Alternatives

TO THE HIGH COST OF LITIGATION

The Newsletter of the International Institute for Conflict Prevention & Resolution

VOL. 39 NO. 4 • APRIL 2021

ADR & Technology/Part 1 of 3

A Guidebook to Arbitrating Disputes Involving Blockchains and Smart Agreements

BY PETER L. MICHAELSON & SANDRA A. JESKIE

Blockchain-based distributed ledgers, referred to here as Blockchain Ledgers, provide an immutable, secure, and tamper-evident alternative to conventional transactional modalities, one which also yields enhanced accountability, traceability, and transparency.

These inherent benefits, and hence growing adoption of, Blockchain Ledgers, Smart Contracts and recently Smart Legal Contracts (the latter two being built on blockchains), across a wide range of the economy, has caused and is now accelerating a fundamental paradigm shift. This movement, in certain sectors of society, is increasingly displacing traditional written and oral contracts with automatically executing blockchain-implemented agreements.

For ease of reference and to prevent confusion, when "Smart Contracts" and "Smart Legal Contracts" are collectively discussed below, then, depending on context, they will be referred to as "smart agreements."

This article begins a series that will explain how blockchain technology is being used to change the way contracts are written, executed, and maintained, and how the disputes that arise are best addressed.

The authors first provide in this Part 1 background and a contextual foundation, and conclude the introduction to Blockchain Ledgers next month. Also, see box at end of Part 1 on page 69. Part 2 in May also will address certain inherent limitations and examine common legal issues underlying smart agreements. And finally, in June the authors discuss arbitration, and its various advantages, as the most viable approach for handling blockchain-based disputes.

In addition, the charts in the accompanying article in this issue, "Key Issues in

(continued on page 61)

Peter L. Michaelson is an arbitrator, mediator and attorney with Michaelson ADR Chambers LLC in New York City and Rumson, N.J. He arbitrates and mediates international and domestic disputes primarily involving IP, IT and technology, and secondarily other commercial areas. He is a panelist with the American Arbitration Association (including its commercial, large complex case, technology SEP-FRAND, and other specialty panels) and its international division, the ICDR; WIPO; SIAC; HKIAC; and CPR, which publishes this newsletter. He is a Fellow of the College of Commercial Arbitrators; a member of the National Academy of Distinguished Neutrals; a Chartered Arbitrator and Fellow of the Chartered Institute of Arbitrators (CIArb), and Chair Emeritus and Co-Founder of the New York Branch of CIArb. He has been recognized by the Silicon Valley Arbitration & Mediation Center as a leading technology arbitrator and mediator on its "Tech List." He holds an LL.M. (Trade Regulation) from NYU School of Law, a J.D. from Duquesne University, and an M.S. in Electrical Engineering and a B.S. in Electrical Engineering and Economics, both from Carnegie-Mellon University. Further information is available at www.plmadr.com.

Sandra A. Jeskie is an arbitrator, mediator and attorney in complex disputes involving technology, intellectual property, and complex commercial matters. She also serves the courts as a special master, mediator, and judge pro-tempore in a variety of business disputes. She holds an MBA in finance and a B.A. in computer science. Before practicing law, she worked as a computer scientist. She serves as a neutral for the AAA, ICDR, and CPR; is a Fellow and immediate past Chair of the North American Branch of CIArb; and has also been recognized by the SVAMC as a leading technology arbitrator and mediator on its Tech List. She is past president of the International Technology Law Association and a member of the American Law Institute. She is a partner in Duane Morris; further information and locations are available at http://bit.ly/3sNxQep.

Alternatives DOI: 10.1002/alt

an optimal decision, the parties will certainly spend more than three times the cost of a single arbitrator to produce a final award—of course, the arbitrators often confer with one another throughout the course of the arbitration, during deliberations and editing of the final award. Such costs may be more palatable for high-stakes cases, but they may be difficult to justify in smaller matters.

The AAA also offers a Streamlined Three-Arbitrator Panel option for Large Complex cases, which permits the parties in large cases where a three-member panel is required to instead work with a single arbitrator (usually the chair) during the preliminary procedural and discovery phases. The full panel joins only for the final hearing and award. (Available at https://bit.ly/3e5Imqr.)

Choice of Law: The choice of law can be outcome-determinative in a given dispute.

Drafters need to understand the choices of law that might be available to them and select the one that bests suits their client. Of course, an applicable statute may "select" the law for the matter, but that does not obviate the need to consider the types of common law claims that could be brought in tandem with such statutory claims. To take a "belt and suspenders" approach to this question, the drafter may want to place the choice-of-law provision in the arbitration section of the agreement, in addition to wherever else it may be found in the contract.

Choice of Forum: Under which provider's auspices do you want to proceed? CPR? JAMS? AAA? Purely private? As this discussion indicates, the different providers have somewhat different rules, methods of administration, options for streamlining their procedures and costs, all of which should be taken account in choosing a provider.

Choice of Rules: Do you want the arbitration forum's rules—if you are using a particular provider—to apply, or do you want to employ the more cumbersome and expensive federal or state rules of procedure or evidence?

Some arbitration clauses do not address this issue, and the parties and/or the arbitrator may be left to develop their own. Some adopt the Federal Rules of Evidence in whole or in part.

Venue: The applicable venue will affect the availability of witnesses, costs and travel time. If the choice of law is not addressed elsewhere, the venue clause might affect the choice of law.

Prevailing Party Attorney's Fees: While the prevailing party attorneys fees clauses are the most popular, some arbitration agreements specifically state that the parties are to split attorney's fees and costs regardless of which side prevails. Of course, any claims brought under a statute providing for fee shifting will likely trump whatever the arbitration agreement says.

MEDIATION FIRST?

Mediation usually works, although with a somewhat lower degree of success pre-suit than once litigation and/or arbitration are underway.

Whether the slightly lower earlier success rate is a function of the need for more information or the fact that the parties have yet to feel the pain of litigation may be hard to discern.

But early mediation is still worth trying and, if unsuccessful at first, might well result in settlement at a juncture when the parties have engaged in some discovery and experienced the outflow of costs, fees and personnel time devoted to the case.

* * *

This discussion highlights the need to give due consideration to the myriad of important factors at the outset that will affect your client's arbitration experience and outcome and to draft your arbitration clauses accordingly.

ADR & Technology

(continued from front page)

Arbitrating Disputes Involving Blockchains and Smart Agreements," beginning on page 62, show examples that illustrate exactly how Blockchain Ledgers work, breaking the process down into its constituent parts.

