SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Blockchain Technology in Overcoming Security Threats for Smart Manufacturing System - A Systematic Literature Review

Ahmed Mohamed Gaafar Mahmoud Ali[1,*], Kelvin Chong Boon Kai[1], Zool Hilmi Ismail[1,2]

[1] Malaysia–Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, Kuala Lumpur 54100, Malaysia
[2] Center for Artificial Intelligence and Robotics, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, Kuala Lumpur 54100, Malaysia

ARTICLE INFO

Article history:
Received 6 June 2023
Received in revised form 14 December 2023
Accepted 6 January 2024
Available online 7 February 2024

Keywords:
Blockchain; systematic literature review; security threat; Industrial Revolution 4.0; smart manufacturing system; computer-aided manufacturing

ABSTRACT

Blockchain is a new emerging technology that is mainly used to add security layers to many applications. Studies showed that businesses and manufacturing industries suffer from cyber-attacks, especially after the emergence of Industry 4.0 and IoT devices connected to the cloud for data sharing purposes, these interactions between IoT devices and the information involved in the transactions between companies and customers produce a massive amount of data daily. This phenomenon becomes an easy target for attackers due to the security limitations, data corruption and compromised reliability of the traditional manufacturing systems during data transferring. Many have focused on the methods to address these security limitations of the manufacturing businesses. This paper shed the light on the major smart manufacturing sectors that can potentially benefit from blockchain technologies, including cloud manufacturing, collaborative manufacturing, digital twin manufacturing, robonomics based smart manufacturing and the supply chain industry. The blockchain can enhance the security by creating a decentralized environment for the data to be stored, which will make the data stored immutable for improved security. These immutable data are nearly impossible to manipulate, replace, or falsify the data stored on the blockchain secured network.

1. Introduction

1.1 Background on Smart Manufacturing Systems

Smart manufacturing is a general technique that is powerful to automate and ease the manufacturing tasks, it can be applied to production and adopted to other technologies that a specific industry need. The general goals of smart manufacturing focus on optimising the generation, production, and product transaction. Manufacturing in general can be defined as multiphase process of creating new products out from raw materials, hence; a smart manufacturing is a one subset of manufacturing that employs a computer-aided control of the tasks of one industry. By utilising the most recent technologies (e.g., IoT devices, Industry 4.0) and advanced information (e.g., big data),

* *Corresponding author.*
E-mail address: amdgaafar@gmail.com

https://doi.org/10.37934/araset.39.1.4358

the manufacturing process becomes more effective and flexible, which is more helpful in addressing the dynamic needs of the global market, rather than a specific process hardcoded as in traditional manufacturing as discussed by Yoo *et al.,* [1]. Blockchain is a new generation of secure information technology that is fueling business and industrial innovation.

1.2 Background of Blockchain

Blockchain is the peer-to-peer distributed ledger technology that powers the digital currency "Bitcoin". It is a trending and emerging technology that is influencing many businesses and communities, demonstrating significant success in a variety of fields such as finance, government, supply chain management, health, and many others [2].

Blockchain network or database consists of several decentralised nodes and each node can only append to the network or read from the network; the data cannot be altered once placed on the network. The nodes verify any new additions to the network, and they have the ability to enter new information to the database with the condition that all nodes must reach a consensus. The agreements between the nodes are the source of the security of the network, making it near impossible to temper with the data. In comparison, the traditional database that utilises a client-server network architecture, the client can create, read, update, or delete the data stored on the server. The control of the database and the entity who give permissions to the client to access the server remains with a centralised designated authority. The security of the centralised network could be compromised as the data could be altered or even deleted [3].

The blockchain network is cost-effective and efficient as it eliminates the need for intermediaries and reduces duplication of effort. It is also less vulnerable because it validates information using consensus models. Therefore, data stored on blockchain networks are safe, secure, and verifiable by other nodes. Many studies have been conducted on key enabling technologies for resource organisation and system operation of blockchain secured smart manufacturing in Industry 4.0. However, the advancement and promotion of these blockchain applications have been severely hampered by a variety of scalability, flexibility, and cybersecurity issues. This systematic review investigates on how blockchain systems can overcome potential cybersecurity barriers on their way to intelligence in Industry 4.0.

A smart manufacturing system is an unavoidable outcome of smart, personalised, and sustainable manufacturing processes. Large-scale manufacturing data will be constantly exchanged. Machines will be able to make local decisions autonomously, which will undoubtedly have an impact on the entire manufacturing process. This creates a security risk that cannot be ignored, necessitating the development of security tools.

The following sections highlight on the history of smart manufacturing and how it evolved over time. Then in section 3, the research methodology, the selection of the data base, and the result from our search will be further elaborated. In section 4, a discussion on the results and the research papers that have been found is done by showing how smart manufacturing is integrated with other technologies. Finally in section 5 includes a conclusion that summarizes all of our findings.

2. Related Works

2.1 A History of Smart Manufacturing

The first time the term "Smart Manufacturing" was revealed was at a National Science Foundation workshop titled "Cyberinfrastructure" in 2006. Initially, it was referred as "Smart Process Manufacturing", however, it was quickly shortened to "Smart Manufacturing". During that period,

cyber-infrastructure was applied to innovations that combine new applications with the power of data sharing by using connected networks that harvest information from various locations. The workshop presented the techniques used for multi-scaling dynamic modelling and simulation, large-scale optimization, sensor networks, data interoperability, and requirements-driven security, as well as coining the term “Smart Plant”. At the time, Germany was working on a similar initiative called “Smart Factory”, which was renamed to Industry 4.0 a few years later. Smart Manufacturing and Industry 4.0 have evolved concurrently. Industry 4.0 emphasised on cyber-physical systems, whereas Smart Manufacturing emphasised highly on connected information-driven manufacturing. Both agendas have a lot of overlaps, and there will be more parallel and collaborative efforts in the future.

