

ing or harming a participant. The medical profession tenet of “doing no harm” is always applicable to the mediator.

\* \* \*

There are many reactions and strategies

mediators employ on an ad hoc basis when confronted by parties and advocates guided by religious or spiritual principles. This is a thorny situation where there are no right answers. There can be wrong ones which will create an impasse, intensify the conflict, or

harm the disputants.

My experience is for mediators to tread lightly and respond to the cues, build alliances, and focus on the disputants’ beliefs and core values—which are inconsistent with continued conflict. ■

## ADR & Technology/Part 2 of 3

# Where the Disputes Lie: When Blockchain Technology Will Need Help Sorting Out Its Contracts

BY PETER L. MICHAELSON & SANDRA A. JESKIE

*Last month, the authors introduced the types of agreements that use blockchain technology at “A Guidebook to Arbitrating Disputes Involving Blockchains and Smart Agreements,” 39 Alternatives 57 (April 2021) (available at <https://bit.ly/3uLC32i>). In this month’s Part 2, the authors continue their discussion of the types of agreements using Blockchain Ledger technology by completing their introduction with an examination of smart agreements. Then, they move on to the disputes that can arise, and the issues of jurisdiction, enforceability, and antitrust, ahead of next month’s conclusion and its focus on the resolution mechanism, arbitration.*

\* \* \*

**B**ecause smart agreements are based on code, they are, by their very nature, inflexible and incomplete. They are neither designed for general use, nor are they suited for it.

If smart agreements are, as some in the field ascribe them to be, “immutable, unstoppable, and irrefutable computer code,” that

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. Jeskie is a partner at Duane Morris, working in California and Philadelphia offices, and is an arbitrator, mediator and attorney in complex disputes involving technology, intellectual property, and complex commercial matters. For their full bios, see the box accompanying Part 1 of this series at the link in the introductory paragraph above.



code must declare what will happen as a result of every possible contingency that might occur during the life of the contract.

Inflexibility results because the code is completely deterministic, embodying predefined rules typically reduced to codified “if-then-else” conditional programming statements. Any conduct by the parties that does not fall within the rules is simply ignored.

Consequently, the use of smart agreements is usually limited to situations where parties, at the outset of their transactions, can anticipate every contingency that might arise affecting their contractual performance. The underlying transactions tend to be relatively simple, as their performance is predicated only on whether particular conditions are satisfied or not, which, in turn, can be easily translatable into rule(s) of performance that can be readily codified.

But, for many legal contracts that are less simplistic, contractual performance is not so easily assessed because it is not simply a question of whether predefined conditions have been objectively satisfied or not. Rather, for those contracts assessing performance calls for a determination that requires some degree of human judgment.

Specifically, the parties or an adjudicator may need to subjectively assess the effect on the parties’ contractual rights and obligations resulting from an intrinsic or extrinsic contingency that occurred and/or prior conduct by one or more of the parties.

In those situations, significant portions of the parties’ agreement cannot be coded, as they

are encompassed by non-deterministic concepts and general clauses, such as good faith, reasonableness, intent, excused performance, and many others, which collectively form the foundation of contract law. Pietro Ortolani, “The impact of blockchain technologies and smart contracts: arbitration and court litigation at the crossroads,” 24(2) *Uniform L. Rev.* 438 (June 2019) (available at <http://bit.ly/3t04zwX>). Consequently, these legal agreements, by their very nature, are inappropriate for codification and implementation as smart agreements.

Further, for many such less-simplistic legal contracts, deterministic completeness is unattainable. In practice, it is often extremely difficult, if not impossible, for contract drafters, dealing with anything other than relatively simple, straightforward transactions, to anticipate every such contingency that might possibly arise, no matter how small its probability of occurrence.

Consequently, many commercial legal contracts are incomplete. By leaving certain contingencies and hence their outcomes undefined, the drafters introduce, whether intentionally or not, ambiguities and gaps into commercial legal contracts for later resolution.

Oftentimes, it is simply too costly to proceed otherwise. Parties may also recognize and intentionally retain ambiguities and gaps in their legal contracts so that, if a corresponding situation arises later, the incompleteness can be exploited in a way that results in a better contract for them, ex-ante.

Renegotiation is a common way that ambiguities are resolved and contractual gaps filled.

