Health Law Daily Wrap Up, STRATEGIC PERSPECTIVES: Packing the health industry's data issues into the blockchain, (Feb. 16, 2018)

Health Law Daily Wrap Up

Click to open document in a browser

By Kayla R. Bryant, J.D.

Although the first block on the Bitcoin blockchain was mined 2009, the first description of a secured chain of blocks was released in 1991, and an idea patented in 1979 (Merkle trees) was added in 1992, digital currency and blockchain technology are still considered "emerging." Affected industries take time to adapt to innovation, and regulation grinds along slowly—especially for difficult-to-understand topics. Unfamiliar terminology, skepticism, speculative investing, novelty, and unanswered legal questions are all barriers to adoption, but blockchain and similar approaches can offer significant benefits for every field. This Strategic Perspective will explore the history of both Bitcoin and blockchain and how the buzzwords of immutability, decentralization, distribution, cryptocurrency, smart contracts, blocks, and hashes might relate to health care operations and policy. In particular, blockchain holds the promise of providing better data integrity for all parts of the health care industry. What this Strategic Perspective will not do, unfortunately, is uncover the identity of Satoshi Nakamoto.

Satoshi Who?

The creator (creators?) of Bitcoin, the beginning of blockchain technology, hid behind the name Satoshi Nakamoto. To this day, it remains unknown if Satoshi was a man, woman, or group. Satoshi authored a white paper introducing Bitcoin and describing the technology and currency approach in October 2008, claiming to solve the problem of "double spending" currency (basically, creating digital counterfeit money) without relying on a central banking organization. The timing for presenting a new method of handling money could not have been better—just one month after the failure of Lehman Brothers. The general unrest and distrust created by the Great Recession not only led to the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (P. L. 111-203), designed to increase transparency and stability in the financial realm, but creative solutions like blockchain that are much harder to regulate.

What does this have to do with health? While there is disagreement as to whether Bitcoin is a currency, a store of value, a bubble, or worthless, it is based on a technology—blockchain—that developers love to tweak. Bitcoin, the currency, will not be used to support networks operating in various industries—it is the blockchain technology that lends itself to potential adoption and disruption across perhaps every industry. Understanding the potential uses for the health industry requires an explanation of how blockchain works.

Trust No One, Verify Everything

The Bitcoin blockchain consists of a leger of transactions, with the data contained in "blocks," created every 10 minutes, and linked together by an unbreakable chain. The blocks are linked together using an algorithm that reads a block of data and creates what is known as a "hash," which is then used to create the next block. One small change in the data results in a wildly different hash.

The blockchain is considered "decentralized" because the data is not contained in one place, but rather replicated across many computer systems. The combination of decentralization plus the changing hashes result in a system of data that is incredibly difficult to attack, crack, and change. If one block in the middle of the chain is altered, the hash changes, as does every block thereafter. The connected system will detect and reject the change. For a slightly more in-depth description, see the article in Above the Law by Wolters Kluwer's Vice President of Legal Markets, Innovation, Dean Sonderegger.

Mining Bitcoin. Bitcoin miners work as auditors, verifying previous transactions and ensuring that Bitcoin owners are not spending the same coins multiple times. When a miner verifies one block worth of transactions,

totaling one megabyte worth of data, the miner receives the current reward of 12.5 Bitcoin. The original reward of 50 Bitcoin in 2009 continues to halve as additional blocks are mined. These rewards for miners will end once the full pool of Bitcoin is tapped at 21 million.

Blockchain Design and Mining Face a Myriad of Issues, with No Consensus on Solutions

Verifying the blockchain requires consensus among the system, but there are a number of issues with Bitcoin that developers cannot come to a consensus on. The lack of consensus has resulted in a number of "forks," where the blockchain splits at a certain block number. Blocks prior to the split will be identical between the two chains, while the remaining blocks on each chain comply with the established requirements. The chains' survival depends on the miners. If the majority of miners decide to follow the new (or stick with the old) parameters, only one chain will remain. However, if enough of a minority decide to stay with the old rules (or proceed with the new) opposite the majority, the second chain will survive.

Mining is energy intensive. For Bitcoin, miners verify transactions by applying a brute force approach to guess a number that is equal to or less than a 64-digit hash in a system known as "proof of work." Proof of work requires an intense amount of computing power, in turn requiring expensive equipment and a large amount of energy. It is impossible to truly pin down how much energy is being used, and different sources disagree. Still, mining profitability depends on using cheap energy sources. Many large scale miners (a concept that some argue goes against Bitcoin's entire goal of decentralization) are located in China to take advantage of cheap energy. Companies like Bitmain Technologies are reportedly looking into moving to Quebec in light of expectations that China will continue to crack down on cryptocurrency by limiting electricity to miners.

