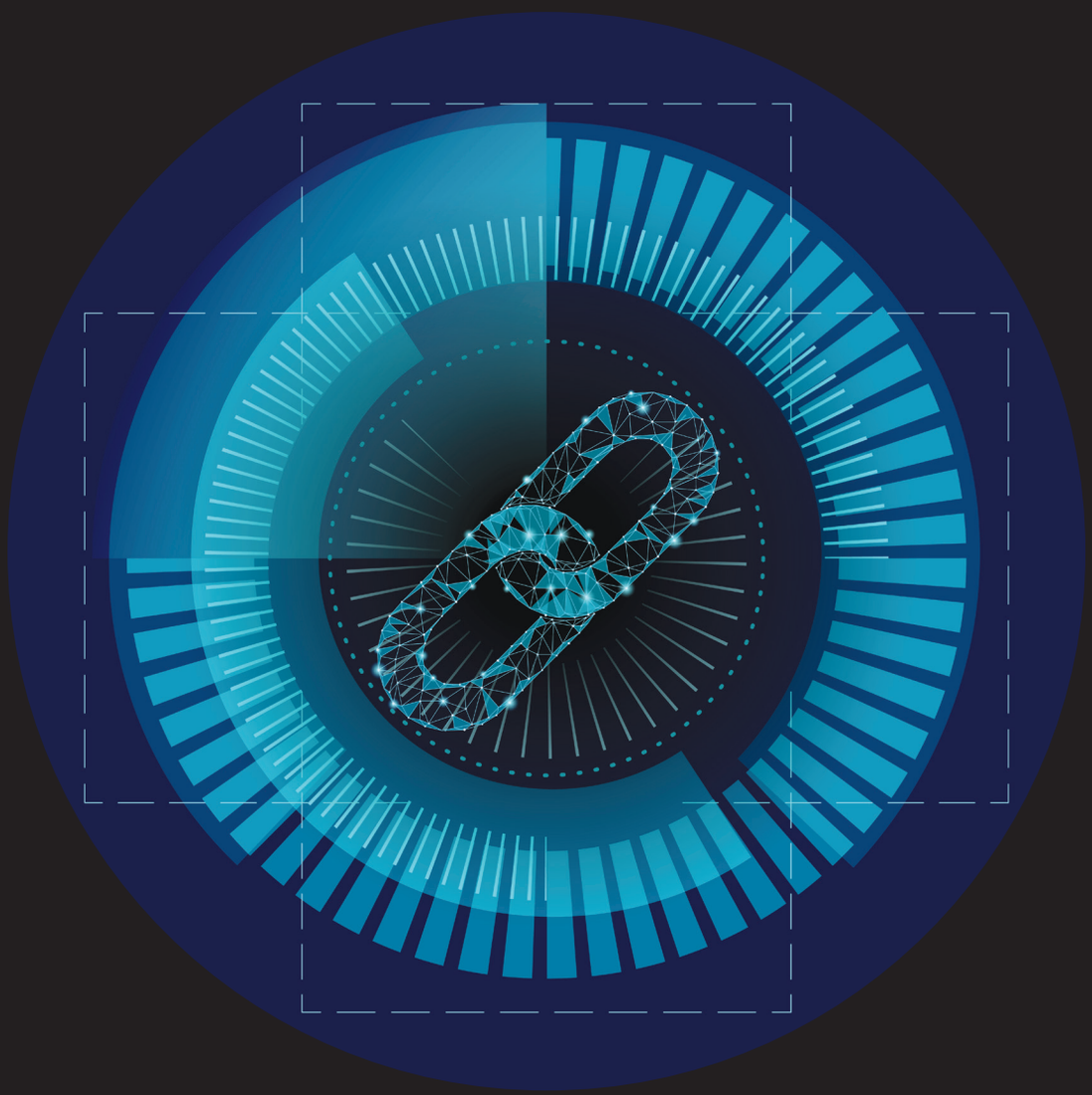
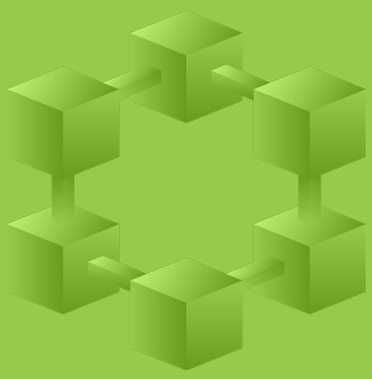
Deloitte.
Legal



Blockchain

Legal implications, questions, opportunities and risks

March 2018



Blockchain is increasingly in the news, but still primarily as the underlying software used for cryptocurrencies such as Bitcoin. Many businesses have yet to realize its potential and the extensive ways in which blockchain can be used to make processes more efficient or to develop new service offerings, but momentum is gathering as its applications are more widely understood.

