A novel paradigm for managing the product development process utilising blockchain technology principles

Nikolaos Papakostas (2), Anthony Newell, Vincent Hargaden

Laboratory for Advanced Manufacturing Simulation and Robotics, School of Mechanical and Materials Engineering, University College Dublin, Belfield, Dublin 4, Ireland

The product conceptualisation, design and manufacturing phases are becoming increasingly complex, since more available resources, stakeholders and sophisticated technologies are involved during product development. The exchange and management of product-related information is often a challenging task, affecting significantly the intellectual property protection process as well as the distinction of roles among stakeholders. This paper proposes a conceptual framework that utilises blockchain technology principles for managing product development information and processes with the goal of providing new approaches to extending the functionality of product data management systems. A test case focusing on products developed with additive manufacturing technologies is presented.

Design, Product Development, Additive manufacturing

1. Introduction

In order to remain competitive, manufacturing companies need to securely manage their intellectual property (IP). Lifecycle Management (PLM) platforms that are available in the market nowadays have been typically used to manage this data across relevant stakeholders. However, the high expenses associated with the adoption of PLM has hindered its integration in small to medium enterprises (SMEs) [1]. At the same time, IP data, if corrupted or stolen, can compromise products when infringed [2], leading to lost revenue, or by modification of the original design to a functionally impaired configuration. Different data-centric security mechanisms may be used in manufacturing [3].

The vulnerabilities associated with digitally interconnected industry 4.0 manufacturing process chains are further increased by the higher number of attack points along the product lifecycle [4], [5]. Additive manufacturing (AM), in particular, with its layer-wise production method, affords almost limitless design potential [6] and enables the mass customisation of end-user parts across a diverse range of manufacturing industries [7]. However, a series of vulnerabilities associated with AM technology, compounded by its digital nature, could potentially enable malicious agents to introduce internal defects, such as pores or internal geometrical inaccuracies, compromising the mechanical and functional properties of the product, without being readily detectable by traditional qualification methods [8]. There is also a potential to cause harm to AM system equipment as well as to their operators and to final product end-users [8]. This needs to be seriously considered when mission-critical parts, such as customised medical implants and avionics parts are planned to be produced.

At the same time, the consideration of the needs related to the tasks of cyber-physical systems design and verification is very important [9]. Blockchain technology is among the most promising technologies for recording transactions involving multiple engineering disciplines, since it can be used to verify transactions of product data information among stakeholders along the process chain in a decentralised manner. This may protect the production chain from malicious attacks, while improving accountability.

This technology has been tested for AM product information management in [10], whereby the implementation of order provisioning and processing only was handled via blockchains, which removed the need for an intermediate data platform between the consumer and the producer.

IP protection of AM product information was addressed in [2] using digital rights management, whereby licenses to produce AM products are stored in a blockchain-enabled data platform termed 'Secure Additive Manufacturing Platform' (SAMPL), using the blockchain platform Ethereum. This system allowed for greater data traceability. Kennedy et al [11] developed an anti-counterfeiting measure for AM products by linking a part-specific unique chemical signature associated with embedded nanomaterials to an Ethereum-based blockchain ledger entry. This is expected to make the cost of counterfeiting AM parts and products increasingly expensive.

The use of agent-based systems enables autonomous decision making in an effective, decentralised manner in manufacturing processes [12]. Multi-agent systems implementing blockchain technologies were reviewed by Calvaresi et al [13]. The domains of application generally included collaborative governance, big data management, data integrity and reputation management but no applications were noted for manufacturing specifically.

This paper outlines the deployment of a multi-agent system employing blockchain technology to manage the security of IP transactions containing manufacturing technical data across relevant stakeholders.

