CHEAT SHEET

- *Speaking your language.* In the healthcare industry, blockchain has three applications: 1) it employs cryptography to immutably record transactions and ensure integrity; 2) it is a distributed platform that keeps many copies of the transactional ledger; and 3) it enables transactional automation via smart contracts.
- *Privacy is primary.* Privacy and security are essential to the success of blockchain. Make sure to stay abreast of changing privacy and data security laws to ensure that using blockchain does not lead to infringement.
- *Healthcare uses.* Blockchain applications promote efficiencies by reducing administrative costs and delay in the contractual promise. With regard to payment models in the healthcare industry, blockchain can be used to create a common platform to administer payments and adjudicate claims.
- *Fraudulent violation.* There are two blockchain characteristics that may lead to allegations of fraud: (1) the use of the crypt-currency such as Bitcoin, and (2) the potential for having blockchain technology control referrals.

Blockchain Meets Healthcare:

Understanding the Business Model and Implementing Initiatives

By Les Wilkinson, Jason I. Epstein, and Roy Wyman The way we think of healthcare IT (HIT) is undergoing a radical shift. HIT resources currently revolve around central hubs and intermediaries for data and transactions. Hospitals, payors, electronic health record (EHR) vendors, supply chain management companies, and others serve these roles at great cost in time and money. The entire healthcare industry, like many others, is considering blockchain technologies to deliver more efficient ways to share and use data and transact business in secure environments.

A recent survey from IBM indicates that 16 percent of healthcare entities may already be working with blockchain in 2017. Often businesses interested in blockchain may not fully understand how the process works or applies to them. This article provides a summary of blockchain, identifies legal issues, and discusses some of the exciting possibilities and challenges to execution. As lawyers, our goal should be to understand blockchain business models and "use cases," avoid the hype, and help our clients determine if and how to implement blockchain initiatives.

Origin of blockchain technology

The origins of blockchain lie in the advent of Bitcoin, the decentralized virtual currency. Bitcoin can be thought of as three layers of technology: On top is the actual digital currency that bears its name; in the middle is the protocol layer, which enables and provides utility to the currency; and at the bottom is the Bitcoin blockchain that forms a trusted or — perhaps better stated — trustless record of all Bitcoin transactions that have ever been executed. The "blocks" in "blockchain" are the ordered, time-stamped, and digitally encrypted records or transactions connected to the immediately preceding block. The blocks are connected through cryptographic algorithms or "hashes." The chain of blocks is thus called a "blockchain."

The language of blockchain

Industries are coming together to form consortia such as R3 for financial services and most recently HashedHealth in the healthcare space. Projects like Ethereum and Hyperledger are working to collaboratively build an open-source, cross-industry protocol blockchain platform for use beyond cryptocurrency. There is no single definition of "blockchain," but Hyperledger provides a pretty good one:

> A shared ledger between a set of entities that faithfully records a series of transactions, without needing trust and a smart contract platform, for embedding scripts that run across the network and can add new entries to that ledger. Some systems are permissioned (where entities are named/known), and others are unpermissioned (where anyone can participate, even anonymously).

Blockchain has exciting applications in healthcare because it, among other things:

- Employs cryptography to immutably record transactions, and thus ensure transactional integrity;
- Is a distributed platform that automatically keeps many copies of the transactional ledger in consensus, which ensures integrity in transactions among many enterprises; and,
- Enables transaction automation via smart contracts, allowing even greater transactional efficiency and savings.

Here is a graphic representation of the difference between the traditional, centralized network and a distributed blockchain network:

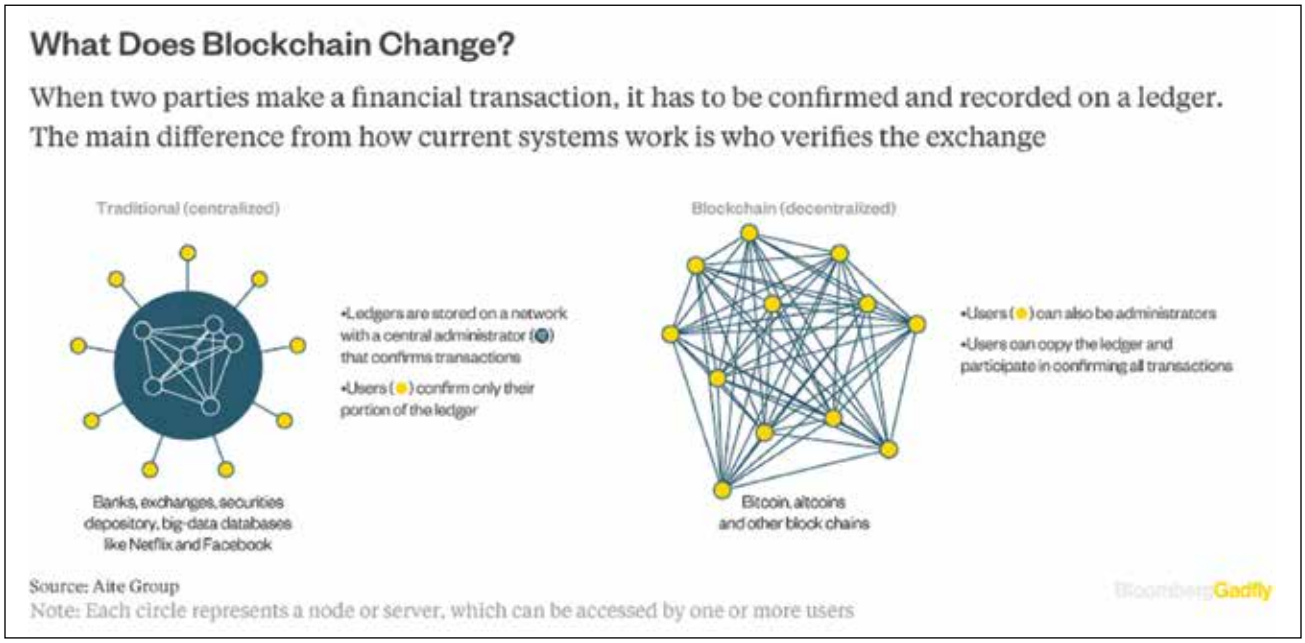
One of the defining attributes of blockchains is that they are decentralized and distributed networks. Blockchain is often referred to as a "distributed ledger technology" (DLT). Instead of using a clearinghouse or EHR to provide centralized functions, a blockchain technology application could be managed by the network of participants — in effect, computers — that validate transactions by consensus (or, at least portions of the job of these intermediaries could be made more efficient and less costly).

The evidence of any transaction in the "blockchain" is in a shared ledger that is on every computer participating in the network. Because of the algorithms coded into the protocol layer, network participants operate within systems of "carrots and sticks" that reward participants for correctly validating transactions and penalize them for attempts to game the system, thereby creating a trustless system. The practical effect of this is that there is no "trusted intermediary" required to verify a transaction (and expecting to collect a service fee). All of the ledgers and transactions are encrypted using cryptography, so any unauthorized changes would be recognized immediately. Because of the algorithms involved, unauthorized changes are highly unlikely.

Les Wilkinson is general counsel and chief development officer at Nashville, Tennessee-based company Hashed Health, a leading consortium of healthcare companies focused on accelerating meaningful innovation using blockchain and distributed ledger technologies. He manages strategic partnerships and corporate development. *lwilkinson@hashedhealth.com*

Jason I. Epstein is a partner and co-leader of the Technology and Procurement Group at Nelson Mullins in Nashville, Tenn. He also is an adjunct professor at the Vanderbilt University Law School, where he teaches "Law of Cyberspace." Epstein has experience in blockchain, AI, cognitive computing, Internet of Things, electronic signatures, cloud computing, privacy and security, and open source code, as well as many other technology issues facing healthcare and other companies. *jason.epstein@nelsonmullins.com*

Roy Wyman is a partner and member of the Healthcare Regulatory and Transactional Team at Nelson Mullins in Nashville, Tenn. He previously served as chief privacy officer and associate general counsel for a leading hospital staffing firm. Prior to that, he was senior legal counsel for CVS. In his practice, he counsels healthcare companies on the regulatory and transactional aspects of day-to-day business matters, including the integration of technology into their operations. *roy.wyman@nelsonmullins.com*



"Permissioned" blockchains are networks with known participants. "Unpermissioned" blockchains are open networks where participants are not known. Some blockchain applications have both types of participants. Depending on the industry, knowing who is on the network may not only be desired but legally required. In healthcare, for example, it will be important to control which providers and other entities have the ability to access and control patient data managed by blockchain applications. Another example is in the financial world, where know-your-customer and anti-money-laundering statutes require identification of customers. As mentioned below, sometimes those regulations can be addressed by combining blockchain technology for transactional efficiency with applications on or "off the chain" — which use blockchain but then "reconnect" identities.