Decentralized technologies such as blockchain are expected to be the next big wave, comparable in many people's eyes to the transformation that followed the development of the Internet, so a basic understanding blockchain is essential.

However, users need to be very clear about the legal implications, risks and opportunities that blockchain presents, as well as its relative immaturity and current technological limitations, including capacity.

Contents

What is blockchain?

At its simplest, blockchain involves recording information in a way that creates trust in the information recorded. The blockchain software is used to synchronize data stored in a distributed manner amongst peers on all the computers or servers ("nodes") participating in a particular network. This allows for multiple records of identical data. Trust is created because all the nodes in the network control, check and consent to any additions or changes to what is recorded. Blockchain can be used for record keeping, transferring value (via cryptocurrencies or otherwise) and smart contracts to automatically execute a transaction when one or more preconditions is met.

Once stored on the blockchain, the data cannot be manipulated or changed – it is immutable. Every block contains a unique summary of the previous block in the form of a secure hash value – think of the way a jigsaw puzzle pieces fit together. And because each block is connected, the timing, order and content of transactions cannot be altered and blocks cannot be replaced unless all the nodes agree with the proposed change.

At its simplest, blockchain involves recording information in a way that creates trust in the information recorded.

Immutability

As a distributed ledger containing immutable data, a blockchain can be trusted as a single source of truth. But what does immutability mean in practice? That the piece of information was included in the blockchain at some verifiable point in the past – not necessarily that the information is correct. The garbage-in, garbage-out principal is as applicable here as with any other process, the difference being that we cannot go back and correct the mistake. It can only be corrected by adding another block to the chain with the consent of all the participants.

A blockchain records tangible and intangible assets and obligations between a network of peers using the same software, algorithms and cryptography to maintain the records. These assets and obligations can then be transferred between participants with the consent of all other nodes. A blockchain allows participants to share data and code without the need for intermediaries to operate or maintain the service. All parties share the same data, which is replicated across all the nodes in the network. The records included in the blockchain are immutable (even if they are wrong) and provide an unchangeable, timestamped audit trail.

Permissioned vs. permissionless

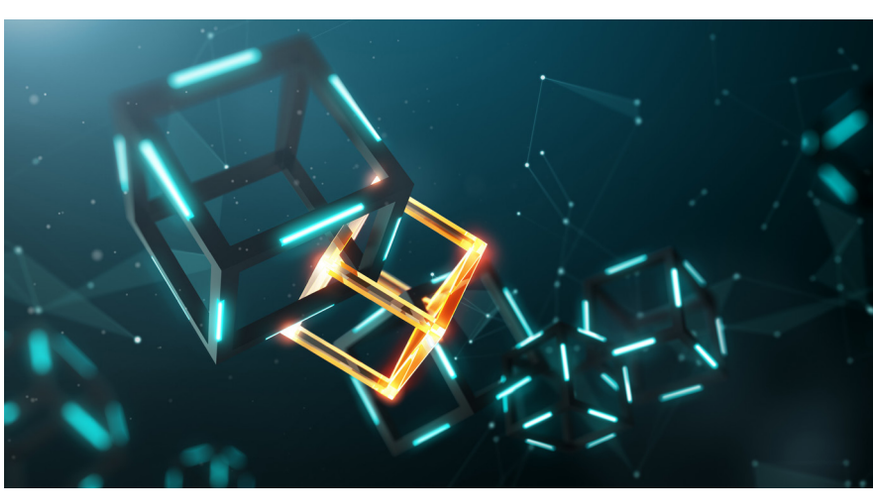
There are two types of blockchain: permissionless (in which anyone can participate) and permissioned (in which a participant has to be approved in order to participate). This might be to protect the privacy or trade secrets of those involved or to ensure compliance with regulations, such as those designed to prevent money laundering or financing of terrorism. Permissionless blockchains are public; participants use pseudonyms to protect their identity and there is no identification or authentication of participants. Permissioned blockchains are private and protected by access control and (potentially) different reading and writing privileges. Participants are known, identified and authenticated and the network may be controlled by a super-user. Authentication and identification use highly secure cryptography. Permissionless blockchains are generally considered to be more reliable because the consensus principle works better the more participants there are in the network. In a permissioned blockchain with a super-user there is a greater risk of manipulation.

