FOLEY
FOLEY & LARDNER LLP

Blockchain in Supply Chain Series

Editors: Eugenia Wang and Kathleen E. Wegrzyn

2022

EDITORS

Eugenia Wang
Associate
Milwaukee
ewang@foley.com

Kathleen E. Wegrzyn
Partner
Milwaukee
kwegrzyn@foley.com

FOLEY
FOLEY & LARDNER LLP

TABLE OF CONTENTS

© 2022 Foley & Lardner LLP

An Overview of Blockchain in Supply Chain: What's the Link?

AUTHORS

Eugenia Wang | ewang@foley.com

Kathleen E. Wegrzyn | kwegrzyn@foley.com

Managing the supply chain is one of the biggest challenges faced by modern-day global companies. These companies devote a tremendous amount of resources to investigating inefficiencies and identifying areas of cost reduction.

Forward-thinking companies are now investigating blockchain as a technology that could potentially revolutionize supply chain as we know it. Analysts predict that blockchain technology is capable of improving the contemporary supply chain structure by increasing supply chain trust, efficiency, and transparency.[1]

Increasingly, supply chain leaders are recognizing that the future of supply chain may lie in blockchain solutions. In 2019, a survey performed by PwC revealed that 24% of industrial manufacturing CEOs were planning, piloting, or implementing blockchain technology.[2] Then, in 2020, Deloitte's Global Blockchain Survey revealed that 55% of its senior executive and practitioner respondents viewed blockchain as a top priority.[3] In 2021, Business Wire reported that the market for blockchain in supply chain is predicted to grow from $253 million in 2020 to over $3 billion by 2026.[4]

How Blockchain Works

Blockchain is often equated with cryptocurrency, but in fact, blockchain technology has many applications beyond functioning as a virtual currency platform. To understand how blockchain fulfills a need in supply chain, it is first necessary to understand how blockchain works.

1. Definition of Blockchain

A blockchain is a string of encrypted data blocks. Let's break that down: The "blocks" of the blockchain can be conceptualized like a file containing information (the "data"), and that information is locked so that only those with the key can access the information (the "encryption").

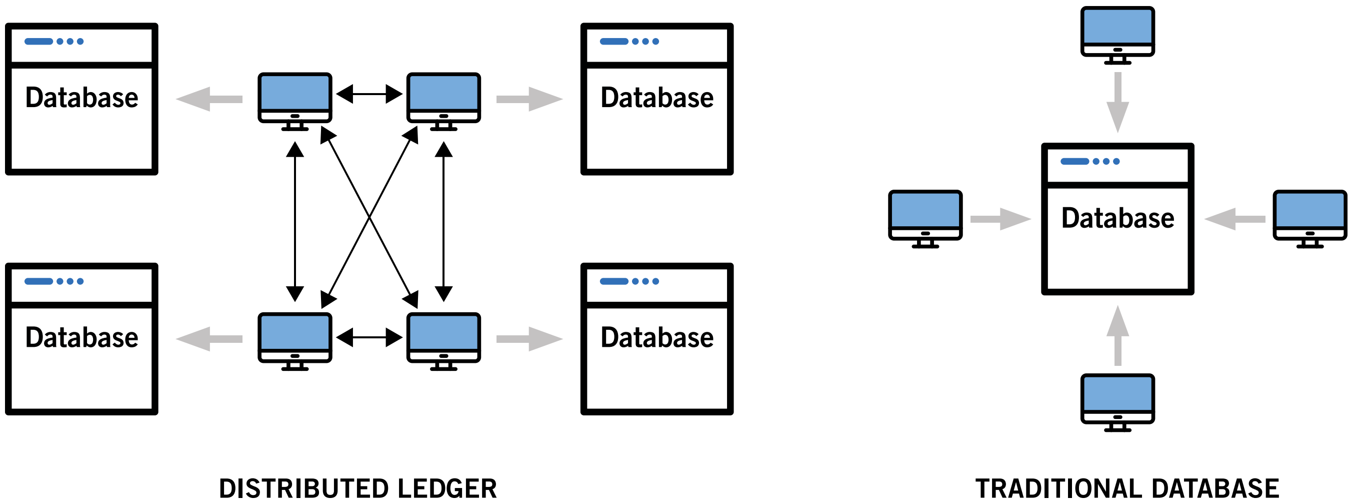
Many files (or blocks) are linked one after another into a "chain." Each file (or block) of data includes the following types of information – a timestamp to indicate when it was created, historical information about the blocks that precede it in the chain, and information that is new to that block. All the blocks together make up the blockchain.

2. Blockchain Infrastructure

Computers, laptops, servers, or other computer devices connected to the internet are needed to access the blockchain. When these devices are connected together, they are called "nodes" of the blockchain. The nodes store the blockchain (and the users of the nodes may be anybody in the world as in permissionless blockchains or may be limited to certain users as in permissionless blockchains, which will be discussed further in "Types of Blockchain: Public, Private, or something in Between").

The storing of the blockchain across the nodes creates a type of distributed ledger, which is a system in which data is stored and shared across multiple sites, countries, or institutions. A distributed ledger can be contrasted with a traditional database in which all the digital data is stored in a centralized location. In the case of blockchain, the different nodes typically store identical data.

Distributed Ledger vs. Traditional Database

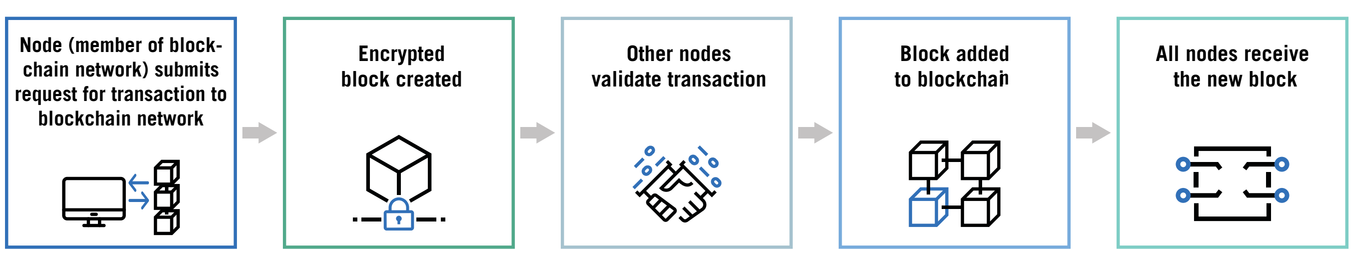


3. Adding to the Blockchain

In order to add a new block of data to the blockchain, a node must send out a transaction request with the new data to other nodes on the blockchain network, triggering the creation of a block. Before the new block is added to the chain, a select number of nodes must first agree that the addition of the new block to the blockchain is valid. When validating the new block, the nodes confirm that the block is correctly formatted and that it does not contain duplicate transactions. After the block is validated, the encrypted block is added to the string of existing blocks and stored by the other nodes on the blockchain network.

Because blockchain is encrypted and in a distributed ledger format, the data on the blockchain are thought to be virtually unhackable, thereby lending trust and confidence in the data stored on the blockchain.

Blockchain Process



Real-Life Uses of Blockchain in Supply Chain

Although we do not know whether blockchain will revolutionize supply chain any more than we know whether bitcoin will be the currency of the future, several prominent companies are testing blockchain solutions and investigating blockchain uses for their supply chains. By 2023, it is projected that 30% of manufacturing companies with more than $5 billion in revenue will be engaging blockchain technologies.[5] To name a few:

- Blockchain company Everledger partnered with IBM to create a blockchain solution to ensure diamonds are ethically sourced.[6] Everledger has also branched out into other industries by developing blockchain solutions for the fashion industry, electronics producers, and electric vehicle manufacturers.[7]
- Walmart, Carrefour, Nestle and Dole have partnered with IBM on a trial blockchain system that tracks food products through their respective supply chains.[8]
- Amazon boasts managed blockchain solutions for supply chain and other business applications that integrate Hyperledger Fabric, an umbrella of blockchain management tools developed by the Linux Foundation.[9]

> Because blockchain is encrypted and in a distributed ledger format, the data on the blockchain are thought to be virtually unhackable, thereby lending trust and confidence in the data stored on the blockchain.

Types of Blockchain: Public, Private, or Something in Between

AUTHORS

Eugenia Wang | ewang@foley.com

Kathleen E. Wegrzyn | kwegrzyn@foley.com

When a company is formulating a blockchain solution to fill its supply chain needs, inevitably the decision must be made as to what type of blockchain is best suited for the project. Therefore, it is essential to have a clear understanding of the options available for blockchain structures. Not all types of blockchains are appropriate for supply chain information management.

Permissionless vs. Permissioned Blockchains

All types of blockchains can be characterized as permissionless, permissioned, or both. Permissionless blockchains allow any user to pseudo-anonymously join the blockchain network (that is, to become "nodes" of the network) and do not restrict the rights of the nodes on the blockchain network.

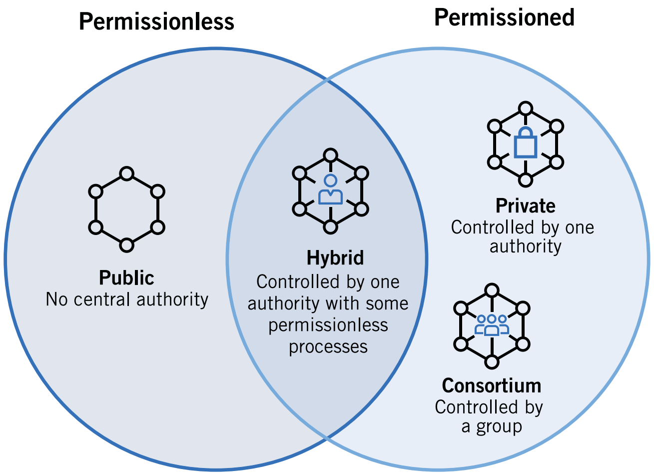
Conversely, permissioned blockchains restrict access to the network to certain nodes and may also restrict the rights of those nodes on that network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain.

Permissionless blockchains tend to be more secure than permissioned blockchains, because there are many nodes to validate transactions, and it would be difficult for bad actors to collude on the network. However, permissionless blockchains also tend to have long transaction processing times due to the large number of nodes and the large size of the transactions.

On the other hand, permissioned blockchains tend to be more efficient. Because access to the network is restricted, there are fewer nodes on the blockchain, resulting in less processing time per transaction.

Like so many things, pros come with cons, and the reduced processing time in permissioned blockchains is no exception: the centralization of permissioned blockchains to some central authority (be it a government, a company, a trade group, or some other entity or group that is granting the permission to nodes and creating the restrictions of the blockchain) makes it a less secure system that is more prone to traditional hacking vulnerabilities. The fewer nodes there are on a blockchain, the easier it is for bad actors to collude, so private blockchain administrators must ensure nodes adding and verifying blocks are highly trusted.

When a company is formulating a blockchain solution to fill its supply chain needs, inevitably the decision must be made as to what type of blockchain is best suited for the project. Therefore, it is essential to have a clear understanding of the options available for blockchain structures. Not all types of blockchains are appropriate for supply chain information management.



Types of Blockchains

There are four types of blockchain structures:

1. Public Blockchains

Public blockchains are permissionless in nature, allow anyone to join, and are completely decentralized. Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data.

To date, public blockchains are primarily used for exchanging and mining cryptocurrency. You may have heard of popular public blockchains such as Bitcoin, Ethereum, and Litecoin. On these public blockchains, the nodes "mine" for cryptocurrency by creating blocks for the transactions requested on the network by solving cryptographic equations. In return for this hard work, the miner nodes earn a small amount of cryptocurrency. The miners essentially act as new era bank tellers that formulate a transaction and receive (or "mine") a fee for their efforts.

2. Private (or Managed) Blockchains

Private blockchains, which may also be referred to as managed blockchains, are permissioned blockchains controlled by a single organization. In a private blockchain, the central authority determines who can be a node. The central authority also does not necessarily grant each node with equal rights to perform functions. Private blockchains are only partially decentralized because public access to these blockchains is restricted. Some examples of private blockchains are the business-to-business virtual currency exchange network Ripple and Hyperledger, an umbrella project of open-source blockchain applications.

Both private and public blockchains have drawbacks - public blockchains tend to have longer validation times for new data than private blockchains, and private blockchains are more vulnerable to fraud and bad actors. To address these drawbacks, consortium and hybrid blockchains were developed.

3. Consortium Blockchains

Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain. Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.

However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk (which we examine in "Legal Implications of Blockchain in Supply Chain: What's Law Got to Do With It?"). Further, some members of supply chains may not have the needed technology nor the infrastructure to implement blockchain tools, and those that do may decide the upfront costs are too steep a price to pay to digitize their data and connect to other members of the supply chain.

A popular set of consortium blockchain solutions for the financial services industry and beyond has been developed by the enterprise software firm R3. In the supply chain sector, CargoSmart has developed the Global Shipping Business Network Consortium, a not-for-profit blockchain consortium which aims to digitalize the shipping industry and allow maritime industry operators to work more collaboratively.[1]

4. Hybrid blockchains

Hybrid blockchains are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations. An example of a hybrid blockchain is IBM Food Trust, which was developed to improve efficiency throughout the whole food supply chain. We discuss IBM Food Trust in more detail in "The Fast Track: Using Blockchain to Trace Products Through the Supply Chain".

Blockchain Types for Supply Chain Use

Because members of supply chains have important data privacy and competition considerations, blockchain for supply chain requires some extent of permissioned functionality, which exists in private, consortium and hybrid models of blockchain. It is therefore not surprising that Businesswire recently reported that consortium and hybrid blockchain types are expected to grow at the highest rate in the supply chain market from 2020-2026.[2]

Decisions, Decisions

When creating a permissioned system, many decisions must be made by the central authority (whether that is a group of companies, one company, or some other hybrid model). Some of the decisions that the central authority of a permissioned blockchain must make include:

Who can join?
Unlike a permissionless blockchain in which anyone can join, the central authority of a permissioned blockchain can limit who has access to the blockchain.

What are the rules for the blockchain?
A permissioned blockchain allows for the central authority of the blockchain to establish rules such as which users can see which data, which users can add blocks to the blockchain, and how many users are needed to validate blocks.

How will the governance of the blockchain be funded?
A permissionless, public blockchain is funded by small transaction fees paid by users requesting to add data to the blockchain. Miner nodes in permissionless blockchains get paid in virtual currency for performing the work to create a new block. However, permissioned blockchains do not require the same incentive structure; because the parties are known, customized funding structures can be created to fit the creation and validation model. In determining how to customize the funding structure in a permissioned blockchain, it must be decided how fees will be allocated and charged for financing the creation and validation operations as well as for the labor performed by the central authority.