Another attribute of blockchain technologies is the concept of a "smart contract," which is a computer program that sits on top of the blockchain. It facilitates and completes a transaction automatically and often is referred to as "self-executing." In the healthcare context, a smart contract could be as simple as a patient granting access to her healthcare record to her doctor through computer programming. Also, personal health information can live behind a smart contract that requires proof of an executed business associate agreement, which could also be confirmed through programming.

As discussed more fully below, many times it is the application used in conjunction with the blockchain that provides the greatest value in healthcare. The convergence of blockchain and artificial intelligence (AI), for example, is giving rise to what some refer to as "cognitive contracts," which are smart contracts that have auto-executing contract features on the DLT, with an AI component. In such cases, the AI learns over time to help with more personalized medicine decisions based on personal habits, family history, review and analysis of massive amounts of research data, and other unstructured data points.

Legal issues in blockchain

As with other technologies, practicing law in the blockchain space requires the application of pre-existing legal constructs with an eye toward new issues.

Despite the hype, many of the legal issues related to blockchain are not new and can be found in technology practices generally. These include issues found with open source initiatives, intellectual property and patents (including the defensive use of patents), privacy and security, electronic signatures, and contracts. Likewise, the regulatory issues that arise in a healthcare setting largely remain the same: Federal Trade Commission requirements regarding privacy and other statements; Health Insurance Portability and Accountability Act (HIPAA); Family Educational Rights and Privacy Act limits; and European Union Data Protection Directive requirements.

In addition, having an understanding of the small but potentially growing number of laws specific to blockchain often is required. As with any new technology, addressing those issues may require new approaches, but we believe that they can be conquered with sufficient creativity.

A threshold question for clients using or developing blockchain applications is the view toward open source. Open source technology is well established and, like blockchain, comes

Executive summary

When most people hear about blockchain, they think of Bitcoin, the virtual currency. But blockchain is a lot bigger than Bitcoin. In the years to come, blockchain could enable magnitudes of efficiency in many business sectors, with special implications in intellectual property, financial services, mergers and acquisitions, insurance, and anything involving the security and exchange of data. It is this last sector — data and security — that will make it attractive to healthcare, an industry built on layers and layers of medical, patient, and reimbursement data in which security is mandated and regulated.

Blockchain is a distributed ledger of transactions that is validated and maintained by all the computers in its network. Every user has a real-time copy of the ledger, and for a transaction to be validated, the other computers on the network must authenticate the integrity of each past transaction — contained in linear "blocks" of data — to give permission for a new transaction. There is no central server to hack into, and all users are authenticating one another before a new block of data can be added to the chain of data.

The promise for healthcare is a secure system for improving audit and compliance processes, financial and contract management, resource tracking and verification, and overall data liquidity at a cost that is a fraction of today's centralized databases.

Blockchain has the potential to revolutionize how we think about and use data, but we are in the early days. The promise of blockchain is too much for business to ignore, and networks are forming to build and test early-use cases. Look for financial services to lead the way as an early adapter, and health care shouldn't be far behind.

with its own emotions and confusions. Open source purists, for example, require that a contributor release its own source code along with the code received under the open source license (often referred to as "copyleft," "reciprocal," or "viral" licenses). Others view open source in a broader sense in that it can include copyleft licenses but is now required to do so.

This is a key issue to address representing blockchain consortia or the decision to participate in an open source project. In fact, this led to the incompatibility of two of the major blockchain entities: Hyperledger and Ethereum.

The Hyperledger Project uses an open source license, Apache 2.0, that does not require releasing any modifications to the software received under it. Hyperledger wanted to collaborate and connect Etherium's code, which was licensed under a copyleft license, the GPL-3. To be compatible, all of the contributors to the Etherium code would need to agree, in effect, to relicense it for use under the Apache 2.0 license. This effort failed, and so did the collaboration. Again, open source is not new, but a knowledge of it is required to assist clients in navigating the open source landscape in blockchain.

