Blockchain or Bitcoin based Industry 4.0, and 3D printing security, faces threat from quantum computer

3D printing or additive manufacturing is ongoing revolution in manufacturing with its potential to fabricate any complex object and is being utilized from aerospace components to human organs, textiles, metals, buildings and even food.From the creation of the additive manufacturing (AM) design to final production on the shop floor, AM files can be easily transmitted with the click of a mouse. The digital nature of AM means that parts and products are easier to share and transmit, enabling the creation of digital supply networks and supply chains. Additionally, it creates the opportunity to make AM part development fully documentable and attributable, write Stuart Trouton and others in Deloitte University press.

In future AM shall become part of ongoing evolution of the Internet through the “Internet of Things” to the “Internet of Industry”. Another name for the Internet of Industry, common in Germany, is “Industry 4.0”. In this vision, people will be able to study designs, modify them, download them onto nearby 3D printers, and thereby create new goods.

3D printing is also revolutionizing defence by printing small components to full drones on naval vessels, replacement parts for fighter aircrafts to printing ammunition. Substantial improvements have been made in 3D printing with the fabrication of 3D objects from metals, ceramics, plastics, and even multi-material capabilities. John Burrow, deputy assistant secretary of the Navy for Research, Development, Test and Evaluation said, “I think you are about to see its operational and technical potential literally explode off the

map.” Burrow and Navy officials envision a future with 3-D printers forward deployed with Marines and installed aboard warships as well as shore-based commands.

However digital and networked nature of AM also give rise to many vulnerabilities. In the absence of a strong data-protection framework, a digital design-and-manufacture process creates the potential for data theft or tampering. Hackers can exploit 3D printing technology by stealing or altering information designs, rendering your printers unusable, or corrupting your settings to make devices overheat or even explode. And of course, there is the theoretical possibility that 3D printing designs are altered with malicious intent as a method to sabotage constructions, weapons or defense systems.

Blockchain a transformative decentralized digital currency, a secure payment platform free from government interference, is being considered for security of additive manufacturing . The technology has the potential to enhance privacy, security and freedom of conveyance of data. Blockchain is based on open, global infrastructure, decentralized public ledger of transactions that no one person or company owns or controls, ensures security of transfer of funds through public and private cryptology and third parties to verify that they shook, digitally, on an agreement.

However in Oct 2017 paper, Researchers mostly from Singapore claimed that key protocols securing technology undergirding bitcoin are “susceptible to attack by the development of a sufficiently large quantum computer”, in their paper “Quantum attacks on Bitcoin, and how to protect against them (Quantum),” made available through the Cornell University Library.

3D printing could be exploited by Hackers

A report was developed by the National Institute of Standards and Technology – NIST, which is part of the Department of Commerce – to warn contractors of the various vulnerable and exploitable points in the way 3D printing is used by various companies, and is not something that has come out of nowhere.

The two primary threat vectors are via network connectivity and nonvolatile storage media. When devices are not protected by applicable security controls, network connectivity and information stored within nonvolatile storage media may be used to compromise organizational information or disrupt the device.

According to the report, hackers can exploit unprotected 3D printers in a variety of ways. Some of the dangers listed are:

- Denial of service (DoS): to make printing services unavailable.
- Spams may waste materials while also result in denial of service for legitimate users.
- Exploiting default administration/configuration passwords to control the device locally or remotely via a web interface.
- Intercepting / Alteration / Corruption of unencrypted data and information.
- Vulnerabilities of commercial embedded operating system.

DOD aims to use additive manufacturing techniques in conjunction with blockchain

The Defense Department aims to use additive manufacturing techniques in conjunction with blockchain technology in efforts to address intellectual property challenges related to

the production of military standard parts, as reported by GCN. John Bergin, business technology officer at DoD's Office of the Chief Information Officer, told a defense contracting forum that the U.S. Navy's carriers can serve as a model for a use case of blockchain. He added he believes the technology has the potential to help military organizations and industry partners to accelerate the supply chain process for "mil-spec" components.

Bergin mentioned, "What happens, when an F-18 on that carrier breaks a pin in its landing gear? They need a part, but they don't have the part on the aircraft carrier," he said. "How do I use additive manufacturing to get there, while still respecting Boeing's intellectual property rights for that pin? Bergin suggested, "Blockchain -The encrypted and distributed ledger system that makes the Bitcoin cryptocurrency possible could be the answer"

If any part of the aircraft gets faulted due to damage in a small component in that part, the broken component cannot be replaced by substitute component due to intellectual property rights of the vendor. As a result, a new whole part has to be bought.