The Pros and Cons of Blockchain in Supply Chain

AUTHORS

Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

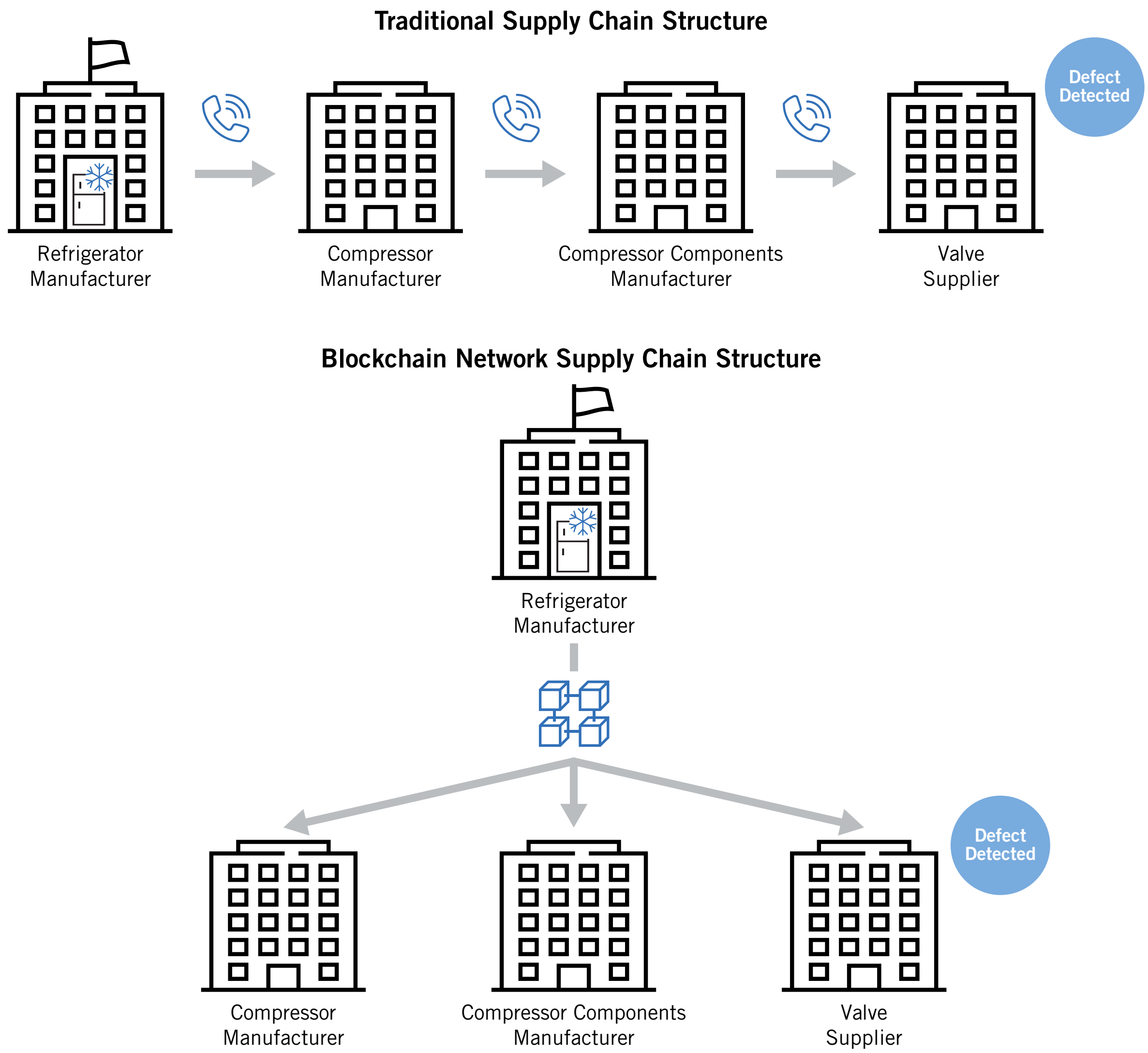
Blockchain has been heralded as a cutting-edge technology that will improve the contemporary supply chain structure by increasing supply chain trust, efficiency, and transparency. However, as promising as blockchain technology is, blockchain is not a panacea for supply chain issues. There are numerous pros and cons of using blockchain in the supply chain:

Some Pros of Blockchain

- **Trust**. Because data on the blockchain is decentralized and immutable, members of the supply chain can trust the data they see on the blockchain. Conversely, a traditional supply chain data storage structure typically requires all members of the supply chain to keep their own records, and therefore disputes arise when those records do not match up.
- **Efficiency**. Because all data is recorded at every step in the supply chain, and every member of the supply chain can see the data, it is easy to quickly identify where in the supply chain a nonconformance (*e.g.*, a product defect or missing product quantity) has occurred, because the life cycle of a product is tracked at every step. Let's take, for example, the construction of a refrigerator. In the case of a traditional supply chain structure, if the refrigerator manufacturer discovers that the compressor of a finished refrigerator contains a defective valve, the refrigerator manufacturer will then need to reach out to the compressor manufacturer, who will need to reach out to the manufacturer of compressor components, and so on and so forth, up the supplier tiers until the supplier of the defective valve is reached. In contrast, if all members of the refrigerator supply chain were members of the same blockchain network, the refrigerator manufacturer would be able to query the blockchain to find the entire tracing history of the defective valve almost instantaneously, cutting investigation time down considerably. Using blockchain technology allows for less time lost sending emails and making phone calls to find out the cause of the nonconformance. Additionally, because documents are stored on a shared ledger, physical paperwork is largely unnecessary.

DEFECT DISCOVERY PROCESS

Without Blockchain vs With Blockchain



- **Transparency**. Blockchain engenders transparency because all data on the blockchain is recorded automatically with a time stamp, including certain data that usually would not be recorded in a traditional supply chain system (such as the steps completed in a production process or the time of a seller's receipt of a purchase order). Blockchain technology also creates transparency by enabling end-to-end tracking (*i.e.*, traceability from one end of the supply chain to the other), which can be enjoyed by all supply chain members on the blockchain. Blockchain transparency can accomplish quicker resolutions to disputes than with traditional supply chain systems.

> While blockchain technology can potentially provide huge advantages to supply chains, there are also potential disadvantages that make it clear that any blockchain solution must be well-tailored to the targeted supply chain.

Some Cons of Blockchain

- **Permissioned Blockchains**. Because supply chain information can be sensitive, a permissioned blockchain (that is, a blockchain that is not open to the public) is usually preferred. However, a permissioned system is less secure, because there are fewer nodes to make up the blockchain and those nodes are typically known to each other, resulting in an easier ability to collude to change a block.
- **The Human Element**. While there is great value in all members of a supply chain knowing that the data on the blockchain cannot be changed once it is established, there can still be human error or intentional misconduct in inputting the initial data onto the blockchain. Therefore, blockchain data is not perfect information – it could be false or even fraudulent. For instance, a bad actor could fill a container with rocks and record on the blockchain instead that the container was filled with auto parts. Blockchain technology could make it easier to detect at which stage in the supply chain the container was filled with rocks, but would not prevent the fraudulent data from hitting the blockchain in the first place. Essentially, blockchain technology does not prevent incorrect information from being entered onto the chain; it just allows every user on the blockchain to confirm that the data on the blockchain has not changed since a certain point in time. Because blockchain technology is traditionally immutable, fraudulent data inserted onto the chain is problematic. Accenture has developed a prototype to allow authorities of permissioned blockchains to edit previous transactions in extraordinary circumstances in order to resolve human error,[1] although some blockchain technologists have criticized such approaches to blockchain, stating that erasing immutability defeats the purpose of using blockchain over a traditional database.[2]
- **Scaling**. Blockchain solutions are far slower to process transactions than traditional databases, because the transactions must be validated on many different computers or servers. In addition, due to the high volume of transactions in supply chain, having a permissionless aspect of a blockchain solution could be costly, since transaction fees would need to be paid to fund the work performed by the miner nodes to create the blocks. Considering certain supply chains execute millions of transactions a day, the method in which blockchain technology is implemented must be thoughtfully approached with an eye towards scalability.
- **Upfront Costs**. The upfront costs of implementing a blockchain solution have the potential to be steep. There are costs associated with hiring blockchain developers, which tend to cost more than traditional developers due to their specialized area of expertise. Planning costs, licensing costs, and maintenance costs can also contribute to a hefty price tag.

While blockchain technology can potentially provide huge advantages to supply chains, there are also potential disadvantages that make it clear that any blockchain solution must be well-tailored to the targeted supply chain.

The Fast Track: Using Blockchain to Trace Products Through the Supply Chain

AUTHORS

Nathan A. Beaver | nbeaver@foley.com
Joanne Molinaro | jmolinaro@foley.com
Gary B. Solomon | gary.solomon@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Many companies need strong supply chain traceability. For the most prevalent tracing challenges, blockchain may provide a formidable solution.

Real-World Applications

Using blockchain to trace products is especially promising for certain industries, including the food, fashion and regulated products industries.

Food Industry

Supply chain traceability is crucial in many industries, but arguably none more so than the food industry, where concerns about contamination, intentional adulteration, and bioterrorism are ever-present.

The most promising applications in the food industry involve conducting product recalls and ensuring consumer satisfaction for perishable products.

1. Food Recalls and Market Withdrawals

Some of the keys to successfully stopping outbreaks of foodborne illnesses through food traceability protocols include the accuracy and speed of obtaining tracking information and the inability of third parties to manipulate that tracking information. Companies that attain top recall accuracy and speed by implementing investigation improvements can reduce recall costs, loss of profits, and reputational damage, and in the case of food recalls, save lives. Enter blockchain.

In response to a series of devastating E.coli outbreaks in romaine lettuce as well as salmonella-laced eggs and breakfast cereal in 2018, Walmart decided to leverage blockchain to increase the safety of its food supply.[1] Walmart describes the food supply industry as one that frequently employs a paper-based tracking system for supply chain, which can lead to delays and dead-ends in tracking contaminated food.[2] Walmart invited its suppliers to ditch the paper trail and join Walmart's blockchain program.

Today, Walmart can track a head of lettuce from a store all the way back to the farm where the lettuce was cultivated by the farmer in just seconds.[3] In fact, Walmart tracks over 500 food items using blockchain, and, in 2020, was able to provide FDA investigators with detailed information on the original source of a potential contamination within an hour, a stunning reduction from the seven days that this process used to take.[4] This year, Walmart arranged with U.S. Customs and Border Protection to pilot a program to track imported foods.[5]

As the use of blockchain becomes more prevalent, retailers will increase their ability to determine exactly which batch of products to recall when an issue arises. As a result, in its supply agreements with retailers and distributors, a manufacturer may want to address the scope of recall expenses and chargebacks differently, as opposed to recalls without the use of blockchain where the parties anticipate a lack of clarity around which batches of products to recall.

2. Perishable Products

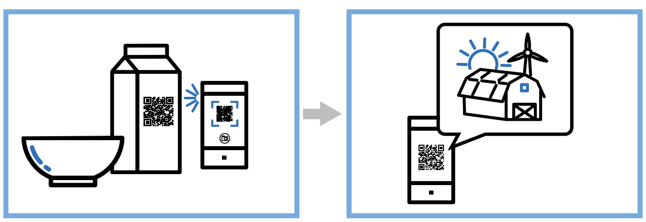
The journey of a perishable product from the country of origin to the final destination can be long and difficult to track. As a result, some companies turn to blockchain to trace products in order to ensure end users receive a responsibly-sourced product with an ample shelf life.

IBM Food Trust is an example of a hybrid blockchain solution that allows supply chain partners to securely share tracking information related to perishable food

© 2022 Foley & Lardner LLP

supplies.[6] IBM Food Trust aims to improve food safety and freshness, identify supply chain inefficiencies, minimize waste, improve brand reputation, and ultimately add value to a company's bottom line. European grocery chain, Carrefour, uses IBM Food Trust to trace chickens from farm to grocery store. In 2019, Carrefour reported that its blockchain-tracked chicken outperformed other chicken in sales growth.[7]

Carrefour credits blockchain with sales increases because blockchain reassures customers of the quality of items they buy and assists them with avoiding products with genetically modified organisms, antibiotics or pesticides.[8] In fact, Carrefour tags certain products, such as tomatoes, oranges, fresh micro-filtered milk, and Rocamadour cheese, with QR codes that allow consumers to learn where their food originated by taking a picture of the QR code with their smartphones.[9]



While you have your bowl of cereal in the big city, you can trace your milk to the farm from which it came. With greater visibility into sourcing, customers can make more informed decisions about their purchases, leading to greater sales of those products for which visibility is afforded.

Fashion Industry

The end-to-end tracking that blockchain provides could be particularly beneficial for the clothing supply chain. Clothing supply chains often look less like a straight line and more like a web, because these supply chains typically span many countries across the globe and contain multiple raw material sources, multiple factories that process the raw materials, multiple subcontracted clothing manufacturers, and a complex distribution network. As a result, clothing manufacturers have difficulties determining where each part of their product originates. Determining responsibility for a batch of defective buttons in a line of dress shirts could be a Sisyphean task without blockchain technology.

Complete oversight over production of fashion products via a blockchain solution can assist companies in determining exactly where along the supply chain a product was damaged by allowing companies to track components back to the original supplier. In the event of a recall, blockchain technology can assist by pinpointing which defective components were incorporated into which final products so that manufacturers can issue recalls quickly and precisely.

Another benefit of using blockchain for global supply chain management is the ability to manage and track timing of raw materials and sub-components in the production process. Supply chain management systems may be configured to monitor and generate notifications and scheduling updates based on updates to the blockchain to help manufacturers and distributors with production and distribution timing and cost projections.

Regulated Industries

Tracing products through the supply chain can help companies comply with applicable laws. For instance, in November 2013, Congress enacted the Drug Quality and Security Act, which requires members of a drug supply chain to track and trace certain prescription drugs.[10] On May 4, 2020, Merck reported that it, IBM, KPMG, and Walmart had completed an FDA pilot program designed to evaluate a consortium blockchain's usefulness in protecting pharmaceutical product integrity. According to Merck, the pilot was a success, and pharmaceutical supply chains can use blockchain to help meet the FDA's tracking and tracing requirements.[11]

In addition, the Bioterrorism Act of 2002 and the Food Safety Modernization Act of 2011 require the traceability of food. Manufacturers may find blockchain solutions helpful to meet these traceability requirements as well.

Tracing Challenges and Blockchain Solutions

Unintegrated Legacy Digital Systems. Even if a company already uses a digital system for tracking products, that system may not integrate with different digital systems used by other members of the applicable supply chain. Helpfully, blockchain can lie on top of these enterprise applications and provide the connection between them. Blockchain can integrate enterprise resource planning systems, customer relationship management systems, warehouse management systems, and manufacturing execution systems to increase transparency of the supply chain and reduce the cost of tracking products and running reports.[12]

Inconsistent and Duplicative Records. Because companies in a supply chain tend to keep their own records using centralized databases, these companies frequently have duplicate copies of, or inconsistent records relating to, the same transaction. In contrast, blockchain stores information on an immutable, decentralized ledger accessible by all members of the supply chain. This structure allows all members of the supply chain to have eyes on the same data and to have confidence that the data is accurate. Ultimately, companies can use blockchain to reduce costs associated with reconciling records across the supply chain.

Root Cause Determinations. In order to identify product shortages and defects, companies typically audit supply chain partners. However, while auditing helps determine if a problem exists, it is less adept at determining the root cause of that problem. For instance, an audit of inventory held by a warehouse could reveal missing product, but the audit may not reveal the reason the product went missing. Did a stocker misplace the product after it arrived at the warehouse? Did a warehouse employee make an error in tracking product quantities?

