Transdisciplinary Engineering Methods for Social Innovation of Industry 4.0
M. Peruzzini et al. (Eds.)

doi:10.3233/978-1-61499-898-3-103

Intellectual Property Protection and Licensing of 3D Print with Blockchain Technology

Felix ENGELMANN[a], Martin HOLLAND[b], Christopher NIGISCHER[c] and Josip STJEPANDIĆ[b,1]
[a]*Ulm University, Ulm, Germany*
[b]*PROSTEP AG, Darmsadt, Germany*
[c]*NXP Semiconductors Germany, Hamburg, Germany*

Abstract. Within the "Industrie 4.0" approach, 3D printing technology is characterized as one of the disruptive innovations. Conventional supply chains are replaced by value-added networks. The spatially distributed development of printed components, e.g. for the rapid delivery of spare parts, creates a new challenge when differentiating between "original part", "copy" or "counterfeit" becomes necessary. This is especially true for safety-critical products. Based on these changes classicly branded products adopt the characteristics of licensing models as we know them in the areas of software and digital media. This paper describes the use of digital rights management as a key technology for the successful transition to Additive Manufacturing methods and a key for its commercial implementation and the prevention of intellectual property theft. Risks will be identified along the process chain and solution concepts are presented. These are currently being developed by an 8-partner project named SAMPL (Secure Additive Manufacturing Platform).

Keywords. Additive Manufacturing, Intellectual Property, License Management, Blockchain Technology, Plagiarism, RFID

Introduction

Within „Industrie 4.0“, 3D printing technology emerges as one of the disruptive innovations. Conventional supply chains are replaced by value-added networks [1]. The spatially distributed development of printed components, e.g. for the rapid delivery of spare parts, creates a new challenge when differentiating between "original part", "copy" or "counterfeit" becomes necessary [2]. Based on these changes classicly branded products adopt the characteristics of licensing models as we know them in the areas of software and digital media [3]. Further, 3D printers for synthetic materials have already become very cheap, so that plagiarism and the protection against it have naturally gained the relevant importance [4].

The entry of Microsoft into that issue even strengthens this trend. Thereby, one comes to the conclusion that this process has already become commodity [5][6]. Hence, it is important that counterfeiting and protection against it will be granted the required

[1] Corresponding Author, Mail: josip.stjepandic@opendesc.com

attention, as product and trademark counterfeiting cause billions of losses to German companies [2][7].

The remainder of this paper is structured as follows: In Section 1 we present the background and basic approaches for intellectual property protection in the Addivive Manufacturing. Our approach for secure process chains in Additive Manufacturing is described in Section 2, its licensing scenario in Section 3 and its implementation in Section 4. After the description of the new built SAMPL ecosystem (Section 5), we express closing thoughts and outlook in Section 6.

1. Background

At present, the theme of plagiarism is strongly related to 3D printing. Thus, the trade association Spectaris is warning that „3D printing considerably increases the danger of plagiarism in the sector of medical technology". Even technology lawyers warn of counterfeiting risks through 3D printers [7]. In the case of falling prices for copy technologies, plagiarism risks will increase significantly.

This also means that the transfer of 3D printing design data for decentralized creation of objects is only economically viable, if there are appropriate security mechanisms and a suitable digital license management in place, that ensures fair rewarding and control over who is creating samples of the licened 3D object by the copyright holder [2][3]. Local manufacturing of additively produced components aggravates this, as customs control becomes more difficult. New business models, such as spare part manufacturing by 3D printing, lifts the risk of plagiarism to a new dimension [8].

The integration of Additive Manufacturing procedures into the production process and the complete product life cycle rises significant challenges regarding authorized access to product data, assured supply of the agreed quantity, distinction of original parts from counterfeits as well as prevention of intellectual property, product liability and warranty [2][3].

Copyright in the consumer area, according to §53 Copyright Law, also applies to parts additively manufactured by the end-user and allows copies for private use without the agreement of the author [9]. Originals from other authors - such as templates from the internet - may as well be printed. However, a few conditions have to be taken into account: The number of copies must not exceed a maximum 7 copies, which can be passed on to friends and relatives free of charge. But the printer operator may not receive remuneration for the printed pieces, as the parts otherwise would then be sold for profit, being plagiarism. Furthermore, the copy may not originate from an obviously illegal source [9].

