversions and reconciliations with legacy systems.



## Security

---

Blockchain technologies give rise to a number of security-related issues that will need to be considered in use cases for the adoption of the technology by a business. Although dealt with in more detail in a subsequent chapter dealing with IP and IT issues, at high level such security-related issues include:

- So-called “51% attacks”
  - Forking: when some nodes in the participating community build on a block, while others choose to build on a separate block.
- 

Whatever system (whether a blockchain or a conventional database) is used in relation to data, security will always be an issue. Traditional database technologies have to date proved to be far from secure. More theoretical as well as more likely security risks both need to be evaluated in use cases by a business considering deploying blockchain technologies. Factors to take into account in making such an evaluation include:

- Whether the authorisation and encryption processes inherent in the use of the technology will improve the overall security of the relevant business process and its data. Blockchain technologies typically encrypt individual messages. In contrast, a traditional database typically deploys a database-wide security layer. Once that is breached, the content of the whole database is accessible. No-one has yet managed to break the encryption and decentralised architecture of a blockchain.<sup>16</sup>
  - The fact that the technology removes single points of failure, and so potentially enhances security. (This is because replicated copies of the data are distributed across multiple nodes. If a node fails or is corrupted, the other nodes still have access to the data).
  - For blockchains that use consensus protocols, as the number of participants grows, it becomes more and more difficult for someone to maliciously overcome the verification activities of the majority by a 51% attack (the system therefore becomes increasingly secure).
- 

<sup>16</sup> Deloitte, *Blockchain: Enigma. Paradox. Opportunity*, 2016, page 12.



## Immutability

---

A key virtue of a blockchain is that its transactions are commonly regarded as immutable (subject to the security issues already described) and irrevocable.

---

What is a strength, however, can also be a weakness. Immutability and irrevocability mean that there may be no ability to reverse, cancel or amend a transaction (it is a common enough occurrence for such ability to be built into, for example, many trading activities within financial markets). For more information on the legal issues concerning irrevocability in the context of smart contracts deployed on blockchains, see our publication, *Smart Contracts: Coding the Fine Print*.



---

## Data-related functionality limitations

---

Although some blockchain solutions may address some of the following problems, as it stands currently, blockchain technologies are typically somewhat lacking in relation to data manipulation functionality in a number of ways. For example:

- Blockchain technologies may not significantly improve data interrogation (that is, inquiry and retrieval of data).
- Search functionality may not be as good as that currently provided by a typical database.
- Blockchain technologies may not yield the same amount of data in the same speed as big data analytics typically would do.
- Unlike modern data applications, blockchain technologies may not, without significant additional integration, interface with other data management applications.

These issues are likely to be addressed as blockchain technologies develop.

## What are the key legal and regulatory issues?

The legal and regulatory issues relating to blockchain technologies include the following:

### Can blockchains affect legal relations?

A transaction on a blockchain may involve a smart contract which may sometimes have contractual effect as between the participants to it. In the absence of the programmable logic of a smart contract, a transaction conducted over a blockchain may, depending on the facts, still sometimes affect legal relations between the participants to it. The factors that the courts are likely to take into account in determining whether this is the case are analysed in our publication, *Smart Contracts: Coding the Fine Print*.

### Governance issues

Governance in the context of blockchain technologies means self-regulating arrangements that control the way in which participants are admitted to a permissioned system and the basis upon which consensus (or the updating of the blockchain to reflect then current state) will occur. Such arrangements are analogous to the private rule-making implemented by well-known credit card scheme operators that govern the actions of all participants in the relevant card scheme.

In the case of a blockchain deployment, these arrangements may currently be found (if

at all) in ad hoc contracts, in non-disclosure agreements or in informal or undocumented understandings between permissioned participants (or potentially not at all in the case of permissionless systems).

Currently there is considerable debate within the blockchain industry as to what governance in the context of blockchain technologies should look like. In the case of permissioned systems, the business or entity that establishes a blockchain has the ability to prescribe what the governance should be. Entry (and therefore governance) could be prescribed contractually.

