International Journal of Production Research

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tprs20

Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing

Dhruv Patel, Chandan Kumar Sahu & Rahul Rai

To cite this article: Dhruv Patel, Chandan Kumar Sahu & Rahul Rai (2024) Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing, International Journal of Production Research, 62:3, 1041-1071, DOI: 10.1080/00207543.2023.2262050

To link to this article: https://doi.org/10.1080/00207543.2023.2262050

Published online: 26 Sep 2023.

INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH
2024, VOL. 62, NO. 3, 1041–1071
https://doi.org/10.1080/00207543.2023.2262050

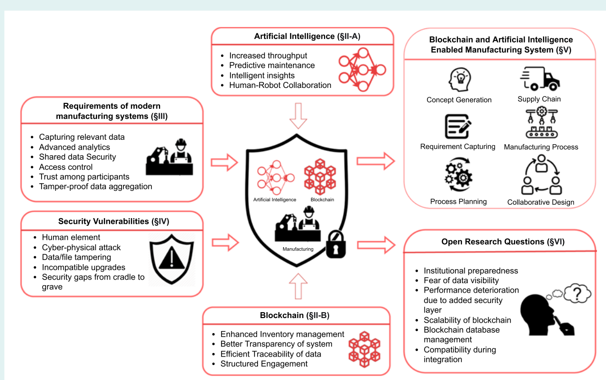
Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing

Dhruv Patel [a,†], Chandan Kumar Sahu [b,†] and Rahul Rai [b,c]

[a]Manufacturing and Design Lab (MADLab), Department of Mechanical and Aerospace Engineering, University at Buffalo, Buffalo, NY, USA; [b]Geometric Reasoning and Artificial Intelligence Lab (GRAIL), Department of Automotive Engineering, Clemson University, Greenville, SC, USA; [c]Computer Science Division, School of Computing, Clemson University, Clemson, SC, USA

ABSTRACT

Process automation and mass customisation requirements of modern manufacturing systems are driven by artificial intelligence (AI). As AI derives decisions from data, securing the data against tampering is crucial to prevent ensuing operational risks. Additionally, manufacturing systems necessitate collaboration, transparency, and trust among participants while preserving a competitive advantage. Thus, we position blockchain, an enabler of transparent and secure operations, as a security solution for AI-assisted manufacturing systems. In this conceptual viewpoint paper, we present a framework to integrate blockchain in AI-assisted manufacturing systems. We highlight the special needs of manufacturing BCs over generic BCs. We delineate the ways in which manufacturing can be a beneficiary of the synergy between AI and BC. We discuss how BC and AI can accelerate early-phase product design, collaboration, and manufacturing processes and secure supply chains against counterfeit products and for ethical consumerism. Lastly, we identify the needs of modern manufacturing systems and cite a few examples of organisational failures to underscore the importance of security while delineating the significant challenges in adopting blockchain-based solutions in the manufacturing industry.



ARTICLE HISTORY
Received 12 April 2023
Accepted 24 July 2023

KEYWORDS
Blockchain; industry 4.0; machine learning; manufacturing; security

1. Introduction

The manufacturing industries are increasingly evolving to a more consumer-centric model (Business-to-consumer, B2C) that caters to individual needs. Through the use of emerging technologies like Computer-Aided Design (CAD), Artificial Intelligence (AI), Additive Manufacturing (AM), the Internet of Things (IoT), and human-robot collaboration, these industries are moving towards 'mass individualisation' or 'mass customisation' (Kim and Lee 2023; Mourtzis 2021; Rai et al. 2021). The manufacturing facilities of the future are expected to blend the affordability of mass production with the specificity of customised products, thus maximising business interests. There has been a gradual progression in the sector with the digitisation of existing systems to keep pace with evolving customer demands and maintain a competitive edge. Mass customisation is visible through the surge in digital manufacturing operations, with more

CONTACT Rahul Rai rrai@clemson.edu Geometric Reasoning and Artificial Intelligence Lab (GRAIL), Department of Automotive Engineering, Clemson University, Greenville, SC 29607, USA; Computer Science Division, School of Computing, Clemson University, Clemson, SC 29634, USA
†Equal contribution

than two million autonomous robots operating on the shop floor to match supply with demand (IFR Press Release 2020). The process starts with product concepts conceived or customised for consumers, designed using CAD, simulated, and finally materialised via AM. This approach accommodates consumer expectations while optimising design and processing using machine learning (ML), thereby saving time and resources. As a result, digitisation and automation facilitate mass individualisation, creating manufacturing environments independent of human intervention by equipping them with decision-making capabilities. The rise of intelligent data analysis has been instrumental in overcoming traditional bottlenecks by aiding in decision-making. This transformation is propelled by *Industry 4.0* (Rüßmann et al. 2015) by enabling machine-to-machine (M2M) and machine-to-human (M2H) communication (Cheng et al. 2018) and extensive automation by integrating several transformative technologies such as internet of things (IIoT) (Sisinni et al. 2018), augmented reality (AR) (Sahu, Young, and Rai 2021), cloud manufacturing (CMfg) (Mourtzis 2021), additive manufacturing also known as 3D printing (3DP) (Bogue 2013), simulation and virtualisation (Ullah 2019), big-data analysis (Frank, Dalenogare, and Ayala 2019), autonomous robotics (Javaid et al. 2020) with the manufacturing sector. The dynamic M2M and M2H interconnection between the interacting entities is the digitisation of the physical realm. Digitized manufacturing facilities improve collaboration and efficiency and enable self-monitoring production systems and problem analysis without human intervention.

The interconnected digitised manufacturing environment gives rise to data, and precisely, it is *big data*. Manufacturing system with autonomous capability (of **C**ognition, **C**ommunication, **C**omputation, and a**C**tuation) become cyber-physical systems (CPS) that integrate cyber and physical components using a network infrastructure to communicate and transfer data (Rai and Sahu 2020). The cyber component is dominated by data (among others like computational algorithms and network protocols) from sensors and computational devices which are communicated by the network. Additionally, digital operations integrated with the product's lifecycle are also one of the reasons behind the boost in data. The upsurge in data availability opens the scope for data analysis and data engineering for better decision-making. It is important to emphasise that traditionally data were analysed to derive analytical insights using *human knowledge*. The human component in data analysis inhibited complete autonomous operations. Earlier autonomous operations leveraged functional programming where the functions ($\approx$ operations on the data) were constructed based on *human knowledge*. Lately, the functional programmes are being replaced by *generic functions* that learn the mapping ($\approx$ function) between the input and output data by mimicking *human intelligence*. This paradigm is referred to as *artificial intelligence* (AI). Many researchers have deployed AI on data to replicate the decision-making process of 'human brains' to solve complex industrial problems such as process optimisation, predictive maintenance, intelligent inspection, quality control, and improvement (Bielecki et al. 2021; Z. Zhang, Jaiswal, and Rai 2018; Z. Zhang et al. 2023, 2022). The AI-based solutions are quite encouraging since they enhance the cost-effectiveness, adaptability, safety, reliability, and flexibility of the manufacturing systems, as well as provide tools for accelerating the development of optimised solutions. The paradigm shift to AI has shown performance at par or (in some cases) even better than humans. This exemplary performance can be attributed to the tacit knowledge we have, which has not been translated into any functional programming.

The future of mass customisation and autonomous operations *depends* on data and the decisions derived from data. The industry's emphasis on extracting insights from big data using computational methods like AI underscores our focus on the connection between data and decisions. Data from Cyber-Physical Systems (CPS) or autonomous systems, characterised by volume, value, velocity, variety, and veracity (Rai and Sahu 2020), demand particular attention to *veracity* – the consistency and trustworthiness of data. Trusted data is not tampered with. It is devoid of unknown biases or errors, or missing values. More importantly, it is fully utilisable. The value offered by a dataset that lacks trust undermines the derived insights and restricts confident deployment. The analytical insights can be skewed. Trust in data becomes paramount when multiple sensors/systems interact and communicate. We highlight the importance of security in data using a few cues. *First*, with the emergence of data-driven techniques (particularly AI) in the last decade, the quality of data has become crucial in decision-making as the effectiveness of AI algorithms depends on the quality and quantity of data. Without guaranteeing the quality of data, the results from the AI tools in the manufacturing systems can impose low yield risks in production. The quality of data is improved by preprocessing the data. It involves normalisation, noise removal, data transformation, etc. Poor quality of data needs more preprocessing. *Secondly*, a challenging task that is indirectly connected with the quality of data is trust, transparency, and traceability of manufactured products. The manufacturing industry's massive growth and interdependence require a seamless flow of information. Data is collected from various sources, including third parties, as in crowdsourcing (A. Liu and Lu 2016). Crowdsourcing has been increasing at a significant pace in the product design process where the design process is creative, like those in the food (Bech et al. 2018), bikes (Tan et al. 2017), apparel (Bellemare 2018) and footwear (Berry, Wang, and Hu 2013) industry. Initiatives like *Creator's club* by Adidas[1] and *Nike by you*[2] have brought customisation capability to the customers beyond research arenas. The sources of errors increase as the number of actors on the product increase. *Thirdly*, increased digitisation in the manufacturing ecosystem demands data storage systems to manage big data. The manufacturing firms rely heavily on private centralised cloud-based systems, such as CLoudNC[3] and Xometry,[4] to access and store data. Even though cloud services prioritise data security, exclusive ownership or control of data raises the broad issues of data theft, cybersecurity, and loss of intellectual property (Boccella et al. 2020). Managing and possessing enormous amounts of information, sometimes confidential data, is a crucial but controversial task. *Lastly*, Data security and privacy concerns are often compounded by underdeveloped IT infrastructures commonly employed in manufacturing industries. IIoT captures the data from the shopfloor through the sensors and stores it in centralised servers (Ordieres-Meré, Villalba-Díez, and Zheng 2019). Sometimes, large-scale data is aggregated and stored in geographically distributed locations before being clustered into a centralised server. However, collecting data from different sources and transferring it to a centralised server becomes challenging when suppliers, facilities, and customers are geographically dispersed. Single points of server failure have led to system breaches in the past, further raising data security concerns (Franzen et al. 2008). The transfer process is also susceptible to missing values and incurs irrelevant and redundant information. *Overall*, Industry 4.0 adds value to the manufacturing system; while simultaneously increasing vulnerability. These challenges emanating from the lack of trust in available data restrict the utilisation of ML in manufacturing systems. Thereby, it impedes the decision-making capacity of the machines. In view of data transfer, data storage, and multiple sources of data, it is prudent to emphasise that manufacturing industries are unable to provide a robust information management system for AI-assisted decision-making. Data preprocessing consumes significant effort for accurate analysis using AI to derive any insight from data. So, it is high time to realise the importance of secure systems and trustworthy data to utilise the power of AI to harness its full potential in decision-making.

It is evident that data security is of utmost importance in modern manufacturing systems for a foolproof decision-making process. Data flow, from collection to processing to disseminating information, is a salient feature of digitised manufacturing systems. Therefore, data security is a grave concern, especially in the AI-assisted (data-driven) manufacturing industry. A prudent approach for mitigating the above-mentioned security challenges is integrating manufacturing systems with *Blockchain* technology. Blockchain offers a combination of tools to address the sustainability, efficiency, robustness, and security of systems. Blockchain is a decentralised network. A single entity does not have the power to alter anything without the consensus of other stakeholders. In this context, it is essential to note the work of Vitalik Buterin, who founded the Ethereum cryptocurrency (based on Blockchain) after getting disappointed by the nerfing of his favourite Warcraft character by the game developer (Blizzard Entertainment) in one of its patches (WoW Patch 3.1.0) (Dannen 2017; Good 2021). Decentralizing the power from a single authority can prevent the powerful from going rogue. The Blockchain was originally developed for making data transactions peer-to-peer (P2P) without the need for a central governing authority. Removal of the central authority can prevent it from declaring a completed transaction illegal or void and penalising the transactors. The Blockchain consists of a distributed ledger that records each movement and activity in the system. The distributed ledger is a consecutive list of activities with timestamps shared across the network. The ledger is shared across the network, which makes it secure against data tampering. Blockchain has consensus protocols that check whether the transacted data is valid and accurate. Blockchain uses a smart contract, a programmable protocol that allows the execution of agreements and terms. Smart contracts allow the incorporation of application-specific constraints. Such a combination of shared ledger, consensus protocols and smart contact creates a trustless, tamper-proof environment for storing manufacturing data on Blockchain. Thus, Blockchain has become an incentive-based system that encourages more people to join, making the network even more robust. Due to these valuable characteristics of Blockchain, data privacy and security issues can be minimised in AI-assisted manufacturing. It can make data processing and decision-making faster and produce trusted results.

Presently, research at the intersection of '*blockchain and Manufacturing*' and '*AI (or ML) with manufacturing*' are extensive. However, no conceptual framework has been proposed for integrating 'Blockchain and ML technologies in manufacturing', even when security and trust have become critical factors. The reason for the void is a lack of understanding of Blockchain technology and its possible use cases beyond cryptocurrencies.

It is important to understand that a clear parallel can be drawn between the P2P transactions in cryptocurrencies and manufacturing industries. For instance, the transaction of products between *supplier and manufacturer* or *manufacturer and customer*; and the monetary transactions between *manufacturer and customer* or *the supplier and the bank* are all P2P. We lay the foundation of our work on this parallel to fill the void by combining the three domains '*Manufacturing, Machine Learning, and Blockchain*'. Precisely, this conceptual viewpoint paper seeks the answers to the following research questions: (1) What are the requirements of modern smart manufacturing systems? (2) Why has security become critical in manufacturing environments? (3) How can blockchain solve the security issues of manufacturing industries? How can we integrate blockchain in manufacturing systems seeking autonomy? (4) What are the challenges in incorporating blockchain as a security solution in manufacturing organisations? Our work delineates the utility of integrating Blockchain and ML in manufacturing operations for research endeavours and practical applications. Specifically, our contributions are:

- Investigate the current challenges faced by modern manufacturing systems
- Highlight a few incidents to underscore the need of security measures in manufacturing environments
- Identify the scope and need for integrating Blockchain in AI-assisted manufacturing systems
- Provide a conceptual framework for fusing AI and Blockchain technologies in manufacturing applications
- Discuss the open research questions for integrating Blockchain in manufacturing systems

A brief discussion on the Blockchain and ML technologies is included in Section 2 for completeness and convenience to an uninformed reader. The requirements of modern manufacturing systems are detailed in Section 3. A few actual incidents of breaching into the manufacturing systems due to ineffective security measures are highlighted in Section 4. Section 5 discusses a manufacturing system enabled by both Blockchain and ML. It also includes key differences between a manufacturing Blockchain and a generic (e.g. finance like cryptocurrency) Blockchain. We also discuss some open challenges and broader perspectives in Section 6 that consider Blockchain and ML jointly from a manufacturing perspective. Finally, this paper concludes in Section 7. Figure 1 summarises our work.

2. Background

2.1. Artificial intelligence assisted manufacturing

Sentient beings use their intelligence to distil knowledge. When they observe any process (system), they use their intelligence to extract the correlation between the factors affecting the process (system) and the responses

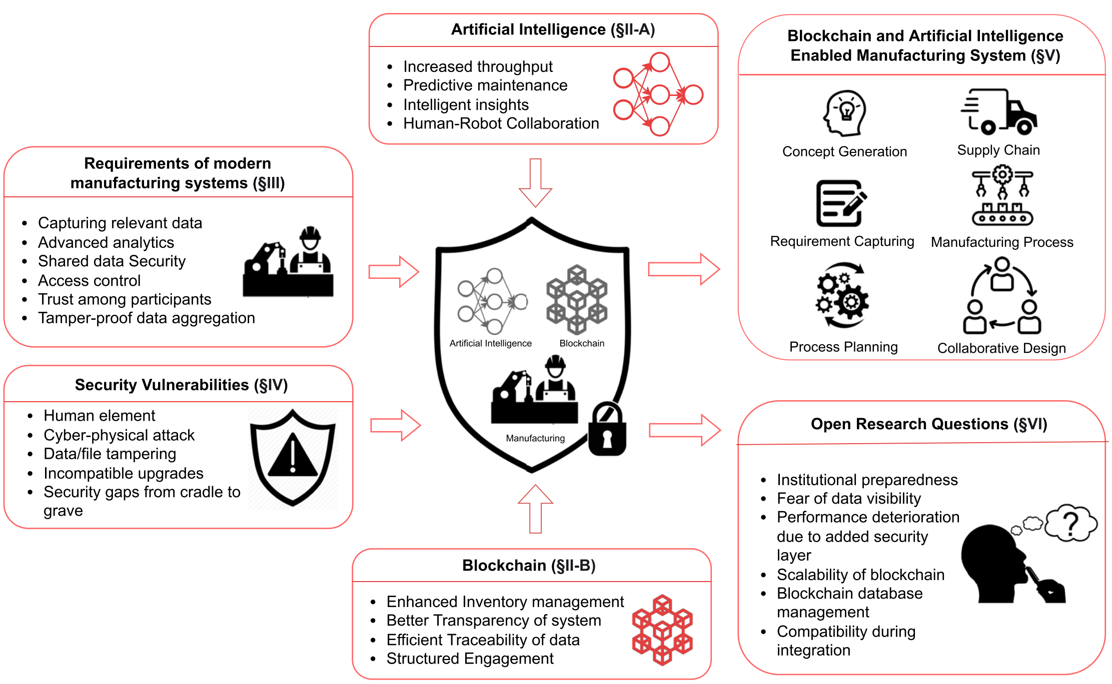


Figure 1. Integration of blockchain in artificial intelligence assisted manufacturing operations.

generated by the process (system). A successful correlation becomes knowledge. That knowledge was used for automation. Such an automated system had knowledge but lacked the intelligence to discover any new knowledge. Thus, they failed whenever the environmental uncertainty (or factors) went beyond the limits. Additionally, the *volume* factor of big data poses a critical challenge for autonomous systems. The massive volume of data is likely to cover the state space completely. Hence, autonomous systems will have to handle exceptional cases as well (Rai and Sahu 2020). Each of these exceptional cases can give rise to new knowledge. But, as our system is not intelligent, it cannot discover this knowledge. That's where humans have played a vital role traditionally. They debugged the system wherever it failed. If we want to automate the system *fully*, we have to remove the human component by making the system intelligent to discover knowledge wherever it needs. That's where we need AI to make the system fully autonomous to handle changing demands in mass individualisation or while maneuvering in unknown terrain or to handle errors on the factory floor. Nowadays, the terms AI and ML (machine learning) are used interchangeably. In summary, the utmost functionality of ML is to make the system intelligent enough so that it can learn to *autonomously* make the decision and respond to the changes in the system dynamics effectively with no to nominal interference from humans. ML tools and algorithms utilise data (input and output data) to extract the knowledge to automatically perform intelligent tasks like those by humans, such as perceiving, learning, reasoning, and ultimately solving the problem. Training ML models on raw data equip the model with the intelligence to extract actionable information for classification, regression, control, and generation tasks. We skip the details of AI as they have been widely used in manufacturing scenarios. We suggest the reader to visit Goodfellow, Bengio, and Courville (2016), LeCun, Bengio, and Hinton (2015), Kurtz et al. (2023) and Wuest et al. (2016) for details on AI.