Proof of work may not always be the default, as alternative options are making themselves known. One popular option is proof of stake, where the participants validating the next block are given weight to their votes by how much of a particular currency they hold. As noted in the Ethereum GitHub repository, there are various ways to implement proof of stake, but there are several notable characteristics inherent to the design. Proof of stake is less energy intensive than proof of work and, therefore, the existing pool of coins overall does not need to be as large as the pool for proof of work coins to keep stakers involved in maintaining the network. The technology also lends itself to increased security by reducing the risks of centralization and attacks.

Yet, not everyone holds such an opinion, with some finding proof of stake's issues just as bad as proof of work's. The problem of determining a proper method of securing a network and rewarding those who secure said network does not escape those who are attempting to solve real-world issues, including health industry issues, with this technology. In an interview with Wolters Kluwer, Roger Cohen, partner at Goodwin Procter LLP and an expert in health information technology (health IT), noted that blockchain creators must determine a "substitute incentive" for contributing computing resources. Bitcoin miners receive Bitcoin as rewards, but developers of new blockchain solutions will be creating their own networks, powered by a new coin. If that coin is not able to be sold for a significant profit, there will be no incentive for committing computing power to secure the network.

Transactions are expensive. In addition to mining rewards, miners get paid from transaction fees. During times of high volume, miners will prioritize transactions offering higher fees. This is where the mandate of 10-minute, one-megabyte blocks becomes extremely important—there is a limited number of transactions that can be packed into one block. Transactions sent with no or low fees will be pushed down the list. On October 1, 2017, the average transaction fee was $2.53. Gradual growth led to a spike of $19.20 on November 12, then the price dropped before spiking to $27.20 on December 8 and then to an all-time high of $55.16 on December 22. Fees have fallen since, in line with the drastic fall in Bitcoin's value, but several dollars per transaction is still a barrier to adoption.

Exchanges are mostly centralized, unregulated, and unable to keep up with demand. It's easy (but not necessarily simple) to get Bitcoin and other cryptocurrencies without mining by registering with an exchange. In the United States, fiat currency is usually exchanged for Bitcoin, Litecoin, or Ether using Coinbase/GDAX or Gemini—US-based exchanges that cooperate with government regulation (such as it is). From there, a US customer can register with a large number of exchanges across the world and use those to send, receive, and trade cryptocurrencies. Other exchanges are located in the US, but do not offer U.S. dollar trading pairs.

Although Bitcoin was created as a decentralized currency to take the power out of the hands of an entity, exchanges are inherently centralized places to facilitate trades. The infamous Mt. Gox exchange hack highlighted the very danger of such a system. Launched in 2010, the Tokyo-based exchange handled a large volume of transactions as Bitcoin adoption increased. Between 2011 and 2014, hackers stole at least 650,000 Bitcoin from the exchange, which halted trading and filed for bankruptcy in February 2014. More recently, $500 million of a cryptocurrency was reportedly stolen from Coincheck, another Japanese exchange. More eyes are turning to decentralized exchanges, which do not hold customer funds and facilitate direct transactions. Still, decentralized exchanges are far from a perfect solution—they are less user friendly, and the exchange EtherDelta was replaced with a fake site that stole customers' money in December.

The ease of sending cryptocurrencies to various exchanges across the globe makes it difficult to regulate, and customers often find themselves without recourse when facing issues of missing money. Most exchanges have no way of contacting customer support outside of submitting tickets—there are no phone numbers or e-mail addresses offered. Exchanges are reportedly bogged down from increased demand, and several recently halted new customer registration, citing up to 250,000 sign-ups per day. Many users take to social media to complain about lost money, failure to respond to support tickets, and frozen accounts.

Not All Coins Are Legitimate, and the Government Hasn't Decided How to Handle It

The applications of blockchain and other related technologies now extend far beyond just Bitcoin. Other developers have decided to start their own chains from scratch and create alternative coins (altcoins), fork off of altcoins, or copy existing altcoin technology and tweak it. Currently, CoinMarketCap lists 1511 cryptocurrencies—but not all are successful or traded. Although some coins are legitimately needed to facilitate the technology, consumers who are uninterested in using that technology can trade coins as speculative investments.