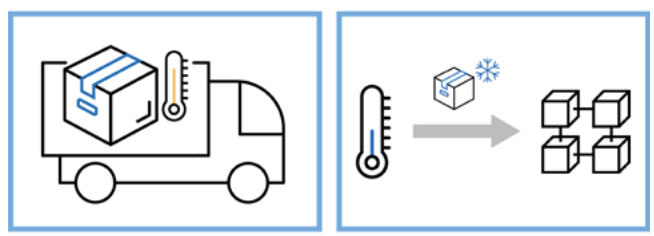
Having all members of a supply chain participate in a blockchain solution would assist in the determination of root cause because the blockchain process affixes a timestamp to every transaction entered onto the blockchain, and the transaction history is immutable. Blockchain technology can automatically provide visibility into all stages of the supply chain, allowing for decreases in the costs of labor-intensive in-person auditing.

Using IoT to Overcome Human Error and Misconduct

One of the limitations of blockchain is that, while the data on the blockchain is secure, such data is not necessarily free of human error or misconduct. That is, when a human inputs data onto the blockchain, he or she may accidentally or maliciously enter incorrect information. Using the internet of things ("IoT") to link the data derived from the physical world directly to the digital world reduces the risk of incorrect data caused by human intervention because no human inputs data on to the blockchain.

IoT refers to the network of real world physical objects connected to the internet via sensors, software, and other technologies embedded or otherwise connected to those physical objects. IoT transfers data related to the physical objects over the internet, and therefore perfectly complements blockchain when it comes to tracing products.

One potential use of IoT for tracing is to attach smart tags to materials as they travel along the supply chain to ensure traceability of such materials after processing or after combination with other materials.



A smart thermometer transmits data from the physical world to the blockchain for improved temperature tracking.

AUTHORS

Richard H. Casper | rcasper@foley.com
Jose A. Lazaro | jlazaro@foley.com
Peter Vogel | pvogel@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Smart Supply Chains Using Smart Contracts

One benefit of blockchain includes its ability to harness the power of smart contracts.

What is a Smart Contract?

Although the term "smart contract" sounds like a legal instrument, a smart contract is actually a computer program that performs a task when triggered by the occurrence of a predetermined event. Smart contracts live on blockchain, which processes the terms of the smart contract, thereby enabling the smart contract to automatically execute the coded task when the triggering event occurs.

Nick Szabo, a computer scientist and cryptographer who coined the term "smart contract," likens a smart contract to a vending machine.[1] A consumer inserts money into a vending machine (*i.e.*, satisfies the condition of the contract), and the vending machine automatically dispenses the treat (*i.e.*, honors the terms of the "contract").

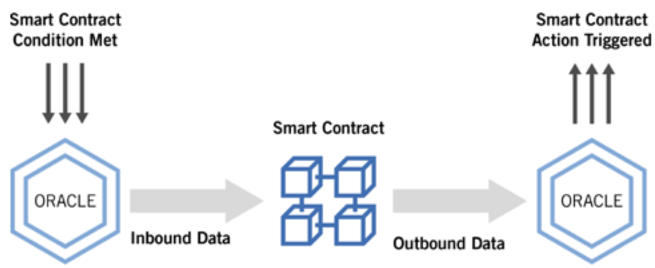
Oracles

In order to trigger the automatic performance of a function, the smart contract uses "oracles" to receive information from the outside world.

Inbound vs. Outbound Oracles

An oracle can provide data from the outside world for consumption by the smart contract living on the blockchain (an "inbound oracle") or allow smart contracts to send data to the outside world (an "outbound oracle"). As an example of the latter, an IoT-enabled lock functions as an outbound oracle when the smart contract triggers the lock to unlock automatically if a party transacts a certain payment across the blockchain.

Smart Contract Process with Inbound and Outbound Oracles



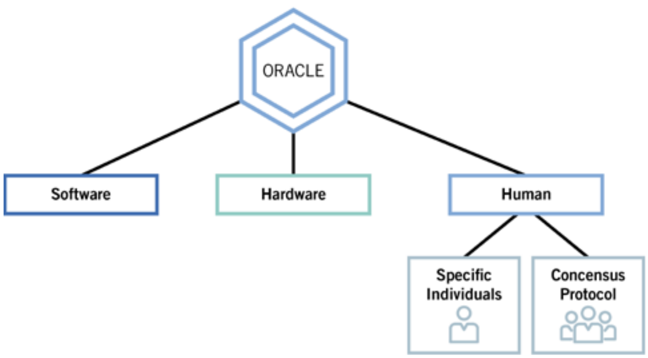
Types of Oracles

Types of oracles include hardware, software, and human:

- **Software Oracles**. Software functions as an oracle by connecting smart contracts to online data sources, such as temperature, commodity prices, and transportation delays.
- **Hardware Oracles.** Hardware oracles include pieces of equipment that communicate real-world information to the smart contract. RFID sensors, for instance, can detect environmental changes that link to blockchain to trigger a smart contract.

- **Human Oracles.** Humans act as oracles when they provide real-world information to a smart contract, often with cryptography in place to ensure the proper individual provides the information. Another human-based approach to oracles uses a consensus protocol, meaning that different humans vote on the input to provide to the oracle. In any case, using a human oracle introduces the potential for human error. A party may nonetheless opt to use a human oracle when a decision requires subjectivity or when the nature of the triggering event makes continuous monitoring difficult.

Types of Oracles



In order to strengthen the trust of the oracle system, supply chain members can use a combination of oracle types for the same smart contract.

Examples of Smart Contracts for Supply Chain

In supply chain, smart contracts are particularly useful for releasing payment, recording ledger entries, and flagging a need for manual intervention.

- **Releasing Payment**. A party could use a smart contract as a means to automatically release payment upon the satisfaction of a condition. For example, two parties, such as a manufacturer and a supplier, could set up digital wallets and a smart contract in order for the manufacturer to pay the supplier for the purchase of goods. After the manufacturer inspects and accepts the goods, the smart contract would automatically move cryptocurrency from the manufacturer's digital wallet to the supplier's digital wallet to effect payment.
- **Recording Ledger Entries.** A party could write a smart contract to record to a blockchain ledger if some specified event occurs or does not occur. For example, if an IoT-enabled device detects the opening of a container during transit, a smart contract could automatically record this information. A party may find such monitoring particularly useful for goods that require a tight chain of custody, such as with the transport of pharmaceuticals.
- **Flagging a Need for Manual Intervention.** Smart contracts are also useful for flagging the occurrence of an event that requires manual intervention. For example, for temperature-sensitive products, a smart contract tied to temperature monitors could alert all concerned parties if an out-of-range temperature occurs. This would allow the parties to promptly take action to correct the temperature, conduct an investigation into the reason for the out-of-range temperature and, when necessary, pull the affected products (and only the affected products) from the stream of commerce.

Steps to Creating a Smart Contract

1. **Identify the goal of the smart contract.**
2. **Determine the triggering event.**
3. **Determine the response to the triggering event.**
4. **Program the triggering event and response to the triggering event (and any other terms and conditions of the smart contract) onto the blockchain.**
5. **Deploy the blockchain. When the smart contract self-executes, the nodes on the blockchain will save the outcome of the smart contract.**

When is a Smart Contract a "Contract" from a Legal Perspective?

A smart contract may constitute a legal contract if the smart contract contains the elements of valid offer and acceptance, as well as adequate consideration. The general principles of contract law define an offer as a manifestation of willingness to enter into a bargain[2] and acceptance as an agreement to that offer,[3] while consideration denotes something of value exchanged by the contracting parties.[4]

In addition, for the smart contract to constitute a legally binding contract for the sale of goods, the contract must also satisfy the various requirements of Article 2 of the Uniform Commercial Code (UCC), including its statute of frauds requirements and its requirement that the contract set forth a quantity in order to be enforceable.[5] Practitioners will need to evaluate on a case-by-case basis whether a smart contract meets these elements and therefore represents a binding legal contract for the sale of goods.

The Uniform Law Commission and the American Law Institute established a Uniform Commercial Code and Emerging Technologies Committee[6] to study and evaluate the UCC in the context of "among other issues, distributed ledger technology, virtual currency, electronic notes and drafts, other digital assets, payments, and bundled transactions," and the Uniform Law Commission released an issues memorandum[7] discussing these topics in July 2021 following two years of committee meetings. While smart contracts have been part of the discussion, no formal evaluation for smart contracts has been performed by the Uniform Law Commission or the American Law Institute, leaving open the opportunity for clearer guardrails in the future as to whether a smart contract amounts to a legal contract.

Smart Contracts vs. Smart Legal Contracts

Smart contracts are not to be confused with smart legal contracts. While a smart contract is a computer program coded to effectuate an outcome upon the occurrence of a triggering event, a smart legal contract is "a legally binding agreement that is digital and able to connect its terms and the performance of its obligations to external sources of data and software systems."[8] The Accord Project makes clear that, although a smart legal contract can use smart contracts via blockchain technology, a smart legal contract can also be created using traditional software systems without the use of blockchain.[9]

	Legally Binding?	Uses Blockchain?
Smart Contract	Sometimes	Always
Smart Legal Contract	Always	Sometimes

Vulnerabilities

While properly coded smart contracts could dramatically increase efficiencies in supply chains, companies face a risk that their smart contracts contain bugs or other technical issues such as data block corruption. There are three common types of vulnerabilities that arise from improperly coded smart contracts: greedy contracts, prodigal contracts, and suicidal contracts.[10]

Greedy contracts are improperly-coded smart contracts that lock funds indefinitely, which can happen, for instance, if the coder fails to code instructions for the release of funds.

Prodigal contracts are smart contracts where the coder incorrectly sets the parameters of a smart contract in such a way that leaks funds to random blockchain users.

Suicidal contracts are smart contracts where the coder incorrectly sets the parameters of a smart contract in such a way that permits blockchain users to destroy the smart contract altogether.

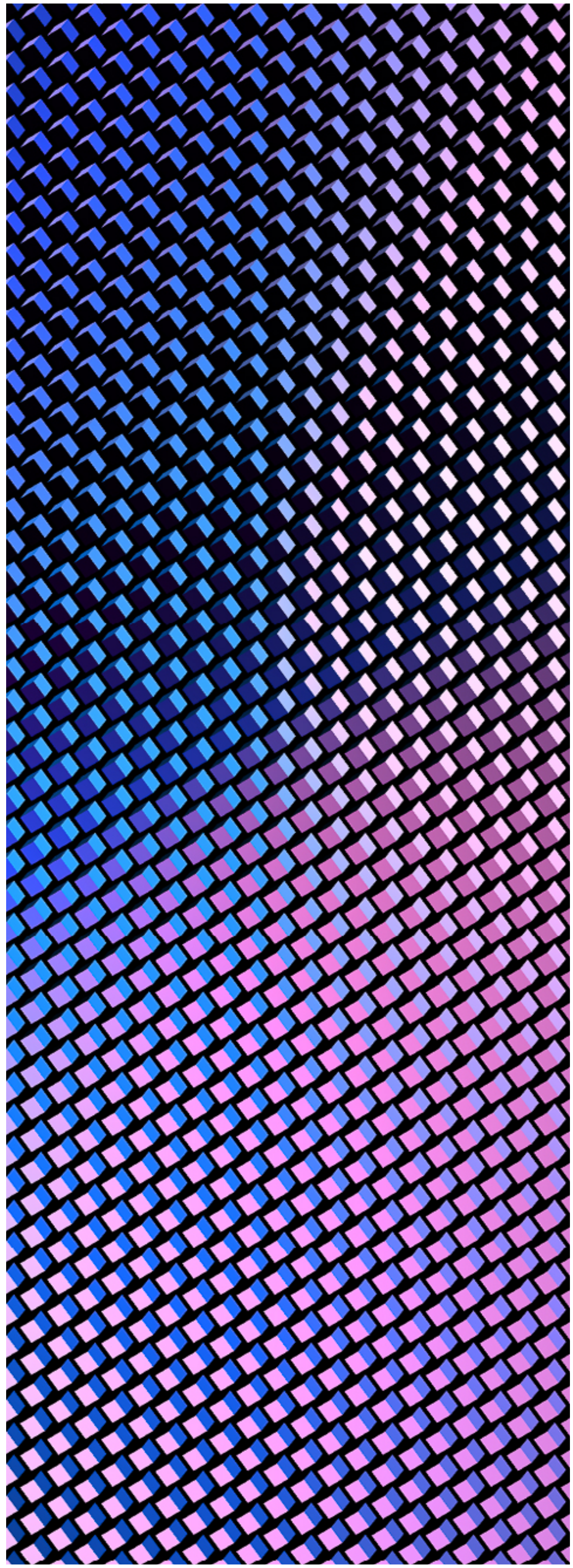
© 2022 Foley & Lardner LLP

In addition, another complicating factor for using smart contracts is the inability of a non-coder to read whether the smart contract actually does what he or she wants it to do. Even though the parties may have a traditional text-based agreement in place that provides the parameters for the smart contract, the programmer could code the smart contract in a way that is not consistent with the written agreement. If the businessperson were unable to read code, he or she would have no way to verify whether the coded smart contract matches the text-based agreement.

Finally, because the immutable nature of blockchain also extends to smart contracts (which live on a blockchain), once a programmer codes and deploys a smart contract, immutability prohibits the addition of any new functions to the smart contract. Upgrading and otherwise altering smart contracts is an active area of research in the blockchain community, and mechanisms for altering smart contracts and best practices are still being developed.

While smart contracts could increase efficiency in the supply chain, real risks exist that the coder could set the smart contract up improperly or that the smart contract fails to account for a change in circumstances. Businesses seeking to employ smart contracts will need to weigh the pros and cons carefully and allocate the risks between the participants in the smart contract accordingly.

> In order to trigger the automatic performance of a function, the smart contract uses “oracles” to receive information from the outside world.



Legal Implications of Blockchain in Supply Chain: What's Law Got to Do With It?

AUTHORS

Richard H. Casper | rcasper@foley.com
Nicholas J. Ellis | nellis@foley.com
Kate E. Gehl | kgehl@foley.com
Elizabeth A. N. Haas | ehaas@foley.com
John D. Lanza | jlanza@foley.com
Steven M. Millendorf | smillendorf@foley.com
Vanessa L. Miller | vmiller@foley.com
Aaron K. Tantleff | atantleff@foley.com
Peter Vogel | pvogel@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

The advent of new technology brings along with it the murkiness of how the American legal system will treat such technology. Before the rise of blockchain for instance, businesses were uncertain how courts would treat electronic records and signatures until the federal legislature enacted the E-Sign Act on June 30, 2000.[1] To provide even more clarity to businesses, the National Conference of Commissioners on Uniform State Laws drafted the Uniform Electronic Transactions Act (the "**UETA**")[2] to provide states with a framework to enact laws governing the enforceability of electronic records and signatures. Now, almost every state in the U.S. has adopted some form of the UETA,[3] and industry heavily relies on electronic contracting.

