Protecting Manufacturing Supply Chains through PLM - Blockchain Integration and data model encapsulation

Abdelhak Belhi[1, (✉)], Abdelaziz Bouras[2]

[1] Joaan Bin Jassim Academy for Defence Studies, Al Khor, Qatar
abdelhakbelhi@gmail.com
[2] College of Business and Economics, Qatar University, Doha, Qatar
abdelaziz.bouras@qu.edu.qa

Abstract.
Product design is often a process that involves multiple parties collaborating with each other to design a final product. The involvement of multiple parties induces several risks associated with cyber security and intellectual property theft. These risks are hard to address especially in the case of traditional centralized platforms which may be prone to misconfiguration and software vulnerabilities. As a potential solution, we aim at addressing the issue of design data exchange through decentralized platforms such as the blockchain. Our solution leverages data formats that can segment product data models and gives the ability to control access to data through a decentralized platform which can be fully integrated with PLM processes through APIs. A proof of concept of this solution using the open-source Odoo PLM platform as well as the Hyperledger Fabric blockchain development platform is demonstrated.

Keywords: Product Lifecycle Management, Blockchain, Supply Chain Management, Odoo, Hyperledger Fabric

1 Introduction

Given the nature of PLM processes which involve dealing with multiple parties in most of the product lifecycle, securing the information that is shared among the parties involved has different objectives. The first and the most important is related to the protection of the product's intellectual property (IP) and this is usually two folds. On the one hand, the IP needs to be secured so that critical information is not threatened by mostly focusing on the aspects of confidentiality and integrity to the outside world. The second aspect is that some of the parties collaborating in some area of the product development might have some conflict of interest related to another area and this has indeed been the case in several legal battles between companies where for example, in a case involving two companies A and B, Company A outsourced some parts from company B to develop Product 1 and the two companies shortly found themselves in a court case of IP theft over Product 2 from Company B (Company A accused B of IP theft) [1]. For these reasons a lot of researchers dedicated efforts to developing solutions to address the security of product lifecycle processes.

In an aim to control shared product data in PLM context, in the paper, we propose a blockchain-based access control solution to control access to design data models. Our solution leverages a blockchain-PLM integration platform we developed, and adds an access control component to enable a role-based product development environment fully customizable. This solution uses a prototype we built to integrate information systems to blockchain platforms. Figure 1 below explains how our blockchain-based interaction works where all transactions between involved parties are managed by blockchain smart contracts.

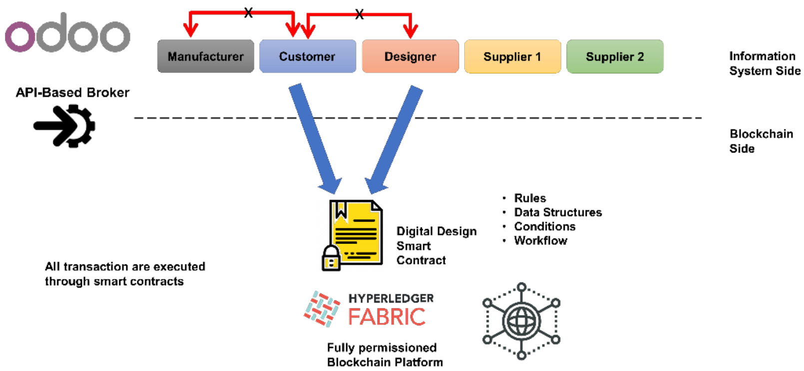

Figure 1. Blockchain-Integration scenario with supply chain: the Odoo Hyperledger Fabric Integration

The rest of this paper is organized as follows. In section two, we present a review of works related to access control in product data models as well as the uses of blockchain in industrial applications. In section three, we present the methodology of our data model access control through blockchain integration, and in section four, we present our proof-of-concept blockchain-based access control approach and discuss its strengths and weaknesses. We draw our conclusion in section five and give some future work perspectives.