2. Proposed approach

Nowadays product data exchange may be handled by Product Lifecycle Management (PLM) platforms. Their deployment is quite costly, and it is often the case that SMEs cannot easily afford them. Whenever these companies become part of larger OEMs' networks, the PLM platforms used typically belong to an OEM and therefore the transparency of the information contained is limited. Furthermore, these platforms constitute single points of attack and their security may be compromised. For these reasons the employment of blockchain technologies is considered in this paper, as a way towards increasing security and transparency.

2.1. Blockchain technologies

A blockchain is a list or chain of blocks, which are linked together using cryptographic methods. Each block contains information about a number of transactions, for instance the uploading of a CAD file to a collaborative cloud platform so that a set of cooperating partners in an engineering or manufacturing network can work on. Each subsequent block holds information related to previous blocks. Cryptographic hashes are used for linking blocks together. A blockchain is typically distributed and decentralised and is resistant to modification by external agents, leading to a permanent record of transactions available in an open and transparent way [14]. If data within a blockchain was to be altered, all of the data within the subsequent blocks would also need to be altered as the digital signature is intrinsically associated with the data content of the blocks i.e. changing the data necessarily changes the digital signature [15]. There are public blockchain networks, with the largest one being bitcoin. A disadvantage of maintaining a distributed ledger of this size is the vast quantity of computational power required by anonymous nodes to achieve consensus through 'proof of work' [16], whereby a computationally demanding and complex cryptographic problem is solved, referred to as mining when applied to cryptocurrency. The harder to control privacy of transaction's data in a public blockchain is also of concern for enterprise applications, since engineering files contain high IP value.

On the other hand, in a private blockchain, participants are invited to join on a permissioned network according to network-specific access control mechanisms. They do not require validation of transactions in the same 'proof of work' method but instead rely on trusted validators to achieve consensus [17].

2.2. Agent-based engineering data sharing

In this paper a novel approach is presented, utilising the main principles of private blockchains. A blockchain, storing the technical transactions, will be accessible by all networked partners. Each stakeholder is represented by a software agent, which may automate the process of updating the blockchain while exchanging information. Each agent will own a private and a public key. Transactions among manufacturing and engineering nodes are recorded and become part of blockchain blocks (Fig. 1). Each transaction is 'signed' by the data sender agent, utilising their private key, so that any change of its content be prevented. This way, every transaction is associated with the node that carried it out in practice as well as with the node that received this information. Transactions need to be agreed upon before they become part of the blockchain. Each block contains open public access data, such as the product id, user manuals, that may later be retrieved by consumers, or disassembly or recycling guidelines that may be retrieved by recycling companies, as well as encrypted limited access data that are only used by the manufacturing network nodes. This data may contain engineering documents with information, such as material specifications, mechanical properties, colour, weight, assembly number, CAD files and other transaction information.

A cloud-based repository may be used for storing the files, thus keeping the blockchain as lightweight as possible. All data becomes part of the blockchain and is verifiable according to the checksum of the CAD files and all other technical information relevant to the products. This data, together with the public keys of the data sender and recipient are then used to generate the cryptographic hash for that block such that modification of it would require modification of all subsequent blocks, reducing the likelihood of fraud. All relevant stakeholders have access to the block data allowing for a verifiable record of the product IP.