Applications

There are various uses enabled by blockchain software. These include tokenization to protect sensitive data; timestamping because of blockchain's immutability; serving as a payment channel that enables the transfer of assets and liabilities; and, as discussed below, facilitating smart contracts, which is of greatest interest to lawyers.

Bblockchain technology has been used either to render processes more efficient by replacing existing components or to provide a new service using blockchain as its backbone. The most obvious example of this is the much-discussed cryptocurrencies. However, its use is being explored across a range of industries, including aviation (where smart contracts are easing clearing between airlines), ticket agents and banks, mining (to create a blockchain-based virtual marketplace), transport (with virtual passports for locomotives), oil and gas (to monitor good corporate governance of affiliates and financial services in a variety of ways, from clearing to loyalty programs). The Russian central bank has commissioned the creation of a permissioned blockchain for the banking industry to facilitate transactions in a trusted environment.

Blockchain is considered disruptive because it is transparent and eliminates the need for intermediaries and other third parties while being both safe (in terms of security and trust) and cost efficient (thanks to disintermediation). However, each of these characteristics is open to challenge – can a network be said to be transparent when its participants hide behind pseudonyms? Until law and regulation catches up, some transactions are impossible without the involvement of a third party to validate or perfect the transaction. Coding flaws may compromise the safety of a blockchain, and cost efficiency is open to question when the volume of computing power used in a highly distributed network is taken into account.



Practicalities

Right the first time

Since blockchain records are immutable, it is essential that the technical requirements are established up front depending on the number of processes that will be executed on the blockchain and the amount of logic required. It is also necessary to understand the legal implications of the use to which the blockchain will be put. Disintermediation allows for the speed of transactions to be increased and the cost reduced. However, the intermediaries who are being excluded from these transactions may have performed valuable functions beyond simply recording a transaction. This includes protecting the interests of the parties to the transaction and third parties, and fulfilling the regulatory tasks without which the transactions are invalid or illegal.

For example, it may be technically possible to transfer the ownership of a house from one participant in a blockchain to another, but in many jurisdictions it is not legally valid without registering the transaction on the national cadastre. Consequently, legal input is essential to understand what requirements must be fulfilled or avoided, and any regulatory frameworks – such as data protection and anti-money-laundering provisions – must be complied with. These may necessitate the ongoing involvement of third parties until the law catches up with blockchain.

