Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 91 (2020) 278–283

www.elsevier.com/locate/procedia

30th CIRP Design 2020 (CIRP Design 2020)

# Smart contract based framework to increase transparency of manufacturing networks

Fabian Dietrich[a,b,*], Daniel Palm[a], Louis Louw[b]

[a]*Reutlingen University, Alteburgstrasse 150, 72762 Reutlingen, Germany*
[b]*Stellenbosch University, Banghoek Road, 7600 Stellenbosch, South Africa*

* Corresponding author. Tel.: +49 15119442706. fax: +49 71212719031 05. *E-mail address:* fabian_tobias.dietrich@student.reutlingen-university.de

**Abstract**

Globalisation, shorter product life cycles, and increasing product varieties have led to complex supply chains. At the same time, there is a growing interest of customers and governments in having a greater transparency of brands, manufacturers, and producers throughout the supply chain. Due to the complex structure of collaborative manufacturing networks, the increase of supply chain transparency is a challenge for manufacturing companies. The blockchain technology offers an innovative solution to increase the transparency, security, authenticity, and auditability of products. However, there are still uncertainties when applying the blockchain technology to manufacturing scenarios and thus enable all stakeholders to trace back each component of an assembled product.

This paper proposes a framework design to increase the transparency and auditability of products in collaborative manufacturing networks by adopting the blockchain technology. In this context, each component of a product is marked with a unique identification number generated by blockchain-based smart contracts. In this way, a transparent auditability of assembled products and their components can be achieved for all stakeholders, including the customer.

*Keywords:* Manufacturing Supply Chain; Blockchain; Transparency; Auditability

## 1. Introduction

The globalisation has an impact on every country regardless of its economic, political or social situation and it is not slowing down. In fact, the globalisation has initiated an innovation driven era that is mainly characterised by intense competition, shorter product life cycles, and high product varieties [1].

The rapid changes due to the globalisation and the increasing complexity of supply chains also influence the manufacturing landscape [2,3]. That is why properly configured and easily adaptable manufacturing networks are required, which are capable of handling the complexity and enormity of the supply chain structures. These qualities represent a critical factor for companies in order to maintain their viability [4]. According to Rudberg & Olhager [5], the vast majority of manufacturing is carried out in so-called value networks, which are defined as networks of facilities, possibly owned by different organisations, where time, place or shape utility is added to a commodities in various stages such that the value for the ultimate customer is increased. Camarinha-Matos & Afsarmanesh [6] define a similar type of network as collaborative network. Therefore, collaborative networks consist of a variety of entities (e.g. organisations and people) that are largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital and goals, so they can collaborate to better achieve common or compatible goals, and their interactions are supported by computer networks.

In addition to the structural complexity of collaborative global supply chains, companies have to deal with growing interests of customers, governments, and non-governmental organisations in having a greater transparency of brands,

10.1016/j.procir.2020.02.177

manufacturers, and producers throughout the supply chain. For manufacturers social and environmental sustainability issues have become increasingly important in order to maintain a flawless reputation of their brand. However, as supply chains become more global, many suppliers in the network can be located in developing economies where governments have only a limited ability and willingness to enforce their own laws. Therefore, the dispersed nature of today's supply chains creates increasing levels of risk for multinational businesses, making transparency of supply chains both critical and complex. [7–9]. Especially for organisations operating in complex and dispersed supply chains, the expansion of measures to increase the supply chain visibility can be of great advantage to reduce these risks [8,10].

Barratt & Oke define supply chain visibility as ''the extent to which actors within a supply chain have access to or share information which they consider as key or useful to their operations and which they consider will be of mutual benefit'' [11]. Doorey [12] extends the aspect of supply chain visibility with a transparency aspect by the disclosure of all information of a product's flow throughout the production process and its supply chain to all stakeholders, especially the customers. Duckworth [13] points out, that in this context the terms visibility and transparency are frequently used interchangeably. For Duckworth, the term visibility focuses more on the data sharing within the supply chain to make a collaboration between the network partners more efficient. Transparency however, refers to the disclosure of information to all stakeholders, including the customer.