Later in 2010, as part of the Smart Manufacturing Leadership Coalition (SMLC), more than 50 industry leaders gathered in a workshop to advance the development of the infrastructure and capabilities required to realise the full potential of smart manufacturing. The outcomes of this meeting have documented the goals of smart manufacturing as well as the challenges they face (e.g. affordability, usability, interoperability, customer integration, protection of proprietary data, and cyber security) Following that, in 2014, the first version of Industry 4.0, German Standardization Roadmap was released, it pointed out that standardisation is the main key to continue the success of smart manufacturing.

By 2016, United States advanced the implementation of smart manufacturing techniques. Manufacturers, consultants, technology vendors, and academia were brought together by organisations such as the Manufacturing Enterprise Systems Association (MESA), the Industrial Internet Consortium (IIC), and the Smart Manufacturing Leadership Coalition (SMLC) to accelerate the implementation and document the practises and progress in Smart Manufacturing. Smart Manufacturing had gained traction by 2017. Trade organisations and consulting firms were documenting success stories and practises, such as in Deloitte’s “The Smart Factory” report. Consulting firms have also begun to publish guidance, such as the Singapore Smart Industry Readiness Index [5], to assist manufacturers in assessing their business practises and developing roadmaps to higher levels of Smart Manufacturing adoption.

Smart Manufacturing was defined as the vertical and horizontal integration of connectivity, intelligence, workforce, and automation across multiple business process dimensions such as product lifecycle, operations, and supply chain. Nowadays, smart manufacturing has had evolved and many interties are adopting and integrating new technologies to catch with the flow of never-ending new innovations, the history of smart manufacturing is depicted in Figure 1. Given all the attention smart manufacturing was given, its technologies i.e. Internet of Things has been researched and employed in the education system as concluded by Zainal *et al.,* [4].

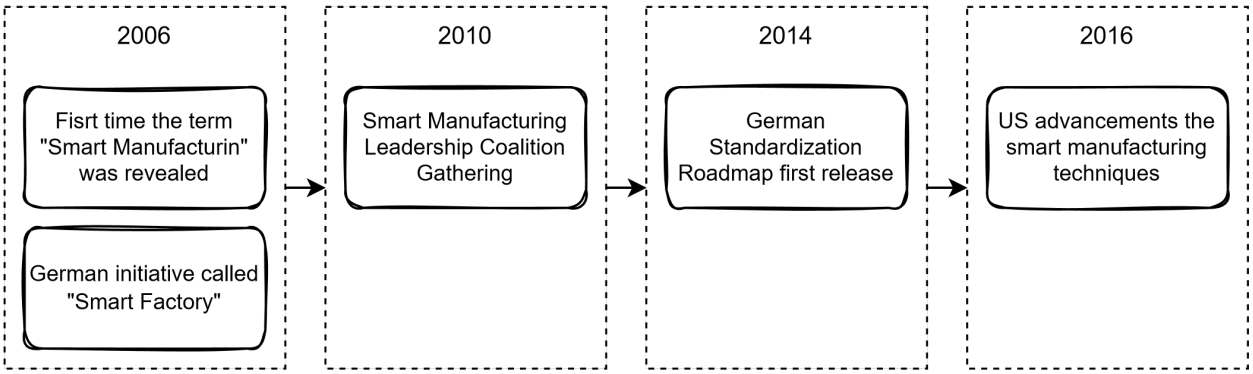

Fig. 1. Brief history of smart manufacturing

3. Research Methodology

A related works section is conducted by using databases declared in the references section, which included 4 references about the history of smart manufacturing and blockchain. A systematic literature review was conducted using the IEEE and ScienceDirect databases, which included many studies on the manufacturing industry and how blockchain can be applied to it. The articles are retrieved in order to answer the survey's specified research question.

3.1 Research Question

i. RQ1: What are the major shortcomings of the traditional manufacturing system?
ii. RQ2: What are the advantages of blockchain technology?
iii. RQ3: What are the security threats that are potentially possessed by smart manufacturing systems?
iv. RQ4: How can blockchain technology resolve the shortcomings of the traditional manufacturing system?

3.2 Databases for Systematic Literature Review Searching

This systematic review was conducted on two well-known literature databases with scientific scope, which are IEEEXplore Digital Library and ScienceDirect. The results of chosen articles have been filtered according to the specified exclusion criteria.

3.3 Exclusion Criteria

i. EC1: Works that include history on smart manufacturing and blockchain.
ii. EC2: Works not related to Blockchain, Smart Manufacturing and Security threats.
iii. EC3: Works that do not present any type of experimentation or comparison results, and make only propositions.
iv. EC4: Works dated before the year 2017.

3.4 Execution

The keywords for each database were chosen based on the literature review conducted and the application of blockchain technology, which includes "smart manufacturing" as the application, "blockchain" as the technology used for the application, and "security" as the benefit of using the technology in use. These keywords have been placed in the search bar of each database as follows:

i. IEEE-Xplore: "blockchain" AND "smart manufacturing" AND "security"
ii. ScienceDirect: "blockchain" && "smart manufacturing" && "security"

3.5 Results

Based on our exclusion criteria, 9 articles have been chosen from IEEE-Xplore and 8 articles have been chosen from ScienceDirect. The research trend by applying these keywords in each of the databases resulted in the trend illustrated in Figure 2.

