

Robots redux: blockchain, augmented reality, quantum computing and the future of arbitration

03 September 2019



Augmented reality (AR) goggles (Credit: istock.com/Just_Super)

*Two years after addressing the impact of artificial intelligence on international arbitration in an article entitled ‘March of the Robots’, **Paul Cohen** and **Sophie Nappert** explain blockchain, augmented reality and quantum computing and predict their future impact on the arbitral process, arguing that lawyers must act now to address those challenges.*

In Ernest Hemingway's *The Sun Also Rises*, one character asks another how he went bankrupt. "Two ways," comes the reply; "gradually and then suddenly."

Such is the way of disruptive innovation. It comes slowly from apparently afar, and before we know it, it's upon us. Arbitration is not immune. The developments that are beginning to transform our field are there to be seen; we know them today, perhaps without fully understanding them, as tech trends and buzz phrases: "blockchain", "AR", "AI", "crowdsourcing".

Their impact thus far has been confined to small-scale, online disputes. But no longer. Take Kleros, the smart-contract dispute resolution protocol that relies on game-theory incentives to motivate anonymous, crowdsourced jurors to rule on disputes through a system of "rewarded consensus" (we'll explain below). Kleros' creators see the system moving beyond software development disputes and into the more mainstream commercial field: credit card fraud, house rental disputes, copyright infringement on decentralised music platforms, crowdfunding, e-commerce. In May 2018, Kleros was accepted into Thomson Reuters' Incubator Program. An initial coin offering has been announced.

Then there's augmented reality. Right now, it's a technology better suited to video games than to vital legal issues. But its uses for arbitration are obvious; its threat to the business-as-usual arbitration hearing is equally so, upon reflection, as we again discuss below.

Last but not least, there's quantum computing. A cutting-edge computer innovation, quantum computing stands to accelerate the (already impressive) speed at which computers process information. That in turn could revolutionise artificial intelligence (AI), a topic to which we devoted considerable space in a 2017 article for GAR entitled "March of the Robots".

Technology has advanced considerably since the publication of that article. The technologies mentioned above and described below are paving the way for what we call alternative alternative dispute resolution (AADR) – non-court methods of dispute settlement that bypass arbitration in its current incarnation – or that resemble it in name only.

Now is the time for arbitration to address the challenges that technology presents to the way we operate. We proffer some thoughts to that end throughout this article.

Blockchain, disintermediation and the promise of decentralised dispute resolution

Many of you have heard of blockchain technology. It is the technology of a distributed ledger system and its first widely known application was associated with the trading of cryptocurrencies such as Bitcoin. You could spend weeks discussing blockchain's finer points – indeed, one of us (Sophie) did, at a course offered at Oxford's Saïd Business School. The essentials are these: blockchain permits a disintermediated approach to the creation, tracking and preservation of information that hitherto existed in centralised locations.

An obvious example, and that which blockchain was designed to disrupt, is banking and the trading of financial instruments. Traditionally, our account information sits in the computers of our respective banks. So, when a claimant deposits money with an arbitral institution for a case, the only two entities involved are the claimant's bank and the institution's bank. The claimant's bank verifies that the claimant has the money for the deposit; the institution's bank verifies that the money has been received; both banks debit and credit the accounts accordingly.

What's wrong with that? Nothing, unless you don't like banks knowing every detail of your business, or you're worried that the banks are vulnerable to being hacked.

Enter the blockchain

A blockchain is a growing list of records, data and information, called blocks. The blocks are identically replicated across various computers (the chain), linked using cryptography; instead of sitting in one database, the information on the blockchain can be found – and verified – on all the relevant servers.

This, and the cryptographic technology that links the chain, make a blockchain resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without also altering all subsequent blocks, which requires consensus of the network majority.

Think about a family tree. Andy is your long-lost great-uncle. A lifelong bachelor, he collected first-edition comic books throughout his life. His harmless obsession is now worth millions. Andy's will leaves his comic book collection to his nearest surviving relative under the age of 50 at the time of his death. That happens to be you. Congratulations.

But not so fast – out of the proverbial woodwork comes Bob. He is 44 years old. Bob claims that he is Andy's illegitimate child from a fling with Lynda Carter (she of Wonder Woman fame in the 1970s – Google it if you're too young to remember.) Andy was cremated and his DNA destroyed; in any event, his will specifies that his heir will be decided by the family tree alone, not by any DNA analysis.

