Artificial Intelligence and blockchains are vulnerable to cyberattacks

April 6, 2018

Author

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Technologies based on blockchains and AI imply a considerable change for our society. Being that the security of data exchanged is vital, companies must begin adopting a long-term approach right now.

Many businesses develop services based on blockchains, in particular in the financial services sector. Cryptocurrencies, one example of blockchain use, transform the way in which some monetary transactions are made, far from the oversight of financial institutions and governments.

With regard to AI, businesses sometimes choose technological platforms involving data sharing in order to accelerate the development of their AI tool.

Quantum revolution’s impact on cybersecurity

In 2016, IBM made a computer for testing several quantum algorithms, available to researchers.[1] Quantum computers work in a radically different way from traditional computers. Some ten years in the future, they will be able to perform quick calculations that exceed the capacity of today’s most powerful computers. Indeed, quantum computers use the quantum properties of matter, in particular the superposition of states, to simultaneously process linked data sets.

Shor’s algorithm uses the quantum properties of matter and can be used by quantum computers.

Shor’s algorithm enables a quantum computer to factor a whole number very quickly, much more so than any traditional computer. This mathematical operation is the key element to decipher information that has been encrypted by several commonplace computing methods. The technology, which physicists have long been studying, now constitutes a major risk for the security of encrypted data. Data meant to remain safe and confidential are thus vulnerable to being misappropriated for unauthorized uses.

Are blockchain encrypting methods sufficiently secure?

There are several encrypting methods available today, with several of them needing to be strengthened to preserve data security. And these are but a few examples of vulnerability to quantum computers.

SHA-2 and SHA-3 methods

The US National Institute of Standards and Technology (NIST) has issued recommendations for the security of various encrypting methods.[2] The SHA-2 and SHA-3 methods, namely the algorithms that ensure the integrity of blockchains by producing a “hash” of previous blocks, need to be strengthened to maintain current security levels.

Signature methods used by Bitcoin and other cryptocurrencies

Elliptic curve cryptography is a set of cryptography techniques using one or more properties of mathematical functions that describe elliptic curves in order to encrypt data.

According to the NIST, elliptic curve cryptography will become ineffective. Worryingly, we are talking about the method used for the signature of cryptocurrencies, including the famous Bitcoin. Recent studies indicate that this method is highly vulnerable to attack by quantum computers, which, in a few years’ time, could crack these codes in under 10 minutes.[3]

RSA-type cryptographic algorithms

RSA-type cryptographic algorithms,[4] which are widely used to forward data over the Internet, are particularly vulnerable to quantum computers. This could have an impact in particular when large quantities of data need to be exchanged among several computers, for example to feed AI systems.

More secure cryptographic algorithms

The NIST had indicated some approaches that are more secure. An algorithm developed by Robert McEliece, mathematician and professor at Caltech, seems to be able to resist such attacks[5] for now. For the longer term, we can hope that quantum technology itself makes it possible to generate secure keys.

Legal and business implications of data protection

Companies are required by law to protect the personal and confidential data entrusted to them by their customers. They must therefore take suitable measures to protect this valuable data.

Therefore, companies must choose an AI or blockchain technology as soon as possible, while taking into account the fact that, once adopted, the technology will be used for several years and may need to survive the arrival of quantum computers.

What is more, we will need to fix the security flaws of technologies that are not under the control of government authorities or of a single company. Unlike the solution with more traditional technologies, we cannot install a simple update on a single server. In some cases, it will be necessary to reconsider the very structure of a decentralized technology such as blockchain.

Choosing an evolving technology

The key will therefore be to choose a technology enabling businesses to meet their security obligations in a post-quantum world, or at least to choose an architecture that will enable such encrypting algorithms to be updated in a timely manner. It will therefore be necessary to establish a dialogue among computer scientists, mathematicians, physicists and…lawyers!

Lavery created the Lavery Legal Lab on Artificial Intelligence (L3AI) to analyze and monitor recent and anticipated developments in artificial intelligence from a legal perspective. Our Lab is interested in all projects pertaining to artificial intelligence (AI) and their legal specifics, particularly the various branches and applications of artificial intelligence which will rapidly be appearing in all companies and industries.

---

1. Press Release: *IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation*: https://www-03.ibm.com/press/us/en/pressrelease/49661.wss; see also: Linke, Norbert M., et al. "Experimental comparison of two quantum computing architectures." *Proceedings of the National Academy of Sciences* (2017): 201618020.
2. Chen, Lily, et al. *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.
3. Aggarwal, Divesh, et al. "Quantum attacks on Bitcoin, and how to protect against them." *arXiv preprint arXiv:1710.10377*(2017).
4. This acronym comes from Rivest, Shamir, and Adleman, the three developers of this kind of encryption.
5. Supra, note 2; see also Dinh, Hang, Cristopher Moore, and Alexander Russell. "McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks." *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2011.