Unlike the rights for private use in the consumers' sphere, These practices may quickly become a risk factor in the B2B field. It is important to address the questions of IP- and counterfeit protection and take corresponding protective measures [2]. Although there will never be a 100% protection, the barrier has to be set as high as economically justifiable for the copyright holder, such that it is not financially profitable for a pirate to produce counterfeits [10]. The subject of counterfeit protection is to be bound into a company-wide concept for product and know how protection [11]. Measures for counterfeit protection can be divided in four categories (internal security, external security, product labelling and legal safeguards) [12]. In particular, the external security analysis reveals a few highly sensitive points for attacks [2] with the risk of total loss (Table 1) where the external partner gets the access to almost all the data.

Table 1. Attackpoints along the process chain of Additive Manufacturing.

Process step	Result	Point of Attack	Impact
CAD design	CAD model	Modification of CAD model	Impact to product capabilities, quality and function
		Copy of CAD model	Arbitrary use; not prepared for print
Adaption of CAD model, addition of support geometry, voids	CAD model ready for print production	Modification of CAD model	Impact to productability, quality and function
Creation of 3D print data e.g. STK, AMF, 3MF	File ready to print	Modification of file	Impact to quality and function
		Copy of file	Arbitrary printing with high risk due to the missing process data
Creation of process data	Process data in a file	Modification of process data	Impact to quality and function
Agglomeration of process and 3D print data	Fully print data	Copy of file	Arbitrary printing with highest risk

Special attention regarding the usability in court has to be paid when selecting the right procedure for an individual application. Usability in court means recognition and admission of a procedure by the court. This might be a crucial factor in case of a defence against a product liability claim or against unjustified warranty claims [11].

Within the additive manufacturing process chain, the preparation of a geometry, determination of the process parameters or manufacturing of components is often done by external partners with whom the copyright questions have to be answered. In the case of a service provider preparing the geometry model for printing and subsequently creating the print template with a slicing software, he may eventually have created a work according to copyright law, §3 section 1 No. 1 or No. 7. The author is then granted the protection by preparing the file. Thus, to protect the work, it does not have to be registered. The conditions required to classify it as authentic work is, that it has to be created by a human and also requires an "intellectual creation" [9].

In this case, the resulting work must not be copied and distributed without approval of the copyright holder. Public availability needs the approval of the author as well. Furthermore, the original product manufacturer could be restricted of amendments to the prepared geometrical model. Thus, the rules for the legal boundary conditions must be defined clearly when entrusting service providers with the creation of a print template, because printing a template means copying it. As the reproduction rights are based on §16 copyright law, printing means copying, because the work – the template – is made perceptible as a physical object. The work itself is not changed thereby, but merely the form of expression. Thus, the number of printed works does not matter, already the first workpiece is a copy of the template. The reproduction right according to §16 Copyright Law is the main standard for the manufacturing of the workpieces. In case the printing file is passed on to a service provider for production, he has no property rights with regard to the protected work. In case of the mere process of the printing order, the intellectual creation is missing [9][2].

When registering a 3D brand name it has to be considered that the form distinguishes itself by special aesthetic features from others and, secondly, that it is not only required to reach a technical effect but as well as an aesthetical. Lego, for example, did not succeed by arguing that the clamping effect of toy bricks could as well be reached by a different construction and design of the coupling elements (nubs) without qualitative, technical, functional or economical benefit against those having been built differently [13]. In contrast, the classical Cola bottle or Toblerone chocolat are registered 3D trademarks.

2. Our Approach: Secure Process Chains for Additive Manufacturing

Owing to the special features in Additive Manufacturing, in particular 3D printing, a „Chain of Trust“ is currently in widespread discussion. The idea is to reduce risks to a minimum by using the according technologies. At present, there are different, primarily cryptographic approaches to secure the authenticity of printing data and prevent unauthorized use of it [4].

Encoding and licensing of data by using Blockchain Technology provides an opportunity. The relevant data is encoded and the identification of the print template and the licensing of the printing process is done by means of Blockchain Technology. So far, this is mainly known from the finance world. It is a cryptographic procedure to proof the authenticity of financial transactions at digital payment. A specific Blockchain Application, for example, is the cryptocurrency Bitcoin. Blockchain Technology, however, may basically be used as well for the application of transactions in terms of franchising. Instead of Bitcoins, the license allows to print a certain number of a component.

