# Blockchain and Supply Chain Management

JEFFREY D. NEUBURGER, WAI L. CHOY, AND JONATHAN P. MOLLOD, PROSKAUER ROSE
WITH PRACTICAL LAW COMMERCIAL TRANSACTIONS



A Practice Note providing an overview of the use of blockchain and smart contracts in the supply chain context including the legal issues, concerns, benefits, and risks associated with its use. It includes information on key distinctions between public and private blockchains and important considerations regarding the use of blockchain consortia

The term blockchain refers not to a single entity or network, but rather to a type of technology. There are many existing and potential implementations of blockchain. Some are made available by vendors to be used as a standard platform for accomplishing a defined objective. Others are custom designed and built specifically for a customer's needs. In many cases, blockchains are not interoperable with other blockchains, requiring parties wanting to transact using a blockchain to coordinate on an appropriate implementation.

Blockchains can be useful in supply chain management, the administration of systems that move goods around the world, including by providing a secure way to verify transactions involving multiple parties that typically do not know or have reason to trust each other.

This Practice Note provides an overview of some of the important issues surrounding the implementation of blockchain for supply chain management. It includes fundamental legal issues that entities wanting to experiment with blockchain solutions should consider before testing or implementing them. It also introduces blockchain-based supply chain consortia and related considerations.

## PUBLIC/OPEN/PERMISSIONLESS BLOCKCHAIN

In a classic implementation of blockchain, copies of a complete ledger (the distributed database), which includes both the current state of a network and its entire history, are distributed among many or all the computer systems of participants on the network (**nodes**) and updated simultaneously. Each node that elects to be a "full node" by maintaining a full copy of the blockchain has access to the blockchain's entire database and complete history. No single party controls it.

Participants in this type of blockchain are pseudonymous. This means that, while they do have unique identifiers associated with them, the actual identities associated with those identifiers are not discernible based on information on the blockchain. Each time a user submits a transaction (i.e., a proposed change to the distributed ledger), the details of that transaction are broadcast to the network and waits in a pool of unconfirmed transactions to be validated by validator nodes on the network (which, for the most well-known implementation of blockchain, the Bitcoin network, for example, are referred to as **miners**).

Validator nodes must first independently check unconfirmed transactions against the blockchain's history to verify legitimacy, using computational methods hard-coded into the network. Once transactions are verified, each validator node groups them into a proposed block. For a block generated by a given validator node to be added to the blockchain (so that all nodes' ledgers are updated to include it), it must be selected by the blockchain network through its consensus mechanism. In the Bitcoin network, this is called **proof of work** and requires a miner to solve a complex computational challenge before all other miners for its proposed block to be added to the blockchain.

Once a block is selected through the consensus mechanism and verified by the network, it is added to the blockchain, logically and inextricably linked to the chain of all of the verified blocks that preceded it and then distributed to all of the nodes on the network. In doing so, the transactions embodied in the new block are etched across the network as the verified "truth," and the network's "chain" is extended. In this way, all of the full nodes have a full and complete copy of every valid transaction ever conducted through that network.

Once a new block is added to the chain, it cannot be modified without sufficient consensus of the network due to the cryptographic way each block and its contents are linked to all that came before it (for example, with Bitcoin, most of the nodes on the network). This fundamental feature of blockchain is often called **immutability**.

Unlike centralized databases, a blockchain can be updated with a new transaction submitted by any node on the network (assuming it passes verification by the network), with all nodes' copies of that blockchain being identical.

## PRIVATE/CLOSED/PERMISSIONED BLOCKCHAINS

For many reasons, including the ability of each node in a public or permissionless blockchain to view all data on the blockchain, purely public blockchains are unlikely to be adopted by enterprises, although certain elements of public blockchains will likely still be found in enterprise applications.