Could Bob graft himself onto the family tree? Not in a blockchain system. Each step in the system – each transaction, data point, piece of information – follows on from the previous one, after all the nodes in the distributed chain have ratified it. On the blockchain, the verification that Noah begat Ham, Shem and Japheth is preceded, on each and every node where the family tree exists, by the information that Noah is the son of Lamech, who was the son of Methusaleh, who was the son of Enoch, who was the son of Jared, who was the son of Mahaleel, who was the son of Cainan, who was the son of Enos, who was the son of Seth, who was the son of Adam and Eve.

You can see why blockchain technology is proving seductive for securing chains of property title. With a little further explanation, it will also be clear how blockchain is used to support crypto-currencies such as Bitcoin or Ethereum.

Imagine you want no part of any paper currency or any central bank. You need to make transactions, so you make up a currency of your own. But without a central authority to monitor it, who's going to trust you when you

say you have three zillion of the new currency (let's call a unit of our new currency an "arby") ready to spend? Who's going to trust someone else who says you just paid her one zillion arbies to buy the last remaining hard copy of the first-ever GAR 100?

Now the mechanics of blockchain's distributed ledger technology start to come in handy: everyone who deals in your currency has a truthful, verifiable record of where all the currency is. You start with three zillion arbies; perhaps others have some too. You covet the hard copy of GAR 100 2007. You find the seller. You offer one zillion arbies; she accepts. This transaction is recorded not in some bank, but on the blockchain. Everyone with a stake in your virtual currency is apprised that you are down two zillion arbies, and your seller (who might remain anonymous) now holds one zillion.

The more technically-minded among you might be asking yourselves, "How is this different from the way banks today record their information?" One key difference lies in the combination of blockchain's reliability and anonymity. Banks – provided their servers aren't hacked – keep reliable records about their customers. If you transfer [annual subscription amount] to GAR to use its services, your bank and GAR's bank know how much was transferred and how much now sits in your respective accounts.

But as for anonymity – forget about it. Your bank can't process a transaction from you without debiting your account; and it can't debit your account if it doesn't know who you are. Currencies trading on the blockchain, such as Bitcoin, let you transact without needing to know who you are. That is their distinguishing characteristic.

A bit of technology

It's difficult to explain how this works without getting technical, but it is important to get to grips with at least the basic concepts to understand these technologies' practical application: instead of an identity that can be verified with a passport or a national ID number, your virtual currency "wallet" contains a cryptographic key. That key tells the virtual currency world that you – whoever you may be – are ready to buy and sell.

Let's return to the example of buying the 2007 edition of the GAR 100. If there's no bank for your seller to contact, and she doesn't know who you are, how is the transaction safe and verifiable? The answer is that the blockchain generates a cryptographic problem, or puzzle, that takes a lot of computing power to solve but is easy for other computers to verify. Solving and verifying the problem adds a block to the blockchain stating that you just transferred one zillion arbies to your seller. Everyone remains as ignorant of your identity as they were before; the system just collectively knows that your seller is one zillion arbies better off than she was before.

It's worth taking a moment at this juncture to understand the basics of encryption. Not only will this help explain the lure of blockchain; it will also elucidate the potential dangers of quantum computing, which we discuss in a section below.

We all know that computers can calculate incredibly quickly. There are some calculations, however, that current computers (to say nothing of humans) can't perform with any great speed. One of these is prime factorisation.

It sounds like a made-up term from Star Trek, but prime factorisation is simply a calculation of which prime numbers you can multiply to make a higher number (a prime number can only be divided by the number one and itself.) It starts out easily enough – if we ask you which prime numbers combine to form 21, you won't scratch your head very long before arriving at 3 and 7.

But what if the number you need to factor is 496,972,844,573,606,300? Not so easy to perform by trial and error. By contrast, if someone told you that the prime numbers that multiply to make up the large number above are 694,947,839 and 715,225,739, you'd have a decent chance of slogging through that calculation in a few minutes, depending on how well you remember multiplication by hand.

That's essentially how internet-based encryption works. You have a giant number (dozens, or hundreds, of digits) that's divisible by two much smaller (but still giant) prime numbers. If you know the two prime

numbers, a computer can easily multiply them to know the encryption key. But if you don't know them, a computer will take days, months, or even years of brute-force calculations trying to figure out which prime numbers are involved.