In October 2008, the pseudonym Satoshi Nakamoto published the famous Bitcoin whitepaper and thus described the blockchain technology for the first time [14]. Nowadays, the blockchain is defined as a technology to process and verify data transactions based on a distributed peer-to-peer network using cryptographic procedures, consensus algorithms, and back-linked blocks to make transactions practically unchangeable [15]. As a result of bitcoin's success in the year 2009, the blockchain technology was mainly associated with financial applications at this time [16–18]. In 2013, Vitalik Buterin extended the idea behind Bitcoin and introduced the whitepaper of Ethereum. Compared to Bitcoin, the platform Ethereum moves far beyond using the blockchain technology just as a currency. It is a decentralised platform with a Turing Complete programming language [19]. Turing Completeness is a mathematical concept and is a measure of the computability of a programming language. Therefore, the language design includes complex constructs such as loops and conditions which enable to create all types of general purpose programs [20]. Through the embedment of Turing Completeness into the blockchain technology, Buterin coined the term 'smart contract' with blockchain-based applications [19].

The code of each smart contract is stored on the blockchain and can be identified by a unique address. Users can interact with a smart contract in present cryptocurrencies by sending transactions to the contract address. When a user causes a valid new transaction with a smart contract address as recipient, all participants on the mining network execute the contract's code with the current state of the blockchain and the transaction's content as inputs. The network then agrees on the output and the next state of the contract by participating in a consensus protocol. [21]

The possibility to run decentralised applications on blockchains platforms initiated a hype around the technology with inflated expectations [22]. Especially when applying the blockchain technology to supply chain management, companies have high expectations to solve transparency and auditability issues of complex collaborative supply chains [15,23–25].

In 2016, Abeyratne and Monfared published a first approach adopting the blockchain technology in manufacturing supply chains. This approach proposes, that physical assets in combination with their 'unique digital profiles' on the blockchain could potentially solve transparency problems of manufacturing supply chains [26].

## 2. Background and rationale of the paper

A lack of transparency can result in various vulnerabilities of manufacturing supply chains. For example in the automotive industry, counterfeit parts are increasingly putting consumer's safety at risk. Automotive parts that are frequently counterfeited in huge volumes are for example airbags, engine and drivetrain components, brake pads, automotive body parts, electrical components, wheels, and windscreens [27]. Especially the counterfeiting of electronic parts causes potential risks including safety and loss of profits to companies, as well as maligning the reputation of manufacturers and distributors. Due to the complexity of global supply chains, it increasingly becomes difficult to maintain the traceability of all components even from very reputable authorised distributers. This increases the probability of counterfeit components being introduced into a supply chain [28–30].

Beside the complexity of supply chains, the storage of component related data in central systems or the existence of paper-based certificates also increases the probability of counterfeit parts entering the supply chain. For example in the aviation industry, organisations file paper documentation of parts such as certificates of conformance, packing lists, and test documentation in archives and store the data in central systems according to their own information policy. Typically, the certificates are not directly linked with the physical batch/shipment of parts. After a certain record retention is elapsed, organisations are allowed to destroy the paperwork, while the physical product can still be in circulation [30]. The result in a confusing number of suspected unapproved parts, which are aircraft parts that do not qualify to meet the provisions of an approved part and do not meet the quality constraints of the industry. So, suspected unapproved parts are seriously violating the strict aircraft security standards [31].

An important method of avoiding the incorporation of tampered counterfeit parts in assemblies is to gain complete traceability of all parts and therefore to increase the transparency throughout the whole supply chain. However, achieving full transparency and detecting counterfeit components is extremely complex and can be a costly undertaking. [28,32,33]. In addition, this turns out to be even more challenging, since counterfeit parts are often originated in developing countries where governments have only limited abilities to enforce laws [7,34].

To improve the avoidance and detection of overproduced, cloned, and tampered counterfeit types represents a present research gap. Especially the problem of incorporating tampered counterfeit parts in assemblies introduces a vulnerability that must be prevented [28].