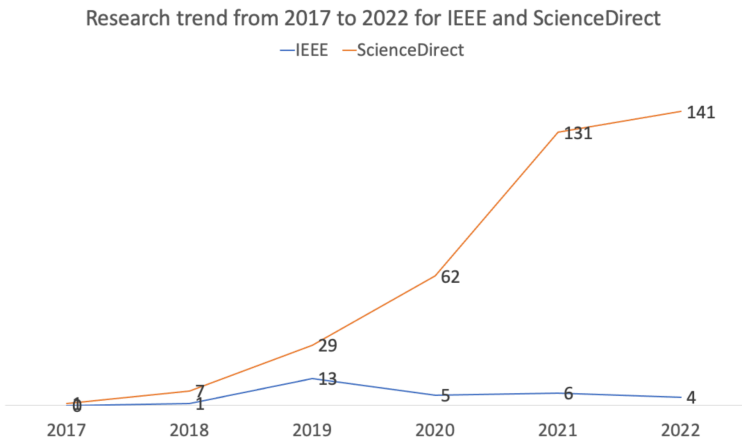

Fig. 2. Research Trend from 2017 to 2022 for IEEE and ScienceDirect

The survey was performed on July 2022, which produced the following results in each of the databases, IEEE Xplore revealed 29 articles and ScienceDirect produced 371 articles as shown in Figure 3.

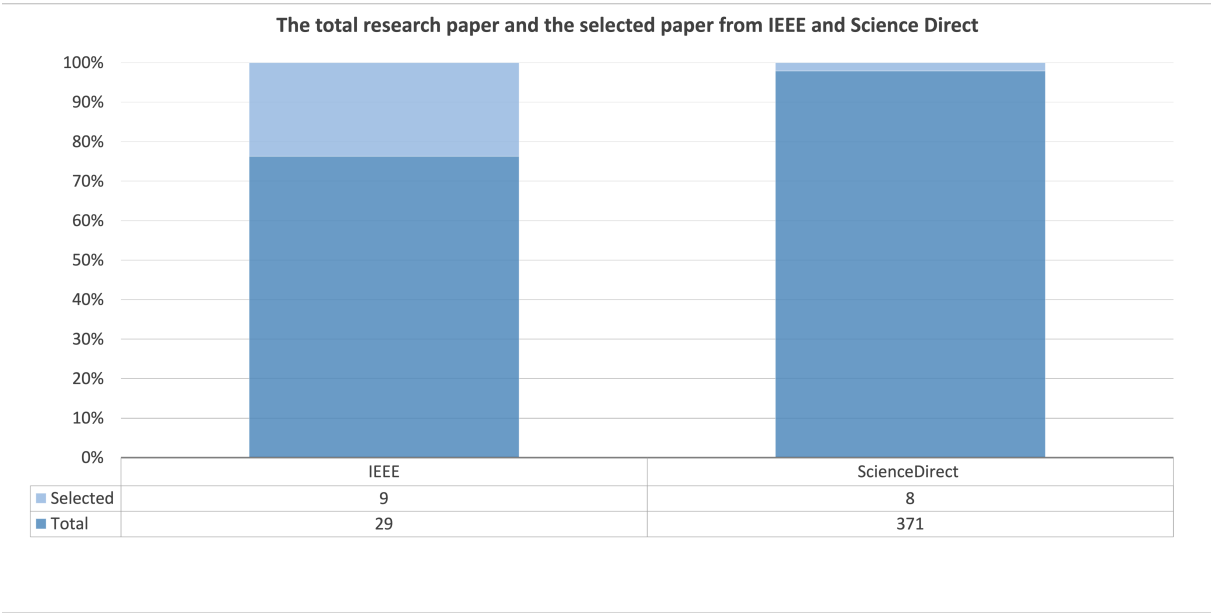

Fig. 3. The total research paper and the selected paper for IEEE and ScienceDirect

Throughout the screening process, only the relevant articles which fulfilled the keywords will be chosen. Hence, a total of 381 articles have been removed from the selection process. 1 article is excluded from the selection due to duplication between the two domains, IEEE Xplore and ScienceDirect. At the end, a total of 17 articles are selected for this systematic review.

i. IEEE Xplore: 29 / choose 9
ii. ScienceDirect 371 / choose 8

4. Discussion

4.1 The Different Types and Categories of Blockchain Algorithm and its Advantages

According to [5-7], a consensus protocol refers to a set of rules that is known as the heart of all transactions of blockchain. It is the agreement of adding a block to the blockchain through the consensus protocols. It is to make sure all the transactions are trusted and anonymous by validating every transaction to be legal. As the goal of blockchain system's integrity, consensus protocol has been used as a foundation in which the trustworthy Blockchain system is built. As a contrary, the distributed and centralised systems are built without a universal trust mechanism such as consensus protocol, blockchain-secured system is capable of compensating the security issue of the conventional system. The consensus layer is the layer between the application and the network layer as shown in Figure 4. A number of blockchain's consensus protocol has been introduced, which include but not limited to Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT) [8].

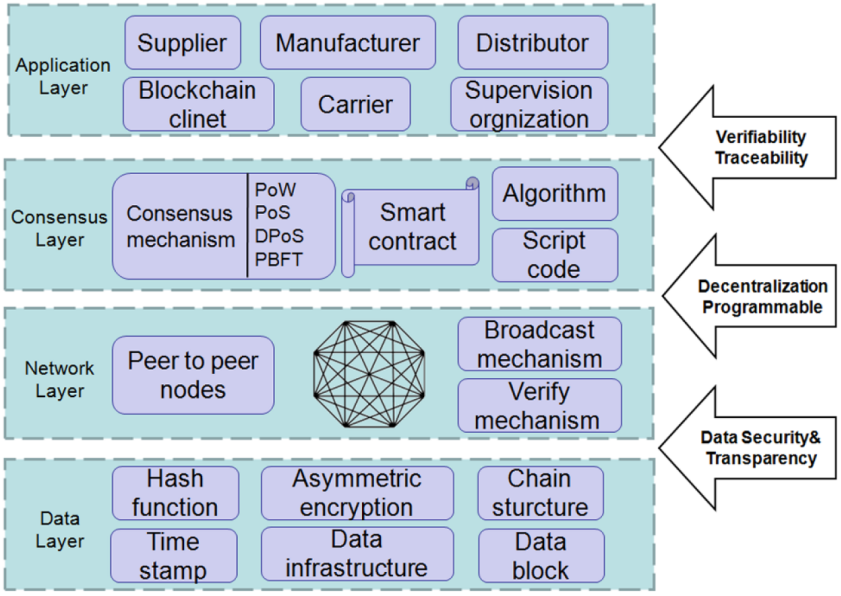

Fig. 4. High level overview of a blockchain structure [7]