The authors examined these issues last fall, and have expanded from their original article to create this three-part *Alternatives* guidebook. The earlier article can be found at Peter L. Michaelson & Sandra A. Jeskie, "Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts," 74(4) *Dispute Resolution Journal* 89 (American Arbitration Association October 2020) (available at https://bit.ly/3obooh3).

Rebuilding Trust

The deep technical dive: You have heard about Blockchain Ledgers. Here's everything you need to read up on for familiarity now, and the fluency you'll develop later.

Why this, why now? Financial ledgers, 'predicated on human-based accounting systems, have repeatedly been corrupted by fraudulent actions taken by individuals or institutions specifically entrusted to maintain the ledgers.'

The ADR component: Wait for it, coming up later in this three-part series. 'Arbitration,' the authors note, 'is the only viable approach for blockchain-based disputes.'

Absolute Trust on the Blockchain

Trust is essential. All transactions are based on counterparties trusting each other.

Parties will not transact with each other if they cannot establish sufficient trust in each other—either directly or indirectly. Where counterparties have either insufficient or no prior knowledge of each other—and, hence, little or no trust in each other—they will traditionally employ an intermediary each party trusts. Whether that intermediary is an attorney, accountant, bank, underwriter, surety, or other person or institution will depend on the specific transaction's specific nature.

Over time, financial ledgers, which are predicated on human-based accounting systems, have repeatedly been corrupted by fraudulent actions taken by individuals or institutions specifically entrusted to maintain the ledgers, thus substantially undermining their accuracy and reliability, and often causing significant financial injury to others.

Consequently, a profound need exists for accounting systems that can provide undeniable trust. Systems based on Blockchain Ledgers can not only do so but also create, through

(continued on next page)

ADR & Technology

(continued from previous page)
a new decentralized approach to accounting, an increasingly beneficial and societally efficient way to structure transactions.

Blockchain Ledgers establish unassailable trust: trust that cannot be violated, trust that is absolute—and in an efficient, de-centralized manner without any need for intermediation. Moreover, trust is provided at far higher levels than attainable through conventional human-based accounting modalities and at significantly reduced cost.

By relying on mathematical rules and impregnable cryptography, blockchains supplant trust previously reposed in individuals and institutions through traditional written and oral contracting and, in doing so, guarantee the integrity of a Blockchain Ledger.

Smart agreements are built on a Blockchain Ledger and constitute software code that executes on the blockchain (i.e., on any of the computers that also hosts the Blockchain Ledger). This code automatically processes applied external data (obtainable through, e.g., autonomous internet-of-things (IoT) sensors) to yield corresponding entries on the ledger. The result is computer-implemented, automatically executing agreements that do not require any intermediary, whether human or institutional, at all, saving considerable costs and yielding significant efficiencies.

Legal Contracts, Smart Contracts, And Smart Legal Contracts

Smart Contracts: The Smart Contracts Alliance (see http://bit.ly/3a3YSW2), an initiative of the Chamber of Digital Commerce (see https://digitalchamber.org/), defines a Smart Contract as "Computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the ledger."

Smart Contracts can be used in various contexts, but they are particularly useful when integrated into Blockchain Ledgers. As the use

Key Issues in Arbitrating Disputes Involving Blockchains and Smart Agreements

BY PETER L. MICHAELSON & SANDRA A. JESKIE

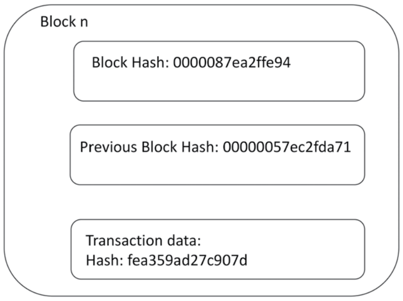
The following companion article to Part 1 of a three-part ADR & Technology series defines the workings of blockchains, Smart Contracts and Smart Legal Contracts. The operations of technologies illustrated below are more fully explained in the accompanying article. In the final Part 3 in June, the authors will examine "the only viable approach for blockchain-based disputes," arbitration.

* * *

Blockchains and Distributed Blockchain Ledgers

A blockchain stores transaction data in blocks. A typical such block (labeled "Block n") is depicted in Figure 1 below.

FIGURE 1 -- TYPICAL BLOCKCHAIN BLOCK


Block n
Block Hash: 0000087ea2ffe94
Previous Block Hash: 00000057ec2fda71
Transaction data:
Hash: fea359ad27c907d

As shown, the block contains data for a given transaction and its hash value. (As more specific details are irrelevant to this explanation, they have been omitted for simplicity.) Transactions can represent almost anything (often referred to as a "digital asset"), such as actual exchanges of money, as occurs on blockchains that underlie cryptocurrencies like Bitcoin. Alternatively, transactions could represent exchanges of other assets represented digitally, such as digital stock certificates, deeds, bills of sale, transfers, and so forth.

For any given transaction, its transaction data contains valid pertinent information specifying the nature of the underlying transaction (such as the specific goods or amount of money involved, the parties involved and their locations) and also a timestamp of when (date and time) that transaction occurred. That data is collectively processed through a cryptographic hash function, which is a predefined mathematical algorithm (e.g., the SHA256 algorithm) that yields a hash value. See, e.g., XORBIN.com, SHA-256 hash calculator (available at http://bit.ly/3rIdO3B).

The moment a block is created, its host computer automatically computes and inserts its block hash value into the block. The hash algorithm has critical properties essential to cryptography and, here, blockchains:

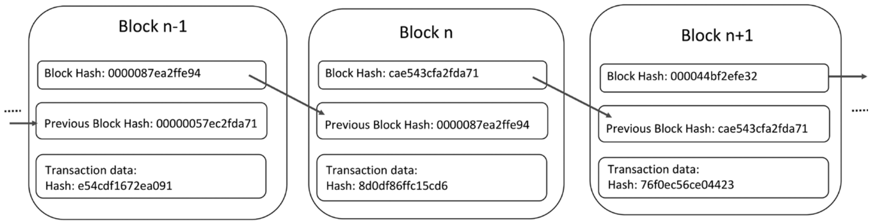
- the algorithm is irreversible, meaning that the underlying input information cannot be determined from its hash value;
- the algorithm is deterministic, meaning that the same input data will always generate the same hash value;
- the hash value can be computed relatively quickly; and
- importantly, a small change in the input data will so extensively change the resulting hash value that the new hash value appears to be uncorrelated (i.e., random) with respect to the immediately preceding hash value.