To make things more complex still, blockchain usually uses a somewhat different kind of encryption than the standard one (known as RSA encryption) described above. The details need not detain us, but the essential point is that, as with RSA encryption, a computer takes a long time to authenticate an encrypted transaction, but other computers will need a relatively short time to verify that transaction once they know what the encryption keys were. The computer servers that spend the time and energy (literally) doing this grunt-work are rewarded with virtual currency of their own. This is known in the jargon as "mining."

What about arbitration? (And a word about smart contracts)

You can be forgiven at this point for wondering what all this has to do with arbitration. The answer is that a new form of dispute resolution is developing that makes use of the blockchain's features.

Blockchain arbitration – for want of a better term – works from the premise that automated contracts are the wave of the future. These automated contracts, known (ironically or otherwise) as "smart contracts," embed the key contractual terms, comprising an agreement in computer code. This means – to put it in its simplest form, "if this, then that" – that those terms will be performed without the need for substantial human input.

The typical illustration of a basic smart contract, given by Nick Szabo, the computer scientist, legal scholar and cryptographer who coined the phrase and developed the concept of smart contracts, is a vending machine that releases your drink or snack once you have put in your coins.

For a more sophisticated example, take a construction project. Imagine a smart contract that stipulates milestone payments for particular phases. Once a builder had satisfactorily completed a phase, the contract would

automatically send a payment. That might not sound terribly radical; a computer programme is just shortcutting a process that used to require more human interaction – just like a visit to a cash machine can accomplish much of what used to require a visit to a bank teller.

The radical implications stem from what some programmers would like to do with smart contracts in the event that a dispute arises between the parties. Again, the coding is easy to conceptualise without any technical knowledge: if parties agree, then move on to next phase of contract; if parties do not agree, then move to the dispute resolution mechanism.

And here it gets interesting. Some blockchain and smart contract entrepreneurs have simply set up a process whereby a dispute is referred to an arbitrator, much as any “dumb” contract might be. Others, however, have made use of blockchain’s attributes to establish a dispute resolution system in which anonymous, crowdsourced decision-makers can resolve a dispute by “voting” on which party is right and – importantly for us – being incentivised to vote by consensus.

One of the better-known of these AADR blockchain mechanisms is Kleros, to which we referred in our introduction. The word kleros is ancient Greek for a share, an allotment, or an object used for casting votes. Under the Kleros system, a dispute in a smart contract is assigned to a number of anonymous decision-makers (called jurors). The contract is undergirded by a virtual currency (in the case of Kleros, one called Ethereum). Would-be jurors – the terminology of Kleros switches between the language of courts and that of ADR – bid in virtual currency to serve on a dispute. The higher their bid, the more likely they are to be selected.

In a dispute, each juror votes anonymously. Those in the majority are rewarded with a bonus to their currency holdings; those who vote against the prevailing decision lose some of their virtual currency.

This is dispute resolution through the wisdom of crowds, with an incentive for the crowds to converge on one viewpoint. It is not arbitration in any sense that we now understand and practise it. But that is the point – and the threat: whatever we may think of the fairness and thoughtfulness of

this method of dispute resolution, it has no room for anyone likely to be reading this article.

Today, the type of dispute that a system such as Kleros's handles is straightforward and usually binary: pay the claimant, don't pay the claimant. But as with all technology, this initial simplicity is deceptive. There's nothing technically that prevents greatly more involved decision trees and concomitantly greater numbers of decisions for jurors to make, up to and including the number and range of decisions that arbitrators make in major international disputes.

We may scoff at the relative care, or lack thereof, that any such system might apply in these major disputes. But we will not be able to match these systems for speed, low cost or security. And perhaps, for a generation that puts a premium on likes and influencers, the common-sense input of dozens or hundreds of people will come to be seen as a significant virtue over the drawn-out musings of a mere one or three individuals with arcane knowledge of obscure arbitration proceedings. Time, of course, will tell.

