NATIONAL CENTER FOR MANUFACTURING SCIENCES

COLLABORATION THAT WORKS

Protecting the Additive Manufacturing Workflow with Blockchain Technology

THE NEW DECENTRALIZED MODEL OF SECURE MANUFACTURING

Co-Authors
Chris Adkins, Identify3D
Dana Ellis, NCMS

www.ncms.org
June 2018

Digital Supply (Block)Chain

As more and more industries are realizing the benefits of additive manufacturing (AM), the transportation, distribution, and security of the needed digital files has become a major topic of consideration. The products of AM are only as viable as the integrity of the digital files and the printers that create them. The Department of Defense (DoD) is using AM for several maintenance activities and the security of those pieces cannot be left to chance.

Today, the sheer volume of data produced by supply chains and their newly formed digital ecosystems is overwhelming. If unsecured, this data has the potential to harm through counterfeit, maliciously modified, and poor quality technology data packages. The National Center for Manufacturing Sciences (NCMS) and their partners seek to investigate how a blockchain enabled security solution can improve the digital supply chain and enable new manufacturing and sustainment models across DoD.

The National Center for Manufacturing Sciences (NCMS) has identified cybersecurity for manufacturing as a key challenge that needs to be addressed for companies to be able to fully achieve the benefits of Industry 4.0. The manufacturing sector is the third most targeted sector for cyberattacks after the government and the financial sectors.[1] A recent LNS Research study presented by NCMS at the Automation World's conference in Chicago last month showed that more than 50% of respondents confirmed having experienced cybersecurity breaches at manufacturing plants over the last 12 months.[2] The next logical target of potential attacks after sites and machines will be the parts themselves and more specifically their digital version.

Technologies such as additive manufacturing (AM) are fundamentally changing how companies manufacture, distribute, and maintain products. Companies are moving toward decentralized manufacturing models that allow for manufacturing at the place and time of need. As highly sensitive product data travels between industrial companies, suppliers, and subcontractors, ensuring the security and integrity of intellectual property becomes a major challenge. The integrity and traceability of the AM digital flow is critical to prevent counterfeits, maliciously modified, poor quality, or uncertified parts from entering the physical supply chain.

NCMS, in collaboration with Identify3D, has launched an initiative to adapt blockchain technology for AM. This pilot project will enable the creation, secure distribution, and traceability of digital assets in various government supply chains including those of Fleet Readiness Center South West, Naval Undersea Warfare Center (NUWC) Keyport, WA, Defense Logisitic Agency (DLA), Marine Corps FAB Lab, U.S. Army Aviation and Missile Research, Development and Engineering Center (AMRDEC), and others.

A digital supply chain has four main distinct phases: design, distribution, manufacturing, and in-field. This whitepaper explains the theory behind securing supply chain data with blockchain.

1 https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers

2 https://www.packworld.com/article/trends-and-issues/business-intelligence/cyberattacks-directed-manufacturing-could-shut-your

DESIGN

During this phase a future product is designed, tested, and prototyped. Once ready for production, both the final design of the part and all of its associated engineering data (i.e., how to build the part) are considered highly valued assets requiring protection.