An Interconnection Chain

The block also contains the hash value for the entire block (i.e., the block hash) and the block hash for an immediately preceding block in the blockchain. The block hash results from applying the hash function to the hashed transaction data and the previous block hash, hence effectively creating a hash of a hash. Manav Gupta, Blockchain for Dummies, IBM Limited Edition, 13 14 (John Wiley & Sons 2017) (available at https://bit.ly/36ZuCLs); see also Anastasia Lastovetska, "Blockchain Architecture Basics: Components, Structure, Benefits & Creation," *MLSDev* (Jan. 31, 2019) (available at http://bit.ly/2Z3wEG4).

The existence of the prior block hash value in each block is what allows the blocks

FIGURE 2 – INTERCONNECTED BLOCKCHAIN BLOCKS


Block n-1
Block Hash: 0000087ea2ffe94
Previous Block Hash: 00000057ec2fda71
Transaction data:
Hash: e54cdf1672ea091
Block n
Block Hash: cae543cfa2fda71
Previous Block Hash: 0000087ea2ffe94
Transaction data:
Hash: 8d0df86ffc15cd6
Block n+1
Block Hash: 000044bf2efe32
Previous Block Hash: cae543cfa2fda71
Transaction data:
Hash: 76f0ec56ce04423
.....
.....

to be linked (i.e., chained) together. This is shown in Figure 2 above, which depicts three successive blocks in the blockchain, Blocks n-1, n, and n+1.

Each block stores information for a corresponding transaction. As the number of transactions grows, so does the number of blocks in the blockchain and hence its size.

All the transaction data stored across all the blocks in a blockchain collectively forms a ledger.

Conventional business networks for recording transactions, simplistically illustrated by that depicted in Figure 3, below, rely on each party, A-D, to write transaction data into its own database (containing respective Ledgers A-D). They communicate transaction and other data through a data network, such as the Internet, with every other party making corresponding updates to their own ledgers.

This arrangement requires all four parties to maintain four separate ledgers. Critically, this arrangement is susceptible to being compromised because, if any one ledger is improperly altered due to fraud, cyberattack, or just a simple human mistake, incorrect transaction data will eventually propagate to and adversely affect transaction data stored in all the other ledgers.

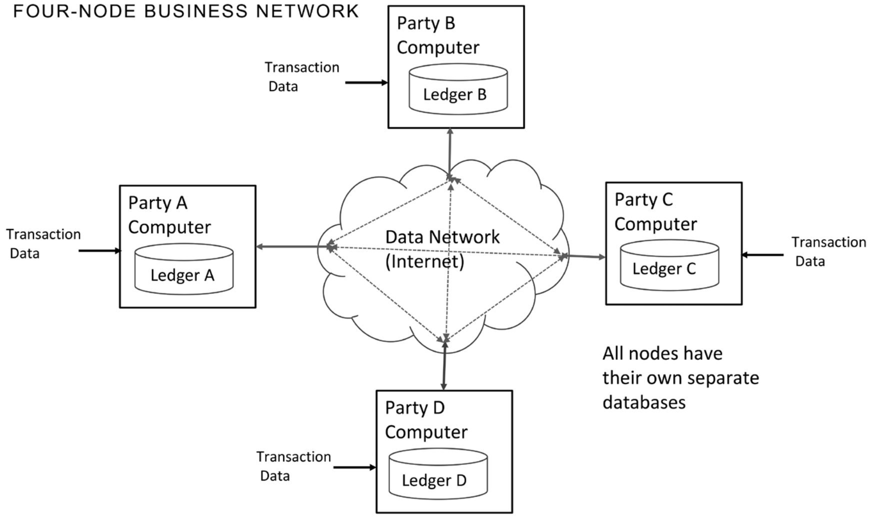
By contrast, Figure 4 on page 64 depicts a blockchain network. For ease of understanding, it is a simple four-node network consistent with that shown in Figure 3, though in actuality, blockchain networks can contain tens, hundreds, or thousands of "nodes" (such as that used in a public blockchain for Bitcoin and other cryptocurrencies).

The blockchain, as shown in Figure 4, is stored in multiple copies across multiple independent computers, each forming a node in the data network, with each node storing a complete local copy of the blockchain, forming a decentralized structure.

As the transaction data stored within the blockchain on each node constitutes a complete copy of the ledger, by virtue of the

(continued on next page)

FIGURE 3 -- CONVENTIONAL FOUR-NODE BUSINESS NETWORK



and development of distributed ledger technology has increased enormously, considerable confusion had arisen regarding the differences between Smart Contracts and conventional—non-computer implemented—legal contracts. Mark M. Higgins, "Blockchain in Energy: Smart Legal Contracts on the Rise," *Nat'l L. Rev.* (July 26, 2019) (available at http://bit.ly/2Yd6xvT).

A fundamental difference between a Smart Contract and a legal contract is the authority that enforces the contract: essentially, a Smart Contract is self-enforcing in that a computer automatically enforces a relationship specified in code (the computer software that, when executed, implements the Smart Contract) solely by the act of executing the code. A judicial system, arbitrator, or some other authority enforces the terms of a legal contract. Ibid.

A Smart Contract contains no independent means of enforcement. It is simply executed when a predefined condition—determined by a sensor or a so-called "oracle," which retrieves and verifies external data for blockchains and Smart Contracts—either occurs or, within a specified period or under some other constraint, does not occur.

Many aspects of legal contracts, such as those which rely on the exercise of human judgment and insight, are presently incapable, and may never be capable, of being represented by condition-based functions used in Smart Contracts.

SMART LEGAL CONTRACTS. A Smart Legal Contract is considerably more sophisticated and complex than a Smart Contract. The former, having both "smart" (computer-executed) and "non-smart" (traditional text-based) clauses, is an amalgam of a Smart Contract and a legal contract.

The Smart Contracts Alliance defines a Smart Legal Contract as "a smart contract that articulates and is capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties." Smart Contracts Alliance, "Smart Contracts: Is the Law Ready?" *Chamber of Digital Commerce* 12 (2018) (available at https://bit.ly/368DKgu).