A participation contract could regulate, for example, the following (many of these requirements are more apposite in the case of a permissioned system than for a permissionless one):

- Conditions for admission as a participant (for example, KYC and AML requirements), in the case of a permissioned system.
- The consensus protocol applicable, or the basis for determining the then current state of the blockchain (for example, as determined by an administrator).
- In the case of consensus, commitments of the participant to provide node processing.
- Provisions relating to trust boundaries (see *Trust Boundaries*, on page 32).
- Service levels for latency, bandwidth and other technical requirements of the system.
- Software updates for the system, designed to minimise disruption as well as improve performance.
- Other technical aspects of the operation of the system.
- Termination rights, if any.
- Risk allocation in relation to liability for failure of the system (including in respect of failed transactions).
- The extent to which particular transactions conducted across a blockchain change legal relations between participants (for example, by creating a contract between them relating to a transaction, and what the terms of that contract should be).

In the absence of formal contracts, businesses participating in blockchain deployments run the risk of uncertainties over whether a contract (or contracts) exist between participants in relation to a blockchain (and transactions undertaken using a blockchain), and what the terms of such a contract (or contracts) might be. (For more information on what a court might take into account in determining whether a contract might exist, and its terms, see our publication, *Smart Contracts: Coding the Fine Print*.)

Businesses will wish to avoid exchanging value over a blockchain in the absence of clearly defined contractual parameters, and run the risk of exposing themselves to uncapped liability and counterparty risk if such arrangements are not put in place. The contractual status relating to participation in a blockchain deployment should therefore be ascertained during the use case for the technology, and provided for prior to go-live.

### Trust boundaries

Although in essence a self-regulatory issue, businesses proposing to deploy blockchain technologies should give consideration to trust boundaries in governance arrangements between the participants.

A trust boundary is “the place where the ledger integrates with anything that is not in the ledger, such as onboarding trusted entities as ledger members or entitling an entity to issue an asset into the ledger and validating that the rights to the specific asset are owned by that entity and that those assets are properly secured off the ledger.”<sup>17</sup>

A record constituted by a blockchain can reflect a transfer of an asset for value, but if the asset itself is in physical form (or not otherwise wholly stored on a blockchain), then something more may be required to ensure that the asset exists, is protected and that multiple dealings in respect of it have not been entered into.

Governance arrangements would need to prescribe when and how such external confirmations are sought and recorded. For example, some form of certification by a third party may be required. A participation agreement could provide for such certification and for its legal status as between counterparties to a blockchain transaction (or as between all participants in a blockchain).

### Regulatory considerations

“There are ... opportunities to take advantage of the potential interactions between legal and technical code. For example, public regulatory influence could be exerted through a combination of legal and technical code, rather than exclusively through legal code as at present. In essence technical code would be used to assure compliance with legal code, and, in doing so, reduce the costs of legal compliance.”

*UK Government Chief Scientific Adviser, Government Office for Science, Distributed Ledger Technology: Beyond Blockchain, 2016, page 12*

The chapter of this Guide concerning the regulatory considerations relevant to blockchain deployments deals with the regulatory issues in detail, including recent regulatory initiatives.

---

<sup>17</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016, page 10.



For the moment it is worth noting one important concept we are currently seeing a number of commentators discuss: “code is law”.<sup>18</sup> The idea is that the programmable logic in a blockchain could be used to enshrine and implement legal code (that is, regulations, prudential guidance etc), so that, in participating in a blockchain, a business has no choice but to adhere to legal code in the way that a blockchain performs its functions.

Many blockchain applications are currently being developed in silos. There are pockets of developments but no centralisation across regulated industries. This development pattern potentially has regulatory implications (although views differ as to how these might manifest themselves). For example, while some commentators have suggested that:

- Decentralised blockchain deployments could potentially make activity invisible to a regulator; and
- Centralised systems may be better able to act as shock absorbers in a time of crisis, and “decentralised networks can be much less resilient to shocks.”<sup>19</sup>

others take different or opposing views.

