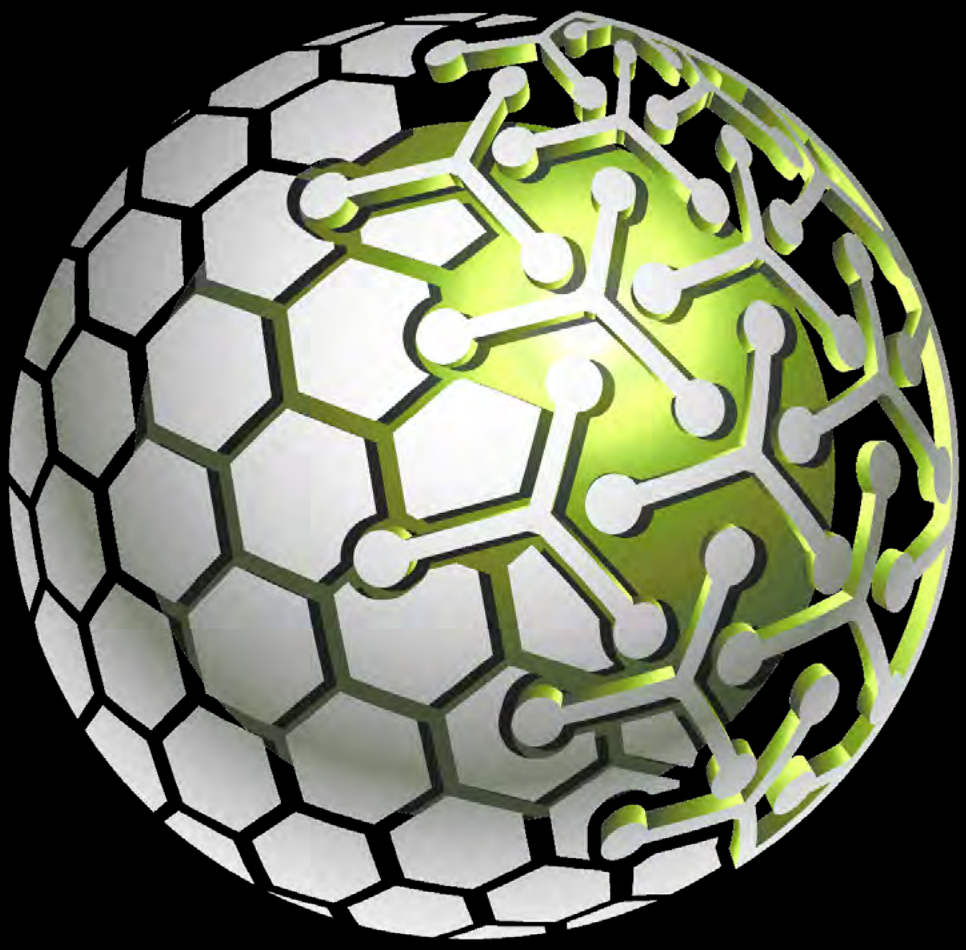
Deloitte.
Legal



Blockchain: Legal implications, questions, opportunities and risks

September 2022

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Introduction	01
What is blockchain?	02
Practicalities	05
Smart contracts	07
A blank canvas	12
Solutions	13
Global trade aspects	14
What’s next?	17

Introduction

Blockchain continues to be the most polarizing concept in technology – with its advocates and critics each fervently making their case for the technology's potential and necessity, or its folly and waste. There is, however, consensus that 'blockchain' is relevant.

Enormous sums of capital (wholesale and retail) are being deployed, with value created, destroyed and re-allocated through the use of blockchains. Large engineering efforts, and research and development, are being applied to iterate and to create new flavours of 'level 1' blockchains, along with software to make those blockchains accessible to users. Blockchain-based technologies raise fundamental questions as to the nature of property, contracts and legal persons, which are being seriously revisited in jurisdictions around the world. Macro-economic concepts such as the 'soundness' of money and the nature of central bank money, are being consulted on by central banks. Micro-economic concepts such as the nature of scarcity of an asset and new manifestations of 'status' goods are being experimented on, and are forming part of the social zeitgeist. Hardware supply chains and component prices are being impacted by the demand for specialist 'proof-of-work' mining equipment used to power blockchains – which varies based on cryptoasset prices, and on technological roadmaps that might obviate the need for this kind of mining. Social concepts of sovereign identity, pseudonymity, reputation, new forms of governance and audit, along with proving information to a third party, without needing to share context, are all being experimented on, trialled, and tested.