Instead, companies have been looking to private, closed, or permissioned blockchains which, while retaining the concept of an immutable distributed ledger, are characterized by some different features, including that:

- The right to participate in the network is restricted to pre-selected participants or institutions authorized to transact on the network.
- Participants are likely identifiable, rather than pseudonymous.
- Outside of the blockchain itself, participants may be parties to written agreements relating to their use of and interactions using the blockchain. This may include commitments covering:
  - responsibility for maintaining the blockchain;
  - remedies in case of technology failure or error; and
  - governance matters.
- Different nodes may be allocated different permissions and powers, such as the ability to:
  - decrypt and read only certain types or silos of data, rather than all data;
  - modify the blockchain or its governance rules;
  - participate as a transaction validator; and
  - submit transactions to the network or alternatively be limited to read-only access.
- There may be some degree of centralization, with a primary organization or organizations managing, running, or maintaining the blockchain in some respects.

Public and private blockchains are not mutually exclusive. Hybrid blockchains combining attributes of both can be established.

## SMART CONTRACTS

One key feature of blockchains is the smart contract. A smart contract is a software application designed to execute the arrangement agreed on by parties to a transaction on the occurrence of a pre-programmed triggering event. They can be run on blockchain platforms that are programmed to support them, and they automatically execute, verify, and enforce the performance of the agreed-on transaction. Through smart contracts, blockchains can help the automatic execution and settlement of business rules without human intervention and with limited counterparty risk.

In the supply chain context, a smart contract can be used, for example, for paperless transactions with strangers across borders in a secure manner, and smart contracts' fully automated and self-enforcing nature make them ideal for escrow and conditional payment arrangements. Using smart contracts can involve the use of oracles (web services or other external sources of information, such as GPS trackers and other Internet of Things (IoT) devices) to trigger contract execution (e.g., money transfers, customs filings, or releasing funds on the receipt of goods), which makes them useful in many contexts. Depending on the kind of transaction, parties may decide to still execute a traditional written agreement, with smart contracts used as an agreed-on mechanism to quickly execute payment and other obligations in the manner dictated by the agreement. For information on IoT, see Practice Note, The Internet of Things: Key Legal Issues (W-002-6962).

## BLOCKCHAIN AND THE SUPPLY CHAIN

There can be many participants in a single supply chain, including:

- Raw material providers, manufacturers, and suppliers.
- Resellers, distributors, wholesalers, and retailers.
- Franchisers.
- Sales representatives, agents, and brokers.
- Shippers, carriers, freight forwarders, warehouses, and other logistics providers.
- Insurers, banks, and trade financers.
- Customs officials and regulators.
- Consignees.
- End users.

For more information on supply chains, see Practice Note, Supply Chain Overview (0-523-6390).

Even though all participants are involved in furthering the same goal, getting the product from the original source to the ultimate customer, there is often no:

- Visibility from one part of the supply chain into another.
- Coordination of the databases used by each of the supply chain participants.
- Agreements or understandings that tie all the participants together.
- Communication among the supply chain participants.

Depending on the goods involved, a supply chain can span numerous stages and multiple ports and require multiple forms and documents. A missing form or a logistical failure can delay delivery and financial settlements for suppliers and can cause smaller entities to endure administrative burdens and difficulties in obtaining trade financing. It can also be difficult and time-consuming to trace the origin and journey of a specific good in a traditional supply chain framework.

Traditional supply chains can therefore be inefficient, complex, data-intensive, and costly, and can lead to:

- Burdensome paperwork.
- Imprecise communications.
- Conflicting records.
- Errors, redundancies, delays, fraud, and resulting excessive costs.

Blockchain can offer supply chain participants:

- Access to real-time, immutable, validated information about the status of any specific product in the supply chain flow anytime.
- Transparency into the participants' respective actions.
- The ability to leverage automation, digital records, and Internet-connected devices to conduct business more efficiently.

