Blockchain Is Unbreakable? Think Again

Stuart Madnick

Working Paper CISL# 2019-15

June 2019

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

Blockchain Is Unbreakable? Think Again

Stuart Madnick
MIT Sloan School of Management

Blockchain technology has tremendous advantages that many organizations are eagerly looking to exploit in sectors as diverse as shipping, real estate and diamonds. The advantages are so compelling and hyped that I sometimes say the easiest way to make money with a startup is to put "blockchain" in the company name, such as when the shares of the British investment enterprise On-line Plc surged 394% in direct response to the company's new name "On-line Blockchain PLC."

In addition to the touted advantages of transparency, distributed control and anonymity, blockchain systems are also considered by many as a great way to improve security, since they are thought to be "unbreakable."

Not so fast. We've documented a wide range of blockchain security breaches. In a forthcoming MIT study, we analyzed 72 cases of publicly reported blockchain system security breaches that occurred between 2011 and 2018. Since many cyberattacks are not publicly reported, there may have been more.

Some attacks resulted in relatively small losses in the range of $12,000, but others have cost companies as much as $600 million. In total, the publicly reported losses by cyberattacks against blockchain systems during the past eight years exceed $1 billion.

In our research, we have developed a taxonomy of blockchain vulnerabilities. A key to understanding these vulnerabilities is to understand the difference between "blockchain the concept" and "blockchain the system." A simple analogy that I use is that splitting the atom isn't easy and, conceptually, banks are made of atoms, but banks can get robbed without needing to split any atoms. So blockchains can be hacked without actually having to "crack the chain."

One example involved an experiment where a bitcoin owner printed his blockchain key on his T-shirt. He wanted to see if a theft would occur. It did: Someone took a photo of him and used it to drain his account. It was a classic case of leaving the key under the mat—or more like on top of the mat—for the burglar to find. As we know from many other cyberattacks not limited to blockchains, once you have the key or password—and there are many ways to accomplish this—you are in control. A blockchain system still has that risk.

Although the blockchain ledger itself is essentially just data, to add information to the blockchain or make use of the information stored there requires software code. It's common to have subtle flaws in the writing of software, such as the Ethereum hack where an intruder discovered a programming mistake and used it to move money into his account. More about this case a bit later.

Ultimately, blockchain may be its own worst enemy, as many of the things that make it so great also increase its vulnerability when it comes to security. Three examples are transparency, distributed control and anonymity.

Transparency clearly cuts both ways. The blockchain ledger itself (unlike the databases locked away in a bank's computer system) is distributed and copied on many servers, easily visible. Furthermore, the software code that processes the blockchain is publicly available and viewable (also unlike the walled-off software of a bank's computer system.) On the one hand, the logic goes, many people can view the software and verify that there are no flaws. But, on the other hand, a "bad guy" can easily access and study it to uncover flaws in the logic not yet noticed by anyone else, as happened **in the Ethereum case**.

Distributed control is a defining feature for blockchain systems. In a traditional centralized system, if the central computer fails, the system stops. With blockchain, the software operates simultaneously on many, possibly thousands, of servers around the world. If one or more servers fail, the system continues to operate. That has many obvious positive benefits. But it also means that there is no central “on” or “off” switch. For example, if a centralized stock market system runs into a problem, such as a flash crash, one solution is to shut the market off. But, in the case of an attack discovered on a blockchain system, it is essentially impossible to turn it off. In the example of the software flaw on the Ethereum system mentioned earlier, there was no way to stop the intruder from siphoning off more and more money. The ad hoc solution developed was to have a group of “good guys” use the same flaw to siphon off the remaining money faster than the “bad guy,” and then return as much money as possible to the legitimate owners.

Anonymity is another important feature. Access to your blockchain account requires your blockchain key, which is a long number—not possible to guess. It is the only way that you are identified so you are anonymous, which is why it is popular for illegal transactions, such as ransomware payments. If you had a safe-deposit box at a bank and lost your key, the bank could force the door open either using a locksmith or crowbar. But, there is no such override capability on your blockchain account. If you lose your key, the account is lost, which leads to headlines like: Cryptocurrency CEO Dies, $137M Funds Missing and Cryptocurrency Exchange Locked Out of Funds After CEO's Death.

The bottom line is that while the blockchain system represents advances in encryption and security, it is vulnerable in some of the same ways as other technology, **as well as new vulnerabilities unique to blockchain**. An important notion that our research is intended to dispel is that blockchain technology can protect data from misuse. In fact, human actions or inactions still have significant consequences for blockchain security.