JANUARY 2022

FSBC Working Paper

Blockchain in the Manufacturing Industry – Key Use Cases

Johannes Schwab

While blockchain technology is believed to disrupt the financial sector, research and empirical evidence about its application in the manufacturing industry is relatively scarce. With this paper, we provide an analysis of challenges and benefits that blockchain technology holds for three different use cases in the manufacturing industry: (1) smart maintenance, (2) dynamic leasing, and (3) quality assurance.

Introduction

Blockchain technology became popular by providing the technical foundation for the cryptocurrency Bitcoin and is since then believed to transform many aspects of the financial services sector (Cong & He, 2019). Nevertheless, the possibilities of this innovative technology reach far beyond the facilitation of payments. With the creation of touring-complete blockchains such as Ethereum and Hyperledger, a broader and more flexible range of applications was made possible (Nærland et al., 2017). They have the potential to affect a wide range of sectors besides the financial industry. Especially in conjunction with Industry 4.0 and the Internet of Things (IoT), blockchain technology might also play an essential role in overcoming current challenges in the manufacturing industry (Babich & Hilary, 2020).

Frankfurt School Blockchain Center
www.fs-blockchain.de
contact@fs-blockchain.de

Follow us
www.twitter.com/fsblockchain
www.facebook.de/fsblockchain

Frankfurt School of Finance & Management gGmbH
Adickesallee 32-34
60322 Frankfurt am Main
Germany

With a 30% compound annual growth rate, the Boston Consulting Group expects the industrial IoT (IIoT) segment to be one of the fastest growing in the IoT market (Lorenz et al., 2019). Smart factories making use of IoT will allow for a higher degree of automation, lower costs, and enhanced efficiency (Kusiak, 2017). As hard- and software required to establish inter-machine connectivity tend to get more efficient and affordable (Almada-Lobo, 2016) also small and medium-sized companies can benefit from this innovation, leading to a widespread implementation of smart manufacturing solutions throughout the manufacturing industry.

However, these innovations also entail myriad of challenges that have to be addressed from a conceptual and technological perspective. Machine-to-machine communication in smart factories enabled by IoT raises concerns about data integrity, privacy, and data management (Whitmore et al., 2014). Equipped with innovative features, blockchain technology has the potential to serve as a backbone framework for the IIoT, providing data integrity, security, and transparency without involving a trusted third party (Lao e al., 2020).

Smart factories and the IoT

The IoT. Combining the concepts and technologies inherent in Industry 4.0, the picture of a smart factory is drawn. This vision depicts a fully autonomous factory where machines communicate with each other and make decisions in the absence of human interaction based on data received from various sensors. One of the leading technologies believed to enable smart factories is the IoT. With the rise of IoT, borders between the physical world and the internet will vanish (Ng & Wakenshaw, 2017). With relatively inexpensive technologies such as radio-frequency identification (RFID) tags, physical objects can be uniquely identified in a virtual system and real-time statements about their status, location, and other properties can be made (Ng & Wakenshaw, 2017). Known as the IIoT, this concept is expected to have a major impact on the manufacturing industry. However, certain crucial challenges arise with the implementation of this concept.

Privacy and security. To connect machines and other objects, a tremendous amount of data is collected from all kinds of sensors and other measuring devices. This data reveals very critical and intimate insights into the business and production processes of a company and must be treated with the utmost confidentiality. Therefore, crucial privacy and security issues arise (Whitmore et al., 2014). Considering machines and other devices base their autonomous decisions on this information suggests the distorting impact forged data could have.

Interoperability. A further hurdle arising on the path towards broad IoT adoption is the interoperability of different IoT devices and IT systems within a company or a consortium of partner companies. Different standards across companies and devices might obstruct efficient communication and data exchange (Zhao et al., 2019).

Smart Maintenance

Effective maintenance of machines has an important effect on a firm's performance and is therefore a crucial managerial challenge as stated by de Jonge and Scarf (2020). They also find that firms increasingly recognize the benefits of planning maintenance measures proactively instead of just reacting to occurred incidents. Nevertheless, many companies still leave the potential of machine data unused (Bokrantz et al., 2020) and therefore also lack automation in maintenance processes. According to Bokrantz et al. (2020), one of the main features of so-called smart maintenance is data-driven decision-making. With the availability of IIoT, this can be made possible based on data provided by smart machines. Sensors and other measurement technologies integrated into the equipment could, for instance, track erosion and the status of specific parts and inform the machine operator in real-time about their insight.

Data about the degree of utilization of machinery, past incidents as well as conducted maintenance can be saved in a digital logbook (Aleshi et al., 2019). Sharing this logbook could help the manufacturer or an external mechanic to get a better overview of the state of the machine and to react faster and more targeted in case of an outage. It becomes obvious that the success of smart maintenance heavily depends on data-driven decision-making. Therefore, great attention has to be paid to how data is collected, processed, stored, and distributed over a network of participants. Blockchain as the underlying technology of the use cases is especially interesting due to the advantages it provides over centralized systems when implemented in intercompany transactions.