By successfully validating the data using various consensus mechanisms, smart contracts work by only allowing the validated data to be stored in the blockchain network. The blockchain's ability to write a highly objective computer code that specifies how a process will be managed and what steps will be taken when an event occurs in addition to providing a distributed, unalterable record of all the various events that have occurred is what makes the smart contract another wonderful aspect of the technology. Breaking the constraints of Bitcoin was one of the objectives of the smart contract proposed in Ethereum. The concept of a smart contract is computer code that is written to react to specific kinds of important events. The smart contract does not have to be legally binding or involve more than two parties. The smart contract, which is the foundation for enterprise blockchain applications, will revolutionise the way we conduct business. Smart contracts can be created by anyone without the use of middlemen. The smart contract offers independence, effectiveness, efficiency, and cost savings.

i. Proof of Work (PoW): PoW works by selecting a problem that can be solved by guessing. Every node (also known as a mining node) in the network is guessing various nonce values

at random until one node accidentally discovers the nonce value that corresponds to the difficulty first. In order to successfully create a block to link to the blockchain and earn an incentive mining reward, a mining node must expend a lot of computational resources on it (hence called "work") and solve the problem faster than others. The PoW consensus algorithm's central cryptographic puzzle, on the other hand, is comprised of hash functions. PoW is adopted by Bitcoin, and Ethereum as their consensus algorithm. However, it requires a considerable amount of time and energy.

ii. Proof of Stake (PoS): PoS is the second most prominent consensus after PoW. It is a refinement of PoW where it requires less computations than PoW. It is built to address the time and electricity consumption problem of PoW. To be selected as the next block creator in a PoS network, nodes must stake some money. The creator of each chosen block will get the transaction fees related to that block. A block winner will forfeit their stake if they attempt to add an invalid block. Ethereum 2.0 adopted PoS as its consensus algorithm.

iii. Delegated Proof-of-Stake (DPoS): All token holders in DPoS have the ability to cast votes for a certain number of delegates and to assign voting authority to other users. Then, in order to secure the network, the delegates are in charge of validating transactions and blocks. Unlike PoW and PoS, DPoS only reward the best miners through voting, instead of the miners with the most computing power. One blockchain system that employs the DPoS algorithm is EOS.

iv. Proof of Elapsed Time (PoET): PoET is developed by Intel as a different rewarding mechanism for miner to mine a block. To validate a node, a randomly generated waiting time is produced on a reliable platform. The first node to finish waiting for the allotted amount of time is the validation winner and is able to add the new block. Because of the trusted computing platform, each node has a chance to win.

v. Practical Byzantine Fault Tolerance (PBFT): The goal of Byzantine Fault Tolerance (BFT) is to find a suitable consensus while resolving the dishonesty problem. BFT is optimised by the consensus algorithm known as PBFT [9]. In PBFT, the blockchain system will come to consensus on the blockchain's present state as long as the number of malicious or hostile nodes is less than one-third of all the nodes. The security of a blockchain system increases with the number of nodes. PBFT is currently employed by Hyperledger Fabric.

Table 1
Types of Blockchain

Label	Blockchain type	Characteristics	Example of usage
B1	Proof of Work (PoW)	Public permissionless/ private blockchain	Bitcoin
B2	Proof of State (PoS)	High cost and power	Ethereum
B3	Delegated Proof of State (DPoS)	consuming, but high return	Ethereum 2.0
B4	Proof of Elapsed Time (PoET)	Public permissionless/ private blockchain	EOS
B5	Practical Byzantine Fault Tolerance (PBFT)	low cost, and high energy efficiency, lower return	Sawtooth

4.2 Security Threats Possessed by Blockchain

According to [5,6], blockchain security merits are further studied because it is decentralised without involving a third party and requires building trust into a trust-less infrastructure. This section will highlight the security risks associated with blockchain technology and provide an analysis of

actual hacks and flaws in blockchain systems [10]. The types of security threats are summarised in Table 2.

Table 2
Types of security threats

Attack	Description
Network Attacks	A denial-of-service attack (DoS) may disrupt the functionalities of blockchain and make it unavailable by submitting many transactions at once as the blockchain can only process a certain number of transactions at a time.
Endpoint Security	Endpoints may be diverse, giving hackers more ways to take advantage of security holes. Endpoints may also be homogeneous, meaning that a problem in one system may affect all other systems.
Intentional Misuse	The attackers may control more nodes to launch attacks like 51% type of attacks.
Code Vulnerabilities	Smart contracts, which are open-source and anyone can create, or the platform code itself, can both contain vulnerabilities. Due to the distributed network and the inability of the code to be changed once it has been deployed, the vulnerabilities have a significant impact.