In short, blockchain continues to develop beyond its initial cryptocurrency use case, into areas such as 'non-fungible tokens' (NFTs), 'decentralized autonomous organizations' (DAOs), and decentralized finance (DeFi) – often with little respect for the status quo. To blockchain proponents these use cases are overpowering and underway. To critics, they are overcooked and underwhelming. In any case, it behoves us to pay attention and to understand the 'what', 'how', and 'why' of blockchain, as its relevance looks set to continue.

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, participants are incentivized to not manipulate or change the data – in practice, the data 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, altering the timing, order or content of a transaction would create an invalid configuration, unless all subsequent blocks were also changed (which would be computationally expensive or slow).

Participants in the blockchain (miners to validate transactions, nodes, and wallet users) are all expected to use the longest blockchain (with the most blocks in it) as the definitive version. This norm perpetuates because users are expected to be self-interested: being in the minority is expensive because you would input resources (electricity, capital, etc.) but not see the returns that come from being in the majority. In practice, a consensus forms as the definitive version, based on the actions of the majority.

While any one node could change the data in its copy of the blockchain, those amended records would be rejected by other participants because either the blocks would not 'add up' properly, or the chain would be shorter, and therefore represent an expensive 'minority' view.

Where this paper describes a public blockchain as 'immutable', it does not mean that any particular data record literally cannot be amended. Instead it means, 'the blockchain' is defined as the version of a blockchain which has a prevailing consensus by the majority of participants as being the preferred version, and that: (a) it is expensive for any one user of the network to adopt a minority, non-consensus view; (b) it is not technologically possible to force users to change their records; (c) it is legally unfeasible to force users to change their records, as they are decentralized and not identified; and (d) that no one person has the computing power to write a longer blockchain that they control – to do so would require more computing power than the rest of the network combined, but that computing power would be expensive to gather and use, and would have no benefit until the 51% point was reached.

In practice therefore, the longest version of a public blockchain is immutable.

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 information representing 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.

A blockchain allows participants to publish signed information (including messages) without the need for intermediaries to operate or maintain the service, or verify the real identity of authors (or senders). 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 must be approved in order to participate). The need for permission 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 have ID numbers, and so can operate pseudonymously, without identification or authentication.

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.

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 to create legal contracts. Blockchain technology has been used either to make existing processes more efficient, faster or cheaper, or to create new methods or services previously not possible. The most obvious example of this is the much-discussed cryptocurrencies. However, blockchain use is being adopted 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); and
- Oil and gas (to monitor good corporate governance of affiliates and financial services in a variety of ways, from clearing to loyalty programs).

Blockchain is considered disruptive because it is transparent and eliminates the need for intermediaries and other third parties while being both robust (in terms of base layer dependability) and cost efficient (compared to the total cost of equivalent checks and balances created in a traditional way).

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 in the software that uses the blockchain may compromise users' assets and undermine security, and cost efficiency is open to question when the externalities of blockchain use, such as the volume of computing power used are taken into account.

Practicalities

Right the first time

Since blockchain records are immutable, it is important to understand the use case requirements (technical, legal, and commercial) up front. 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, guaranteeing performance of parties' obligations, netting off risks, 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 real property transactions are not legally valid without registering the transaction on the national cadastre or land registry. 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 to perform these formalities and duties, unless and until the law directly acknowledges blockchain records and processes.

Data protection

Data protection is a hot topic and a key challenge for those using blockchain. 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 EU (European Union) General Data Protection Regulation (GDPR)?

Because smart contracts are based on distributed ledger technology, the first issue is data export out of the initial territory. The GDPR and UK Data Protection Act 2018 broadly restrict transfers of data outside the European Economic Area (EEA) with certain exceptions. How can this be complied with when validators are global? One way to address this is via the level of encryption and control with the validator. If set correctly, the information sent outside the EEA can be encrypted or anonymized so that no personal data remains in it, or the personal data in it cannot be read or used. Therefore, this type of approach could meet the criteria required for transferring personal data outside the EEA.

Another issue is the right to be forgotten or 'right to be erased'. This is a right of data subjects that typically applies where their personal data is processed following their consent. Here, we need to be more precise again on the nature of 'immutability'. While the person that initially put the information on the blockchain (the 'data controller') might be able to erase the relevant personal data in their own records, this would have no practical benefit to the data subject, because all the other blockchain records would remain unchanged. The operators of all the other 'nodes' cannot be identified or practically compelled to update their records, and they have no incentive to adopt a non-consensus blockchain with the erased data removed.