Obtaining and using patents for offensive and defensive use is also not new, and it has been an issue in open source licensing. Apache 2.0, for example, includes a patent license that grants the licensee any licenses necessary to use the code without infringement. The license goes even further, stating that any patent licenses issued to the user under the license terminate if the user initiates a patent lawsuit.

Privacy and security are a primary issue for technologies, and blockchain is no exception. One of the biggest attractions to blockchain is that it is secure and immutable. Blockchain uses cryptography to encrypt each block in the chain, making it extremely difficult to hack. Each transaction and record, for the same reason, is also immutable. If any transaction or record is tampered with, it will be recognized by the other ledgers on the chain and rejected. Hashing and encryption are familiar concepts in the world of electronic signatures and contracts. Digital signatures and records are similarly encrypted and provide very reliable evidence if needed as proof.

Electronic signature and contract laws also apply to smart contracts generally. The Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transaction Act (UETA), for example, are the primary laws establishing that no signature or transaction will be denied legal effect merely because it is in electronic form. The definitions of electronic signatures and electronic records already include smart contracts, but a potential gap could be the scope of those laws. The scope of both laws relates specifically to transactions in the business, including commercial (including consumer) and governmental spaces. While most smart contracts would still fall within those parameters, in healthcare, for example, there could be a gap where a patient merely wants to share protected health information with a professional. While that sharing of information may not qualify under the scope of the laws, the related sharing of insurance, payment, and other transactions clearly would qualify.

Vermont took the opportunity be a first mover in blockchain, recently passing a blockchain-enabling law that creates a rebuttable presumption of authenticity from an evidentiary standpoint. The report to the Vermont

legislature, "Blockchain Technology: Opportunities and Risks," gives insight into Vermont's desire to create more certainty and foster an environment of acceptance around blockchain. The report briefly discusses the potential issues with UETA and is careful to note that the state's law will not affect UETA. This concept is not new in the international community. Digital signatures, known as qualified electronic signatures in the European Union, are digitally encrypted and are given a presumption of validity under the new EU regulation eIDAS. An interesting question, however, is whether we will begin to see a patchwork of different laws with different definitions and standards.

Arizona took a different tack by recently passing a law that amended the Arizona version of UETA, the Arizona Electronic Transactions Act (AETA). AETA was amended to state that a signature that is secured through blockchain technology is considered to be in electronic form and is an electronic signature. Further, a smart contract transaction may not be denied legal effect solely because it contains a smart contract term. Arizona provides its own definitions of smart contacts and blockchain that are different from Vermont's.

As this article is written, Nevada is in the process of amending its electronic transactions law to define blockchain and include it in the definition of electronic records. It also forbids boards of county commissioners or city councils from imposing taxes or fees on the use of blockchain.

UETA and eSIGN are decidedly technology-neutral laws. They do not assume or discuss any particular type of technology platform. The rise of certain state laws are designed to address or create certainty around blockchain technology. Does the fact that Arizona amended its electronic signature law mean smart contracts were not already covered, or was it merely for clarification? Are various state and federal laws going to suggest different definitions? Clearly, there are some gaps to fill, especially in specific circumstances, but perhaps it is time to consider the creation of uniform state or federal laws. Only time will tell, but these issues illustrate that lawyers must provide input into the debate around emerging blockchain laws.

Healthcare use cases

Healthcare is dominated by closed, controlled operating systems with a lack of interoperability between data silos. These operating systems are controlled by market competitors with a highly complex and overlapping regulatory framework. At a high level, use cases for blockchain can be thought of in the following general areas — audit and compliance, financial and contract management, Internet of Things (IoT), and data liquidity — with identity management and security, privacy, and confidentiality applications that span those core areas.

Blockchain offers the promise of an immutable, single source of "truth" from multiple enterprise sources. Physician Payment Sunshine Act compliance provides a good example. The Sunshine Act was passed as part of the Affordable Care Act to shed light on financial relationships between drug and medical device manufacturers and doctors in order to control costs and help patients make more informed decisions when choosing healthcare professionals and treatments. The law requires manufacturers of pharmaceuticals, biologics, and medical devices to collect and track data regarding payments and other transfers of value that they make to physicians and teaching hospitals, including physician ownership and investment interests, and electronically submit such data to the Centers for Medicare & Medicaid Services. This creates a daunting administrative challenge and risk of duplicative reporting when there are multiple entities making payments on behalf of a manufacturer (e.g., clinical research organizations and group purchasing organizations). A blockchain-supported, coordinated, decentralized framework for tracking and reporting these payments would address these issues.