4.3 Cybersecurity Issues in the Manufacturing System

Industrial 4.0 promises individualisation, system flexibility and product quality, as the benefits from the change from a centralised manufacturing system to a decentralised manufacturing system. The smart manufacturing system as a result of rapid development of Industry 4.0 will see massive improvement in its autonomous and highly flexible manufacturing technology. It is achievable by the seamless integration of immediate and fast communication of system across its operation and manufacturing system. However, it is harder as it is more complex to build a smart manufacturing system with intelligence, traceability, security, and flexibility. For example, the integration of advanced information techniques in the operation and configuration stage can result in or become very vulnerable to malicious attack. Nevertheless, the centralised-controlled manufacturing system has a downside of device spoofing and false authentication in information sharing. A centralised-controlled platform will fail to protect data privacy from other participants as the flow of coordination decision making involves knowing the capabilities and status of each other. The vulnerability to fault of a single key node in centralised-controlled platform will only result in unreliable networking and data service. Peer-to-peer interaction is also difficult due to the heterogeneous nature of diversified equipment and the individualised service requirements. Confidentiality and trust issue between participants remains the critical issue in the control and management of distributed manufacturing network [6].

Additionally, because industrial products require widespread mass personalization across systems in addition to these security concerns, it greatly complicates the activities involved in production and supply. Since it is necessary to be aware of each other's capabilities and status in order to make coordination decisions, a centralised platform cannot safeguard participant data privacy. Additionally, manufacturers must address the single key node's weak robustness to faults in unreliable networking and data service [7,11,12]. The types of risks and threats are summarised in the Table 3.

Table 3
Types of manufacturing system's security threats

Label	Security threats
T1	Traceability of operations
T2	Cyber-attacks to the digital trend
T3	Advanced virus on control system
T4	Device spoofing and false authentication in data sharing
T5	Interoperability among heterogeneous equipment
T6	Confidentiality and trust between participants
T7	Information vulnerability and reliability across systems
T8	Failure of key nodes in centralised platforms.

4.4 Implementation of Blockchain in Smart Manufacturing's Supply Chain Trust Management

According to [7], information about supply and demand as well as supply chain management are all included in the flow of the supply chain. It is continuously produced through logistics operations. The management of information flow in real time can increase the effectiveness of supply chain management. All parties in the supply chain can obtain accurate management information, timely transmission of demand, supply information, and real-time information to better direct the operation of logistics and capital flow. The information carrier has become more varied with the development of the new generation of information technology, the digital development of information systems. The problems associated with the conventional supply chain management are depicted in Table 4.

Table 4
Problems associated with the conventional supply chain

Problem	Description
Data Ownership	While some data can be kept indefinitely, others are only useful in the short term. As digital resources, data involves ownership which includes the right to use, right to abolish and other rights.
Data Quality	As it is easy to generate new data, it becomes more challenging to ensure the data to be traded are scientific, true, and reliable. Thus, it is imperative to have a data quality evaluation system that could handle all aspects of data collection, data cleaning, data sorting and data transaction backed by authoritative standards and specialised certification organisations. The implementation could promise the circulation of reliable transaction by ensuring the data quality and credibility.
Data value	Given the variety of data types, it can be difficult to assign a price or value to them. A fair range of data prices in terms of standard specifications can be created with the help of the unified standard pricing model and strategy. A neutral, reliable, and substantial transaction platform can establish a market mechanism that leads to a reasonably priced data price system between supply and demand parties.
Data security	Numerous amounts of data shared are exposed to data leakage, especially in the big data era. In the light of this, information security is currently a crucial national security concern that cannot be neglected. The blockchain technology is adopted which can effectively address the aforementioned security issues to enhance individual privacy and national wide security.

The data management based on blockchain is primarily where the trust management of supply chain information flow is embodied in order to ensure the authenticity and security of data. The blockchain system is implemented in various phase, namely, the initialisation phase, data encryption phase, data on-chain phase and data access phase. The phases are descripted and summarised in Table 5 and the implementation is illustrated in Figure 5.

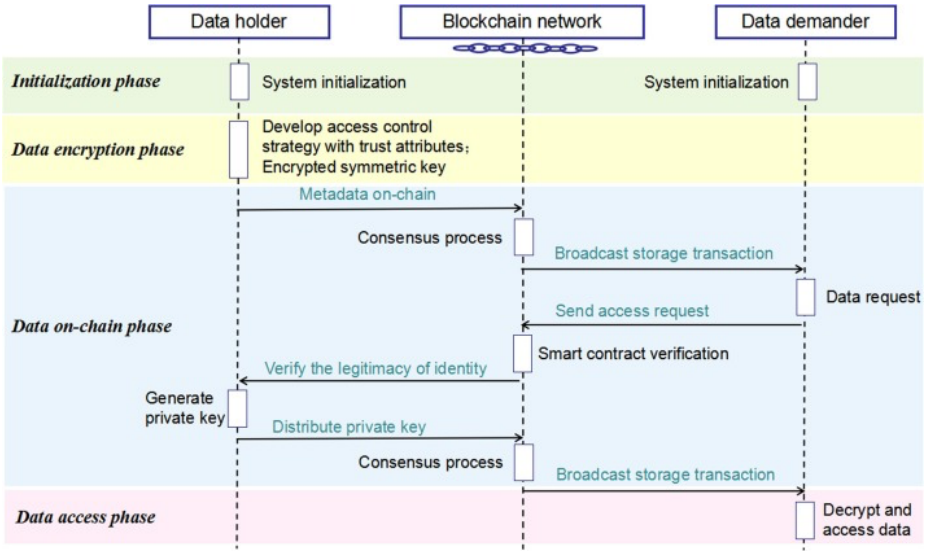

Fig. 5. The overview and illustration of blockchain implementation in supply chain trust management system [7]

As shown in Kobzan *et al.,* [13], a permissioned blockchain-based data sharing solutions for supply chain was released by IBM. Blockchain has also been used in the tracking and monitoring of logistics information. The implementation of blockchain on the tracking and monitoring system creates a transparent, secure, and traceable system. The online coordination of regional operations is the role of the Manufacturing Execution system (MES) for smart manufacturing. Blockchain offers a unified computing and networking model, allowing data to be processed quickly and effectively locally close to end devices. Moreover, Stanciu [14] developed the distributed control system by integrating the blockchain, smart contracts, and microservices technologies. Function blocks for actual production process control are implemented at the lower executive level using microservices in edge node Docker containers. Smart contracts are implemented at a higher supervisor level to coordinate the network-wide execution of microservices running in containers.

