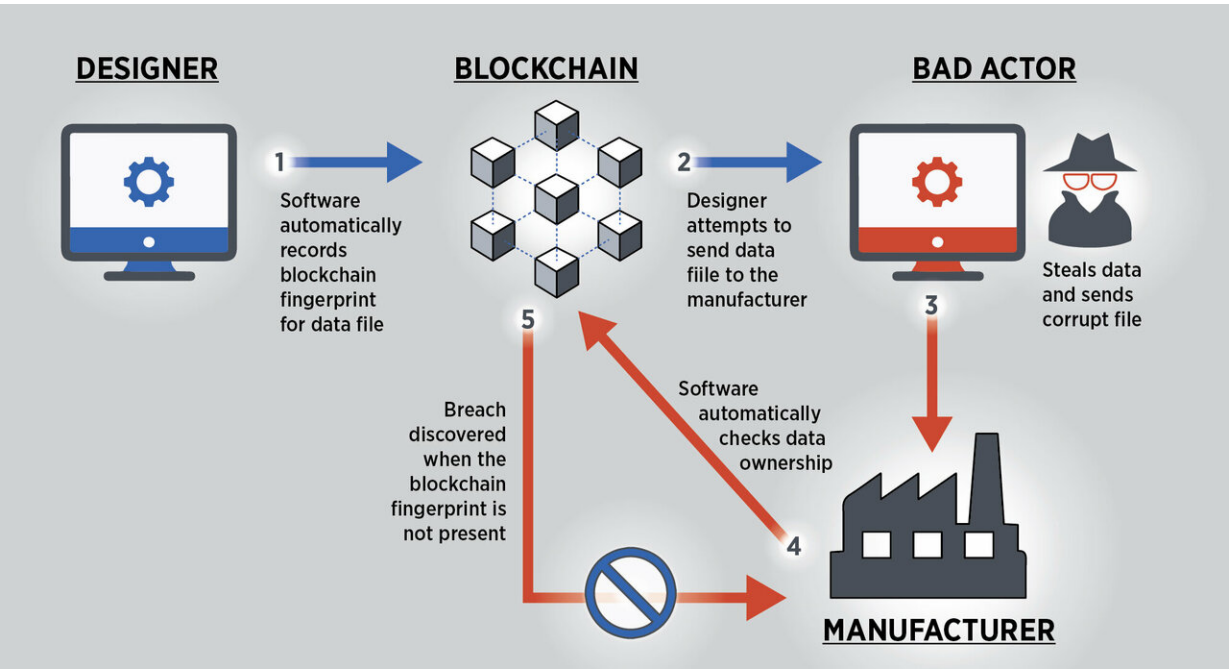
NIST: Blockchain provides security, traceability for smart manufacturing

February 11 2019



Blockchain technology could help deter digital threats in smart manufacturing systems. Credit: N. Hanacek/NIST

Engineers at the National Institute of Standards and Technology (NIST) needed a way to secure smart manufacturing systems using the digital thread , so they turned to the new kid on the block ... blockchain, that is.

According to a new NIST report, the security system better known for

underpinning Bitcoin and other digital currencies not only provides tamper-proof transmission of manufacturing data, it also yields something just as valuable to its users—traceability of that data to all participants in the production process.

"Because blockchain gives us both capabilities, we can build trustworthiness into digital manufacturing networks," said NIST mechanical engineer Thomas Hedberg, one of the authors of the report.

Blockchain, first used for Bitcoin a decade ago, is an expandable list of records, or blocks, that each contain data representing an individual transaction by members of a network. Each block consists of the data set, a time stamp, a cryptographic hash (an algorithm serving as a "cybersecurity fingerprint") and the hash of the previous block to mathematically link the two together. Therefore, each block in the chain is connected to the one after, the one before and all the way back to the original transaction (known as the genesis block). This means that the information contained in any block cannot be altered without changing all subsequent blocks and alerting the record-keepers in the network that foul play has occurred.

The digital thread was created to replace two-dimensional design and fabrication information, what we know as blueprints, that has traditionally guided a product through its manufacturing lifecycle. However, it requires humans to interpret, translate, re-enter and transmit data at each step. Processes using the digital thread method rely instead on a set of three-dimensional, digitized instructions that can be electronically exchanged and processed from start to finish, saving time, money and the risk of human error. Because the steps in the process are aligned chronologically, just like financial transactions, blockchain is extremely well-suited to provide a digital thread network with the same protection it gives to cryptocurrencies.

"In other words, if I'm a manufacturer making a part for a product and I receive the specs for that part from the designer who's upstream in the process, blockchain ensures that I can trust the data actually came from that person, is exactly what he or she sent, and was not interfered with during transmission," said NIST research associate and computer scientist Sylvere Krima, the lead author of the new report. "Because the chain is tamper resistant and the blocks are time stamped, a blockchain is a robust solution to authenticate data at any point during the product lifecycle."

In their report, Hedberg, Krima and co-author Allison Barnard Feeney describe potential digital threats to smart manufacturing such as product data theft, tampering and corruption. They then show how blockchain can help reveal and thereby deter these threats, which could each produce catastrophes in the manufacturing process.

"For instance, we give the example of product data being sent by a designer to one manufacturer who then must transmit updated data to a second manufacturer for further product processing," Hedberg said. "If a data thief, someone we call a 'bad actor,' grabs the file from Manufacturer 1 and attempts to send Manufacturer 2 a fake data file to cover his crime, Manufacturer 2 will know something's wrong because the true file's blockchain fingerprint won't be there."

The NIST report also details codes and statements in the Unified Modeling Language (UML), a standardized system for computer modeling, that are needed to successfully apply blockchain to a smart manufacturing network.

"Following our reference information model will enable users to authenticate everything within their blocks: where are the data coming from and going to, who is executing the data exchanges, when are the exchanges taking place, what is being exchanged, and how are the

exchanges being conducted," Krima said.

"The goal of this reference model is to secure the digital thread for smart manufacturing while enhancing collaboration and establishing trust between production partners," Hedberg said.

To further illustrate blockchain's value to smart manufacturing, a second NIST report features case studies from three different industrial sectors—additive manufacturing, autonomous vehicles and pharmaceutical—showing how the cybersecurity and traceability system would work for each.

To further illustrate blockchain's value to smart manufacturing, a second NIST report features case studies from three different industrial sectors—additive manufacturing, autonomous vehicles and pharmaceutical—showing how the cybersecurity and traceability system would work for each.

More information: Sylvere Krima et al, Securing the digital threat for smart manufacturing:, (2019). DOI: 10.6028/NIST.AMS.300-6

Provided by National Institute of Standards and Technology