Blockchain applications promote efficiencies by reducing administrative costs and delay in multiparty contractual processes. There is tremendous promise in the potential for blockchain-enabled technologies to support innovative payment models. The use of blockchain to create a common platform to administer payments and adjudicate claims would address the roadblocks of trust and payment administration costs currently inhibiting those efforts.

Furthermore, such a system could bind an individual's benefits to the payment mechanism itself. The idea of programmable payments opens the door to new payment models and new, value-based market concepts.

Additionally, a distributed platform could become an enabler of self-organizing care teams that take clinical and financial responsibility for the management of conditions and delivering care. Payments could be tied to quality gates. Such payment models are not limited to our current concept of "bundles," and they can serve to support the physician-focused models emerging as a priority of the new administration.

A common legacy IoT use case lies in securing high-value assets in the supply chain. In many cases, healthcare providers, manufacturers, and suppliers still suffer from a wasteful, inefficient supply chain. IoT solutions are being deployed to help solve these problems, but current systems have their shortcomings caused by data centralization, which results in system inefficiencies and security risks.

For example, current methods can track when a shipment arrives but require an invoice, internal ticket, account payable review, and disbursement. Blockchain solves these issues by decentralizing the control of registration, verification, and ownership, chronologically tracking activities from each device.

Filtered device data can be translated to blockchain application program interfaces and business rules established by participating peers that can then trigger real-time workflows, alerts, invoicing, or payment. Current tracking methods, if tied to a blockchain in the future, could register delivery of a product and automatically trigger requests for payment. Device wallets could enable machine-to-machine transactions that are not possible in today's centralized systems. The result would be improved trust, accountability, transparency, and automation between devices.

Recently, the Illinois Department of Innovation & Technology announced new blockchain "use case" projects that it seeks to develop with industry partners, with each project utilizing "light-touch" regulation, community building through education and outreach, and the integration of the technology through use cases. While still in its early stages of development, one use case would reconcile healthcare provider data from the Centers for Medicare and Medicaid Services, the Drug Enforcement Agency, state licensing boards and insurance providers and act as a single source of licensing information for providers and payers. One can easily envision such a use case creating far more efficient and accurate credentialing practices and protecting both providers and the public.

Connected devices of the future can enforce contracts, enable new collateralized finance models, and execute payments. Digital certificates can prove authority, origin, and compliance. Transfers of ownership of pharmaceutical, medical equipment, and all other assets become properly structured and auditable. IoT data can be monetized in new ways that empower patients. Connected devices will help shift more services out of expensive hospitals to the home or an alternative site where patients can access services at a lower cost and risk.

Perhaps the most heralded use cases for blockchain in healthcare stem from the idea of universal data interoperability. Most of us are familiar with the troubles caused by data silos. The upside to interoperability includes facilitating more effective patient-reported outcome measures, data management, and self-sovereign consumer health data aggregation. Credentialing provides a good use case. Providers must be credentialed and approved to treat patients, write prescriptions, and receive payment. Yet, oftentimes, more than 20 percent of the data in a payor's directory that lists credentialed providers is incorrect. The current process of confirming provider credentials, granting privileges, and enrolling physicians in payor networks is managed in many different systems, making it difficult to keep it current. The credentialing and enrollment processes are lengthy and cumbersome, rife with inconsistent data formats and workflows. A blockchain-enabled, decentralized, transactional layer that allows providers, health systems, and health plans to share updates and corrections of provider data files in real time will address these issues.

Healthcare blockchain legal concerns

Healthcare has a long history of addressing novel and complex models. This history, at a minimum, provides hope for resolution and perhaps some guidance on specific answers from a legal standpoint.

