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.

**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. 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.

### 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 Article 5 of this “Blockchain in Supply Chain” series 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
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.


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.


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

9. 15 U.S.C. § 1


© 2021 Foley & Lardner LLP

National Law Review, Volume XI, Number 280