Some industry-owned incumbents believe that “the technology and the ledger should be industry-owned so that there is strong alignment with industry-wide needs and that opportunities are focused on benefitting the industry in the broadest manner possible.”<sup>20</sup>

Other key regulatory issues include whether blockchain technologies will be able to accommodate consumer protection issues in B2B/B2C interactions over a blockchain.

### Identity and data privacy issues

Blockchains do not recognise jurisdictional boundaries. They may be used to collect, store, process and transmit personal data. They may themselves also provide functionality for the “passporting” of identity for KYC, AML or other client onboarding purposes.

The identity use case chapter of this Guide examines the various data privacy issues that arise in relation to blockchains and personal data.

### Competition/anti-trust considerations

Blockchains could potentially give rise to competition/anti-trust issues in relation to a number of areas – for example:

- The gating effect for participating in a permissioned blockchain where this potentially excludes competitors.
- The adoption of technical standards that prevent participation by competitors.
- The risk of collusion among competitors involved in a blockchain.
- The exchange of commercially sensitive information between competitors participating in a blockchain.

The various competition/anti-trust issues relating to blockchain deployments are considered in detail in the competition/anti-trust chapter of this Guide.

---

<sup>18</sup> Lawrence Lessig, *Code and Other Laws of Cyberspace*, Version 2.0, New York: Basic Books, 2006.

<sup>19</sup> Deloitte, *Blockchain: Enigma. Paradox. Opportunity*, 2016, page 12.

<sup>20</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016, page 9.

## IP and IT issues

Blockchain technologies give rise to a number of intellectual property and IT issues which are considered in the IP and IT chapter of this Guide. Among the issues to be considered, the key intellectual property issues include:

- Patentability (or otherwise) of, or the use of trade secret protection in relation to, component parts of the technology making up a blockchain system (for example, algorithms, databases, software).
- Infringement risk associated with the use of the technology.
- Impact of the use of open source software in blockchain technologies.

Among the IT issues to be considered, the key IT issues include:

- The applicability of law regulating digital signatures.
- The legal effect of bugs in blockchain systems and in messages (transactions) or in the programmable logic included within a message or a block.
- Cyber security considerations.

## Litigation and dispute resolution

In order to be legally valid, the common law of many jurisdictions provides that a contract must be entered into by a legal person (a human or other legal entity) having legal capacity to do so. There is also common law authority (for example, in English law) to the effect that, for a contract to arise, there needs to be sufficient certainty over who the other contracting party actually is. Civil law jurisdictions may lay down other requirements. (These kinds of legal requirements are considered in detail in our publication, *Smart Contracts: Coding the Fine Print*.)

Legal requirements such as these can make disputes relating to blockchain technologies particularly problematic. For example:

- There may be no central administering authority to decide a dispute between participants, forcing the participants to seek recourse in the courts. There may simply be no obvious defendant against whom legal action could be brought. For example, who would be responsible for system operational defects, corrupted messages, or defective programme logic? A permissioned blockchain might include binding protocols for dispute resolution to address some of these issues.
- It may be unclear if a contract exists between participants if they seek legal redress for breach of contract in the courts.
- Even if there is no clear contract, a blockchain transaction may itself have an effect on property rights – for instance, if it is a register of legal ownership – and so any dispute would need to be resolved as between the rival claimants to those property rights.
- Transactions using blockchain technologies can be conducted pseudonymously. If a dispute arose, how would an aggrieved participant identify the other party in order to bring legal proceedings against it? Would a court regard a smart contract hosted on a blockchain as having legally binding effect if it is simply not possible to identify who the other contracting party to it is?
- Enforcement of a court judgment or arbitration award in respect of a transaction using blockchain technologies may be problematic.
- Even where dispute resolution mechanisms exist for blockchain technologies, there may be problems applying them beyond the “trust boundaries”, that is, where the blockchain technologies interact with third party systems.

These issues are examined in the litigation and dispute resolution chapter of this Guide.