Governance

Many of the issues relating to governance will, to those familiar with healthcare arrangements, sound familiar. Recent trends toward edge computing, for example, are nothing new to HIT, where the rise of health information exchanges (HIEs) more than 10-years ago created dispersed networks, often without the need for a central repository. Governance of these networks took many forms, from common agreements executed by all parties to creation of a centralized entity that operates the HIE. Examples include the Nationwide Health Information Network (NHIN), a program established by the federal government that uses a common set of agreements among participants. Other governance approaches have been adopted in California, and in several, such as Manifest MedEx, a separate entity has been created that serves as a central control structure.

Before HIEs were popular, management services organizations, integrated physician associations, physician-hospital organizations, and numerous other types of arrangements were used to integrate diverse entities. Again, these arrangements often lacked a single, central entity to control governance, and decision-making was pushed to the edge of the entity, with a mixture of collaboration through committees and dispersed control — where each entity controlled its own, limited sphere.

Theoretically, blockchain should permit the epitome of decentralized governance. The structure itself has no central control, and the rules governing transactions are written directly into the code that sits atop the DLT. Stated starkly, by using the software resting on the distributed ledger, some would argue that the individual is agreeing that the software code is, itself, the law. In at least one case, however, the code for a smart contract on blockchain technology itself was exploited. In that case, cryptocurrency software had a bug that permitted a single user to divert approximately US$50 million, a significant portion of the total value in the currency.

Such diversion, however, complied with the network's rules and, apparently, the relevant law. In such a situation, does the network simply accept the outcome as an unfair windfall? Is the blockchain network permitted to split the chain — called a hard fork — and fix the software?

As is often the case with technology, the issue does not arise in the context

of a purely technological environment, or a purely human context, but rather in the rough patches where human and code interactions take place. If the community were comfortable allowing software to control all outcomes, then there would be no governance issue. If the network relied solely on traditional, "dumb" contracts, the legal system would address the question.

But our expectations of justice tend to bump up against the hard-and-fast realities of living in a world controlled by software. Ultimately, how these issues are resolved — whether by acceptance of all outcomes, invocation of traditional legal structures, or some hybrid — likely will evolve, much like the technology itself. In the interim, communities supporting a blockchain often will act after the fact to coordinate a response to these situations.

Other communities, seeing these risks, will create structures to discuss and coordinate. The hope that a sort of governance meta-software sitting on top of the distributed ledger could be drafted to resolve these issues, at this stage, seems overly optimistic, given the vagaries and incredible creativity of human beings in creating new problems.

Privacy and security

Privacy and security concerns are areas where one might argue that current laws make DLT difficult, if not impossible, to implement in certain circumstances. Certainly, the structure of laws and regulations like the administrative simplification rules of HIPAA assume a world that involves centralized control over records and did not envision blockchain technologies. Nonetheless, we believe that well-designed blockchain structures can avoid many of the pitfalls found in state and federal privacy and security laws.

For example, some have assumed that for electronic medical record software to set on top of a blockchain, every person in the blockchain network would need to execute a business associate agreement (BAA), allowing it to access such records. We believe that this fear misunderstands both the nature of a distributed ledger and the nature of HIPAA.

With regard to the ledger, each block within a blockchain will hold a relatively small amount of information. As such, space within the blockchain per se is cramped, and there would never be sufficient room to hold all of the records for every individual within a good-sized EHR. To get around this, the blockchain uses data pointers to non-blockchain storage where data is kept. The pointers are encrypted so that security is retained while not overstuffing the blocks. As such, to say that each computer in the network would need a BAA because each maintains protected health information is incorrect — only the location of the actual protected health information (PHI), pointed to by the blockchain, would maintain such PHI.

One might assume, then, that a single BAA with the entity maintaining the actual PHI would be required and sufficient. HIPAA, however, is not so straightforward. Rather, a BAA is only sufficient when a business associate, such as a vendor, is acting on behalf of a covered entity such as a healthcare provider, payor, or clearinghouse or on behalf of another business associate. In this case, the party holding the data may or may not be acting on behalf of such an entity. If one assumes that the nature of health records will remain fixed in amber, regardless of technological advances, and that EHRs will remain the same, except resting on top of a distributed ledger, then a business associate agreement between the relevant covered entity, such as a hospital, and the party holding the PHI would make sense.

For numerous reasons, however, we doubt that a blockchain-dependent EHR would necessarily be operated by a traditional healthcare provider. One of the great advantages of the technology is its ability to give individuals control over data. If an individual patient is able to access, distribute, and control his or her own data, why would a hospital need, or even want, to maintain the data for nonclinical purposes? Instead, when an individual visits a care provider, a smart contract could automatically transfer relevant information regarding the details of the visit to the relevant payor or could simply confirm the nature of the visit and automatically credit the provider's account with the relevant amount of money.