AI was introduced in the manufacturing industry in 1955 (H.-C. Zhang and Huang 1995). The manufacturing sector has been exploiting ML tools for prediction, classification, regression, and forecasting tasks by extracting complex and non-linear patterns from the raw data and converting them into valuable features to improve *quality* of the products and *quantity* of production (Paturi and Cheruku 2021). Given the current abundance of data, ML can monitor system dynamics in real-time and adapt to chaotic environments, with proven algorithmic accuracy and reproducibility (Impagliazzo et al. 2022). These insights facilitate necessary system modifications and future behaviour prediction, optimising parameters to reduce waste and save time. We include a few cases to show the effectiveness of AI in diverse applications. Metal AM components were inspected using a CNN (B. Zhang, Jaiswal, et al. 2019). The costs of circuit boards were estimated using a CNN-based deep regressor and an autoencoder in an automotive OEM (Bodendorf, Merbele, and Franke 2022). The assembly process was optimised by determining the line feeding mode using a classification and regression tree (CART) in four companies: (1) an original equipment manufacturer (OEM), (2) an electric motor manufacturer, (3) a naval equipment producer, and (4) an automotive manufacturer (Zangaro, Minner, and Battini 2021). The unstructured machine log data of three companies were processed using AI-based NLP (natural language processing) techniques for predictive maintenance (Usuga-Cadavid et al. 2022). They were able to handle class imbalance arising due to a lesser number of machine failure data using random oversampling. R. Nguyen, Singh, and Rai (2023) used generative adversarial networks for robust failure prognosis. ML has also been used for optimisation and to control the process parameters for troubleshooting and maintenance. The automated fault detection and diagnosis ML techniques have significantly increased the utilisation rate of the machines, minimised downtime, and increased their overall useful lives. Multiple organisations have been pioneering the adoption of AI. For instance, (1) Danone Group, a french food manufacturer, uses AI for demand forecasting, (2) the Japanese automation company 'Fanuc' uses AI for robotic operations, (3) BMW uses AI-based image recognition for quality inspection and defect reduction, (4) Porsche is using unmanned ground vehicles for automated manufacturing (El-Sherif 2019; Kamath and Mewari 2021). These organisations and many others are exploring new avenues to incorporate AI.

2.2. Security and blockchain

As alluded in Section 1 - Introduction, a key enabler of Industry 4.0 and mass customisation is the *interaction* between several components as part of IIoT and CPS. The interaction exchanges different kinds of data through an interconnecting network. There is a flow of data within the network in a manufacturing setup which usually contains information about *inventory*, *finances*, and others which we generically refer to as *information*. Existing record-keeping infrastructures to track data flow fail in certain crucial cases. We will quote a few instances in the next paragraph to realise how integrating blockchain can solve those issues. Blockchain, at the core, is a digital ledger shared across its participants. This digital ledger can do the usual record-keeping task. It has some additional properties that are valuable to solve the problems conventional record-keeping techniques cannot solve.

Consider a notional example of a manufacturing company that manufactures customised shoes or other assembled products of relatively higher complexity which the customers will buy repeatedly. Let's consider a few instances to understand how Blockchain can help modern manufacturing systems. *First*, traditional record-keeping procedures (like Enterprise Resource Planning (ERP) tools) are prone to errors as information can be overwritten without notifying all the involved stakeholders. The transactions, whether with suppliers or across different departments within a company, involve several steps which may introduce discrepancies as the data operator can overwrite the data as recorded during its generation. Periodic internal and external audits are required to ensure correctness. However, integrating Blockchain, which shares and synchronises data across all participants, can make the system error-proof and more efficient. With Blockchain, any transaction modification needs validation from all parties, thus eliminating the need for audits. Secondly, the company keeps track of manufactured products by using batch codes. They store the complete process history and include the machines used to manufacture the product. Even then, there are instances of product recall, especially in the case of the automotive industry. In case of any defect in the product, the company has to trace it to the machine and quality checkpoints. Tracing the product history became crucial in the drug industry for compliance with the Drug Supply Chain Security Act of 2013 (U.S. Food and Drug Administration 2013). Counterfeit drugs need to be traced to the source. Legacy systems are ineffective at tracing. Blockchain can trace the defective products (or counterfeit drugs or masks Shen et al. 2023) to the origin of the defects. Third, manufacturing a product while managing multiple components and tracking their utilisation poses challenges due to the absence of real-time traceability. The lack of real-time information about the supply chain can lead to significant disruptions if a supplier faces material shortages and fails to deliver on time. This issue arises from the limited availability of up-to-date information at the company's disposal. In legacy systems, the information is usually intimated as per need. There's no real-time information sharing. There are trust and security issues that prevent information sharing. Blockchain can eliminate this issue as it shares the encrypted information in real-time. Participants with access can decrypt the information to review the shared data. Lastly, legacy systems do not encrypt the data. Thus, special measures need to be taken for security purposes. The company and suppliers become vulnerable if any wrongdoers get access to the data. Blockchain can be instrumental in addressing these vulnerabilities as Blockchain prevents access to the data beyond the participants. As the data is encrypted by Blockchain, wrongdoers cannot do any harm even if they get access to the data. Additionally, Blockchain can ease cross-border trade. Skuchain[5] is developing a currency agnostic Blockchain for global business-to-business trade and finance. Hence, it is prudent to integrate Blockchain into manufacturing operations to make secure and error-proof systems (Gaur and Gaiha 2020).

Blockchain is a *chain* of *blocks* containing the details of the data transacted in the system in chronological order. In technical terms, the Blockchain is essentially a distributed, immutable, open-source, public data ledger (Zheng et al. 2018) which contains the transactions among untrusting parties without any centralised controller. A basic blockchain structure is shown in Figure 2. A general block in Blockchain consists of two parts of data. The first one is *header data* which includes (1) hash value of current block, (2) block ID, (3) hash value of previous block (also referred as parent block), (4) block version (includes validation rules), (5) transacted data or information, and (6) timestamp (the time at which

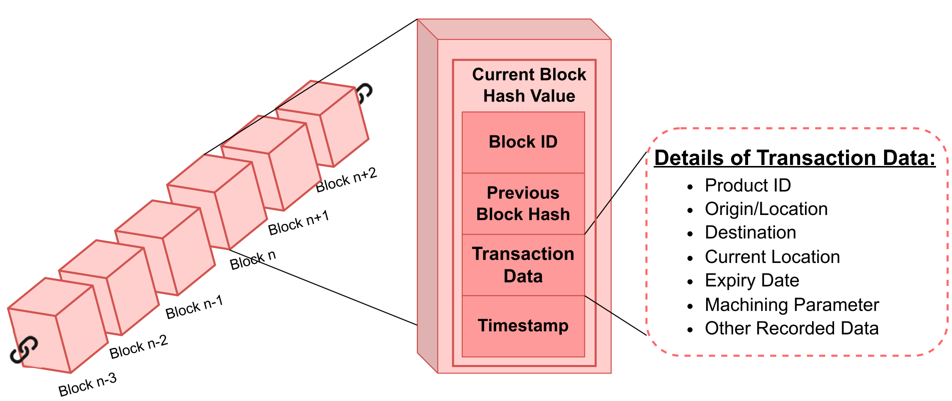


Figure 2. Structure of a single block in the blockchain.

the block was generated). The integration with timestamp and position (relative to the parent block) makes the block immutable and reliable. The nonce is mainly used in cryptocurrency mining. It refers to the number of characters in the hash while calculating its value. It could be optional in manufacturing applications. And other part of data is *main data* which stores all the information transactions ever executed within the Blockchain network. As shown in Figure 2, the data contains details of the product (like its ID, expiry date, machine parameter, etc.) as well as the origin, destination, and current location of the product.

An inactive blockchain is triggered when a transaction request is passed to the P2P nodes in the blockchain network. When a new request is executed, all the authorised members in the network participate in the block validation. Block validation is a process of ensuring genuine transactions. Once the nodes validate the transaction request, a block consisting of the details of the transaction request is generated. The verified block is forwarded to the validating authorities to check the authenticity of the requester and details of the block. The block will be discarded if the validating nodes reject the request. It ensures that only valid transactions are allowed while sharing with unknown organisations. A validated block is appended at the end of the chain, just like a queue. This operation is illustrated in Figure 3. Thus, as more and more information is passed through the blockchain, the blockchain grows continually with the execution of information transactions.

Each block includes the hash of the preceding block. The hash of the current block is generated using data within the block and the hash of the preceding block. Therefore, whenever a new block is generated, it produces a unique hash value. Since each block consists of the hash value of the previous block, it creates a hash tree (J. Wang et al. 2020). Therefore, any alterations in the block can easily be detected since the hash value of each block is interrelated. Changes in block data will affect the hash value of each block and, subsequently, the hash of other connected blocks. Hence, the immutability. All the information on the current block can be verified conveniently by utilising the hash value of the hash tree root in the blockchain. This way, the more blocks added to the network, the more it becomes secure and safe.

The type of blockchain to be used depends on the application and the operations to be performed. A blockchain is divided into three types: *public*, *private*,

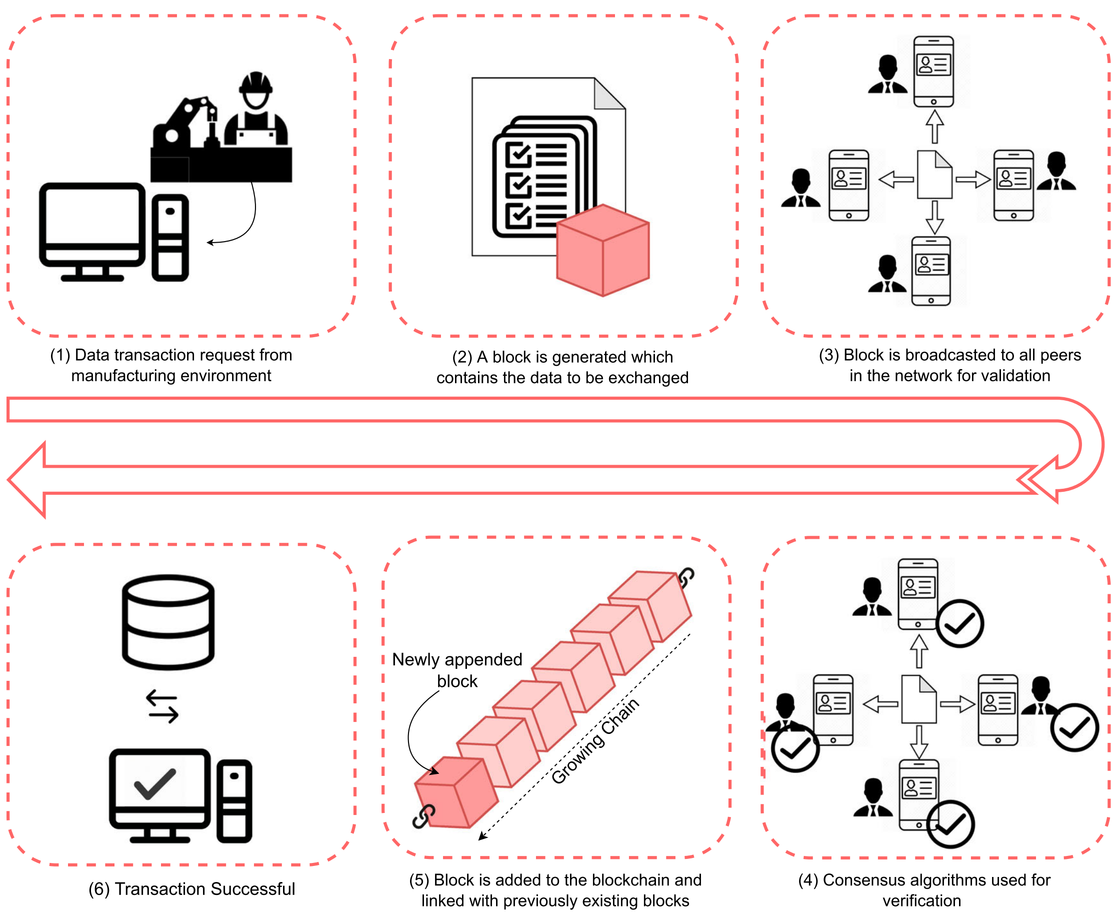


Figure 3. Working mechanism in a blockchain enabled system.

and *consortium*. A *public* blockchain system is fully decentralised. A blockchain becomes *private* if controlled by a single entity. The *consortium* is a combination of both public and private blockchain, in which the blockchain is partially controlled by a group of organisations. A public blockchain is nearly impossible to tamper with, as majority of the participants participate in the validation process. To date, the famous examples of public blockchains are cryptocurrencies like Bitcoin (Nakamoto 2008), Ethereum (Dannen 2017) and Dogecoin (Chohan 2021). In the case of private and consortium blockchains, the dominant member or group has control and access over the blockchain network. Ripple (Akcora, Gel, and Kantarcioglu 2022) and Hyperledger (Cachin 2016) are examples of private blockchain. They are developed as business-to-business virtual currency exchange platforms. Consortium blockchain is more associated with the supply chain industry in which different organisations can join the network. R3 (Y. Guo and Liang 2016), an enterprise technology and service provider, is an example of consortium blockchain. From the characteristics of the three blockchain systems, it is evident that public blockchain has scalability issues even though it gives assurance over immutability, transparency, nonrepudiation, and traceability. Public blockchain is permissionless, which allows the participant to have access to everything in the network. On the contrary, the permission-less characteristic of public blockchain also lacks in providing flexibility in terms of change in blockchain norms. Private and consortium blockchain has better scalability than the public as access is controlled by a few or one entity to reach a consensus. Access control rules make private and consortium BCs more secure than public BCs. Table 1 characterises different types of BCs according to the application requirement. The comparison illustrates that consortium blockchain is more suitable for manufacturing applications. Salah et al. (2019) is a good reference for a detailed taxonomy of the blockchain platforms.

Blockchain builds trust using consensus algorithms based on the mathematical principles of asymmetric cryptography (Bahga and Madisetti 2016). The consensus algorithm allows the users to make a transaction with other entities while being anonymous. There are different types of consensus mechanisms built for blockchain technology as per requirements, such as energy requirements, the security level they offer, and the scalability level. Mourtzis, Angelopoulos, and Panopoulos (2023) presented the most common consensus algorithms, such as (1) Proof of Work (PoW) (Kiayias and Zindros 2019), (2) Proof of Stake (PoS) (Gaži, Kiayias, and Zindros 2019), (3) Delegated Proof of Stake(DPoS) (Hu et al. 2021) (4) Proof-of-Activity(POA) (5) Proof-of-Authority(PoA) (6)

Table 1. A comparison of different kinds of blockchain.

Public blockchain	Private blockchain	Consortium blockchain
Open and permissionless	Restricted access to specific participants	Operated by a consortium of organisations
Decentralized	Permissioned network	Permissioned participation
Transparent and immutable	Higher privacy and controlled access	Balances decentralisation and controlled access
Ledger open to Public	Ledger restricted	Ledger accessible to specific user
Low Latency	High Latency	Latency depends on the transaction type
High energy consummation	Low energy consummation	Energy consummation depends on transaction load
Public participation in consensus	Small group participation in consensus	Consensus participation allowed to the public and specific group

Proof-of-Burn(PoB) (7) Proof of Capacity/Proof of Space (PoC/PoSpace) (8) Proof of Elapsed Time (PoET) (9) Proof of History (PoH) and (10) Proof of Importance (PoI). All of the mentioned algorithms are transplantable in blockchain. In the context of a public blockchain, it refers to an open-source platform facilitating data transactions accessible to anyone. Transactions made on the blockchain are validated and added to the chain by the consensus algorithm, which determines the chosen block. This process ensures the creation of a reliable (and unified) transnational ledger. For example, when a transaction triggers the blockchain, miners collect a few transactions, validate it and create the block. Then miners compete to solve the 'mathematical puzzle' (consensus algorithm). This is why block creation is a power-hungry process. The one who solves the puzzle first gets to add the next block and gets rewarded. It is called proof-of-work (PoW). Different blockchain networks has different consensus algorithms, e.g. *Solana* has proof-of-history(PoH) (Yakovenko 2018), *Binance* has practical Byzantine fault tolerance (pBFT) (Abraham et al. 2017) and *Polkadot* has hybrid consensus protocol (Wood 2016). Proof-of-history is a sequence of computation that cryptographically verifies the passage of time between two events. Practical Byzantine Fault Tolerance (pBFT) (Castro and Liskov 1999) is designed to reach consensus even when some of the nodes in the network respond with incorrect information. This way, the consensus algorithm paves the way to transact data between untrusting participants in decentralised networks (Lakshman and Agrawala 1986). Therefore, the consensus algorithm is selected so that it should fulfill the purposes of the application with the necessary security. It is a wise option to choose an optimised algorithm to save computational resources and power (Cachin, Sorniotti, and Weigold 2016). In manufacturing industries, it is advisable to use Permissioned or private Blockchains. Most Private Blockchains are based on the Byzantine Fault Tolerant (BFT) consensus protocols (Abraham et al. 2017; Crain et al. 2018). BFT is more suitable for manufacturing operations (Muzammal, Qu, and Nasrulin 2019). BFT is better than PoW (Proof of Work) and PoS (Proof of Stake) in terms of security and resource intensiveness (Sousa, Bessani, and Vukolic 2018).

Another proponent of integrating blockchain with complex manufacturing operations is its autonomous transaction capability using the 'Smart Contracts (SC)' attribute of blockchain. SC is a computerised transaction protocol that executes contractual terms automatically when enforced conditions are matched (Ream, Chu, and Schatsky 2016; Szabo 1997). SC is one of the productive elements of blockchain that helps automate predefined operations and applications. It contains a simple series of operations in the form of code and works like a conditional and predefined decision support mechanism inside the blockchain network. SC makes the functioning of blockchain easy by assigning access permission and making each action deterministic (Makhdoom et al. 2019) and reduces human interference and error in manufacturing processes. Design, implementation, and validation of SC are done under the supervision of multiple parties involved in the system and the network to ensure appropriate access control and contract enforcement. Once finalised, SC is deployed on the top of blockchain. It makes the operations safe because SC cannot be modified once deployed in the blockchain network. The defined SC provides automation, intelligence, and privacy protection to the system.