## Tax

Blockchains perform “in the ether”. There may be no obvious place of performance. International allocation of taxing rights has traditionally focused on the place where contracts are concluded. Blockchain technologies will therefore present yet another challenge to traditional tax systems. A number of complex tax issues accordingly arise. For example:

- In jurisdictions where stamp taxes are payable, could the monitoring of whether stamp duty reserve tax (and other equivalent taxes, such as financial transaction tax) is payable be replicated within a blockchain?
- How do you determine who will be receiving fees for operating blockchain technologies for direct tax purposes?
- Jurisdictions are likely to want to impose sales taxes (like VAT and GST) on supplies of services of blockchain technologies. What sort of services are these and who are they supplied between?

The tax chapter of this Guide examines these and other tax issues.

## Insurance

As described above (see *Which Industry Sectors Might be Affected?*, on page 9), the insurance industry is considering a number of potential applications for blockchain technologies. The insurance use case chapter of this Guide examines the use case of blockchain technologies for insurance.

## Clearing and settlement

Clearing and settlement is thought to provide considerable scope for the adoption of blockchain technologies. The US Depository Trust & Clearing Corporation has, for example, proposed exploring its adoption of blockchain technologies for clearing and settlement services.<sup>21</sup> The clearing and settlement use case chapter of this Guide considers the use case of blockchain technologies for clearing and settlement.

## Securitisation and trade receivables finance

Another area where blockchain technologies are being evaluated is in relation to securitisation and trade receivables finance. The securitisation and trade receivables finance use case chapter of this Guide considers the use case of blockchain technologies for them.

## Supply chains

Among other things, the provenance of component parts of technology, pharmaceutical drugs, and medical devices is subject to increasing scrutiny and regulation. Blockchain technologies can be used to facilitate and record transactions down a supply chain. Supply chain management issues are considered in detail in the context of blockchain technologies in the supply chain management use case chapter of this Guide.

## DAOs

DAOs (decentralised autonomous organisations) rely on blockchain technologies. What is a DAO and how might one be used within an industry? What are the legal and regulatory implications of setting up a DAO or in interacting with one? These issues are examined in the DAOs use case chapter of this Guide.

<sup>21</sup> DTCC, *Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape*, January 2016.

## What are the implications for business?

---

In a recent poll, legal and regulatory requirements came second only to establishing a business case as the greatest challenge within the financial services sector for implementing blockchain technologies.<sup>22</sup> There is no reason to suppose other industries would take a different view.

“There are a lot of regulatory and consumer issues that will need to be discussed as the technology evolves.”

*Christopher Woolard, Financial Conduct Authority Director of Strategy and Competition, UK FinTech: Regulating for Innovation, www.fca.org.uk, 23 February 2016*

The legal and regulatory implications of blockchain technologies will therefore need to be analysed before deployment. Businesses proposing to use blockchain technologies would be well advised to obtain a regulatory and legal assessment for any deployment that is likely to pass the proof-of-concept phase.

Value creation remains key to investment decisions and successful commercialisation of the technology. Some blockchain solutions being proposed “are not sufficiently better than existing or alternative, already-feasible solutions.”<sup>23</sup> It is expected that potential investors in the technology, as well as businesses considering large-scale deployments, will become increasingly attuned to such considerations.

“One strategy that does offer certainty, however, is not advisable: sitting on the sidelines and waiting for others to pioneer this technology. Choosing that seemingly safer option merely raises the likelihood that when today’s risks have been resolved, it will be difficult to catch up with market leaders.”

*IBM Institute for Business Value, Empowering the Edge: Practical Insights on a Decentralised Internet of Things, 2015*

---

<sup>22</sup> DTCC Connection, *Blockchain Symposium Audience Poll*, 18 April 2016.

<sup>23</sup> Kwori Ltd, *Blockchains and Distributed Ledgers in 2016*, 2016.