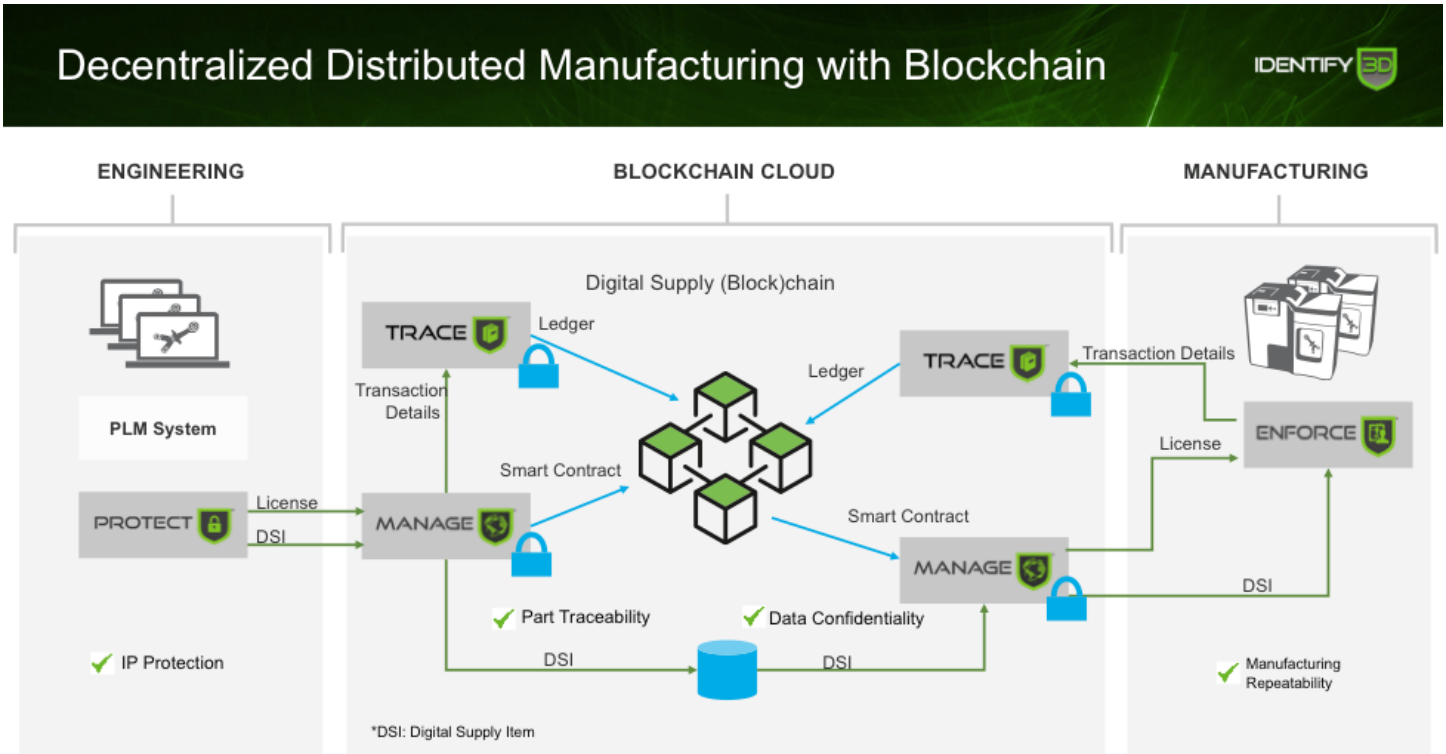
Encryption of design files at this stage is best practiced in order to ensure that only authorized users have access to the information enclosed. An encrypted digital container, called a digital supply item (DSI), can be created for each part so that the design files cannot be accessed until decrypted by an AM machine.

Through a mechanism of licensing, the intellectual property (IP) owner can define who has access to the data, for how long, and how the data should be used for manufacturing the part, e.g., which machine, material, and parameter set and how many parts can be manufactured.

DISTRIBUTE

In a traditional manufacturing process, the company that creates the design files would manufacture the parts and ship them. However, in a digital supply chain the company that designs the parts sends the encrypted design files and digital license to the next downstream actors in the supply chain. Files may be transmitted via email, an off-line system, or direct access to the company server from one system to another, depending on the level of security measures.

Using a smart contract enabled blockchain, the digital distribution license can be authenticated, transported, and recorded by blockchain transactions. This allows all members of the blockchain to participate and enforce the distribution and asset management rules set by the smart contract.



MANUFACTURE

From that point on, the production of parts may be licensed out to multiple manufacturers. Each manufacturer will use the design files to produce parts in accordance with digital parameters set out by the licensing agreement.