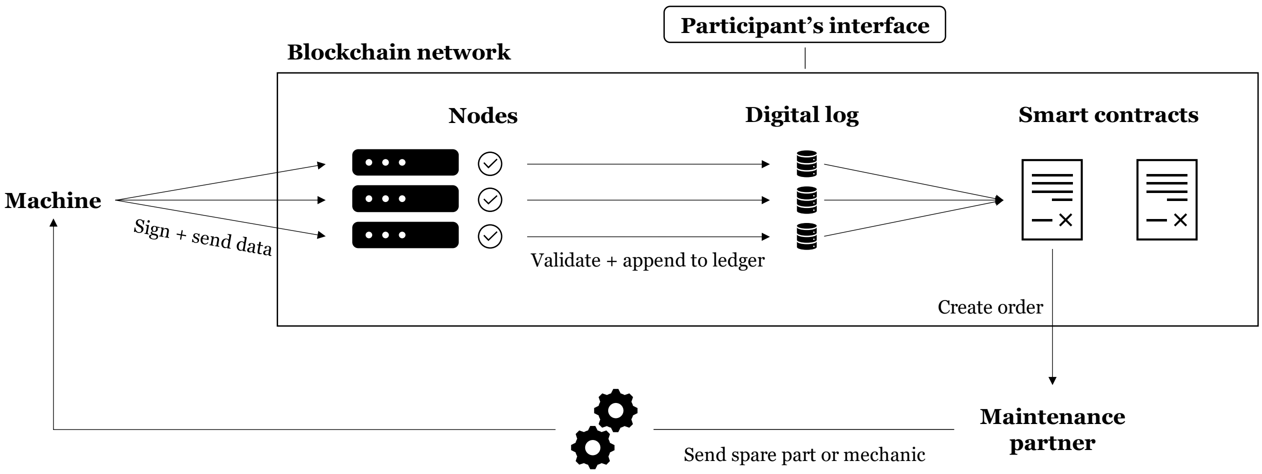
Security. Current IoT devices and applications are prone to data getting changed, forged, or otherwise misused by cyber attackers (Zhao et al., 2019). In the case of a blockchain, however, the data and therefore also the created maintenance log are by design stored immutably, meaning they can hardly be changed once validated and stored on the chain (Zhang et al., 2019). Furthermore, as data is distributed for verification and storage between the participants every full node holds an identical copy of the blockchain and can transparently stay informed about the current state of the machine (Cong & He, 2019). In contrast to a centralized platform where data is stored with a single entity, a blockchain system stores data at every node. Thus, if cybercriminals or even the machine operator him-/herself tries to forge data, it would not be enough to simply attack one entity. Another important component of security is identity management which is especially crucial in the IoT to distinguish different devices (Whitmore et al., 2014). Only if machines and other devices in a network can be identified uniquely, they can be associated with their actions such as machine-to-machine payments. This is also crucial to allow the assignment of rights to certain machines. Blockchain provides this kind of identification functions allowing to uniquely identify nodes in the network and the respective transactions they were involved in without a central server (Lao et al., 2020). As stated by Babich and Hilary (2020, p. 9):

> Blockchain has the potential to provide a decentralized identity management with strong security features.

Trust/Automation. According to Pereira et al. (2019), the security features of blockchain combined with a robust consensus mechanism could contribute to shifting trust from third parties to executable code. This executable code can be introduced in the form of smart contracts, which act on predefined conditions. Yermack (2017) mentions that smart contracts ensure that both contract parties fulfill their promise and hence overcome moral hazard problems like strategic default. Combining the trust participants put into blockchain technology and the automation features of smart contracts, new forms of automation are enabled. As illustrated in Figure 1, in case of planned or unplanned maintenance, the machine could autonomously react within a predefined smart contract and for instance call a mechanic, assign an external service provider to execute repairs, or order respective replacements if they are not in stock (Babich & Hilary, 2020). As no human intervention is needed, this would reduce the time until a mechanic or spare part arrives at the production plant and hence also decrease downtime as well as the opportunity cost associated with production shutdown.

Figure 1

Blockchain in Smart Maintenance



Disintermediation. Additionally, blockchain renders third-party platforms obsolete as consensus can be found through the inherent consensus protocol and therefore contributes to disintermediation (Pereira et al., 2019). According to Gulati (1995), transaction costs are mainly driven by the possibility for opportunistic behavior which can be eliminated using smart contracts that act automatically and according to predefined code. Pereira et al. (2019) also state that disintermediation does not only achieve cost efficiency, it also impedes a third party's control over the data since the maintenance log is distributed over the different participating nodes. Catalini and Gans (2020) show that extensive control over data by an intermediary or centralized platform can have negative consequences such as high switching cost, censorship or fraudulent behavior. As data recorded in the maintenance log can give insights into production processes and utilization this information has to be treated highly confidential and should therefore only be within the control of participating parties.

Transparency. Another advantage of a digital and trusted maintenance log is that the history of the respective machine can be proven reliably which might influence a potential buyer's decision in case of a resale of the machinery (Babich & Hilary, 2020). In addition to the maintenance history, various certificates could be stored on the blockchain and be attached to the digital twin of the respective machine.