2 Related work

2.1 Encapsulation and access control on data models

From an access control point of view, multiple contributions had the goal to address concerns related to permissions. The authors of [2] proposed a role-based technique for the visualization of CAD models using security policies and innovative methods to reduce the fidelity of product component drawing to protect intellectual property. In [3], the authors use a similar approach but focus on providing users with more levels of access control rather than granting or denying access. This is achieved by reducing the fidelity of 3D models. A lot of approaches investigate the use of encryption to enforce access control in collaborative CAD environments. The authors of [4] propose two encryption approaches for CAD data focusing mainly on efficient 3D data compression and cryptanalysis resistance. In [5], a new parametric approach for CAD model encryption in cloud environments is proposed. The authors use an approach they call Enhanced Encryption Transformation Matrix to alter the structure of CAD models. Similar approaches relying on 3D model tampering were proposed in [6–8]. Although these model tampering approaches are innovative, traditional approaches for access control to CAD data are the most realistic and better suited for production environments. Most of these approaches [3, 9, 10] consider the fragment of the design data and applies access control policies on these fragments so that users with different roles can access assigned fragments.

2.2 Integration of Blockchain and Enterprise information systems

Blockchain integration was investigated in many contributions focusing on multiple aspects of collaboration in industrial applications. As an example, the authors of [11] proposed an empirical study that focuses on blockchain integration in the contexts of manufacturing and operation management. They depicted a detailed evaluation of the different disadvantages preventing effective blockchain integration. In [12], IoT and machine learning integration with blockchain were studied to improve smart manufacturing quality control. The authors of [13], proposed a new productivity improvement application based on blockchain in the context of auto manufacturing and spare parts manufacturing. In [14], the authors investigated the blockchain and supply chain integration impact on additive manufacturing. In a more practical fashion, in [15], the authors presented Block-SC, a new blockchain service for cloud manufacturing with the goal of establishing a service composition collaboration platform. In the context of manufacturing, the authors of [16] proposed an architecture based on blockchain for cyber-physical systems. The authors of [17] presented a shared-manufacturing blockchain-based framework. This framework enables resource sharing in a peer-to-peer fashion whilst maintaining trust using a consensus mechanism based on proof-of-participation and smart contracts [12].

Numerous applications in the supply chain management context were proposed. The authors of [18] proposed a blockchain and supply chain integration model. In [19], a blockchain-based supply chain is developed where the authors investigated the use of ontologies and design tools to translate traceability information to enforce domain constraints in smart contracts.

Blockchain technology was used by the authors of [20] to design an industrial platform with a product-centric information system used as a backbone.

In [21], the authors presented a blockchain integration study in the context of the aircraft parts supply chain. Beyond traceability, Blockchain was used to monitor performance and parts usage, thus impacting positively data integrity as well as safety.

In the era of Industry 4.0, emerging technologies such as IoT, cloud manufacturing, AI, and blockchain are making smart manufacturing a reality. To improve supply chain efficiency and attain business innovation, blockchain is adopted by big manufacturers such as Ford and BMW.

Blockchain is a secure and efficient platform that has multiple benefits and can be used for improving collaborative applications. However, its integration requires a lot of work in terms of development and integration. This technology received a lot of attention and interest in the context of manufacturing and supply chains as it enables a large variety of applications and introduces peer-to-peer trust [22].

3 Methodology

From a high-level standpoint, our solution consists of integrating blockchain technology with PLM systems and handling critical processes and confidential data through the blockchain platform. Both platforms will communicate with each other using an API broker. The data models' access control will be handled by blockchain smart contracts and for our proof of concept, we aim to mainly investigate the feasibility as well as the impact of blockchain-based access control in PLM data models.