Patients are not covered entities under HIPAA. Because the patient's information is controlled and maintained solely by the patient and/or an entity acting on behalf of the patient, no covered entities are implicated and HIPAA becomes irrelevant. We believe

Estonia and Dubai are blockchain innovators

In the United States, there is great hope that blockchain can help us curb our addiction to inefficient, high-cost healthcare. But perhaps the most exciting opportunities for distributed ledger solutions exist in the global public health arena. Leading examples are Estonia and Dubai, which are implementing electronic medical records on blockchain to enable the use of secure and reliable health records, create efficiencies, and allow patients to take control over their own records. Further, public health problems related to medical record portability, medical identity, siloed disease registries, provider access, and immature health supply chains are more pronounced in some of the developing world. Many other locales have the potential to leapfrog legacy infrastructure and regulatory concerns that, in many ways, have become a limiting factor for progress in some markets.

a third error in the naysayers' concerns is the assumption that HIPAA and other laws will also remain encased in amber. While the law can be slow to respond, respond it eventually does. The speed with which Arizona and Vermont have implemented changes in law specific to blockchain suggest that, even if the technology outpaces legal structure for a time, fixes to such shortcomings can and will be implemented to promote the ends of those laws — increased security and privacy of personal information.

Likewise, clinical records could be controlled by both the provider and patient, and a smart contract could set rules for how data would be accessed and shared. The provider, its agent, or an unrelated third party could house the data.

Fraud and abuse

Another area that healthcare counsel must address regularly relates to improper payments and bills, including statutes such as federal and state anti-kickback statutes, physician self-referral statutes such as the Stark Law, and actions under federal and state False Claims Acts.

These regulatory constructs are not likely to be implicated by typical blockchain use cases per se. We eagerly anticipate the first article on whether participation in a blockchain provider community would be deemed a "referral" by each member of the network. Our short answer is no.

Nonetheless, there are two blockchain characteristics that may make these issues relevant.

First, the most famous (or infamous) use case for blockchain is in cryptocurrency and, specifically, Bitcoin. While such a use case has great value in proving the ability to create and maintain value in a currency without a centralized bank or intermediary, Bitcoin in particular has gained notoriety as the go-to currency of illicit trade. We see no reason why those wishing to illegally reward referrals would not similarly use such currency. This concern, however, is far from unique to healthcare.

Second, and of greater interest perhaps, is the potential for having blockchain technology control referrals and payments that limit the ability to game payors such as Medicare. The ability to automatically pay verified claims could limit greatly the opportunity to make false claims.

Likewise, when a provider determines that a patient needs a referral to a specialist or for a service, software setting on the blockchain could automatically generate the needed referral and control the ability of a physician or other provider to refer the individual to an entity with which the provider has a financial relationship. It also would prevent a provider from billing for services or viewing records of an individual not referred to the provider or approved by the patient. In other words, the rules contained in the Stark Law, anti-kickback statutes, and other statutes could be contained in a smart contract, reducing the likelihood of fraud and the ever-present risk of inadvertent violations of these complex statutes and regulations. Of course, many of the regulations addressed in this section are incredibly complex and open to interpretation, making them difficult to fit within a software program. Our, perhaps naïve, hope is that smart contracts and other technologies would encourage legislators and regulators to draft straightforward rules that are code ready such that they could be enforced automatically via software.

This transformative technology will take time

Blockchain has the potential to be a transformative technology in healthcare, and, as with any new technology platform, adoption will take time. But make no mistake, blockchain will affect healthcare in a very meaningful way, and industry, government, and consortia will do their best to accelerate its use. Our job is to make sure we understand the business models and then help clients break through the hype with answers, or at least help identify issues that need to be tackled and, if possible, provide some action plans. Staying on top of emerging legal issues, and figuring out what is new and not new, should help us do our part. **ACC**

ACC EXTRAS ON … Blockchain

ACC Docket

The Rise of Fintech: An Impact Analysis and Blockchain Case Study (April 2017). *www.accdocket.com/articles/the-rise-of-fintech.cfm*