There is only one blockchain-based approach tackling similar problems described in literature. Thereby, special non-fungible tokens can be used to represent batches of manufactured products [35] in order to represent their 'unique digital profile' [26]. In a figurative sense, this concept creates numerous individual currencies representing batches of manufactured products. With this approach, users have possibility to define rules or 'token recipes' before deploying the tokens. After the deployment however, this approach does not consider any possibility for any pre-defined authority to conduct changes at the 'token recipe' [35]. According to Abeyratne & Monfared, being able to constantly update the 'digital profiles' is essential when adopting the blockchain technology in an industrial scale [26].

This paper however, proposes a smart contract based solution, which only requires all kind of Turing Complete blockchain platforms and therefore enables a more versatile application. The proposed virtual identities combine the advantage of unique non-fungible 'token recipes' with the possibility to assign clear authorities when deploying the smart contract. Additionally, assemblies can be summarised in smart contracts and the transparency can be achieved for all stakeholders by simple query functions embedded in the smart contracts.

## 3. Smart contract based framework design to increase transparency

This chapter proposes a framework design to increase the transparency and auditability of products in collaborative manufacturing networks by adopting the blockchain technology. The framework logically interconnects the concept of blockchain-based smart contracts and their relationship to manufacturing supply chains in order to answer the defined research problem.

### *3.1. Identification and enlistment of all stakeholders*

As the first step, it is necessary to identify and enlist all stakeholders involved in a certain manufacturing process. Depending on the level of detail and the complexity of the supply chain, this process can be a very complex one. This step includes a clear distribution and the clarification of roles of all participants and tasks of the supply chain. This is necessary in order to clarify the concrete process affiliation and composition of the manufactured product.

A simplified manufacturing process forms the basis for presenting the approach of this paper. The manufacturing process involves the production of a product $P_1$ consisting of the two different components $C_a$ and $C_b$. In order to constitute a collaborative manufacturing network, the components and the product are produced by the independent entities Supplier A, Supplier B, and Manufacturer 1. All products can only be produced, when each entity owns a certain certificate Z provided by a Certifier. Depending on the characteristics of the supply chain, the role of the Certifier can be taken over by the manufacturer itself, but also by other independent organisations. This relationship is shown in figure 1.

To ensure traceability by using the blockchain technology, a link between the blockchain platform and the physical product must be established. Accordingly, this approach assumes that all data can refer to an asset itself. For this purpose, smart contracts generate unique identification numbers. In this paper, these numbers are therefore called Hash IDs. Within the platform, these Hash IDs represent a virtual identity of their physical counterparts. In order to map a manufacturing process, the Hash IDs must have the same ownership and conversion characteristics as their physical counterparts. Therefore, they must always be clearly assigned to an owner and must be able to change their owners, for example when the physical product is sold. Furthermore, the Hash IDs must be able to be summarised when combining individual components to a new product.

Because the Hash IDs represent a product or component in the physical world, these numbers must also be attached to the physical counterpart for unambiguous assignment. Therefore, each physical part can be attached with an information tag in the form of a barcode, RFID or QR code to link the physical part to its virtual identity on the blockchain network [26].

Due to the immutability of the Hash ID in this approach, it is also possible to consider a direct attachment of the Hash ID on each physical part for example in form of engraving or in the course of an adaptive manufacturing process.

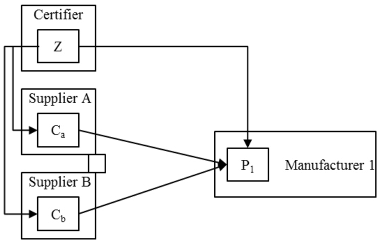

Fig. 1. Exemplary manufacturing process to produce product $P_1$

The Certifier represents a special peculiarity. Theoretically certificates can also have counterparts in the physical world, but it is not mandatory necessary. In this case, the Hash ID does not relate to a physical asset, but it represents a necessary certificate. This exemplifies, that Hash IDs can also refer to licences, certificates or other types of non-physical assets.