Data protection

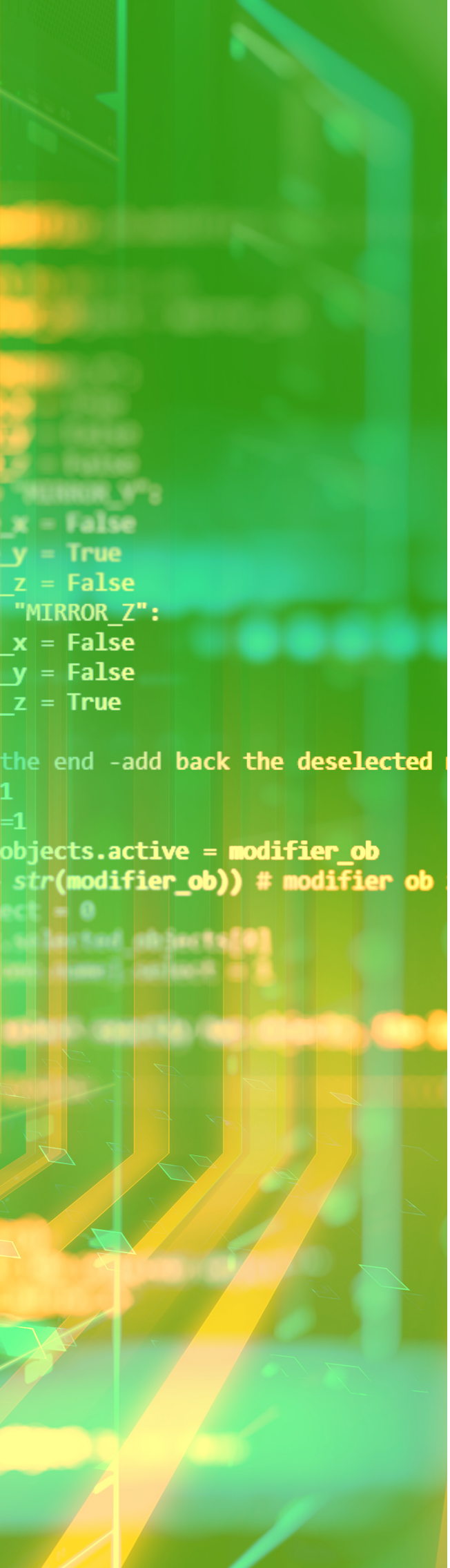
Data protection is a hot topic and a key challenge for those using blockchain. Natural persons already have the right to be forgotten, to have personal data deleted or corrected. Where personal data is recorded in a blockchain, who is responsible for protecting that data and complying with national and supra-national regulations, such as the General Data Protection Regulation (GDPR), which is effective from May 2018? In a permissioned blockchain this could be the super-user as data controller, in a permissionless blockchain it would potentially be every member of the network. As a natural person, how do I get my data deleted or corrected if I cannot identify the data controller(s) using pseudonyms, and how can my data be removed from an immutable record?

Smart contracts

Smart contracts are pieces of code that execute a transaction when a precondition occurs ("if it is the first of the month, then my insurance premium is paid").

As such, the name smart contracts is a misnomer: They are neither smart (there is no cognitive component, simply automatic execution once a precondition is fulfilled), nor a contract in a legal sense. Taking our earlier example, were ownership of a house to be recorded in a blockchain, it would be possible to transfer ownership to another party within the network. But, based on the smart contract alone, would that transfer be legally valid or are other formalities outside the blockchain required to perfect the transaction?

The "if…." component of the smart contract relies on data from outside of the blockchain provided by an "oracle" – which could be a database or a person – providing confirmation that the precondition has been fulfilled. A smart contract is reactive, and only as smart as the self-executing code on which it is based and the factual accuracy of the data input by the oracle. Where data is automatically obtained and input from a reliable source, its accuracy may be relied upon. For example a smart insurance contract might have as its oracle a database of meteorological statistics. If the database records a storm or drought (as defined in the insurance contract) occurring, then insurance payouts are automatically triggered. Where the oracle is a person inputting data manually there is obviously a risk of human error. In the event of error in the coding, the result may be wrong regardless of the accuracy of the oracle.



Legal manifestations

A blockchain solution can have a variety of manifestations, some of which could have a legal component.

Amongst many possible applications, one could use a blockchain solution to record agreements between two or more parties or to record a unilateral act under private law, for the execution and publication of a resolution subject to public law, as a single source of truth (in other words, as proof), for the execution of a legal procedure or judgement subject to different domains of law, for compliance with tax obligations or for the use of suspensive and/or dissolving solutions to legal acts.

Depending on the intention of the parties, more than one of these legal manifestations could be combined in a particular blockchain solution.

Legal issues

Blockchain participants need to be aware of the legal ramifications of the solution they are using, including public law, private law, criminal law and financial and regulatory law.

Private law

In the private-law domain, there are a host of legal issues to consider when using smart contracts on a blockchain. In the previous example, the issue of liability needs to be addressed if the contract has been miscoded such that it doesn't achieve the intent of the parties, or the oracle makes a mistake or deliberate error. In addition, the parties will need to agree on applicable law, jurisdiction, general principles of proper governance, dispute resolution, privacy and the means of digital identity. Is the contract available in writing as well as code so that the parties know what they are agreeing to? Can the identity of the parties be established with sufficient certainty to render the contract valid? If these challenges are not addressed in advance, despite the parties acting in good faith they may find that they do not actually have a contract, and if problems arise they have no agreed-upon means of resolving them.