3.1 Solution Idea

To address confidentiality and access control concerns to PLM systems' data, we propose to use a blockchain platform to serve as a secure and efficient alternative to traditional relational databases often used by PLM systems and enterprise information systems. In traditional and cloud-based PLM systems, data is often centralized in databases or cloud storage buckets. This approach has several disadvantages related to security, availability, tamper-proofness and access control. Our solution integrates permissioned blockchains with PLM systems to handle collaborative data in a decentralized paradigm. Blockchain will be used to store PLM transaction data as well as to handle these transactions using smart contracts. Additionally, the novelty in our approach comes in the form of enforcing access control policies to all the data present in the blockchain in multiple formats focusing mostly on formats directly related to product design such as CAD and mostly all portable documents. The access control module we integrate into our earlier prototype [23–25] serves as a blockchain-based reference that manages role-permission associations to PLM process assets meaning data visibility as well as actions permissions. Figure 3 highlights the overall architecture of our solution.

Due to the nature of the blockchain platform and given that the system data is present at all nodes, the need to enforce access control is tightly associated with data confidentiality. Thus, in our solution, encryption is used to enforce data visibility. Actors having the rights to a certain category of information (a role) will have keys to this information associated with their blockchain wallet.

3.2 Design and Implementation

Our solution is centered around the Odoo PLM as well as the Hyperledger Fabric Blockchain platform. The two platforms are mainly chosen due to their functionalities as well as being open source, thus allowing the maximum level of customization.

Odoo PLM focuses mostly on the lifecycle aspects of PLM but unfortunately does not allow the ability to preview advanced design models such as CAD models or portable documents. We thus had to integrate web-based plugins into Odoo in order to allow the visualization of these data models inside Odoo.

Although in the case of CAD, the interface only allows viewing the files, we aim in the future to integrate it with CAD editors such as CATIA, SolidWorks, and Revit.

Figure 2 below represents a laptop manufacturing scenario where several actors have to access different parts of the laptop design specifications. In this scenario, and to secure the data encapsulation, we leverage a blockchain-based solution through smart contracts to manage the access control to different design data depending on the role of the actor.

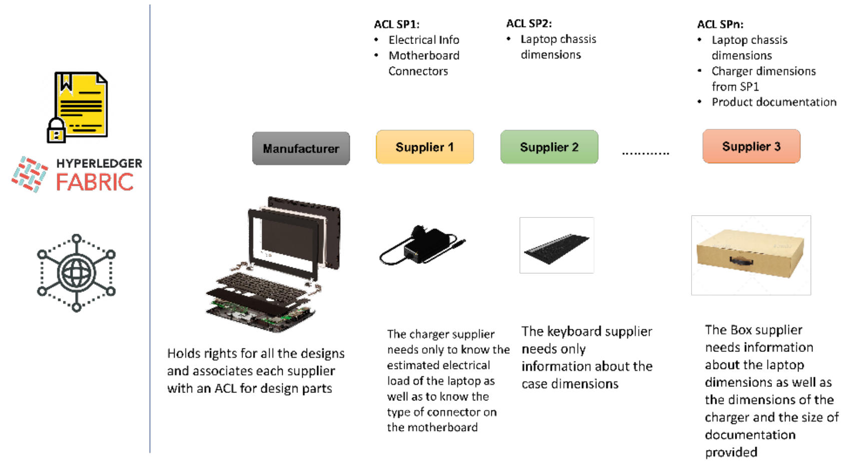

Figure 2. A Collaborative PLM Process with different levels of access to data models

Blockchain – Odoo Integration

All communication between Odoo and HyperLedger fabric is managed through a broker component. This broker is implemented in Node.JS and its main task is to transmit transaction data back and forth between the platforms. It relies on the HyperLedger Fabric JavaScript SDK for the connection to the blockchain network. To allow reliable and secure communication between the two systems, a RESTful API is used for data and transaction transfer. Client interfaces such as our Odoo interface or a mobile logistics app (developed for real-time asset tracking for the Transporter actor) use this API to connect to the blockchain network through the broker.