## Glossary

---

<b>address</b>	an alphanumeric string constituting a participant's public key for encryption of messages
<b>block</b>	a message sent by a participant in a blockchain system that has been authenticated and verified by that system and consensus reached on it, and which has then been added (as a block) to the previous block in the chain of blocks. Blocks typically record transactions or the change in status of something
<b>blockchain</b>	a distributed ledger taking the form of an electronic database that is replicated on numerous nodes spread across an organisation, a country, multiple countries, or the entire world. Records in a blockchain are stored sequentially in time in the form of blocks. Each hash for a block depends on the block header for that block. The block header for that block contains a reference to the previous block in the chain. Accordingly there is a continuous chain back in time. In order to change one block in the chain it would be necessary to change every block that came after it
<b>block header</b>	a message or messages relating to a transaction are bundled together in a block and given title known as a block header. The block header is dependent on the combination of messages in the block. A block header lists the transaction(s), the time at which the list was made (that is, a time stamp), and a reference back to the most recent block
<b>consensus</b>	more than 50% of nodes conclude that a message is authenticated and verified, so that the message can be added as a block to a blockchain
<b>consensus protocol</b>	a computer protocol in the form of an algorithm constituting a set of rules for how each participant in a blockchain should process messages (say, a transaction of some sort) and how those participants should accept the processing done by other participants. The purpose of a consensus protocol is to achieve consensus between participants as to what a blockchain should contain at a given time (including by the addition of new blocks). Terms used to describe consensus protocols in the context of blockchain technologies include "proof of work" or "proof of stake"
<b>distributed ledger</b>	a collection of data (making up a database), an identical copy of which is held on numerous computers across an organisation, a country, multiple countries, or the entire world. A blockchain is a form of distributed ledger, but not all distributed ledgers are blockchains

---

<b>fork/forking</b>	occurs when participants in a blockchain system cannot immediately choose between two (or more) blocks upon which to continue the chain of blocks, so that two (or more) separate blocks are built on at the same time, creating a “fork” in the chain
<b>hash/hashing</b>	the process by which a grouping of digital data is converted into a single number, called a hash. The number is unique (effectively a “digital fingerprint” of the source data) and the source data cannot be reverse engineered and recovered from it. In the context of blockchain, what is hashed is the block header
<b>message</b>	a submission of data (typically a transaction) for processing by nodes with the object of having the message authenticated and verified and consensus reached in respect of it as a transaction record (so that it can be added as a block to a blockchain). Messages may act as inputs or outputs of computer programs, and may themselves contain or point to computer code
<b>node</b>	a single computer involved in processing a message in order to reach consensus. Nodes are connected to each other via the Internet
<b>off-chain transaction</b>	a transaction occurring outside a blockchain (for example, on a legacy system)
<b>peer-to-peer</b>	where participants to a network send information to one another without using an intermediary or central point
<b>permissioned</b>	a blockchain is permissioned where its participants are pre-selected or subject to gated entry on satisfaction of certain requirements or on approval by an administrator of the blockchain. A permissioned blockchain may use a consensus protocol for determining what the current state of a blockchain should be, or it may use an administrator or sub-group of participants to do so
<b>permissionless</b>	a blockchain is permissionless when anyone is free to submit messages for processing and/or be involved in the process of reaching consensus. While a permissionless blockchain will typically use a consensus protocol to determine what the current state of the blockchain should be, it could equally use some other process (such as using an administrator or sub-group of participants) to do so
<b>private key</b>	an instance of code, privately held, and paired with a public key to initiate algorithms for text encryption. A private key is created as part of public key cryptography during asymmetric key encryption

---

<b>public key</b>	an instance of code, available to anyone, paired with a private key to decrypt text as part of public key cryptography during asymmetric key encryption
<b>shared ledger</b>	another name for a distributed ledger or a blockchain
<b>smart contract</b>	smart contracts are made from software coding and have the ability to self-perform autonomously. Depending on a range of factors, they may sometimes amount to binding contracts in the legal sense or otherwise affect legal relations between parties. Smart contracts that are linked to blockchains could move value or information across blockchains
<b>time stamp</b>	a number representing a point in time at which something was created or done