Public law

From a public-law perspective, there are obviously risks that permissionless blockchains are used for illegal purposes such as money-laundering or to take advantage of pseudonymous involvement to get around competition-law issues. Participants may be exposed to the "miners" who create new blocks acting irresponsibly or not acting in good faith. Currently there are no specific legal remedies against corrupt miners.

Since smart contracts run on a blockchain, they cannot be manipulated after the event and, as they are self-executing, execution cannot be prevented. If the precondition is met, then the transaction is automatically executed, even if the parties have good reasons for no longer wishing that to be the case.

Solutions

Combinations

As lawyers and technologists wrestle with these issues, a number of solutions are being explored. One is to combine permissioned and permissionless blockchains where components of the proposed transactions require some intervention by a responsible party, such as compliance with Know Your Client regulations. All participants in and users of blockchains and smart contracts in which personal data is exchanged are data controllers and must comply independently with all data protection requirements. All parties that run nodes in the blockchain are data processors and must comply with relevant provisions. This is more easily managed in a permissioned than a permissionless blockchain.

On- vs. off-chain

Another solution is to decide what goes on the chain or in the smart contract and what is taken care of off-chain. While it is possible to include provisions as to liability, jurisdiction and other legal aspects in the smart contract, this allows no room for maneuver or interpretation because it is based on conditions. A better solution may be to have a "real" contract stored off the chain, but linked to it with a hash secure value so that the parties can have confidence that the agreed version is the one being relied on by taking advantage of blockchain's timestamping capability.

In addition to general legal considerations, there are also industry-specific ones such as the European Market Infrastructure Regulation for financial services companies, CE marking in the automotive sector and nature conservation regulations that affect the extractive industries. In some cases it may be possible to build demonstrable compliance into the blockchain while others may require an off-chain solution.

Global trade aspects

The ongoing regulatory push for more data – together with other trends, such as controlled free trade, higher border security and integrated border management, accreditation of economic operators, and the outsourcing of regulatory functions to them – is leading to higher compliance costs.

In response, parties trading globally need higher supply chain visibility and security – data that is both of high quality and secure, as well as trade compliance systems that can cope with electronic exchange of data. Technology solutions such as blockchain allow businesses to cope with these challenges.

A multi-party solution

Global trade involves a variety of parties beyond the buyer and seller, including the customs and regulatory authorities in the countries of origin and destination, financial institutions, shippers, brokers and insurers. Between those parties there are multiple exchanges of (first- and second-hand) data. As such it presents many opportunities for the implementation of a blockchain to trigger and record invoicing, bills of lading and customs compliance. Record keeping on blockchain allows parties to trace documents throughout the supply chain: from the beginning, when origin is a determinant of access to free trade agreements and other preferential systems and non-preferential origin claims, and at the end when it can be used to demonstrate compliance with export controls and sanction regimes, and to prove the end-use of the goods.

Blockchain can also facilitate trade in the context of trusted trader schemes such as the EU's authorized economic operator (AEO) program. It can also be combined with other technologies, such as the Internet of Things (IoT), to track and trace shipments and enable paperless trade.

Whether the blockchain is used within a group of companies (where, as trust should be assumed, it might be redundant), between the buyer and seller or involving the authorities, it allows for tracking and visibility of the supply chain. By enabling this tracking, the parties are also able to ensure that they are not unwittingly breaching sanction provisions by exporting to black-listed countries. Smart contracts could automatically execute payment for the goods and any associated duties once the relevant preconditions have been triggered, while ensuring that access to preferential trade agreements is optimized. In the compliance domain, applications of blockchain include: batch management, quota allocation, document certification and certified end-user statements to comply with export control regulations. Within a group of companies, a permissioned blockchain could be implemented to automatically attribute and collect duty payments from relevant companies within the group by a central import- and export-management function.

Trade finance application

A blockchain could also be implemented to execute the trade finance process in a transparent and trustworthy manner that minimises the risk of fraud. It would also eliminate the volume of documentation and the time-consuming manual processes that create a drag on the speed with which transactions occur while increasing costs.