*(continued on next page)*

## ADR & Technology

(continued from previous page)

Larry D. Wall, “‘Smart Contracts’ in a Complex World,” Notes from the Vault, Federal Reserve Bank of Atlanta (July 2016) (available at <http://bit.ly/2M1IheY>). Parties need some degree of flexibility in resolving contractual incompleteness that avoids locking themselves into rigid commitments and outcomes which they did not anticipate and do not want. Houman B. Shadab, “What Smart Contracts Need to Learn,” *Lawbitrage* (Sept. 4, 2014) (available at <http://bit.ly/2KWfuXq>).

Consequently, for other than relatively simple, completely deterministic transactions, it is quite possible that the code in smart agreements will fail to reflect some contingencies. Code is not subject to renegotiation. Smart agreements, once they are embodied into code, are fixed. If parties decide to modify their smart agreement, they then need to change its code accordingly.

Some smart agreement adherents vociferously advocate that “The Code is Law”—i.e., that the code itself is the ultimate arbiter of a deal it represents, a standalone, self-enforcing agreement not subject to interpretation by outside entities or jurisdictions. David Siegel, “Understanding the DAO Attack,” *CoinDesk* (June 25, 2016) (available at <http://bit.ly/2LZUdwB>).

Yet, what happens in a smart agreement if an unanticipated (non-coded) contingency occurs? Does the contract just assume a default or error state, pending some human intervention to clear that state—which lies directly contrary to the autonomous, self-executing nature of a smart agreement? Should the contract simply report that event to the blockchain and then reset itself once that event ceases and then return to normal execution?

At present, there are no definitive answers. When such a situation arises—as with, e.g., the DAO exploit (discussed below)—an errant result can flow from execution of a smart agreement which, in turn, could lead to a dispute between the contracting parties with potentially significant attendant legal liability.

### Likely Disputes

Bill Gates famously said, “Software is a great combination between artistry and engineer-

ing.” But like artistry and engineering, perfection is illusive.

Smart contracts are nothing more than software code written by humans, and are therefore imperfect by their very nature. Any number of issues could arise in the design, development, or execution of software code, and smart agreements are not immune to such problems. A few of the more common technical issues associated with smart agreements are briefly discussed below.

*Technical Issues: Design Flaws*—Software design is the process by which a programmer translates user requirements into software code. A flawed software design will likely lead to unexpected results and, sometimes, catastrophic consequences.

Sadly, a design flaw in the software for a new flight-control system on the Boeing 737 MAX plane was responsible for several plane crashes killing 346 people. David Slotnick, “The DOJ is reportedly probing whether Boeing’s chief pilot misled regulators over the 737 Max,” *Business Insider* (Feb. 21, 2010) (available at <http://bit.ly/3opXFgS>).

Another design flaw that caught widespread attention occurred when a smartphone application developed for the Iowa Democratic Party was rushed into use with technical and design flaws that caused a significant delay in reporting Iowa 2020 presidential caucus results. Ben Popken & Maura Barrett, “Iowa caucus app was rushed and flawed from the beginning, experts say,” *NBC News* (Feb. 5, 2020) (available at <http://nbcnews.to/36kIdfQ>).

While it is unlikely that most design flaws in a smart agreement could have such tragic or newsworthy consequences, such a flaw could result in significant financial losses and complex business disputes, among other things.

Flaws could occur anywhere in the design, such as in the underlying algorithms or the communications protocol. No matter what the cause, design flaws can lead to significant issues and therefore liability on any number of theories, such as negligence, product liability, or breach of contract resulting from injury to a participant or third party proximately caused by a defect in a smart agreement.

To mitigate risks, appropriate steps should be taken both during the development and the coding of smart agreements to prevent, detect, and remediate design flaws and coding errors. Further mitigation can be achieved by the

procurement of adequate insurance coverage against any potential residual exposure.

Potential liability can also arise when smart agreements are operated beyond their design limits, i.e., under conditions that were not contemplated, particularly where they invoke unintended, possibly even adverse, results. While the underlying code itself may not be flawed, the design, in not accommodating and properly handling extreme conditions, may contain flaws.

*Technical Issues: Coding Errors/Bugs*—As blockchain technology begins to permeate every industry, the importance of smart agreements will increase significantly with the underlying software code supporting those smart agreements eventually controlling billions of dollars of digital assets. Kai Sedgwick, “The Billion-Dollar Quest to Eliminate Smart Contract Bugs,” *Bitcoin.com* (July 12, 2018) (available at <http://bit.ly/3iT5aft>).

While software development has existed for decades, development platforms for Smart Contract code were only developed in 2015, with software ecosystems and standardization efforts being developed through, for example, the Accord Project and the GLBC, respectively, having started just within the past few years.