Senate hearing. The Securities and Exchange Commission (SEC) takes investing seriously, and the agency is extremely concerned about protecting uninformed investors from scams. Despite significant scrutiny of the cryptocurrency markets and global crackdowns, the Senate Committee on Banking, Housing & Urban Affairs' February 6, 2018, hearing on virtual currencies saw favorable testimony from SEC Chairman Jay Clayton and Commodity Futures Trading Commission (CFTC) Chairman Christopher Giancarlo.

Clayton noted that while the SEC regulates securities transactions without direct oversight of currencies and commodities, and while many U.S. exchanges are regulated largely by states as money-transmission services, simply calling something a "currency" does not preclude it from being considered a security and therefore subject to compliance with securities laws. Although the SEC continues to monitor the sphere and has taken action on offerings it considered clearly fraudulent, Clayton noted that the warnings in his testimony "are not an effort to undermine the fostering of innovation through our capital markets." Giancarlo is quite supportive of blockchain technology, even emphasizing the benefits to market regulators. While emphasizing the necessity of "sound policy" and a properly regulatory response, he supported the innovation of blockchain technology and its connection to the American markets.

Blockchain Technology and Health Care

In recent years, most people have probably received a notice that their personal information may have been compromised in a cybersecurity incident of some sort. Personal health information is particularly vulnerable, and the attacks continue despite increased scrutiny from the government and intensified security efforts by the industry (see *Top 5 cybersecurity developments for 2017*, December 21, 2017). Compliance with security regulation can result in stifled innovation as companies struggle to properly secure large amounts of data. Billing becomes increasingly complicated as the International Classification of Diseases (ICD) system evolves. Electronic health record (EHR) systems have interoperability issues. Blockchain developers strive to create a new solution for all of these problems—and more. Even the Office of the National Coordinator for Health Information Technology (ONC) has gotten involved and, in 2016, solicited white papers on the topic of managing EHRs using blockchain technology.

Data integrity. R. Douglas Vaughn, a partner at Deutsch Kerrigan LLP and chair of the Medical Defense and Health Law Committee of the International Association of Defense Counsel (IADC), told Wolters Kluwer that blockchain's promise for the health care industry lies in enhancing data integrity. He said, "the security aspect of blockchain is in making it very difficult to change the identity of the data exchanged. As blockchains are one part of a larger data infrastructure solution, use of blockchain can allow for the elimination of some administrative processes, thereby allowing larger volumes of data to be processed more expediently."

Vaughn added, "An Electronic Medical Chart using blockchain cannot easily be tampered with after an adverse event. When sitting across the table from an adversary in litigation, all parties should be confident in the integrity of the chart entries." He also noted that if "blockchain is used between a health provider, a patient and an insurance company, blockchain can increase efficiencies and reduce delays in the payment for services."

Robert J. Zafft, an attorney (of counsel) with Greensfelder, Hemker & Gale, P.C., told Wolters Kluwer, "to further implementation of electronic medical records, the formatting of blockchain healthcare data will have to be systematized. Fields within each record will have to be encrypted in a way that third parties can be given need-to-know access to information."

Data storage and analysis. Cohen listed several exciting potential uses of blockchain technology, first and foremost access to and control of health information. He noted that although patients legally have the right to copies of their own health data, collecting such data from all sources and keeping it up to date is a difficult task, and blockchain is in a position to engineer solutions to the problem.

Founded in 2015, BurstIQ strives to find a solution for integrating data, combining and sharing information in a manner compliant with the Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191), and improving patient understanding of data. BurstIQ's white paper identifies the convergence of health data sources as a health singularity, and offers a platform to handle it. Although a traditional blockchain is open and transparent and therefore inappropriate for protected health information (PHI), BurstIQ uses cryptography to keep data in motion and separated to maintain security. To solve scalability issues, the platform's BurstChain™ blockchain technology replaces proof-of-work with a "voting paradigm." The LifeGraph™ operates as a platform for patients to manage all of their health data from all providers in one place, and Consent Contracts allow patients to set rules for access to their information.

BurstIQ also offers protocols for other developers that wish to create third-party applications on the platform. The company suggests that other solutions may include analysis of risks of developing diseases, social pairing of patients with similar conditions, or connection with clinical trials or precision medicine approaches.

Vaughn noted that while "the current state of blockchain technology accessible in the market is best understood by IT professionals and engineers … the future of blockchain lies in the promise of development of apps to be available for use by consumers."