Blockchain solutions in the supply chain area are chiefly aimed at reducing existing "pain points," including by:

- Allowing for end-to-end "track and trace" and a secure, validated record of the provenance of goods.
- Lowering costs associated with documentation and bureaucracy.
- Improving quality control through integrated IoT sensors to maintain the "cold chain" for temperature-regulated goods and deter product tampering.
- Digitizing bills of lading and other documents into a single shared, auditable form that is continuously validated through network consensus.
- Automating trade documentation for legal and customs compliance including items like:
  - freight invoices;
  - proofs of delivery;
  - proof of insurance;
  - manifests;
  - letters of credit;
  - receipts; and
  - tax documents.
- Reducing error and waste in processing transactions and mistakes in freight invoices that result in overcharges.
- Using smart contracts and digital tokens (a digital representation of value issued by a virtual organization that can be digitally traded) to facilitate transaction payments and increase liquidity in trade finance (especially for small and medium-sized enterprises).

## LEGAL AND PRACTICAL ISSUES

Though adoption of blockchain by participants in supply chains has many advantages, there are legal and practical concerns.

### GOVERNANCE

Entities participating in a private or permissioned blockchain in a supply chain must understand and be satisfied with how the blockchain will be implemented and administered. In many situations, an overarching traditional legal agreement among the various participants will be necessary, covering points such as:

- The rights and obligations of each participant.
- How decisions on implementation are to be made and how much centralized control to maintain.
- Who is responsible for maintaining the blockchain, what types of service level commitments apply to the platform's operation, and what remedies, if any, are available for network downtime.
- How permission to access the blockchain will be determined, who will have the ability to participate in the validation of transactions, and what the consensus mechanism used to verify transactions will be.
- What safeguards there will be to prevent a given participant, a group of participants, or malicious third parties from taking unauthorized control over the network.
- How data confidentiality will be handled on the platform among the participants and how each participant's read access will be limited to the appropriate subsets of data.
- What data security requirements will be implemented regarding:
  - private keys (a means through which a participant can encrypt and decrypt data);
  - digital wallets (a means of blockchain-based digital assets and effectuating transactions); and
  - smart contracts.
- What antitrust issues are associated with forming a closed and permissioned implementation (which may involve competitors in the same industry) and how they can be overcome. Exploitation of blockchain across an industry may require collaboration among competitors, and participants must be cautious as they get involved in this collaboration, including the creation of closed systems, information sharing, and standardization efforts, to not violate antitrust laws. For more information on the antitrust considerations of working with competitors, see Practice Note, Competitor Collaborations in the US (0-202-2806).
- Whether the technology behind the platform is proprietary or open source. If proprietary, who will own the intellectual property and what rights will non-owner participants have regarding it. For information about ownership of intellectual property, see Practice Notes, Intellectual Property Rights: the Key Issues (2-500-4365) and Intellectual Property: Overview (8-383-4565).
- Who owns the data and what incentive there will be to share data within the private blockchain.
- Who bears the costs.
- What exclusivity obligations participants will have to each other. For information on exclusive dealing arrangements, see Practice Note, US Antitrust Laws: Overview: Clayton Act (9-204-0472).
- Under what circumstances a participant will be allowed to exit the blockchain and, what would happen to the data associated with that participant.
- When the blockchain will go live and whether there is a critical mass of participants that must be reached to launch.
- In what event(s) would the network be shut down.

These governance questions are complex, and agreement often becomes more difficult to achieve as the number of participants increases, so they must be addressed early in the process. Coordination issues can be challenging, as supply chain blockchain systems may require the use and acceptance by a critical mass of suppliers, manufacturers, buyers, shippers, freight forwarders, logistics providers, ports, and customs officials.

### VERIFICATION

Blockchain technology is not necessarily a cure-all for dishonest participation or fraud, particularly regarding the points at which the external world and the blockchain intersect. For example, whether the appropriate documents are paper or digital and whether the validity of transactions is verified on a shared ledger,

fraud can still be perpetrated in the physical world (for example, a shipping container full of rocks instead of televisions). In a supply chain system, unless the blockchain implementation incorporates communications with **oracles** (external electronic data inputs that can validate that the assets in the supply chain are what they claim to be), there is some risk of fraud. Some external off-chain element of trust, such as an individual that can confirm the nature of the assets being supplied, is necessary.