### *3.2. Creation of a smart contract logic*

In the second step, all processes in the supply chain must be logically linked with each other. This logic must then be reflected in the smart contracts on the blockchain platform. For this to be possible, all requirements of the physical supply chain must be transferred to the virtual supply chain. In the physical world, the relationships between processes are usually very clear. For example it is not possible to assemble a certain product, without having the required parts on hand. This relationship must exactly be found in the smart contracts. In addition, in the physical world only certain entities are able to create certain parts. This means, that only the entity which ‘owns’ the process of creating a certain part in the physical world, is able to have access to the smart contract to create the virtual identity of the part. To guarantee this, the smart contracts must be linked with the account of the competent entity when deploying them on the blockchain network. Additionally, a smart contract based structure enables the embedment of voting mechanisms allowing to constantly update the code of the smart contract, even after the contract has been deployed [37].

A typical smart contract based application consists of three elements: Contracts and logic on the blockchain, user interface, and backend resources such as off-blockchain storage [38].

When the possession of the smart contract is clearly assigned and the ownership of all required Hash IDs is clarified, information for creating a new Hash ID can be entered into the user interface. The information stored behind each Hash ID at the time of creation, can for example come from conventional central systems owned by the entity creating the Hash ID. This also creates an interface between conventional systems and the blockchain. The basic smart contract logic is shown in figure 2.

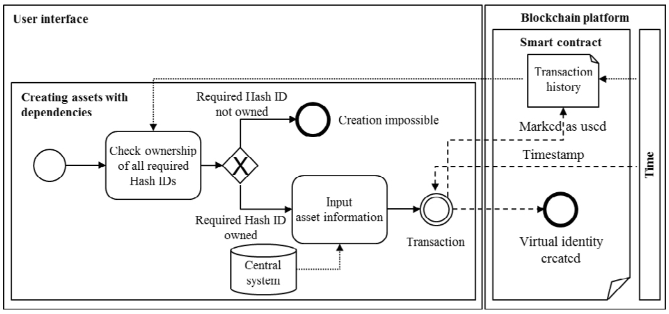

Fig. 2. Smart contract logic to create Hash IDs

By supplementing the timestamp function of the blockchain when hashing all important information, it can be guaranteed that each Hash ID is unique. Therefore, the blockchain can also be seen as a database of timestamps with the ability for anyone to state, publicly and immutably, that a certain thing has happened at a certain time [39].

Applying this logic to the production process of $P_1$, shown in figure 1, only the certifier is able to create certificates without any additional conditions. Supplier A and B, on the other hand, must first be assigned a certificate to create the Hash ID of $C_a$ and $C_b$. The creation of the Hash ID of $P_1$ requires and assignment of a certificate, Ca, and $C_b$.

Figure 2 exemplifies that in addition to assigning Hash IDs, also the creation of such IDs result in a transaction on the blockchain. From this it can be deducted, that every change of state of a product or component in the physical world is resulting in a transaction on the blockchain.

### 3.3. Platform decision

In this approach the logic described in the previous section requires smart contracts in order to enable a mapping of manufacturing processes on the blockchain. Therefore, Turing Completeness of the blockchain platform forms the first fundamental prerequisite.

Due to the current limitation in terms of scalability of the blockchain technology [40], it is necessary to precisely analyse the amount of transactions caused by the manufacturing supply chain. When transferring the proposed smart contract logic to a manufacturing supply chain, the number of transactions caused in order to produce one product depends on the number of state changes and ownership changes. In this context, state changes refer to the changes of a product, for example in production processes, where two components are assembled to create one new product. The number of total transactions caused by one product, is therefore the sum all its changes of state $s_n$ and all its changes of ownership $o_n$. Additionally, it is not only important to calculate the total number of transactions, but also in which period of time these transactions take place. This does not only apply to one production process, but to all parallel concurrent processes taking place in the same time interval $\Delta t$. Equation (1) below shows this mathematical relationship between a number of n concurrent processes in a certain time interval to calculate the predicted transactions per second *PTPS*.