AR, VR and their challenge to the bricks-and-mortar arbitral centre

In our previous article, we devoted a good deal of space to discussing the benefits and drawbacks of video conference technology in arbitral hearings. A mere two years later, it might seem strange that anyone doubted the viability of the video conference. That's because, like so many technologies, the costs of a video conference have plummeted, at the same time as video and audio quality have improved exponentially. Yes, there are still blips and lapses, but we are past the period when they were the rule rather than the exception.

One of the signal evolutions in the (physical) infrastructure of international arbitration has been the development of arbitral centres for holding hearings. If a locale aims to compete as a leading seat, an arbitral hearing centre has become de rigueur.

The principal function of hearing centres remains to provide a place for the participants to meet in person. But where one or more participants are unable to sit in the hearing room, video technology has bridged the gap. To that end, most centres incorporate, or accommodate, sophisticated video equipment.

The rationale for centres, however (with or without video equipment), is premised on the notion that participants in an arbitral hearing ideally need physically to be in the same place at the same time. Technology is seriously challenging that premise.

Many readers will have heard of virtual reality (VR) and augmented reality (AR). VR uses a headset to immerse the wearer in a digitally recreated space. That space can be anything and anywhere – the top of Mount Everest, a rollercoaster, the Louvre, a computer game designer’s rendering of another planet. We briefly alluded to VR in our earlier article.

AR is a cousin of VR. It (currently) requires a headset, a pair of glasses, or at least the screen of a smartphone or tablet. Unlike VR, AR does not blank out the rest of the world; rather, it superimposes images onto the wearer’s field of vision. So, to take a current example, surgeons can look in on operations remotely, either to learn from them or to supervise them.

Just as video conference technology started out as expensive and unreliable, VR and AR as we write this have limited application. The highest quality headsets still cost thousands of dollars, and graphic design is either very costly or quite basic. But this will change.

We can sketch out the probable course of VR/AR technology if we use science fiction writer William Gibson’s adage as our guide: “The future is already here; it’s just not evenly distributed.” Looking at the cutting edge of high-price VR and AR, we see that companies are beginning to experiment with projecting holograms of people. Today, those holograms need to be created in a specialised studio; it’s unlikely to be more than a few years before the technology is sufficiently affordable to permit images to be projected from virtually (pun intended) anywhere.

It's not difficult to conceive of how this might look in an arbitration: imagine a world where everyone is equipped with smart-glasses instead of a smartphone. Counsel for the Claimant enters the virtual hearing room. She sees holograms of the arbitrators seated before her. The arbitrators, from their various physical locations, see the counsel's holographic form wink into existence.

If you have endured and cared to remember anything about the Star Wars prequels, this might call to mind the Jedi Council, where the participants assemble entirely holographically. Arbitrations of the 2020s and 2030s are likely to look like that (hopefully minus the lightsabers).

If they do, this raises the question what use remains for hearing centres. Certainly there could be rooms with specific places – the arbitrator chair, the counsel table, the witness box – the various participants could “appear” via hologram. But one wonders who would pay for space in a hearing room simply for these decorative details – especially when they could be replicated in a virtual room by merely donning a headset.

There remains, as there has throughout the arbitral world's contemplation of a technological future, the question whether people will still congregate in one place, at one time, for the sake of human interaction and using all their five senses in a high-stakes legal dispute. For reasons we discussed extensively in “March of the Robots”, there appears to be a psychological preference, at least among today's more experienced practitioners, for the known quantity of human contact.

We should also not underestimate the power of nostalgic thinking (we mean the term neutrally, not as an insult) in organising the procedures of international dispute resolution. For all but the youngest among us, nostalgic thinking about dispute resolution entails the trappings of mid- and late-20th century courts and their procedures, suitably and (more or less) subtly adapted for arbitration. The question for us to contemplate is: what, if anything, about in-person dispute resolution will remain essential or desirable to retain in the next decade?

Younger practitioners' nostalgic thinking harks back only as far as a world that was already digital. Will they see any point in expending massive greenhouse gas emissions to converge on one place? Will in-person hearings, indeed, be considered a moral choice, if adequate virtual alternatives exist?

The arbitration community would do well to look closely at how judicial courts are proactively addressing these same challenges – a stance that it is urgent for the arbitration community also to adopt. Users of arbitration will have little appetite to pay for a process mired in nostalgic thinking and may look more favourably to the technological solutions adopted by modern judicial courts.