Because these platforms have only been in existence for a short time, there are no handbooks for software developers to use in coding smart agreements, and particularly Smart Contracts. Yos Riady, Best Practices for Smart Contract Development (Nov. 10, 2019) (available at <http://bit.ly/39nYhzp>). The development of smart agreements and associated development platforms and related software tools are still in their embryonic stages.

While those platforms are likely to mature quickly, no matter what the technology, coding errors can and will happen, and the risk associated with such errors increases as the code complexity increases. Like design flaws, coding errors may lead to unexpected consequences and attendant legal liability.

It has been estimated that the amount of cryptocurrency lost to coding errors is quickly approaching \$1 billion. The most well-known episode involves “The DAO” exploit, discussed below.

*The DAO Incident*—Distributed Autonomous Organizations, or DAOs, are early-stage investment funds that lack a manager. A DAO is run by programming code and constitutes a collection of Smart Contracts operating inde-

pendently of any human intervention, as long as funding covers a DAO's survival costs and provides a useful service to its participant base.

[Ethereum is a global, open source, blockchain-based distributed computing platform and operating system (so-called Ethereum Virtual Machine), featuring Smart Contract functionality, for building decentralized applications. While blockchains can process code, most are severely limited in what they can do. Rather than providing a limited set of operations, the Ethereum Virtual Machine allows developers to create whatever applications they want on the Ethereum network, including, e.g., DAOs. See Ameer Rosic, "What is Ethereum? [The Most Updated Step-by-Step-Guide!]" *Blockgeeks* (available at <https://bit.ly/2ZfHsRD>).]

An initial funding period exists during which a DAO's participants add funds, typically through what is referred to as a "crowd sale," to provide the DAO with operating resources. Investors vote on which projects to fund, with the code implementing the Smart Contracts doing the rest.

On April 30, 2016, a particular DAO called "The DAO" was launched with a 28-day funding window. It raised more than \$150 million from more than 11,000 participants.

In June 2016, one of its participants exploited a known vulnerability in The DAO's code and drained about \$53 million from The DAO into an account the person controlled. The specific error in the code was known to The DAO's creators, but it was not remedied in time to prevent the error from being exploited.

The appropriate response to the attack created an interesting dilemma. If "the code is the law," as some Smart Contract proponents asserted, what happened was perfectly legal because the code executed as it was intended.

As such, some participants in The DAO took the position that the transfer did not violate the Smart Contract itself and, instead exploited a code vulnerability. Other participants felt their funds had been stolen and allowing the attack to stand would discourage participants from making future investments.

Ultimately, the Ethereum organization, which implemented the code, voted to restore the funds to the original investors. Since an error existed in the code, The DAO sought to renegotiate the terms—notwithstanding the

fact that renegotiation is arguably contrary to the fundamental notion of Smart Contracts.

*Technical Issues: Security Vulnerabilities*—Smart agreements are often designed to manipulate and hold funds denominated in Ether, a payment mechanism for Smart Contracts' transactions, making them tempting targets because a successful attack would result in stealing funds from the contract. Daniel Perez & Benjamin Livshits, "Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited" arXiv:1902.06710 [cs.CR] (October 2020) (available at <https://bit.ly/3rB2Z30>). While exploited vulnerabilities have captured headlines and imaginations, academic research reported that, out of 21,270 vulnerable Smart Contracts, at most only 504 have been subjected to exploits, likely due to the fact that a majority of Ether is held by only a small number of contracts. *Ibid.*

While the number of exploited vulnerabilities may be relatively low currently, as the technology becomes more widely accepted and more money is exchanged through smart agreements, there can be little doubt that vulnerabilities will be substantially exploited. Such vulnerabilities will therefore expose parties directly or indirectly responsible for the problem to liability, including developers, contract administrators, or the entity that hosted the contract.

*Technical Issues: Privacy*—Information stored on a Blockchain Ledger may identify aspects of a user's identity and include financial, medical, or consumer personal information. Care must therefore be taken to ensure compliance with applicable privacy laws.

Over the past few years, there have been a proliferation of new privacy laws, each one placing more emphasis on the right of consumers to protect their own personal information. The General Data Protection Regulation, or GDPR, addressing data protection in the European Union and the European Economic Area, and the California Consumer Privacy Act, or CCPA, addressing personal information of California consumers, are recent additions to ever-expanding privacy regulations.