### TECHNOLOGICAL HURDLES

Blockchain platforms must work with legacy systems or current technologies such as radio frequency identification tags (RFID) and electronic data interchange (EDI) systems. This can present potential middleware and integration hurdles. Relatedly, the development of multiple blockchain solutions presents interoperability issues, a problem that is being addressed by industry blockchain consortia pushing for standardization. For information on blockchain consortia, see Blockchain Consortia Considerations.

### ELECTRONIC CONTRACTING

Questions remain about the enforceability of blockchain-based transactions and related, self-executing smart contracts, including whether existing state contract and business laws would cover these transactions (or whether these laws must be amended to recognize blockchain records). The Uniform Electronic Transactions Act (UETA), which has been enacted by most states, and the federal Electronic Signatures in Global and National Commerce Act (E-Sign) Act (15 U.S.C. § 7001), generally provide that records or signatures in electronic form cannot be denied legal effect and enforceability based on the fact they are in electronic form. For more information on requirements for enforceability, see Practice Note, Signature Requirements for an Enforceable Contract (6-518-3096).

Seeking legal clarity regarding blockchain, some states have begun to enact legislation to address the enforceability issue. For example, in 2017, Arizona passed legislation (Ariz. Rev. Stat. §44-7061) that clarified some of the enforceability issues associated with the use of blockchain and smart contracts under Arizona law, specifically for transactions relating to the sale of goods, leases, and documents of title governed respectively under UCC Articles 2, 2A, and 7.

Subsequently, many other states, including Nevada, Tennessee, and Ohio have also passed blockchain legislation that generally gives legal recognition to blockchain transactions by including blockchain within the definition of electronic records. The need for these state statutes is questionable, as it is likely that the framework for enforceability is already in place under the E-Sign Act and state adoption of UETA.

### OPEN SOURCE SOFTWARE

The Bitcoin protocol was released in 2009 as open source code under the permissive MIT license. The code underlying many blockchain platforms is also available under a variety of open source licenses. Some are more restrictive, with copyleft provisions and limitations on enforcing patents (for example, GPLv2, v3, Apache 2.0) while others are more permissive (for example, MIT, BSD licenses). Companies working on blockchain projects need to understand the implications of the open source nature of the blockchain code and the relevant underlying licenses to fully understand their rights and obligations regarding the code and derivative works based on the code. For information on the issues related to open source software, see Practice Note, Open Source Software (0-500-4366).

### PATENTS

Numerous individuals and entities have sought and are seeking to patent blockchain developments. With many industries looking toward collaborative blockchain uses, patent filings can help maintain control until the technology matures or translate into having an interest in a future initiative. Efforts to own blockchain should focus on:

- Improvements to the technology, as the software of the Bitcoin blockchain, which was released under the MIT open source license, is itself unpatentable.
- Improvements to generally-applicable underlying technologies, such as better encryption that can be used as part of a blockchain.
- Application of the technology in innovative ways for specific purposes or fields, such as blockchain optimized to support transactions of a specific type.

The extent to which distributed ledger software is, in fact, an unpatentable abstract concept is not entirely clear. In *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, the Supreme Court invalidated multiple patents covering a computer software-implemented electronic escrow service for enabling financial transactions because they covered abstract ideas implemented via a computer and did not have sufficient additional features capable of rendering them significantly more than abstract ideas (134 S.Ct. 2347 (2014)). Since then, many software patents have been invalidated and software patent applications have been denied, although the analysis is fact-specific. Regardless, litigation is likely to ensue, and companies and startups might see defensive filings or patent pools as a beneficial strategy in this area. It is not clear how a patent pool would best be structured.

### CYBERSECURITY

The cryptography, encryption, and other aspects of the technological architecture of blockchains foster enhanced cybersecurity. In a properly coded blockchain, unless a back door is built in or a single entity controls more than the percentage of the nodes or controls the specific nodes necessary to dictate changes to it (called a consensus attack), blockchain transactions are likely to be immutable and the software can likely detect and prevent attempts to wrongfully access or modify network data.