The legislative process has already begun for blockchain technology. Arizona and Tennessee both enacted laws stating that (1) a blockchain technology signature is considered an electronic signature, and (2) a blockchain technology record is considered an electronic record. Further, these laws say that courts may not deny a contract legal validity because the contract contains a "smart contract" term.[4] Other states are also attempting to adapt their current commercial laws to blockchain technologies. Wyoming, for example, is breaking ground by addressing blockchain's impact on the attachment, perfection, and priority rules of Article 9 of the Uniform Commercial Code.[5] Similarly, Delaware and Maryland have amended their general corporation and limited liability company laws to permit the use of blockchain technologies for creating and maintaining company records with respect to equity interests.[6]

Beyond when and how legislatures and courts will solidify blockchain technology as a valid platform for contracting, there are other possible legal questions and ramifications for the use of blockchain in the supply chain. Some possible areas of legal considerations follow below.

Potential Modifications to Contract Terms in Supply Agreements

As companies begin to implement blockchain solutions, drafters should give thought as to what contract terms to adjust in supply agreements and other commercial contracts related to the use of blockchain in the supply chain. Some potential modifications to consider follow:

Blockchain Governance

Parties to a supply agreement will need to decide whether a supply agreement should detail which transactions can (or must) occur on the blockchain, or whether the parties should set forth which transactions should occur on the blockchain in a separate agreement governing the implementation, governance, funding and maintenance of the supply chain blockchain. Flexibility will be important as blockchain technology continues to evolve and becomes more prevalent, so it may be most practical for both parties to execute an addendum listing transactions that the parties can agree to update.

© 2022 Foley & Lardner LLP

Requirements on Suppliers and Sub-suppliers

A buyer may consider whether it would be beneficial to contractually require its suppliers to join the buyer's supply chain blockchain. A buyer could take this approach a step further and extend it to sub-suppliers as well. A contract could require both the supplier and its suppliers to join the buyer's supply chain blockchain, which would provide the buyer a deeper visibility into its supply chain. For smaller suppliers and sub-suppliers, the ability to keep up and participate in this evolving area may present a challenge that impacts their ability to compete for certain business.

Confidentiality

With multiple member blockchains, the parties may want to explicitly state whether or not a receiving party adding certain confidential information of a disclosing party to the blockchain would be considered a permitted disclosure by the receiving party. The parties must also consider the contract's provisions on removal and return of confidential information at the end of a contract with the immutability of blockchain in mind.

Purchase Orders and Payment Terms

If a buyer must place purchase orders or releases through the blockchain system, the parties will need to revise the ordering mechanism of the contract to reflect this process. Additionally, if the parties plan to handle payment by blockchain smart contracts, the parties will need to revise the traditional approach of invoicing after shipment and paying within a certain period to account for the terms of any smart contract.

Product Acceptance

If the buyer will make payment automatically via smart contract at the time of product acceptance, the supply agreement should be very precise as to when product acceptance occurs.

Indexing and Shipping Costs

Many supply chain contracts use some form of indexing for raw materials or other cost inputs to adjust pricing periodically. Blockchain has the potential to significantly streamline this process by allowing parties to modify contract pricing that is linked to an index faster and easier by using a smart contract to rewrite the new price to the ledger and automatically update payments via blockchain based on the new contract pricing. Although traditionally raw materials have been the focus of indexing provisions, given the recent massive fluctuations in freight and container costs, contracting parties can share risk for fluctuating shipping costs by indexing through blockchain technology as well.

Force Majeure

When drafting force majeure provisions, the parties may want to explicitly define whether issues with the blockchain such as smart contract malfunction or compromise of a party's access to the blockchain would be considered a force majeure event that can be relied upon by a party to excuse from performance under the contract. In most cases, parties may want to align this issue with whether existing language covers IT system issues. If such issues are included as force majeure events, the parties should consider adding a threshold requirement that a party cannot claim force majeure for issues resulting from the party's own failure to maintain industry-appropriate protective measures.

Effect of Termination

In the event of termination of a supply agreement, the parties will want to explicitly set forth any requirements to unwind the blockchain or terminate the related smart contracts. Alternatively, the effect of termination provisions could point to a separately executed agreement specifically dedicated to blockchain governance which would cover the rights and responsibilities of the parties if the supply agreement dictates the parties must unwind the blockchain.

Conflicts

In the resolving conflicts section of the supply agreement, which provides the order of precedence of contract terms in the event of conflicting language, the parties should detail how to resolve a conflict between a coded smart contract or other blockchain terms and conditions and the text of the supply agreement.

Entire Agreement

When drafting the entire agreement section of a supply agreement, the parties will want to identify what, if any, terms and conditions set forth in the applicable blockchain network are part of the agreement between the parties and then provide that all other terms are not part of the agreement.

Service Level Credits

For logistics agreements, the parties may want to define key performance indicators (KPIs) or service level agreements (SLAs) based on data from the blockchain, because that data is considered trusted. For instance, the parties could define processing time to receive inventory to a warehouse (*i.e.* "dock-to-stock" time) as the difference between the date and time of receipt of product at the warehouse and the date and time of stock of product in the warehouse, in each case, based on the data uploaded by any applicable IoT device to the supply chain blockchain.

Data Privacy Considerations for Blockchain

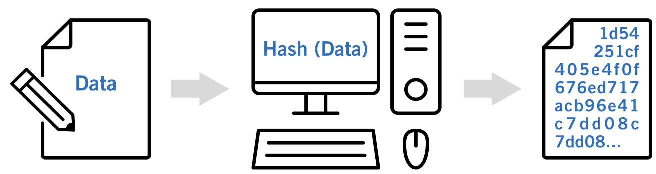
While blockchain is considered a highly secure means of data storage, paradoxically, some of blockchain's other attributes (being decentralized and immutable), pose a compliance barrier with many data privacy regulations, such as the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.105) ("CCPA") and the EU's General Data Protection Regulation ("GDPR").

Blockchain's decentralized platform makes it tricky to determine which privacy laws apply. The nature of a decentralized platform permits processing of an individual's information in any number of locations around the world, because an individual's personal data (such as a person's full name, social security number, or email address) could be located on different nodes, each of which could exist in a different jurisdiction. As each jurisdiction regulates the processing of personal data differently, attempting to manage the plethora of privacy laws, some of which may conflict with others, could be a daunting, if not impossible and cost-prohibitive effort.

The immutable nature of blockchain also poses a potential issue for data privacy. For instance, Article 17 of the GDPR as well as the CCPA set forth the "right to be forgotten." The GDPR and CCPA require that processors of personal data erase the personal data of a person under certain circumstances, including if the person withdraws consent for the processing of their personal data.[7]

Because of the decentralized and immutable nature of blockchains, some potential approaches to handling personal data related to transactions on the blockchain are to store the personal data completely off the blockchain, or store only a hash of the personal data (a one-way mathematic function that represents the personal data, but from which the personal data cannot be determined) on the blockchain while storing the actual data on a private encrypted database. Taking another approach, programmers could write smart contracts to allow for the revocation of access rights or deletion of information on the blockchain.[8] Companies would have to customize any supply chain blockchain solution for data privacy compliance issues based on what personal data will be stored, what jurisdictions the data will be stored in, and the nature of the related blockchain concept.

How is a Hash Created?



Write the "data" in plain text | **Run the plain text through a hash function using a computer** | **Get the hash which uniquely identifies the "data"**

Smart Contracts

Smart contracts are not necessarily contracts in the traditional sense. Rather, a smart contract is a computer program stored on a blockchain that performs an action when triggered by an event. Smart contracts take the agreement of two adverse parties to the next level. When two parties execute a traditional written agreement, they are promising to act in accordance in that agreement. When two parties implement a smart contract, it is not a mere promise; they have already effected an outcome.

As previously discussed, certain states such as Arizona and Tennessee have laid the groundwork for courts to enforce smart contracts. If blockchain continues to become more prevalent in business, the need for decisive regulations will pressure other states to follow suit and address smart contracts through legislation.

See "Smart Supply Chains Using Smart Contracts" for more information on smart contracts.

Antitrust Considerations for Blockchain

Blockchain provides an avenue for competitors to cooperate, particularly in a consortium or other permissioned structure. As with any collaboration or joint venture among competitors, such collaboration raises potential antitrust risks and can create a slippery slope to claims of collusion and anticompetitive exclusionary conduct, among other anticompetitive practices.

For most blockchain collaborations among actual or potential competitors, the greatest practical antitrust risk involves collusion and implicates Section 1 of the Sherman Act.[9] Section 1 prohibits agreements that unreasonably restrain trade, such as agreements among competitors to fix prices, rig bids or allocate customers or markets. Oftentimes, courts can infer such anticompetitive agreements based on the exchange of competitively sensitive information among the participants. Blockchain participants therefore must be mindful of the heightened antitrust risks that come into play should the blockchain arrangement involve the sharing of competitively sensitive information, such as pricing, costs, output or customer specific information.

To minimize this antitrust risk, particularly in a blockchain consortium involving competitors, participants should either avoid the exchange of competitively sensitive information altogether or narrowly tailor the information exchanged and adopt other appropriate safeguards where reasonable. Safeguards to consider include setting up permissions so that only intended recipients of data have access to a block of information and adopting read permission restrictions to prevent employees who have responsibility over pricing, marketing, strategy and competitively important strategic decisions from accessing competitively sensitive information shared on the blockchain. Aggregating or anonymizing sensitive data or limiting the information exchange to historical information only (instead of current or future data) could also minimize the antitrust risks associated with any information exchange that is necessary to the blockchain arrangement. In any event, participants in a blockchain arrangement should be prepared to articulate why the participants need to exchange the specified type or level of information to achieve pro-competitive benefits of the blockchain arrangement.

Consortium blockchain participants may also face antitrust liability under Section 1 if they reach an agreement to exclude competitors from the blockchain collaboration where accessing a blockchain has become essential to doing business in a particular market or industry. Participants should document and consistently enforce well-defined and reasonable criteria for membership. Participants should also exercise additional caution in restricting membership if development of the blockchain technology or any related applications involve standard-setting or the adoption of standard, essential patents, both of which present unique antitrust risks.

Relatedly, antitrust scrutiny may also extend to the way in which consortium members approve transactions. Nodes (or members of the supply chain) validate transactions to be added to a blockchain in accordance with certain pre-determined validation rules. Then, nodes only add transactions to a blockchain if the rules for adding a block to the blockchain are satisfied ("consensus"). Antitrust risk can increase where these consensus mechanisms prioritize clearance of transactions by certain members or decline to validate transactions by particular parties without a legitimate and objective basis for doing so. Participants should ensure the validation and consensus mechanisms use objective criteria and that no single participant controls these processes.

In addition to the most prevalent antitrust risks highlighted above, participants should consider other potential antitrust complications when forming or participating in a collaboration with competitors to develop blockchain technology and related applications. Participants should be mindful of these risks and consult antitrust counsel early in the process as they harness the benefits of blockchain technology to meet their supply chain needs.

Areas of legal considerations for blockchain use in the supply chain include modifications to contract terms in supply agreements, compliance with data privacy and antitrust laws, and the legal treatment of smart contracts.

Get Real: Preventing Counterfeit Product with Blockchain

AUTHORS

Nathan A. Beaver | nbeaver@foley.com
John D. Lanza | jlanza@foley.com
Daniel Rose | drose@foley.com
Gary B. Solomon | gary.solomon@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

The counterfeit business is booming. In fact, counterfeit goods account for a whopping 3.3% of global trade[1] and cost the U.S. economy approximately $600 billion a year.[2]

Counterfeit goods account for a whopping

and cost the U.S. economy approximately

$600 billion a year

See Footnote 2

The Dangers of Counterfeit Products

Counterfeiting has an extensive negative impact, leading to product recalls, lawsuits, consumer injuries, loss of sales, loss of consumer trust and, eventually, long-term reputational harm. Some of the most dangerous counterfeit products on the market today include counterfeit airbags that malfunction during car crashes, counterfeit lithium-ion batteries that self-ignite or explode, counterfeit helmets and baby carriers that easily break, counterfeit prescription drugs that cause accidental overdoses, and counterfeit cosmetics that cause severe skin reactions.[3]

Blockchain for Provenance

Blockchain helps tackle counterfeiting by identifying provenance (*i.e.*, proof-of-origin) of a product, because blockchain provides a secure and trusted tracking system from one end of the supply chain (the creation or mining of raw materials) all the way to other end of the supply chain (where the end user enjoys the finished product). Because blockchain can identify provenance, legal enforcement agencies can more conclusively establish the counterfeit nature of suspect products, and companies can protect their bottom line.

Companies implement blockchain provenance identification through the use of smart tags, which when attached to a good will identify its place of manufacture, track its location, and assign other relevant information to it at each stage in the supply chain. Common types of smart tags include:

- **QR Codes**. QR codes (Quick Response codes) are a type of barcode easily read by smart phones or tablets that can encode information like phone numbers or internet addresses.
- **RFID Tags**. RFID tags (Radio Frequency Identification tags) are tags that use radio waves to communicate information to readers. A reader is a device that emits radio waves and subsequently receives signal back from an RFID tag.
- **Signatures on Metallic or Ceramic Surfaces**. Laser marking machines etch barcodes and graphics onto metallic or ceramic surfaces. Some such marking machines produce 2D data matrix metal tags that users scan with a special scanner to perform data collection and product tracing functions.

Once a user affixes a product with a smart tag, the smart tag sends to the blockchain data for each new transaction with corresponding immutable time stamps. Therefore, at any point on the supply chain, a supply chain partner can trace that product back through the supply chain to see where and when such product originated.

While it would be practically difficult to accomplish, a scammer could create a counterfeit tag by duplicating a genuine smart tag. However, scanning that counterfeit tag would reveal the history of the genuine item, which would help a customer ascertain that the scanned tag is a counterfeit.[4] For instance, if a leather purse with a counterfeit smart tag states the purse was sold by the distributor to ABC Purse Company for sale to the general public, yet the customer found the purse for sale at XYZ Purse Company, the customer could conclude that the smart tag was counterfeited.

Counterfeit Prevention by Industry

The prevalence of counterfeit products has dealt a heavy blow to the fashion, electronics, and pharmaceutical industries. Recognizing the importance of minimizing counterfeit product in the marketplace, leading companies are looking to blockchain to identify product provenance.

Fashion

High-value products that counterfeiters can reproduce swiftly for sale at a premium prove very vulnerable to counterfeiting. In 2019, Harvard Business Review reported that fake luxury merchandise accounted for 60 to 70% of all counterfeit goods sold annually and represented approximately a quarter of the $1.2 trillion total global trade in luxury goods.[5]

Fake luxury merchandise accounts for

See Footnote 5

To protect its lines of luxury products on the market, the LVMH group, which boasts such brands such as Louis Vuitton and Bvlgari, partnered with two other luxury brands, Prada and Cartier, to develop the Aura Blockchain Consortium.[6] The LVMH group unveiled the collaboration in April 2021, and describes it as the world's first global luxury blockchain, which has the objective of providing consumers with the ability to trace a luxury product through its life cycle.[7] The Aura Blockchain is a private blockchain engineered by ConsenSys, a software engineering pioneer in blockchain, and Microsoft.[8]

Using Aura, the luxury brands are able to:

- Create a unique digital identifier for each product at the time of manufacture;
- Keep a record of every transaction related to the product in the product's certificate;
- Deliver an authentication certificate to customers to provide access to information about the product's production;
- Allow customers to track maintenance and repairs of the product;
- Guarantee product authenticity during any resale of the product without the need of third party verification.