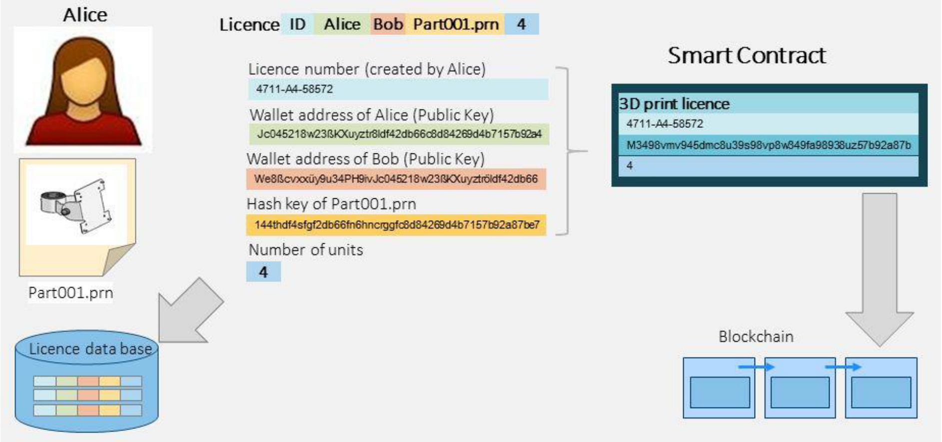

Figure 1. Licence Information pictured by means of Blockchain-Technology.

Figure 1 displays how to represent the transaction „Alice authorizes Bob to print four copies of a certain product“ in a Blockchain. A so called Smart Contract files the license information in the Blockchain and secures that only the receipient, Bob, has the permission to update the license, e.g. register a printer part to it. Later, Bob‘s printer verifies the license before starting to print. Additionally, the serial numbers of the separately printed components can be written into the Blockchain to proof type and quantity having been printed in accordance with the license terms [4].

To completely close the Chain of Trust, the machine and automation suppliers have to be taken into account. Similar concepts as those of manufacturing copiers can be realized. Like copying money is being prevented by the installation of so called Secure Elements into machines for Additive Manufacturing, trusted printers communicating with the Blockchain are realized. Thereon, you can build up a complete Chain of Trust from copyright holder to service provider [14][15]. Other ways to improve Trademark Protection are certified partners and the use of trusted printers ("Block-Chain Ready") [4].

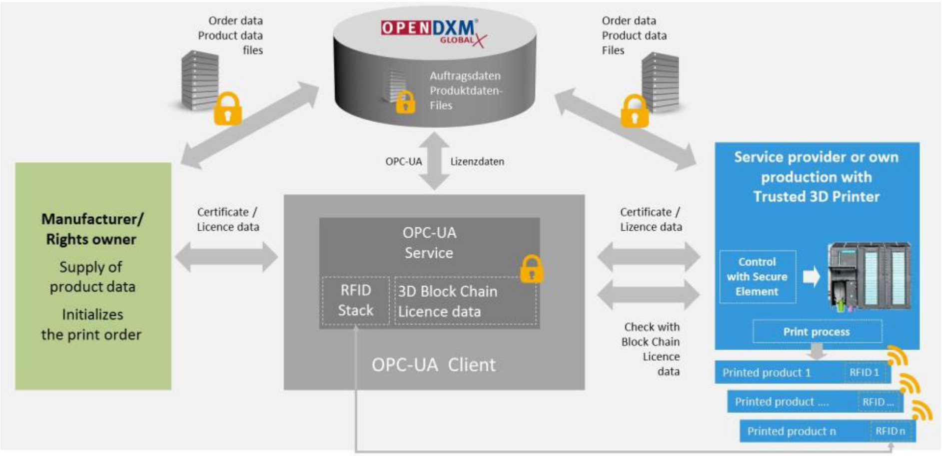

Figure 2. SAMPL System Architecture.

The project Secure Additive Manufacturing Platform (SAMPL) aims at developing consistent Chains of Trust for Additive Manufacturing Procedures for a commercial purpose. The entire process is seen – from development of digital 3D printing data via the exchange with a service provider of 3D printers trusted by specific secure elements up to labelling of printed components by means of RFID-Chips. In addition to the available encoding mechanisms, a digital license management based on Blockchain Technology will be integrated into the data exchange solution OpenDXM GlobalX of PROSTEP AG. The interface for the exchange of certification and license data between copyright holder and receiver is Industry 4.0 Standard OPC-UA. Figure 2 illustrates the System Architecture [4].

