Proskauer

Blockchain and Quantum Computing

Blockchain and the Law Blog on **December 21, 2017**

2018 promises great inroads in the realm of "quantum computing." While conventional computers use binary data or bits (i.e., 0s and 1s) to store and process information (a bit can either store a 0 or 1), a quantum computer operates based on the laws of quantum mechanics and uses quantum bits or "qubits," which can be in a "superposition" state of zero and one at the same time (e.g., a qubit can store a 0, 1, or a summation of both 0 and 1). Ultimately, it is expected that quantum computers will be able to solve complex computations exponentially faster – as much as 100 million times faster — than classic computers.

While currently not ready for general commercial applications, quantum computers could someday allow scientists and others to solve very complex problems in chemistry, applied mathematics, biology and engineering, and also push huge advances in areas such as artificial intelligence, machine learning, large database searching and big data processing.

How could quantum computing impact blockchains?

Current encryption, cryptography and private/public key systems are premised on the assumption that there are limits to the resources and processing power that can be applied to break such systems. Quantum computers may be powerful enough (perhaps) to break the systems currently in use that protect secure online communications and encrypted data. If the resources of quantum computers are ever generally available or otherwise fall into the "wrong" hands, encryption and cryptography, as we know it today, could be in jeopardy. This has led the National Institute of Standards and Technology to begin the process to standardize so-called post-quantum cryptography. Clearly, basic password protection would appear quaint and merely "a nice try" in light of the resources quantum computing could bring to a "brute force" hack.

Blockchain technology relies on public key cryptography to maintain the security of the ledger. Moreover, bitcoin relies on the work of "miners" to use computing power resources to solve certain complex mathematical problems to verify transactions, a task that could be upended by entities with quantum computing platforms. Again, quantum computing presents a real threat to existing blockchain algorithms. As a result, developers are working on quantum-resistant ledgers.

While widespread use of quantum computing in the commercial context may be a bit far off, significant resources are being applied in that area. When quantum computing becomes readily available, blockchain will have to adapt to this new technological capability. The process is already underway.

View Original

Related Professionals

- **Jeffrey D. Neuburger**