

Corporate Compliance Insights

THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

September 2017

The Regulatory Tortoise and The Technology Hare

Balancing Innovation and Compliance

By David Katz and
Jim O'Hare

Blockchain as a disruptive and revolutionary technology has pierced executives' consciousness and can no longer be dismissed as a mere fad. The C-Suite has taken notice and businesses will need the advice of seasoned and informed practitioners to establish compliant applications utilizing this technology. Inevitably, fast-moving technological developments will cause some to take risks to be first to market with the hopes of a large reward. Analyzing the risks and consideration of existing laws in conjunction with the development of use cases and business plans could pay off big time for the smart and prudent company.

Blockchain has been trumpeted as a major step forward in refining the internet and related commercial and governmental commerce. Early on, *The Economist* declared blockchain to be "the great chain of being sure about things." Other tech visionaries have predicted that blockchain infrastructures have the power to reduce the costs of bargaining, policing and enforcing social and commercial agreements while rewarding integrity, security and collaboration.

In any event, blockchain is fully recognized as having value beyond its role as the technology infrastructure facilitating Bitcoin transactions.



No doubt you've now heard about blockchain – at least the word. The hype cycle has been in full swing since late 2015, so fairly soon, someone from the C-Suite will be asking you about compliant ways to operate that blockchain pilot application going live next month.

MIT Sloan Professor Christian Catalini describes blockchain at a high level as a technology that allows a network of computers to agree at regular intervals on the true state of a distributed ledger. Ledgers can contain different types of shared data, such as transaction records, attributes of transactions, credentials or other pieces of information. The ledger is then secured through a mix of cryptography and game theory and does not require trusted nodes like traditional networks.

In reality, blockchain is a suite of existing, well-understood technologies that in combination have the potential to disrupt how countless industries track, verify and share transactional information.

First and foremost, blockchain utilizes a "ledger" and is alternatively referred to as "distributed ledger technology," just like a green paper of rows and columns – a long-standing approach for tracking ownership and transactional information. The techniques securing each block of transactional information utilizes recognized cryptographic processes for public and private key security, ensuring transactional integrity. Transactions are

recorded chronologically, forming an immutable chain.

The authenticity of transactions is then verified across private or public networks of computers on a peer-to-peer basis. This eliminates the need for a central intermediary or clearinghouse (think bank or health record) and the time and cost resulting from a central clearing function.

The public domain is full of descriptive information on the various blockchain structures with varying levels of technical depth. Much in the way that backbone systems for e-mail and internet access are not scrutinized based on their utility-like status, the internal clients relying on your compliance advice are more likely to consult you on the application of the technology and any legal potholes to be avoided.

The tired refrain that "the law just can't keep up with technology" is meaningless when it comes to setting a compliance plan, and some recent examples are illustrative. A strong foundation in current regulatory practices is critical for advising on matters of compliance.

Continued

The Securities and Exchange Commission (SEC) recently weighed in on the “DAO” fiasco occurring in the summer of 2016 – the fiasco was long over and the SEC did not recommend an enforcement action, but the agency’s less-than-timely response did provide guidance. This article isn’t the place for an exposition on the shortcomings of the DAO and the “hack,” which imperiled millions of dollars in value of cryptocurrency, but it is instructive to contemplate that the SEC applied its long-standing 1946 guidance of what constitutes a security for purposes of invoking the coverage of the federal securities laws.

The traditional four-part “Howey” test applied by the SEC doesn’t include an escape route for transformative technology, so a slow-to-evolve regulatory template trumps disruptive technology.

Recently IBM and Sony Global Education announced the development of a new blockchain-based student education records platform to be launched in 2018. With the solution, student records, including granular performance information from SIS systems, will be consolidated across several schools during a student’s career, creating a reference point for learning history and digital academic transcripts with more certainty. Postsecondary certifications and nontraditional educational achievements would also be recorded to provide an in-depth view of student accomplishment. A secure, verified, immutable digital record is of value to students, academic institutions and employers alike.

Digital transcripts and trusted verification of global achievements sounds like an educational Shangri La. Unfortunately, the tremendous technological advantages just don’t override the need to run the operation of the platform through the federal and state requirements covering student information and privacy. The Family Education Rights and Privacy Act (FERPA) protects the privacy of student education records. The law is applicable to all schools that received funds under an applicable program of the U.S. Department of Education. Among the protections FERPA provides to students is the ability for parents to have the right to inspect and review student records maintained by the school. Moreover, parents have the right to correct records they believe to be inaccurate or

misleading. The dual concepts of the right of inspection and the right of correction require considered analysis in the context of the blockchain.

“In reality, blockchain is a suite of existing, well-understood technologies that in combination have the potential to disrupt how countless industries track, verify and share transactional information.”

For blockchain application developers servicing education institutions subject to FERPA, understanding the applicable law and ensuring the technology operates in accordance with the law will be crucial to remaining viable in their respective markets.

Consider as an additional example California’s Student Online Person Information Protection Act. This law requires operators to delete student information if requested by the school or district. Operations can be educational websites, online services, online applications or mobile applications. For technology creating a fixed and immutable ledger, deletion can be a difficult concept to reconcile.

BlockRX is a blockchain-based solution addressing the challenges of the global drug supply chain and data management for drug development and logistics. In part, the platform is intended to facilitate compliance with the U.S. Drug Supply Chain Security Act (DSCSA) which requires full compliance by 2024. The DSCSA requires pharma companies to implement a national track-and-trace system by which they must affix product identifiers to each package of product that is introduced into the supply chain. This regulation is designed to create an “interoperable system to identify and trace certain prescription drugs as they are distributed in the U.S.” Multinational regulatory compliance (such as the EU Falsified Medicines Directive) will also need to be covered due to the global reach of the pharmaceutical industry.

The success of BlockRX and other similar supply chain blockchain applications involving regulated goods will depend partly on the creation of auditable, traceable and immutable records and effective data ex-

change. A failure to comply with regulatory guidelines – even those hopelessly behind the innovation curve – will undoubtedly impair even the most elegant blockchain implementations.

Weighing innovation and technological advancement against compliance risks is a timeless consideration for the C-Suite. In an evolving market, the ability to foresee compliance risks and adjust accordingly to avoid surprises could result in significant rewards. For companies considering adoption of this technology, careful planning and consultation with experts should be an early part of the business plan.



David F. Katz is a partner in Nelson Mullins Riley & Scarborough’s Atlanta office where he leads the Privacy and Information Security Practice Group. He

provides legal advice on matters related to the privacy laws affecting multiple sectors of the economy including retail, financial services, education, health care and technology. He counsels corporate clients on the development, management and oversight of privacy and compliance programs, vendor management programs and assists them in developing policies and procedures, education strategies, implementation of auditing and monitoring controls, reviews of disciplinary and enforcement activities, and risk assessments. He may be reached at (404) 322-6122 or by email at david.katz@nelsonmullins.com.



Jim O’Hare is a partner in the Boston office of Nelson Mullins’ and represents technology-based companies, their boards of directors, and investors

in the areas of mergers & acquisitions, strategic technology implementations, dispute resolution, and public and private financings. He may be reached at (617) 217-4712 or by email at jim.ohare@nelsonmullins.com at david.katz@nelsonmullins.com.