"For example, a Smart Legal Contract may include a smart payment clause," with code determining the amount due for a particular payment and, based on monitoring a payee's bank account, whether that payment was made by a date certain or not, "while all of the other provisions of the contract (Definitions, Jurisdiction clause, Force Majeure clause)"

(continued on next page)

ADR & Technology

(continued from previous page)
appear "solely in regular natural language text." Accord Project, Overview (available at http://bit.ly/3oe3qhU).

In that regard, the Accord Project, a nonprofit open-source consortium aimed at transforming contract management and contract automation, is developing an open, standardized format for Smart Legal Contracts. See Accord Project at www.accordproject.org.

Similarly, Clyde & Co., a London-based global law firm focusing on insurance and international trade, developed an off-the-shelf connected parametric insurance contract for use by insurers through its Smart Contract group, Clyde Code.

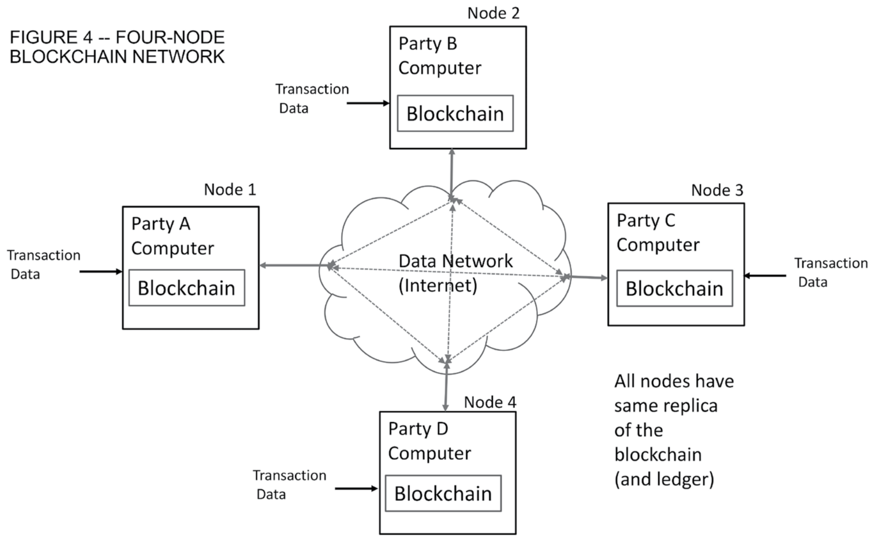
The contract has been built in collaboration with the Smart Legal Contracts Platform Clause and according to the specifications developed by the Accord Project, although it can be deployed on other systems and platforms. "Clyde & Co launches connected parametric insurance contract," *Clyde & Co. Newsletter* (May 15, 2019) (available at https://bit.ly/3iFVpRH).

In the U.S., "Latham & Watkins has teamed up with ConsenSys to develop a Smart Legal Contract that automates convertible note agreements. … [T]his effort, like other efforts to create legally enforceable code, necessitates the engagement of an attorney. Counsel is necessary to determine the parameters of a specific deal and move beyond a standard suite of documents." See Higgins, Blockchain in Energy, above.

In addition to development of standardized Smart Legal Contracts, the Accord Project is working on a software ecosystem and open source tools to digitize new or existing legal contracts, connect them to web services, and deploy them to the cloud or a blockchain platform. The Accord Project views a Smart Legal Contract as both a human- and machine-readable agreement that is digital, consisting of natural language and computable components.

The human-readable aspect of the agreement ensures that signatories, lawyers, contracting parties and others can understand the contract. The machine-readable aspect enables the contract to be interpreted and executed by computers, making the document "smart."

FIGURE 4 -- FOUR-NODE BLOCKCHAIN NETWORK



All nodes have same replica of the blockchain (and ledger)

(continued from previous page)
blockchain being copied across all nodes, the ledger is effectively distributed, in copies, across all the nodes. Michael J. Casey & Paul Vigna, "In blockchain we trust," *MIT Tech. R.* (Apr. 9, 2018) (available at http://bit.ly/3aKI0nK).

As will be described in further detail below, each node writes all transactions, once validated, into its replica of the blockchain, thus the common ledger is always synchronized across all four notes. Each node can be a PC, workstation, server, laptop, mobile device, or any computer-based device that has network connectivity and sufficient processing power to execute software application programs which implement the blockchain and related functionalities.

Furthermore, although each node is illustrated as a physical element located outside the data network, that node can just as easily be located within a cloud environment and implemented either physically or, more likely, in a virtualized form.

Chain Control

No single entity controls the ledger.

Any node can make a change to the ledger by requesting that a new block be added to an end of the blockchain. Once that request is made, the requesting node sends the request and the new block to every other node on the network. Each node that receives the new block verifies that block and determines whether its transaction data is valid. The new block will only be added if pre-defined rules implemented through a consensus protocol are satisfied.

That protocol is a mathematical algorithm which requires at least a majority (and sometimes all, depending on the amount of consensus to which the blockchain is configured) of the nodes which received the new block to agree with the change.

Once consensus is reached and communicated to all the nodes on the network, the nodes will simultaneously update their copies of the ledger by inserting the new block. If any node attempts to add a block to the ledger without achieving consensus, all the other nodes automatically reject the attempt as invalid and the addition is not made.

Once a block is added to the blockchain, the entry is permanent. It cannot be deleted. It cannot be altered. Blocks are entered in an append-only fashion; they are only added to the end of the blockchain: one after another.

Should a node subsequently request a modification to an existing block, such as in the case of a transaction that has been modified (as to amount, such as a refund or discount, change of a party or location), that node requests the addition of a new block which provides the modification. No existing block is modified. As a result, the blockchain records, stores, and reflects each action that involved it, thus forming a complete sequential historical ledger of transactions.

A blockchain network has the following key characteristics:

- Consensus—For a transaction to be valid, at least a majority (and in some instances all) of the parties (participants) on the blockchain must agree on its validity.
- Provenance—By virtue of each transaction affecting a digital asset being entered into the blockchain, all the participants know where that asset originated and how its ownership changed over time.
- Immutability—No participant can tamper with a transaction after it has been entered into the Blockchain Ledger. If a transaction is in error, a new transaction must be entered to reverse the error and both transactions are visible on the blockchain. See Gupta, supra, at 15.

The need to achieve consensus among replicated blockchain nodes coupled with the linkage of successive blocks in each replica through their block hash values renders a blockchain, for all practical purposes, impervious to hacking.