In the European framework of data protection law, there is on-going legal debate as to whether each of these other nodes are operating as 'sub-processors' of the personal data (meaning overall the initial data controller is responsible for their actions) or as 'controllers' (meaning each node would be responsible for its own actions) – in reality it would depend on the particular facts of the situation. One approach to this challenge is not to use blockchain technology for processing personal data where the legal basis to do so is based on consent. If the transfer of personal data is reliant on consent, then as personal data relating to a transaction cannot be erased or forgotten, the requirement cannot be met when consent is withdrawn. However, if a process disapplies the right to be forgotten (e.g., the land registry), then this is not a consideration.

Another personal data issue occurs with the right to rectification, such as in the GDPR. Much like with erasure, there is no mechanic to change the data on the other blockchain nodes, however additional data can be added to the blockchain to correct and update the old data. The blockchain system and processes should be constructed such that the latest record is read and relied upon, and the older records are identified as incorrect, and only to be used for audit/logging purposes (or even not to be used at all).

Smart contracts

The common definition is a computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract. Blockchain-based smart contracts are often criticized as not being 'smart' (as they do not have intelligence or think for themselves) – however they can outperform humans in arithmetic, memory, speed, and logical processing. They are also criticized as not being 'contracts' – but this is based on a misunderstanding of what a contract is.

A 'contract' is the abstract bargain between parties that creates a legal relationship. The contract can be documented on paper, and represented in words, but it is intangible, and can both differ from the words the parties used to record it (for example, implied terms and pre-contractual representations) and may have restrictions on how it can be enforced from legislation (such as consumer rights and unfair terms). In this sense, the criticism is akin to saying a piece of paper is not a contract: it could never be, but it might be the most accurate and useful representation of the terms of a contract.

The smart contract, or the sheet of paper, might not be a contract however – they might be a summary only of the contract, might be directions where to find the contract, might be the contract expressed in another language, might be a message which is itself performance of a contract, might be a notice in relation to a contract, etc. As we see, fundamental analysis of the bargain, and the words and messages between the parties is needed to understand what contractual relations are created, and whether they meet the standard requirements to form a contract (typically offer, acceptance, certainty, consideration, and intention to create legal relations).

Smart contracts raise a range of legal issues – not just relating to contract law or contractual interpretation – for example agency and tort factors come into play. How to interpret a contract written in code, rather than words, is the first challenge. We are lacking in clear legal authority on this, however, think tanks and policy statements around the world continue to explore and propose approaches in this regard. For example, the UK Law Commission has proposed a novel method of contractual interpretation by objectively assessing how a reasonable coder would interpret the software code (the 'reasonable coder test'). Note, crucially, that this may well depart from how a computer processor would interpret and perform the software code.

Agency law applies when an individual is given agency to fulfil or enter into a contract on another's behalf: the autonomous performance of a smart contract by a blockchain adds some complexity to the normal analysis. Often the operator of a computer system that does something on behalf of a user would be held to be an agent for the user, who is the 'principal'. With the automatic performance of actions by a decentralized system of ever-changing participants, there seems to be a vacuum: the principal is quite far removed from the actions, but there is no identifiable agent performing the actions on behalf of the principal. The developers might be seen to be an agent (despite perhaps not being involved after they wrote the code), or the individual miner that happened to verify the transaction in question, or perhaps there is no agency relationship at all. Again, complex, novel, legal issues arise, which will be very fact dependent.

Tort law also applies (more so than with traditional contracts) due to potential issues with 'drafting' (coding) of the smart contract. A tort could be triggered if the design of the smart contract did not contain all the terms of the underlying contract meaning the legal contract did not occur properly, arguably leading to a claim of negligence against the designer.

Regulations and statutes also need to be considered. EDIAS (Electronic Identification and Trust Service) is a European regulation that allows for electronic signatures and other electronic actions to substitute real life actions, for example a digitally signed contract versus a wet signature which is crucial for the validation of smart contracts. This has been adopted in England via the Electronic Communications Act 2000.

NFTs (Non-Fungible Token)

Being non-fungible means that these tokens are not equivalent to each other and can be distinguished. For example, a one of a kind token that represents ownership of, or rights in relation to, a real or digital asset.