See Footnote 9

On the secondary market, blockchain provides a tool for verifying authenticity of fashion items. For instance, a retail store could use blockchain to record the identity of the original customer for a luxury purse sale, and a subsequent buyer could register with the blockchain to record the purse sale to another downstream buyer. The decrease in resale value that may result from a break in the chain of traceability may incentivize downstream buyers to register their ownership on the blockchain.

Moreover, blockchains can maintain or grow product value over time because consumers can verify product authenticity without the need for expert assistance. By using a proper blockchain construct, luxury brand companies can produce product that consumers can authenticate without the use of the luxury company's internal company resources. Smart contracts programmed into blockchain can also automatically execute downstream transactions and provide compensation to producers and prior owners for the resale of a product.

Pharmaceuticals

Counterfeit drugs often look exactly like real drugs, with the same branding and packaging. Yet, the fake drugs can be contaminated or ineffective. Merck KGaA reported that counterfeit antimalarial drugs alone could be responsible for the deaths of up to 155,000 children annually.[10]

In response to the FDA's call in 2019 for companies to create pilot projects to test electronic inter-operable systems, two dozen companies in the pharmaceutical industry, ranging from drug makers (including Pfizer Inc. and Eli Lilly and Company), to distributors and retailers, developed a blockchain platform named MediLedger Network to track prescription drugs around the globe in hopes of eliminating counterfeit medicines.[11]

Counterfeit antimalarial drugs alone could be responsible for the deaths of up to

155,000

children annually

See Footnote 10

Electronics

Identifying counterfeit products in a supply chain proves difficult, because counterfeiters package the counterfeit products to appear legitimate and because the counterfeit products often function adequately for at least some period of time. Additionally, because many electronic products end up as internal components in other devices, downstream consumers could find it difficult to detect knockoff parts. Failure to detect counterfeit electronics in the supply chain creates a risk for product malfunction, which could lead to injury or death.

As a result, Honeywell has partnered with iTRACE and SecureMarking to increase the security of the e-commerce market of its aerospace parts using blockchain technology.[12] Honeywell's new process involves laser-etching a data matrix on the identification plate for a part and then adding a high-security invisible ink on top of the plate. Honeywell's digital blockchain ledger records the digital authenticity record for the part, allowing Honeywell to secure, track, trace and authenticate any part submitted to Honeywell's blockchain process anywhere in the world.

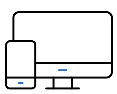
To protect its lines of luxury products on the market, the LVMH group, which boasts such brands such as Louis Vuitton and Bvlgari, partnered with two other luxury brands, Prada and Cartier, to develop the Aura Blockchain Consortium. The LVMH group unveiled the collaboration in April 2021, and describes it as the world's first global luxury blockchain, which has the objective of providing consumers with the ability to trace a luxury product through its life cycle. The Aura Blockchain is a private blockchain engineered by ConsenSys, a software engineering pioneer in blockchain, and Microsoft.

© 2022 Foley & Lardner LLP

Financial Benefits

In 2019, BCG, a consulting firm for business strategy, calculated that, by implementing blockchain-enabled authentication of products, businesses could reap financial benefits ranging from 2% to 5% of revenues.[13] For example, electronics and technology companies lose somewhere in the realm of 4-7% of revenue to counterfeit products on an annual basis.[14] If the same electronics and technology companies were to implement blockchain solutions paired with smart tag technology, these companies could reduce fraudulent sales by 60-80%, therefore allowing manufacturers to recoup an average of 3.85% in revenue.[15] This translates into almost $40 million in savings for a $1 billion electronics company.[16]

However, blockchain solutions for counterfeit prevention may not be the appropriate solution for every manufacturer. Factors to consider before implementing a blockchain solution include the value of the target product, the size and complexity of the supply base, and the level of counterfeiting occurring with respect to the product at issue.[17] Companies contemplating the launch of a blockchain system to combat counterfeiting should perform a careful analysis to determine whether the financial benefits of tracking with blockchain outweigh the costs and challenges of implementing the blockchain technology.

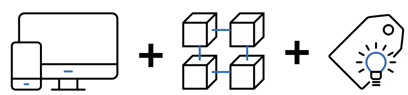


Electronics and Technology Companies

4-7%

OF REVENUE LOST

to counterfeit products
on an annual basis



**Electronics and Technology Companies
with Blockchain and Smart Tag Technology**

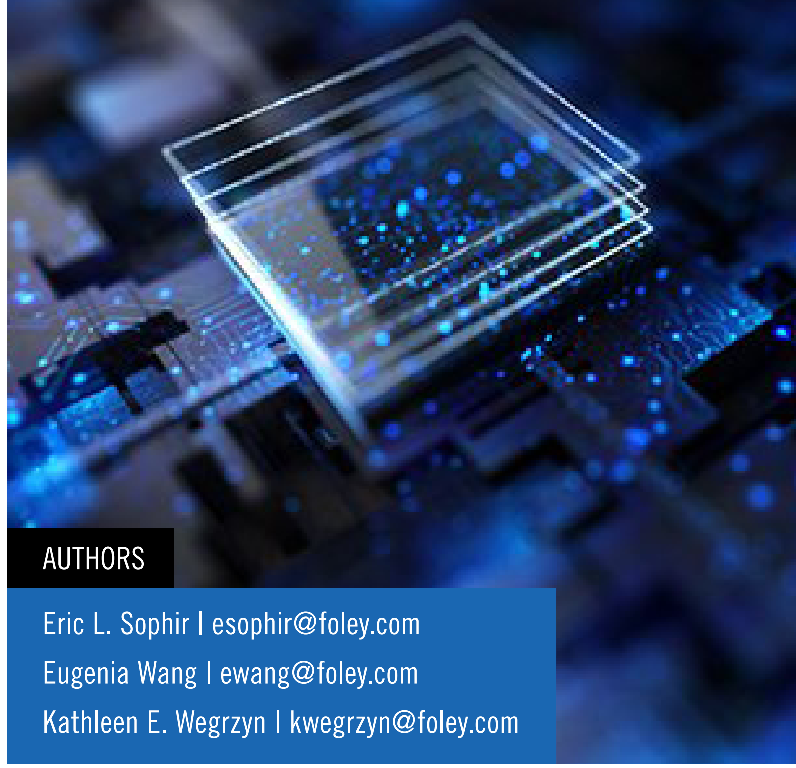
**FRAUDULENT SALES
REDUCED BY**

60-80%

allowing manufacturers to recoup
an average of **3.85%** in revenue

See Footnote 4

Not By the Same Token: NFTs in Supply Chain



AUTHORS

Eric L. Sophir | esophir@foley.com

Eugenia Wang | ewang@foley.com

Kathleen E. Wegrzyn | kwegrzyn@foley.com

What do teen digital artists, Tom Brady, Doja Cat, and Foley & Lardner LLP all have in common? They are all trending in popularity for their use of NFTs.

Jaiden Stipp is a digital artist, who at only 15 years old sells pieces of his digital artwork as NFTs.[1] "Forever Colored," one of Stipp's top-selling NFTs located here, sold for 20 ETH (ETH is the acronym for Ether, a form of cryptocurrency on the Ethereum blockchain). At the time, the 20 ETH from the sale of Stipp's "Forever Colored" traded for $30,000 USD, and a month after the sale, traded for closer to $60,000 USD.

Tom Brady is capitalizing on the popularity of NFTs through his launch of the startup NFT platform, Autograph, located here.[2] Tom Brady has teamed with the Hollywood studio Lionsgate and the sports betting site DraftKings to launch movie and sports-related NFTs.[3] In August of this year, Simone Biles announced she would release her first ever NFT collection on Autograph.[4]

Doja Cat launched her "Planet Doja" collection of NFTs in several tiers of tokens located here. Doja Cat's gold-tier NFTs come with a chance to win Doja Cat concert tickets, platinum-tier NFTs come with a chance to win VIP Doja concert tickets and other perks, and diamond-tier NFTs come with guaranteed VIP concert tickets.[5] The highest tier NFT, which comes with an all-expenses paid VIP experience for two fans to one of Doja Cat's concerts, sold for $188,888 USD.[6]

Foley & Lardner LLP is one of the first AmLaw 50 law firms to create, mint, list, sell and pursue the secondary market of an NFT live during the webinar entitled "Minting & Selling an NFT | Live Demo & Legal Analysis," presented by Foley attorneys Patrick Daugherty, Laura Ganoza, Jonathon Israel, Andrew Lee, Louis Lehot, Byron McLain, Eric Sophir, and Catherine Zhu.[7]

In addition, Foley represented the Utah Jazz in launching its Jazz NFT program, JAZZXR (where JAZZXR NFT owners receive exclusive access to a virtual tour of the Jazz's locker room using virtual reality technology),[8] and the Milwaukee Bucks on its NFT launch (which provided a limited edition series of digital artwork commemorating the Bucks' 1971 NBA championship).[9]

What is an NFT?

NFT is short for "non-fungible token." Fungibility refers to the ability of an item to be interchanged with other items of the same type. Cryptocurrency coins, for instance, are fungible because cryptocurrency coins are interchangeable—each coin is the same. On the other hand, NFTs are non-fungible because they are unique tokens (representing digital assets) that cannot be interchanged with other tokens.

When an NFT is minted, the NFT is recorded onto the blockchain. Due to the nature of blockchain, NFTs contain immutable data stored across a distributed ledger. This means that no one can unilaterally modify the record of ownership associated with an NFT, nor can anyone make another copy of an NFT.

While the media has recently highlighted NFT use for art and other high-end collectibles, NFTs have other valuable applications. For instance, users can mint NFTs for recording ownership of any unique asset. Users can even mint NFTs corresponding to items in

© 2022 Foley & Lardner LLP

the physical world, such as a deed to a car or a concert ticket. Those NFTs can be used to conduct transactions or represent those items in a virtual environment.

Uses for NFTs in Supply Chain

NFTs work for supply chain purposes because companies are particularly concerned with maintaining trustworthy digital data related to their physical world assets. Therefore, companies can benefit by using NFTs to represent their physical assets digitally. Some ways in which NFTs address supply chain needs are in the areas of tracing products through supply chains, identifying product origin and authenticating ownership, and verifying product certifications.

1. Traceability

Because NFTs can represent real world objects, supply chains can use NFTs to track a variety of products and materials. To track physical world objects via NFTs, the owner must create a digital representation of the physical object on the blockchain so that transactions related to the physical object can be safely stored and tracked.

Some ways NFT tokenization helps supply chains with traceability include:

Tracking Packages

Warehouse companies can create NFTs for packages upon shipment to a consumer so that at each step of the delivery, the blockchain records the new owner of the token, thus preventing loss of packages due to lack of visibility.

Tracking Packing Materials

3PL companies can assign NFTs to reusable packaging so that they can track who possesses the reusable packaging at all times.

Tracking Luxury Goods

Manufacturers can create NFTs to track luxury or other expensive goods, which may otherwise disappear within the company's internal supply chain as well as downstream.

Tracking Expensive Materials

Service providers for installation or construction work can create NFTs to track expensive materials such as optical fiber and network cards. Since service providers often rely on a network of subcontractors to handle expensive materials, using NFTs can minimize the loss of these materials and assist service providers in managing inventory.

2. Product Origin and Authentication

Because NFTs contain an immutable record of transactions, third parties can easily confirm the origin of a physical world product connected to the NFT as well as current and past owners of the product connected to the NFT. Programmers can even design NFTs to automatically kick a royalty back to the original creator of the NFT every time the NFT is resold.

For instance, the luxury watch brand, Breitling, introduced an NFT passport for each of its watches, which allows customers to receive the physical watch along with a digital version of the watch.[10] Customers can then use the digital passport to verify authenticity of their Breitling watch, prove their ownership of their Breitling watch, and transfer ownership of their Breitling watch upon resale.[11] Breitling has also tied the digital passport to its warranty program, allowing owners to track repairs to their watches.[12] Breitling plans to add functionality to the digital passport to allow users to extend the warranty period and add theft or loss insurance.[13]

3. Product Certifications

The modern-day consumer is selective about product certifications. As a result, providing consumers with trusted certifications such as "organic" and "fair trade" can increase sales. To accomplish this, third party certifiers for product standards or labor safety requirements could mint an NFT with the appropriate certification onto the blockchain, which supply chain members would pass downstream until it reaches the end user in the supply chain who can ultimately access the certification via a web link.[14]

Legal Issues Relating to NFTs

Largely, governments have not yet regulated NFTs. Still, NFTs pose a handful of legal issues, some of which are particularly applicable to supply chain uses of NFTs, including:

1. **Terms and Conditions.** Purchasers should pay attention to any standard terms and conditions applicable to the sale of an NFT, which could apply not only to the NFT itself, but also to any underlying physical or digital asset. If the NFT represents a physical good sold by a merchant to a consumer-purchaser, the seller will want to set forth terms and conditions governing issues such as redemption, warranties, return policy, and product defect, to avoid ambiguity and disputes over what rights the purchaser is entitled to with respect to the physical good. Merchants commonly provide consumer-purchasers with a web link to the terms and conditions related to the NFT.
2. **Transfer of Intellectual Property.** In the U.S., a copyright owner owns the exclusive rights to his or her own work.[15] Therefore, the intellectual property right related to an NFT does not automatically transfer with the sale of an NFT. Instead, the original owner selling an NFT must indicate upon minting, which intellectual property rights, if any, will transfer to the purchaser of the NFT.
3. **Royalties.** U.S. law may not entitle an original owner to resale royalties, but sellers may set up NFTs with smart contracts to provide automatic royalties to the original owner upon resale.[16] One potential challenge is to counter efforts by resellers that attempt to get around a programmed royalty fee by reselling the NFT on a different platform than the NFT was minted on.

Although NFTs are still nascent, they could provide companies with the opportunity to improve the efficiencies of their supply chains. The applicability of NFTs in supply chain are becoming increasingly apparent as companies continue to explore NFT uses and contribute to adoption of NFTs and other blockchain solutions.

Foley & Lardner LLP is one of the first AmLaw 50 law firms to create, mint, list, sell and pursue the secondary market of an NFT live during the webinar entitled "Minting & Selling an NFT | Live Demo & Legal Analysis," presented by Foley attorneys Patrick Daugherty, Laura Ganoza, Jonathon Israel, Andrew Lee, Louis Lehot, Byron McLain, Eric Sophir, and Catherine Zhu.

© 2022 Foley & Lardner LLP

Blockchain for Capital Equipment in a Machine-as-a-Service Model

AUTHORS

Emory Ireland | eireland@foley.com
John D. Lanza | jlanza@foley.com
Daniel Rose | drose@foley.com
Michael J. Walsh, Jr. | mike.walsh@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Subscription-based services, embraced by the software industry as an alternative to traditional models of selling product, provide a steady income stream to providers. Software-as-a-Service, along with the related Platform-as-a-Service, Network-as-a-Service, and Infrastructure-as-a-Service models, provide benefits to customers by shifting maintenance responsibilities to the vendor and exchanging large capital expenses for lower subscription fees.

What is a Machine-as-a-Service Model?

Following in the footsteps of the software industry, capital equipment manufacturers are beginning to adopt Machine-as-a-Service ("MaaS") models, providing manufacturing equipment such as Computerized Numerical Control ("CNC") machines or automated manufacturing systems on a subscription basis.