First applications of blockchain in maintenance operations can be found in the aviation sector. Honeywell Aerospace, for instance, created a digital marketplace called GoDirect Trade selling used aircraft parts using blockchain to store the history of the parts in a trustful manner to protect market participants (Kearney, n.d.).

Dynamic Leasing

Dynamic leasing does not only follow current trends towards performance or condition-based contracting, it can also provide significant benefits for the operating company and the machine manufacturer. Dynamic leasing describes the idea that monthly leasing rates are adjusted based on predefined parameters such as hours of usage or conducted maintenance measures. As an increasing number of machines and factories in Industry 4.0 will be equipped with sensors (Lasi et al., 2014), technically, this model is already feasible. What might suppress the broader application of this business model is the need for close relationships in performance-based contracts (Hypko et al., 2010) and missing trust in the correctness of the machine data. Blockchain technology has the potential to establish the required confidence and trust for both parties to enter into a condition-based contract (Cole et al., 2019).

As in smart maintenance, to enable efficient interactions with and between machines, a digital twin has to be set up (Huang et al., 2020) which is tied to the respective data on the blockchain. The data, in this case, is information collected about leasing rate relevant parameters such as hours of production per day. This data is collected by sensors at the machine level and will immediately be signed and sent to the blockchain network for validation. Due to predefined rules the data is validated by the nodes and appended to the blockchain where it can hardly be tampered or changed (Biais et al., 2019). The nodes within this network storing the entire blockchain can comprise those of the manufacturer of the machinery acting as lessor and those of the operator of the machinery acting as lessee. Smart contracts can be implemented to calculate the current leasing rate. Due to the predefined rules encoded in the smart contract, certain sensor information such as an exceeded threshold of production hours can trigger the smart contract to increase the leasing rate. In the same way, a planned maintenance inspection that was not adhered to can also raise the payment.

Digital money. Full automation and trust into the process can only be reached if the payment process is also being automated and no human intervention is required. For the automation of the payment process a digital money can be used which enables fast transactions and does not require trusted third parties such as banks to transfer values. Smart contracts can be used to issue a payment when predefined conditions are met (Kolb et al., 2020).

Powered by an appropriate form of digital money, the machine would be able to pay and receive funds autonomously via smart contracts as stated by Stöcker (2017). He also explains that a machine could then act as a fully automated profit center, getting paid for its services and, on the other hand, settle expenses such as the leasing rate and maintenance expenditure. The machine would have its own profit and loss statement and cash flows which enables the operating company to observe the machine’s profitability directly. This way the lessor can better assess the economic feasibility of dynamic leasing models and evaluate adoptions.

Security/Trust. Without a blockchain or a trusted third party, the lessor, which in this case is also the manufacturer, would have to be on site to check the parameters that flow into the calculation of the leasing rate. As in the blockchain-based process data is immediately signed and sent to the blockchain network, it is assured from an early stage that data cannot be corrupted or changed. Furthermore, as both participants store a full history of the blockchain on their nodes, they can easily and with certainty look up and verify historic parameters and leasing rates. The immutable ledger of leasing rate relevant data creates trust between the two parties (Cole et al., 2019) as it assures the manufacturer and the customers that the parameters have not been tampered with malicious intent.

Automation. As the machines are now capable of communicating and interacting with the manufacturer directly, human interaction can be minimized, and administrative efforts are reduced. That is, once the system and smart contracts are set up, the leasing rate calculation as well as the payment process can be conducted automatically. Nevertheless, automation in general can also be achieved without blockchain technology. However, according to Babich and Hillary (2020), blockchain enables increased coordination between all parties or machines involved in an automated process and furthermore decreases potential credibility problems.

Transparency. With blockchain technology the lessee and the lessor both have the complete and identical history of sensor and transaction data stored in their IT system. This trusted set of data could then easily be used by the lessor to observe the machine's production properties and run analyses to identify potential pain points. This also benefits the machine user if error sources can be detected and eliminated efficiently.

Information asymmetry. According to Sharpe and Nguyen (1995), a significant risk for the lessor is the salvage value in case the machine has to be re-leased or is sold after the lease contract has ended. They explain that under an operating or true lease the lessor holds all risks associated with the ownership of the machine such as the uncertainty of the salvage value. As this salvage value also depends on the physical deterioration of the machine, the history of usage saved on the blockchain can simplify the re-sale or re-lease of the machine for the manufacturer. On sale the former owner could hand over the physical asset as well as the digital twin of the machine (Huang et al., 2020) and therefore decrease the information asymmetry between the involved parties. The salvage value could therefore be estimated more reliably and possibly enable higher prices paid for the used equipment.

Quality Assurance

Product quality is an important factor for manufacturers and their reputation. Blockchain technology can offer benefits for quality management as well as anti-counterfeiting policies in many ways.