Table 5
Phases of supply chain

Information of blockchain	Methodology	Results
Initialization phase	Initialise parameters to generate system public key and master key. The parameters include bandwidth, transmission delay, and packet loss rate as the trust factor for trust management model based on blockchain.	Encourages each node to actively share data and resist malicious users.
Data encryption phase	Encrypt the shared data released by the data holder via the blockchain network, and ensure the safe storage of the original data file. The symmetric key is too encrypted.	Only visitors who meet the reliability attributes formulated by the data holder have the view and download permission to the data.
Data on-chain phase	Shared data information, storage address and encrypted keys are stored in new block, and sync with the entire blockchain network.	Every transaction record is traceable and immutable.
Data access phase	Address of the data and the symmetric encryption key can be found in the blockchain network.	The key to access the data can only be decrypted for data demander if the basic attributed and trustworthiness are met.

4.5 Implementation of Blockchain in Cloud Manufacturing System

Most manufacturing systems involve the use of IoT, Industry 4.0 and centralised databases which result in a massive amount of data known as the big data. These are intruding concerns and flows regarding the security, privacy, and reliability of the data being stored and shared. Therefore, many researches have brought the light on addressing these issues and one of the most promising solutions is by incorporating blockchain technology in the manufacturing systems.

According to authors in Wan *et al.,* [15] have introduced a blockchain architecture to be mainly used in smart factories, the architecture of the blockchain consists of five layers: the sensing layer, the management hub layer, the storage layer, the firmware layer, and the application layer. Moreover, Ray [3] explored the applications of blockchain on cloud manufacturing; which has emerged following the evolution of Industry 4.0 and IoT. In short, the shortcomings of cloud manufacturing are related to reliability, security, continuity, and scalability. Therefore, they introduced a blockchain architecture specific for cloud manufacturing.

Li *et al.,* [16] highlights the limitations of the conventional methods of the centralised network, and proposed a blockchain-based architecture named "BCmfg"; which consists of five layers. On a case study, they demonstrated the main benefits of implementing this blockchain-based network architecture. 32 cloud services and 15 connected users are taken into account in the case study. They assessed the blockchain architecture with regard to confidentiality, integrity, and availability and demonstrated that the blockchain-based network ensures that all three issues are taken care of.

4.6 Implementation of Blockchain in Collaborative Manufacturing System

Collaborative manufacturing has been discussed in detail by Zhang *et al.,* [17], which involves the use of IoT devices, connected to the cloud for collaboration purposes and one of the main challenges faced in collaborative manufacturing is the high expenses imposed when sharing the data between industries; especially with the countless collaborations are made with customers. The challenges also include the security, privacy, and scalability issues found in manufacturing systems in general since IoT devices generates a massive amount of data with the large number of sensors and information which increase the privacy and security concerns for both customers and industries. Therefore, the main issue is the high expenses imposed, and is paid by the manufacturing industries to ensure trust. The cycle of these expenses is depicted in Figure 6. The proposed solution for this type of manufacturing requires a decentralized network, known as blockchain. However, they found that traditional blockchain is limiting in terms of the size of data, the transaction processing rate, and the latency of data transmission. Therefore, they proposed a better implementation of blockchain specific application for collaborative manufacturing which improves the security and reduce the cost of trust significantly. It is achieved by encapsulating all data, such as task information, service information, identity data, transaction data, asset data and contact data; into one block for asymmetric encryption. It is integrated into the blockchain to meet security requirements and ownership verification requirements.

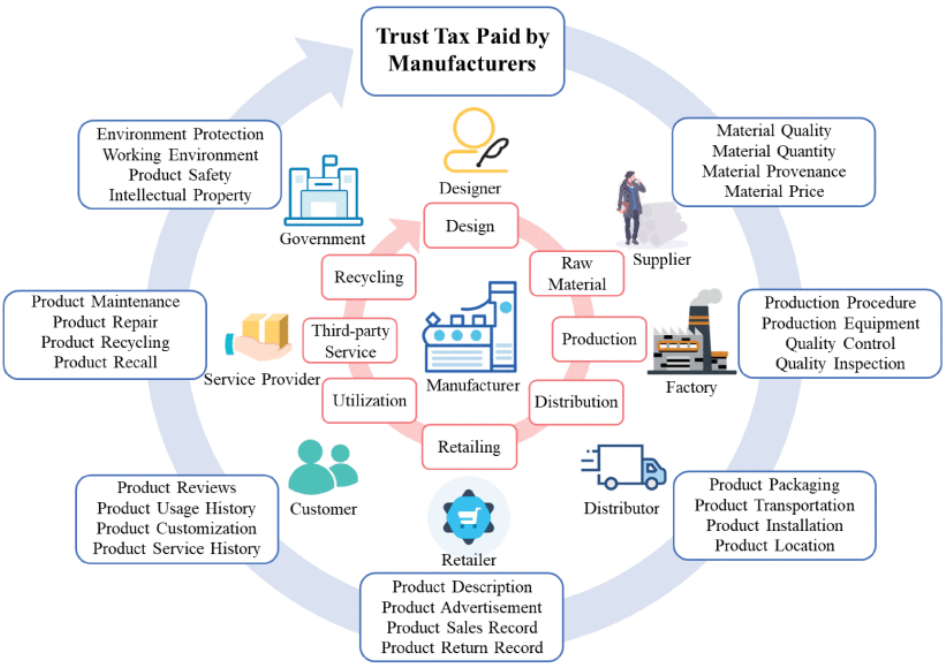

Fig. 6. The tax bored by manufacturing industries to insure trust [17]