Both GDPR and CCPA expansively define "personal information" to include information that directly or indirectly identifies a person and therefore could impose significant obligations, as well as risk, on Blockchain Ledger administrators to ensure that personal information is properly secured.

GDPR and CCPA also present interest-

ing questions about how an individual whose personal information appears on a Blockchain Ledger can exercise his or her right to have that personal information deleted (also known as the "right to be forgotten" under GDPR).

By 2023, Gartner predicts that 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% in 2020. Susan Moore, Gartner Predicts for the Future of Privacy 2020, Smarter with Gartner (Jan. 20, 2020) (available at <http://gtnr.it/3cTPaZr>). As such, privacy and security of personal information on a Blockchain Ledger and/or associated with Smart Contracts could pose a significant liability.

Consideration should also be given to whether the Smart Contract is stored on a public, private or hybrid blockchain. Public blockchains are visible to all users, while private blockchains are permission-based and visible only to persons or entities with appropriate permissions.

Another option is a hybrid blockchain that includes both public and private aspects. Decisions regarding the storage of a Smart Contract on a public, private, or hybrid blockchain may depend on the nature of the information stored.

## Jurisdiction, Enforceability, Antitrust

*Jurisdiction*—Blockchains present a unique jurisdictional challenge that may bar lawsuits that directly involve them. To date, while a small number of suits has been filed that implicate blockchains, these related mainly to claims of securities fraud and misrepresentation in the public sale of initial coin offerings, or ICOs, where the ICOs were to be implemented on blockchains. See, e.g., *In re Tezos Sec. Litig.*, No. 17-CV-06779-RS, 2018 WL 2387845 (N.D. Cal. May 25, 2018) and related litigations *Baker v. Dynamic Ledger Sols. Inc.*, No. 17-CV-06850-RS, 2018 WL 656012 (N.D. Cal. Feb. 1, 2018); *MacDonald v. Dynamic Ledger Sols. Inc.*, No. 17-CV-07095-RS, 2017 WL 6513439 (N.D. Cal. Dec. 20, 2017); *Okusko v. Dynamic Ledger Solutions Inc.*, Case No. 17-cv-6829; *GGCC LLC v. Dynamic Ledger Sols. Inc.*, No. 17-CV-06779-RS, 2018 WL 1388488 (N.D. Cal. Mar. 16, 2018); see also, e.g., *Rensel v. Centra Tech Inc.*, 17-cv-24500-JLK (S.D. Fla.); *Hodges v. Monkey Capital LLC*, 17-81370 (S.D. Fla.); *Balestra v. ATBCOIN LLC*, 17-10001

(continued on next page)

## ADR & Technology

(continued from previous page)

(S.D.N.Y.); *Stormsmedia LLC v. Giva Watt Inc.*, 17-00438 (E.D.Wash.); *Davy v. Paragon Coin Inc.*, 18 00671 (N.D. Cal.). Also, for SEC concerns regarding ICOs, see <https://www.sec.gov/ICO>.

The authors are not presently aware of any lawsuits that yet exist directly concerning transactions that occurred on blockchains themselves or issues surrounding execution of the blockchains themselves, though it is fair to predict that such lawsuits will occur eventually.

For an adjudicator, whether a court or an arbitral tribunal, to consider and rule on a dispute, it is canonical law that the adjudicator must be seized with jurisdiction: over the parties for *in personam* jurisdiction or over an object for *in rem* jurisdiction. In either instance, the location of the person or object determines whether jurisdiction arises.

A blockchain is a decentralized structure of information: stored bits of information (code and data) effectively disbursed over many different “locations,” as is an entire blockchain infrastructure implemented as “blockchain-as-a-service.”

One cannot point to a blockchain or reach out and touch it as it is not physical; it is a data structure, nothing more. It has no physical presence. It is not a physical object. It is an abstraction: a collection of either the presence or absence of electronic charges in separate memory locations respectively representing binary “ones” and “zeroes” typically accessed by virtualized servers that execute blockchain code and process its data, all residing, often piecemeal, somewhere in a cloud or even across multiple interconnected clouds. Even a virtualized server is nothing more than an abstraction: computer code that, when executed, collectively emulates a physical server.

[See the article accompanying Part 1 last month by the authors, Key Issues in Arbitrating Disputes Involving Blockchains and Smart Agreements, 39 *Alternatives* 62 (April 2021) (available at <https://bit.ly/3uLC32i>). But as the concept of hardware virtualization is well beyond the scope of this paper, it will not be addressed in any detail. For further insight, the reader is referred to virtualization software providers, such as VMware Inc. (available at [www.vmware.com](http://www.vmware.com)) and Microsoft Corp. (available at <https://bit.ly/3mugzEj>).]