3. Licensing scenario

In our scenario with several untrusted participants, we need a consensus about existing licenses and their ownership. The the trust is modeled as follows. The customer, the printing service provider and the licensee do not trust each other. It is necessary to ensure that in case of a dispute, the licenser can verify whether a part has been printed with a valid license from him in order to provide warranty claims for the object design. Subsequently, when receiving the part from the printing service provider, the customer wants to be able to verify that the received part has been manufactured with a valid license in order to prove this to the licensor. In between, there is the printing service provider, who needs a hedge against the licensor, so that in case of a dispute, he can prove exactly which 3D model he has received to print. The quality management of the printing service provider is responsible for the check whether the produced part meets the requirements after printing and to bind the license exactly to this part. Provided that the parts are clearly identifiable, the same license cannot be assigned to multiple parts.

Our smart contract on an Ethereum Virtual Machine compatible Blockchain enforces the correct execution of these transactions. In the beginning, it must be determined who owns the design and whether the part has already been licensed by someone else. Basically, as a metric of equality of designs, we use a cryptographic fingerprint (hash code) of the file. A small modification of the file, which does not even have to affect the model itself, alters this fingerprint, so it would be possible to re-register the same model. Several works [16][17][18][19] deal with the similarity of models, however, the implementation of the comparison as a smart contract is very computationally intensive and therefore expensive. Also, the algorithm must be completely deterministic and must not use heuristics, otherwise they can be bypassed on purpose.

Once a customer buys a license from an owner, this can be done atomically on the Blockchain by exchanging the cryptocurrency for a license token. This ensures that none of the parties withdraws prematurely from the transaction. The customer gets the license only if he has already paid, and the licensor must transfer the license as soon as he has received the money. For example, the licensor cannot receive the payment and disappear afterwards. Once a license has been acquired, it can be "sold" by the customer to a print service provider. From that moment, the relationship of trust is expanding to the physical world and there is no immediate service in return. The license can then be transferred to the print service provider, for example with a time lock. The provider will not be able to resell the license and if it is not printed within the specified time, it will be returned to the customer. The Blockchain has a global time which enables the verification of the license by the Smart Contract, and once the time has expired, the customer can again claim ownership of the license.

Once the printing service provider has a license, he can download the corresponding CAD file. Often and especially in metal printing, it is necessary to make non-deterministic changes to the model to obtain optimal results. These cannot be understood by the smart contract. Therefore, the quality management of the print service provider must serve as an oracle after printing, to authoritatively confirm on the Blockchain that a part was manufactured correctly. This step is done with the clear identification of the part, for example with a tamper-resistant chip.

The identification of singular parts is then bound in a process to a license token. This process is not revocable by the smart contract. After receiving the part, the customer can look up in the Blockchain, whether the part has been registered for a license.

To completely close the Chain of Trust, the inclusion of the machines and control-manufacturers is necessary. In this way, similar concepts, as they are already used in the production of copiers, can be realized. Similar to how the copying of banknotes is prevented, suitable trusted printers can be realized by installing so-called secure elements in machines from the additive manufacturing sector, which then communicate with the Blockchain. In this way, a complete Chain of Trust can be built up from the rights holder through the print service provider to the licensee. In addition to the certification of a partner, the use of certified printers ("block-chain ready") is an additional way to put plagiarism protection to the next level.

4. Implementation

As basis for implementation, the Ethereum Blockchain has been selected, which offers many software tools in good quality and documentation as well as the option to map complex workflows with smart contracts in the Blockchain. Licensor and licensee record the licensing and the license consumption in the Blockchain. This is done through transactions whereof the signature is secured by a public/private-key procedure based on the industry standard ECDSA (Elliptic Curve Digital Signature Algorithm). Both licensor and licensee each have a private key, which is stored in a wallet and serves for creation of the signature. For the location of these wallets there are two options, which are both implemented in the current software:

- The central wallets, managed by a lightweight component called Secure Printing Bridge (SPB). Advantages are the easier installation and administration as well as protection against losses of the wallets. Disadvantages are the reduced privacy and the increased risk of unauthorized access by third parties.
- The decentral wallets, managed directly by licensor resp. licensee. This brings improved privacy and protection, but an increased risk of loss. In addition, this model increases the demands on the software, which runs at the partner site and, in particular, on the printer.