An example by Angrish et al. (2018) is simplified to illustrate the integration of blockchain in manufacturing applications. Manufacturing service providers have multiple manufacturing machines, each with a unique identity. Every operation on a particular machine is recorded and stored in the blockchain. These transactions (i.e. manufacturing data or events details) include diverse information such as (1) machine information like machine installation, service, upgrades, breakdowns, and access log, etc.; (2) machine utilisation can include recording events such as overall equipment effectiveness (OEE), maintenance records, downtime, up-time, and power consumption; and (3) machine capability, such as consumed materials, workpiece type, process capabilities, etc. It is shown in Figure 4. The machine utility information is meticulously recorded, forming a continuous chain of events within the system. Subsequently, this recorded data is disseminated to all nodes in the blockchain network, ensuring comprehensive verification and validation. Each validated sequence of operations contributes to the creation of a trusted ledger with a reliable database. Such ability gives

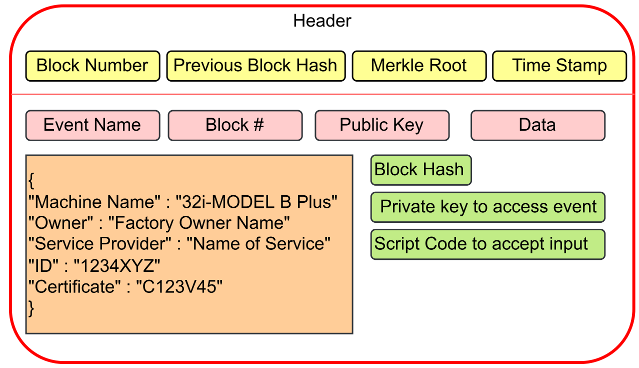


Figure 4. A Block with an event related to a machine asset.

blockchain an exceptional quality of micro-metering, micro-measurement, and dynamic adjustment at the root level. This feature can help evaluate the services and manufacturer's activities and analyse the quality of information flow (Takahashi 2017).

It is evident that each attribute of blockchain can serve as a benefactor in manufacturing operations. BC can secure storage and information transactions. A suitable kind of blockchain with the required attributes shall be integrated as per the necessity of the specific manufacturing application for the best performance. For instance, A private blockchain is advisable in an operation in which there is a need for high scalability for confidential data transactions. Blockchain is getting more and more recognition in industries. Hardly within a decade of the democratisation of blockchain, IBM's (IBM 2017) study revealed that major C-level executives are considering engaging with 'blockchain technology'. We are yet to see the potential of the full-fledged adoption of blockchain in manufacturing industries.

2.3. Convergence of blockchain and AI

It is evident that (1) the efficacy of AI is completely dependent on data that is vulnerable in terms of security, and (2) blockchain can aid in mitigating the security issues of data. However, the integration of AI with blockchain is not a one-way relationship. AI and blockchain can form a synergistic relationship to enhance each other's capabilities.

Blockchain can accelerate the performance of AI by offering it an abundance of secure data. Blockchain platform makes it possible to have access to intra- and interlayers of the system through data tracking. Similarly, having access to multiple layers of data allows the system to operate on more relevant information to enhance performance. Due to Blockchain's secure and privacy-preserving properties, it can encourage industries or individuals to share more data (Tanwar et al. 2019).

Blockchain can easily implement a reliable incentive-based system. Blockchain has also served as a coordinating platform for connecting untrusted devices for joint decision-making. There is always a risk while extracting data from a centralised server due to the singular control over accessibility. Chen et al. (2018) raised concerns about storing the data from different sources at a centralised server. The monopoly of authority in the case of a centralised server compromises the guarantee of tamperless data. The decentralised property of Blockchain yields the provenance and historical aspect of information, which makes it secure from hackers and prevents data manipulation (Ferrer 2018). The decentralised nature of Blockchain, as in Ethereum or Bitcoin, with thousands of online participants, will never go offline. The decentralised server can help extract assured knowledge, perception, learning, and reasoning by abolishing the centralised server. The decentralised nature of Blockchain helps in achieving privacy-preserved learning and enables the development of personalised models (Kurtulmus and Daniel 2018). We can integrate Blockchain with federated learning, where the AI algorithm is trained on data available locally across multiple edge devices without any data sharing or exchange (McMahan and Ramage 2017). Fu et al. (2020) presented a blockchain-based AI-enabled connected and autonomous vehicle platform to train ML models locally and uploaded the model to the Blockchain to utilise the collective intelligence. Just like the incentivization of the data providers for providing high-quality data, the AI model owners can also be rewarded for deploying their models for use by others. Deploying the AI models on the decentralised Blockchain can aid in the validation and verification of the AI models by the other participants of the blockchain (Mougayar 2016). The parameters of the trained AI model can be stored in the Blockchain to ensure its integrity. Any change in the model parameters, as during fine-tuning for a specific task, will be reflected in the Blockchain. Overall, Blockchain can ensure ownership and control over the data as well as the AI models. Lastly, we want to emphasise that Blockchain's consensus algorithms can prevent the incorrect predictions of AI from propagating in the network or the manufacturing systems. If, at all, an incorrect prediction of AI propagates through the manufacturing system, the error can be traced back to its source. Thus, Blockchain can improve the decision-making in manufacturing systems by offering better data to AI as well as offering the correct predictions of AI to the manufacturing systems. In other words, Blockchain can improve the data to and from AI for the betterment of manufacturing systems.

Just like BC can ensure the security of the data for the AI algorithms, AI can also enhance the efficiency and usability of BC in many ways. Consensus algorithms, like PoW, are energy intensive. AI algorithms can be employed to optimise the energy consumption of BC operations (Olaniyi, Alfa, and Umar 2022). ML can be used to predict the optimal strategy for a consensus protocol in a given environment, such as predicting the best time to mine a block in PoW or deciding the optimal bet in Proof-of-Stake (PoS) systems (L. N. Nguyen et al. 2019). ML can help identify anomalous patterns and malicious nodes to detect potential security threats in blockchain transactions. Thereby improving the security of the BC network. For instance, consider the multiple incidents of stealing cryptocurrencies (De 2017). The leak of identities of the nodes and the issue of pseudo-identities can be resolved using AI-based proof-of-conformance mechanisms. One of the major causes is exploiting a bug in the smart contracts. In such cases, AI can detect if the BC network is under attack to invoke suitable defense mechanisms. For instance, AI can classify the nodes if they are malicious and then isolate them from transacting to save the network. AI can enhance the performance of blockchain by accelerating transaction speeds. With intelligent algorithms, transactions can be processed and validated more quickly, thereby increasing the overall efficiency of the blockchain. Sarda et al. (2018) demonstrated how BC can also verify the work history of job applicants in real-time. Machine learning can be used to analyse and validate smart contracts in blockchain systems, helping to prevent fraud and malicious activity (Nikolić et al. 2018). AI can help in achieving efficient blockchain scaling by intelligently managing resources and transaction verification processes, thereby increasing the transaction throughput and overall performance of the blockchain network (Zheng et al. 2017). AI can address the scalability issues in BC by optimising the handling of the vast amount of data blocks in the blockchain, making the system more efficient. AI algorithms can be used for data pruning, compression, and optimisation. Machine learning techniques can also be employed to improve user privacy on the blockchain. Techniques like differential privacy can be applied to ensure that individual data within the blockchain remains confidential (Abadi et al. 2016). AI can help improve the quality of data on the blockchain. By employing ML techniques, the system can identify and correct erroneous or incomplete data, thereby ensuring that only high-quality, reliable data is stored on the blockchain (Hoy 2017).

From the above discussion, it is evident that blockchain and AI can have a synergistic relationship where they can amplify each other's capabilities while undermining each other's shortcomings. Blockchain suffers from scalability and efficiency, while ML has trustworthiness,

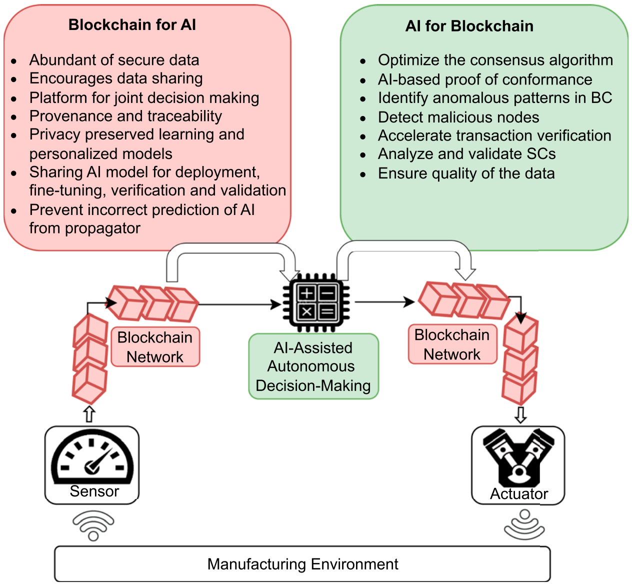


Figure 5. A cyber-physical system model of an AI-assisted manufacturing system integrated in a blockchain fabric.

explainability, and privacy issues. Combining both technologies has a significant potential in industries dominated by data (Dinh and Thai 2018). Blockchain will help ML's decisions to be more transparent, explainable, and trustworthy. As all the imported data into the ML model will be visible to permitting authorities operating within the blockchain network, this gives surety to the organisation while sharing data and offers more confidence in the decisions made by the ML model (Mettler 2016). So far, ML has been utilised in manufacturing applications without any regard for data security. Blockchain could work as a security layer for ML to produce trustworthy decisions for better functionality of manufacturing operations. A CPS model of a manufacturing system that makes autonomous decisions using AI which is connected using a blockchain network is depicted in Figure 5. The convergence of blockchain and ML make a secure solution that can enhance the productivity of manufacturing application and could open the door to new possibilities. Still, the integration of blockchain in practical applications is in its infancy. Our work moves a step ahead by integrating blockchain in AI-enabled industries. For that, we need to understand the requirements of modern manufacturing systems.

3. Requirements of modern smart manufacturing systems

In light of mass individualisation, it is essential to emphasise the *smart* nature of modern manufacturing systems, which allows them to reconfigure to meet the customised demands with the best system performance while using optimal resources. Mourtzis (2020) emphasises the significance of digital manufacturing technologies, such as simulation, in facilitating product experimentation and validation. These smart manufacturing systems involve *collaboration* among various organisations, industries, and individuals on a macro-scale, as well as *interconnection* and *interoperation* among different systems, sub-systems, and components on a micro-scale. The U.S National Institute of Standards and Technology (NIST) defines smart manufacturing as 'a fully-integrated, collaborative manufacturing system that responds in real-time to meet changing demands and conditions in the factory, in the supply network, and customer needs' (Thompson 2014). These smart systems need to learn from *data* to handle environmental uncertainties and faults. Data is *accessed* in a controlled fashion from all stages of the product's lifecycle to make the system really smart. Manufacturing data has played a crucial role since the beginning of Industry 4.0. The volume of data has increased to 40,000 Exabytes in 2020 and will double every two years, according to an IDC (International Data Corporation) report (Gantz and Reinsel 2012). With the advent of AI, new intelligent insights about the system can be discovered from its data which was impossible in the case of model-based approaches practiced earlier. As AI relies purely on the system's data for deriving analytical insights, data quality becomes a decisive factor in enhancing its performance. So, the accuracy of the data dictates the accuracy of the outcome. In other words, *tampered data* could lead to erroneous decisions and potentially jeopardise the product or the manufacturing system. We also highlight the need for contrasting goals of *data security* and *transparency* in modern manufacturing systems. They are summarised in Table 2.

Table 2. Requirements of modern manufacturing systems.

Requirements	Challenges	References
Interoperability	Secure coordination of disparate complicated systems with synchronous data	Lee, Bagheri, and Kao (2015)
Relevant data	High degree of irrelevant and redundant information	Yu and Liu (2003)
Access control	Difficulty in managing the control policy for accessing data	Outchakoucht, Hamza, and Leroy (2017)
Interconnectivity	Increased likelihood of faults and their propagation in cross-connected network systems	Sadeghi, Wachsmann, and Waidner (2015)
Data and System Security	Security problems when sharing their datasets inside and outside industry	Y. Liu, Yu, et al. (2020)
Tamper proof data aggregation	Use untampered data to get true results	Leng, Jiang, and Zheng (2017)
Transparency	Privacy-preserved transparency	Punter (2013)
Trust among participants	Building trust among participants for sharing data	Camarinha-Matos et al. (2009)

3.1. Interoperability

Complex systems usually consist of multiple systems and components that accomplish different functions to achieve a common goal. Those systems can be diverse in terms of their operations, the data they create, process, store and transmit, and the software or algorithm that they use. As the data is exchanged from one form to another, there is a risk of loss in semantics. A complex system requires more than one datatype and software to manage its value chain effectively, including personnel, materials, products, control systems, and equipment. Thus, *interoperability* is crucial for coordinating different systems, enabling the transformation of data for seamless communication, computation, and inference. Interoperability in manufacturing can be defined as the degree of communication and sharing of data among different stakeholders of the value chain (Lee, Bagheri, and Kao 2015). Technological compatibility and security remain two major hurdles in interoperability. Adoption of sophisticated components in the presence of legacy systems is difficult and is cost-intensive. Furthermore, proper integration of disparate systems for coordinated functioning while being secure to prevent theft of intellectual properties (IP) is challenging. Government regulations (e.g. Health Insurance Portability and Accountability Act Accountability Act 1996) demand even more stringent security measures.

3.2. Relevant data

As knowledge is distilled from data, data has become the new currency. Acquisition of relevant data remains a challenge for making decisions. Availability, quality, and composition of data influence the performance of ML algorithms. The dataset can have a very high dimension, which can adversely affect the performance of ML algorithms. In complex systems, each sensor adds a new dimension. While such sensory data is useful, some may contain a significant amount of redundant and irrelevant information. That irrelevant data can impact the performance of learning algorithms (Yu and Liu 2003) and call for better algorithms and computing resources. Each manufacturing operation could generate a tremendous amount of data at a time. It becomes cumbersome and time-consuming while selecting the features for analysis. Therefore, a data management system should be designed to reduce or handle the complexity of high volume. Additionally, the data management system shall be secure to not incur irrelevant information during transmission.

3.3. Access control

IIoT usually deals with a colossal number of devices for data collection and integration. The security policy for each connected devices is managed by the access control system of IoT. Static privacy policies and written access control rules make it difficult to manage each operation. The static nature of these policies fails to detect if it contains rules leading to security limitations that create conflicts or are sub-optimal. This approach never considers feedback from the results of its operation (Outchakoucht, Hamza, and Leroy 2017). The digitised equipment is the primary source of data through IIoT devices, sensors, and smart devices (Sadeghi, Wachsmann, and Waidner 2015). The end-to-end vertical and horizontal integration of the IIoT opens up loopholes for multiple vulnerabilities at the equipment level. For example, if the industry is manufacturing military equipment, national security becomes a concern. This risk inhibits ML engineers' access to data and fosters departmental silos that inhibit information sharing. Thereby, complicating data preprocessing and hampering ML model development. So, secure cyber tools are essential to establish consensus and ensure the authenticity of the manufacturing network. Standardized protocols are necessary to protect intellectual property and define the manufacturer's role in the decentralised manufacturing platform (Lee, Azamfar, and Singh 2019). The manufacturing industry requires strong coordination between upstream and downstream network operations, fostering mutual trust and security measures to promptly detect faults within the network.

3.4. Strong interconnectivity

Interconnection can open up a plethora of possibilities in manufacturing operations by harnessing the additional value offered by the inter-operation and information exchange among disparate systems, manufacturing facilities, and organisations. The interconnection of manufacturing operations can lower the lead time and drive to quicker customer satisfaction, thereby boosting revenue. An interconnected supply chain can reduce downtime in case of jerks in the supply chain and changes in the demands of consumers. Connections among the machines on the shopfloor can facilitate preventive maintenance, analysis of faults, and downtime. A variety of manufacturing models has been proposed to digitise the manufacturing industry, such as social manufacturing (Jiang et al. 2016), peer production (Kostakis and Papachristou 2014), open production (Wulfsberg, Redlich, and Bruhns 2011) and crowd manufacturing (Bonvoisin and Boujut 2015). The only goal of all these forthcoming innovations is to make the system crowded, clustered, and decentralised for global **c**ommunication, **c**ollaboration, and **c**ompatibility (three **C**s) to enable cross-enterprise manufacturing with interconnected networks. The key idea of interconnectedness is to propagate change throughout the network. For instance, an increase in the demand for a product shall propagate until (1) the machines that manufacture the product adapt to increase the capacity; (2) raw material supply increases accordingly; and (3) the quality control remains effective. However, this propagation needs to prevent the propagation of anomalies. The faults shall be suitably contained by appropriate security measures to avoid a domino effect. Thus, strong interconnectivity calls for a stronger security system.

3.5. Data and system security

The security of information and data hinges on three key aspects: confidentiality, integrity, and availability (CIA), known as the CIA pillars of data security (Prinsloo, Sinha, and von Solms 2019). Implementing these three pillars requires high computing capacity, enabled with computers and servers for information processing, often not readily available in manufacturing systems. Major IT communication protocols are designed to support the CIA pillars. However, it is not always compatible with manufacturing systems. There is a need to develop a personalised communication protocol for manufacturing. For example, hypertext transport protocol (HTTP) is designed explicitly for IT structure. There is a one-way control authority between the server and the client, which is not suitable for manufacturing systems. The manufacturing systems can act as a server as well as a client. Transferring high-performance technology to a low-level system leaves the system doors open for hacking and malicious attacks. Such vulnerable environments can be amplified due to poor selection of technological platforms. Security and privacy preservation becomes critical particularly in ML-based approaches where information exchange is amplified. Manufacturers face security problems while sharing data with insiders as well as outsiders. Generally, ML adopts a centralised architecture for accessing data. Centralized servers are prone to hacking, and any malicious activity can manipulate the data. Furthermore, the data used for training ML models are usually in large quantities, which may involve private information. Therefore, protecting the data from hackers is a critical issue (Y. Liu, Yu, et al. 2020). Lately, browsers like Chrome and Edge have introduced password monitoring services (O'Donnell 2021). It shows the severity of the data breach. Lastly, aggregation of data from different sources also raise privacy concerns.

3.6. Tamper-proof data aggregation

Recognizing that more data equates to a better understanding of their systems, modern organisations dedicate resources to data aggregation and deploy ML algorithms for analytical insights. Those ML models need a safe platform for performing analysis on outsourced data. The imported data should be tamper-less, without error and noise. The ML model needs to use tamper-less data to get true results, and the final aggregated result needs to be stored securely. For instance, mean square error (as with any p-norm error with $p \geq 2$) used as the loss function in ML models for regression tasks can shift the learned function in the presence of significant abnormal data. It underlines the importance of untampered data in industrial applications. A minor error in the final decision in mass production could be hazardous and result in a loss of millions of dollars in revenue and a waste of time. Moreover, tampered data can compromise the customers' trust and violate government regulations for preserving privacy. So, the manufacturing platform should be robust enough to avoid erroneous, illegitimate, and tampering with data (Leng, Jiang, and Zheng 2017).

