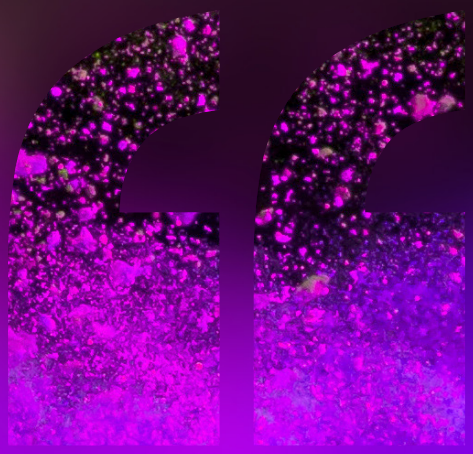
CLIFFORD
CHANCE



# BLOCKCHAIN
## WHAT IT IS AND WHY IT'S IMPORTANT

**— THOUGHT LEADERSHIP**

APRIL 2018

# BLOCKCHAIN

## WHAT IT IS AND WHY IT'S IMPORTANT

Blockchain is the technology that underpins the digital currency Bitcoin – but it has far wider applications and is being commercialised in a growing number of areas. It has generated much interest in technology circles and beyond, because of the new possibilities it opens up in financial services, the public sector and other areas.

Blockchain and Bitcoin are not the same thing – Bitcoin is implemented using blockchain technology, but blockchain technology can be used in contexts much wider than Bitcoin or cryptocurrencies. The term blockchain refers to the combination of a number of technologies, including:

- The blockchain data structure.
- Public key cryptography.
- Distributed ledgers.
- Consensus mechanisms.

### The blockchain data structure

A blockchain is a special type of data structure (ie a database), in which the data is set out and built up in successive blocks. Each of the blocks of data includes a small piece of data that verifies the content of the previous block. As a result, if an attempt is made to modify an earlier block in the chain, all of the later blocks cease to match up. Imagine that the database looks like a tower of Lego pieces which follow a particular sequence red-green-green-blue-yellow-red. If a change is made to the second block, the rest of the sequence upwards from the second block will change and become, say, red-black-brown-orange-purple-pink. The system that maintains the blockchain will be able to detect and reject the attempted modification, and this is what makes the blockchain tamper-proof.

### Public key cryptography

The use of public key cryptography ensures that each participant in the system is uniquely identified and can validate any change to the blockchain using a cryptographically secure private key. While public key cryptography is not unique to blockchain, it is one of the essential underlying technologies which ensure that blockchains are secure and that only authorised participants can make changes to a blockchain. It can also be used to encrypt data stored on the blockchain so that the data can only be accessed by those with the key to decrypt it.

### Distributed ledgers

Traditional ledger systems either require each participant to maintain its own decentralised ledger or they require the participants to trust a centralised ledger. The problem with decentralised ledgers is that they can be costly to maintain and to keep secure, and it may not become immediately apparent when they diverge – until a transaction down the line reveals that each ledger in fact records a different version of the facts. A centralised ledger, on the other hand, requires all the parties to trust the holder of the authoritative central ledger and creates a critical vulnerability – what happens if the central ledger is hacked or a disgruntled employee deletes it? The key to a distributed ledger is that each authorised participant (a node) maintains a complete version of the ledger and each transaction, ie each proposal to modify the ledger, is sent out to all of the nodes and is only approved if a sufficient number of nodes agree that it is a valid transaction.

## Consensus mechanisms

This validation of proposed changes to the blockchain is performed by the nodes in accordance with certain pre-set rules whereby the nodes will reach a consensus as to whether the new data entry will be permitted (eg, the nodes might conduct a check to confirm that according to the records on the blockchain, the participant purporting to conduct a particular transaction owns the relevant asset which is the subject of that transaction). This is the consensus mechanism and only if there is agreement between the nodes as to the validity of the transaction represented by that data entry will that data entry be permitted to be appended to the blockchain (ie another Lego block will be added to the tower). Once that transaction has been approved, however, the updated version of the blockchain with the newly-appended entry will rapidly spread throughout the system, so that that all of the nodes end up with an identical version of the ledger.

This consensus mechanism means that there is a rigorous means, applied uniformly by all participants, that ensures that only valid data can be appended to the blockchain. It is the consensus mechanism that enables the gate-keeping function to be entrusted to a network of participants, rather than a single central authority.

## Why is blockchain technology relevant?

In the early days blockchain technologies first captured the imagination of Bitcoin and cryptocurrency enthusiasts – often of a techno-utopian and libertarian persuasion – the versatility of the technology means that it is now being embraced, at least experimentally, by more established sectors of the economy.

Compared with traditional database technologies and centralised systems, blockchain implementations can be relatively cheap and require considerably less IT investment to maintain. However, as the technology is still relatively immature, for the time being these savings on the ongoing operational costs may be offset by significant upfront development costs.

Because of its application to ledger technologies, blockchain has generated particular interest from the financial sector. Initiatives have included bank-specific cryptocurrencies modelled on Bitcoin and self-executing smart contracts that can automatically implement certain types of simple financial contracts. One of the most high-profile initiatives in this space has been R3, a consortium of over 70 financial institutions launched in September 2015 and dedicated to developing blockchain technologies for use in the financial sector.