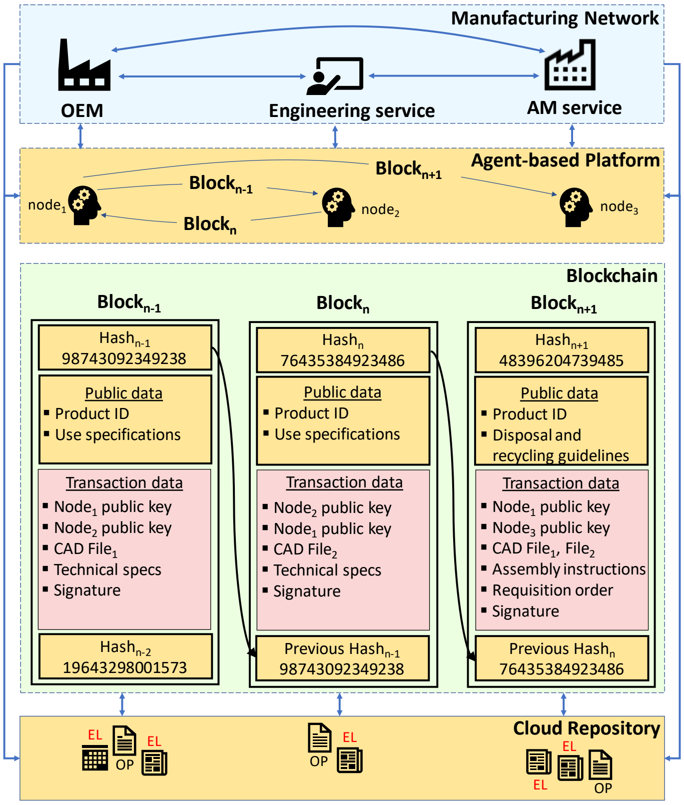

Figure 1. Example of blockchain containing encrypted limited access (EL) and open access (OP) manufacturing process chain data.

Across the product lifecycle, external stakeholders may also have access to the blockchain data in order to gain access to engineering information, so that they may recommend maintenance, disassembly and recycling procedures. Information generated during the product lifecycle may be provided back to the OEM so that the blockchain be updated continuously.

3. Implementation

A test case was conceived for evaluating and validating the proposed approach. The case includes the production of a customised assembly of two parts to be used in the cabin of a passenger vehicle. The proposed platform for this implementation is based on the Java Agent Development Framework (JADE) [18], and contains Engineering, Machine and Lifecycle Agents. The blockchain functionality was implemented separately in Java.

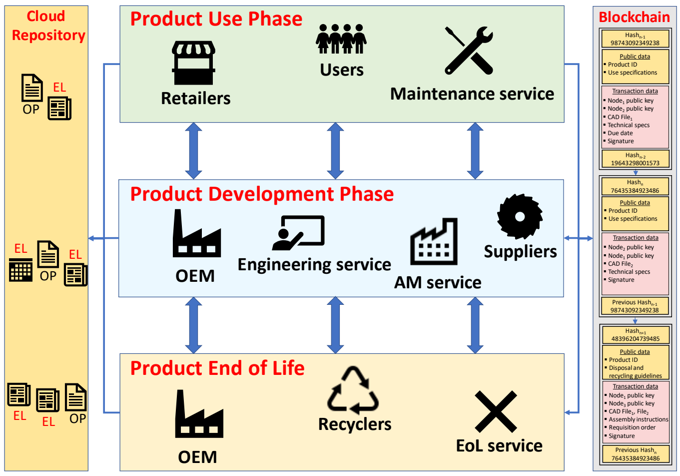

Figure 2. Utilisation of blockchain across product lifecycle

Engineering Agents represent Original Equipment Manufacturers (OEMs) and engineering service providers. They are used by engineers for specifying data in the form of part technical information, such as CAD, material specifications, required mechanical properties such as density, tensile strength and task or order due dates. An Agent Management System (AMS), providing the naming service, and a Directory Facilitator (DF), providing a Yellow Pages service, allowing agents to find other agents are also part of the proposed platform as standard parts of JADE. Machine Agents represent AM service providers and interface with the CAM software of the AM machines and Manufacturing Execution Systems (MES) in order to retrieve information, such as machine availability and to calculate the product build time and cost, utilising machines and materials that can meet the minimum quality and mechanical specifications of the Engineering Agents' input. Lifecycle agents represent other stakeholders that may require product data during the product lifecycle, including companies requesting information about the product recycling or dismantling. Fig. 3 shows an example implementation of 7 transactions input to the blockchain between an OEM, an Engineering Service Provider, 2 AM service providers and a Recycling company. The public and private information stored in each block together with the corresponding documents, which are stored in the cloud repository are also shown in Fig. 3. The case was tested in a networked multi-computer environment, where users interacted with the software agents in a number of transactions, which are listed below:

1. The OEM sends technical information for one component of the product assembly to an Engineering Service Provider, requesting the design of a second component. This technical information can contain CAD files, material specifications, mechanical properties, task due date.
2. The second transaction includes the CAD file and all relevant technical information for the second component and is sent back to the OEM.
3. After verification, the technical information for both components is sent by the OEM to 2 AM service providers. CAM tools and the corresponding process profiles may be used by each Machine Agent for generating alternative process plans.
4. The output of the CAM tools, a number of alternative process plans, is returned through the 2 Machine Agents back to the OEM. Information in this transaction includes the process time, delivery time, cost per part and alternative process configurations (material and process parameters). This is the most computationally intensive process and in this case scenario each Machine Agent required about 2.5 minutes to generate and evaluate 12 process alternatives.
5. Then, the AM service provider with the best process configuration is selected, considering the time, cost and quality performance of all alternative configurations. The next transaction between the OEM and the selected AM service provider includes the components order details, such as the quantity, final technical specifications and due date.

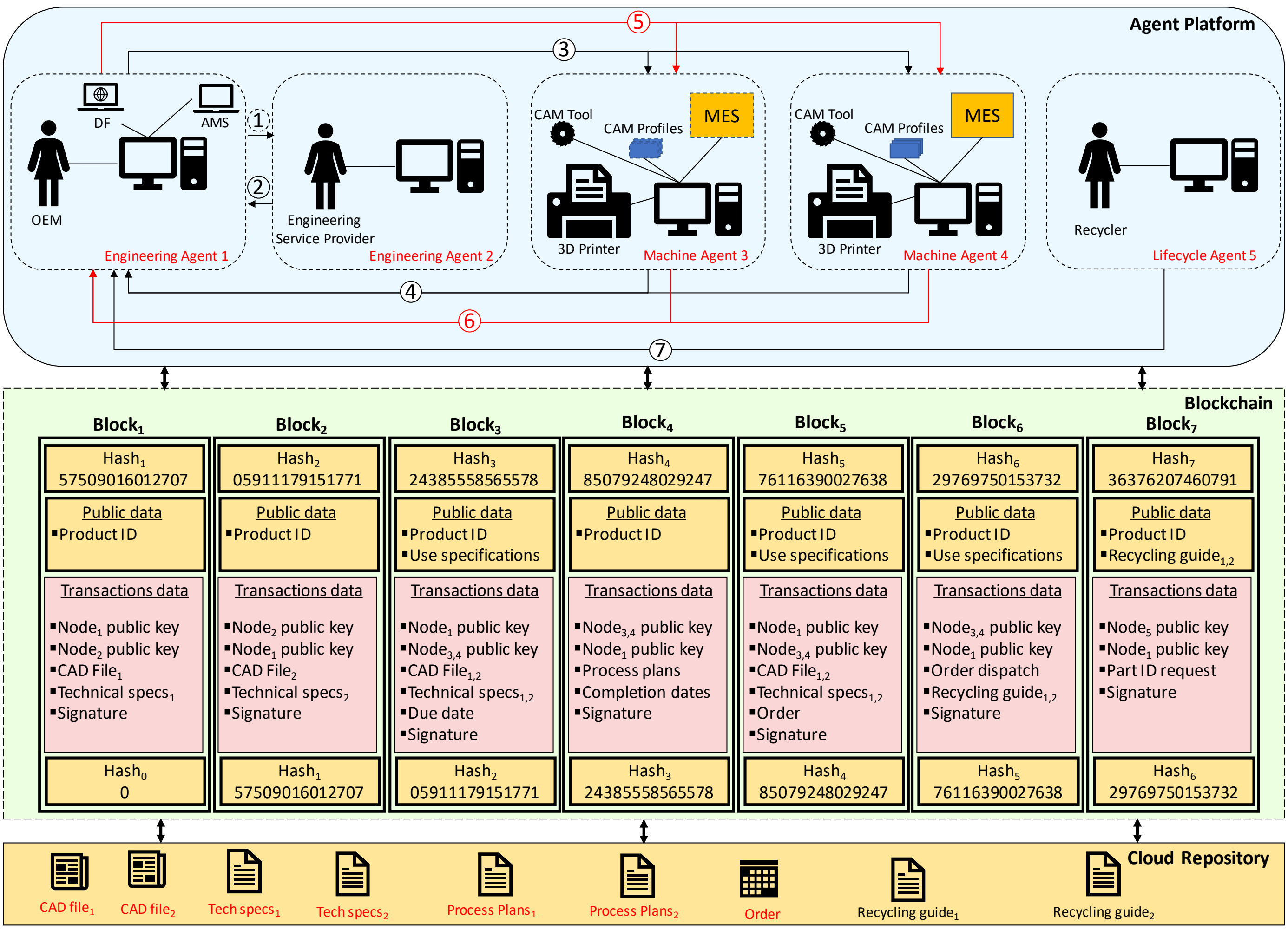

Figure 3. Agents transactions, resulting blockchain and corresponding cloud repository documents.

6. The order dispatch transaction details are then sent from the AM service provider to the OEM; the transaction data includes the weight of the package, assembly details, material details and recycling or dismantling instructions.
7. The transaction at the product end of life requests the disassembly and recycling instructions such that the part can be recycled or disposed of in a sustainable manner.

The advantages of the proposed approach over product lifecycle management systems include:

- An affordable data exchange mechanism, allowing companies and especially SMEs to directly interact with OEMs and other partners in a straightforward, cost-efficient manner.
- Greater transparency for all networked partners and transactions. All nodes share the same information and documents as opposed to maintaining individual copies.