That code, too, can be stored and executed virtually anywhere on a cloud, or even, like any

code, transferred from storage in one location to another so that, rather than executing on one physical host computer, it will execute on another, perhaps half a world away. Hence, the traditional notion of a “location,” as a physical situs of a person or an object and upon which adjudicators assess jurisdiction, has no meaning for a blockchain.

Consequently, traditional physical measures of national court jurisdiction would fail. Absent an agreement by the parties conferring jurisdiction on a particular court, no national court could exert requisite physical jurisdiction over a blockchain.

*Legal Enforceability: ESIGN, UETA, and Other State Statutes*—Both the Electronic Signature in Global and National Commerce Act, or ESIGN (see 15 U.S.C. § 7001, et seq. (2000)), and the Uniform Electronic Transactions Act were enacted to help ensure the validity of electronic contracts and the defensibility of electronic signatures. (The UETA was approved and recommended by the Uniform Law Conference in 1999 for state enactment.)

To the extent contract formation occurs through a Smart Legal Contract rather than through a separate preliminary interaction between the parties, it may be necessary to ensure the contract fully complies with these acts.

By contrast, Smart Contracts—which, as discussed, involve nothing more than providing incoming data (including measured values) to coded logic to correspondingly condition the execution of a blockchain entry—do not implicate electronic formation of contractual obligations. Those obligations are previously agreed to by the parties involved before being defined in code. Accordingly, Smart Contracts are not likely to implicate these and similar acts.

The UETA, currently enacted in 47 states, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia, provides the states with a framework for determining legality of an electronic signature in both commercial and government transactions. Washington State, New York, and Illinois have not yet enacted the UETA; however, similar legislation governing electronic transactions has been enacted in each of these three states. The UETA is limited to electronic contracts related to business, commercial (including consumer), and governmental matters.

Effective since Oct. 1, 2000, ESIGN accords, as does UETA, electronic signatures and records

the same legal status as manually inked signatures and paper-based records. ESIGN only affects the medium through which a contract is made and does not change the underlying substance of any law within its scope.

It treats commercial and consumer transactions differently: for commercial transactions, intent to enter into an electronic contract is implied from the surrounding facts and circumstances or by an express statement of intent; for consumer transactions, it requires the consumer to receive specific disclosures before agreeing to proceed electronically.

ESIGN affects interstate commerce. See RightSignature, UETA—Uniform Electronic Transactions Act (available at <http://bit.ly/3bcmlFp>). Though ESIGN will preempt any inconsistent state law, it expressly precludes UETA preemption in any state or territory that enacted the latter. Margo H. K. Tank, et al., “A short primer on applicable U.S. eSignature laws,” DLA Piper (May 2, 2018) (available at <http://bit.ly/2Nfznt5>).

UETA, in contrast to ESIGN, has no consumer notice provision, though certain enacting states have enacted their own variations to UETA to include, among other aspects, such notice. And unlike ESIGN, UETA addresses when an electronic record has been sent and received.

The provisions of both UETA and ESIGN are liberal to encourage adoption and use of electronic contracting. During 2019, some states enacted legislation specifically enabling the use of Blockchain Ledgers in smart agreements or for storing certain records (Illinois—May 29, 2019; Maryland—April 30, 2019; Nevada—June 7, 2019, and Texas—June 10, 2019) or have established a task force to implement and expand the blockchain industry in that state (Florida—May 23, 2019). Other states have amended their UETA Acts to recognize blockchain technology (North Dakota and Oklahoma—both late April 2019, and Nevada—June 7, 2019). Margo H. K. Tank, et al., “Blockchain and Digital Assets News and Trends,” DLA Piper (May 24, 2019, and June 24, 2019) (available at, respectively, <http://bit.ly/3q4ty0o>, and <http://bit.ly/3jALk9a>).

*Antitrust Considerations*—Blockchains have the potential to displace traditional networks or at least lower their costs—the costs related to the value created for users when more users join a network. In traditional net-



working, a company that owns a network infrastructure can raise the cost of doing business on the network as the network becomes larger and more ubiquitous.

As discussed above, a blockchain provides an ability to operate a network or marketplace without a centralized intermediary, therefore, resulting in lowered network costs which could provide profound pro-competitive implications.

