Blockchain Hype: Irrational Exuberance Redux

Stuart Madnick

Working Paper CISL# 2019-09

March 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Blockchain Hype: Irrational Exuberance Redux

MIT Sloan Professor Stuart Madnick is not necessarily predicting a repeat of the dot-com bubble. He is concerned, however, that the proliferation of blockchain hype obscures some serious weaknesses in the technology and makes entrepreneurs overeager to adopt it.

Madnick is only half joking when he says that the easiest ways to make money with a startup in the current climate is to put "blockchain" in the company name. *Bloomberg.com* reported on a version of this phenomenon in October 2017, noting that shares of the British investment enterprise On-line Plc surged 394% in direct response to the company's new name "On-line Blockchain Plc."

A wide range of financial losses

Madnick cautions business executives, investors, the financial press, and his students not to be blinded by the sparkle surrounding the technology. At latest count, Madnick and his researcher colleagues have gathered 72 cases of blockchain security breaches that occurred between 2011 and 2018.

"Some attacks resulted in relatively small losses in the range of $12,000, but others have cost companies as much as $600 million," says Madnick. "In total, the publicly reported losses by cyberattack against blockchain systems during the last eight years exceeds $1 billion. Our research reveals that such attacks happen much more often than is commonly appreciated. You can lose a lot of money, IP, network trust, and market confidence in a very short period of time."

As many vulnerabilities as participants

Madnick and his team are currently developing a taxonomy of vulnerabilities, and he notes that certain analogies come to mind when he seeks to promote security consciousness among blockchain advocates and potential developers. "Splitting the atom is not easy and banks are made of atoms, but banks and bank vaults can get robbed. Blockchains can be hacked without actually having to 'crack the chain.' Blockchain may be tamper resistant, but it certainly isn't tamperproof.".

One of the earliest cases from Madnick's research involved a Bitcoin owner who printed his blockchain key on his t-shirt. Someone took a photo of him and used it to drain his account. "It never occurred to him that someone would do that—a classic case of leaving the key under the mat for the burglar to find," says Madnick. "Much more common and subtle are flaws in the writing of algorithms, such as the Ethereum hack where an intruder discovered the programming mistake and used it to move the money into his account."

Blockchain may be its own worse enemy

"The things that make blockchain great also make it vulnerable—especially when it comes to security. For example, blockchain's distributed control is an important feature meaning that there is no central authority. But it also means that there is no central 'On' or 'Off' switch. Thus, an attack is almost impossible to turn off even after you detect it – and this has happened." One of the key notions Madnick and his team hope to dispel is that blockchain technology involves no elements of human control. And where humans are present, so is the possibility of human error. "That's why I urge decision-makers to reflect carefully on the risks involved before jumping on the blockchain bandwagon," says Madnick.