In order for a hacker to successfully change a particular blockchain transaction, that hacker would not only need to change the corresponding block containing that transaction on any one node but also, due to the distributed nature of the ledger, the same block on each and every other node of the chain. And since each block contains its own block hash value and that of its immediately prior block, the hacker would also need to properly change the hash value on each and every block in the blockchain subsequent to the corresponding block and on each replica of the blockchain stored on each and every node.

All of this, practically speaking, is a virtually impossible task. Thus, a Blockchain Ledger provides its users with impregnable trust: they need not trust each other, but each can repose undeniable trust in the distributed ledger itself.

Within this general framework, many differences can arise depending on specific characteristics of the blockchain network. For example, public "permissionless" blockchain networks exist through which any computer can become part of the network—as is the case with cryptocurrencies such as Bitcoin, as well as private "permissioned" ledgers to which access is strictly limited to certain credentialed users having appropriate "permissions" and, for those users, certain purposes.

Permissioned ledgers are typically used by a particular group of organizations (parties) that are transacting together, such as a supply chain, which requires a common, secure, immutable record-keeping system but where those organizations are otherwise independent of each other and may not fully trust each other. Loic Lesavre, et al. "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," NIST (National Institute of Standards and Technology) Cybersecurity White Paper (Draft) (July 9, 2019) (available at https://bit.ly/3e89Ugz); see also Gupta, supra, at 15, and Andrew Tar, "Proof-of-Work, Explained," *CoinTelegraph* (Jan. 17, 2018) (available at http://bit.ly/3baaJnj).

New Block Messaging

Figures 5-7, on pages 66-67, diagrammatically and successively depict, in a simplified fashion, messaging and corresponding operations that occur within a blockchain network whenever a new block is being appended to the blockchain.

To facilitate understanding, these figures use the same four-node blockchain network shown in Figure 4. For further simplification, this example assumes that the consensus algorithm is implemented only within one node and requires complete consensus (i.e., every node must validate a new block before it can be added to end of the blockchain).

As illustrated in Figure 5, depicted on the next page, a new transaction occurred resulting in Data A being sent to Node 1; the operation symbolized by numeral 1. In response, Node 1 constructs, as symbolized by numeral 2, a new block containing this data and Request 3 to add that block to the blockchain. Node 1 then transmits, as symbolized by numeral 4, Request 3 to each of the other nodes.

Next, as shown in Figure 6, on page 66, each node independently determines whether the new block is valid, with this operation symbolized by block 5. Each block then trans-

(continued on next page)

Its goal is for anyone, through use of those tools and the ecosystem, to be able to draft Smart Legal Contracts in a standardized neutral, technology-agnostic format once—and then use and reuse those contracts, as often as desired, across a variety of supported technologies.

The Global Legal Blockchain Consortium is another nonprofit organization that is highly active in this area. The GLBC aims to drive the adoption and standardization of using blockchain technology throughout the legal industry while ensuring data integrity, authenticity, and privacy, and improving the security and interoperability of the global legal technology ecosystem.

The GLBC comprises more than 300 large companies, law firms, software companies, and universities, all seeking to collaboratively develop standards governing the use of open-source blockchain technology in the legal industry (see http://bit.ly/3pdQNVm).

Ricardian Contracts. A Ricardian Contract, which is similar to a Smart Legal Contract and conceived of by financial cryptographer Ian Grigg, is a contract "represented both in plain text and in digital code[,]" digitally signed to provide it with all the elements of a standard legal contract. See "Filling in the Missing Piece of Smart Contracts," (Aug. 15, 2018) (available at http://bit.ly/2Y6VX9A).

Grigg defined the role of the Ricardian contract as "a document that attempts to recognize the intent of the agreement between the parties, while the Smart Contract is the machine that executes that agreement." Id. (citing Ian Grigg, "On the intersection of Ricardian and Smart Contracts" (Feb. 2015).) *Forbes* described the Ricardian Contract as "a smarter and more useful digital contract." Chao Cheng-Shorland, "Moving Beyond Smart Contracts: What Are the Next Generations of Blockchain Use Cases?" *Forbes* (Dec. 5, 2018) (available at http://bit.ly/39e4zSh).

There are obvious efficiency and cost advantages to Smart Legal Contracts and Ricardian contracts. Not surprisingly, various parties in the legal industry have started to capitalize on implementing and using these contracts, though these efforts, as with the Accord Project and the GLBC efforts, are still early in the development phase. See the Accord Project link above.

(continued on next page)

ADR & Technology

(continued from previous page)

Illustrative Smart Contract Examples

As the benefits of using Blockchain Ledgers and smart agreements are increasingly recognized in practice, applications of these technologies, which are likely to exponentially increase with time, are being envisioned across many diverse facets of commerce, industry, and government. The following examples reflect the breadth of these applications and the societal benefits obtainable through these technologies.

Securing the U.S. Electrical Grid. During a frigid day in December 2015, the Ukrainian power grid was hacked. More than 230,000 Ukrainians lost power for an afternoon. The hackers exploited a software vulnerability in a central control system to attack Ukrainian power plants.

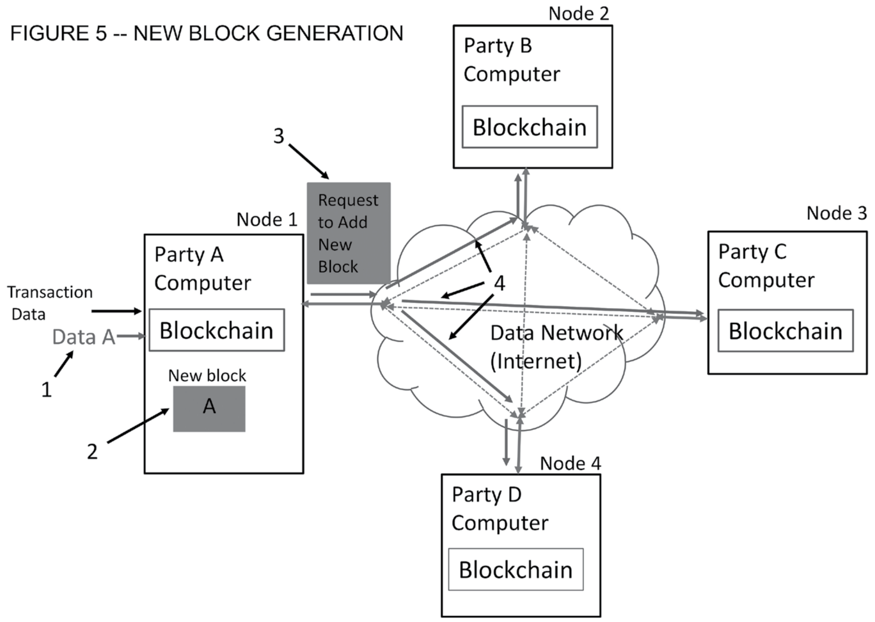
In the U.S., power plants are fed data from the Supervisory Control and Data Acquisition (SCADA) system that U.S. power plants use to decide how much power to generate and where to send it. As SCADA can be a huge central point of attack, the U.S. Department of Energy recently awarded a $400,000 grant to researchers at Pittsburgh's Carnegie Mellon University to substantially harden SCADA from hacking by placing its incoming data on a Blockchain Ledger.