Quantum computing and the dawn of generalist AI

We devoted a substantial portion of “March of the Robots” to discussing the potential effect on arbitration of artificial intelligence (AI). Once again, the passage of a mere two years has been instructive in showing the speed with which technology can move from cutting-edge to commonplace. Two years on, we do not need to explain what AI is and how, in general terms, it works.

We have seen AI begin to make footholds in international arbitration – particularly with internal analyses of case outcome probabilities, assistance with legal research, and refinements to calculations of quantum.

Thus far, however, we remain a long way from the kind of all-knowing, multipurpose AI that populates the dreams of futurists. We discussed two years ago the remarkable proficiency of AI algorithms in performing discrete tasks. An AI programme can now: detect cancer in a patient x-ray more accurately than a radiologist; defeat world champion gamers of all kinds, from Chess to Go to Jeopardy; drive a car more safely than most humans; predict the outcome of US Supreme Court decisions more reliably than most prognosticators; and translate a book much more quickly – though as yet much less elegantly – than professional linguists.

In all these fields and others, AI has either surpassed or is rapidly catching up to the capabilities of human experts. But it remains an exercise in specialisation. The most sophisticated medical diagnostic programme could not tell you the first thing about chess; the machine-learning algorithm that can compose a cantata in the style of Bach or solve the disputed songwriting credits of Beatles hits wouldn't even know how to turn on your car, let alone be dangerous enough to crash it.

These limitations on AI stem from the fact that an algorithm requires large volumes of data to learn anything useful and accurate. A facial recognition system requires the input of hundreds of millions of data points to detect the difference between one face and another. Likewise, an AI diagnostic assistant needs more than 100,000 examples of correct and incorrect diagnoses before it can perform usefully as a pattern-spotting predictor of disease.

Even though computers can crunch data incredibly fast and with ever-increasing speed, it remains beyond their current ability to absorb data on completely divergent subjects in such a way as to be useful in all of them. Don't expect even a supercomputer today to be much help supporting a single algorithm that can thrash you at chess, safely drive you to work, and invent a nice little tune in the style of Lennon and McCartney.

The good – or bad – news is that this may all be about to change. That change will be due to an entirely new form of computer processing known as quantum computing. The “quantum” here has nothing to do with damages calculations. Rather, it is about harnessing the weird properties of sub-atomic particles to make computer processing exponentially faster. This requires a short, non-technical digression into the mechanics of computing and the physics of the quantum world. If you have read this far, you are up to it.

A brief history of microprocessors

The basic component of the modern computer is the transistor. A transistor is simply a device used to direct electrical current. Transistors are made with semiconductors. A semiconductor is a material that conducts

electricity under some circumstances but not under others. This makes semiconductors ideal for use in controlled electrical circuits.

The most common semiconductor by far is silicon. By adding impurities to silicon – usually boron or aluminium to give a slight positive charge, and phosphorus to do the opposite – a series of transistors can direct or block the flow of a tiny electrical current on and off, like a microscopic light switch.

Now imagine that we married these fortunate properties of slightly impure silicon with the Boolean logic that many of us suffered through in school algebra classes. Boolean algebra, to put it basically, represents an attempt to put propositions in the form of being either true or false. True is usually represented by 1; false is denoted by 0.

With the ability to manipulate these tiny electrical currents, transistors can be used to mimic the activity of Boolean algebra: a current that is flowing through the circuit at high voltage is designated as “on” or 1; a current that is impeded in the circuit is designated as “off” or 0. A series of transistors therefore can generate a series of binary code that corresponds to a Boolean proposition: $10 + 10 = 100$ (in base ten, $2 + 2 = 4$).

Each of these ones and zeros is known as a bit. And it doesn't take the proverbial rocket scientist to see that an awful lot of bits are needed to do anything useful with computers. Fortunately, the size of transistors – these little pieces of impure, current-carrying silicon – has been going down reliably for the past 50 years. Gordon Moore, the founder of Fairchild Semiconductor and later CEO of Intel, famously (and accurately) predicted in his eponymous law that the number of transistors you could put in an integrated circuit doubled every two years or so. Thus, the microprocessor (or silicon chip in the jargon of old) in your smartphone today is probably about 64 times more powerful than the microprocessor in the original iPhone of 2007.