1. Create purchase agreement (smart contract)

- A buyer agrees to purchase goods from a seller; a purchase agreement is created and shared via a smart contract
- Terms of the purchase are laid out in the smart-contract conditions
- Smart contract is sent to requred parties for approval

2. Smart contract approval

- Both financier and seller reviews the shared agreement and digitally signs the contract upon agreeing with the parties involved and terms of purchase

3. Ship goods and generate invoice

- Seller initiates the shipment of goods and updates the smart contract to reflect the shipment
- Shipper acknowledgements receipt and updates the contract in return by providing a bill of lading
- Seller invoices the buyer for the shipment goods; goods are tracked throughout transit using data inputs from IoT devices

4. Complete payment

- Upon delivery, the buyer will digitally acknowledge receipt of goods and trigger payment
- Using the provided acknowledgement, smart contracts can initiate / execute / track payments both within the blockchain network and externally

Additional considerations

For customs duty purposes, an ideal future state would involve the relevant public authorities being participants in a blockchain with all other parties to a cross-border trading relationship, allowing for automated authorizations and duty payments, which is already envisaged by article 185 of the Union Customs Code. This would enable an enhanced and more effective "Single Window," providing every party to the transaction with transparency into its progress and compliance.

Whilst implementing a blockchain offers many benefits to those involved in global trade, there are undeniable risks and barriers that must first be mitigated or overcome. These include addressing data privacy and security concerns, gaining the commitment of all parties to the transaction to maximize the benefits, understanding the level of financial and technological commitment required to implement and operate the blockchain, and accounting for prior registration requirements with the relevant government bodies.

Using blockchain in a supply chain allows complete traceability of a product's origin and final recipient. By way of simple example, at the factory where a drug is manufactured it can be recorded using RFID, barcode or other technology. This would be registered in the first block in the chain. Having checked against block one, the second block would record the drug's updated status as it is moved to a warehouse. Permissions built into the blockchain would limit its onward sale to approved trading partners. Having checked the validity to date as recorded in the earlier blocks, block three would update the drug's status again as it is received at its final destination.

Future opportunities

In future, as the technology matures, capacity issues are addressed and the law catches up, we can expect to see complete global trade supply chains using blockchains, with participation from the authorities to monitor transactions and compliance with rules of origin, customs declarations and duty payments and sanctions rules. Combining blockchain with the Internet of Things will enable manufacturers to track and trace batches of product to manage the risk of grey imports within their distribution networks and demonstrate good corporate governance throughout.

It currently takes roughly ten minutes for a transaction on a blockchain to be validated, which means that transactions that need to happen in real time are off-limits for this technology. As processing capacity and speed increase this will open up new applications and opportunities for the deployment of blockchain.

In the meantime, companies exploring blockchain applications are starting small, with a focus on one country or process, and learning from these experiments before implementing more widely. At the same time, some participants are taking blockchain issues through the courts to get clarification through binding verdicts that can be relied on in future. Over time international coordination and collaboration will be needed to facilitate the greater use of blockchain to manage global trade supply chains and other cross-border uses of the technology.

What's next?

A multi-party solution

Deloitte Legal is involved in the Deloitte Blockchain Institute, which offers an end-to-end portfolio of services from ideation to implementation to make your blockchain vision work. We already have more than 20 prototypes in development and combine our legal, technological, talent, strategy and operations expertise to provide fully integrated blockchain capabilities.

Blockchain is a nascent field in both law and business. Our comments are not intended to be exhaustive but rather to present various aspects of blockchain from a legal perspective and the associated issues to keep in mind. We will continue to investigate the many opportunities that blockchain presents as they emerge and to exchange ideas as the landscape evolves.

To discuss the legal implications of blockchain implementation in your business contact:

Philippe Heeren	Lawyer	pheeren@laga.be	+32 472322871
Inger Bijloo	Senior Legal Consultant	ibijloo@deloitte.nl	+31 613907028
Sven Buschke	Senior Manager	sbuschke@deloitte.de	+49 15158005227
Alexander Tyulkanov	Senior Manager	atyulkanov@deloitte.ru	+79 647639993

Deloitte.
Legal