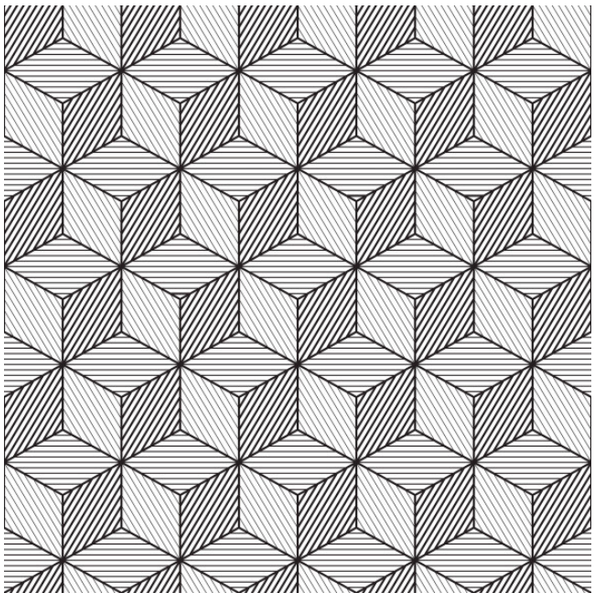
KLINT FINLEY 06.02.15 7:00 AM

HOW THE TECH BEHIND BITCOIN COULD STOP THE NEXT SNOWDEN



GETTY IMAGES

THE NATIONAL SECURITY Agency knows Edward Snowden disclosed many of its innermost secrets when he revealed how aggressive its surveillance tactics are. What it doesn't know is just how much information the whistleblower took with him when he left.

For all of its ability to track our telecommunications, the NSA seemingly has little clue exactly what documents, or even how many documents, Snowden gave to the media. Like most large organizations, the NSA had tools in place to track who accessed what data and when. But Snowden, a system administrator, apparently was able to cover his tracks by deleting or modifying the log files that tracked that access.

An Estonian company called Guardtime says it has a solution to that: using the same ideas that underpin the digital currency Bitcoin, the company says it can ensureno one can alter digital files, not even an organization's most senior executives or IT managers. The idea is to stop the next Snowden in his tracks by making it impossible to tamper with data, such as the NSA log files, in secret.

To prevent people from spending a single bitcoin twice, all transactions are recorded in a global, distributed ledger called the blockchain. All copies of the bitcoin client software include a copy of the blockchain, and falsifying the ledger would require controlling at least half of all the copies in existence.

Guardtime's Black Lantern uses the same idea applied to any chunk of data, such as an access log file or the data gathered by Internet of Things sensors. The blockchain could then be distributed to every executive, or even every employee, to ensure no one person can alter it. It doesn't encrypt the data, but it can let you know if someone has tampered with it.

Had the NSA been using Black Lantern, the agency would have been able to detect Snowden's activities early on, or at least would have much better idea of what Snowden took, says Guardtime CTO Matt Johnson, a former agent with the Air Force Office of Special Investigations agent and defense contractor.

"It keeps honest people honest," he says. "It makes it impossible for them to lie."

Securing Digital Assets

There's irony in a former federal law enforcement officer pitching a bitcoin-style decentralized cryptography system as a way of securing the NSA's data. Bitcoin proponents praise the blockchain as a way for citizens to hide their online tracks from the government; but Guardtime shows how the same technology could be used as a tool for surveillance.

We've already seen others repurpose bitcoin's code to create applications like Bitmessage, (an attempt to create a secure peer-to-peer messaging platform) andNamecoin (a decentralized alternative to the domain name system). Some hackers even aspire to createautonomous distributed corporations: online services that could exist without any human owners.

But Guardtime suggests these technologies are good for more than creating highly decentralized applications that replace or circumvent governments and corporations. Large organizations could use this technology to secure their assets.

Guardtime isn't the only company working on this. Last year IBM published a report proposing the creation of a blockchain-driven communications system for the Internet of Things. But Guardtime's product isn't theoretical. The Estonian government is using it for a range of purposes, including protecting data archives and patient health records. And through a partnership with telecom company Ericsson, Black Lantern is being sold to private firms.

Making Data Tamper-Proof

Like IBM, Guardtime thinks the Internet of Things could be the killer application for the blockchain. As more and more connected devices gather data and store it in the cloud—and governments and private citizens alike create automated systems that respond to that data—ensuring data hasn't been tampered with is crucial — especially if you have to trust outside vendors or hosting providers.

"We have to demonstrate the the hardware has not been tampered with," says Ericsson CTO Jason Hoffman.

That could be especially important for securing safety critical systems such as connected cars, implanted medical devices and airplane control systems.

It is important to understand the data itself isn't stored in the blockchain. Rather, it stores what's called a cryptographic hash, a long and unique mathematically-generated string of letters and numbers that corresponds to the original piece of data. Cryptographers can use these hashes to tell whether a file or piece of data has been changed. If you've ever downloaded a piece of open source software that displayed a bunch of random characters with a label like "SHA" or "MD5″ next to the download link, you've seen this in action.

These sorts of hashes are what Guardtime distributes to various machines. The upshot is that private data, such as health care records, can be monitored with the blockchain without those records ever needing to be shared.

Frank Cilluffo of the George Washington University Center for Cyber and Homeland Security is intrigued. Cilluffo says a properly implemented version of the concept could have huge security ramifications because it addresses internal, not external, attacks. "This is throwing the way we think on its head," he says.

The big question is whether any of this will work the way the company says it will. But the theory is sound says Matthew Green, a cryptographer and assistant research professor computer science at Johns Hopkins University. Although he isn't familiar with Guardtime's product, Green says some of the basic ideas have been explored before, including in this paper co-written by cryptographer and former WIRED columnist Bruce Schneier. "Block chains and decentralized systems seem like an obvious extension to this idea," Green says. The limitations are the cost of running additional servers to host the blockchain, and the fact that you're just monitoring whether data is changed, not protecting the data itself.

Keeping Governments Honest

While Black Lantern could be used by governments to protect its secrets, it just as easily could be used as a tool to keep government accountable.

Using Guardtime, a government could, in theory, give all citizens a copy of a blockchain that records changes to email log files. It wouldn't stop a political leader from deleting important email, and it wouldn't place the contents of the email, or even the metadata, in the ledger. But it would alert auditors and investigators to changes.

In other words, using the blockchain as a surveillance tool could go both ways. Convincing any government agency to implement such a radical safeguard, however, is another matter.