Because of its application in creating resilient, tamper-proof distributed records, a number of initiatives have been proposed in the public sector for government-maintained registries to be implemented as blockchains, eg real estate title registries in Honduras and Sweden and the aid/public interest sector, eg blockchain-based tracing of donations from donor to recipient to ensure the money goes where it is needed.

Enthusiasm for blockchain has not abated among technologists, who have continued to push the boundaries of blockchain technology. The same self-executing smart contracts technology (mentioned above) that financial institutions have been cautiously exploring, has been taken much further by blockchain pioneers. May 2016 saw the launch of the DAO (Decentralized Autonomous Organization) which was effectively an autonomous crowd-sourced venture capital fund implemented by way of smart contracts, without recourse to traditional legal structures. An exploit that enabled one of the participants to extract a large part of the funds resulted in the DAO's prompt demise, but the ambitious project demonstrated the potential of blockchain technologies.

## What legal issues does blockchain present?

- **Real world vs blockchain.**
  Where the blockchain is used as a ledger for tokenised real-world assets, what happens if a transaction, such as a transfer of an asset, is recorded on the blockchain by means of a technological process but fails as a matter of law? For a given application, is it possible to create a consensus mechanism that is legally watertight, so that a transaction on the blockchain always moves in lockstep with a valid legal transaction?
- **What goes on the blockchain?**
  Distributed consensus technologies involve the sharing of detailed information on transactions. While access can be implemented in such a way that certain information is only available to certain parties, the shared nature of the blockchain gives rise to a range of issues around information sharing, from questions of confidentiality to cyber-security to data protection.
- **Antitrust.**
  From an antitrust perspective, how much information are participants, who may be competitors, sharing with each other on the blockchain, and could the consensus mechanism have any hidden anti-competitive effects?
- **Should blockchains be regulated?**
  As the new technology emerges and changes the way parties transact, especially in the financial sector, regulators will want to monitor the development of blockchain technologies to ensure the assumptions current regulations are based on have not been superseded.
- **Intellectual property.**
  The basic building blocks of blockchain technology are open source, but those building on top of the founding technologies may want to protect their innovations through patenting and licensing their proprietary technology.
- **Cryptocurrencies.**
  Cryptocurrencies like Bitcoin raise a range of issues of their own, in particular whether they constitute currencies or legal tender at all, and what consequences this has for transactions conducted using a cryptocurrency rather than a traditional currency (eg are cryptocurrency transactions subject to VAT?).
- **Smart contracts.**
  Smart contracts, being self-executing electronic contracts, raise some important issues as to whether they constitute legal contracts at all. The promise of fast, cheap and reliable electronic contracting to replace slow and expensive paper-based contracts has attracted a lot of interest. Early implementations are focusing on simple contracts in well-defined and already largely automated contexts such as simple financial contracts.

## Glossary

- **Bitcoin:** the first successful cryptocurrency and implementation of blockchain, launched in 2009.
- **Blockchain:** the technology underlying Bitcoin and key to implementing distributed ledger technologies. "A blockchain" means a particular instance of the chained data structure that defines the technology, which is typically replicated across multiple nodes or computers.
- **Consensus mechanism:** the consensus mechanism is the body of rules according to which each node in a network validates or rejects any proposed change to the blockchain it administers.
- **Cryptocurrency:** a digital currency implemented by way of cryptographically secure protocols, typically based on blockchain technology. The first successful cryptocurrency was Bitcoin, which has been followed by many imitations and variations.
- **DLT (Distributed Ledger Technology):** a blockchain-based technology for sharing an electronic ledger between multiple participants in such a way as to ensure that the ledger is secure, tamper-proof, and that all of the parties hold an identical copy of the ledger (give or take, momentarily, the very latest additions to the ledger).
- **Distributed consensus:** a distributed consensus is any record of a state of affairs (eg a ledger of transactions) that is electronically shared in identical form by multiple participants.
- **Hash:** a hash is a type of function that converts a piece of data of any length into a short, meaningless string of data. The slightest change to the input completely changes the output of the hash function. Unlike encryption, the hash cannot be reversed to obtain the source information. This enables verification of information without sharing: if the hash of certain data is recorded on a blockchain, I can check I have the same data by comparing the hash, without ever seeing the original source data held by the other party.
- **Hash pointer:** the hash function (above) is also used in blockchains to tie each link of the chain to the previous one: each block of data in the blockchain contains a hash of the previous block, called a hash pointer. Because any change in the input changes the output, any change to the previous block would result in a different hash pointer, and so on with each successive block, which is what makes blockchain tamper-proof (see below).
- **Node:** blockchains are maintained by a network of computers which are authorised to maintain a copy of the blockchain and to validate and implement updates to the blockchain. Each such authorised computer is a node of the network.
- **Permissioned vs permissionless ledgers:** a permissioned ledger is one where only certain authorised parties are allowed to act as a node and administer the ledger. This is the case of most financial sector blockchain initiatives, such as R3's Corda. Bitcoin, on the other hand, uses a permissionless ledger: anyone can download the software onto their computer and set themselves up as a node.
- **Private key:** in public key cryptography, the private key is a unique piece of data that is kept secret and enables the holder to decrypt any message that has been encrypted with the corresponding public key.
- **Public key:** in public key cryptography, the public key is a unique piece of data that can be shared with anyone and will enable that person securely to encrypt a message, but not to decrypt it.
- **Smart contract:** an electronic, self-executing contract. The emergence of blockchain technologies has given rise to a new generation of electronic contracts that are based on distributed ledger technologies and are executed by a network of nodes.
- **Tamper-proof:** describes a data structure that cannot be tampered with without this becoming obvious to the administrator of the structure. In the case of blockchain, this is achieved by the chain structure of successive blocks, where tampering with any individual block creates a mismatch with all subsequent blocks (implemented by means of a hash pointer – see above).
- **Tokenised asset:** a tokenised asset is a real-world asset (eg a real estate title or an amount of currency) that is represented by a "token" on an electronic ledger, such as a blockchain.