---

## Contacts

---

### Asia



**Stella Cramer**  
**Partner, Singapore**  
Tel +65 6309 5349  
stella.cramer@nortonrosefulbright.com



**Barbara Li**  
**Partner, Beijing**  
Tel +86 10 6535 3130  
barbara.li@nortonrosefulbright.com

### Australia



**Warwick Andersen**  
**Special counsel, Sydney**  
Tel +61 2 9330 8050  
warwick.andersen@nortonrosefulbright.com



**Tessa Hoser**  
**Consultant, Sydney**  
Tel +61 2 9330 8083  
tessa.hoser@nortonrosefulbright.com

### Canada



**Anthony de Fazekas**  
**Partner, Lawyer, Patent Agent, Toronto**  
Tel +1 416 216 2452  
anthony.defazekas@nortonrosefulbright.com



**John Jason**  
**Of counsel, Toronto**  
Tel +1 416 216 2964  
john.jason@nortonrosefulbright.com

### Europe



**Imogen Garner**  
**Partner, London**  
44 20 7444 2440  
imogen.garner@nortonrosefulbright.com



**Sean Murphy**  
**Partner, London**  
Tel +44 20 7444 5039  
sean.murphy@nortonrosefulbright.com



**Floortje Nagelkerke**  
**Partner, Amsterdam**  
Tel +31 20 462 9426  
floortje.nagelkerke@nortonrosefulbright.com



**Jamie Nowak**  
**Partner, Munich**  
Tel +49 89 212148 0  
jamie.nowak@nortonrosefulbright.com



**Victoria Birch**  
**Of Counsel, London**  
Tel +44 20 7444 2124  
victoria.birch@nortonrosefulbright.com



**Michael Sinclair**  
**Consultant, London**  
Tel +44 20 7444 2344  
michaelsinclair@nortonrosefulbright.com



---

## Latin America



**Ramón Ignacio Andrade Monagas**  
Partner, Caracas  
Tel +58 212 276 0014  
ramon.andrade@nortonrosefulbright.com

---

## United States



**Ronald Smith**  
Partner, Dallas  
Tel +1 214 855 8349  
ron.smith@nortonrosefulbright.com

---

## South Africa



**Rohan Isaacs**  
Director, Johannesburg  
Tel +27 11 685 8871  
rohan.isaacs@nortonrosefulbright.com



**Susan Linda Ross**  
Senior counsel, New York  
Tel +1 212 318 3280  
susan.ross@nortonrosefulbright.com



**Nerushka Deosaran**  
Associate, Johannesburg  
Tel +27 11 685 8691  
nerushka.deosaran@nortonrosefulbright.com



**Kathleen A. Scott**  
Senior counsel, New York  
Tel +1 212 318 3084  
kathleen.scott@nortonrosefulbright.com

# Global resources



📍 Our office locations

## People worldwide

7400

## Legal staff worldwide

3800+

## Offices

50+

## Key industry strengths

Financial institutions

Energy

Infrastructure, mining and commodities

Transport

Technology and innovation

Life sciences and healthcare

## Europe

Amsterdam

Athens

Brussels

Frankfurt

Hamburg

London

Milan

Moscow

Munich

Paris

Piraeus

Warsaw

## United States

Austin

Dallas

Denver

Houston

Los Angeles

Minneapolis

New York

Pittsburgh-

Southpointe

St Louis

San Antonio

Washington DC

## Canada

Calgary

Montréal

Ottawa

Québec

Toronto

## Latin America

Bogotá

Caracas

Rio de Janeiro

## Asia

Bangkok

Beijing

Hong Kong

Jakarta<sup>1</sup>

Shanghai

Singapore

Tokyo

## Australia

Brisbane

Melbourne

Perth

Sydney

## Africa

Bujumbura<sup>3</sup>

Cape Town

Casablanca

Dar es Salaam

Durban

Harare<sup>3</sup>

Johannesburg

Kampala<sup>3</sup>

## Middle East

Abu Dhabi

Bahrain

Dubai

Riyadh<sup>2</sup>

## Central Asia

Almaty

<sup>1</sup> TNB & Partners in association with Norton Rose Fulbright Australia

<sup>2</sup> Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright (Middle East) LLP

<sup>3</sup> Alliances

# Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to 'Norton Rose Fulbright', 'the law firm', and 'legal practice' are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together 'Norton Rose Fulbright entity/entities'). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a 'partner') accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity. The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