3.7. Transparency

To understand the importance of transparency, trust, and decentralisation in manufacturing, the case of a manufacturing supply chain is considered. A proper supply chain is essential for the timely and safe delivery of goods and services matching the demand. If the supply of a critical component or service is disrupted, the consequences can be devastating in the later parts of the supply chain. It can incur financial losses as well as loss in the organisation's reputation (Punter 2013). Globalization has been increasing the complexity of supply chains. The knowledge of product provenance, process, supply network, and final utilisation is not emphasised and is never recorded due to the diversity (at both micro- and macro-levels) in manufacturing operations. If it is recorded, it is done locally. The record only stays with the individuals (suppliers, transporters, storage facilities, retailers, and distributors). They are never shared due to privacy concerns and for fear of losing competitive advantage. Thus, almost always, the product journeys remain a mystery and cannot be traced back to their provenance (Jessi, Jutta, and Wood 2016). Such behaviour can result in counterfeiting, environmental damage, and unethical trading. This has emerged into *ethical consumerism*, where the product's footprint (How it is manufactured? How it will be used and disposed of?) aligns with the ethical values of the consumer. Transparent trading and enhanced traceability of supplied product networks can help analyse and deter the risk associated with the supply chain.

3.8. Trust in collaboration

Collaboration is another concept that industrialists often emphasise in order to gain the most advantage from cross-functional teams. Manufacturers want to get connected with their clients to get feedback and improvise their products. The majority of companies face security issues when sharing their machine, logistics, and clients' information inside and outside the factory. If a new vendor joins the industry, it takes time to build trust for sharing data. Similarly, whenever there is a need to hire a third-party service provider, a lack of cross-functional support hinders the development. The hesitation to share data for better feedback hinders industries from understanding their product supply flow for monitoring. Therefore, a secure multiparty collaborative platform (Frey, Wörner, and Ilic 2016) that enables manufacturers to connect with other participants while only sharing the necessary data is essential. If the privacy protection issues are resolved, data sharing can increase while decreasing fraud/misuse. In the case of using digital twins for personalised product designing, effective strategies for ownership sharing and dominance over data also need to be considered (Mandolla et al. 2019).

Thus security, end-to-end trust, traceability of products/services, autonomous decision-making, and reliability are indispensable in modern manufacturing systems. Their importance is ever-increasing to maintain the integrity of the system. Fulfilling these requirements is beneficial in making the manufacturing system competitive and flexible to adopt newer product lines and technologies. Securing the cyber component has become crucial with the conversion of legacy manufacturing systems into CPSs and the rise of data. The cyber component was relatively insignificant in legacy systems. There have been many incidents where the integrity of modern manufacturing systems was compromised due to the lack of proper measures for cyber-security. We quote a few before proposing our blockchain-based solution.

4. Case studies of security vulnerabilities

Cyber-security is a relatively new field for the manufacturing industry. It is still nascent due to the lack of knowledge among most manufacturing stakeholders. Often, industrialists and developers consider digital security a secondary priority putting more emphasis on productivity and higher yield of production line (Tuptuk and Hailes 2018). They try to scale the production up and interconnect different systems without considering the new security issues that may arise. So, we briefly discuss manufacturing mishaps to realise the security requirements of modern manufacturing systems. Table 3 summarises them.

Table 3. Security vulnerabilities in manufacturing systems.

Properties	Key Issues	Reference
Security protocols	- Lack of security protocols - Poor communication platform	Schluse et al. (2018)
Global collaboration	- Intellectual property theft - Third party access to classified industrial information	Podgorelec, Turkanović, and Karakatič (2020)
Low level manufacturing information flow architecture	- Less computational power to handle connected equipment - Low level security system	Prinsloo, Sinha, and von Solms (2019)
Scalability	- Needs extensive planning - Maintaining latency, security and throughput	Rahman et al. (2020)
Cradle to grave	- Scope of tampering during data transactions - Difficult to detect malicious files	Lv et al. (2018)
Human Element	- Intentional breach into system by malicious actors	Peng et al. (2017)

4.1. Breach into control systems

The Maroochy Shire sewage incident in Queensland, Australia, in the year 2000 (Sayfayn and Madnick 2017) is one of the examples to understand the impact of cyber theft in operational technology. It is a breach in the security of the SCADA (**S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition) system. Investigations revealed that an ex-employee of the plant hacked the sewage pumping station and telecasted a wrong message to hack the SCADA system, which controls over 140 sewer pumps. The ex-employee was able to access the system due to the incompatibility of the IT security protocols with the communication and control systems. The pumping station and the control system were communicating through a private two-way radio communication system. The hacker was able to access it due to the lack of cyber-security measures in the sewer plant control system. After introducing the SCADA system, which communicates through transmission control protocol, the number of cybersecurity breaches increased dramatically. Stuxnet is notorious (ruined Iran's nuclear facilities (Kelley 2013)) for targeting SCADA systems and PLC control systems. The ease of unauthorised access was due to the deployed security protocols, which were not compatible with operational technologies. Now, if such a mechanical system (e.g. actuator diagnosis scheme) is operated through AI, it can pose a severe threat by providing wrong results

(Delgado et al. 2011). Therefore, it is essential to have a secure infrastructure to implement AI-aided decisions confidently.

4.2. Manipulation of files

Belikovetsky et al. (2017) illustrated the failure of a 3D printed component during operation due to manipulation of its CAD files. The CAD files of propeller blades were manipulated by an intruder. The drone fell as the blades of the drone broke apart during flight because of the reduced fatigue life of the manipulated design. This is a classic case of spoofing CAD files using WinRAR ZIP files. The intruder gained access to the CAD files by using a malicious attachment contained in an email. This illustrated the failure of collaboration due to a lack of security measures. Additionally, by democratising the capability for production, AM also democratises the capacity to copy, thereby violating the ownership of creative designs. The susceptibilities in design can also arise by introducing unwanted voids (Sturm et al. 2017) or contaminants (Zeltmann et al. 2016) in the STL files. Nonetheless, these vulnerabilities are equally applicable in conventional manufacturing as they are in AM. It is just that AM is more investigated because it is in its early stage of commercial adoption. Therefore, it is necessary to take proper security measures in cloud-based operations to reduce hazardous and uneconomical incidents.

4.3. Data breach

Data theft via breaches in CPS is the top-ranked crime in the manufacturing sector. In 2020, World Economic Forum (WEF) has listed data fraud and cyber-attack as one of the top ten economic risks (WEF 2020). DuPont, a large chemical manufacturer, has also been a victim of data theft. Yonggang Min, a former research chemist, pleaded guilty to breaching DuPont's intellectual property (Connolly 2007). Min has been downloading and accessing the company's electronic data for a long time. He was about to start his new employment with Victrex PLC (Asia), which competes with two of DuPont's products (Kapton® and Vespel®). DuPont did not have a strong cyber security layer to protect itself. A recent incident of data theft happened in 2022 with Hanesbrands Inc. (Brown 2022). A hacker accessed to company's customer database through the company website. Hackers pretended to be guest customers to gain access. They stole nearly a million addresses, phone numbers, personally identifiable information (like driver's license numbers and Social Security Numbers) as well as the last four digits of the payment card on file for customers. Hanesbrands had to spend $15 million to fix its disrupted supply chain (Kan 2022). Moreover, it lost about $100 million in sales in the next quarter.

4.4. Security issues in scalability

The manufacturing industry is always keen to expand its production and capacity to meet the market and demand requirements. Moreover, industrialists often opt to modify (rather than installing afresh) the existing production lines to maximise profit while optimising the production time and cost by adopting new digitised technology for a distributed infrastructure. Optimal scalability requires both horizontal and vertical integration. Traditional systems like Manufacturing Execution Systems (MES) and ERP systems are monolithic and thus operate in isolation. They necessitate semantic mediation for effective cooperation between them. As the digital component of the manufacturing systems is based on cyber-infrastructure, it becomes essential to extend the digital thread to support the information flow. However, this extension results in an information surge, highlighting the importance of scalability in data servers and production when incorporating new equipment (Feng et al. 2011). NASA's adoption of complex controllers and interconnected information technology (IT) equipment for automating and scaling up its manual control and legacy operational technologies (OT) illustrates the potential security vulnerabilities in scaling up (Office of Inspector General – Office of Audits 2017). In one instance, a security patch disrupted a monitoring device, causing a fire that destroyed valuable spacecraft hardware because the patch hindered the activation of a safety alarm. This emphasises the need for caution when scaling up to prevent similar incidents.

4.5. Security gaps from cradle to grave

The cradle to grave of any product, starting from conception to CAD design to manufacturing, involves several steps (Apsley et al. 2017). Each step leaves scope for cyber theft or attack (Holland, Nigischer, and Stjepandic 2017). Prior to the actual production, the object is conceptualised, and the concept is documented. It is followed by creating a 3D model in solid modeling software for visualisation. The constructed CAD model is converted into stereolithography (STL) file format, which is readable by manufacturing hardware machines, e.g. CNC machines. It can be deduced that there are multiple stages, and thus, numerous gaps for the attacker to install malicious files and corrupt the process. We have discussed an example of a malicious CAD file in Section 4.2. The CAD files can be corrupted with voids (Sturm et al. 2017) and contaminants (Zeltmann et al. 2016). These subtle malicious files can remain undetected due to the multiple operations going on simultaneously. They can create operational hazards. Another thing to note is the possibility of multiple file exchanges, which raises the question of confidentiality. Manufacturing data is not usually encrypted. Turner et al. (2015) were able to intercept the data by using Wireshark and extract important process parameters. Nowadays, open-source development has become widely adopted in many applications. Moore et al. (2016) analysed the vulnerability of open source 3D printing software like Cura 3D (for slicing) and Marlin firmware. They highlighted the USB communication and undocumented code, among other vulnerabilities, to sabotage the machine or the manufactured product and expose IPs. Al Faruque et al. (2016) showed that every product has a unique acoustic signature which can be inferred upon analysing the sound of the machine during its manufacturing. They were able to reconstruct test objects to demonstrate the physical to cyber attacks. To take control over security situation, the product should only be accessible to authorised users by putting a particular layer of security. It is evident from the above discussion that an optimal balancing point between authorisation, distribution, and confidentiality is necessary to operate smoothly.

5. Blockchain in AI-assisted manufacturing

We start by identifying the key differences between blockchains developed for manufacturing systems and those typically designed for financial transactions, such as cryptocurrencies and supply chains. First, the goal of blockchains developed in general is different from those developed for manufacturing systems. Blockchains for cryptocurrencies attempt to replace fiat currency transactions (backed by government regulations). Whereas manufacturing blockchains strive to replace manufacturing software-based tools (e.g. ERP, CRM, Document Control Systems, etc.). Manufacturing tools usually operate within an organisation. Blockchain can integrate different organisations by supplementing common tools. Second, most blockchains try to facilitate transactions among an unlimited number of anonymous participants. In contrast, manufacturing systems involve a set of known parties, like the manufacturer, its multiple facilities, machines, sensors, suppliers, finance, and optionally a known or relatively unknown customer base. Thus, protection from unknown parties becomes significantly important in manufacturing blockchains. Third, applications like cryptocurrencies want every participant to be able to make new blocks of transactions and to have control of the blockchain. Thus, they adopt public blockchains to make a trustless system. Manufacturing industries are different in the sense that they want only authorised participants to have control over the blockchain and only authorised users should be able to add new blocks. Thus, consortium (and sometimes private) blockchains are more suitable. The consortium can define the SCs and adapt the SCs for new developments. Consortium blockchains can minimise risks in data and collect competitive intelligence. A consortium blockchain was developed for a CPS-based ubiquitous manufacturing (Vatankhah Barenji et al. 2020). Fourth, the public Blockchains follow a Proof-of-Work consensus protocol where the miners try to determine a unique hash to create a new block by solving a computationally hard cryptographic problem. There is a competition. The first one to do that is rewarded with a transaction fee. Manufacturing blockchains need not compete. The consortium or the owner of the blockchain can be responsible for creating the blocks. The lack of competition significantly reduces the energy consumption and computational demand of an operational manufacturing blockchain. Fifth, generic blockchains usually have only one kind of flow: the financial flow of cryptocurrencies. The unit remains the same. Whereas manufacturing blockchains can have more than one kind of flow. It can constitute financial flow (in USD), inventory flow (units of a specific object), and information flow. The information flow is diverse in the sense that it can consist of data from different sensors, power consumption, etc. Nodes consisting of suppliers and manufacturers can add blocks involving transactions of finances and inventory. If we consider sensors as the participants, they can transact information and power. Machines can transact inventory, power, and diagnostic/maintenance information. Maintenance information can aid in the preventive maintenance of the machines. The inclusion of machines as nodes can ease the tracing of products to the machine that processed them in case of defects. Manufacturing environments may need more than one Blockchain, one for each kind of data. Manimuthu et al. (2022) used four blockchains: a financial blockchain, a raw material blockchain, a transportation blockchain and an insurance market risk blockchain. Lastly, generic blockchains are dominated by only a cyber component. Participants have cyber addresses. They make financial transactions. Manufacturing Blockchains need a close integration of cyber and physical infrastructure. IIoT and CPS can enable this. These differences are summarised in Table 4.

A generic blockchain framework can be overlaid on the manufacturing system where all the manufacturing systems and data are integrated into the distributed BC database. As discussed in Section 2.2, manufacturing information such as entry of new equipment, entry of new employees into the system, communications (emails,

Table 4. Comparison of manufacturing blockchains with generic ones (like cryptocurrencies).

Criteria	Generic Blockchains	Manufacturing Blockchains
Applicability	- Financial transactions	- Manufacturing systems
Participants	- Unlimited number of anonymous participants	- Limited number of known participants
Type of Blockchain	- Public	- Consortium (or private)
Consensus mechanism	- Open competition to find the unique hash - Reward for the miner - Huge energy consumption	- Competition and rewards can be optional - Relatively lesser energy demand
Data	- Financial data (e.g. currencies)	- Financial, inventory and other information (e.g. power, sensor data)
Cyber-physical nature	- Purely cyber in nature	- Close integration between cyber- and physical-components is required

chats), and product catalog, production, machine details, down time will be included in the blockchain database. Each node in the blockchain network is a participant with an assigned role, e.g.registrar, certifiers, industrial peers (people responsible for data entry/management), and manufacturing departments (machine shop, supply chain). Each participant accesses the data in the blockchain via a customised user interface (UI) according to their role in the system. The data access granted to the participants changes depending on their authority/role in the network. The BC database can be operated by a user with administrative access privileges in the case of private and consortium BCs. New peers can join the network by registering once they get a unique identity to join the network. Certifiers are responsible for providing certifications to participants. All data in the network is stored on a BC and is available to the participants with the correct authentication (Abeyratne and Monfared 2016). This restricts the users to only access the authorised data. The set of rules that govern the system is written in code and stored in the SC of BC. These rules define (1) the process for new participants to join, (2) how the participants in the BC can interact among themselves and with the system, (3) the rules for sharing the data in the BC, (4) data access privileges, (5) validation rules among many others. The rules cannot be altered by the participants and therefore guarantees the integrity of the data and the blockchain. The rules stored in the SC cannot be modified without alerting all the nodes. Thus, it prevents any user from going rogue and tampering with the data or the rules. All the operational tools are linked to the distributed BC database and its servers. The AI users act as nodes in the BC network to access the authorised data and push the results and analytical insights to the BC. This is depicted in Figure 6. If the data is encrypted prior to sharing, the AI users decrypt it before deploying AI algorithms for classification, control, regression, or generation tasks. The other users can access the AI insights from the BC. The millions of the transactions of manufacturing systems are appended as blocks to the BC upon validation. Each operation in the BC network (like node verification, transaction request, transaction verified, consensus algorithms, smart contracts, and transaction approval) opens up opportunities for attacking the BC. The vulnerabilities can arise due to the intrusion of a malicious node (for data theft or approving fake data), among many others. The 51% attack (attack by miners controlling more than 50% of the blockchain's mining hashrate) and sybil attack (faking the identity) are noteworthy as the BC follows a majority consensus protocol for validation. AI can serve as a solution to safeguard the BC network against such attacks. At each stage of BC operation, adding a layer of AI could increase efficiency and the confidence in the functioning of the blockchain-based manufacturing system apart from just deriving analytical insights from the secure manufacturing data.

There are a few investigations that integrated BC in AI-assisted manufacturing. A private Hyperledger Fabric platform was built by Shahbazi and Byun (2021). They presented a transaction history portal that includes all the activities completed, which are approved transactions. The information contained the dates, times, entry types, and participants. The overlayed AI algorithms (XGBoost and kNN) classified if the data was real or fake. A decentralised blockchain with federated AI was developed by Manimuthu et al. (2022). The acquired data was classified locally using support vector machines before adding to blockchain. Then the data was used to predict the raw materials, energy consumption, and insurance in an automated automotive assembly application. A group of five CNC machines connected by blockchain was able to predict the prices and the profit margins of the products they manufactured using a set of ML models (Hasan and Mullick 2021). We conclude this section by discussing the potential opportunities in a manufacturing system integrated with blockchain and AI.