By doing so, an attacker would need to successfully hack not one, but tens or hundreds of computers depending on the number of nodes in the blockchain—which is an extremely difficult task. Daniel Tkacik, "Securing the Energy Grid with Blockchains," 28 *Carnegie Mellon Eng'g Magazine* (Fall 2019).

Providing Safety in the U.S. Food Supply Chain; Locating Sources of Counterfeit Goods. Blockchain Ledgers can be used to secure food supply chains by allowing users to quickly trace the origin and provenance of contaminated foodstuff back to its source.

Within the past few years, a number of multistate instances of e-coli contamination, which caused illness among a small number of consumers and in some rare instances death, has been found in agricultural products,

FIGURE 5 -- NEW BLOCK GENERATION



(continued from previous page)

mits a message, symbolized by message 6 from Node 2, providing its results back, as symbolized by lines 7, to the requesting node, Node 1.

Thereafter, as shown in Figure 7, on the opposite page, Node 1 determines, as represented by block 8, whether consensus exists that the new block is valid, i.e. whether all the blocks agree. If, as here, consensus exists, then Node 1 generates Add New Block command, indicated by number 9, and then transmits that command to each of the other nodes, the latter operation symbolized by lines 10. Each node, in response to the command, then actually appends the new block onto the blockchain replica stored within that node as the last block, that being symbolized by block 11.

As the reader can now readily appreciate that Blockchain Ledgers, due to the inherent replication—distribution—of the entire blockchain across all nodes in the network and the requirement that all nodes perform all the same tasks (with some exceptions regarding which nodes determine consensus), are highly redundant and thus exceedingly inefficient both in terms of storage and processing.

FIGURE 6 -- VALIDITY DETERMINATION

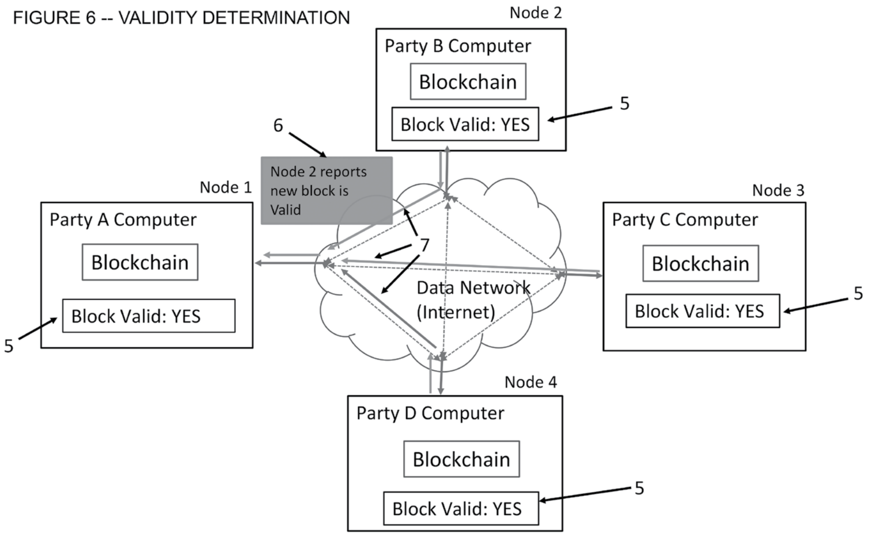
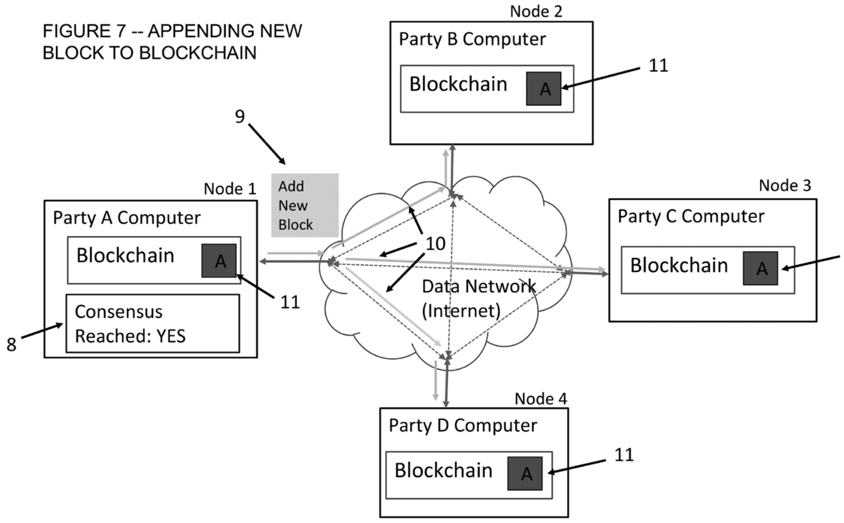


FIGURE 7 -- APPENDING NEW BLOCK TO BLOCKCHAIN



Yet, that redundancy is just what enables, in practice, Distributed Blockchain Ledgers to provide an immutable degree of trust—one that cannot be compromised or violated—to all its participants that any transaction recorded in the ledger has not been illicitly modified, altered, or changed in any way. Demiro Massessi, "Blockchain Consensus and Fault Tolerance in a Nutshell," *Coinmonks* (Jan. 6, 2019) (available at http://bit.ly/3jAMRvB).