By applying business and production rules to the encrypted design files, engineers can set specifications on the machine make and model that will be able to execute the design, the type of build materials allowed, and a variety of other build parameters. Manufacturers will only be able to decrypt the design files once specifications are met, and production rules will control the number of parts that the manufacturer is licensed to print, ensuring both that quality standards are met and that counterfeits cannot be made using authorized equipment.

All events can be tracked and stored on the blockchain ledger, so that the provenance of each part is verified and any errors detected in end products can be traced to their source.

IN-FIELD

When a physical part is manufactured, each part should be tagged with a digital reference that will be recorded in the ledger, providing a link between the digital and physical thread that can trace the part back to its manufacturer, machine that created it, and original design creator. Possible methods of coding parts include embedding chemical trackers, RFID, or serialization numbering that can be matched to information stored in the ledger.

Storing manufacturing data on the blockchain ledger not only ensures traceability, but also can be used for performance modeling, failure simulation, and overall performance improvement of the part.

The blockchain will store information across each phase on participating nodes. A node is any electronic device connected to the blockchain network, each of which automatically downloads and stores a copy of the blockchain. All transactions within a block of data are cryptographically hashed along with the previous block to form the current block. Therefore, any data modifications would compromise the integrity of the entire chain, and since the blockchain network is governed by the consensus, the authenticity of any transaction can be rejected as a fraudulent transaction.

INTELLECTUAL PROPERTY, SAFETY, AND NATIONAL SECURITY

Securing the digital supply chain with blockchain technology is critical and not just because of lost revenue from IP theft. For the government, counterfeit parts represent both safety and national security risk. The Department of Defense (DoD) named supply chain integrity and counterfeit parts two of its top concerns for the electronics sector in its FY 2017 Annual Defense Industrial Capabilities Report.[3] The report identifies technological obsolescence as a key reason that counterfeit parts enter into the supply chain. Obsolescence is defined as equipment no longer manufactured by OEMs, which must then be purchased from 3rd party distributors. According to the DoD report, between 50% and 80% of suspect counterfeit parts were obsolete at the time of discovery. AM can mitigate these risks by allowing suppliers to store designs and produce the replacement parts on-demand using the correct design file validated by the blockchain.

Advanced manufacturing techniques and decentralized manufacturing models will unlock faster production, accelerate time to market, reduce physical storage requirements, and transform sustainment. NCMS seeks to investigate how a blockchain enabled security solution can improve the digital supply chain and enable new manufacturing models by including counterfeit mitigation, data integrity, compliance rights, feedback monitoring, and revocation. Through the NCMS Commercial Technologies for Maintenance Activities (CTMA) Program, the “Adapting Blockchain Technology for Additive Manufacturing” project will develop industry best practices for securing and authenticating data and how blockchain technology can be best utilized to support new distributive manufacturing ecosystems.

3 https://partner-mco-archive.s3.amazonaws.com/client_files/1527002508.pdf

About NCMS

The National Center for Manufacturing Sciences (NCMS) is a cross-industry technology development consortium, dedicated to improving the competitiveness and strength of the U.S. industrial base. As a member-based organization, it leverages its network of industry, government, and academia to develop, demonstrate, and transition innovative technologies efficiently, with less risk and lower cost.
For more information on NCMS, visit www.ncms.org

Media Contact:

NCMS Communications Director Pam Hurt pamh@ncms.org, 248-867-3525

About Identify3D

Identify3D, Inc. is a leader in software for digital supply chain. The Identify3D technology suite protects confidentiality and integrity of data in the digital manufacturing thread providing intellectual property protection, manufacturing repeatability, and traceability from design to finish product. We enable companies to have the confidence that their data are secure and products are manufactured following the right processes and requirements. We deliver greater control over the digital manufacturing process ensuring integrity and authenticity of complex supply chains.

COLLABORATION THAT WORKS

www.ncms.org