5.1. Early phase of product and process planning

Globalization, e-commerce, and digital socialisation have spurred a rise in personalised product demand, reflecting a shift toward a more consumer-oriented industry. Some manufacturers (like *Creator's club* by Adidas,[6] *Nike by you*[7]) even allow the customer to design the product as per their preferences. Customers are getting products and services of their choice instead of choosing something from the available product pool. Moreover, when the demand is not individualised, the manufacturing

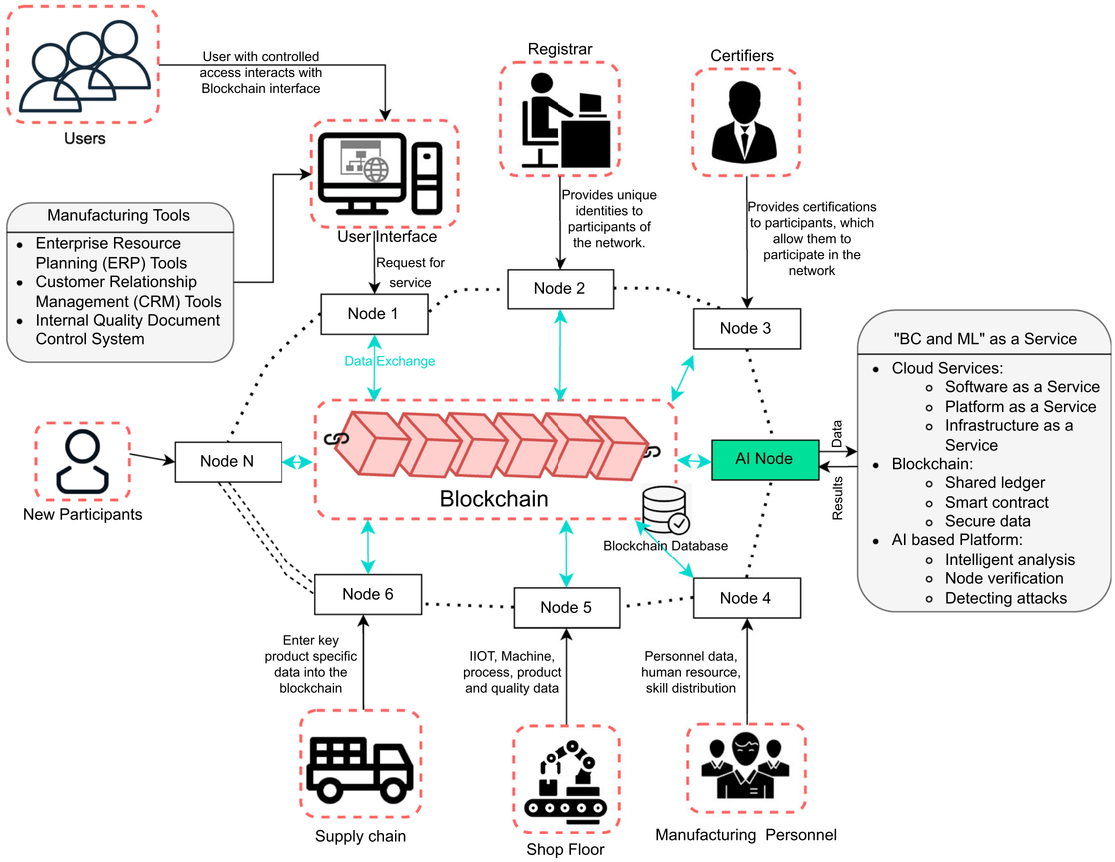


Figure 6. Common System Architecture for blockchain and Machine Learning application in manufacturing.

industry has to involve in various networks to manage a large number of product service groups to fulfill the demands of the consumers quickly (Leng et al. 2018). So, manufacturers need to expedite critical decision-making by understanding customers' demands, responses, and evaluations effectively. ML has become the predominant tool for knowledge extraction and prediction from customers' feedback and opinions. Thus, many critical decisions can be made for early-phase product development using ML (Ullman 1992). Online reviews and surveys can provide product requirement insights, which are then categorised (Aguwa, Olya, and Monplaisir 2017) and analysed (Hoornaert et al. 2017) using AI to align with product specifications. Security concerns can sometimes deter consumers from providing feedback. Blockchain technology addresses these concerns by creating digital identities for consumers, allowing them to participate anonymously in the network. Additionally, newly added participants are allowed to join the network after verification. Thus, BC improves the service offering (Baumung and Fomin 2019). In such cases, BC can serve as a platform for the consumers, and ML can be utilised as a data processing tool to ensure that correct data is being stored and approved into the BC network. AI algorithms can bring in more value from the data after extracting it from the blockchain. It is illustrated in Figure 7 using four distinct blockchains. Blockchain I verifies participants' digital identities with cryptography, maintaining anonymity yet ensuring secure network participation. Blockchain II collects data using AI tools with advanced NLP and machine learning algorithms for processing and extracting necessary information, thereby providing a reliable, auditable data repository. Blockchain III serves organisations involved in product design and prototyping by offering a decentralised data-sharing and access platform, thus facilitating accurate designs based on shared information. Federated learning (Deng et al. 2022) can be used to train the model within the periphery of the data owner and transact the ML model through the BC network. The data can leverage all tools that can add value, such as AI, AR, and data visualisation. Blockchain IV is dedicated to secure document storage, ensuring the integrity, traceability, and accessibility of crucial documents such as reviews, compliance records, and potentially patents (Pradeep et al. 2021). Such blockchain networks provide a cross-domain platform to securely store the operating characteristics of new products and safeguard sensitive product data. Collectively, these blockchains form a robust ecosystem for efficient participant verification, data collection, analysis, collaborative design, prototyping, and secure document management. This network also provides a secure cross-domain platform for storing new product operating characteristics and safeguarding sensitive product data. A Blockchain-operated cloud manufacturing is proposed by Barenji et al. (2019) for on-demand secure service. This can facilitate a secure ML framework, as there will not be any scope for data tampering. Yoo and Won (2018) proposed a smart contract-based architecture that tracks the price of the service for customer relationship management to avoid exorbitant prices and make the transactions more transparent. *ManuChain* incorporated a decentralised blockchain into a digital twin for individualised manufacturing (Leng et al. 2019). This prototype helps eliminate unbalanced data between global planning and local execution using permissioned blockchain and integrates upper-level optimisation with lower-level self-organisation to make the system intelligent.

5.2. Collaborative design

The process of designing a product needs many resources, such as design tools, product information, equipment, and designers (M. Wang, Zhang, and Zhang 2019). The design process needs diverse skills and resources, which entail collaboration among a diverse workforce. Industries are moving toward a ubiquitous and digitised platform to reduce the lead time in all stages of production, including design. Nonetheless, current design issues include weak design ability due to high customisation, object-oriented demand, low concurrent design capabilities, and lack of standardised information for resource sharing. Such complexity is avoided by integrating internal and external design resources through a network-based design pattern (Wu et al. 2015), which will help create synergistic cooperation in enhancing the comprehensive strength (B. Li, Zhang, and Shi 2012). The network-based design includes approaches such as concurrent design, collaborative design, virtual design, optimisation-based design, etc. These methods are implemented with machine learning to better predict optimised parameters, geometric accuracy, thermal deformation, tool wear, and dimensional accuracy (Wuest et al. 2016). While collaboration accelerates information sharing, it also calls for securing the innovators' IPs and rights. Moreover, the collaborators must be prevented from accessing unauthorised data. The involvement of third parties exacerbates the issue further.

Combining blockchain technology with collaborative design addresses several issues that arise in the collaborative design process. As depicted in Figure 8, participants,

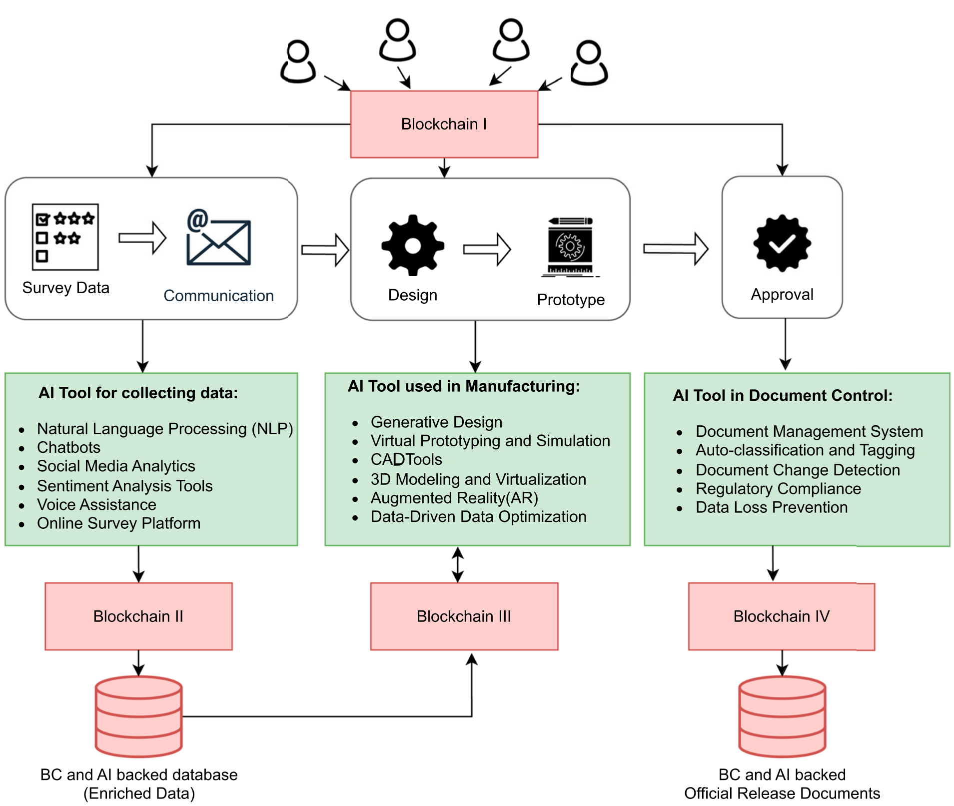


Figure 7. Early phase product design using blockchain.

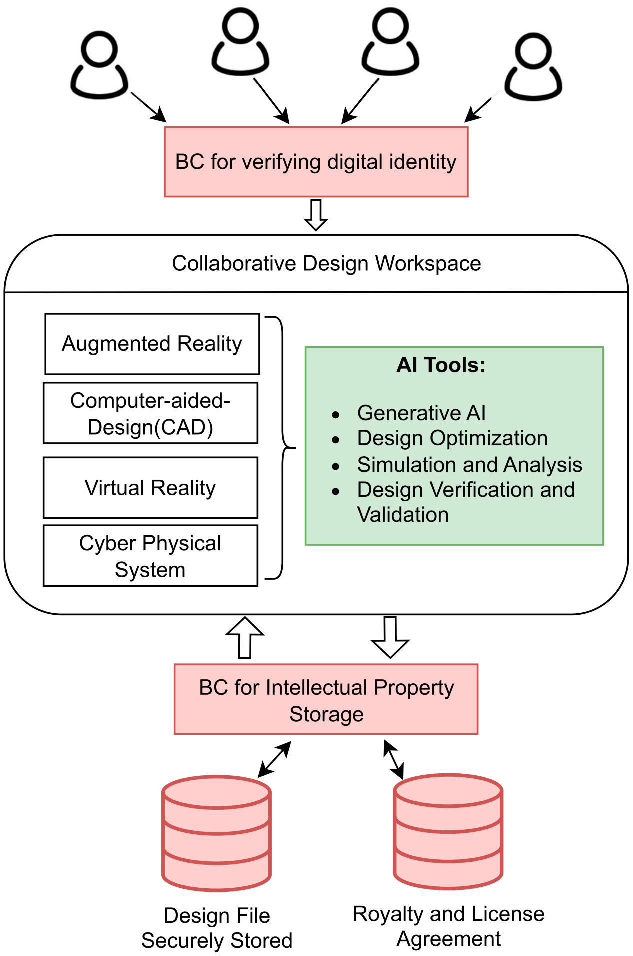


Figure 8. Collaborative design using blockchain.

including designers, scientists, and industrialists, can join a collaborative design network facilitated by blockchain. Blockchain ensures the verification of their identities (Mohamed and Al-Jaroodi 2019), allowing only verified participants to access the collaborative design workspace environment. Within this workspace, participants leverage AR, VR, CAD, and CPS to actively engage in the product design process (Cannavo and Lamberti 2020). Augmented reality (AR) technology (Sahu, Young, and Rai 2021), which can add digital information to the physical environment, is a promising solution for collaborative design assistance. The CAD model, which shapes the idea of a product, can receive feedback using AR technology and facilitate concurrent design. AI tools are seamlessly integrated into the environment, simplifying complex tasks and fostering a productive design workflow. The design variables, historical data of constraints, and objectives can be uploaded to BC. Once the new design is stored in the blockchain, engineers, scientists, or third parties (contingent workers) can work on the documents/data by generating access requests through BC. BC uses SC and consensus algorithms to grant access and store the transaction activity in the BC. Once the design is finalised, it can be securely documented and stored in a blockchain-backed database. This database serves as a repository for design files, as well as royalty and license agreements (Alkaabi et al. 2020). Design files can be requested through the blockchain network, with SC granting access based on specified accessibility requirements. Additionally, smart contracts can be designed, as referenced in Mehta et al. (2021), to automate the process of granting royalties upon the utilisation of specific designs and patents. By establishing this environment supported by blockchain, collaborators can work with confidence and peace of mind, knowing that their data is safeguarded against theft or unauthorised access. Collaborative CAD environments have been proposed by Q. Liu et al. (2019) and H. Zhang et al. (2017) for system design, product lifecycle management (PLM), and data management. It gained popularity because of its integration with blockchain to enable data integrity in collaborative CAD environments (Lemeš and Lemeš 2019). D. Guo et al. (2020) proposed a framework for customer participation in the product's life cycle management through BC and digital twin technology. Blockchain-based collaborative CAD environment is used in product data/lifecycle management and building information management. A blockchain-based reengineering system is proposed by Comuzzi, Unurjargal, and Lim (2018) that analyses design use cases to construct the design space. The SCs can aid in automating the maintenance alerts in PLM services (X. L. Liu, Wang, et al. 2020).

5.3. Manufacturing process

Modern manufacturing systems have evolved to become autonomous, facilitated by the Industrial Internet of Things (IIoT), enabling continual M2M and M2H communications. IIoT-based sensors primarily monitor the manufacturing system and environment to identify malfunctions. This data informs automated systems, which use AI to identify optimal process parameters, predict errors, and manage dynamic situations. AI aids in decision-making, predicting failures, suggesting maintenance procedures, and enhancing functions like image recognition, feature extraction, and text mining, thereby improving efficiency. However, in such AI-assisted automation, data safety and security protocols must be in place before offering data-driven intelligence services. Here, blockchain can provide a security solution. This is illustrated in a conceptual framework (Figure 9) for integrating BC and AI in manufacturing systems, where the system is connected to IIoT devices that record data into a BC database. Manufacturing data is fortified

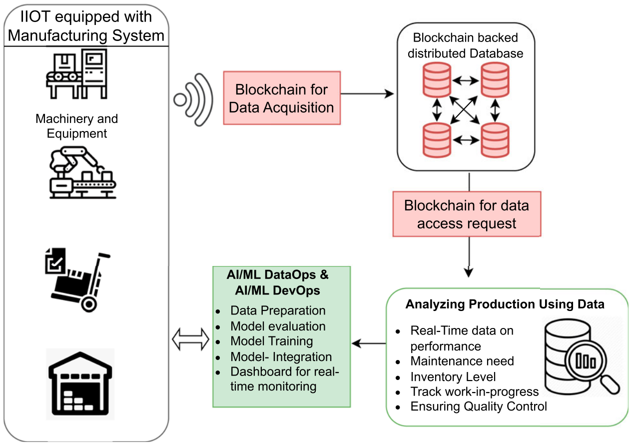


Figure 9. Machining process analysis in a blockchain-enabled system.

with robust access control mechanisms, enabling seamless data communication with the blockchain database and providing convenient access to stored data for effective monitoring and control of manufacturing systems. SC integrated into blockchain automate data collection and verification processes. They trigger data submissions based on predefined conditions or events. SC enables direct data sales to interested parties, eliminating intermediaries, ensuring fair compensation, and leveraging decentralised storage to unlock opportunities for data monetisation during data sharing. Blockchain provides secure and controlled access to IIoT data (Y. Zhang, Xu, et al. 2019). Participants can access the data stored on the blockchain using permissioned or permissionless blockchain protocols, ensuring data privacy and ownership control. SC and consensus algorithms utilise standardised protocols for data exchange among different IIoT devices, enabling seamless data collection and aggregation capabilities. Moreover, the standardised process of data collection and decentralised storage system reduces the risks of data tampering, unauthorised access, and data manipulation. Blockchain-based data collection establishes an ideal system for data analysis and AI model preparation.

Industries are inclined to leverage cloud-based solutions to handle connected functionalities to bank on the operational flexibility and shared services to fulfill on-demand products. Z. Li, Barenji, and Huang (2018) proposed a distributed P2P network architecture, named ‘BCmfg’, for cloud manufacturing that improves scalability and security. It leveraged BC to secure data. They defined two main characteristics of BCmfg: on-demand secure services and support for secure data exchange. While they did not consider integrating AI, AI can be integrated as part of DevOps (software **Dev**elopment and IT **Op**eration**s**) and DataOps (**Op**eration**s** on **Data**). DataOps can integrate and streamline data analysis with the operational BC framework. Once the ML model is ready for deployment, DevOps can integrate the ML model with the production environment. Blockchain tracks the data being utilised. Cloud manufacturing redefines intelligence in a manufacturing system by deploying supplementary models for visualisation, IIoT, and other value-added services. Essentially, such services connect different parts of manufacturing sectors and distributed systems to support secure data exchange and off-cloud service execution.

5.4. Supply chain management

The primary goal of the supply chain is to manage services to deliver quality products on time at minimal cost. Given the vast, geographically diverse logistics network, managing and tracking goods becomes complex. Here, blockchain can introduce transparency and traceability to assure quality, minimise counterfeiting, and improve regulatory compliance. Recording product history, provenance, movements, and quality inspections on a blockchain can provide tamper-proof data that ensures accountability and resolves potential conflicts. For instance, blockchain is used in medical and pharmaceutical supply chains to counteract drug counterfeiting (Kanawaday and Sane 2017) and easing compliance with various regulatory acts like the Drug Supply Chain Security Act of 2013 (U.S. Food and Drug Administration 2013) and the California Transparency in Supply Chains Act (Harris 2015). Additionally, the integration of ML, big data analytics, and IoT is creating new opportunities and speeding up decision-making in supply chains. AI-enhanced supply chains are more resilient. Rodríguez-Espíndola et al. (2020) integrated AI and BC to improve humanitarian logistics during disasters (Flood in Tabasco, Mexico in 2007), utilising technologies like 3D printing for optimal onsite production. Figure 10 depicts the involvement of various entities, primarily from the global supply chain, in the blockchain network to streamline processes. From product development to manufacturing, blockchain securely handles material information delivery, ensuring accurate verification and robust traceability. In this fast-paced sector, AI tools enhance the speed of raw material acquisition, final product delivery, sales forecasting, marketing, pricing, and customer segmentation via predictive analysis. ML models, fed with periodic supply chain transaction data, facilitate this enriched analysis. Once the product is ready for shipment, blockchain secures the final transaction details in an immutable database, improving decision-making, optimising operations, and enabling swift response to customer needs.

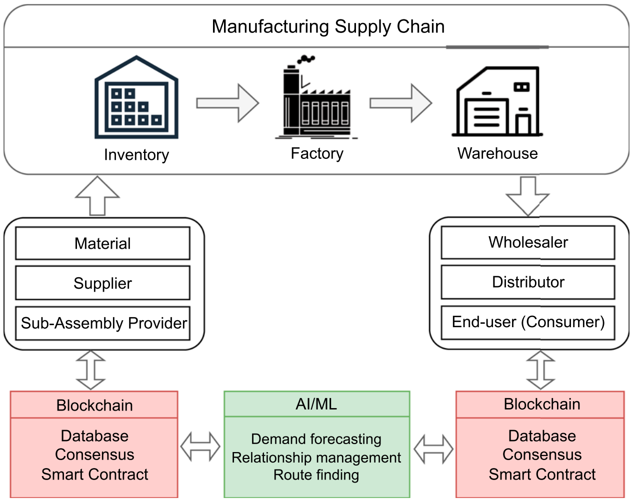


Figure 10. Blockchain and AI-based supply chain.