NFTs use the same core technology and programming language as other cryptocurrencies such as blockchain. NFTs mainly exist on the Ethereum blockchain due to its ability to write more complex smart contracts.

DAO (Decentralized Autonomous Organizations)

Essentially a DAO is a method using a blockchain and smart contracts to organize and co-ordinate the actions and preferences of a decentralized group of participants, often based on pre-agreed software rules. For example, instead of deciding who to hire from a list of applicants a smart contract can assess the applicants based on pre-agreed criteria, and issue services agreements without any human input. Every part of the digital process performed by a human could (in theory) be replaced with autonomous code.

Traditional companies have shareholder meetings where members can vote on resolutions for the management board to implement. In a DAO this management board can be done away with in respect of digital activities: once a decision is made the code and operation of the platform can immediately and automatically perform the decision and its consequences.

DAOs can continually improve and grow because their participants can submit and vote on changes to them, based on number of tokens held, perhaps with additional rules such as the need to 'stake' tokens to register a vote, or with different classes of tokens carrying different rights.

The activities of the DAO might generate revenue by it charging a fee for its services – which gives the tokens value in controlling the revenue stream and representing a claim on that revenue and profit. A DAO itself, without additional steps, is generally not a legal person, capable of suing and being sued, or owning property. In legal terms, its activities are typically done by the underlying actors and participants, not the DAO itself. Myriad legal issues therefore arise, relating to agency, securities law, financial promotions, collective investment schemes, trusts and beneficial title, unincorporated associations, and more.

There are significant benefits to a DAO structure however, in respect of transparency, speed and resistance to certain types of corruption, and so various approaches are being tested and adopted to address these legal issues. Legislation has been created in various jurisdictions to put on a clear footing how a DAO can lawfully operate and is governed. Also, structures have been established for the use of legal persons such as companies to act and operate the DAO in accordance with the DAO rules. This gives a mechanic for the DAO to hold property, to perform off-chain activity, to assert its rights, and to enter into contracts with third parties.

DeFi (Decentralized Finance)

Decentralized finance aims to make a new financial system that is open to everyone and does not require trust in intermediaries. To achieve this, DeFi relies heavily on blockchain and smart contracts. Most DeFi projects are built on Ethereum because of its widely adopted program language called solidity, which allows for the writing of advanced smart contracts that control the logic of the DeFi applications.

Stablecoins are cryptoassets created to reduce volatility as they are 'pegged' to a more stable asset such as fiat currencies. In centralized stablecoins, the theory is that the cryptoasset represents a claim on an equivalent amount of the pegged currency (e.g., US dollars in a bank account). For the purpose of DeFi, a stablecoin is need that does not use fiat money reserves for maintaining a peg, as this would require a central authority. Decentralized stablecoins, pegged to fiat currencies, have been created by holding overcollateralized cryptoasset reserves, with the stablecoin representing a senior debt claim (of an amount measured in the relevant fiat currency) against those reserves.

This mechanic allows for volatility in the underlying reserves, provided that the reserves continue to exceed the claims against them, represented by the stablecoins issued. This trustless, permissionless, stable asset class can subsequently form the basis of decentralized financial services, without needing the participant to be exposed to the general volatility of the 'cryptocurrency' asset class.

A common use case is decentralized exchanges or 'DEX'. These operate according to a set of rules (smart contracts) allowing users to buy sell or trade cryptocurrencies.

When trading on a DEX there is no exchange operator, no sign up, no identify verification, no withdrawal fees and instant settlement. Instead, the smart contracts enforce the rules, execute trades, and securely handle funds. Unlike centralized exchanges, there is often no need to deposit funds into an exchange account before conducting a trade, or to separately withdraw funds from an exchange account, eliminating the major risk of exchange hacking.

Decentralized money markets also connect borrows with lenders. These services allow for peer-to-peer based borrowing and lending, without being exposed to non-performance by the counterparty, but also without needing a centralized party. This allows for cryptocurrencies can be leant out to earn interest, and for them to be 'staked' as collateral to borrow against. Novel contractual arrangements are often put in place, for example that non-payment of interest on a loan does not represent a breach of contract, but instead an election to forego the relevant collateral. This can have important consequences in terms of contractual remedies, rights to sue, liability limits, the rule against penalties, and more.

There are risks involved with DeFi, most importantly DeFi is still in its infancy, and things can go wrong. Smart contracts are frequently mis-programmed, meaning third parties can drain the treasury of funds by sending them rogue instructions. As these DeFi applications can carry risks, decentralized insurance has been created to pool and mitigate these risks. Decentralized platforms can connect insurers with insured parties autonomously, again without any insurance company or agent in the middle.