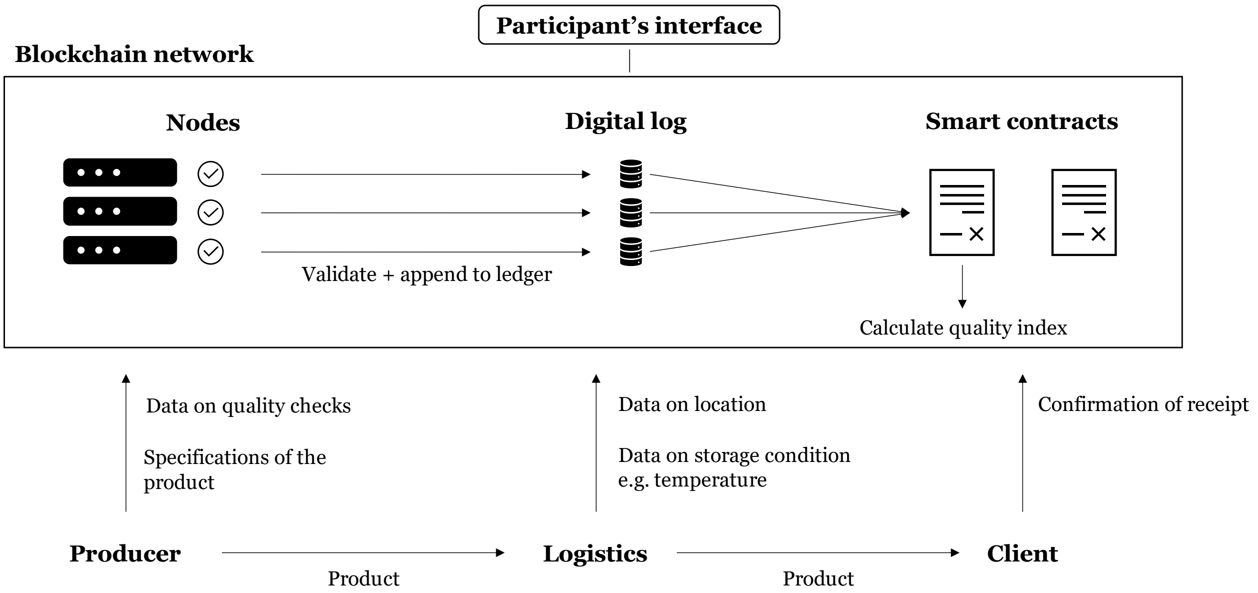
Quality control. Jraisat and Sawalha (2013) found that quality control should not only be applied on the firm level but span throughout the whole supply chain. Two important factors for quality control in supply chains pointed out in their paper are communication between the members of the supply chain and the quality of information the supply chain members share. With this in mind, it becomes evident that tracking products along their way in the supply chain is an integral part of quality assurance which can be facilitated by blockchain technology.

Ngai et al. (2014) describe how RFID technology can be applied to aircraft parts to track them throughout the supply chain. They mention that each part can be assigned a unique RFID tag and ID to track it throughout every step in its lifetime. Blockchain can be used to complement this technology. When a respective RFID tag is scanned, the data could immediately be sent to the blockchain and assigned to the digital twin of the product identified by the unique product ID inherent in the RFID tag. This would allow every participant in the network to transparently see a tamper-proof and therefore trusted movement history of a certain product according to George et al. (2019). They apply this concept to a food supply chain and aim to create a food quality index for meat. They do not merely track the food along the supply chain but also include other quality measures such as the storage temperature or humidity.

A similar concept could be imagined for other products with certain quality requirements along the supply chain. Predefined upper and lower bounds could tell the receiver of the product if it is of sufficient quality. The full nodes of the network could comprise every participant within the supply chain starting from the source of commodities over the logistics firm up to the end-user, which would allow for high visibility of the finished product (Wang et al., 2019). Figure 2 illustrates these ideas and shows how a blockchain-enabled quality tracking system could work.

Figure 2

Blockchain in Quality Assurance



A report published by the Boston Consulting Group about the "Factory of the Future" sees blockchain as an enabler to simplify quality checks (Küpper et al., 2019). According to the authors, every step along the production process including quality checks could automatically be assigned to the specific product's digital twin and be sent to the blockchain. This would enable the manufacturer or buyer to transparently check the quality of the product in the sense that the product went through all necessary production steps and quality checks and furthermore fulfills the stipulated specifications.

Counterfeiting protection. Another important aspect of preserving the quality standards of a firm is to assure that no counterfeits are being distributed in the market which could be harmful to the own brand. Conducting supply chain expert interviews, Wang et al. (2019) found that knowing about the provenance of a product is of high value as fraudulent parts can cause severe consequences for instance in the aircraft sector. They state that an immutable, transparent, and distributed ledger of transactions based on blockchain technology can enable product provenance and therefore help mitigating counterfeit risk. If every step from the sourcing of the material up to the finished good is traced transparently on the blockchain and assigned to the digital twin, a customer can be more confident that the physical product they buy is not a forgery (Wang et al., 2019).

Transparency. Without blockchain technology, partners in the supply chain have to rely on declarations by their supplier or perform extensive and time-consuming status queries about a variety of processes via a pull mechanism as stated by Chang et al. (2019). They also state that data in current systems is exchanged between various databases aggravating real-time tracking. However, a traceability system for food based on Hyperledger Fabric showed that blockchain-based systems could significantly increase the visibility and traceability of products in the supply chain (Hyperledger, n.d.). This so-called IBM Food Trust Project in cooperation with Walmart decreased the time to determine the origin of mangos from seven days to 2.2 seconds (Hyperledger, n.d.).