- Enhanced security since transactions must be agreed upon before they become part of the blockchain. Sensitive or crucial information is encrypted as part of transactions, and the information is stored across a network of computers thus avoiding single point attacks.
- Improved traceability of transactions, which would also lead to higher accountability for all networked partners.

4. Conclusions

The implementation of blockchain technology in a multi-agent system was demonstrated in this paper for easier verification and transparent distribution of manufacturing IP.

Security and verifiability of product IP are necessary for a successful manufacturing business model. IP management is however fraught with issues in terms of how to store and secure it during its development and later use. PLM systems are frequently used to manage product data in a centralised manner, though this leads to transparency and verifiability issues when files need to be validated at a later stage. For a lot of companies and particularly SMEs, the deployment of a PLM system and subsequent training, or licensing as an IT client can be a costly and time-consuming process on top of the transparency and verifiability issues. The problem also exists in reverse, in terms of how an OEM can guarantee that their own IP, associated with the engineering information and files of the PLM system, does not go out of their network.

Blockchain in a manufacturing context can be utilised in order to store IP or product data and secure it between transactions of this data across designers and engineers, managers and other stakeholders within a company and also when showing IP to stakeholders outside of the network. The advantages of using blockchain are that the system imparts intrinsic confidence in its data due to the enormous difficulty in tampering with it such that this wouldn't be noticed and can, therefore, be used to demonstrate data authenticity. This means that IP remains verifiable with all of its associated data, such as developer information, CAD files, material specifications and so on. Blockchain can also be used for data management in a considerably more lightweight manner than some PLM systems. At product end-of-life, stakeholders outside of the network, such as recycling companies could also search through the blockchain in order to find the ID and all necessary documentation for how, for instance, to recycle and disassemble the product. Overall, it is expected that the proposed approach will become increasingly relevant as production becomes more networked.