Web 3.0

Web 1.0 platforms are publishers: statis information is published, and users consume it, on a read-only basis, without interaction. Although Web 1.0 includes dynamic content such as that via 'flash' and 'java' added more features, users were still just consumers of information.

Web 2.0 is characterized by the two-way flow of information, not only did users get information from pages, but pages got information from its users. Web 2.0 brought about forums, message boards, social networks, user-generated content, and platforms, but also targeted advertising and the erosion of privacy for users. The hosting assets are however run and owned by centralized companies, who own the profits and capital in relation to those websites and services.

Web 3.0 is an ambition to remove the need for centralized third parties to operate websites and services, so the value created can be owned by the users, rather than a service provider, so they are transparent, and so they do not require the consent of any third parties to operate. There are necessary building blocks, and implementations, to this Web 3.0 vision: blockchains, cryptoassets, DeFi, NFTs, decentralized identity services and DAOs. The combinations of these building blocks enhance their power and potential, but also the complexity, novelty, and therefore the legal uncertainties.

A blank canvas

Like paper, a blockchain can be used to write and record many different types of legal instrument.

Amongst many possible use cases, 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.

Solutions

As lawyers and technologists wrestle with the legal issues we describe, a number of solutions are being explored.

Combinations

One solution 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. In this setup, 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. Meanwhile, 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 subjective interpretation, or 'efforts'-based obligations, because it is programmable logic. Where a human readable contract is needed, but the parties want to memorialize the terms in a provable way, the "real" contract can stored off the chain, but linked to it with a blockchain-based hash secure value so that the parties can have confidence that the agreed version is the one being relied on, 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, along with general evidence of provenance, members of the supply chain, quality, freshness and sustainability.

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 blacklisted 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 decreases 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 required parties for approval

2. **Smart contract approval**

   Both financier and seller review 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 increase 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

Future events can be generally classified into technology improvements, legal changes, and adoption increases.

Core blockchain improvements are expected in the next few years to greatly increase the number of transactions per second. In terms of Ethereum, high increases are hoped for by changing to a 'proof-of-stake' consensus method (rather than 'proof-of-work'), 'rolling-up' transactions so that some transactions can be processed on 'side-chains', 'sharding' so that processing can be done in parallel, and making the blockchain 'stateless', so a node does not need to download the entire ledger history before it can function. Novel implementations are also expected to become more mainstream as applications for them become more user friendly, such as 'zero-knowledge SNARKS' which allow selected sub-facts to be proven to a particular third party without such proof being onwardly shareable, or the entire 'fact' having to be revealed (for example, that income is within a range, but not what it is).

Legal changes are also continuing at pace. The US, UK, and EU are all introducing legislation to regulate core blockchain and cryptoasset use (not just anti-money laundering, financial promotions, and tax, which has historically been the case). In particular, stablecoins are receiving particular scrutiny as an area in which retail consumers need protection. Multiple central banks are consulting on 'central bank digital currencies' and how they would fit into their money supply. A handful of jurisdictions have created new categories of legal person to give legal personality to DAOs, or to smart contracts. Novel categories of property right are being dreamt up by IP lawyers, and seriously proposed as being worthy of introduction to the statute book. In short, expect to see more legitimacy, more regulatory checks and balances, and more certainty.

Adoption is also showing little sign of slowing down. At a fundamental level, the number of bitcoin and Ethereum wallets with a non-zero balance continues to increase linearly. Surveys show merchants are expecting widespread cryptocurrency and stablecoin adoption in the next five years, and that financial services leaders see digital assets as very important to their industry in the medium run. At a more commercial level blockchain-based projects are being built, planned, promoted and launched by brand owners, CPG manufacturers, and across the entertainment industry, in every geography, at an unprecedented pace.

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:

Paul O'Hare
Deloitte Global Technology Law Leader – Deloitte Legal
pohare@deloitte.co.uk
+44 20 7303 3545

Richard Folsom
Partner, Deloitte Legal UK
rfolsom@deloitte.co.uk
+44 20 7303 0117

Richard Morgan
Consultant, Deloitte Legal UK
richardmorgan@deloitte.co.uk
+44 20 7303 3130

Deloitte.
Legal

Designed by CoRe Creative Services. RITM1153882.