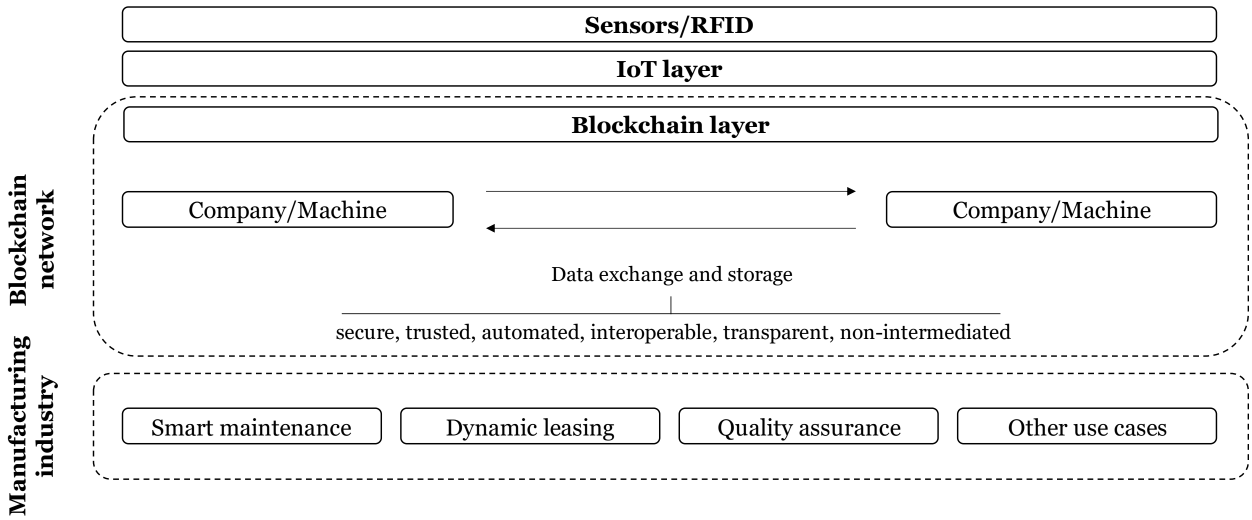
Security/Trust. It becomes evident that for more extensive supply chains with various participants, quality assurance is a challenge every involved party contributes to. This requires communication, information sharing, and trust between the supply chain members (Jraisat & Sawalha, 2019). Blockchain technology can establish multilateral relations between untrusted parties (Schmidt & Wagner, 2019). Trust in this use case is established by the immutability of data entries meaning the participants can be assured no entry has been tampered (Beck et al., 2016). As the data entries also get time-stamped, one can also be sure about the sequential order of the entries and the lifespan of the product within the production or supply chain.

Automation. The created trust can be beneficial to automate processes. As described above, quality checks on the physical product can be executed automatically and the specifications consequently can be recorded in a trusted manner on the blockchain, making inbound quality checks by the receiver unnecessary (Küpper et al., 2019). This could allow for further automation as machinery could accept goods autonomously based on the quality measures saved with the digital twin of the product. Blockchain technology can result in less paper-based, manual transactions throughout the supply chain and along quality checks and therefore enhance process efficiency (Chang et al., 2019).

Interoperability. An additional advantage which refers to all three use cases is interoperability. Many IoT applications lack interoperability with systems of other manufacturers or even other business units within the same company as different platforms or data formats are used. Especially when working with an extensive supplier network it is crucial that every participant can interact with the system, meaning the data uploaded by one party needs to be accessible and readable by other participants or IoT enabled machines. The interconnecting role of blockchain technology in the manufacturing industry is illustrated in Figure 3. Nevertheless, interoperability between different blockchains can be challenging as further outlined in the next section.

Figure 3

The role of blockchain in manufacturing



Risks and challenges of blockchain technology

Compared to other technologies, blockchain is a relatively young and at least for its implementation in the IoT or manufacturing not prevalent technology (Schmidt & Wagner, 2019). It becomes evident that there are also substantial risks, challenges, and prerequisites that need to be addressed and evaluated in the light of the respective use case.

Cost. Blockchain technology and smart contracts generally have the potential for cost savings associated with opportunistic behavior, as the protocol as well as the conditions that trigger a smart contract are defined in advance (Pereira et al., 2019). Nevertheless, Pereira et al. (2019) also identify downsides concerning cost. They state that blockchain systems compared to centralized systems have higher storage costs as data is saved multiple times and higher verification costs as data needs to be verified by multiple nodes. According to the authors, this cost is even higher if the respective assets are not purely digital as a continuous link needs to be established to the offline world. A certain infrastructure of sensors and RFID tags is required to establish the link between the blockchain and the physical world. Kumar et al. (2019) also state that blockchain compared to existing inter-organizational systems comes with high setup and overhead cost which can only be justified upon careful use case analyses has been undertaken.