4.7 Implementation of Blockchain in Digital-Twin Based Manufacturing System

Digital Twin (DT) is another important sector in the smart manufacturing systems, which is a virtual representation of a physical object or process in industrial applications. DT technology is built on the foundations of several other technologies, including artificial intelligence, IoT, and big data analysis. As shown by Khan *et al.,* [9], in traditional manufacturing systems, the data collected by a DT are stored in clouds or fog which introduces many deficiencies related to security, privacy, and reliability. Therefore, they have introduced merging blockchain with IoT to tackle these weaknesses. The traditional blockchain introduces shortcomings, including high transaction processing delays and unusually expensive consensus mechanisms, therefore, the authors have introduced a new variant of blockchain which they called Twinchain, specifically designed for DT manufacturing systems. The main advantage of this proposed blockchain is that it is quantum resilient.

4.8 Implementation of Blockchain in Robonomics Manufacturing System

Kapitonov *et al.,* [18] sheds light on the use of robonomics based smart factories, which involve a large number of autonomous agents and are also known as robot economies. The authors detailed the structure of one solution by adding a security layer to robonomics based smart factories. This included the use of blockchain technology and the ethereum network's smart contact. The robonomics infrastructure finds a match between supply and demand, and then smart contracts for factories and warehouses are created.

The main challenges that are faced by smart factories in general are:

i. Flexibility of work
ii. Scalability
iii. High quality feedback
iv. Fault tolerance
v. Security

The challenges that are faced by robonomics based smart factories specifically that can be addressed by considering the:

i. Organization of agent's intelligent behaviour.
ii. Effectiveness and unified protocol of interaction between a variety of agents, different in physical action and software.
iii. Standardized method of cooperation, coordination, and joint decision-making between agents.

Therefore, they have created an environment for organizing the workflow of the robonomics network, which have used blockchain as a technical foundation for interaction between agents.

4.9 Smart Grid in Local Energy Markets

As concluded by Khattak *et al.,* [19], the energy consumption in Malaysia is in continuous increase due to the growth in population and energy resources becoming more expensive. Therefore, it is crucial for the Malaysian government to invest in a reliable and affordable energy access to keep up with the ongoing development in energy consumption. This highlights the importance of a careful planning by the government to ensure energy security for the population. Moreover, it is important for all stakeholders to acknowledge the urgency of implementing a more efficient grid system for the country.

As the renewable energy sources increase, Mengelkamp *et al.,* [20], proposed a Local decentralised approach based on blockchain technology which could be implemented in the local energy market. They demonstrated methodology of a decentralised market approach and provided a simulation of 100 local residential households. This approach utilises a distributed information and communication technology that is the private blockchain, which is the base of the decentralised nature of the local energy markets (LEM). This approach provides energy consumers a platform that does not depend on a central intermediary, this approach requires more research and real-life implementation. Moreover, Mollah *et al.,* [21] reviewed the works where blockchain is applied to smart grid and concluded that digitalising the conventional legacy will translate into a more accurate and efficient access to Energy and better delivery system. The primary goal of incorporating blockchain technology into smart grid systems is to create a reliable and reliable billing and metering framework. In this context, various consensus algorithms, such as B1 and B2, are commonly used, each tailored to the specific requirements of each grid system.

4.10 Comprehensive Implementation Overview of the Applications in Blockchain

The security threats in Table 3 that addressed by different industries are summarised in Table 4 with respect to the industry's type. The blockchain consensus types adopted by the industries in the blockchain network are grouped in accordance to their industry types. Hence, the summary of the technologies, challenges, and solutions are tabulated in Table 6.

It is observed that the most common security threats to the traditional manufacturing system in various industries are T2, cyber-attack. Due to the centralised database, it gave everyone easy access to the data without an additional layer of security. Nevertheless, it is clear that blockchain has been efficient in addressing and resolving each manufacturing system's respective security threats. From various industries, they use mostly B1, B2, and B3 consensus algorithm as these prominent consensus mechanisms are proved to be effective in lowering cost of trust and reducing the security flaws. In

the supply chain's trust management system of smart manufacturing, data security has been a common concern. The integration of blockchain has encrypted every phase of data to ensure its data integrity and quality without compromises.

Table 6
Summary of blockchain implementation on different manufacturing sectors

Industry type	Technologies used	Challenges	Security threat	Solution	Blockchain's consensus	key advantages
Cloud manufacturing	Industry 4.0 and IIoT	Centralised architecture is very fragile	T1, T2, T4	Introduce a new IIoT architecture and a 5 Layer blockchain	B1, B2, B3	Extendable
Collaborative manufacturing system	IoT	Expensive collaboration taxes	T2, T4, T7	Use a private blockchain network	B1, B2, B3, B5	Reduce the cost and improve the security and reliability
Digital Twin manufacturing	IoT and cloud database	Weak against quantum attacks	T2, T8	Blockchain network specified for the needs of Digital Twin	B1, B2, B3, B5	Resilient to the quantum attacks
Robonomics based smart factory	Robonomics, autonomous agents, multiagent systems	Organisation and effectiveness of multi-agent systems	T5	Blackchin as a technical basis for interaction between agents	-	Assist in Organising multiagent systems
Supply Chain Trust management system in smart manufacturing	Smart manufacturing, Industry 4.0	Vulnerable to data leak and compromised data system	T1, T2, T3, T6, T7	Blockchain secured data encryption system	-	Better data integrity and quality
Smart Grid	Industry 4.0 and IoT	Integrating large amount of connection, especially with the renewable energy	T1, T2, T6, T7, T8	Decentralised local energy markets	B1, B2, B3, B4, B5	More efficient, especially for renewable energy