Smart Contracts and Smart Legal Contracts

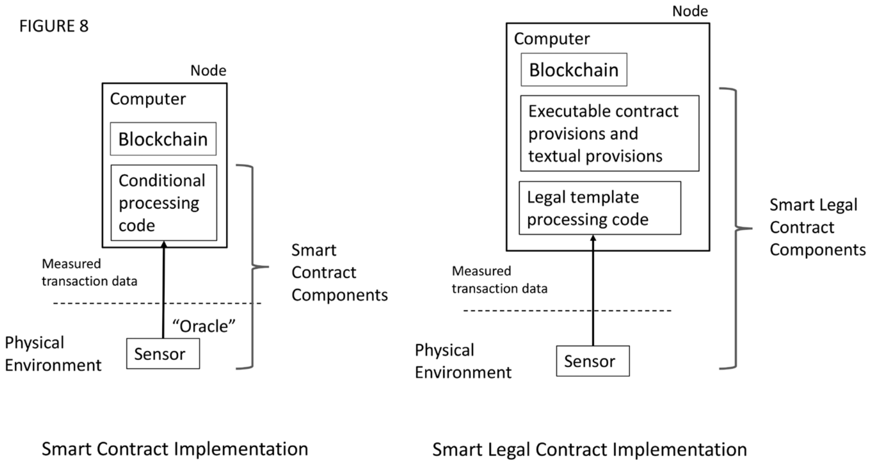
Figure 8, below, depicts at a very high level, the additional components within a Blockchain network node for implementing Smart Contracts and Smart Legal Contracts, as shown, respectively, in the block diagrams on the left and right sides of the figure.

As discussed in the accompanying article, Smart Contracts are self-executing computer code programmed to execute transactions when pre-defined conditions occur (i.e., they automatically enforce a relationship specified in code). As Smart Contracts run on the blockchain, they run exactly as programmed without censorship, fraud or third-party interference.

The contract code and conditions are publicly available on the Blockchain Ledger. "What is Ethereum?" *Blockgeeks* (available at

(continued on next page)

FIGURE 8



Smart Contract Implementation   Smart Legal Contract Implementation

such as romaine lettuce, originating from various growers, agriculturally related facilities or growing regions in California and other producing states.

Historically, the Centers for Disease Control required considerable time and effort to manually trace contaminated produce backward from the affected consumers and ultimately locate the source of contamination to specific producers, facilities, or regions for appropriate remediation. Centers for Disease Control, "Outbreak of E. coli Infections Linked to Romaine Lettuce—Final Update" (Jan. 9, 2019) (available at http://bit.ly/3pzbV8o).

To appreciably shorten this time, each and every different point along a chain of custody—starting with an individual grower, through all intermediate points where possession changes, to ultimately an endpoint in the chain which either uses the produce or sells it to a consumer—can be permanently recorded, via Smart Contracts, on a Blockchain Ledger.

The ledger provides an irrefutable shared record of ownership, custodial transfers, location, and movement along every facet of the food supply chain, thus increasing efficiency, transparency, and trust, with information being simultaneously and securely available to each entity along the chain as well as regulators. See IBM, "Transform supply chain transparency with IBM Blockchain" (available at https://ibm.co/3plYVmN) [hereinafter "IBM Supply Chain White Paper"]; IBM, "Who will win the race to blockchain supply chain supremacy?" (available at https://bit.ly/2KXfA12; see generally https://www.ibm.com/blockchain/industries/supply-chain); see also Sloane Brakeville, et al., "Blockchain basics: Glossary and use cases," *IBM Developer* (Aug. 21, 2017) (available at http://ibm.co/3pm04e5).

By simply inspecting the ledger, a regulator can pinpoint, within seconds rather than weeks, a particular grower, facility, or region for investigation, thus significantly reducing the spread of contamination and the number of instances of consumer illness, and significantly improving public safety.

Similarly, Blockchain Ledgers can be used to find the source of counterfeit or faulty goods by tracing the origin and provenance

(continued on next page)

ADR & Technology

(continued from previous page)

of previously shipped goods, including, e.g., investigating industry certifications, tracking restricted or dangerous components, and discovering storage anomalies. See IBM Supply Chain White Paper, above; see also Chamber of Digital Commerce, "National Action Plan for Blockchain—The Need for a Comprehensive, Coordinated, Pro-Growth Approach to Developing Blockchain Technology in the United States," (February 2019) (available at https://bit.ly/3sZgzyF).

For example, in June 2019, the FDA chose Merck & Co, IBM, KPMG, and Walmart to form a pilot project aimed at evaluating the use of blockchains to protect pharmaceutical product integrity, by identifying and tracing certain prescription drugs as they were distributed within the United States.

The project was authorized under the U.S. Drug Supply Chain Security Act, which increased the FDA's ability to help protect consumers from exposure to counterfeit, stolen, contaminated or otherwise harmful drugs. Edward Pearcey, "U.S. border agency tests IP blockchain solution," *World Intell. Prop. Rev.* (Feb. 3, 2020) (available at http://bit.ly/2MpOzUm).

Migration of Financial Markets to Blockchain Distributed Ledgers. As reported in the financial media, Goldman Sachs is investing heavily, including significant expansion of its internal development staff, in developing and implementing a blockchain-based ecosystem in which financial assets would reside on Blockchain Ledgers.

The overall goal is that activities "that today require squadrons of bankers and lawyers like initial public offerings and debt issuances could be largely automated" and in five to 10 years' time evolve into a "financial system where all assets and liabilities are native to a blockchain, with all transactions natively happening on chain … [a]nd that can include debt issuances, securitization, loan origination." "Goldman Names New Head of Digital Assets in Bet that Blockchain is the Future of Financial Markets," *CNBC.com* (Aug. 6, 2020) (available at https://cnb.cx/3iQU0HT).

To do so, an early project underway at Goldman is to digitize and automate the "repo" (repurchase agreement) market through which banks and hedge funds rely on short-term funding for daily operations—a market where more than $1 trillion flows through daily. The intent is to use distributed ledger technology to standardize many legacy processes that are cost inefficient and, by doing so, yield a much more efficient real-time settlement process.

Further out in time, Goldman intends to apply distributed ledger technology in

(continued from previous page)

http://bit.ly/2ZfHsRD). That code, basically implementing conditional logic, accepts measurements, in the form of measured real-world transaction data, whether from a remote sensor or from some other source which, with appropriate data retrieval and verification functionality, can also, as shown, be an oracle, (which is discussed in the cover article).

The sensor measures some aspect of the real world. The code implements specific and alternate contract terms and is triggered depending on the value of the incoming data, whether measured by the sensor or directly applied through a remote source.