Data model access control

Realistically, we cannot focus on all data models, but we can prepare scenarios for the most used format in PLM. Our main idea behind this solution is that for a given product, the parties collaborating for its development focus on certain aspects of the product only. And thus, restricting access to the parts which are not needed is better from an Intellectual property standpoint to avoid issues such as the one highlighted in [1]. As proof of concept, we implement file-level access controls in our solution. In this scenario, we assume that for a given product, each major aspect of its design is represented by a design file (a CAD model). Each actor in the PLM network will then be assigned access rights to the parts he has privileges on. We achieve this by implementing an Odoo data model that is fully controlled by a blockchain smart contract. This model incorporates access control features for all the data files as well as the associated files. Securing access can be through visibility, meaning hiding the related parts from unauthorized users, or by encryption. When a user attempts to view a given part, the blockchain-based reference manages checks the user's privileges on that part and then either send him the data or the encryption keys. The users identity verification aspects are fully managed by the Hyperledger platform which provide excellent certificate-based identity management.

In the future, we aim at using formats that allow for inner encapsulation through encryption such as formats based on OBJ, etc., or by using approaches similar to the ones discussed in section two where the data is encrypted using different methods. By doing this, we ensure that a single model can be used to represent the product and can allow for different access levels securely.

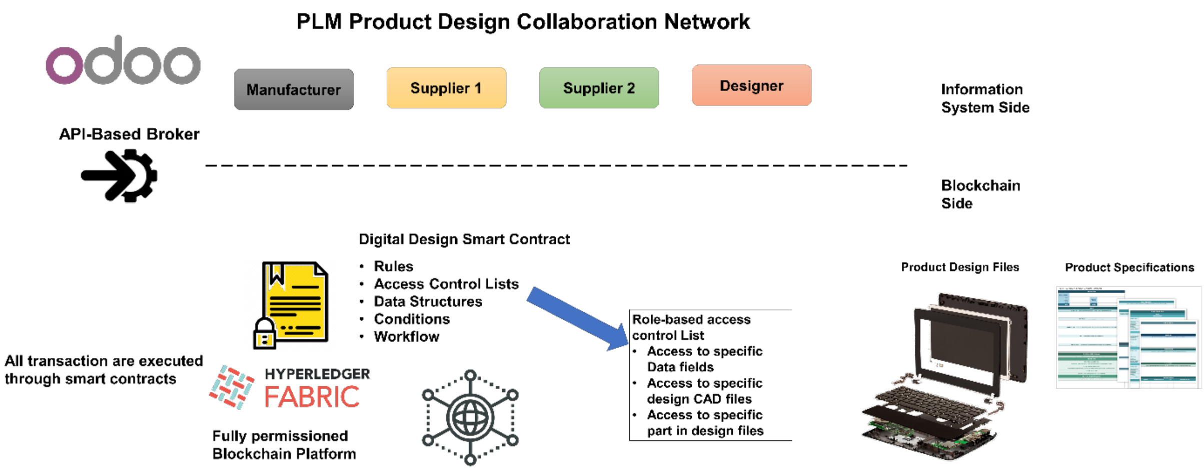

Figure 3. Blockchain-based PLM data models access control

4 Results and discussions

To evaluate and validate our proof-of-concept, we implemented a small collaborative design scenario involving one manufacturer and multiple suppliers. The scenario interface was implemented on Odoo using Python. All data handling and transaction management was shifted from Odoo to the blockchain through smart contracts. The scenario we investigate involves a laptop as a product and the manufacturer sets up a network with a different supplier for the parts. For each part, a 2D and a 3D data model is associated, and an access control list ACL specifies which other suppliers have the rights to see the data models. The access control list can be updated dynamically. We, unfortunately, could not cover partial access control due to the nature of the data models we

used. We aim in the future to investigate using specific file and data formats to allow for more granularity in access control.
For our scenario, Figure 4 represents a warning message for an unauthorized user trying to view a data model to which he has no rights. The data model will be hidden.