Technology and the Power of the Easily Overlooked (April 2017). *www.acc.com/legalresources/resource.cfm?show=1455651*

The Future of Contracts: Automation, Blockchain, and Smart Contracts (Dec. 2016). *www.acc.com/legalresources/resource.cfm?show=1454306*

Program Material

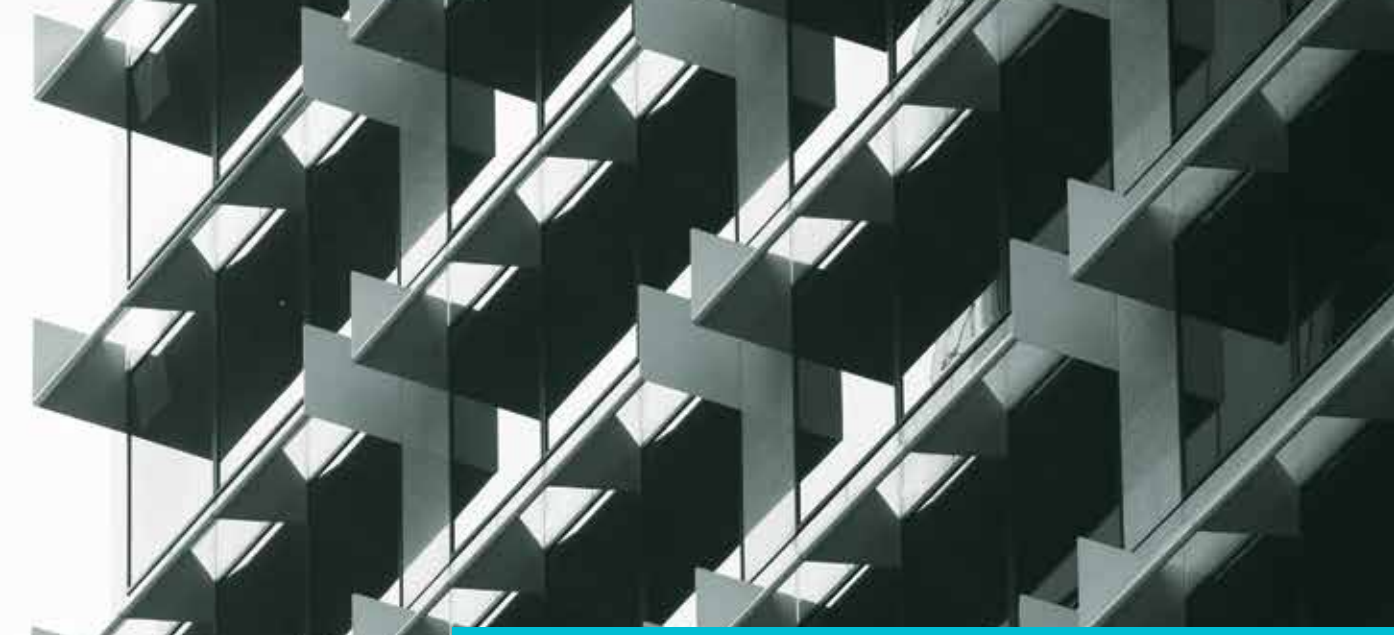
Smart Contracts (Oct. 2016). *www.acc.com/legalresources/resource.cfm?show=1445248*

Explanation, Regulation, And Litigation of Virtual Currencies (Oct. 2015). *www.acc.com/legalresources/resource.cfm?show=1414841*

Top Ten

Top Ten Tech Tips for Corporate Lawyers (May 2016). *www.acc.com/legalresources/publications/topten/top-10-tech-tips-for-corporate-lawyers.cfm*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.



What is Craftsmanship℠?

To be crafted is to meet exacting standards.

It's the human touch that combines art and science to create something unique.

We tend to think about craftsmanship in terms of physical things: fine wine, classic cars, custom furniture and iconic structures.

But what about the underwriting of insurance to craft protection for your unique and valuable things? And the service behind that coverage when you need it most – like claims and loss prevention?

For your business.

Your employees.

Your home.

The people you love.

Things that need a particular kind of protection and service.

The kind Chubb provides.

Not just coverage. Craftsmanship.℠

Not just insured.

Chubb. Insured.℠

chubb.com

CHUBB®