Moore's Law is a useful heuristic, but it isn't a law of nature. Soon enough, the rate of processing power will slow down. And as they get smaller, transistors are beginning to deal with currents that consist of individual

electrons. And individual electrons, because they are subject to the rules of quantum mechanics, act in weird ways; very weird ways.

Everything you wanted to know about quantum physics but were afraid to ask

Now for the second part of the digression: the wonderful world of sub-atomic particles. The physics of Isaac Newton describes the workings of the universe perfectly well for the most part. The exceptions are when things get too big (for which you need Einstein's Theory of General Relativity), or when they get too small. At a certain level, roughly the size of a few atoms and smaller, the world as we know it completely stops making sense.

Here is not the place for a disquisition on quantum physics (assuming we were even competent to write one). For our purposes, let it suffice to say that, at a sub-atomic level, particles can exist in more than one place, or one state, at the same time. An electron, for example, has a property called spin. Its spin can be both "up" and "down" at the same time. In the macro-world, that would be like the North Pole doubling as the South Pole.

Again, it makes no sense; Danish physicist Niels Bohr quipped that anyone who is not shocked by quantum physics has not understood it. It's not susceptible to everyday explanations, but it can be described perfectly in mathematical terms. Indeed, the predictive power and practical power of the mathematics behind quantum mechanics has worked wonders: everything from lasers to fluorescent lightbulbs depends on quantum-level interactions.

Now let's turn back to computers and the bits that make them work. Remember that, in the quantum world, a particle can exist in two states at once. What could happen if you could use properties of these particles, instead of a larger electrical current, as the pieces of information used as bits?

The practice – again vastly oversimplified – goes something like this: instead of a higher or lower voltage translating as a 1 or 0, an electron's spin

(“up” or “down”) forms the basis for a measurement. But because of an electron’s quantum weirdness, it’s spin can be “up” and “down” at the same time. So, instead of registering as a 1 or a zero, it can register as a 1 and a zero.

A quantum bit is known as a qubit. And qubits, with their flexibility to be in two states at once, pretty quickly become vastly more useful than plain old bits. One qubit can render two states; two can render four; three can render eight; four can render sixteen; and so on.

By the time you reach 72 qubits, you have enough processing power to exceed even the most powerful conventional computers. This is known as quantum supremacy. It’s the Holy Grail of quantum computing. Google and some of its rivals claim to be only months away from this milestone.

If it’s that straightforward in theory, why hasn’t it been done yet? The answer is that keeping particles in their quantum state isn’t easy. It’s an engineering conundrum that requires a great deal of energy and ingenuity. Sub-atomic particles have a habit of collapsing out of their quantum states, especially when you observe them (another strange phenomenon of the quantum world.) You need a busload of spare qubits and a bunch of other redundancies to correct for errors.

Nonetheless, quantum computing is on the verge of exploding into the commercial sphere. When it does, AI’s current limitations will be a thing of the past. The algorithms that previously could either walk or chew gum will now do both, while whistling a happy tune.

And that possibility will take AI right into the realm of the Robots – algorithms that could learn every legal system on the planet, review every arbitral treatise and award, analyse hundreds of thousands of cross-examinations, assimilate every principle of damages calculation, and learn more about human psychology than any professional – all within minutes.

We’re not there yet. But we really aren’t as far away as we might like to think – or as we thought a mere two years ago.

Conclusion: coping with the threat of AADR

Upon receiving his lifetime achievement award from GAR in 2015, the late Arthur Marriott QC said: “We must get a hold of technology, or it will surely get a hold of us.” The choice is ours, or is it? In the words of Sir Geoffrey Vos, the chancellor of the High Court, the way we resolve disputes arising in a world of smart legal contracts will be critical to the rule of law in the future.

Given the important role played historically by international arbitration in upholding the rule of law in cross-border disputes, do we have the luxury of passively waiting until arbitration as we know it is replaced by AADR’s incentivised consensus?

We think not. We believe that, as a community of users of and actors in arbitration, we have no choice but to be proactive and to consider, as a matter of priority, how we anticipate, adopt, and co-opt emerging technologies to the benefit of arbitration as we know and understand it.

At its best, arbitration in the mid-21st century will be a process with a core of human control, flexibility and initiative, yet enhanced by a modern, technology-savvy approach to dispute resolution and decision-making. This can be the best of both worlds. Let’s work to make it so.