The fact that blockchain's peer-to-peer nature does not require a centralized database and the true copy of the database is continuously replicated and reconciled across all the nodes makes it less susceptible to hackers. This is because a successful hack of a specific node's copy of the database would soon be invalidated and overwritten by the network's consensus mechanism. There can still be security vulnerabilities in technology ancillary to blockchain (e.g., flaws in digital wallets or smart contracts) which can have unintended consequences on the blockchain.

### CHOICE OF LAW AND FORUM

Choice of law, jurisdiction, and similar issues present challenges in the world of global transactions where records are kept on a decentralized basis on every node in the network, wherever they

may be located. Considering that blockchain technology is inherently borderless and decentralized, significant conflict among federal, state, and local regulations is likely inevitable. Considering this uncertainty, parties participating in a permissioned implementation should, where possible, include jurisdictional and dispute resolution provisions, particularly with respect to operations that may include smart contracts.

### REGULATORY COMPLIANCE

Using an immutable distributed ledger coupled with IoT-connected solutions in the supply chain can improve the traceability of the source and transport of goods and simplify compliance with consumer protection regulations surrounding temperature-sensitive goods. The ability to audit the origin and shipping history of a specific shipment can potentially offer companies speedier and more efficient compliance with regulators and customs officials.

### AUDIT AND RECORD KEEPING

Using blockchain may potentially create efficiencies for financial institutions in complying with Know Your Customer (KYC) and anti-money laundering rules (AML). This allows smaller transactions to receive financing, since some banks are reluctant to expend resources on complying with KYC regulations on low-value trades. It is not yet clear whether a blockchain record will satisfy audit and record keeping requirements or whether linking a blockchain address to an identity will be sufficient to comply with applicable regulations. Similarly, it is not certain that blockchain's immutable record and bank-intermediated trade finance transactions will aid compliance with AML regulations.

For more information on KYC and AML obligations, see Practice Notes, USA PATRIOT ACT and Know Your Customer Requirements for Lenders (6-504-7122) and US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions (7-521-3248).

### UNIFORM COMMERCIAL CODE

Another unsettled question is which portions of the Uniform Commercial Code (UCC) will hold up in a blockchain world and which ones must be revised to reflect this new digital paradigm. For example, blockchain assets could potentially be treated as general intangibles or investment property under Article 9 of the UCC, but they could potentially also be considered financial assets under Article 8 of the UCC. The answer to the question of which of these Articles will ultimately apply will help determine how parties to a financial transaction could perfect a security interest in virtual currencies or other blockchain assets (a transaction that might include the use of smart contracts).

### CONFIDENTIALITY

Supply chain participants may be concerned that blockchain provides other blockchain participants with too much visibility into their data, for example, that competitors participating in the blockchain may be able to access pricing or other data that provides it with a competitive advantage. Take caution in constructing the blockchain's permissions architecture to appropriately limit participants' ability to decrypt and read network data.

### GDPR AND OTHER DATA PRIVACY ISSUES

Blockchain implementations must take into account the EU's General Data Protection Regulation (GDPR), particularly given the inherent conflict between the immutability of data on a blockchain and instances where the GDPR requires that consumer data be erased or removed under the right to erasure (also known as the "right to be forgotten") under Article 17 of the GDPR.

If personal data is involved, one potential solution is to store personal data in separate off-chain databases (which are not immutable), with the blockchain merely containing pointers that link users to the off-chain data. Doing so may sacrifice some of the benefits of blockchain. Implementations involving personal data must be carefully constructed to comply with applicable data privacy laws. For more information on GDPR and other data privacy issues, see Practice Notes, Overview of EU General Data Protection Regulation (W-007-9580) and US Privacy and Data Security Law: Overview (6-501-4555).

### LITIGATION AND DISCOVERY

The impact of blockchain on the litigation process remains to be seen. For example, open questions include:

- Whether there will be a "master" record keeper in this process.
- How litigation issues around discovery will be addressed.
- How audits, subpoenas, and investigations will be handled.