Interoperability. Cohen also pointed out that blockchain has the potential to facilitate compliance with the 21st Century Cures Act's (Cures Act) (P.L. 114-255) provisions promoting EHR interoperability (see *Building trust one network at a time*, January 8, 2018). His ideas about the importance of blockchain solutions in achieving interoperability were echoed by Randy Peak of Perkins Coie LLP, who offered the example of hospital acquisition as an opportunity for blockchain to shine. Peak noted that in such a situation, integrating IT systems to allow patient data to be accessed across an entire hospital is system is "critical and potentially life impacting to the extent dad is needed for urgent patient treatment," and that blockchain could speed up the integration process.

Patientory attempts to be one of those solutions, and declares itself to be an EHR network that bridges existing systems. Providers and patients will use PTOY, the platform's token, to secure PHI and rent computing power. Patients can also purchase extra storage in addition to the allotted space using PTOY. Similar to BurstIQ, Patientory uses the blockchain to separate and encrypt data for storage. The technology uses a multi-tiered framework, with a middle layer that allows data to connect with sources off the blockchain. Patientory's approach aims to solve interoperability issues. Tools like Patientory may help providers avoid becoming a target of the

HHS Inspector General's (IG) newly acquired authority under the Cures Act to investigate and penalize claims of information blocking (see *Cures Act gave agencies tools to unblock health IT*, November 2, 2017).

Tracking. Blockchain can do more than track and store patient data. Medileger hopes to establish a network to track the pharmaceutical supply chain. By doing so, Medileger believes that this will provide regulators with an easier way to audit and investigate reported issues, especially since all information will be verifiable against a secure ledger. Verifying the drug supply chain is of utmost importance to the FDA, as the agency phases in compliance requirements under the Drug Supply Chain Security Act (DSCSA), implemented as part of the Drug Quality and Security Act (P.L. 113-54), through 2023. The requirements apply to manufacturers, repackagers, wholesale distributors, and third-party logistics providers—a large number of potential customers for blockchain solutions providers.

"Blockchain should make supply chains more secure while also promoting wellness," Zafft said. "For example, blockchain should help ensure that a hospital's shipment of artificial knees came from Stryker and not a knock-off plant in China. As blockchain connects with the Internet of things, wellness programs will become more effective. So, your gym treadmill will tell your Fitbit that you walked three miles, which will tell your health plan to rebate part of your premium or to issue you wellness points for plan prizes."

Vaughn said, "What blockchain brings to the market not previously seen is uniquely represented critical data, meaning once the data is transmitted over a blockchain—think of a prescription for a patient to receive a specific drug or a payment of a specific amount—if anyone attempts to change that data the falsity is easily demonstrated. Likewise, the time stamp of the transmission is affixed and cannot be surreptitiously changed."

Don't Forget About Human Error

Blockchain will not solve all issues regarding the integrity of health data—humans are still the weakest link. Vaughn said, "it must be remembered that the use of blockchain does not guarantee your data can not be hacked or stolen. The term used by those in the industry is 'perimeter security' meaning passwords and server protections. Data on a computer or smart phone can still be stolen if care is not taken to secure passwords. The security of blockchain is the resistance to tampering with the data itself—the unique representation of the data itself—is the current promise blockchain offers, and that is quite a promise in itself."

Conclusion

Although blockchain solutions hold promise, many questions remain. No products have yet achieved broad adoption. The technology is still being developed, and regulations will need to be shaped around the technology. Blockchain solutions must do more than promise to be compliant with HIPAA and other regulations—it must prove itself to be so. The government must decide how to handle the speculative nature of investing in the cryptocurrencies that power the technology, and how to tax the profits. Then the industry will be forced to decide which products have merit, and those will be forced to compete. It remains to be seen whether these products will offer solutions to interoperability, or result in additional fractures in EHRs. Further, human error can still undermine the security promised by blockchain.

Still, the health care industry is in a good position to rapidly adopt blockchain technology in some way. Zafft noted, "By its nature, blockchain requires collective action. The high market concentration of health care payors will speed adoption, particularly if some economies pass through to employers and consumers."

Fortunately for the industry, the U.S. government has so far encouraged the development and implementation of blockchain products, and such support will go a long way. Over the next few years, watch for continued development in this space with implications for the health care industry, and far beyond.

Attorneys: Roger Cohen (Goodwin Procter LLP). Randy Peak (Perkins Coie LLP). R. Douglas Vaughn (Deutsch Kerrigan LLP). Robert J. Zafft (Greensfelder, Hemker & Gale, PC).

Companies: BurstIQ; Patientory; Medileger; International Association of Defense Counsel

MainStory: StrategicPerspectives FDCActNews AuditNews ConfidentialityNews CyberPrivacyFeed DrugBiologicNews EHRNews GenericDrugNews HITNews HIPAANews