BlockTribune
All the News that's fit to Mine

Cross-Industry Blockchain and Bitcoin Challenges

James P. O'Hare
Nelson Mullins Riley & Scarborough

What do cross-border remittances, the pharmaceutical supply chain, land titles, electronic health records and digital content have in common? Each are among the hundreds of applications that are poised to capitalize on the massive efficiencies available using blockchain platforms. Initially viewed as exclusively linked to the Bitcoin cryptocurrency, over the last 24 months the blockchain hype cycle has been in full gear for everything from the clearing of public stock transactions to the verifying vintage year and winery location for fine wines.

Despite the variety of potential applications, there are some common cross-industry challenges.

Public or Permissioned Blockchains? Blockchain and their associated distributed ledgers can operate on the basis of a public or private network. Private (or permissioned) networks allow participants in the network to restrict those who can both enter into transactions and participate in the consensus mechanism of blockchain transactions. This "private" approach to controlling participation is similar to the adoption progression for TCP/IP networks that progressed from e-mail to more robust applications running on World Wide Web in the 1990s. Private and Public Cloud adoptions followed a similar pattern. The challenge of uncontrolled

participation in blockchain networks may be a bridge too far for first time entrants. The infrastructure is transformational, but baby steps are likely to be needed before a flat out sprint.

Regulated Industries. A number of consumer goods companies transact commerce using bitcoin – Overstock.com and Dell Technologies – to name a couple of well-known names. In buy-sell transactions, the standard rules related to currency transactions and consumer rights are applicable. When blockchain applications are used in regulated industries – financial services, healthcare, content creation and ownership – the legal overlay cannot be ignored. Your novel application of blockchain ledgers and transaction veracity may be world-changing, but if you ignore the existing regulatory imperatives, your sea-change transformation may be short-lived.

Not Just Cybersecurity. Blockchains are perceived as more secure that traditional databases and better platforms for transactions susceptible to manipulation and fraud. Despite that perception, traditional notions of information security and privacy continue to apply. As computer hardware vendors have pointed out, the promise of reliability, scalability, security and privacy will need the support of continuing hardware advancements that deliver large scale performance.

Although not cybersecurity, the "promise" of Smart Contracts took a major hit in June 2016 when The DAO – a Smart Contract governed on-line "investment club" structured exclusively on the basis of Smart Contracts was compromised. The operation and governance of The DAO enterprise was based exclusively on the computer code – "Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code." No middlemen needed and no counter-party risk possible due to the immutable nature of the cryptographically secure blockchain ledger.

Over $150 million in value was committed to The DAO during the funding process. While the funding window was still open, questions arose regarding vulnerabilities involving the platform. The specifics of the "hack" and fork "fix" are widely available on the Internet, but the critical issue for The DAO participants and the self-proclaimed "Attacker" is whether the computer code really is the last word when it comes to sorting this out. The Attacker's position was that manipulation of The DAO code was a code "feature" available to The DAO participants. Any legal concepts related to intent of the participants in entering into the enterprise, deception by the Attacker or theft do not apply. Access to the code (in this case dropping crypto currency into a sub-DAO) was permitted and any application of the code is legitimate.

The more complex the transaction, the greater the likelihood that a gap will exist in the application of the business rules creating an "unintended consequence" risk. Modern contract law helps fill in the blanks where contractual terms do not cover a contractual dispute. Whether parties can agree to abide by these unintended consequences and forgo intervention by a court should be an issue to be addressed.

The "blank filling" exercise applied by a court or any involvement by any central authority is antithetical to the administrative efficiency and immutable nature of a blockchain. The application of contract, tort and criminal law principles to the current controversy will by necessity involve the institutions of authority that The DAO was created to avoid. It is doubtful that this type of regulatory intervention will accelerate blockchain adoption.

In the end, some lessons are best learned the hard way (over $50 million worth) and the resulting wakeup call should drive crisper logic and transaction structures more appropriate for initial blockchain implementations.

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. Mr. O'Hare has served clients as a lawyer, a public company general counsel and senior executive, and an investment banker.*

4812-6024-4039 v.2