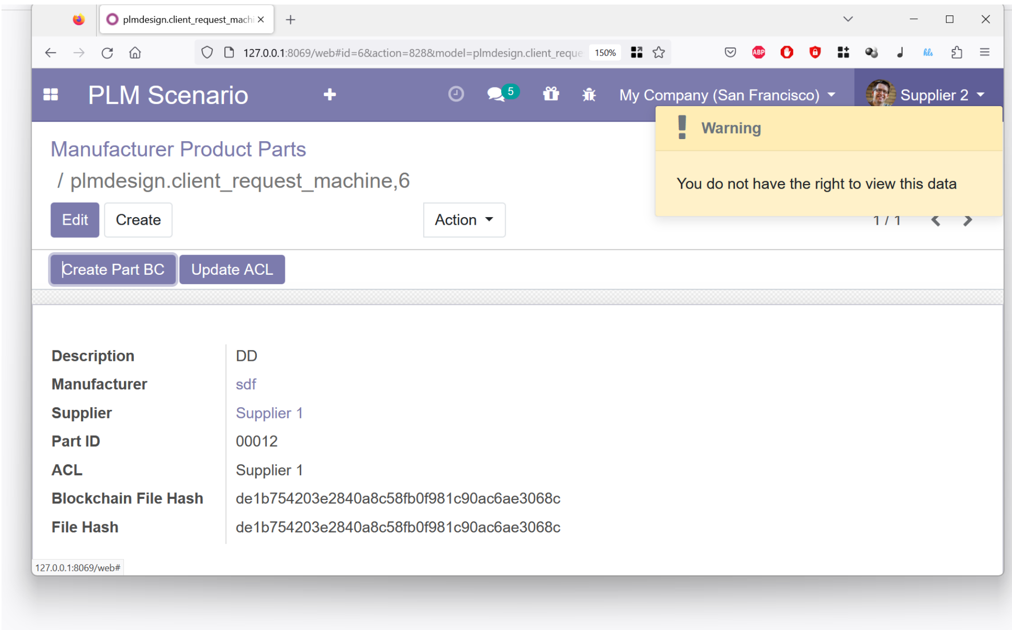

Figure 4. Access Control enforcement scenario through blockchain integration

Figure 5 shows a screenshot of a user viewing a data model in 2D and 3D for a part he has the right to see.

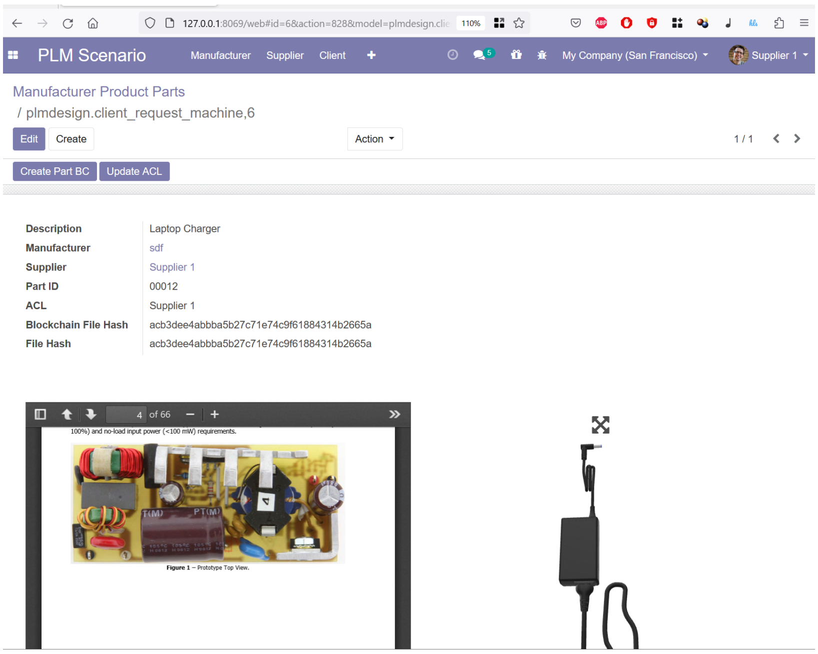

Figure 5. A product component (Laptop charger example) with PDF and 3D data models + Blockchain-based access control

Figure 6 shows the interface of the manufacturer where he can add suppliers and parts to a product design while assigning dynamic access control rights (see Figure 7).