### QUANTUM COMPUTING

Current encryption, cryptography, and private and public key systems are premised on the assumption that there are limits to the resources and processing power that can be applied to break these systems. Quantum computers may be powerful enough to break the systems currently in use that protect secure online communications and encrypted data. Ultimately, quantum computers may be able to solve complex computations as much as 100 million times faster than classic computers. If the resources of quantum computers are ever generally available or otherwise subject to misuse, encryption and cryptography as they currently exist could be in jeopardy. The National Institute of Standards and Technology (NIST) has therefore begun the process to standardize so-called post-quantum cryptography, and developers are working on quantum-resistant blockchains.

### FORCE MAJEURE PROVISIONS

Force majeure concepts, which are often glossed over in contracts as boilerplate, demand special consideration in the blockchain context. These contractual provisions relieve a party from a contractual duty if performance has been prevented by a force beyond its control. For example, under UCC § 2-615(a), which concerns frustration of purpose, "delay in delivery or non-delivery in whole or in part by a seller ... is not a breach of the seller's duty under a contract for sale if performance as agreed has been made impracticable by the occurrence of a contingency the non-occurrence of which was a basic assumption on which the contract was made or by compliance in good faith with any applicable foreign or domestic governmental regulation or order whether or not it later proves to be invalid."

In smart contracts, a force majeure provision should be viewed as a key allocation of risk. Parties on a blockchain platform should understand certain questions before negotiating an agreement covering their supply chain interactions on a blockchain, such as:

- What is an unforeseeable force majeure event in the blockchain/smart contract environment.
- Who will be responsible if the technology fails and whether this failure would be considered a force majeure event.
- Who is responsible if a hacker exploits a smart contract vulnerability and makes performance impossible for either party and what are the procedures for remedying such a hack.
- Whether force majeure procedures should be written into the smart contract code, thereby:
  - allowing the system to suspend performance obligations if a force majeure event occurs; or
  - allowing the parties to terminate the transaction under these conditions. The parties should consider whether this determination is so subjective as to require human intervention and not be delegated to code.
- Whether the agreement should contemplate a contingency to revert to a paper-based system in the event of a technology failure.

In smart contract situations, where technology failures may prevent performance by one or both parties, common law force majeure or impossibility of performance doctrines may apply. (See, for example, *Kel Kim Corp. v. Cent. Mkts., Inc.*, 70 N.Y.2d 900, 902 (N.Y. 1987) ("Impossibility excuses a party's performance only when the destruction of the subject matter of the contract or the means of performance makes performance objectively impossible. Moreover, the impossibility must be produced by an unanticipated event that could not have been foreseen or guarded against in the contract ....").)

## BLOCKCHAIN CONSORTIA CONSIDERATIONS

When a company decides to test a supply chain blockchain solution, it is necessarily a collaborative affair, as a working platform that delivers business value will require the participation of multiple parties, potentially including government authorities. A variety of industry consortia have formed to:

- Foster experimentation.
- Encourage participation.
- Develop standards and governance structures.

Consortia raise their own set of legal implications, however. The fact that competitors would be working together in these groups brings with it many antitrust considerations. For more information on the antitrust considerations of working with competitors, see Practice Note, Competitor Collaborations in the US (0-202-2806).

Additional legal and practical concerns about the vision and governance of the consortium include:

- Who may join, who may not, and whether it will be a public, private, or hybrid blockchain.
- What is the funding structure.
- Who may participate in standard-setting meetings.
- How will the consortium be controlled, what are each participant's rights and obligations, and whether members are barred from working with other consortia.
- How is confidentiality of data to be handled.
- How are antitrust issues to be addressed, given that competitors within the same industry are collaborating and sharing data about their operations. Whether some parties' transactions will be given priority over others, and whether some parties will be excluded.
- How the platform will be built, whether aspects of the platform are proprietary, and who owns the intellectual property.
- What is the technology roadmap and how will goals be achieved from a technical standpoint.
- What are the exit scenarios, both voluntary and involuntary, for members.