| | |
|---|---|
| PTPS | : Predicted transactions per second |
| $s_n$ | : Changes of state of $\text{asset}_n$ |
| $o_n$ | : Changes of ownership of $\text{asset}_n$ |
| $\Delta t$ | : Time interval in seconds |

$$PTPS = \frac{s_1 + o_1}{\Delta t} + \frac{s_2 + o_2}{\Delta t} + \dots + \frac{s_n + o_n}{\Delta t} = \frac{\sum_{i=1}^{n}(s_i + o_i)}{\Delta t} \tag{1}$$

The calculated prediction is an important component needed for the platform decision. In particular, critical intervals must be checked with small time intervals in order to identify bottlenecks with a high number of transactions per second Furthermore, it must be taken into account that in case a public blockchain platform is chosen, the whole transaction capacity of the network is not only available for one’s own application.

An essential element of the platform decision process, is the selection of the blockchain type. In general one can differ between permissionless and permissioned blockchain. While in a permissionless blockchain everyone can check and verify the transactions on the network and can participate at the consensus process, in a permissioned blockchain the access to the network is restricted and only a selected group of nodes can participate at the blockchain [40,41].

For manufacturing networks, the question must be answered, if all network participants are known at the time of creation and at any point in the future. If this is the case, for example with strictly regulated and organised supply chains with a high number of participants, a permissioned blockchain platform can be considered. However, if a high number of customers is involved as a stakeholder with full transparency, it automatically will result in an unknown number of network participants. Thus, full transparency for all stakeholders can only be achieved with a permissionless blockchain platform. There is only the possibility of restricted transparency for the customer in a private network. These participation differences are shown in figure 3.

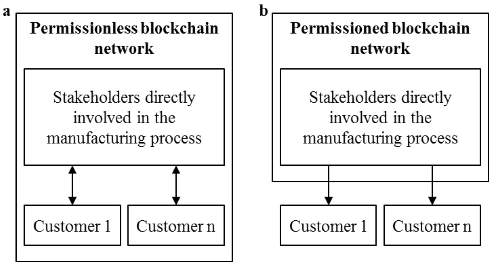
a
Permissionless blockchain network
Stakeholders directly involved in the manufacturing process
Customer 1
Customer n
b
Permissioned blockchain network
Stakeholders directly involved in the manufacturing process
Customer 1
Customer n

Fig. 3. (a) Full transparency for customers; (b) Restricted transparency for customers

### 3.4. Blockchain integration

The vertical and horizontal integration of the blockchain in the supply chain takes place as a final step. The supply chain and all its logical interrelationships must be completely mapped in the blockchain network in order to ensure a complete traceability, authenticity, and auditability of each product and its components.

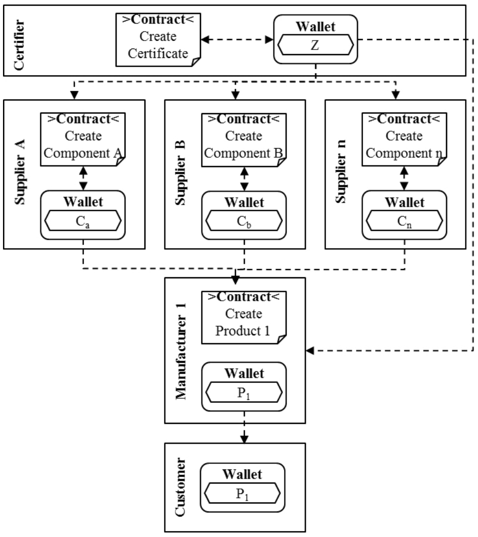
Certifier
>Contract< Create Certificate
Wallet Z
Supplier A
>Contract< Create Component A
Wallet C_a
Supplier B
>Contract< Create Component B
Wallet C_b
Supplier n
>Contract< Create Component n
Wallet C_n
Manufacturer 1
>Contract< Create Product 1
Wallet P_1
Customer
Wallet P_1

Fig. 4. Blockchain integration scheme

Each stakeholder involved in the manufacturing supply chain, owns an account consisting of a blockchain wallet to have access to the network. The account of the stakeholders directly involved in the manufacturing process, is additionally linked to the respective smart contract. By applying the smart contract logic described in Section 3.2, the chronological sequence of the physical process can be virtually mapped on the blockchain.