# YOUR GLOBAL BLOCKCHAIN CONTACTS

## Amsterdam

**Marian Scheele**
**Senior Counsel**
T: +31 20711 9524
E: marian.scheele@cliffordchance.com

## Beijing

**Hong Zhang**
**Counsel**
T: +86 106535 2256
E: hong.zhang@cliffordchance.com

## Dubai

**Jack Hardman**
**Senior Associate**
T: +971 4503 2712
E: jack.hardman@cliffordchance.com

## Frankfurt

**Dr. Marc Benzler**
**Partner**
T: +49 697199 3304
E: marc.benzler@cliffordchance.com

## Hong Kong

**Oliver Kronat**
**Partner**
T: +49 697199 4575
E: oliver.kronat@cliffordchance.com

**Francis Edwards**
**Partner**
T: +852 2826 3453
E: francis.edwards@cliffordchance.com

**Mark Shipman**
**Partner**
T: +852 2825 8992
E: mark.shipman@cliffordchance.com

**Brian Harley**
**Registered Foreign Lawyer**
T: +44 20 7006 2412
E: brian.harley@cliffordchance.com

## London

**Rocky Mui**
**Senior Associate**
T: +852 2826 3481
E: rocky.mui@cliffordchance.com

**Kate Gibbons**
**Partner**
T: +44 20 7006 2544
E: kate.gibbons@cliffordchance.com

**Jonathan Kewley**
**Partner**
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

**Stephen Reese**
**Partner**
T: +44 20 7006 2810
E: stephen.reese@cliffordchance.com

## Luxembourg

**Peter Chapman**
**Senior Associate**
T: +44 20 7006 1896
E: peter.chapman@cliffordchance.com

**Laura Nixon**
**Senior Associate**
T: +44 20 7006 8385
E: laura.nixon@cliffordchance.com

## Madrid

**Steve Jacoby**
**Partner**
T: +352 485050 219
E: steve.jacoby@cliffordchance.com

**Eduardo García**
**Partner**
T: +34 91590 9411
E: eduardo.garcia@cliffordchance.com

## New York

**David Felsenthal**
**Partner**
T: +1 212 878 3452
E: david.felsenthal@
cliffordchance.com

**Allein Sabel**
**Associate**
T: +1 212 878 3371
E: allein.sabel@
cliffordchance.com

**Alice Kane**
**Counsel**
T: +1 212 878 8110
E: alice.kane@
cliffordchance.com

**Nicholas R. Williams**
**Partner**
T: +1 212 878 8010
E: nick.williams@
cliffordchance.com

## Paris

**Frédérick Lacroix**
**Partner**
T: +33 14405 5241
E: frederick.lacroix@
cliffordchance.com

**Sébastien Praicheux**
**Counsel**
T: +33 14405 5156
E: sebastien.praicheux@
cliffordchance.com

## Singapore

**Paul Landless**
**Partner**
T: +65 6410 2235
E: paul.landless@
cliffordchance.com

**Lena Ng**
**Partner**
T: +65 6410 2215
E: lena.ng@
cliffordchance.com

## Sydney

**Lijun Chui**
**Senior Associate**
T: +65 6506 2752
E: lijun.chui@
cliffordchance.com

**Lance Sacks**
**Partner**
T: +61 28922 8005
E: lance.sacks@
cliffordchance.com

**Alastair Gourlay**
**Counsel**
T: +61 28922 8043
E: alastair.gourlay@
cliffordchance.com

## Washington, D.C.

**Megan Gordon**
**Partner**
T: +1 202 912 5021
E: megan.gordon@
cliffordchance.com

CLIFFORD

CHANCE



www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ



Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571
Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications.



Abu Dhabi • Amsterdam
Barcelona • Beijing • Brussels
Bucharest • Casablanca • Dubai
Düsseldorf • Frankfurt • Hong Kong
Istanbul • London • Luxembourg
Madrid • Milan • Moscow • Munich
New York • Paris • Perth • Prague
Rome • São Paulo • Seoul • Shanghai
Singapore • Sydney • Tokyo • Warsaw
Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

J20170706171611