Baker McKenzie.

# UNHASHING BLOCKCHAIN

## Blockchain Explained

Have you heard of blockchain but aren't really sure what it is, what it can do, and what the legal issues might be?

In this introduction to blockchain, we put this fascinating new technology into context and provide an overview of the technology, how it is being used and the potential legal issues.

Baker McKenzie.


## Hype or Hero?

Blockchain rose to fame as the technology underpinning bitcoin, but its promise goes much further.

Blockchain enthusiasts believe that the technology has the potential to be the most transformative technology since the internet. Sceptics argue that it's a "solution looking for a problem".

Whichever camp you sit in, it's clear that this technology has drawn significant interest from companies who have identified blockchain's potential to transform business processes. In addition, blockchain is being closely monitored by regulators around the world, who recognise blockchain's potential opportunities, plus the risks and challenges.

## What is blockchain?

Blockchain is a peer-to-peer, decentralised, immutable and distributed ledger which consists of validated blocks of data that are linked in a time sequenced chain.

Imagine a spreadsheet which is not operated by one central party, but by a network of computers (each, a "node") which verify and time stamp each entry. This spreadsheet then contains a complete audit trail of all transactions conducted over the network.

## Bitcoin example

In order to see how this technology works in practice, let's look at the best known blockchain.

Historically, in order to make an online payment you would rely on a trusted third party (e.g. a bank) to process your transaction. That third party would confirm whether you had sufficient funds to make the transaction, as well as providing a secure pathway for the transaction to take place.

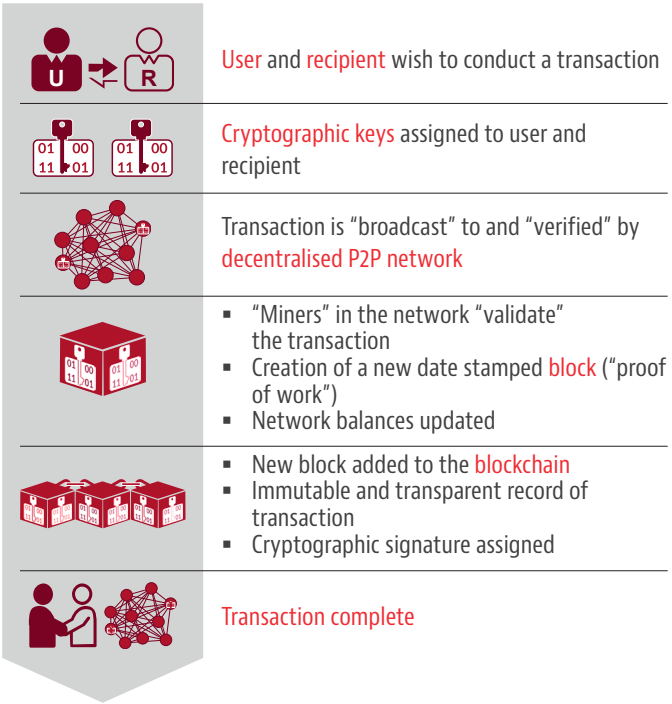
The idea behind bitcoin was, in effect, to enable banking without banks.

The bitcoin blockchain sits on top of the Internet, like the Web. By using blockchain, bitcoin is able to use the distributed ledger as a record of all bitcoin transactions. When someone wants to make a transaction, the bitcoin blockchain can review the person's transaction history to calculate whether, at that point in time, they have sufficient funds. There is, therefore, no need for a third party to check the person's account.

The integrity and transaction history of the ledger are enforced with cryptography. Each new bitcoin transaction is transmitted to the nodes in the network and must be validated by the network solving a cryptographic problem.

Each transaction block added to the ledger contains a representation (hash value) of every previous block - which creates a chain of blocks (hence, the "blockchain").

The use of encryption and the distributed nature of the ledger makes it very secure. Once a block is validated, it's virtually impossible to change.




User and recipient wish to conduct a transaction

Cryptographic keys assigned to user and recipient

Transaction is "broadcast" to and "verified" by decentralised P2P network

- "Miners" in the network "validate" the transaction
- Creation of a new date stamped block ("proof of work")
- Network balances updated

- New block added to the blockchain
- Immutable and transparent record of transaction
- Cryptographic signature assigned

Transaction complete

That is a very simplified explanation of a complex technology. Ultimately, it's important to recognise that there is currently a lot of focus on how blockchain works largely because its deployment is immature. Once blockchain matures, the technology is likely to become less visible - instead we will concentrate on what it enables. Think to yourself - do you know how the internet works, how your smart phone works? Perhaps not, but you know what you use them for!