Several industries, from pharmaceuticals to aviation, are embracing BC-based operating systems for supply chain management. For instance, blockchain's integration with machine learning suggested top-rated drugs to customers and tracked the medicine's origin and authenticity (Abbas et al. 2020). Madhwal and Panfilov (2017) proposed a decentralised system powered by BC for monitoring operational usage and easing the maintenance of aircraft inventory. This integration is even applied in tracking the provenance of goods like tuna fish in line with ethical consumerism (Provenance 2016). Blockchain use in supply chain management is a thriving area of research, promising to revolutionise industries with enhanced transparency, efficiency, and accountability.

Lastly, the marketability of manufactured products can be enhanced by integrating commerce platforms with blockchain, which records product history and quality checks, simplifying customer verification. For instance, Honeywell Aerospace developed GoDirect Trade (in beta stage) (Kucinski 2019), a blockchain-based online marketplace for aviation parts, ensuring listings include proper images, service history, and quality reports. This practice expedites purchasing by eliminating the need to contact multiple suppliers for price and quality verification and stock confirmation. Additionally, the customer can track manufacturing progress and deviations. The sensors connected to machines can initiate maintenance processes. The SCs of the blockchain can verify the completion and initiate payment for the work. Similarly, blockchain can maintain a record of the maintenance history of products under (and beyond) warranty. Mohamed, Al-Jaroodi, and Lazarova-Molnar (2019) has illustrated that BC can also be used to improve energy efficiency and subsequent energy cost reduction. Lastly, BC can enable machines as a service (Kupper et al. 2019).

6. Open research questions

Blockchain holds significant promise for ensuring security in collaborative and globally integrated manufacturing systems, helping build trust by preventing any participant from dominating. However, more research is needed to understand how to best integrate it with various applications and identify key success factors for its implementation. Blockchain adoption is growing rapidly, and interoperability and standardisation issues remain (Casino, Dasaklis, and Patsakis 2019). Combining blockchain with machine learning can reduce documentation and human errors, improve security, enable traceability, and help identify and trace duplicate products. Even though blockchain is a valuable addition to AI-assisted manufacturing, organisational readiness is often lacking due to a limited understanding of the technology and its integration. A comprehensive guideline encompassing opportunity identification, cost-benefit analysis, and implementation details is needed to facilitate organisational redesign for optimal blockchain integration in AI-assisted manufacturing. So, we delineate avenues for future studies for all-around improvement and accelerated adoption.

6.1. *Blockchain adoption and implementation*

Blockchain opens up a portal of opportunities. However, its adoption is still in its infancy and requires a detailed evaluation. Factors such as organisational requirements, employee skill sets, available infrastructure, and organisational willingness or resistance play pivotal roles. Hurdles such as institutional skill gaps and data ownership concerns pose significant challenges to blockchain adoption. A lack of standardisation to protect privacy is another major issue (Babich and Hilary 2018), along with difficulties faced due to decentralised infrastructure lacking defined standards, rules, and compatibility (Lima 2018). The reluctance of organisations to share proprietary data on public platforms and the potential loss of control for dominant stakeholders transitioning from private to public blockchains also raise concerns. Furthermore, regulatory restrictions often hinder adoption, emphasising the need for smart contracts to accommodate these regulations. At the same time, governing bodies must promote innovation by establishing conducive regulations for blockchain solutions. Lastly, the lack of common standards among different organisations looking to join a shared blockchain creates obstacles to scaling and introduces interoperability issues (Sharma, Kumar, and Park 2018).

6.2. Data visibility

Blockchain's notable advantage is its ability to unify all manufacturing entities and authorised external parties within a secure network. However, integrating BC in manufacturing makes the important proprietary data accessible to all the network participants. Access to proprietary data may adversely impact the confidentially and relationships among the insiders and outsiders of an organisation (Pournader et al. 2020). There is a fear of loss of competitive intelligence and advantage. Security concern is incredibly genuine for the public blockchain when private data are stored in a publicly shared ledger, even though they are encrypted.

6.3. Performance deterioration

Blockchain is a combination of a set of technologies (SC, consensus algorithm, decentralisation, and cryptography) that add multiple layers of security. Adding more and more secured layers slows down the system and increases its complexity. Block processing time and security validation may need many seconds, which shows that blockchain-backed infrastructures would encounter latency issues. Each transaction needs to be validated by every node in the blockchain. So, poor infrastructure can hinder real-time monitoring in blockchain-backed infrastructures. This has been a bottleneck of the blockchain-based crypto-currency *Bitcoin*, whose public consensus needs every node to be updated with each transaction (Nakamoto 2008). The process is energy-intensive. Additionally, ML-based computation is also a power-consuming process. More focus should be given to cloud-based blockchain architecture to achieve high performance, especially for machining operations. Cloud manufacturing has not exploited the benefit of blockchain yet. As cloud technology is booming due to its high performance and easy access, blockchain should attract more industries.

6.4. Scalable network

Blockchain makes the data storage infrastructure tamper-proof and the transactions highly secure. However, the number of blocks in a blockchain limit the performance and utilisation if scalability is important. Scalability issues include limitations in the speed of execution with big block sizes (information contained in the block), longer response times, and a perpetually increasing number of transactions. Moreover, with the ever-increasing number of users, the challenges in blockchain scalability also increase.

6.5. Blockchain database management

Manufacturing occurs in a complex network and includes the simultaneous occurrence of multiple activities. Each activity is recorded in the blockchain. The record includes product history, origin, process history, and additional details per requirements. The eclectic mix of datatypes, which is also voluminous, needs a database management system to access the recorded data. The simultaneous recording could mix up the information flow. It is critically important to accurately and adequately store and present product information. Due to the consensus algorithms, the transactions become a bit slower. In simpler terms, a blockchain can be said to have a data structure similar to that of a chain or a linked list. Thus, latency in accessing the data also increases in comparison with legacy systems. Applications with real-time performance requirements have to consider this latency.

6.6. Compatibility with new technology

It is crucial to consider compatibility before integrating BC with manufacturing to ensure uninterrupted and efficient operation. Cryptography, widely used in Blockchain for secure message exchange, has limited implementation in manufacturing. This limitation stems from the stark difference between operational technology and information technology, as well as the platforms that integrate them. Cryptographic techniques require high computational power to generate ciphers, while most manufacturing platforms do not require extremely high computational power. Moreover, the overall network needs to maintain a delicate balance between the ongoing manufacturing operations' computational power while generating cryptographic ciphertext without compromising the security and core functionality of the operating facility. Therefore, more research is needed to maintain balance before implementing BC in manufacturing.

7. Conclusion

Security has never been prioritised holistically in modern manufacturing systems. SMEs are quick to bank on technological innovations and feel the brunt of Pandora's box of uncontrolled security measures. Large organisations like NASA, DuPont, and national nuclear facilities have not been exempted. Inadequate security measures lead to breaches into control systems, reduced product life, data theft, and disruptions in upscaling. Security measures become even more critical as organisations automate their processes to improve their productivity and the quality of their products to meet the needs of mass individualisation. The need for complete autonomy has geared the manufacturing industries toward leveraging artificial intelligence algorithms to make data-driven decisions. The security of data becomes crucial as tampered data can compromise the decisions, which could create operational hazards. Moreover, modern manufacturing systems need interoperation and interconnection among disparate systems; controlled access to data to preserve privacy and maximise utility; transparent and trustful collaboration that respects privacy.

Thus, we position *blockchain* (BC) as a security solution in modern manufacturing systems assisted by AI, and present a framework for integration. BC can eliminate the audits, trace the product's history in real-time, and offer privacy along with transparency. Manufacturing operations can be coded into the smart contracts. Smart contracts, data encryption, and consensus protocols of blockchain can enable process automation, ensure privacy and build trust. Nonetheless, manufacturing blockchains differ from generic ones in terms of the nature of transactions and data, the number of participants, and consensus mechanisms. Consortium blockchains are more suitable for manufacturing systems to ease scalability and ensure data privacy (for competitive advantage) with low latency, but without fully losing the controlling authority. BC and AI can synergize in manufacturing environments to offer an abundance of secure data for better decision-making, enable privacy-preserved learning, share learned system models for validation, prevent incorrect predictions from propagation, detect sources of error, and optimise the operations. In addition to being a security solution, blockchain and AI in manufacturing can increase the willingness to share data, accelerate early-phase product planning, prevent counterfeit products, and improve collaboration, manufacturing processes, and the supply chain.

While integrating blockchain is the way to go for modern manufacturing systems, its integration has several hurdles to clear. Identifying blockchain as a solution, organisational willingness to adopt, the readiness of infrastructure, and skill-gap of the employees thwart the adoption of blockchain. Organizational reluctance to share data and fear of losing competitive advantage cannot be avoided. Moreover, the smart contracts need to be modified suitably to incorporate the regulations of local governments. The added layers of security in terms of smart contracts, consensus algorithms, cryptography, and block validation increase the latency of manufacturing systems. They also increase the energy demand. As the blockchain expands in size, there will be an increase in latency in accessing data compared to legacy systems. This trade-off between blockchain's enhanced security and the legacy system's real-time performance should be carefully considered to retain or improve the overall responsiveness of the system. These roadblocks need to be cleared to harness the full potential of blockchain in artificial intelligence-assisted manufacturing systems.

Notes

1. https://www.adidas.com/us/creatorsclub
2. https://www.nike.com/nike-by-you
3. https://cloudnc.com/
4. https://www.xometry.com/
5. https://www.skuchain.com/
6. https://www.adidas.com/us/creatorsclub
7. https://www.nike.com/nike-by-you

Disclosure statement

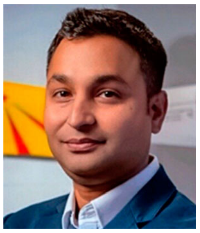
No potential conflict of interest was reported by the author(s).

Notes on contributors

Dhruv Patel received his Master of Science degree in Mechanical Engineering from State University of New York at Buffalo, USA, in 2021. His thesis research focused on 'Blockchain Based Secure Machine Learning Model Integration For Collaborative Manufacturing'.
He is currently working as Data Process Engineer at Radiometer America in California, USA. In this role, he analyses complex production datasets to improve processes and product reliability working along with the R&D team. He specialises in the analysis and interpretation of intricate data sets derived from diverse production processes and equipment. His expertise lies in harnessing the power of manufacturing insights and data analytics to propose enhancements in processes, modifications in measurement techniques, and design refinements, all aimed at elevating product manufacturability and reliability. His work involves close collaboration with cross-functional teams, including Quality, Research and Development, and Production, to identify and implement valuable opportunities for enhancement.

Chandan Kumar Sahu is currently pursuing his Ph.D. degree in automotive engineering at Clemson University. He received his bachelors from National Institute of Technology Rourkela, India, in 2014, and his masters from the State University of New York at Buffalo, USA, in 2020, both in mechanical engineering. He led the homologation of the development of new models at Honda Motorcycle and Scooter India from 2014 to 2017.
He is interested in machine learning in general, with a focus on its geometric attributes and mechanical applications. His research investigated additive manufacturing, augmented reality, cyber-physical systems, and engineering design applications using computational tools like machine learning, graph

theory, and natural language processing. His current research aspires to develop mathematical models of requirements to capture their interrelationships to investigate the role of requirements during the evolution of a system.?



Rahul Rai joined the Department of Automotive Engineering in 2020 as Dean's Distinguished Professor in the Clemson University International Center for Automotive Research (CU-ICAR). He also holds appointments in the Computer Science and Mechanical Engineering departments at Clemson University. He is Associate Director of Artificial Intelligence Research Institute in Science and Engineering (AIRISE) at Clemson University. He directs the Geometric Reasoning and Artificial Intelligence Lab (GRAIL, which is located at both CU-ICAR and Center for Manufacturing Innovation (CMI). Previously, he served on the Mechanical and Aerospace Engineering faculty at the University at Buffalo-SUNY (2012–2020). Dr. Rai also has industrial research centre experiences at United Technology Research Center (UTRC) and Palo Alto Research Center (PARC). Dr. Rai received his B.Tech. degree in 2000 and M.S. degree in 2002 in Manufacturing Engineering from the National Institute of Foundry and Forge Technology (NIFFT), Ranchi, India, and Missouri University of Science and Technology (Missouri S&T) USA, respectively. He earned his doctoral degree in Mechanical Engineering from The University of Texas at Austin USA in 2006.

Dr. Rai's research is focused on developing computational tools for Manufacturing, Cyber-Physical System (CPS) Design, Autonomy, Collaborative Human-Technology Systems, Diagnostics and Prognostics, and Extended Reality (XR) domains. By combining engineering innovations with methods from machine learning, AI, statistics and optimisation, and geometric reasoning, his research strives to solve important problems in the above-mentioned domains. His research has been supported by NSF, DARPA, ONR, ARL, NSWC, DMDII, CESMII, HP, NYSERDA, and NYSPII (funding totalling more than $20M as PI/Co-PI). He has authored over 100 papers to date in peer-reviewed conferences and journals covering a wide array of problems. Dr. Rai is the recipient of numerous awards, including the 2009 HP Design Innovation, 2017 ASME IDETC/CIE Young Engineer Award, and 2019 PHM society conference best paper award. Additionally, Dr. Rai is Associate Editor of the International Journal of Production Research and ASME Journal of Computing and Information Science in Engineering (JCISE) journals and has taken significant leadership roles within the ASME Computers and Information in Engineering professional society.

Data availability statement (DAS)

Data sharing is not applicable to this article as no new data were created or analysed in this study.

ORCID

Dhruv Patel http://orcid.org/0000-0002-8913-1722
Chandan Kumar Sahu http://orcid.org/0000-0001-5893-4031
Rahul Rai http://orcid.org/0000-0002-6478-4065

References

1996. "Health Insurance Portability and Accountability Act of 1996." *Public Law* 104:191.

Abadi, Martin, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang 2016. "Deep Learning with Differential Privacy." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 308–318. https://doi.org/10.1145/2976749.2978318.

Abbas, Khizar, Muhammad Afaq, Talha Ahmed Khan, and Wang-Cheol Song. 2020. "A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry." *Electronics* 9 (5): 852. https://doi.org/10.3390/electronics9050852.

Abeyratne, Saveen A., and Radmehr P. Monfared. 2016. "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger." *International Journal of Research in Engineering and Technology* 5 (9): 1–10. https://doi.org/10.15623/ijret.

Abraham, Ittai, Srinivas Devadas, Kartik Nayak, and Ling Ren. 2017. "Brief Announcement: Practical Synchronous Byzantine Consensus." In *31st International Symposium on Distributed Computing (DISC 2017)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Aguwa, Celestine, Mohammad Hessam Olya, and Leslie Monplaisir. 2017. "Modeling of Fuzzy-based Voice of Customer for Business Decision Analytics." *Knowledge-Based Systems* 125:136–145. https://doi.org/10.1016/j.knosys.2017.03.019.

Akcora, Cuneyt Gurcan, Yulia R. Gel, and Murat Kantarcioglu. 2022. "Blockchain Networks: Data Structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 12 (1): e1436.

Al Faruque, Mohammad Abdullah, Sujit Rokka Chhetri, Arquimedes Canedo, and Jiang Wan. 2016. "Acoustic Side-Channel Attacks on Additive Manufacturing Systems." In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, 1–10. IEEE.

Alkaabi, Nouf, Khaled Salah, Raja Jayaraman, Junaid Arshad, and Mohammed Omar. 2020. "Blockchain-Based Traceability and Management for Additive Manufacturing." *IEEE Access* 8:188363–188377. https://doi.org/10.1109/Access.6287639.

Angrish, Atin, Benjamin Craver, Mahmud Hasan, and Binil Starly. 2018. "A Case Study for Blockchain in Manufacturing: 'FabRec': A Prototype for Peer-to-peer Network of Manufacturing Nodes." *Procedia Manufacturing* 26:1180–1192. https://doi.org/10.1016/j.promfg.2018.07.154.

Apsley, Linda Knowlton, Colin Ian Bodell, Jacob Conrad Danton, Scott Randall Hayden, Saiprasad Kapila, Eric Lessard, and Robert Benjamin Uhl. 2017. "Fulfillment of Orders for Items Using 3D Manufacturing on Demand." Jun. 6. US Patent 9,672,550.

Babich, V, and G Hilary. 2018. *What Operations Management Researchers Should Know About Blockchain Technology*. Technical Report. Georgetown Working Paper.

Bahga, Arshdeep, and Vijay K. Madisetti. 2016. "Blockchain Platform for Industrial Internet of Things." *Journal of Software Engineering and Applications* 9 (10): 533–546. https://doi.org/10.4236/jsea.2016.910036.

Barenji, Ali Vatankhah, Hanyang Guo, Zonggui Tian, Zhi Li, Wai Ming Wang, and George Q. Huang. 2019. "Blockchain-Based Cloud Manufacturing: Decentralization." arXiv preprint arXiv:1901.10403.

Baumung, Wjatscheslav, and Vladislav Fomin. 2019. "Framework for Enabling Order Management Process in a Decentralized Production Network Based on the Blockchain-technology." *Procedia CIRP* 79:456–460. https://doi.org/10.1016/j.procir.2019.02.121.

Bech, Sofie, Anne-Sophie Schou Joedal, Thomas Ditlev Brunoe, and Kjeld Nielsen. 2018. "Mass Customization in Food Industries: Case and Literature Study." In *Customization 4.0*, 519–529. Springer. https://doi.org/10.1007/978-3-319-77556-2_32.

Belikovetsky, Sofia, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. 2017. "dr0wned–Cyber-Physical Attack with Additive Manufacturing." In *11th USENIX Workshop on Offensive Technologies (WOOT 17),* Vancouver, BC, Canada.

Bellemare, Jocelyn. 2018. "Fashion Apparel Industry 4.0 and Smart Mass Customization Approach for Clothing Product Design." In *Customization 4.0*, 619–633. Springer. https://doi.org/10.1007/978-3-319-77556-2_39.

Berry, Christopher, Hui Wang, and S. Jack Hu. 2013. "Product Architecting for Personalization." *Journal of Manufacturing Systems* 32 (3): 404–411. https://doi.org/10.1016/j.jmsy.2013.04.012.

Bielecki, Dustin, Darshil Patel, Rahul Rai, and Gary F. Dargush. 2021. "Multi-Stage Deep Neural Network Accelerated Topology Optimization." *Structural and Multidisciplinary Optimization* 64 (6): 3473–3487. https://doi.org/10.1007/s00158-021-03028-5.

Boccella, Anna Rosaria, Centobelli Piera, Roberto Cerchione, Teresa Murino, and Ralph Riedel. 2020. "Evaluating Centralized and Heterarchical Control of Smart Manufacturing Systems in the Era of Industry 4.0." *Applied Sciences* 10 (3): 755. https://doi.org/10.3390/app10030755.

Bodendorf, Frank, Stefan Merbele, and Jörg Franke. 2022. "Deep Learning Based Cost Estimation of Circuit Boards: A Case Study in the Automotive Industry." *International Journal of Production Research,* 60 (23): 1–22. https://doi.org/10.1080/00207543.2021.1998698.