Unlike a traditional leasing model with a fixed monthly or weekly payment, customers may make MaaS subscription payments based on usage or outcome, such as monthly payments based on the number of units produced.[1] For example, in addition to conventional air compressor sales, Kaeser Compressors, Inc. now offers a MaaS compressed air service with a subscription fee for a fixed amount of compressed air.[2] The equipment manufacturer takes on additional risk with the possibility that client needs and corresponding revenue may decline but may find a much broader market of willing customers, particularly for the newest or most advanced machines that would be very expensive outright purchases.

Blockchain for Asset Tracking

Asset tracking is crucial for running a successful MaaS-based business. Vendors may collect operational data from manufacturing machines, including hours of operation, units produced, and operating efficiency statistics or faults and use the data for both pricing calculations and maintenance purposes (such as identifying when preventative maintenance operations should occur). Blockchain may collect this data directly at the machine through integrated sensors to provide the parties with an immutable operational record. By utilizing blockchain technology, both the vendor and user can feel confident that operational numbers are accurate and secure.[3]

In some instances, companies may use smart contracts based on data recorded to the blockchain to automatically execute arranged payments as manufacturing thresholds are reached. For example, SteamChain's Secure Transaction Engine for Automated Machinery ("STEAM") uses blockchain technology to generate tamper-free performance records that are accessible by both end users and vendors, and to execute payment transactions in real time.[4] Pearson Packaging Systems uses STEAM to provide packing machines under a MaaS model, with clients providing payments per erected, sealed, or palletized case via smart contracts.[5] By using blockchain for recording case counts and executing payment, the parties benefit from decreased human errors and increased transparency.

Automated Maintenance Requests via Smart Contracts

Companies can use smart contracts to automatically schedule maintenance for deployed MaaS machines. Because updated data and statistics for each machine are recorded to the blockchain ledger, companies can automatically monitor the performance of each machine

If efficiency degrades or other faults occur, a smart contract can dynamically generate a service request. For fee-based service agreements, smart contracts can also automatically process payments.[6]

A blockchain ledger provides a permanent and immutable record of maintenance history for the machine, which potential purchasers may find valuable when the vendor sells used capital equipment. Because each maintenance record is written to the ledger with a timestamp and that timestamp is encoded into each subsequent block, a bad actor would have difficulty faking records in case of missed maintenance windows.[7]

Dynamic Configuration Management

An end user may not want all of the available capabilities provided by a particular machine. Under conventional purchasing models, customers may have to purchase a more advanced or capable machine, at a correspondingly higher cost, in order to fulfill certain requirements, effectively buying "more machine" than they want. Conversely, if they cannot afford the capital expenditure, some customers will purchase less advanced equipment or equipment lacking desirable features. This may result in lower overall productivity and quality.[8]

Under a MaaS model, a vendor may deploy their most advanced machines to clients with one or more features disabled. Because the machines are connected to blockchain nodes for recording performance data, smart contracts may also be used to push configuration changes back to the machines. For example, a client may dynamically elect to enable a particular feature, and a smart contract will automatically process a payment or increased subscription fee and trigger the configuration change for the corresponding machine.[9]

Legal Issues Related to MaaS Models on Blockchain

When considering adopting a MaaS model supported by blockchain, companies will need to evaluate the accompanying legal issues, such as:

Automation. Because many decisions are made upfront for the structure of a MaaS model, and such decisions are executed by smart contracts, the parties will need to consider how to address changes to agreed-upon contract terms. For example, if a machine requests service but the customer would rather defer maintenance, this cannot be accomplished without cooperation from the vendor, as the maintenance is automatically ordered. This is an important consideration because customers likely will want to have the final say in requesting service as the payor, but the vendor will likely have service requirements that it will prefer to be automatically triggered. The parties will need to pay attention to whether a smart contract housed on blockchain has been programmed to be flexible or inflexible for tasks such as ordering maintenance.

Export Control. While dynamic configuration management can deselect certain features on a machine that is supported by blockchain, the parties will still need to comply with export control regulations and ensure that controlled technology is not being exported to a foreign country in violation of export control laws. Under current export control regimes, licensing authorities will evaluate the full capabilities of exported machines. The authorities are unlikely to grant licenses to export machines containing controlled technology that is not enabled, simply because a recipient could take steps to enable that technology. Unless capital equipment manufacturers program the blockchain solution to completely disable controlled functionality, it is unlikely that licensing authorities will relax export control regimes based solely on the adoption of a MaaS model.

"Right to Repair." The "right to repair" movement in the U.S. is growing and gaining influence in the policymaking process. In July 2021, President Biden issued an executive order directing the Federal Trade Commission ("FTC") to issue rules to remedy "unfair anticompetitive restrictions on third-party repair or self-repair of items, such as the restrictions imposed by powerful manufacturers that prevent farmers from repairing their own equipment."[10] While subscription-based MaaS models supported by blockchain technology undoubtedly offer benefits to customers, they allow manufacturers to retain control over the equipment well after a customer purchases a subscription. Manufacturers and customers looking to avail themselves of MaaS arrangements must make clear to the FTC, and to policymakers writ large, that these arrangements are outside the scope of anticompetitive behavior that the July 2021 executive order is looking to prevent.

Uniform Commercial Code. Although a MaaS model is typically characterized as a subscription service, it would likely be subject to Article 2A of the Uniform Commercial Code ("UCC"), which defines a lease as "a transfer of the right to possession and use of goods for a term in return for consideration…"[11] If the customer (lessee) defaults, the capital equipment manufacturer (lessor) will have all the remedies provided by Article 2A, including the right to recover the machine.[12] The manufacturer may want to take a back-up security interest in the machine under UCC Article 9 and file a financing statement to ensure its right to the machine is public record. The manufacturer should consider whether to re-characterize the lease as a sale with retention of a security interest, particularly if the customer has a right to purchase the machine at the end of the term at a price that is reduced by all or some portion of the payments already made.

A blockchain ledger provides a permanent and immutable record of maintenance history for the machine, which potential purchasers may find valuable when the vendor sells used capital equipment. Because each maintenance record is written to the ledger with a timestamp and that timestamp is encoded into each subsequent block, a bad actor would have difficulty faking records in case of missed maintenance windows.

Cryptocurrency for Supply Chain Payments

AUTHORS

John D. Lanza | jlanza@foley.com
Raj Tanden | rtanden@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Today's supply chains are frequently paper-based operations subject to human error and delay. Therefore, some companies are beginning to invest in digital infrastructure, including blockchain tools, to strengthen supply chain efficiency and visibility.

One benefit of using blockchain for supply chain management is that parties can cooperatively use smart contracts to make, track, and manage payments made in cryptocurrency (also referred to colloquially as "crypto"). For example, a smart contract may register and record acceptance of a shipment, triggering a notice message that payment is due to the supplier. A more advanced smart contract implementation allows the smart contract to go beyond sending a message and takes the next step to execute the crypto payment automatically.

Using Smart Contracts to Execute Payment

Using smart contracts to manage the execution of supply chain contracts and associated payments provides several beneficial features:

Accuracy

Smart contracts calculate payment amounts automatically, eliminating errors that may otherwise occur. Moreover, a smart contract can calculate payment amounts due to several parties for a single transaction almost instantaneously, regardless of geographic locations or cross-border issues.

Autonomy

Because smart contracts live on blockchain, they are highly resistant to tampering or manipulation, which makes them ideal for situations in which the parties to a transaction do not know each other well or when one of the parties operates in an unstable conventional economy.

Efficiency

Using smart contracts to execute payment automatically decreases the need for payment intermediaries and their associated fees. This is especially true for cross-border transactions because the parties making payment via smart contract typically use some form of cryptocurrency, which is a borderless currency. Payments made by cryptocurrency eliminate the need for currency conversion, which can be costly in terms of both fees and fiat currency fluctuation. However, cryptocurrency itself can be quite volatile; in 2021, Bitcoin's value ranged from a low of $29,000 to a high of $69,000.00.[1]

Enforcement

Programmers can configure smart contracts to release payment to a provider upon the occurrence of one of more events (such as the verified acceptance of delivery of goods). The smart contract will hold the buyer's payment until the occurrence of the programmed release event. If the release event does not occur, the smart contract will return the payment to the buyer.

Security

The currency used to pay for products or services in a smart contract, whether cryptocurrency or fiat currency, can be included in the smart contract itself. In those cases, there are fewer opportunities for payment information to be "skimmed' and subsequently misused. When fiat currency is included in the smart contract, the payor's bank and the receiver's bank must also be on the blockchain, which is a step that is avoided when payment is made by cryptocurrency.

© 2022 Foley & Lardner LLP

Non-repudiation

A smart contract can verify both delivery of goods and services, as well as the acceptance of the delivered goods and services. This reduces the opportunity for cancellations and chargebacks.

What's the Difference between Crypto Coins and Tokens?

Payors typically make payments via smart contract in one of two forms of cryptocurrency: coins (such as Bitcoin) and tokens.

Coins are built on their own, independent blockchain and are intended as a form of currency in and of themselves. The most well-known example of a coin is Bitcoin, which is built on the bitcoin network. Bitcoin can be used to directly pay for goods or services.

In contrast, **Tokens** are also built on a blockchain but are not considered currency. Instead, a token typically represents a right to a real-world resource, which can include money. For example, Ethereum's ERC-20 token standard defines a protocol for creating tokens that can be exchanged with each other.

It is sometimes said that a **Token** represents what one owns while a **Coin** represents what one can own.

Blockchain-enabled supply chains can be implemented using either coins or tokens and the choice has subtle implications on the operation of smart contract payments in the supply chain.

Scenario 1 – Coin-based Supply Chain

In the scenario of a coin-based supply chain, the payor makes the smart contract payments with a coin defined by the blockchain. Since cryptocurrency coins have inherent value, a payee may use the coins received in the same way that the payee would use currency, including the exchange into fiat currency, such as the U.S. dollar. To facilitate the exchange into fiat currency, a coin-based payment structure may use a stablecoin, which is a cryptocoin tied to a selected form of fiat currency, such as the USD Coin, which is guaranteed to have a 1:1 ratio with the U.S. dollar.

Scenario 2 – Token-based Supply Chain

In the scenario of a token-based supply chain, the payor makes the smart contract payments with a token defined by the blockchain used in the supply chain transactions. Since the tokens have no inherent value, a payee cannot use the received tokens in the same way that the payee would use currency. Instead, the payee must use the tokens to secure other services provided by the blockchain-issuing ecosystem. For example, in a token-based supply chain, tokens may represent physical goods and possession of a token may entitle the bearer to one "tokenized" item.

Legal Considerations for Cryptocurrency Use

Although payment with cryptocurrency provides numerous advantages, payment with cryptocurrency also poses some legal challenges.

US Federal Income Tax Treatment

The federal income tax treatment of virtual currency is uncertain. In 2014, the IRS indicated that, for federal income tax purposes, virtual currency, such as Bitcoin, is treated as property rather than currency.[2] Under this guidance, the receipt of virtual currency for payment is treated as the receipt of cash equal to the fair market value of the property upon receipt. Moreover, if the virtual currency is held as a capital asset, the holder can realize capital gains or losses in the currency when sold.

Securities Laws

William Hinman, Director of the SEC's Division of Corporation Finance, opined on June 14, 2018 that Bitcoin and Ethereum specifically are not securities.[3] However, the SEC has not clearly delineated when a cryptocurrency is considered a "security." It is therefore not clear whether U.S. securities laws apply to a particular cryptocurrency.

Infrastructure Bill (Public Law No: 117-58)

Despite heavy opposition from the digital currency industry, the infrastructure package signed into law by President Joe Biden in late 2021 brought about a series of cryptocurrency tax reporting requirements that will go into effect starting in 2023.[4] One such reporting requirement is that businesses receiving cryptocurrency payments of $10,000 or more must report the identity of the sender to the government, akin to the reporting requirement for cash transactions of the same amount.[5]

Smart Contracts and Blockchain

Because cryptocurrency transactions are accomplished using smart contracts on a blockchain, parties should also be cognizant of issues related to the legal recognition of smart contracts and contract terms related to blockchain. See "Smart Supply Chains Using Smart Contracts" for more information on the legal implications of blockchain in supply chain.

Despite these uncertainties, cryptocurrency payments via smart contracts could be a key to the success of 21st century supply chains.

One benefit of using blockchain for supply chain management is that parties can cooperatively use smart contracts to make, track, and manage payments made in cryptocurrency (also referred to colloquially as "crypto"). For example, a smart contract may register and record acceptance of a shipment, triggering a notice message that payment is due to the supplier. A more advanced smart contract implementation allows the smart contract to go beyond sending a message and takes the next step to execute the crypto payment automatically.

Blockchain for Digital Logistics and Smart Warehouses

AUTHORS

Eric L. Sophir | esophir@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Manufacturers spend a pretty penny managing inventory logistics (the management of inbound and outbound flows of goods) and inventory warehousing (the receipt, storage, and distribution of goods).

In good times, controlling logistics costs presents a challenge. In times of global disruption, the costs can border on unmanageable.[1] COVID-19 alone caused huge shortages of consumer products and surges in shipping costs.

The World Container Index
reflecting the composite cost of shipping a 40-foot container across eight major trade routes globally
is up 360% since 2020

- CNN Business, August 23, 2021

In the warehousing sector, a combination of pandemic-driven demand and big-box stores racing to compete with Amazon have caused the cost of warehouse space to skyrocket.[3] Companies also face continually increasing warehouse costs due to a rise in construction costs, as well as an increase in investment in sophisticated warehouse robots to automate warehousing.[4]

The Bloomberg Industrial/Warehouse Index
which measures the value of real estate investment trusts with **75%** or more invested assets in industrial/warehouse properties
is up 45% since the beginning of 2020

- Forbes, September 3, 2021

Due to the increasing costs involved in managing the flow of inventory, tools to reduce logistics and warehousing costs, such as blockchain technology, are more appealing than ever.

Blockchain Basics for Logistics and Warehousing

Blockchain is a distributed ledger that stores immutable data, shared by participating blockchain network members. A manufacturer can use blockchain to record and view transactions at every step in the supply chain. The distributed ledger format provides companies with a single, unchanging truth to reference for logistics and warehouse planning, management, and dispute resolution.

Companies also benefit from the secure nature of blockchain. Because of blockchain's immutable and decentralized structure, hackers would find it very difficult to target encrypted information stored on blockchain.

Blockchain Benefits for Logistics

Logistics networks today suffer from complexity and inefficiencies due to lack of visibility and antiquated paper documentation systems. Blockchain remedies these issues.

Lack of Visibility

Because of the complexity of logistics networks, companies often have blind spots in their supply chain, making it difficult to locate products at any given time. Because of this lack of visibility, companies face difficulties in identifying performance lapses. Unavailability of real-time tracking further hinders companies attempting to schedule delivery times and efficiently use company assets.

Blockchain combats inefficiencies by allowing companies to track products in real time and store the related data on a tamper-proof ledger. Blockchain stores information on a shared ledger viewable by all permitted parties, so companies can also reduce administrative processes.