Figure 4 shows the blockchain integration scheme according to the exemplary manufacturing supply chain. First, the certifier is creating certificate HashIDs and is assigning them to the addresses of the suppliers and the manufacturer. The introduction of a number of n suppliers in figure 4, elucidates the scalability and the possibility of continuous extension of this scheme. After receiving the certificate, the suppliers are able to create their respective components and submit them to the manufacturer. The manufacturer is only able to create the virtual identity of product 1, if the manufacturer's account owns all the required HashIDs of all components and certificates.

All HashIDs can change ownership as often as desired and, for example, be assigned to the addresses of different distributors, retailers or in case of the end product, also to the customer. Due to the immutability of the blockchain, tracing the history of each asset is possible at any point of the supply chain.

## 4. Conclusion

This paper proposed a blockchain-based framework design to increase the transparency and auditability of products in collaborative manufacturing networks. In this context, each physical asset is marked with a unique identification number generated by blockchain-based smart contracts. By formulating logical requirements to create the identification numbers in smart contracts, the processes and their relations in the physical world, can be mapped virtually on the blockchain. Thus, each asset receives a virtual identity. A complete integration of this approach in the whole manufacturing supply chain ensures a secure traceability, authenticity, and auditability of each assembled product and its components. Therefore, the transparency can be increased for all stakeholders and vulnerabilities allowing counterfeit parts to enter the supply chain can be reduced. The implementation on a public blockchain platform provides full transparency for the customer, while the implementation on a private blockchain network only provides a restricted transparency. Further research is currently being conducted to test and validate the developed framework.

## References

[1] Ernst R, Haar J. Globalization, competitiveness, and governability: The three disruptive forces of business in the 21st century. Cham, Switzerland: Palgrave Macmillan; 2019.

[2] Ueda K, Takenaka T, Vancza J, Monostori L. Value creation and decision-making in sustainable society. CIRP Annals - Manufacturing Technology 2009;(58):681–700.

[3] Mourtzis D, Doukas M. Decentralized Manufacturing Systems Review: Challenges and Outlook. Logistics Research 2012;(5):113–21.

[4] Mourtzis D, Doukas M, Psarommatis F. A toolbox for the design, planning and operation of manufacturing networks in a mass customisation environment. Journal of Manufacturing Systems 2015;(36):274–86.

[5] Rudberg M, Olhager J. Manufacturing networks and supply chains: an operations strategy perspective. Omega - The International Journal of Management Science 2003;(31):29–39.

[6] Camarinha-Matos L, Afsarmanesh H. Collaborative Networks - Value creation in a knowledge society. China: Springer; 2006.

[7] Chen S, Zhang Q, Zhou Y-P. Impact of Supply Chain Transparency on Sustainability under NGO Scrutiny. Prod Oper Manag 2018;63(9).

[8] Linich D. The path to supply chain transparency: A practical guide to defining, understanding, and building

supply chain transparency in a global economy. Deloitte University Press; 2014.

[9] New S. The Transparent Supply Chain; Available from: https://hbr.org/2010/10/the-transparent-supply-chain (22 October 2019).

[10] Brandon-Jones E, Squire B, Autry C, Pertersen K. A contingent resource-based perspective of supply chain resilience and robustness. Journal of Supply Chain Management 2014;(50):55–73.

[11] Barratt M, Oke A. Antecedents of supply chain visibility in retail supply chains: A resource-based theory perspective. Journal of Operations Management 2007;25(6):1217–33.