The data may simply reflect, in a binary "yes/no" manner, whether a given event has occurred or not. The logic is typically implemented using "if-then-else" type conditional processing: "If the data value equals X, then perform Step A, or else perform Step B."

A Smart Contract is not synonymous with a legally binding contract. Smart Contracts can be and are being used in applications that have very little, if anything, to do with acting as a legally binding contract (e.g., supply-chain management, self-sovereign identity, and provenance tracking).

That stated, Smart Contracts can constitute elements of a legally binding contract under common law. "Smart Contracts: Is the Law Ready?" Smart Contracts Alliance 12 (Chamber of Digital Commerce 2018) (available at https://bit.ly/368DKgu).

For example, under a Smart Contract, payment for goods is due a seller when certain goods are delivered to a buyer. At the buyer's facility, an employee at a loading dock may use a handheld barcode reader to scan barcoded information printed on shipment documents for all incoming shipments to confirm receipt. The sensor in this instance is the barcode reader. Once the scanned data is received by the computer, that triggers the Smart Contract logic which, in turn, instructs payment to be made to the Seller and a new block to be added to a Blockchain Ledger reflecting that event.

If the goods have not arrived by a predefined date, then the logic may invoke an alternate action, such as notifying the seller of non-delivery and instructing the Blockchain Ledger to add a new block reflecting that event. The Smart Contract here is simply the sensing of the occurrence or non-occurrence of a delivery and executing a corresponding operation.

A Smart Legal Contract, being far more sophisticated than a Smart Contract, is implemented with both computer-executed contractual clauses and traditional text-based clauses. A Smart Legal Contract, pursuant to a framework similar to that promulgated by the Accord Project (see discussion in the accompanying article), relies on using a legal template and accompanying executable code.

When the executable code is processed, real-time sensed measurement data is inserted into the coded template and, based on the value of the data and the instructions set forth in the template code, specific contractual action as specified in the template is then automatically invoked. An accompanying new block, reflecting that action, is established and added to the blockchain. See the Accord Project at www.accordproject.org.

For example, a Smart Legal Contract may contain a smart payment clause using executable code to determine a specific amount due a domestic supplier in an international sales transaction, then invoke its payment and finally, upon the supplier's receipt of that amount, write a new block reflecting that transaction into a Distributed Blockchain Ledger.

automating the credit and mortgage markets. Goldman recognizes that building industry-wide consensus through, ideally, consortiums with other banks, institutional investors, and regulators, is crucial to the success of any of these efforts, as is gaining a critical mass of users across the financial world.

* * *

In Part 2 next month, Peter Michaelson and Sandra Jeskie continue with their description of Blockchain Ledger agreements by completing their introduction with an examination of smart agreements, and then provide examples of the types of real-world disputes that might arise involving blockchain technology.

Blockchain's Beginnings

For initial context, an early work dealing with a cryptographically secured chain of blocks to implement a system of secure document timestamps was described in Stuart Haber, et al., "How to Time-Stamp a Digital Document," 3(2) *J. of Cryptology*, 99 (January 1991). In 1992, the system was expanded to allow several document certificates to be collected into one block. David Bayer, et al., "Improving the Efficiency and Reliability of Digital Time-Stamping," 2 *Sequences* 329 (March 1992). What appears to be the first conceptualization of blockchain was made by a person or persons known as Satoshi Nakamoto in 2008—though the exact identity of Nakamoto remains a mystery in the cryptographic field—when a paper was published under that name describing the implementation behind the cryptocurrency Bitcoin. Nakamoto incorporated hash methodology to timestamp blocks without requiring them to be signed by a trusted party and to reduce speed with which blocks are added to the chain. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) (available at https://bitcoin.org/bitcoin.pdf); see also, Arvind Narayanan et al., "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" (Princeton Univ. Press 2016).

ADR Brief

COMMERCIAL ARBITRATION GETS A BOOST FROM THE ABA'S HOUSE OF DELEGATES

The American Bar Association has passed a resolution, supported by a report, that backs the use of commercial arbitration. The statement endorses the use and vitality of the process, and means that the support for the ADR process is now ABA policy.

The resolution and its background materials received a sign-off on Feb. 22 by the ABA House of Delegates—the association's governing, policy-making body which is designed to be representative of the U.S. legal profession—at the group's 2021 Virtual Midyear Meeting.

The resolution comes from a joint study committee on business-to-business arbitration set up by the ABA's Section of Dispute Resolution, with representatives from the ABA Litigation and Business Law sections as well as the Section on Infrastructure and Regulated Industries. The Sections of Dispute Resolution, Litigation, and Infrastructure and Regulated Industries formally presented the resolution and report to the House of Delegates. The resolution states,

> RESOLVED, that the American Bar Association supports the use of arbitration of business-to-business disputes, both domestically and internationally, as an efficient and economical method of dispute resolution.

The accompanying report keeps the reasons for the backing general, and expressly avoids hot-button issues of mandatory consumer and employment processes, which are the subject of recent Congressional investigations and proposed legislation. See, e.g., Justice Restored: Ending Forced Arbitration and Protecting Fundamental Rights, House Subcommittee on Antitrust, Commercial, and Administrative Law (Feb. 11) (available at https://bit.ly/2Z6C4QD), and Mark Kantor, "House Passes 'PRO' Act, Which Includes Arbitration Restrictions," *CPR Speaks* (March 10) (available at https://bit.ly/38u5w87) (also addressing the proposed FAIR Act).

> The ABA resolution supporting commercial arbitration 'is a needed policy statement.'

In the report's general information checklist, the drafters note, "There is no known pending legislation that concerns or affects the use of arbitration agreements in the commercial setting. The FAIR Act, which would prohibit the arbitration of all employment and consumer claims, passed in the House of Representatives in 2019; it has not been taken up by the Senate."

The introduction to the resolution's accompanying report says, simply, "The Resolution is a needed policy statement. It does not propose or call for any legislative or regulatory action, nor does it address arbitration in settings other than business-to-business disputes."

The 11-page report—six pages of discussion teamed with five pages of general information and background—backs its support for arbitration by noting in its first section that business-to-business arbitration "serves important commercial and public interests."

The paper states that the general public benefits as well as business from arbitration use because it "reduces the volume of cases that would otherwise absorb a substantial portion of judicial time and resources … freeing those resources for other claims where a judicial forum may be required or preferred. …"

The pandemic adds to the "alignment of public and private benefit" from commercial arbitration, the report notes.

(continued on next page)