The existing GUI clients of OpenDXM GlobalX have been extended with new user interface functions to consider the use cases of licensing (e.g. generation and display of license). The internal and external service interfaces were adapted to support the license management integrated with the Blockchain implementation. For this purpose, the data model of OpenDXM GlobalX has been extended to map the license info and the assignment of GlobalX objects to the Blockchain transactions in the system.

5. Business development by SAMPL ecosystem

Blockchain already has become a disruptive field of business development. After several years of implementation, eight categories of Blockchain projects have been formed [20]. According to this, our application falls into the category “Shared Data”, which comprises the use of Blockchain – among others – in supply chains. Initial Blockchain efforts could have quick impact by transforming even a small portion of the supply chain, such as the information needed for the individual, decentral manufacturing of spare parts instead of gathering dust in warehouses waiting to be used. Typically, markets that have been most attractive for intermediary aggregators are those in which there is a significant barrier to entry in competing directly, but whereby technological advances have created a catalyst for an intermediary to aggregate incumbents, related metadata, and consumer preferences [20]. There are many similar possibilities, as the “open data platform” has been a popular startup idea for a few years now with several companies finding great success with this model. Because business rules and smart contracts can be built into the platform, a Blockchain ecosystem can evolve as it mature to support end-to-end business processes and a wide range of complementary activities.

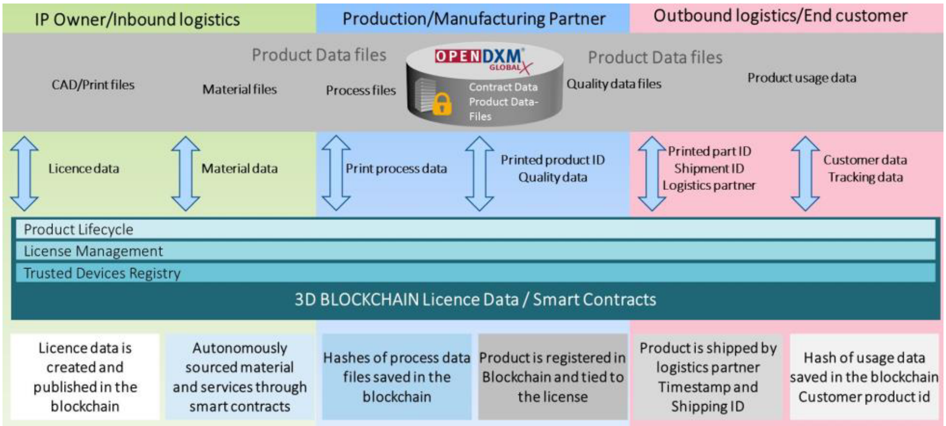

Figure 3. SAMPL extended ecosystem.

Similarly, it is planned to build and gradually extend a corresponding ecosystem for the outcome of SAMPL. By segmenting use cases and end-users, we can gain a better understanding of Blockchain's actual potential. One of the most important measures is the constitution of a project group in the prostep ivip Association to conduct and promote harmonization and standardization activities. The approaches pursued by the demonstrated system architecture aim to develop concrete potential uses for a number of stakeholders in the SAMPL extended ecosystem (Figure 3) based on recent regulation by law [21]:

- Printer manufacturers: Distinguishing Feature „trusted“ 3D printer, integration of a module for copyright protection enables hedge for service provider and user. A service provide can claim the usage of trusted 3D-printers.
- Author/IP owner: IP protection, prevention from pirate copies, make rights enforceable, traceability of use, pricing dependant on usability [2].
- Original Equipment Manufacturer (OEM): secure on-demand-production, reduction of storage and transport costs, lower capital binding, quality guarantee, optimized spare parts distribution, defence against unjsutified product liability or guarantee claims [22].
- Printing Service Provider: reduced transaction costs by using trusted 3D printers, support services on quality control, legal security and competitive advantage [2][23].
- Final Customer: verifiable authenticity, protection against design manipulation, precise and secure billing, confidence in the work, advantages with guarantee claims [2][23].

Further apllications of the developed approach are planned in the following areas of engineering: documentation of the production maturity status of a ship in a shipyard, truck platooning on the highway, sharing test data for autonomous driving, autonomous car software update, wireless remote Blockchain-based software update, speed-up containers.