Opposite situations may also occur as a result of restricted networks arising from the use of permissioned blockchains. There, access to the blockchain's underlying distributed ledger and its beneficial effects could be restricted (through use of, e.g., specialized access credentials or tokens)


to certain market participants with anti-competitive concerns and concomitant antitrust liability potentially stemming out of whatever criteria formed the basis of the restriction.

A key question for antitrust inquiries would be whether use of a blockchain in a commercial setting prevents or limits the concentration of market power. The dream of blockchain developers is that blockchains will enable all the benefits of network effects, while minimizing or eliminating market power that usually comes with those benefits.

With commercial blockchain deployment still in its infancy, it is far too early to determine whether this dream will become reality

or not. The U.S. Justice Department is studying blockchain technology to enhance and improve its enforcement efforts in this area. See "Assistant Attorney General Makan Delrahim Delivers Remarks at the Thirteenth Annual Conference on Innovation Economics—Never Break the Chain: Pursuing Antifragility in Antitrust Enforcement" (Aug. 27, 2020) (available at <http://bit.ly/3q5ncxj>).

\* \* \*

*In the June Part 3 conclusion, Pete Michaelson and Sandra Jeskie focus on the resolution of Blockchain Ledger disputes by arbitration, which the authors state is "the only viable approach."* 

## ADR Skills

*(continued from front page)*

*Participants' behavior has improved, and also mediators'.*

"O, wad some Power the giftie gie us  
To see oursels as others see us!  
It wad frae monie a blunder free us,  
An' foolish notion."

Zoom has given mediation participants something poet Robert Burns believed rested with God—the ability to see oneself in real time. Doing so has improved people's behavior.

Lawyers are less likely to be nasty or insulting or seek to bully an opponent. Philadelphia mediator Bennett G. Picker finds that parties also change their behavior. "One very angry CEO told

me in a caucus session that he was adopting a more reasonable position, in part, because he saw how angry and mean-spirited he looked when in the joint session. He did not like himself very much."

Mediators can also see themselves, providing a new level of insight. One mediator commented that "there is an interesting component of 'self-awareness' that comes from the onscreen version of ADR. I sometimes catch myself looking angry or tired, and I think the participants do too."

## Set Design

A former judge who mediates construction disputes often finds herself the only woman in the process. When she begins a case on video, she makes a point of using a virtual wall with her office logo behind her to establish her authority. Later, to make personal connections, she shows herself in her study.

Another mediator reported that on Zoom, "Parties and lawyers are less confrontational, more friendly. And I *know* I am more friendly."

*It's cheaper and much more convenient.* Parties almost unanimously prefer to mediate virtually. Executives, insurance adjusters and lawyers are delighted to avoid spending the time and expense required to travel to a mediation site.

After an experience with Internet bargaining, a lawyer told Southern California mediator Scott Markus, "I will not be driving to Los Angeles for mediations, and I have a lot of business in Los Angeles. Nor will my clients be spending a day in a conference room away from their office where they could be accomplishing other

## Impatient Signals

I was talking by Zoom with an executive who was explaining, for what seemed like the hundredth time, why a damning email he had sent to the other side would have no impact on a judge or jury. As he talked, I saw myself looking impatient and realized that he was seeing the same thing, probably making him angrier. I quickly adjusted my expression, and afterward wondered what signals I have been unconsciously sending to disputants when no camera was present.

things. I will be participating by Zoom or not at all. It's a voluntary process, right?"

Cases are also easier to schedule if there is no travel involved. And mediators who live far from their offices and can work from home are happy to avoid the commute.

*Key decisionmakers are more likely to be present.* Mediators almost unanimously welcome the fact that a virtual format makes it much easier to get decisionmakers involved. Executives who would never travel to a mediator's office will participate in the process if it is held over the web.

Using video allows mediators to get to know insurance adjusters who were previously only voices over the telephone. The effect, mediators say, is that parties more often make decisions on issues that in an in-person process would be taken back to the office.

*It's easier to talk privately.* A virtual format makes it easier to talk privately with a lawyer  
*(continued on next page)*

## Instant Connection

Scottish mediator John Sturrock was talking with a party whose partner was present to provide support. He asked what the partner was doing that day; "Making a model of a Lancaster bomber," he replied. Sturrock mentioned that his father had been a navigator in a Lancaster and that he had recently rediscovered his logbook. The effect was to make an instant connection with the partner, and provide reassurance to the party. Connections, Sturrock says, can be "most intimate ... candid ... sometimes people even say that they forget they're on Zoom."