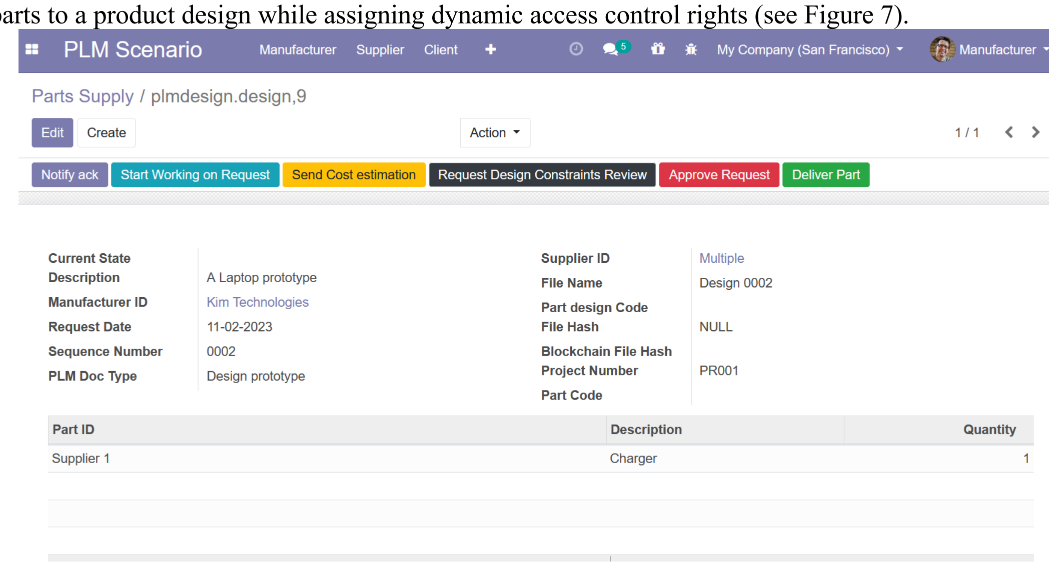

Figure 6. Main product page and parts list (BOM)

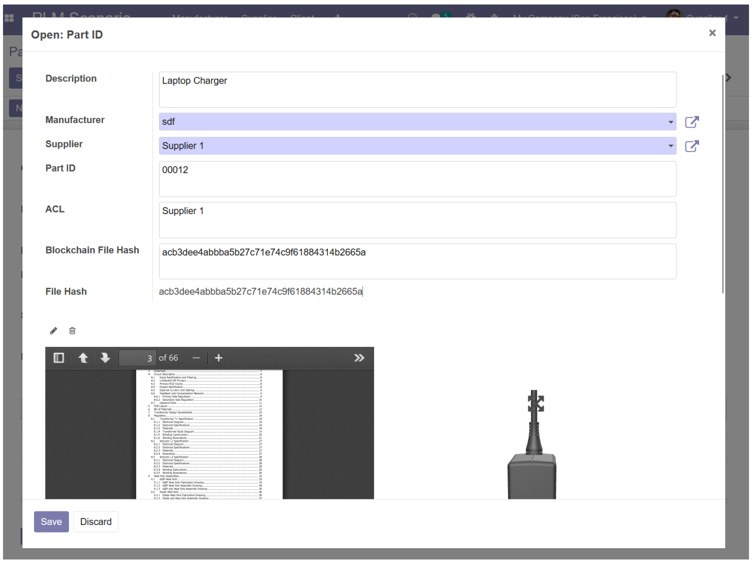

Figure 7. Editing a given design part

Figure 8 and Figure 9 show the blockchain log before and after an update to the access control lists ACLs.