Data acquisition. Data or transactions which are stored on the blockchain are by design stored immutably and distributed which creates trust in the integrity of the information (Kolb et al., 2020). However, blockchain technology cannot prevent data from getting manipulated right at the acquisition stage (Schmidt & Wagner, 2019). According to Babich and Hilary (2020), this represents the so-called "garbage in, garbage out" problem. They state the key issue to be the link between the physical asset and the information saved about it on the blockchain, the product's digital twin. If, for instance, sensors used to implement dynamic leasing are corrupted, they will provide inaccurate data which will then be processed through smart contracts and potentially lead to miscalculated leasing rates.

Source code errors. As all three aforementioned use cases make use of smart contracts another important challenge is the design of these smart contracts themselves. Typically, smart contracts require to be complete contracts meaning every eventuality needs to be included in the smart contract's code (Pereira et al., 2019). According to Kumar et al. (2019), it is challenging to translate every contract correctly into computer-executable language. It becomes clear that smart contracts are limited if more complex or highly fragmented customization is needed but can unfold huge benefits used with repetitive and formal contracts (Pereira et al., 2019).

Storage capacity. Another possible limitation is the preciousness of storage capacity. As blockchain, by design, stores the entire chain of information or transactions, the needed storage capacity is steadily increasing over time (Lao et al., 2020). Additionally, the other nodes in the network hold a replication of the data multiplying the storage requirements for the whole network by the number of nodes as expressed by Kumar et al. (2019).

To reach consensus, new transactions need to be distributed to the network and after validation the nodes also have to communicate the outcome of the validation process generating a high number of messages exchanged throughout the network (Lao et al., 2020). This moreover elucidates another precious resource to the system which enables this frequent communication between the nodes, the bandwidth (Lao et al., 2020). Thinking about quality assurance as an example, we see that, depending on the number of products and updates per day, storage requirements can quickly reach an enormous level if every possible data point and pictures of the product are saved on the blockchain.

To address the storage challenge, only critical data and data needed as input for smart contracts should be stored on-chain (Chang et al., 2019). Kumar et al. (2019) mention a solution where additional data is stored off-chain while its hash is stored on-chain. This way, data storage can be saved but changes in the off-chain data can still be observed by comparing the hash value to the hash value stored on the blockchain. Again, taking quality assurance as an example, important data such as the specifications of the product should be stored on-chain whereas additional data like a picture of the product could be saved centralized on the manufacturer's server. If the manufacturer tries to tamper data on his server, the hash value will change and other participants in the network such as the receiver could detect this change and request the recovery of the original data.

Technological uncertainty. As blockchain is a relatively young technology, especially in manufacturing, investments in the technology at this early stage can be perilous (Schmidt and Wagner ,2019). They point out that other DLTs are currently developed with characteristics and features which could make them more desirable than blockchain in certain use cases. The blockchain alternative IOTA, for instance, is considered especially promising for the usage in IoT and Industry 4.0 as it provides high scalability and is lightweight enough to be implemented within IoT devices (Popov & Lu, 2019). Until the concepts are technologically mature, it remains unclear which technology will prevail and investments could be risky. Additionally, many firms are still not sure about the functionalities and benefits of the technology. Even though blockchain is a trustless system there needs to be a certain trust established in the technology itself for broad adoption (Babich and Hilary, 2020).

Regulation. Additionally, legal uncertainty can expose blockchain investments to substantial risk. As a relatively new technology, the legal enforceability of smart contracts in case of a dispute might be uncertain.

According to Mik (2017), smart contracts can be handled as ordinary and enforceable contracts but each case must be considered individually, and no statement can be made for all smart contracts. To tackle this issue, especially with more complex contracts, smart contracts could be used as an extension to written physical contracts. Regarding, for instance, dynamic leasing, the manufacturer and operator of the machine should clarify what happens if sensors fail to transmit the correct production time and therefore a wrong leasing rate is calculated.

Blockchain design. Many different blockchain designs and consensus protocols exist, and further designs are currently under development. As outlined by Babich and Hilary (2020), determining a technical design that provides an optimal level of verifiability, privacy, and efficiency is a major challenge. It becomes evident that every technological design has its own challenges and features that need to be balanced according to the specific use case. The main technological challenges of different blockchain designs are described in the so-called "Scalability trilemma" by Vitalik Buterin, stating that a single system can hardly satisfy all of the three characteristics security, decentralization, and scalability simultaneously (Lao et al., 2020).

The use cases introduced in this paper require a high degree of privacy and security as confidential operational data is exchanged but also scalability is needed. According to the scalability trilemma, a blockchain that fulfills these needs has to accept shortcomings concerning decentralization. Hyperledger Fabric, as an example, satisfies these needs at the cost of decentralization as only authorized nodes can join the network (Kolb et al., 2020). However, for most B2B blockchain implementations, decentralization is subordinated to scalability and security and permissioned blockchains like Hyperledger Fabric are therefore well-suited (van Laar, 2019). Discussing the scalability trilemma and the arising challenges in detail is beyond the scope of this paper and is therefore condensed as the challenge to find an appropriate blockchain design.