[12] Doorey D. The Transparent Supply Chain: from Resistance to Implementation at Nike and Levi-Strauss. Journal of Business Ethics 2011;(103):587–603.

[13] Duckworth N. Supply Chain Visibility and Transparency: How Everybody Wins; Available from: https://tdwi.org/articles/2018/07/10/data-all-supply-chain-visibility-and-transparency.aspx (20 October 2019).

[14] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System; Available from: https://bitcoin.org/bitcoin.pdf (20 October 2019).

[15] Gentemann L. Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen; Available from: www.bitkom.org (10 October 2019).

[16] Grinberg R. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal 2011;(4):159–208.

[17] Sorge C, Krohn-Grimberghe A. Bitcoin: Eine erste Einordnung. DuD - Datenschutz und Datensicherheit 2012:479–84.

[18] Kaplanov NM. Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. Consumer L. Rev. 2012;(25):111–74.

[19] Buterin V. Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform; Available from: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (20.10.19).

[20] Lee DKC, Deng RH (editors). ChinaTech, mobile security, and distributed ledger. London: Academic Press; 2018.

[21] Luu L, Chu D-H, Olickel H, Saxena P, Hobor A. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications 2016:254–69.

[22] Gartner. 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018; Available from: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/ (21 October 2019).

[23] Iansiti M, Lakhani KR. The Truth About Blockchain. Harvard Business Review; 2017.

[24] Panetta K. Blockchain, quantum computing, augmented analytics and artificial intelligence will drive disruption and new business models; Available from: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/ (22 October 2019).

[25] Hackius N, Petersen M. Blockchain in logistics and supply chain: trick or treat? Hamburg International Conference of Logistics (HICL) 2017;23:3–18.

[26] Abeyratne SA, Monfared RP. Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology 2016;05(09):1–10.

[27] Peresson S. Counterfeit automotive parts increasingly putting consumer safety at risk; Available from: https://www.lexology.com/library/detail.aspx?g=9ecb7809-e01c-4710-ae00-10ec3c1f7e1b (22 October 2019).

[28] Collier ZA, Hassler ML, Lambert JH, DiMase D, Linkov I. Supply Chains. In: Kott A, Linkov I (editors). Cyber Resilience of Systems and Networks, Vol. 2. Cham: Springer International Publishing; 2019. p. 447–62.

[29] Pecht M. The Counterfeit Electronics Problem. JSS 2013;01(07):12–6.

[30] DiMase D, Collier ZA, Carlson J, Gray RB, Linkov I. Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems. Risk Anal 2016;36(10):1834–43.

[31] Acharjya DP, Geetha MK. Internet of Things: novel advances and envisioned applications. Cham: Springer; 2017.

[32] Machado SM, Paiva EL, da Silva EM. Counterfeiting: addressing mitigation and resilience in supply chains. Int Jnl Phys Dist & Log Manage 2018;48(2):139–63.

[33] Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor M, Makris Y. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. Proc. IEEE 2014;102(8):1207–28.

[34] Domon K. An Economic Analysis of Intellectual Property Rights Infringement: Field Studies in Developing Countries. Cham: Springer International Publishing; 2018.

[35] Westerkamp M, Victor F, Küpper A. Tracing manufacturing processes using blockchain-based token compositions. Digital Communications and Networks 2019.

[36] Abeyratne SA, Monfared RP. Blockchain ready manufacturing supply chain using distributed ledger; 2016.

[37] Frantz C, Nowostawski M. From Institutions to Code: Towards Automated Generation of Smart Contracts. International Workshops on Foundations and Applications of Self-* Systems 2016;01:210–5.

[38] Dhillon V, Metcalf D, Hooper M. Blockchain Enabled Applications. Berkeley, CA: Apress; 2017.

[39] Grossman N. The Blockchain as verified public timestamps; Available from: https://www.nickgrossman.is/2015/the-blockchain-as-time/ (21 October 2019).

[40] Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE 6th International Congress on Big Data 2017:557–64.

[41] Lin I-C, Liao T-C. A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security 2017;19(5):653–9.