Bogue, Robert. 2013. "3D Printing: the Dawn of a New Era in Manufacturing?." *Assembly Automation* 33 (4). https://doi.org/10.1108/AA-06-2013-055.

Bonvoisin, Jérémy, and Jean-François Boujut. 2015. "Open Design Platforms for Open Source Product Development: Current State and Requirements." In *DS 80-8 Proceedings of the 20th International Conference on Engineering Design (ICED 15) Vol 8: Innovation and Creativity, Milan, Italy, 27-30.07. 15*, 011–020.

Brown, Colleen. 2022. "Data Breach Notifications, Office of the Maine Attorney General." https://apps.web.maine.gov/online/aeviewer/ME/40/6f9be6c4-7e0f-4015-a7b1-1d6dcc66ccd1.shtml.

Cachin, Christian. 2016. "Architecture of the Hyperledger Blockchain Fabric." In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, Vol. 310, 1–4. Chicago, IL.

Cachin, Christian, Marko Vukolic Sorniotti, and Thomas Weigold. 2016. "Blockchain, Cryptography, and Consensus." *IBM Res., Zürich, Switzerland, Tech. Rep.*, 2016.

Camarinha-Matos, Luis M., Hamideh Afsarmanesh, Nathalie Galeano, and Arturo Molina. 2009. "Collaborative Networked Organizations–Concepts and Practice in Manufacturing Enterprises." *Computers & Industrial Engineering* 57 (1): 46–60. https://doi.org/10.1016/j.cie.2008.11.024.

Cannavo, Alberto, and Fabrizio Lamberti. 2020. "How Blockchain, Virtual Reality, and Augmented Reality are Converging, and Why." *IEEE Consumer Electronics Magazine* 10 (5): 6–13. https://doi.org/10.1109/MCE.2020.3025753.

Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. 2019. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." *Telematics and Informatics* 36:55–81. https://doi.org/10.1016/j.tele.2018.11.006.

Castro, Miguel, and Barbara Liskov. 1999. "Practical Byzantine Fault Tolerance." In *OsDI*, New Orleans, LA, Vol. 99, 173–186.

Chen, Xuhui, Jinlong Ji, Changqing Luo, Weixian Liao, and Pan Li. 2018. "When Machine Learning Meets Blockchain: A Decentralized, Privacy-Preserving and Secure Design." In *2018 IEEE International Conference on Big Data (Big Data)*, 1178–1187. IEEE.

Cheng, Jiangfeng, Weihai Chen, Fei Tao, and Chun-Liang Lin. 2018. "Industrial IoT in 5G Environment Towards Smart Manufacturing." *Journal of Industrial Information Integration* 10:10–19. https://doi.org/10.1016/j.jii.2018.04.001.

Chohan, Usman W. 2021. "A History of Dogecoin." *Discussion Series: Notes on the 21st Century*.

Comuzzi, Marco, Erdenekhuu Unurjargal, and Chiehyeon Lim. 2018. "Towards a Design Space for Blockchain-Based System Reengineering." In *International Conference on Advanced Information Systems Engineering*, 138–143. Springer.

Connolly, F. Colm. 2007. "Guilty Plea in Trade Secrets Case, U.S. Department of Justice." https://www.justice.gov/archive/criminal/cybercrime/press-releases/2007/minPlea.pdf.

Crain, Tyler, Vincent Gramoli, Mikel Larrea, and Michel Raynal. 2018. "Dbft: Efficient Leaderless Byzantine Consensus and its Application to Blockchains." In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 1–8. IEEE.

Dannen, Chris. 2017. *Introducing Ethereum and Solidity*. Vol. 1. Springer. https://doi.org/10.1007/978-1-4842-2535-6.

De, Nikhilesh. 2017. "Hacks, Scams and Attacks: Blockchain's 2017 Disasters." https://www.coindesk.com/markets/2017/12/29/hacks-scams-and-attacks-blockchains-2017-disasters/.

Delgado, M., A. García, J. C. Urresty, J.-R. Riba, and J. A. Ortega. 2011. "Evaluation of Machine Learning Techniques for Electro-Mechanical System Diagnosis." In *Proceedings of the 2011 14th European Conference on Power Electronics and Applications*, 1–10. IEEE.

Deng, Tianchi, Yingguang Li, Xu Liu, and Lihui Wang. 2022. "Federated Learning-Based Collaborative Manufacturing for Complex Parts." *Journal of Intelligent Manufacturing* 1–14.

Dinh, Thang N., and My T. Thai. 2018. "Ai and Blockchain: A Disruptive Integration." *Computer* 51 (9): 48–53. https://doi.org/10.1109/MC.2018.3620971.

El-Sherif, Osama. 2019. "Fast, Efficient, Reliable: Artificial Intelligence in BMW Group Production." Accessed July 15, 2019. https://www.press.bmwgroup.com/middle-east/article

/detail/T0299271EN/fast-efficient-reliable:-artificial-intelligence-in-bmw-group-production?language=en.

Feng, Deng-Guo, Min Zhang, Yan Zhang, and Zhen Xu. 2011. "Study on Cloud Computing Security." *Journal of Software* 22 (1): 71–83. https://doi.org/10.3724/SP.J.1001.2011.03958.

Ferrer, Eduardo Castelló. 2018. "The Blockchain: A New Framework for Robotic Swarm Systems." In *Proceedings of the Future Technologies Conference*, 1037–1058. Springer.

Frank, Alejandro Germán, Lucas Santos Dalenogare, and Néstor Fabián Ayala. 2019. "Industry 4.0 Technologies: Implementation Patterns in Manufacturing Companies." *International Journal of Production Economics* 210:15–26. https://doi.org/10.1016/j.ijpe.2019.01.004.

Franzen, V., L. Kwiatkowski, J. Neves, P. A. F. Martins, and A. E. Tekkaya. 2008. "On the Capability of Single Point Incremental Forming for Manufacturing Polymer Sheet Parts." In *Int. Conf. Technol. Plast*, Vol. 2008, 890–895.

Frey, Remo, Dominic Wörner, and Alexander Ilic. 2016. "Collaborative Filtering on the Blockchain: A Secure Recommender System for E-Commerce".

Fu, Yuchuan, Fei Richard Yu, Changle Li, Tom H. Luan, and Yao Zhang. 2020. "Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles." *IEEE Wireless Communications* 27 (2): 197–203. https://doi.org/10.1109/MWC.7742.

Gantz, John, and David Reinsel. 2012. "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East." *IDC IView: IDC Analyze the Future* 2007 (2012): 1–16.

Gaur, Vishal, and Abhinav Gaiha. 2020. "Building a Transparent Supply Chain." Online; Accessed August 28, 2022. https://hbr.org/2020/05/building-a-transparent-supply-chain.

Gaži, Peter, Aggelos Kiayias, and Dionysis Zindros. 2019. "Proof-of-Stake Sidechains." In *2019 IEEE Symposium on Security and Privacy (SP)*, 139–156. IEEE.

Good, Owen S. 2021. "NFT Mastermind Says He Created Ethereum Because Warcraft Nerfed His Character." Accessed February 03, 2022. https://www.polygon.com/22709126/ethereum-creator-world-of-warcraft-nerf-nft-vitalik-buterin.

Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. 2016. *Deep Learning*. MIT press, ISBN: 9780262035613.

Guo, Ye, and Chen Liang. 2016. "Blockchain Application and Outlook in the Banking Industry." *Financial Innovation* 2 (1): 1–12. https://doi.org/10.1186/s40854-016-0034-9.

Guo, Daqiang, Shiquan Ling, Hao Li, Di Ao, Tongda Zhang, Yiming Rong, and George Q. Huang. 2020. "A Framework for Personalized Production Based on Digital Twin, Blockchain and Additive Manufacturing in the Context of Industry 4.0." In *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, 1181–1186. IEEE.

Harris, Kamala D. 2015. "The California Transparency in Supply Chains Act." *Office of the Attorney General*. https://oag.ca.gov/sites/all/files/agweb/pdfs/sb657/resource-guide.pdf.

Hasan, Mahmud, and Tahsin Mullick. 2021. "Blockchain and Artificial Intelligence Enabled Autonomous Smart Manufacturing Consortium." In *IIE Annual Conference. Proceedings*, 920–925. Institute of Industrial and Systems Engineers (IISE).

Holland, Martin, Christopher Nigischer, and J. Stjepandic. 2017. "Copyright Protection in Additive Manufacturing with Blockchain Approach." *Transdisciplinary Engineering: A Paradigm Shift* 5:914–921.

Hoornaert, Steven, Michel Ballings, Edward C. Malthouse, and Dirk Van den Poel. 2017. "Identifying New Product Ideas: Waiting for the Wisdom of the Crowd Or Screening Ideas in Real Time." *Journal of Product Innovation Management* 34 (5): 580–597. https://doi.org/10.1111/jpim.2017.34.issue-5.

Hoy, Matthew B. 2017. "An Introduction to the Blockchain and Its Implications for Libraries and Medicine." *Medical Reference Services Quarterly* 36 (3): 273–279. https://doi.org/10.1080/02763869.2017.1332261.

Hu, Qian, Biwei Yan, Yubing Han, and Jiguo Yu. 2021. "An Improved Delegated Proof of Stake Consensus Algorithm." *Procedia Computer Science* 187:341–346. https://doi.org/10.1016/j.procs.2021.04.109.

IBM. 2017. "Three Ways Blockchain Explorers Chart a New Direction. (Global C-suite Study 19th Edition)".

IFR Press Release. 2020, September. "IFR Presents World Robotics Report 2020." https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe.

Impagliazzo, Russell, Rex Lei, Toniann Pitassi, and Jessica Sorrell. 2022. "Reproducibility in Learning." In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Rome, Italy, 818–831. https://doi.org/10.1145/3519935.3519973.

Javaid, Mohd, Abid Haleem, Raju Vaishya, Shashi Bahl, Rajiv Suman, and Abhishek Vaish. 2020. "Industry 4.0 Technologies and Their Applications in Fighting COVID-19 Pandemic." *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14 (4): 419–422. https://doi.org/10.1016/j.dsx.2020.04.032.

Jessi, B., S. Jutta, and G. Wood. 2016. "Provenance White Paper." https://www.provenance.org/whitepaper.

Jiang, Pingyu, Jiewu Leng, Kai Ding, Peihua Gu, and Yoram Koren. 2016. "Social Manufacturing As a Sustainable Paradigm for Mass Individualization." *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* 230 (10): 1961–1968. https://doi.org/10.1177/0954405416666903.

Kamath, G., and M. M. Mewari. 2021. "17 Remarkable Use Cases of AI in the Manufacturing Industry." Accessed February 03, 2022. https://www.birlasoft.com/articles/17-use-cases-of-ai-in-manufacturing.

Kan, Michael. 2022. "Ransomware Attack Costs Hanesbrands $100 Million in Lost Sales." https://www.pcmag.com/news/ransomware-attack-costs-hanesbrands-100-million-in-lost-sales.

Kanawaday, Ameeth, and Aditya Sane. 2017. "Machine Learning for Predictive Maintenance of Industrial Machines Using IoT sensor data." In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 87–90. IEEE.

Kelley, B. Michael. 2013. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Kiayias, Aggelos, and Dionysis Zindros. 2019. "Proof-of-Work Sidechains." In *International Conference on Financial Cryptography and Data Security*, 21–34. Springer.

Kim, Songi, and Keeheon Lee. 2023. "The Paradigm Shift of Mass Customisation Research." *International Journal of Production Research* 61 (10): 3350–3376. https://doi.org/10.1080/00207543.2022.2081629.

Kostakis, Vasilis, and Marios Papachristou. 2014. "Commons-Based Peer Production and Digital Fabrication: The Case of a RepRap-Based, Lego-Built 3D Printing-Milling Machine." *Telematics and Informatics* 31 (3): 434–443. https://doi.org/10.1016/j.tele.2013.09.006.

Kucinski, Willaim. 2019. "Honeywell Aerospace Launches B2B E-Commerce Site for Aerospace Components." https://www.sae.org/news/2019/01/honeywell-aerospace-launches-b2b-e-commerce-site-for-aerospace-components.

Kupper, Daniel, Johannes Strohle, Thomas Kruger, Kaj Burchardi, and Neil Shepherd. 2019. "Blockchain in the Factory of the Future." https://www.bcg.com/publications/2019/blockchain-factory-future.

Kurtulmus, A. Besir, and Kenny Daniel. 2018. "Trustless Machine Learning Contracts; Evaluating and Exchanging Machine Learning Models on the Ethereum Blockchain." arXiv preprint arXiv:1802.10185.

Kurtz, Michael A., Ruoyu Yang, Mohan S. R. Elapolu, Audrey C. Wessinger, William Nelson, Kazzandra Alaniz, Rahul Rai, and Jeremy L. Gilbert. 2023. "Predicting Corrosion Damage in the Human Body Using Artificial Intelligence: In Vitro Progress and Future Applications." *Orthopedic Clinics* 54 (2): 169–192. https://doi.org/10.1016/j.ocl.2022.11.004.

Lakshman, T. V., and Ashok K. Agrawala. 1986. "Efficient Decentralized Consensus Protocols." *IEEE Transactions on Software Engineering* SE-12 (5): 600–607. https://doi.org/10.1109/TSE.1986.6312956.

LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. 2015. "Deep Learning." *Nature* 521 (7553): 436–444. https://doi.org/10.1038/nature14539.

Lee, Jay, Moslem Azamfar, and Jaskaran Singh. 2019. "A Blockchain Enabled Cyber-Physical System Architecture for Industry 4.0 Manufacturing Systems." *Manufacturing Letters* 20:34–39. https://doi.org/10.1016/j.mfglet.2019.05.003.

Lee, Jay, Behrad Bagheri, and Hung-An Kao. 2015. "A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems." *Manufacturing Letters* 3:18–23. https://doi.org/10.1016/j.mfglet.2014.12.001.

Lemeš, Samir, and Lamija Lemeš. 2019. "Blockchain in Distributed CAD Environments." In *International Conference "New Technologies, Development and Applications"*, 25–32. Springer.

Leng, Jiewu, Qingxin Chen, Ning Mao, and Pingyu Jiang. 2018. "Combining Granular Computing Technique with Deep Learning for Service Planning Under Social Manufacturing Contexts." *Knowledge-Based Systems* 143:295–306. https://doi.org/10.1016/j.knosys.2017.07.023.

Leng, Jiewu, Pingyu Jiang, and Mei Zheng. 2017. "Outsourcer–Supplier Coordination for Parts Machining Outsourcing Under Social Manufacturing." *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* 231 (6): 1078–1090. https://doi.org/10.1177/0954405415583883.

Leng, Jiewu, Douxi Yan, Qiang Liu, Kailin Xu, J. Leon Zhao, Rui Shi, Lijun Wei, Ding Zhang, and Xin Chen. 2019. "ManuChain: Combining Permissioned Blockchain with a Holistic Optimization Model As Bi-Level Intelligence for Smart Manufacturing." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50 (1): 182–192. https://doi.org/10.1109/TSMC.2019.2930418.

Li, Zhi, Ali Vatankhah Barenji, and George Q. Huang. 2018. "Toward a Blockchain Cloud Manufacturing System As a Peer to Peer Distributed Network Platform." *Robotics and Computer-Integrated Manufacturing* 54:133–144. https://doi.org/10.1016/j.rcim.2018.05.011.

Li, Bo, Guojun Zhang, and Songxin Shi. 2012. "Cloud Manufacturing Platform and Key Technologies for Mould Industry Supporting Collaboration [J]." *Computer Integrated Manufacturing System* 18 (07): 1620–1626.

Lima, Claudio. 2018. "Developing Open and Interoperable DLTBlockchain Standards [Standards]." *Computer* 51 (11): 106–111. https://doi.org/10.1109/MC.2018.2876184.

Liu, Ang, and Stephen C.-Y. Lu. 2016. "A Crowdsourcing Design Framework for Concept Generation." *CIRP Annals* 65 (1): 177–180. https://doi.org/10.1016/j.cirp.2016.04.021.

Liu, X. L., W. M. Wang, Hanyang Guo, Ali Vatankhah Barenji, Zhi Li, and George Q. Huang. 2020. "Industrial Blockchain Based Framework for Product Lifecycle Management in Industry 4.0." *Robotics and Computer-Integrated Manufacturing* 63:Article ID 101897. https://doi.org/10.1016/j.rcim.2019.101897.

Liu, Yiming, F. Richard Yu, Xi Li, Hong Ji, and Victor C. M. Leung. 2020. "Blockchain and Machine Learning for Communications and Networking Systems." *IEEE Communications Surveys & Tutorials* 22 (2): 1392–1431. https://doi.org/10.1109/COMST.9739.

Liu, Qiang, Hao Zhang, Jiewu Leng, and Xin Chen. 2019. "Digital Twin-Driven Rapid Individualised Designing of Automated Flow-Shop Manufacturing System." *International Journal of Production Research* 57 (12): 3903–3919. https://doi.org/10.1080/00207543.2018.1471243.

Lv, Chen, Yang Xing, Chao Lu, Yahui Liu, Hongyan Guo, Hongbo Gao, and Dongpu Cao. 2018. "Hybrid-Learning-Based Classification and Quantitative Inference of Driver Braking Intensity of An Electrified Vehicle." *IEEE Transactions on Vehicular Technology* 67 (7): 5718–5729.

Madhwal, Yash, and Peter B. Panfilov. 2017. "Industrial Case: Blockchain on Aircraft's Parts Supply Chain Management." In *American Conference on Information Systems 2017 Workshop on Smart Manufacturing Proceedings*, Vol. 6. https://aisel.aisnet.org/sigbd2017/6/.

Makhdoom, Imran, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. "Blockchain's Adoption in IoT: The Challenges, and a Way Forward." *Journal of Network and Computer Applications* 125:251–279. https://doi.org/10.1016/j.jnca.2018.10.019.

Mandolla, Claudio, Antonio Messeni Petruzzelli, Gianluca Percoco, and Andrea Urbinati. 2019. "Building a Digital Twin for Additive Manufacturing Through the Exploitation of Blockchain: A Case Analysis of the Aircraft Industry." *Computers in Industry* 109:134–152. https://doi.org/10.1016/j.compind.2019.04.011.

Manimuthu, Arunmozhi, V. G. Venkatesh, Yangyan Shi, V. Raja Sreedharan, and S. C. Lenny Koh. 2022. "Design and Development of Automobile Assembly Model Using Federated Artificial Intelligence with Smart Contract." *International Journal of Production Research* 60 (1): 111–135. https://doi.org/10.1080/00207543.2021.1988750.