However, if you **are** keen to understand blockchain in more technical detail, please see our **Glossary - an A-Z of Blockchain.**

## Key benefits of blockchain

Indeed, rather than focus on the technology, it can be more productive to focus on the perceived benefits. These include:

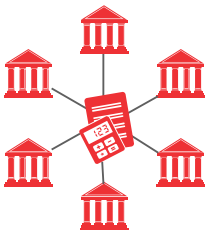
- **Decentralised** - the ledger is not controlled by one gatekeeper. It's distributed, which means that it's more secure as there is no single point of failure.
- **Peer to peer** - blockchain enables transactions without the need for a third party intermediary. The required trust is provided by the network and the technology.
- **Secure** - the blockchain provides for a record of transactions which is very difficult to tamper with. In effect, the platform is protected from attack provided that honest nodes collectively control more power than any cooperating group of attacker nodes.
- **Transparency** - every transaction is recorded in the ledger and (except in a permissioned network where the blockchain technology may place restrictions on the data that is made available to each participant) all participants have access to the transaction information.

## Models of blockchain

It's also important to bear in mind that when we refer to blockchain, there is not one blockchain technology. There are various blockchains or blockchain-like distributed ledger technologies (DLT).

In addition, it's important to understand that there are different models of blockchain/DLT.

In particular, blockchain models may be "permissioned" or "permissionless" (or a hybrid). "Permissionless" means that all computers can access, submit and be selected to finalise transactions into the ledger. Bitcoin is an example of a permissionless, or public, ledger. By way of analogy, think of the internet - available to anyone who has a computer and connectivity.

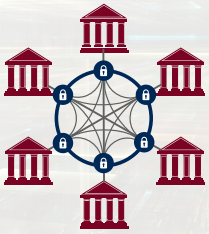


**Model 1**
**Current system**

A centralised system

**Model 2**
**Public blockchain**

An open network that anybody can access. The digital ledger of transactions is shared, transparent and run by all participants



**Model 3**
**Permissioned blockchain**

The preferred option of most regulated entities. It is a system which controls access to certain invited participants.

Click here to access our Glossary: An A-Z of Blockchain

On the other hand, we also have 'permissioned' ledgers. "Permissioned" means a DLT system where only pre-authorised computers can access and finalise transactions in a ledger. By way of analogy, think of an intranet - a private network which controls access to certain invited participants. Unsurprisingly, given confidentiality and regulatory concerns, the permissioned network tends to be the preferred option of most regulated entities and major enterprises.

Some permissioned blockchains are private to a organisation, others are federated or consortium blockchains and involve a group of participants.

## Smart Contracts

Many use cases for blockchain rely on Smart Contract technology which enables the automation of transactions via decentralised apps that sit on top of the ledger. The term "Smart Contract" is rather a misnomer. A Smart Contract is not a contract in the traditional legal sense. Rather, 'Smart Contracts' are programmable transactions - computer code that acts as an execution mechanism. When certain conditions are met, the protocols automatically execute a set of instructions.

> ...'Smart Contracts' are programmable transactions - computer code that acts as an execution mechanism.

## Use Cases - Beyond FinTech

Given its connection with bitcoin, it was unsurprising that the financial services sector was one of the first sectors to explore the potential of blockchain. However, the technology is now being evaluated in a whole host of sectors (including pharma, energy, creative services, real estate and retail). Indeed, it's the technology's flexibility that has led to the claim that it will revolutionise the way we do business.

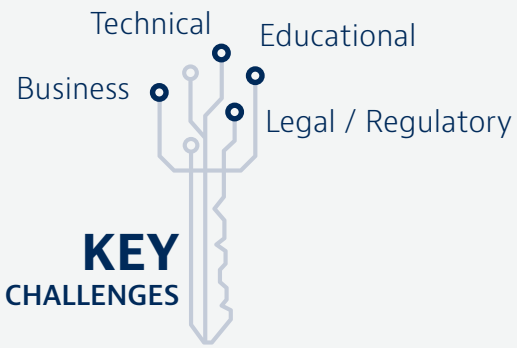
Although the use cases can differ across industries, there are common themes such as reconciliation, trading and supply chain (e.g. business processes where the removal of third party intermediaries could result in significant time and cost efficiencies).

### Applications across industries


### Nature

- Payments
- Reconciliation
- Trading
- Registers
- Supply chain
- Record keeping
- Provenance
- Asset management
- Identity
- Compliance
- Fraud prevention
- Automation

## Blockchain Challenges




Of course, blockchain also has its challenges. Again, these are likely to differ depending on the nature of the technology and model, but will include technical, business, educational and legal concerns.

Challenges with the bitcoin blockchain include scalability and environmental concerns. Challenges with a permissioned blockchain may include increased security risks. There are other challenges inhibiting blockchain adoption in the enterprise, not least interoperability concerns, a limited pool of technical expertise, and more generally a lack of awareness and understanding of the technology and/or a mindset that is reluctant to move away from the traditional way of doing things.

> ...it's the technology's flexibility that has led to the claim that it will revolutionise the way we do business.

## Blockchain and the Law

To date, there have been limited blockchain legal and regulatory developments globally. This is not particularly surprising. Firstly, it's common for the law to play catch-up to new technology. Secondly, we don't tend to regulate technology; we regulate outcomes. Ideally, regulation should be technology neutral so that it is a future-proof as possible.