Figure 8. Blockchain log for supplier part request smart contract

```
{ contractId: 'part6' }
Wallet path: /home/a/fabric-samples/fabcar/javascript/wallet
Transaction readDesignContract has been evaluated, result : {"ID":"part6","Supplier_id":"4","Manufac
turer_id":"1","Item_id":"00012","Description":"DD","ACL":"Supplier 1, Supplier 5, Supplier 6","File_
hash":"de1b754203e2840a8c58fb0f981c90ac6ae3068c"}
{
  ID: 'part6',
  Supplier_id: '4',
  Manufacturer_id: '1',
  Item_id: '00012',
  Description: 'DD',
  ACL: 'Supplier 1, Supplier 5, Supplier 6',
  File_hash: 'de1b754203e2840a8c58fb0f981c90ac6ae3068c'
}
-------------- Part Request Contract --------------
Id : part6
Supplier_id : 4
Manufacturer_id : 1
Item_id : 00012
description : DD
ACL : Supplier 1, Supplier 5, Supplier 6
currentFileHash : de1b754203e2840a8c58fb0f981c90ac6ae3068c
---------------------------------------------
```

Figure 9. ACL update blockchain log

5 Conclusion

Blockchain's impact on manufacturing and industrial applications was compared by some people to the wheel invention. This disruptive technology showed its potential in revolutionizing product design and manufacturing in many ways. In this paper, we investigated a new aspect of blockchain integration with industrial applications related to the access control of data models. We used Hyperledger Fabric as a permissioned blockchain platform to store the transaction data and manage the lifecycle of smart contracts. Hyperledger Fabric was mainly selected as it is an open-source platform used extensively in the product development environment. As for the information system, we used Odoo which is an open-source framework written in Python. Our access control approach assumes that for a given part of a product, an access control list is associated to allow actors in the network to view the part specification depending on their needs. Our approach relies fully on the blockchain to manage transactions between actors as well as to enforce access control for product parts data models. Although it would have been more beneficial to allow more granularity when setting access control policies for certain fields or areas in data models, in the future, we aim to address this aspect using advanced file format and data models.

Acknowledgment

This publication was made possible by NPRP grant NPRP11S-1227-170135 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors (www.supplyledger.qa).

References

1. Saardchom, N.: Design Patent War: Apple versus Samsung. (2014). https://doi.org/10.1177/2277977914548341.
2. Cera, C.D., Kim, T., Han, J.H., Regli, W.C.: Role-based viewing envelopes for information protection in collaborative modeling. Comput. Des. 36, 873–886 (2004). https://doi.org/10.1016/J.CAD.2003.09.014.
3. Qiu, Z.M., Kok, K.F., Wong, Y.S., Fuh, J.Y.H.: Role-based 3D visualisation for asynchronous PLM collaboration. Comput. Ind. 58, 747–755 (2007). https://doi.org/10.1016/j.compind.2007.02.006.
4. Elsheh, E., Ben Hamza, A.: Secret sharing approaches for 3D object encryption. Expert Syst. Appl. 38, 13906–13911 (2011). https://doi.org/10.1016/J.ESWA.2011.04.197.
5. Cai, X.T., Wang, S., Lu, X., Li, W.D., Liang, Y.W.: Parametric and adaptive encryption of feature-based computer-aided design models for cloud-based collaboration. Integr. Comput. Aided. Eng. 24, 129–142 (2017). https://doi.org/10.3233/ICA-160535.
6. Cai, X.T., He, F.Z., Li, W.D., Li, X.X., Wu, Y.Q.: Encryption based partial sharing of CAD models. Integr. Comput. Aided. Eng. 22, 243–260 (2015). https://doi.org/10.3233/ICA-150487.
7. Liang, Y., He, F., Li, H.: An asymmetric and optimized encryption method to protect the confidentiality of 3D mesh model. Adv. Eng. Informatics. 42, 100963 (2019). https://doi.org/10.1016/J.AEI.2019.100963.
8. Cai, X., Li, W., He, F., Li, X.: Customized encryption of computer aided design models for collaboration in cloud manufacturing environment. J. Manuf. Sci. Eng. Trans. ASME. 137, (2015). https://doi.org/10.1115/1.4030592/375274.
9. Fabian, B., Kunz, S., Konnegen, M., Müller, S., Günther, O.: Access control for semantic data federations in industrial product-lifecycle management. Comput. Ind. 63, 930–940 (2012). https://doi.org/10.1016/J.COMPIND.2012.08.015.
10. Kim, T., Cera, C.D., Regli, W.C., Choo, H., Han, J.: Multi-Level modeling and access control for data sharing in collaborative design. Adv. Eng. Informatics. 20, 47–57 (2006). https://doi.org/10.1016/J.AEI.2005.05.016.
11. Lohmer, J., Lasch, R.: Blockchain in operations management and manufacturing: Potential and barriers. Comput. Ind. Eng. 149, 106789 (2020). https://doi.org/10.1016/j.cie.2020.106789.
12. Shahbazi, Z., Byun, Y.-C.: Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing. Sensors. 21, 1467 (2021). https://doi.org/10.3390/s21041467.
13. Hasan, H.R., Salah, K., Jayaraman, R., Ahmad, R.W., Yaqoob, I., Omar, M.: Blockchain-Based Solution for the Traceability of Spare Parts in Manufacturing. IEEE Access. 8, 100308–100322 (2020). https://doi.org/10.1109/ACCESS.2020.2998159.
14. Kurpjuweit, S., Schmidt, C.G., Klöckner, M., Wagner, S.M.: Blockchain in Additive Manufacturing and its Impact on Supply Chains. J. Bus. Logist. 42, 46–70 (2021). https://doi.org/10.1111/jbl.12231.
15. Aghamohammadzadeh, E., Fatahi Valilai, O.: A novel cloud manufacturing service composition platform enabled by Blockchain technology. Int. J. Prod. Res. 58, 5280–5298 (2020). https://doi.org/10.1080/00207543.2020.1715507.