Paper-based Systems

Because logistics networks typically run on paper-based records, each company that touches a product must manually keep records on that product, leading to redundant or potentially inconsistent records. Further, bad actors can easily forge paper documentation. Finally, supply chain members may be slow to deliver and process paper documentation in comparison with digital documentation. In today's logistics supply chain, containers of product can become stuck at the port while officials wait for the paper bill of lading (which acts as contract of carriage, confirmation of product receipt, and document of title) to arrive.

By shifting data and processes to blockchain, companies have access to a system that houses trusted data, which is resistant to cyberattacks and fraudulent manipulation. Blockchain also allows companies to use smart contracts to automate payments and sign documents, which can save time in comparison to traditional manual processes.

With respect to bills of lading, blockchain provides the technology needed to graduate past paper bills of lading and use secure electronic bills of lading ("eB/Ls") instead. However, a single bill of lading can travel though many countries and change hands through a variety of participants (traders, buyers, carriers, etc.). The complexity inherent in coordinating a manual to digital change in process for a large number of participants hinders widespread adoption of eB/Ls. One challenge is that not all participants may want to engage in the blockchain. Another challenge is that many jurisdictions have not definitively addressed the legal status of electronic transferable records. In order to pave the way to digitize the centuries-old bill of lading format, the United Nations Commission on International Trade Law has published a model law to govern the use of electronic transferable records (such as bills of lading and bills of exchange).[7]

Blockchain Benefits for Warehousing

As the demand for warehousing increases, the challenges of tracking and managing warehouse inventory have become ever more apparent. Blockchain alleviates the challenges presented in tracking and managing inventory.

Moving Beyond Reactive Inventory Management

Companies usually operate warehouses on a very reactive basis, meaning that companies order more inventory only when stock runs low or predictive models (which can take time to populate) forecast the need to order more inventory.

Blockchain allows companies to track exactly which product is located in the warehouse at a given time. Blockchain technology also allows manufacturers to see end user demand in real time, allowing for better management of manufacturing planning and nimble inventory allocation and replenishment. Warehouses may still rely on a minimum stock volume or predictive models, but blockchain optimizes the determinations more accurately and more timely.

Minimizing Manual Processes

Companies largely operate warehouses using manual processes, including for tracking locations of inventory, picking inventory, and monitoring inventory. While companies continue to phase out manual processes with the advent of warehouse automation advances (such as drones that count inventory and robots that assist laborers with picking), smart warehouses can further increase automation by implementing blockchain. Blockchain increases stocking, replenishing, picking, and packaging efficiencies due to digitization of recordkeeping and use of smart contracts.

Smart Contract Solutions

Blockchain technology allows for implementation of "smart contracts," which are computer programs that automatically execute an action according to a pre-determined set of rules. This feature can simplify transactions between supply chain members and offer an audit trail for those transactions. Supply chain members can be paid faster and reduce administrative costs. Logistics and warehouse companies can use smart contracts to:

- Automate recordings of delivery times and receipt of goods into inventory.
- Automate payments for inventory received.
- Alert relevant parties if product held in inventory will expire or if the price of product held in inventory has met a strike price.
- Work with IoT devices to trigger alerts if warehouse or shipping container conditions change, such as temperature and humidity.
- Automate payment of credits for failure to meet Service Level Agreement (SLA) and Key Performance Indicator (KPI) metrics.
- Automate recording of product transfers between supply chain members from factory to consumer.
- Execute trade deals automatically by connecting importers, exporters, and their respective banks to the blockchain to reduce duplicative paperwork and redundant quality assurance processes.

See "Smart Supply Chains Using Smart Contracts" for more information on smart contracts and the various legal issues to be considered when using them.

> Due to the increasing costs involved in managing the flow of inventory, tools to reduce logistics and warehousing costs, such as blockchain technology, are more appealing than ever.

Designing Blockchain for Logistics and Warehousing

Blockchain can uniquely address the challenges faced by companies in the logistics and warehousing steps of the supply chain by providing streamlined delivery processes and improved inventory management. However, complexity of supply chains and hesitancy to invest in the blockchain infrastructure could pose barriers to blockchain adoption in the logistics and warehousing spaces.

As a result, leading companies, such as UPS, Penske, and Salesforce, formed the Blockchain in Transport Alliance ("BiTA") the largest commercial blockchain alliance in the world.[8] BiTA has over 500 members in 25 countries,[9] including 3PLs/4PLs, logistics companies, air freight companies, railroads, trucking companies, blockchain consulting services, SaaS technology companies, and original equipment manufacturers.[10] BiTA aims to drive the adoption of blockchain technology forward and develop a framework and standards for marketplace participants to effectively build blockchain applications.

In another effort to digitize the logistics industry, Maersk and IBM developed the TradeLens platform, designed with blockchain technology to create greater collaboration and trust across the global shipping industry.[11] IBM and Maersk built the TradeLens platform using Hyperledger Fabric blockchain technology and IBM cloud[12] to digitally connect shippers, freight forwarders, ports and terminals, customs brokers, and other important members of the global supply chain ecosystem.[13]

Still, there is no standard blockchain solution for logistics and warehousing, so companies should evaluate whether blockchain would be a cost-effective solution for obtaining a leaner and more efficient supply chain.

Blockchain for Critical Minerals

AUTHORS

Michael J. Walsh, Jr. | mike.walsh@foley.com
Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

Critical minerals, which include rare earth minerals, are generally defined as minerals that are important to supply chains, but difficult to mine and ship due to scarcity, geopolitical issues, trade policy, or a combination of the three. The U.S. Department of the Interior identified 35 critical minerals that (1) are "essential to the economic and national security of the United States," (2) have supply chains that are "vulnerable to disruption," and (3) serve "an essential function in the manufacturing of a product, the absence of which would have significant consequences for our economy or our national security."[1] The list of critical minerals includes familiar minerals like aluminum, tungsten, and tin;[2] minerals critical to electrification like lithium and cobalt; minerals critical to manufacturing like magnesium, manganese, niobium, and vanadium; and minerals used for nuclear fuel like uranium. Companies use these critical minerals to make mobile phones, airplanes, advanced electronics, wind turbines, electric cars, solar panels, and electricity generation and transmission systems. They are crucial for innovation, economic growth, and national security. Demand for critical minerals is increasing in the United States and worldwide as countries seek clean energy alternatives.

The United States relies heavily on imports to satisfy its demand for critical minerals, and importers rely heavily on China for critical and rare earth elements. The Trump administration took steps to increase domestic production of critical minerals with bipartisan support, and the Biden administration continues to recognize U.S. reliance on imports from China.[3] In his February 24, 2021 executive order ("EO") on supply chain resiliency, President Biden directed the U.S. Secretary of Defense to identify risks in the supply chain for critical minerals and create policy recommendations to address those risks.[4]

Niobium:

Niobium is used in alloys (mix of metals) for jet and rocket engines due to temperature – stabilizing properties.

Bismuth:

Bismuth oxychloride is used as a pigment in cosmetics, such as eye shadows, due to the iridescent appearance.

Iridium:

Iridium, when combined with Albumin, is used in a process to destroy cancer cells.

Cobalt:

Cobalt, which is found in abundance in seabed roots, is used in rechargeable batteries for electric vehicles.

Zinc:

Zinc pyrithione is used in shampoo to prevent dandruff.

© 2022 Foley & Lardner LLP

Challenges Associated with Critical Mineral Sourcing

Critical mineral supply chains face major challenges. First, the lack of an industry certification standard makes it difficult to compare performance from one mine to another. Second, critical minerals are fungible (*e.g.*, there is no way to differentiate one kilogram of cesium from another). Third, some companies may illegally mine rare earth minerals and sell them into the supply chain without any paper trail. Finally, a number of countries impose restrictions and regulations on critical minerals.

In the United States, the federal government heavily regulates critical mineral sourcing. In June, 2021, the U.S. Customs and Border Protection ("CBP") issued a Withhold Release Order ("WRO") against Hoshine Silicon Industry Co. Ltd. ("Hoshine"), a company located in China's Xinjiang Uyghur Autonomous Region ("XUAR").[5] The WRO instructed personnel at all U.S. ports of entry to detain shipments containing silica-based products made by Hoshine and its subsidiaries.[6] This WRO applies not only to silica-based products made by Hoshine and its subsidiaries but also to materials and goods derived from or produced using those silica-based products.[7] When the CBP issues a WRO pursuant to 19 U.S.C. §1307, the importer of record bears the burden to provide documentation that the withheld product was not produced or mined using forced labor.[8] Given the complexity and opacity of Chinese supply chains, as well as paper recordkeeping practices where records can be lost, altered, or falsified, companies may find this standard difficult to meet, even in instances where the product is in fact free from forced labor.

On December 23, 2021, President Biden signed the Uyghur Forced Labor Prevention Act (the "UFLPA"), which requires the CBP to block all shipments of goods from the XUAR because they are presumed to have been made with forced labor. The presumption is rebuttable, but at the time of this publication, there is no consensus within industry or government on the types of evidence that can be presented to the CPB to rebut the presumption of forced labor. And the stakes are high – when the CBP finds that an importer successfully rebutted the presumption – it must issue a report to Congress stating as much. Fortunately for U.S. importers, the Department of Homeland Security has asked the public to provide input on the types of due diligence, supply chain tracing and supply chain management measures that importers can use to prevent the import of goods made with forced labor and the nature and types of evidence that importers can provide to rebut the presumption of forced labor in products from the XUAR.[9]

Blockchain Technology for Critical Minerals

Blockchain tracing technology facilitates improved management of geopolitical risk and supply chain uncertainty because records held on blockchain are digital, trusted, and time-stamped.

Digitized Records

With blockchain, importers no longer need to ask their suppliers, who must in turn ask their own suppliers, for paper documentation of the origin of critical minerals. The paper process is labor intensive, time consuming, and sometimes not sufficient to satisfy import requirements. Blockchain would allow importers – and the CBP – at the time of import, to differentiate between products subject to, and products not subject to, the UFLPA or a WRO, without referencing a paper trail.

Trusted Records

Blockchain technology provides secure, immutable records that allow importers to confirm accountability from their global suppliers and to rebut the presumption under the UFLPA that the supplier used forced labor to mine the metals. Blockchain technology could prove particularly useful in this context because miners in the XUAR do not necessarily export these rare earth metals directly. For example, the XUAR is an important source of rare earth metals used in consumer electronics and aviation, and products made elsewhere in China may incorporate rare earth metals mined in the XUAR. Further, some rare earth metals enter the global supply chain indirectly after export to other countries. If the CBP were to target rare earth metals mined in the XUAR as part of the UFLPA, blockchain technology would make clear to U.S. importers (and the CPB) whether an engine manufactured in Thailand contains rare earth metals mined in the XUAR.

Time-stamped Records

Because blockchain transactions are time-stamped and may be recorded at every stage of the supply chain, blockchain further helps suppliers to act in real time, ensuring supply chain integrity from start to finish.

Implementing Blockchain for Critical Mineral Tracing

Blockchain technology has arrived at a fortuitous time for U.S. importers and provides a powerful tool for industries struggling with supply chain traceability issues. The government of Australia, the world's second largest producer of critical minerals[10] after China, recognizes as much. In July 2021, the Australian government awarded a $3 million AU pilot project to the blockchain provider, Everledger.[11] The pilot project will use Everledger's blockchain technology to create a "digital certification" for critical minerals throughout the supply chain – from extraction to processing to export to global markets.[12] Australia perceives that companies throughout the critical minerals supply chain could use the technology to simplify traceability, lower costs, and better comply with supply chain traceability regulations in their home countries. The Australian government also hopes this "digital certification" will increase the demand for Australian minerals in global markets while simplifying the process and lowering costs.

Similarly, Teck, one of Canada's leading mining companies with operations in Canada, the U.S., Chile, and Peru[13] has identified potential benefits blockchain could provide to the mining industry and announced a partnership with DLT Labs to harness blockchain technology to trace the critical mineral germanium from the source to the customer.[14] Germanium is used for fiber optic cables and high-speed computer chips and circuitry; Germanium is considered a necessary ingredient for modern-day communications platforms and low-carbon economies.[15] Teck and DLT Labs plan to use the new blockchain solution to go beyond recording data relating to responsible sourcing; they also plan to use it to track environmental, social and governance practices along the supply chain, including greenhouse gas emissions and product certifications.[16]

Given the United States government's increased use of trade policy to promote national security objectives, and given the unreliable nature of manual documentation for supply chain traceability purposes, critical mineral sourcing is ripe for the use of blockchain.

> Blockchain tracing technology facilitates improved management of geopolitical risk and supply chain uncertainty because records held on blockchain are digital, trusted, and time-stamped.

© 2022 Foley & Lardner LLP

Blockchain Buzzwords: Common Blockchain Definitions

AUTHORS

Eugenia Wang | ewang@foley.com
Kathleen E. Wegrzyn | kwegrzyn@foley.com

A Glossary of Blockchain Terms

Accord Project – A non-profit, collaborative initiative for developing an ecosystem and open source tool for “smart legal contracts.”

Block – A set of data.

Block Header – A summary of the data in the block.

Blockchain – A distributed ledger comprised of immutable blocks chained together to create an encrypted history of transactions.

Central Authority – An individual, organization or group which controls a permissioned blockchain.

Centralization (in blockchain) – A system in which control and decision-making is handled by a central authority, which may be an individual, organization or group.

Centralized (or Traditional) Database – A system in which data is stored in a single location.

Consensus – The process for determining the order in which blocks are added onto the blockchain and which nodes get to add the blocks.

Consortium Blockchain – A permissioned blockchain governed by a group of organizations.

Cryptocurrency – A virtual currency that is exchanged using blockchain.

Decentralization (in blockchain) – A system in which control and decision-making is handled by a distributed network instead of by a central authority.

Distributed Ledger – A system in which data is stored and shared across multiple sites, countries, or institutions.

Encryption – The encoding of information which converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.

Full node – A node that contains a complete history of the blockchain and which is responsible for validating blocks.

Hash – A string of characters that uniquely identifies data.

Hash (of a block in blockchain) – A unique identifier for the block attained by performing a cryptographic function on the header of the block. A block stores the hash for the previous block to form a link between the two blocks.

Hybrid Blockchain – A blockchain controlled by a single organization, with a certain level of oversight performed by a public blockchain that is required to perform certain transaction validations.

Immutable – Unable to be altered.

Internet of Things (“IoT”) – Real world physical objects with embedded sensors, software, and other technologies that are used for the purpose of connecting and exchanging data with other devices and systems that are linked to the internet.

Light Node (or Lightweight Node) – A node that only stores block headers in order to validate transactions on the blockchain. Light nodes are dependent on full nodes to function.

Miner (or Mining Node) – A node that creates a block on a permissionless blockchain.

Natural Language – Ordinary speech or language (as contrasted with computer code).

Nodes – Computers, laptops, servers or other computer devices connected to the internet.

Non-fungible Token ("NFT") – A digital asset with a unique identifying code, which represents real-world objects.

Permissioned Blockchain – A blockchain that requires permission from a central authority to join.

Permissionless Blockchain – A blockchain that does not require permission to join.

Private (or Managed) Blockchain – Permissioned blockchains controlled by owners.

Provenance – The origin of something.

Pseudo-anonymity – Designation of a user by a pseudonym whereby no actual identity information is revealed.

Public Blockchains – Permissionless, completely decentralized blockchains.