One of the challenges that needs to be addressed in the future is related to the new skillsets the users of the proposed approach and especially product designers should acquire. These would include a better knowledge of the main principles of blockchain technology, as well as a deeper understanding of the AM process characteristics and capabilities, so that they can validate the AM process configurations, which would be generated by Machine Agents. Future research could focus on how the proposed approach may be utilised for recording supply chain transactions. Further efforts could also be made for alleviating certain shortcomings of multi-agent software systems, such as the difficulty in integrating and validating the complex operation of entities or of the human operators they represent and the computational power limitations that may appear in some cases, where, for instance, a vast number of process configurations alternatives is requested to be generated and validated.

Acknowledgements

This work has been partially supported by a research grant from Science Foundation Ireland (SFI) under Grant Number 16/RC/3872 and is co-funded under the European Regional Development Fund and I-Form industry partners.

References

[1] Holligan, C, Hargaden V, Papakostas N (2017) Product lifecycle management and digital manufacturing technologies in the era of cloud computing. In Proceedings: 2017 Int. Conf. Eng. Technol. Innov. pp 909–918.
[2] Holland M, Stjepandic J, Nigischer C (2018) Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. In Proceedings: 2018 IEEE Int. Conf. Eng. Technol. Innov., pp 1-8.
[3] Chaduvula SC, Dachowicz A, Atallah MJ, Panchal JH (2018) Security in Cyber-Enabled Design and Manufacturing: A Survey. *Journal of Computing and Information Science in Engineering* 18:40802–40815.
[4] Yampolskiy M, King WE, Gatlin J, Belikovetsky S, Brown A, Skjellum A, Elovici Y (2018) Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing* 21:431–457.
[5] Farooq MU, Waseem M, Khairi A, Mazhar S (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computing Applications* 111(7):1-6.
[6] Thompson MK, Moroni G, Vaneker T, Fadel G, Campbell RI, Gibson I, Bernard A, Schulz J, Graf P, Ahuja B (2016) Design for Additive Manufacturing: Trends, opportunities, considerations, and constraints. *CIRP Annals* 65(2):737–760.
[7] Bikas H, Stavropoulos P, Chryssolouris G (2016) Additive manufacturing methods and modelling approaches: a critical review. *International Journal of Advanced Manufacturing Technology* 83:389–405.
[8] Sturm LD, Williams CB, Camelio JA, White J, Parker R (2017) Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. *Journal of Manufacturing Systems* 44:154–164.
[9] Stark M, Kind S, Neumeyer S (2017) Innovations in digital modelling for next generation manufacturing system design. *CIRP Annals* 66(1):169-172.
[10] Baumung W, Fomin V (2018) Increasing the utilization of additive manufacturing resources through the use of blockchain technology for a production network. In Proceedings: CEUR Work Proc Balt 2018 pp 135-141.
[11] Kennedy ZC, Stephenson DE, Christ JF, Pope TR, Arey BW, Barrett CA, Warner MG (2017) Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology. *Journal of Materials Chemistry C* 5:9570–9578.
[12] Monostori L, Váncza J, Kumara SRT (2006) Agent-based systems for manufacturing. *CIRP Annals - Manufacturing Technology* 55:697-720.
[13] Calvaresi D, Dubovitskaya A, Calbimonte JP, Taveter K, Schumacher M (2018) Multi-agent systems and blockchain: Results from a systematic literature review. *Lecture Notes in Computer Science* 10978:110–126.
[14] Bahga A, Madisetti VK (2016) Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications* 9:533-546.
[15] Pilkington M (2016) Blockchain technology: principles and applications. *Research handbook on digital transformations* 225-253
[16] Li J, Li N, Peng J, Cui H, Wu Z (2019) Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, Energy 168:160–168.
[17] Zheng Z, Xie S, Dai H-N, Wang H (2018) Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14(4):352-375.
[18] Bellifemine F, Bergenti F, Caire G, Poggi A (2005) JADE – a java agent development framework. *Multi-Agent Programming* Springer pp 125-147.