16. Lee, J., Azamfar, M., Singh, J.: A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. Manuf. Lett. 20, 34–39 (2019). https://doi.org/10.1016/j.mfglet.2019.05.003.
17. Yu, C., Jiang, X., Yu, S., Yang, C.: Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. Robot. Comput. Integr. Manuf. 64, 101931 (2020). https://doi.org/10.1016/j.rcim.2019.101931.
18. Francisco, K., Swanson, D.: The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics. 2, 2 (2018).
19. Kim, H.M., Laskowski, M.: Toward an ontology-driven blockchain design for supply-chain provenance. Intell. Syst. Accounting, Financ. Manag. 25, 18–27 (2018).
20. Mattila, J., Seppälä, T., Holmström, J.: Product-centric information management: A case study of a shared platform with blockchain technology. (2016).
21. Madhwal, Y., Panfilov, P.B.: Blockchain and Supply Chain Management: Aircrafts'parts'business Case. Ann. DAAAM Proc. 28, (2017).
22. Belhi, A., Bouras, A., Patel, M.K., Aouni, B.: Blockchains: A Conceptual Assessment from a Product Lifecycle Implementation Perspective. In: IFIP International Conference on Product Lifecycle Management. pp. 576–589 (2020).
23. Belhi, A., Gasmi, H., Bouras, A., Aouni, B., Khalil, I.: Integration of Business Applications with the Blockchain: Odoo and Hyperledger Fabric Open Source Proof of Concept. IFAC-PapersOnLine. 54, 817–824 (2021).
24. Belhi, A., Gasmi, H., Hammi, A., Bouras, A., Aouni, B., Khalil, I.: TMSLedger: A Transactions Management System Through Integrated Odoo Hyperledger Smart Contracts. In: Blockchain Driven Supply Chains and Enterprise Information Systems. pp. 201–220. Springer (2023).
25. Belhi, A., Gasmi, H., Hammi, A., Bouras, A., Aouni, B., Khalil, I.: A Broker-Based Manufacturing Supply Chain Integration with Blockchain: Managing Odoo Workflows Using Hyperledger Fabric Smart Contracts. In: IFIP International Conference on Product Lifecycle Management. pp. 371–385. Springer (2021).