In any case, given the variety of potential use cases and models, what would a "blockchain law" look like and who would regulate it?

A few jurisdictions have introduced new laws or regulatory guidance concerning blockchain. Generally speaking, this has been where regulators had particular concerns about consumer / investor protection or money laudering risks (e.g., in the context of cryptocurrency and ICOs), or, arguably, where particular territories want to demonstrate that they have a favourable regulatory regime in order to attract blockchain start-ups.

However, generally speaking, most regulators have wanted to avoid regulating too early and have taken a "wait and see" approach.

But this lack of new law or regulation does not mean that there is no law or regulation affecting blockchain. In each case, organisations wishing to deploy blockchain solutions will need to apply existing law (whilst keeping a close eye out for legal developments).

## Potential Legal Issues

Accordingly, what are the key legal issues that you need to consider when embarking on a blockchain project?

The short answer is "it depends". There is no one size fits all approach. There are various legal issues that could be relevant. But whether these issues are key concerns for your particular project will depend on the use case, the technology and the model being used. These factors will drive the relevant legal risks.

### Issues which could be relevant include:

- Data privacy
- Governing law and jurisdiction
- Who would regulate?
- Regulatory compliance
- Contract law
- Consumer protection
- Competition law
- Corporate law
- Securities law
- Intellectual property
- Dispute resolution
- Tax

For example, data protection is often raised as a key issue because there seems to be a fundamental clash between blockchain's immutable nature and the so-called 'right to be forgotten' under GDPR. Other data protection principles such as storage limitation and data minimisation also appear to conflict with this technology which includes a complete transaction history.

Now, it's certainly true that data protection is a potential thorny topic when the blockchain use case involves personal data.

But, of course, there are many blockchain use cases that don't involve personal data. Data privacy will be a key issue in an AML/KYC use case, but is not likely to be a key concern, for example, when you are using blockchain to track aircraft parts through their supply chain life-cycle.

In addition, the type of technology and whether the blockchain is a permissioned or permissionless system will impact your analysis. In particular, in a permissioned blockchain system, many of the key legal issues can be dealt with upfront in the participating agreements or in the platform rules agreed among participants. However, in a permissionless blockchain, dealing with these issues will be much more complex. How do you identify the applicable governing law and jurisdiction, who the law applies to, who would regulate, what happens if something goes wrong? In the case of data protection, who will be considered the data controller and who will be the data processor? Existing law doesn't envisage a decentralised system.

Please see our series **Blockchain In the Real World** for a more detailed consideration of certain blockchain use cases and some of the legal issues that you will need to consider in the context of your blockchain projects.

## Blockchain at Baker McKenzie

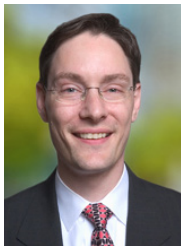
Our initial engagement with blockchain technologies arose primarily in a FinTech context, providing structuring, regulatory, technology and strategic advice for our clients, including large financial institutions and major global technology players. Much of this activity focused on the replacement of traditional intermediary structures with distributed models, across verticals such as payments, banking, InsurTech and wealth management. However, our global multi-disciplinary team, with local blockchain clusters, are now advising across all major industry verticals and have become increasingly involved in enterprise projects beyond the financial services sector, involving a range of use cases including supply chain management, energy, international trade, provenance and asset management systems, and IP and creative content implementation systems. We are also advising clients on projects relating to crypto-assets and tokenization, including token sales.

## If you would like to learn more about blockchain, please contact a member of our Blockchain Group.


**SUE MCLEAN**
Partner, Technology
London
sue.mclean
@bakermckenzie.com
020 7919 1998

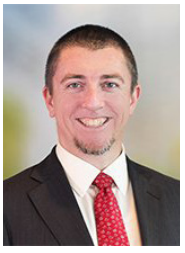
**MAARTEN HOELEN**
Partner, Tax
Amsterdam
maarten.hoelen
@bakermckenzie.com
+312 0551 7822

**MANUEL MEYER**
Partner, M&A
Zurich
manuel.meyer
@bakermckenzie.com
+414 4384 1465



**SAM KRAMER**
Partner, Technology
Chicago
samuel.kramer
@bakermckenzie.com
+1 312 861 7960

**DAVID ZASLOWSKY**
Partner, Litigation
New York
david.zaslowsky
@bakermckenzie.com
+1 212 891 3518



**GAVIN RAFTERY**
Partner, Banking & Finance
Tokyo
gavin.raftery
@bakermckenzie.com
+81 3 6271 9454

**STEPHANIE MAGNUS**
Partner, Financial Services
Singapore
stephanie.magnus
@bakermckenzie.com
+65 6434 2672

**ADRIAN LAWRENCE**
Partner, Technology
Sydney
adrian.lawrence
@bakermckenzie.com
+61 2 8922 5204