Bergin said. "IF DOD's ecosystem of parts management can properly incorporate blockchain ledgers, the 3D printers on a carrier could securely log every pin that's produced at sea. You can print it, I can pay Boeing for it, and [the Navy] has planes that fly," he said. "How do I support the warfighter abroad, respecting the intellectual property of the vendors, and do it as a team? Blockchain is part of that story."

If this kind of system is adopted, it would speed up the process of supply chain by allowing the military force or the navy or the air force to get only the pin it needs, rather than ordering a full landing gear assembly. This would help both the military and its industry partners. Bergin said "Let's stop buying the assembly, and let's start making the

parts where we need them. It reduces your inventory that's idle, and increases our operational capability at the front."

"There are security and quality assurance challenges in addition to the intellectual property concerns", Bergin said, but he urged vendors to work with DOD on these issues.

The US Navy Wants to Connect Its 3-D Printers with a Blockchain

The US Navy's innovation arm has revealed plans to trial blockchain's potential to bring added security to its manufacturing systems. Blockchain quite simply is a "distributed database" shared through peer to peer connections in such a way that each block is a unique record that gets added to the end of the "chain." The records are permanent and are unable to be modified. This bond creates trust between all the members of the chain and removes the need for third party mediators to handle transactions, or any other transfer of information.

This "immutable trust" allows for the removal of members not providing value (formerly used as middle-men or brokers) and allows two or more parties to conduct transactions with complete trust. If you can imagine any transaction in your life that depended on trust between you and someone you did not know, you will immediately see the value in Blockchain.

NIAC has planned to conduct a series of experiments (including a proof of concept) using blockchain technology to both securely share data between Additive Manufacturing sites, as well as help secure the digital thread of design and production. The successful application of this technology in a controlled environment, would then open the gates to revolutionize other aspects of Naval operations.

The ability to secure and securely share data throughout the manufacturing process (from design, prototyping, testing, production, and ultimately disposal) is critical to Additive Manufacturing and will form the foundation for future advanced manufacturing initiatives.

These efforts are pushing the production of critical pieces of gear and equipment closer and closer to deployed forces. While this change is greatly helping our material readiness, it creates the potential for vulnerabilities and makes the need for a cryptographically secure, traceable, immutable, and controllable data flow of utmost importance.

Bitcoin’s Elliptic Curve Signature Could be Broken by 2027

Bitcoins have two important security features that prevent them from being stolen or copied. Both are based on cryptographic protocols that are hard to crack. In other words, they exploit mathematical functions, like factorization, that are easy in one direction but hard in the other—at least for an ordinary classical computer.

Bitcoin transactions are stored in a distributed ledger that collates all the deals carried out in a specific time period, usually about 10 minutes. This collection, called a block, also contains a cryptographic hash of the previous block, which contains a cryptographic hash of the one before that, and so on in a chain. Hence the term blockchain. (A hash is a mathematical function that turns a set of data of any length into a set of specific length.)

The new block must also contain a number called a nonce that has a special property. When this nonce is hashed, or combined mathematically, with the content of the block, the result must be less than some specific target value. This process of

finding a nonce, called mining, is rewarded with Bitcoins. Mining is so computationally intensive that the task is usually divided among many computers that share the reward.

If a group of miners controls more than 50 percent of the computational power on the network, it can always mine blocks faster than whoever has the other 49 percent. In that case, it effectively controls the ledger. That creates an opportunity for a malicious owner of a quantum computer put to work as a Bitcoin miner. If this computational power breaks the 50 percent threshold, it can do what it likes.

“One particular area at risk are cryptocurrencies,” the abstract notes. “We investigate the risk of Bitcoin, and other cryptocurrencies, to attacks by quantum computers. We find that the proof-of-work used by Bitcoin is relatively resistant to substantial speedup by quantum computers in the next 10 years,” the paper declares. This, they claim, is “mainly because specialized ASIC miners are extremely fast compared to the estimated clock speed of near-term quantum computers.”

The good news turns quickly bad, as “the elliptic curve signature scheme used by Bitcoin is much more at risk, and could be completely broken by a quantum computer as early as 2027, by the most optimistic estimates,” state authors Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel.

References and resources also include:

https://gcn.com/Articles/2017/05/15/DOD-blockchain-3D-printing.aspx

http://www.coindesk.com/the-us-navy-wants-to-connect-its-3-d-printers-with-a-blockchain/

http://kryptomoney.com/blockchain-meets-3d-printing/

http://idstch.com/home5/international-defence-security-and-technology/industry/darpa-perfecting-3d-printing-for-military-through-its-open-manufacturing-program/

https://dupress.deloitte.com/dup-us-en/focus/3d-opportunity/3d-printing-blockchain-in-manufacturing.html

https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/