Table 1

Challenges of blockchain technology in the manufacturing industry

Challenge	Rationale	Possible Mitigants
Cost	– Even if blockchain has the potential to reduce transaction cost, it comes at high setup/overhead cost	– Careful assessment of cost advantages and disadvantages in the respective use case
Data acquisition	– Tamper-proof storage is of little value if data input is already corrupted	– Sensor networks – Prevent or reveal human interaction in data acquisition
Source code errors	– Complex business relations make it hard to translate contracts into source code	– Private blockchains allow for relatively easy changes to smart contracts in case of source code errors
Storage capacity	– Blockchain as append-only data base needs ever-increasing and costly storage capacity	– Storing only relevant data on-chain whereas the rest of the data only has its hash value stored on-chain
Technological uncertainty and maturity	– Many firms still do not trust into the technology itself – Alternatives to blockchain are being developed	– More empirical evidence about the benefits and shortcomings of the technology is needed
Regulation and legal	– The legal enforceability of smart contracts especially in cross-jurisdiction transactions is still uncertain	– Until these issues are resolved, smart contracts should exist as extension to traditional contracts
Blockchain design	– Many different blockchain designs exist with individual benefits and disadvantages	– Assessing the needs of the use case keeping the scalability trilemma in mind
Blockchain interoperability	– Different blockchain designs might be unable to communicate in cross-chain transactions	– The development of international standards is needed. Current work is e.g. performed by the International Organization for Standardization Technical Committee 307 (Pólvora et al., 2020)

Blockchain interoperability. Even though blockchain technology can be beneficial for interoperability of different IoT devices, the compatibility with other blockchains can become a challenge. According to Schmidt and Wagner (2019), firms are likely to be participants in different blockchain ecosystems, which might be problematic if cross-blockchain interoperability is required. If, for instance, the quality of a product shall be tracked, and the involved parties already joined different blockchain ecosystems having different designs, the communication between them could be obstructed. Table 1 summarizes the challenges of blockchain technology and provides an overview of possible mitigants.

Conclusion

We find that blockchain technology can be utilized as the underlying technology to facilitate data storage and exchange between participants. This form of data exchange holds significant advantages compared to traditional systems such as enhanced security, transparency, privacy, and interoperability overcoming current challenges of the IoT in these areas. We also found that smart contracts can support the automation of processes in the manufacturing industry, thereby further increasing operational and cost efficiency. Combined with the trust-building feature of the technology, it can enable new forms of intercompany interaction and collaboration.

Nevertheless, the technology also faces challenges which need to be addressed in order to promote a more widespread implementation of blockchain technology in the manufacturing industry. However, especially in the light of Industry 4.0, where manufacturing companies tend to be more interconnected, blockchain can be a promising technology. Building on this form of data exchange and storage, the implementation of use cases such as smart maintenance, dynamic leasing, and quality assurance can be facilitated.

Johannes Schwab is pursuing his Master of Finance at Frankfurt School of Finance & Management. In the course of his bachelor's thesis, he dealt with the application of blockchain technology in the manufacturing sector. You can contact Johannes via mail (johannes.schwab@fs-students.de) or LinkedIn (www.linkedin.com/in/johannesschwab/).

References

Aleshi, A., Seker, R., & Babiceanu, R. F. (2019). Blockchain model for enhancing aircraft maintenance records security. *Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security*. https://doi.org/10.1109/hst47167.2019.9032943.

Almada-Lobo, F. (2016). The industry 4.0 revolution and the future of manufacturing execution systems (MES). *Journal of Innovation Management*, *3*(4), 16–21. https://doi.org/10.24840/2183-0606_003.004_0003.

Babich, V., & Hilary, G. (2020). OM forum—Distributed ledgers and operations: What operations management researchers should know about blockchain technology. *Manufacturing & Service Operations Management*, *22*(2), 223–240. https://doi.org/10.1287/msom.2018.0752.

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain–The gateway to trust-free cryptographic transactions. *Proceedings of the Twenty-Fourth European Conference on Information Systems*. https://aisel.aisnet.org/ecis2016_rp/153.

Biais, B., Bisière, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies*, *32*(5), 1662–1715. https://doi.org/10.1093/rfs/hhy095.

Bokrantz, J., Skoogh, A., Berlin, C., Wuest, T., & Stahre, J. (2020). Smart Maintenance: An empirically grounded conceptualization. *International Journal of Production Economics*, *223*, Article *107534. https://doi.org/10.1016/j.ijpe.2019.107534*.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM*, 63(7), 80–90. https://doi.org/10.1145/3359552.

Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, *144*, 1–11. https://doi.org/10.1016/j.techfore.2019.03.015.

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, *24*(4), 469–483. https://doi.org/10.1108/scm-09-2018-0309.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007.

de Jonge, B., & Scarf, P. A. (2020). A review on maintenance optimization. *European Journal of Operational Research*, *285*(3), 805–824. https://doi.org/10.1016/j.ejor.2019.09.047.

George, R. V., Harsh, H. O., Ray, P., & Babu, A. K. (2019). Food quality traceability prototype for restaurants using blockchain and food quality data index. *Journal of Cleaner Production*, *240*, Article 118021. https://doi.org/10.1016/j.jclepro.2019.118021.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal*, *38*(1), 85–112. https://doi.org/10.5465/256729.

Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361–371. https://doi.org/10.1016/j.jmsy.2020.01.009.

Hyperledger. (n.d.). *How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric*. The Linux Foundation Hyperledger. https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf.

Hypko, P., Tilebein, M., & Gleich, R. (2010). Benefits and uncertainties of performance-based contracting in manufacturing industries. *Journal of Service Management*, *21*(4), 460–489. https://doi.org/10.1108/09564231011066114.

Jraisat, L. E., & Sawalha, I. H. (2013). Quality control and supply chain management: A contextual perspective and a case study. *Supply Chain Management: An International Journal*, *18*(2), 194–207. https://doi.org/10.1108/13598541311318827.

Kearney, K. (n.d.). *Four ways blockchain will change aircraft maintenance*. Honeywell International Inc. https://aerospace.honeywell.com/en/learn/about-us/blogs/2019/08/four-ways-blockchain-will-change-aircraft-maintenance.

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2020). Core concepts, challenges, and future directions in blockchain. *ACM Computing Surveys*, *53*(1), 1–39. https://doi.org/10.1145/3366370.

Kumar, A., Liu, R., & Shan, Z. (2019). Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. *Decision Sciences*, *51*(1), 8–37. https://doi.org/10.1111/deci.12396.

Küpper, D., Ströhle, J., Krüger, T., Burchardi, K., & Shepherd, N. (2019). *Blockchain in the factory of the future*. Boston Consulting Group. https://www.bcg.com/de-de/publications/2019/blockchain-factory-future.

Kusiak, A. (2017). Smart manufacturing. *International Journal of Production Research*, *56*(1–2), 508–517. https://doi.org/10.1080/00207543.2017.1351644.

Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus and traffic modeling. *ACM Computing Surveys*, *53*(1), 1–32. https://doi.org/10.1145/3372136.

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4.

Lorenz, M., Hunke, N., Brown, J., Buchner, T., & Ludwig, M. (2019). *The machinery maker's guide to the IIoT galaxy*. Boston Consulting Group. https://www.bcg.com/de-de/publications/2019/machinery-maker-guide-industrial-internet-of-things-iiot-galaxy.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, *9*(2), 269–300. https://doi.org/10.1080/17579961.2017.1378468.

Nærland, K., Müller-Bloch, C., Beck, R., & Palmund, S. (2017). Blockchain to rule the waves - Nascent design principles for reducing risk and uncertainty in decentralized environments. *Proceedings of the International Conference on Information Systems*. https://core.ac.uk/download/pdf/145226366.pdf.

Ng, I. C. L., & Wakenshaw, S. Y. L. (2017). The internet-of-things: Review and research directions. *International Journal of Research in Marketing*, *34*(1), 3–21. https://doi.org/10.1016/j.ijresmar.2016.11.003.

Ngai, E. W. T., Cheung, B. K. S., Lam, S. S., & Ng, C. T. (2014). RFID value in aircraft parts supply chains: A case study. *International Journal of Production Economics*, *147*, 330–339. https://doi.org/10.1016/j.ijpe.2012.09.017.

Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change, 146, 94–102. https://doi.org/10.1016/j.techfore.2019.04.030*.

Pólvora, A., Nascimento, S., Lourenço, J. S., & Scapolo, F. (2020). Blockchain for industrial transformations: A forward-looking approach with multi-stakeholder engagement for policy advice. *Technological Forecasting and Social Change*, 157, Article 120091. https://doi.org/10.1016/j.techfore.2020.120091.

Popov, S., & Lu, Q. (2019). *IOTA: Feeless and free*. Blockchain IEEE. https://blockchain.ieee.org/technicalbriefs/january-2019/iota-feeless-and-free.

Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, *25*(4), Article 100552. https://doi.org/10.1016/j.pursup.2019.100552.

Sharpe, S. A., & Nguyen, H. H. (1995). Capital market imperfections and the incentive to lease. *Journal of Financial Economics*, *39*(2–3), 271–294. https://doi.org/10.1016/0304-405x(95)00830-8.

Stöcker, C. (2017). *Automating machine transactions and building trust in the 4th industrial revolution*. Medium. https://blog.iota.org/automating-machine-transactions-and-building-trust-in-the-4th-industrial-revolution-d3219a157396.

van Laar, S. (2019). *A shortcoming of blockchain: The scalability trilemma*. Medium. https://medium.com/@s_van_laar/a-shortcoming-of-blockchain-c588ea8e6db2.

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? *International Journal of Production Economics*, *211*, 221–236. https://doi.org/10.1016/j.ijpe.2019.02.002.

Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The internet of things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274. https://doi.org/10.1007/s10796-014-9489-2.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, *21*(1), 7–31. https://doi.org/10.1093/rof/rfw074.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481.

Zhao, S., Li, S., & Yao, Y. (2019). Blockchain enabled industrial internet of things technology. *IEEE Transactions on Computational Social Systems*, *6*(6), 1442–1453. https://doi.org/10.1109/tcss.2019.2924054.