QR (Quick Response) Code – A type of barcode that can encode information like phone numbers or internet addresses, and can be easily read with digital devices such as smart phones or tablets.

RFID (Radio Frequency Identification) – A form of wireless communication that uses radio frequency waves to identify objects.

Smart Contract – A computer program that will perform a task when a pre-determined event is triggered.

Smart Legal Contract – A legally binding agreement that is digital and able to connect its terms and the performance of its obligations to external sources of data and software systems.

Smart Tag – An electronic label that contains a RFID device and/or barcode technology for the purposes of tracking and storing data.

Supply Chain Traceability – The ability to track the movement of a product forward through the supply chain from raw material to finished good and backward from finished good to raw material.

Validating a Block (or Validating a Transaction) – The act of verifying that data in a block comports with the rules of the blockchain.

Article Footnotes

An Overview of Blockchain in Supply Chain: What's the Link?

1 *Building a Transparent Supply Chain*, Harvard Business Review (May-June 2020), *An Integrated Impact of Blockchain on Supply Chain Applications*, Logistics (2021).

2 *How can blockchain power industrial manufacturing?* PwC, (last retrieved July 6, 2021).

3 *Deloitte's 2020 Global Blockchain Survey: From Promise to Reality*, Deloitte Insights (2020).

4 *The Worldwide Blockchain Supply Chain Industry is Expected to Reach $3+ Billion by 2026 – ResearchAndMarkets.com.* Businesswire (March 16, 2021).

5 Dimitrov, Biser. *How Walmart and Others Are Riding a Blockchain Wave to Supply Chain Paradise,* Forbes (December 5, 2019).

6 Kemp, Leanne, *Everledger's Pioneering Blockchain Work for Diamonds*, IBM (May 23, 2018); *Everledger*, Forbes (February 12, 2020).

7 *Our Industry Solutions*, Everledger, (last retrieved July 14, 2021).

8 Dimitrov, *supra* note 5; *IBM Food Trust. A New Era for the World's Food Supply,* IBM, (last retrieved July 6, 2021).

9 *Amazon Managed Blockchain Now Supports Hyperledger Fabric v.1.4*, AWS (September 15, 2020); *Supply Chain Management*, AWS, (last retrieved July 6, 2021); *What is Hyperledger?* Hyperledger, (last retrieved July 11, 2021).

Types of Blockchain: Public, Private, or Something in Between

1 *CargoSmart and Maritime Industry Operators Commit to Transforming the Shipping industry*, CargoSmart (July 12, 2019); *Our Platform*, GSBN, (last retrieved July 19, 2021).

2 *The Worldwide Blockchain Supply Chain Industry is Expected to Reach $3+ Billion by 2026 – ResearchAndMarkets.com.* Businesswire (March 16, 2021).

The Pros and Cons of Blockchain in Supply Chain

1 *Editing the Uneditable*, Accenture, (last retrieved July 20, 2021).

2 *Accenture Breaks Blockchain Taboo with Editing System*, Reuters (September 20, 2016).

The Fast Track: Using Blockchain to Trace Products Through the Supply Chain

1 Smith, Matt, *In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens*, Walmart (September 24, 2018).

2 *Id.*

3 Smith, Matt and Kane Webb, *A Valentine Meal with Food Safety and Sustainability at its Heart*, Walmart (February 9, 2021).

4 *Blockchain 50 2021*, Forbes (February 2, 2021).

5 *Supra* note 4.

6 *IBM Food Trust eBook*, IBM, (last retrieved July 18, 2021); IBM *Food Trust: A new era in the world's food supply*, IBM, (last retrieved July 18, 2021).

7 *The Food on Your Holiday Table May Have Been Verified by Blockchain*, Forbes (December 23, 2019).

8 Thomasson, Emma, *Carrefour says Blockchain Tracking Boosting Sales of Some Products*, Reuters (June 3, 2019).

9 *Carrefour Applies Blockchain Technology to its Eight Product – Rocamadour, the First Carrefour Quality Line Cheese to Use It*, Carrefour (April 26, 2019).

10 *Drug Supply Chain Security Act (DSCSA)*, U. S. Food & Drug Administration.

11 *Merck, IBM, KPMG, and Walmart Successfully Complete FDA Pilot Program to Evaluate the Use of Blockchain to Help protect Pharmaceutical Product Integrity,* Merck (May 4, 2020).

12 Banerjee, Arnab, *Integrating Blockchain with ERP for a Transparent Supply Chain*, Infosys (2018).

Smart Supply Chains Using Smart Contracts

1 Levi, Stuart D. and Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, Harvard Law School Forum on Corporate Governance (May 26, 2018).

2 *See* Restatement (Second) of Contracts § 24 (AM. LAW INST. 1979).

3 *See* Restatement (Second) of Contracts § 22-23 (AM. LAW INST. 1979).

4 *See* Restatement (Second) of Contracts § 71 (AM. LAW INST. 1979).

5 *See* Uniform Commercial Code § 2-201(1).

6 *Uniform Commercial Code and Emerging Technologies Committee*, Uniform Law Commission, (last retrieved September 7, 2021).

7 *Uniform Commercial Code and Emerging Technologies*, Uniform Law Commission (July 9-15, 2021).

8 *Frequently Asked Questions*, the Accord Project (last retrieved August 22, 2021).

9 *Id.*

10 Groschopf, Wolfram et al., *Smart Contracts for Sustainable Supply Chain Management: Conceptual Frameworks for Supply Chain Maturity Evaluation and Smart Contract Sustainability Assessment*, Frontiers in Blockchain (April 9, 2021).

Legal Implications of Blockchain in Supply Chain: What's Law Got to Do With It?

1 *The Electronic Signatures in Global and National Commerce Act (E-Sign Act)*, FDIC Consumer Compliance Examination Manual – January 2014.

2 *Final Act, With Comments: Uniform Electronic Transactions Act* (1999), Uniform Law Commission (last retrieved on September 8, 2021).

3 *Uniform Electronic Transactions Act (UETA)*, Practical Law (last retrieved July 22, 2021).

4 ARS § 44-7061; TN Code § 47-10-202.

5 *Wyoming's Digital Assets Amendments: Marked Out or Missed Out? A Review of Recent Amendments to Article 9 of the Wyoming UCC*, American Bar Association (October 1, 2019).

6 *Id.*

7 Art. 17 GDPR and Cal. Civ. Code § 1798.105.

8 *GDPR & Blockchain: At the Intersection of Data Privacy and Technology*, BDP (last retrieved July 22, 2021).

9 15 U.S.C. § 1.

Get Real: Preventing Counterfeit Product with Blockchain

1 Sularia, Sanjeev, *The Counterfeit Problem and how Retailers Can Fight Back in 2020*, Forbes (March 17, 2020).

2 Schlesinger, Jennifer and Andrea Day, *Here's how the Trade War could Lead to a Boom in Counterfeit Goods*, CNBC (March 13, 2019).

3 *Counterfeit Goods: A Danger to Public Safety*, U.S. Immigration and Customs Enforcement (last retrieved August 9, 2021).

4 Akash Bhatia et al., *Stamping Out Counterfeit Goods with Blockchain and IoT*, BCG (May 17, 2019).

5 Roberto Fontana et al., *How Luxury Brands Can Beat Counterfeiters*, Harvard Business Review (May 24, 2019).

6 *LVMH Partners with Other Major Luxury Companies on Aura, the First Global Luxury Blockchain*, LVMH (April 20, 2021).

7 *Id.*

8 *Id.*

9 *Aura* (last retrieved August 16, 2021).

10 Blockchain: *A New Security Check for Medicines*, Merck KGaA, (last retrieved August 16, 2021).

11 Gertrude Chavez-Dreyfuss, *Companies in Pharmaceutical Supply Chain Develop System to Track Counterfeit Drugs*, Reuters (February 21, 2020).

12 Honeywell, *iTrace and SecureMarking Combat Counterfeit Activity in Aerospace with Blockchain*, Honeywell (December 16, 2019).

13 *Supra*, note 4.

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.*

Not By the Same Token: NFTs in Supply Chain

1 Bruner, Raisa, *Teen Artists Are Making Millions on NFTs. How Are They Doing It?* Time (September 7, 2021).

2 Steigrad, Alexandra, *Tom Brady's NFT Platform Autograph Partners with Lionsgate, DraftKings*, NY Post (July 21, 2021).

3 *Id.*

4 Beer, Tommy, *Simone Biles to Release Her First NFT Collection Tuesday, Cashing in on Booming Market*, Forbes (August 31, 2021).

5 Hissong, Samantha, *Doja Cat Gets Into the NFT Game*, RollingStone (September 8, 2021).

6 *Id.*; *The Rise of Planet Doja*, OneOf, (last retrieved September 23, 2021).

7 *Minting & Selling an NFT | Live Demo & Legal Analysis*, Foley & Lardner LLP (September 14, 2021).

8 *Foley Assists Utah Jazz in Launch of Digital NFT with Virtual Locker Room Access*, Foley & Lardner LLP (September 24, 2021).

9 *Foley Assists Milwaukee Bucks in Launch of 1971 Championship NFT Collection*, Foley & Lardner LLP (June 16, 2021).

10 Girod, Stephane, *Breitling Shows Other Luxury Brands How to Future Proof With Agility*, Forbes (August 27, 2021).

11 *Breitling Becomes the First Luxury Watchmaker to Offer a Digital Passport Based on Blockchain for All of its New Watches*, Breitling (October 13, 2020).

12 *Id.*

13 *Id.*

14 Ricardo Borges dos Santos et al., *Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens*, MDPI, Sensors 2021.

15 U.S. Copyright Act §106

16 *Resale Royalty Right*, U.S. Copyright Office (last retrieved November 6, 2021).

Blockchain for Capital Equipment in a Machine-as-a-Service Model

1 Daniel Küpper et al., *Blockchain in the Factory of the Future*, BCG (July 15, 2019).

2 Ashley Ferguson, *What is an IoT-Enabled Machine-as-a-Service*, Losant (February 6, 2020); *Sigma Air Utility: Air as a Service*, Kaeser Compressors (last retrieved September 14, 2021).

3 *Blockchain and the Making of Making of Machine-as-a-Service*, iTMunch (April 17, 2019).

4 Stephanie Neil, *Blockchain and the Making of Machine-as-a-Service*, AutomationWorld (March 18, 2019); *Using Machine Performance Data to Drive Value*, SteamChain, (last retrieved September 14, 2021).

5 *Machine-as-a-Service (MaaS)*, Pearson Packaging Systems (retrieved September 12, 2021).

6 *Supra* note 1.

7 *Id.*

8 *Supra* note 3.

9 *Supra* note 1.

10 Michael J. Walsh et al., *Right to Repair and the Biden Competition EO – What Manufacturers Need to Know*, Foley & Lardner LLP (July 14, 2021).

11 U.C.C. §2A-103(j)

12 U.C.C. §2A-523

Cryptocurrency for Supply Chain Payments

1 *Bitcoin Price*, Coinbase, (last retrieved November 16, 2021).

2 *Notice 2014-21*, IRS, (last retrieved November 16, 2021).

3 William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)*, U.S. Securities and Exchange Commission (June 14, 2018).

4 Pub. L. 117-58; Davison, Laura, *How Taxing Crypto Got Changed by Biden's Infrastructure Law*, Bloomberg (November 17, 2021).

5 *Id.*

Blockchain for Digital Logistics and Smart Warehouses

1 Ziady, Hanna, *The Shipping Crisis is Getting Worse. Here's What that Means for Holiday Shopping*, CNN Business (August 23, 2021).

2 *Id.*

3 Levy, Ari, *Soaring Warehouse Demand Boost Commercial Real Estate Market as Office Vacancies Mount*, CNBC (July 10, 2021).

4 *Id.*

5 Resource Real Estate Diversified Income Fund, *Certified Shareholder Report of Registered Management Investment Companies*, United States Securities and Exchange Commission (September 30, 2018).

6 Friesen, Garth, *No End in Sight for the COVID-Led Global Supply Chain Disruption*, Forbes (September 3, 2021).

7 Clyde & Co LLP, *The Legal Status of Electronic Bills of Lading; A Report for the ICC Banking Commission*, The International Chamber of Commerce (2018).

8 *BiTA Members*, BiTA, (last retrieved September 6, 2021); *Blockchain in Transport Alliance*, BiTA, (last retrieved September 6, 2021).

9 *Blockchain in Transport Alliance*, BiTA, (last retrieved September 6, 2021).

10 *BiTA Members*, BiTA, (last retrieved September 6, 2021).

11 *About TradeLens*, Maersk, (last retrieved September 6, 2021).

12 *The Platform*, Maersk, (last retrieved September 6, 2021).

13 *The Ecosystem*, Maersk, (last retrieved September 6, 2021).

Blockchain for Critical Minerals

1 *Interior Releases 2018's Final List of 35 Minerals Deemed Critical to U.S. National Security and the Economy*, Department of the Interior, U.S. Geological Survey (May 18, 2018).

2 The U.S. and E.U. designated tungsten, tin, and tantalum as "conflict minerals," a term that is not synonymous with critical minerals. Conflict minerals are minerals mined in parts of the world where conflict affects the mining and trading of the minerals. U.S. and E.U. law requires companies that import these minerals to certify that they were mined outside of a conflict zone or certified as "conflict-free."

3 *See U.S. Department of Commerce Announces Section 232 Investigation into the Effect of Imports of Neodymium Magnets on U.S. National Security*, U.S. Department of Commerce (September 24, 2021).

4 E.O. 14017.

5 *See The Department of Homeland Security Issues Withhold Release Order on Silica-Based Products Made by Forced Labor in Xinjiang*, U.S. Customs and Border Protection (June 24, 2021); Walsh, Michael J. et al., *Forced Labor Sanctions in the Solar Industry – What You Need to Know*, Foley & Ladner LLP (June 25, 2021).

6 *Id.*

7 *Id.*

8 *Forced Labor*, U.S. Customs and Border Protection, (last retrieved December 28, 2021).

9 Walsh, Michael J. et al., *Uyghur Forced Labor Prevention Act – Comment Period Open until March 10, 2022*, Foley & Ladner LLP (January 27, 2022).

10 *Critical Minerals*, Global Business & Talent Attraction Taskforce Australia, (last retrieved September 28, 2021); Daly, Tom, *China Becomes World's Biggest Importer of Rare Earths: Analysts*, Reuters (March 13, 2019).

11 Press Release: *Everledger Wins Major Australian Government Critical Minerals Blockchain Pilot Project*, Everledger (July 12, 2021).

12 *Id.*

13 *About*, Teck (last retrieved February 22, 2022).

14 *Teck and DLT Partner to Pilot Traceability for Critical Minerals with Blockchain*, Teck (January 20, 2022).

15 *Id.*

16 *Id.*

ABOUT FOLEY & LARDNER LLP

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With over 1,100 lawyers in 25 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical, and beneficial to their businesses. Learn more at Foley.com.

FOLEY

FOLEY & LARDNER LLP

FOLEY.COM

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI | MILWAUKEE
NEW YORK | ORLANDO | SACRAMENTO | SALT LAKE CITY | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. Images of people may not be Foley personnel. © 2022 Foley & Lardner LLP | 22.MC38849