6. Conclusions and Outlook

In digital transformation, within the area of Additive Manufacturing, comprehensive research is conducted on the topics of process management, technologies and methods [6]. Extensive research concepts on information security, license management, copyright protection and proof of authenticity, however, are still strongly underrepresented [14][24]. In digitalization and networking, products and production have to be granted a dominant role with regard to the security of the entire system and the risk management [25].

At present, there is no known commercial platform which is required to digitally and treaceably administrate data relevant for 3D printing taking into account digital licenses. This gap is going to be filled by an integration of the SAMPL Platform and a 3D printing Blockchain.

Saving and administrating digital licenses requires a database ensuring the long-term stability of its entries. However, saving new license transactions such as updates of digital versions or changes in ownership are to be made possible. Having proven highest demands in terms of reliability and security with its first big implementation as a basis for the cryptocurrency Bitcoin, Blockchain-Technology offers that kind of register.

The enlargement of the Chain-of-Trust via the 3D printer control into the printed product, e.g. via integration of RFID Chips, represents an interesting option for the organization of future business models culminating in the connection of any product with a digital product memory [26][27][28]. Thus, all 3D printed and RFID-tagged components could be smart products throughout the lifecycle. For example, the evaluation of product use, the analysis of typical damage patterns or repair requirements could lead to a targeted development and improvement. The control circuit, nowadays not closed at many products, could be closed across the product life cycle and, thus, allow new innovations [29][30].

Finally, besides of 3D printing, further areas of application have been identified in shipbuilding, sharing of test data, software update and transportation.

Acknowledgement

The research project “Secure Additive Manufacturing Plattform (SAMPL)” is supported by the German Federal Ministry of Economy (BMWI) within the Framework Concept ”Digitale Technologien für die Wirtschaft (PAiCE)”. Authors are responsible for the contents of this publication.

References

[1] M. Borsato and M. Peruzzini, Collaborative Engineering, in: Stjepandić J. et al. (eds.): *Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges*, Springer International Publishing Cham, 2015, pp. 165–196.

[2] J. Stjepandić, H. Liese and A.C. Trappey, Intellectual Property Protection, in: Stjepandić, J. et al. (eds.): *Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges*, pp. 521–552, Springer International Publishing Cham, 2015.

[3] A. Biahmou and J. Stjepandić, Towards agile enterprise rights management in engineering collaboration, *Int. J. Agile Systems and Management*, Vol. 9, 2016, No. 4, pp. 302–325.