McMahan, Brendan, and Daniel Ramage. 2017. “Federated Learning: Collaborative Machine Learning without Centralized Training Data.” *Google AI Blog*. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

Mehta, Dhyey, Sudeep Tanwar, Umesh Bodkhe, Arpit Shukla, and Neeraj Kumar. 2021. “Blockchain-Based Royalty Contract Transactions Scheme for Industry 4.0 Supply-Chain Management.” *Information Processing & Management* 58 (4): Article ID 102586. https://doi.org/10.1016/j.ipm.2021.102586.

Mettler, Matthias. 2016. “Blockchain Technology in Healthcare: The Revolution Starts Here.” In *2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)*, 1–3. IEEE.

Mohamed, Nader, and Jameela Al-Jaroodi. 2019. “Applying Blockchain in Industry 4.0 Applications.” In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0852–0858. IEEE.

Mohamed, Nader, Jameela Al-Jaroodi, and Sanja Lazarova-Molnar. 2019. “Leveraging the Capabilities of Industry 4.0 for Improving Energy Efficiency in Smart Factories.” *IEEE Access* 7:18008–18020. https://doi.org/10.1109/ACCESS.2019.2897045.

Moore, Samuel, Phillip Armstrong, Todd McDonald, and Mark Yampolskiy. 2016. “Vulnerability Analysis of Desktop 3D Printer Software.” In *2016 Resilience Week (RWS)*, 46–51. IEEE.

Mougayar, William. 2016. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, ISBN: 978-1-119-30033-5.

Mourtzis, Dimitris. 2020. “Simulation in the Design and Operation of Manufacturing Systems: State of the Art and New Trends.” *International Journal of Production Research* 58 (7): 1927–1949. https://doi.org/10.1080/00207543.2019.1636321.

Mourtzis, Dimitris. 2021. *Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology*. Elsevier, ISBN: 9780128236581.

Mourtzis, Dimitris, John Angelopoulos, and Nikos Panopoulos. 2023. “Blockchain Integration in the Era of Industrial Metaverse.” *Applied Sciences* 13 (3): 1353. https://doi.org/10.3390/app13031353.

Muzammal, Muhammad, Qiang Qu, and Bulat Nasrulin. 2019. “Renovating Blockchain with Distributed Databases: An Open Source System.” *Future Generation Computer Systems* 90:105–117. https://doi.org/10.1016/j.future.2018.07.042.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Decentralized Business Review*, Article ID 21260. https://doi.org/10.2139/ssrn.3440802.

Nguyen, Lan N., Truc D. T. Nguyen, Thang N. Dinh, and My T. Thai. 2019. “Optchain: Optimal Transactions Placement for Scalable Blockchain Sharding.” In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 525–535. IEEE.

Nguyen, Ryan, Shubhendu Kumar Singh, and Rahul Rai. 2023. “Physics-Infused Fuzzy Generative Adversarial Network for Robust Failure Prognosis.” *Mechanical Systems and Signal Processing* 184:Article ID 109611. https://doi.org/10.1016/j.ymssp.2022.109611.

Nikolić, Ivica, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor. 2018. “Finding the Greedy, Prodigal, and Suicidal Contracts at Scale.” In *Proceedings of the 34th Annual Computer Security Applications Conference*, San Juan, PR, USA, 653–663. https://doi.org/10.1145/3274694.3274743.

O’Donnell, Lindsey. 2021. “Microsoft Edge, Google Chrome Roll Out Password Protection Tools.” Accessed January 1, 2021. https://threatpost.com/microsoft-edge-google-chrome-roll-out-password-protection-tools/163272/.

Office of Inspector General – Office of Audits. 2017. “Industrial Control System Security Within Nasa’s Critical and Supporting Infrastructure.” https://oig.nasa.gov/docs/IG-17-011.pdf.

Olaniyi, Olayemi Mikail, Abraham Ayegba Alfa, and Buhari Ugbede Umar. 2022. “Artificial Intelligence for Demystifying Blockchain Technology Challenges: A Survey of Recent Advances.” *Frontiers in Blockchain* 5: 927006. https://doi.org/10.3389/fbloc.2022.927006.

Ordieres-Meré, Joaquín, Javier Villalba-Díez, and Xiaochen Zheng. 2019. “Challenges and Opportunities for Publishing IIoT Data in Manufacturing As a Service Business.” *Procedia Manufacturing* 39:185–193. https://doi.org/10.1016/j.promfg.2020.01.308.

Outchakoucht, Aissam, E. S. Hamza, and Jean Philippe Leroy. 2017. “Dynamic Access Control Policy Based on Blockchain and Machine Learning for the Internet of Things.” *International Journal of Advanced Computer Science and Applications* 8 (7): 417–424. https://doi.org/10.14569/issn.2156-5570.

Paturi, Uma Maheshwera Reddy, and Suryapavan Cheruku. 2021. “Application and Performance of Machine Learning Techniques in Manufacturing Sector From the Past Two Decades: A Review.” *Materials Today: Proceedings* 38 (Part 5): 2392–2401. https://doi.org/10.1016/j.matpr.2020.07.209.

Peng, Peixi, Yonghong Tian, Tao Xiang, Yaowei Wang, Massimiliano Pontil, and Tiejun Huang. 2017. “Joint Semantic and Latent Attribute Modelling for Cross-Class Transfer Learning.” *IEEE Transactions on Pattern Analysis and Machine Intelligence* 40 (7): 1625–1638. https://doi.org/10.1109/TPAMI.34.

Podgorelec, Blaž, Muhamed Turkanović, and Sašo Karakatič. 2020. “A Machine Learning-Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection.” *Sensors* 20 (1): 147. https://doi.org/10.3390/s20010147.

Pournader, Mehrdokht, Yangyan Shi, Stefan Seuring, and S. C. Lenny Koh. 2020. “Blockchain Applications in Supply Chains, Transport and Logistics: A Systematic Review of the Literature.” *International Journal of Production Research* 58 (7): 2063–2081. https://doi.org/10.1080/00207543.2019.1650976.

Pradeep, Abhinaw Sai Erri, Tak Wing Yiu, Yang Zou, and Robert Amor. 2021. “Blockchain-Aided Information Exchange Records for Design Liability Control and Improved Security.” *Automation in Construction* 126:Article ID 103667. https://doi.org/10.1016/j.autcon.2021.103667.

Prinsloo, Jaco, Saurabh Sinha, and Basie von Solms. 2019. “A Review of Industry 4.0 Manufacturing Process Security Risks.” *Applied Sciences* 9 (23): 5105. https://doi.org/10.3390/app9235105.

Provenance. 2016. “From Shore to Plate: Tracking Tuna on the Blockchain.” https://www.provenance.org/tracking-tuna-on-the-blockchain.

Punter, A. Dr. 2013. "Supply Chain Failures." http://www.airmic.com/sites/default/files/supply_chain_failures_2013_FINAL_web.pdf.

Rahman, Mohamed Abdur, M Shamim Hossain, Mohammad Saiful Islam, Nabil A Alrajeh, and Ghulam Muhammad. 2020. "Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach." *IEEE Access* 8:205071–205087. https://doi.org/10.1109/Access.6287639.

Rai, Rahul, and Chandan K. Sahu. 2020. "Driven by Data Or Derived Through Physics? a Review of Hybrid Physics Guided Machine Learning Techniques with Cyber-physical System (cps) Focus." *IEEE Access* 8:71050–71073. https://doi.org/10.1109/Access.6287639.

Rai, Rahul, Manoj Kumar Tiwari, Dmitry Ivanov, and Alexandre Dolgui. 2021. "Machine Learning in Manufacturing and Industry 4.0 Applications".

Ream, John, Yang Chu, and David Schatsky. 2016. "Upgrading Blockchains: Smart Contract Use Cases in Industry." *Retrieved December* 12:2017.

Rodríguez-Espíndola, Oscar, Soumyadeb Chowdhury, Ahmad Beltagui, and Pavel Albores. 2020. "The Potential of Emergent Disruptive Technologies for Humanitarian Supply Chains: The Integration of Blockchain, Artificial Intelligence and 3D Printing." *International Journal of Production Research* 58 (15): 4610–4630. https://doi.org/10.1080/00207543.2020.1761565.

Rüßmann, Michael, Markus Lorenz, Philipp Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, and Michael Harnisch. 2015. "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries." *Boston Consulting Group* 9 (1): 54–89.

Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. 2015. "Security and Privacy Challenges in Industrial Internet of Things." In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 1–6. IEEE.

Sahu, Chandan K., Crystal Young, and Rahul Rai. 2021. "Artificial Intelligence (AI) in Augmented Reality (AR)-Assisted Manufacturing Applications: a Review." *International Journal of Production Research* 59 (16): 4903–4959. https://doi.org/10.1080/00207543.2020.1859636.

Salah, Khaled, M. Habib Ur Rehman, Nishara Nizamuddin, and Ala Al-Fuqaha. 2019. "Blockchain for AI: Review and Open Research Challenges." *IEEE Access* 7:10127–10149. https://doi.org/10.1109/Access.6287639.

Sarda, Paul, Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, and Jun Han. 2018. "Blockchain for Fraud Prevention: A Work-History Fraud Prevention System." In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1858–1863. IEEE.

Sayfayn, Nabil, and Stuart Madnick. 2017. "Cybersafety Analysis of the Maroochy Shire Sewage Spill (Preliminary Draft)".

Schluse, Michael, Marc Priggemeyer, Linus Atorf, and Juergen Rossmann. 2018. "Experimentable Digital Twins–Streamlining Simulation-Based Systems Engineering for Industry 4.0." *IEEE Transactions on Industrial Informatics* 14 (4): 1722–1731. https://doi.org/10.1109/TII.2018.2804917.

Shahbazi, Zeinab, and Yung-Cheol Byun. 2021. "Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing." *Sensors* 21 (4): 1467. https://doi.org/10.3390/s21041467.

Sharma, Pradip Kumar, Neeraj Kumar, and Jong Hyuk Park. 2018. "Blockchain-Based Distributed Framework for Automotive Industry in a Smart City." *IEEE Transactions on Industrial Informatics* 15 (7): 4197–4205. https://doi.org/10.1109/TII.9424.

Shen, Bin, Ming Cheng, Ciwei Dong, and Yixuan Xiao. 2023. "Battling Counterfeit Masks During the COVID-19 Outbreak: Quality Inspection Vs. Blockchain Adoption." *International Journal of Production Research* 61 (11): 3634–3650. https://doi.org/10.1080/00207543.2021.1961038.

Sisinni, Emiliano, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. 2018. "Industrial Internet of Things: Challenges, Opportunities, and Directions." *IEEE Transactions on Industrial Informatics* 14 (11): 4724–4734. https://doi.org/10.1109/TII.2018.2852491.

Sousa, Joao, Alysson Bessani, and Marko Vukolic. 2018. "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform." In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 51–58. IEEE.

Sturm, Logan D., Christopher B. Williams, Jamie A. Camelio, Jules White, and Robert Parker. 2017. "Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the. STL File with Human Subjects." *Journal of Manufacturing Systems* 44:154–164. https://doi.org/10.1016/j.jmsy.2017.05.007.

Szabo, Nick. 1997. "The Idea of Smart Contracts." *Nick Szabo's Papers and Concise Tutorials* 2 (9). https://doi.org/10.5210/fm.v2i9.548.

Takahashi, Ryo. 2017. "How Can Creative Industries Benefit From Blockchain." McKinsey & Company.

Tan, Changbai, S. Jack Hu, Haseung Chung, Kira Barton, Cecil Piya, Karthik Ramani, and Mihaela Banu. 2017. "Product Personalization Enabled by Assembly Architecture and Cyber Physical Systems." *CIRP Annals* 66 (1): 33–36. https://doi.org/10.1016/j.cirp.2017.04.106.

Tanwar, Sudeep, Qasim Bhatia, Pruthvi Patel, Aparna Kumari, Pradeep Kumar Singh, and Wei-Chiang Hong. 2019. "Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward." *IEEE Access* 8:474–488. https://doi.org/10.1109/Access.6287639.

Thompson, K. D. 2014. "Smart Manufacturing Operations Planning and Control Program." *Gaithersburg, MD: National Institute of Standards and Technology (NIST)*.

Tuptuk, Nilufer, and Stephen Hailes. 2018. "Security of Smart Manufacturing Systems." *Journal of Manufacturing Systems* 47:93–106. https://doi.org/10.1016/j.jmsy.2018.04.007.

Turner, Hamilton, Jules White, Jaime A Camelio, Christopher Williams, Brandon Amos, and Robert Parker. 2015. "Bad Parts: Are Our Manufacturing Systems At Risk of Silent Cyberattacks?." *IEEE Security & Privacy* 13 (3): 40–47. https://doi.org/10.1109/MSP.2015.60.

Ullah, A. M. M. S.harif. 2019. "Modeling and Simulation of Complex Manufacturing Phenomena Using Sensor Signals From the Perspective of Industry 4.0." *Advanced Engineering Informatics* 39:1–13. https://doi.org/10.1016/j.aei.2018.11.003.

Ullman, David G. 1992. *The Mechanical Design Process*. Vol. 2. McGraw-Hill, New York, ISBN: 9780072975741.

U.S. Food and Drug Administration. 2013. "Drug Supply Chain Security Act (DSCSA)." Online; Accessed August 28, 2022, https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa.

Usuga-Cadavid, Juan Pablo, Samir Lamouri, Bernard Grabot, and Arnaud Fortin. 2022. "Using Deep Learning to Value Free-Form Text Data for Predictive Maintenance." *International Journal of Production Research* 60 (14): 4548–4575. https://doi.org/10.1080/00207543.2021.1951868.

Vatankhah Barenji, Ali, Zhi Li, Wai Ming Wang, George Q. Huang, and David A. Guerra-Zubiaga. 2020. "Blockchain-Based Ubiquitous Manufacturing: A Secure and Reliable Cyber-Physical System." *International Journal of Production Research* 58 (7): 2200–2221. https://doi.org/10.1080/00207543.2019.1680899.

Wang, Jin, Wencheng Chen, Yongjun Ren, Osama Alfarraj, and Lei Wang. 2020. "Blockchain Based Data Storage Mechanism in Cyber Physical System." *Journal of Internet Technology* 21 (6): 1681–1689.

Wang, Miao, Zhenming Zhang, and Zhicheng Zhang. 2019. "Current Research and Prospect of Cloud Application in Manufacturing Equipment Design." In *IOP Conference Series: Materials Science and Engineering*, Vol. 631, 032007. IOP Publishing.

WEF, WEF. 2020. "The Global Risks Report 2020." In *Davos: World Economic Forum. Retrieved November*, Vol. 15, 2020.

Wood, Gavin. 2016. "Polkadot: Vision for a Heterogeneous Multi-Chain Framework." *White Paper* 21:2327–4662.

Wu, Dazhong, David W. Rosen, Lihui Wang, and Dirk Schaefer. 2015. "Cloud-Based Design and Manufacturing: A New Paradigm in Digital Manufacturing and Design Innovation." *Computer-Aided Design* 59:1–14. https://doi.org/10.1016/j.cad.2014.07.006.

Wuest, Thorsten, Daniel Weimer, Christopher Irgens, and Klaus-Dieter Thoben. 2016. "Machine Learning in Manufacturing: Advantages, Challenges, and Applications." *Production & Manufacturing Research* 4 (1): 23–45. https://doi.org/10.1080/21693277.2016.1192517.

Wulfsberg, Jens Peter, Tobias Redlich, and Franz-Ludwig Bruhns. 2011. "Open Production: Scientific Foundation for Co-Creative Product Realization." *Production Engineering* 5 (2): 127–139. https://doi.org/10.1007/s11740-010-0286-6.

Yakovenko, Anatoly. 2018. "Solana: A New Architecture for a High Performance Blockchain v0. 8.13." *Whitepaper*.

Yoo, Minjae, and Yoojae Won. 2018. "A Study on the Transparent Price Tracing System in Supply Chain Management Based on Blockchain." *Sustainability* 10 (11): 4037. https://doi.org/10.3390/su10114037.

Yu, Lei, and Huan Liu. 2003. "Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution." In *Proceedings of the 20th International Conference on Machine Learning (ICML-03)*, Washington, DC, 856–863.

Zangaro, Francesco, Stefan Minner, and Daria Battini. 2021. "A Supervised Machine Learning Approach for the Optimisation of the Assembly Line Feeding Mode Selection." *International Journal of Production Research* 59 (16): 4881–4902. https://doi.org/10.1080/00207543.2020.1851793.

Zeltmann, Steven Eric, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. 2016. "Manufacturing and Security Challenges in 3D Printing." *Jom* 68 (7): 1872–1881. https://doi.org/10.1007/s11837-016-1937-7.

Zhang, H.-C., and S. H. Huang. 1995. "Applications of Neural Networks in Manufacturing: A State-of-the-Art Survey." *The International Journal of Production Research* 33 (3): 705–728. https://doi.org/10.1080/00207549508930175.

Zhang, Zhibo, Prakhar Jaiswal, and Rahul Rai. 2018. "Featurenet: Machining Feature Recognition Based on 3D Convolution Neural Network." *Computer-Aided Design* 101:12–22. https://doi.org/10.1016/j.cad.2018.03.006.

Zhang, Binbin, Prakhar Jaiswal, Rahul Rai, Paul Guerrier, and George Baggs. 2019. "Convolutional Neural Network-Based Inspection of Metal Additive Manufacturing Parts." *Rapid Prototyping Journal* 25 (3): 530–540. https://doi.org/10.1108/RPJ-04-2018-0096.

Zhang, Zhibo, Chandan Kumar Sahu, Shubhendu Kumar Singh, Rahul Rai, Zhuo Yang, and Yan Lu. 2023. "Machine Learning Based Prediction of Melt Pool Morphology in a Laser-Based Powder Bed Fusion Additive Manufacturing Process." *International Journal of Production Research* 1–15. https://doi.org/10.1080/00207543.2023.2201860.

Zhang, Hao, Qiang Liu, Xin Chen, Ding Zhang, and Jiewu Leng. 2017. "A Digital Twin-Based Approach for Designing and Multi-objective Optimization of Hollow Glass Production Line." *IEEE Access* 5:26901–26911. https://doi.org/10.1109/ACCESS.2017.2766453.

Zhang, Yongping, Xiwei Xu, Ang Liu, Qinghua Lu, Lida Xu, and Fei Tao. 2019. "Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System." *IEEE Transactions on Computational Social Systems* 6 (6): 1386–1394. https://doi.org/10.1109/TCSS.6570650.

Zhang, Zhibo, Yanjun Zhu, Rahul Rai, and David Doermann. 2022. "PIMNet: Physics-Infused Neural Network for Human Motion Prediction." *IEEE Robotics and Automation Letters* 7 (4): 8949–8955. https://doi.org/10.1109/LRA.2022.3188892.

Zheng, Xiaochen, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. 2018. "Blockchain-Based Personal Health Data Sharing System Using Cloud Storage." In *2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom)*, 1–6. IEEE.

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. 2017. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." In *2017 IEEE International Congress on Big data (BigData Congress)*, 557–564. IEEE.