[4] M.Holland, SAMPL Secure Additive Manufacturing Platform; Unter: https://www.tuhh.de/fks/010_research/projects/sampl/de/index.html, Darmstadt, 2016.
[5] S. Yang, Y. Tang and Y. F. Zhao, A new part consolidation method to embrace the design freedom of additive manufacturing, *Journal of Manufacturing Processes*, 20 (2015), pp. 444–449.
[6] T.W. Simpson, C.B. Williams and M. Hripko, Preparing industry for additive manufacturing and its applications: Summary & recommendations from a National Science Foundation workshop, *Additive Manufacturing*, 13 (2017), pp. 166–178.
[7] M. Holland, C. Nigischer and J. Stjepandić, Copyright Protection in Additive Manufacturing with Blockchain Approach, in: C.H. Chen et al. (eds.) *Transdisciplinary Engineering: A Paradigm Shift*, IOS Press, Amsterdam, 2017, pp. 914-921.
[8] M.-K. Sini, Spare parts go digital: a boost for the industrial spare parts business, VTT Technical Research, 2017, http://www.vttresearch.com/media/news/spare-parts-go-digital, accessed Feb, 8 2018
[9] A. Lott, Urheberrecht beim privaten 3D-Druck – Plagiat oder Privatkopie?"; Aktuelles Wirtschaftsrecht; Hochschule für Wirtschaft und Recht; Berlin; https://wirtschaftsrecht-news.de/2016/01/urheberrecht-beim-privaten-3d-druck-plagiat-oder-privatkopie/; Berlin; Accessed, Jan, 8 2016.
[10] H. Liese, S. Rulhoff and J. Stjepandić, Securing product know-how by embedding IP-protection into the organisation, *2010 IEEE International Technology Management Conference*, ICE 2010, 2010.
[11] Leitfaden zum Produkt- und Know-how-Schutz; Arbeitsgemeinschaft Produkt- und Know-how-Schutz im Verband Deutscher; Maschinen- und Anlagenbau e.V. (VDMA); http://pks.vdma.org/; Frankfurt.
[12] H. Zeyn, *Industrialisierung der additiven Fertigung, Digitalisierte Prozesskette - von der Entwicklung bis zum einsetzbaren Artikel*, VDE Verlag, Berlin, 2017.
[13] S. Zentek, Das Ende der 3D-Marke für technische Produkte, https://provendis.info/aktuelles/news/aus-der-branche/artikelansicht/das-ende-der-3d-marke-fuer-technische-produkte/.
[14] S. Bondar, J.C. Hsu and J. Stjepandić, Network-centric operations during transition in global enterprise, *International Journal of Agile Systems and Management*, Vol. 8, 2015, Nos 3/4, pp. 355–373.
[15] J.P.T. Mo and W. Lorchirachoonkul, Lifecycle design and support of intelligent web-based service systems, *International Journal of Agile Systems and Management*, Vol. 9, 2016, No. 2, pp. 135–153.
[16] M. Hilaga, Y. Shinagawa, T. Kohmura T.L. Kunii, Topology matching for fully automatic similarity estimation of 3D shapes, *SIGGRAPH 2001*, ACM 1-58113-374-X/01/08.
[17] X. Chen, J. Hao, H. Liu, Z. Han and S. Ye, Research on Similarity Measurements of 3D Models Based on Skeleton Trees, Computers, Vol. 6, 2017, No. 2, 17, https://doi.org/10.3390/computers6020017.
[18] D. Mun and K. Ramani, Knowledge-based part similarity measurement utilizing ontology and multi-criteria decision making technique, *Advanced Engineering Informatics*, Vol. 25, 2011, pp. 119–130.
[19] W. Lu, Y. Qin, Q. Qi, W. Zeng, Y. Zhong, X. Liu and X. Jiang, Selecting a semantic similarity measure for concepts in two different CAD model data ontologies, *Advanced Engineering Informatics*, Vol. 30, 2016, pp. 449-466.
[20] J. Nussbaum, Blockchain Project Ecosystem: Market Map and Musings on the State of the Ecosystem, https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940abababaf27, acc. Feb, 9 2018.
[21] A. Schmoll, Dreidimensionales Drucken und die vier Dimensionen des Immaterialgüterrechts : ein Überblick über Fragestellungen des Urheber-, Design-, Patent- und Markenrechts beim 3D-Druck; Gewerblicher Rechtsschutz und Urheberrecht, S. 1041-1050; Berlin, 2015.
[22] A. Katzenbach, Automotive, in: J. Stjepandić et al. (eds.) *Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges*, Springer International Publishing, 2015, pp. 607–638.
[23] S. Redeker, K. Klett and U. Michel, IP-Recht in der digitalen Welt. in T. Klindt und P. Bräutigam (eds.) Digitalisierte Wirtschaft/Industrie 4.0 - ein Gutachten der Noerr LLP im Auftrag des BDI zur rechtlichen Situation, zum Handlungsbedarf und zu ersten Lösungsansätzen, BDI; Berlin; 2015, S. 58-72.
[24] Y. Chen, F. Dong and H. Chen, Business Process and Information Security: A Cross-listing Perspective, *Journal of Industrial Integration and Management*, Vol. 1, 2016, 1650009.
[25] K. Wen, S. Tan, J. Wang, R. Li and Y. Gao, A model based transformation paradigm for cross-language collaborations, *Advanced Engineering Informatics*, Vol. 27, 2013, pp. 27–37.
[26] Y. Chen, Industrial information integration—A literature review 2006–2015, *Journal of Industrial Information Integration,* Vol. 2, 2016, 30–64.
[27] A. Kiitam, A. McLay and T. Pilli, Managing conflict in organisational change, *International Journal of Agile Systems and Management*, Vol. 9, 2016, No. 2, pp.114–134.
[28] Y, Lu, Industrial Integration-A Literature Review, *Journal of Industrial Integration and Management*, Vol. 1, No. 2, 2016, DOI: 10.1142/S242486221650007X
[29] Y.H. Wang, C.H. Lee,A. Trappey, Modularized design-oriented systematic inventive thinking approach supporting collaborative service innovations, *Advanced Engineering Informatics,* 33, 2017, 300–313.
[30] Y.-T. Chen and M.-C. Chiu, A case-based method for service-oriented value chain and sustainable network design, *Advanced Engineering Informatics*, Vol. 29, 2015, pp. 269–294.