(-): Not specified

5. Conclusion

As a conclusion, the conventional manufacturing system possesses certain security threats, particularly, on the transition to becoming a smart manufacturing system. Blockchain is increasingly becoming popular in the application of data security due to its decentralised and anonymity features. These emerging information security technologies have been slowly adopted in many manufacturing fields to compensate for the security threats possessed by the smart manufacturing system. The different types of blockchain's consensus type have been discussed as these consensuses are the key determining factor to verify legal and valid transaction in the blockchain network. In the end of the section, the adaptation of different blockchain technology by different industries has been compared to provide a comprehensive view of the how blockchain is enhancing the data network to maintain the data integrity and trustworthiness. This paper summarises the implementation of blockchain in

different manufacturing systems to address the different underlying security threats in the existing system for a more secure, reliable, and trustworthy system. More specifically, the implementation of blockchain technology in cloud manufacturing, digital twin manufacturing, robonomics based smart factory, collaborative manufacturing system, and supply chain trust management system of smart manufacturing.

Acknowledgement
This research was not funded by any grant. The authors would like to thank Universiti Teknologi Malaysia (UTM) for facilities support.

References

[1] Yoo, Sangkeun, Yong-woon Kim, and Hoon Choi. "An assessment framework for smart manufacturing." In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 553-555. IEEE, 2018. https://doi.org/10.23919/ICACT.2018.8323827
[2] Usman, Muhammad, and Usman Qamar. "Secure electronic medical records storage and sharing using blockchain technology." *Procedia Computer Science* 174 (2020): 321-327. https://doi.org/10.1016/j.procs.2020.06.093
[3] Ray, Shaan. "Blockchains versus traditional databases." *Online, last accessed* 7 (2018).
[4] Zainal, Salbiah, Rasimah Che Mohd Yusoff, Hafiza Abas, Suraya Yaacub, and Norziha Megat Zainuddin. "Review of design thinking approach in learning IoT programming." *International Journal of Advanced Research in Future Ready Learning and Education* 24, no. 1 (2021): 28-38.
[5] Guo, Huaqun, and Xingjie Yu. "A survey on blockchain technology and its security." *Blockchain: research and applications* 3, no. 2 (2022): 100067. https://doi.org/10.1016/j.bcra.2022.100067
[6] Leng, Jiewu, Shide Ye, Man Zhou, J. Leon Zhao, Qiang Liu, Wei Guo, Wei Cao, and Leijie Fu. "Blockchain-secured smart manufacturing in industry 4.0: A survey." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 51, no. 1 (2020): 237-252. https://doi.org/10.1109/TSMC.2020.3040789
[7] Wu, Yue, and Yingfeng Zhang. "An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing." *Advanced Engineering Informatics* 51 (2022): 101522. https://doi.org/10.1016/j.aei.2021.101522
[8] Imteaj, Ahmed, M. Hadi Amini, Panos M. Pardalos, Ahmed Imteaj, M. Hadi Amini, and Panos M. Pardalos. "Toward smart contract and consensus mechanisms of Blockchain." *Foundations of Blockchain: Theory and Applications* (2021): 15-28. https://doi.org/10.1007/978-3-030-75025-1_2
[9] Khan, Abid, Furqan Shahid, Carsten Maple, Awais Ahmad, and Gwanggil Jeon. "Toward smart manufacturing using spiral digital twin framework and twinchain." *IEEE Transactions on Industrial Informatics* 18, no. 2 (2020): 1359-1366. https://doi.org/10.1109/TII.2020.3047840
[10] Vaghani, Anjali, Keshav Sood, and Shui Yu. "Security and QoS issues in blockchain enabled next-generation smart logistic networks: A tutorial." *Blockchain: Research and Applications* 3, no. 3 (2022): 100082. https://doi.org/10.1016/j.bcra.2022.100082
[11] Mandolla, Claudio, Antonio Messeni Petruzzelli, Gianluca Percoco, and Andrea Urbinati. "Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry." *Computers in industry* 109 (2019): 134-152. https://doi.org/10.1016/j.compind.2019.04.011
[12] Moghaddam, Mohsen, Marissa N. Cadavid, C. Robert Kenley, and Abhijit V. Deshmukh. "Reference architectures for smart manufacturing: A critical review." *Journal of manufacturing systems* 49 (2018): 215-225. https://doi.org/10.1016/j.jmsy.2018.10.006
[13] Kobzan, Thomas, Alexander Biendarra, Sebastian Schriegel, Thomas Herbst, Thomas Müller, and Jürgen Jasperneite. "Utilizing blockchain technology in industrial manufacturing with the help of network simulation." In *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, pp. 152-159. IEEE, 2018. https://doi.org/10.1109/INDIN.2018.8472011
[14] Stanciu, Alexandru. "Blockchain based distributed control system for edge computing." In *2017 21st international conference on control systems and computer science (CSCS)*, pp. 667-671. IEEE, 2017. https://doi.org/10.1109/CSCS.2017.102
[15] Wan, Jiafu, Jiapeng Li, Muhammad Imran, and Di Li. "A blockchain-based solution for enhancing security and privacy in smart factory." *IEEE Transactions on Industrial Informatics* 15, no. 6 (2019): 3652-3660. https://doi.org/10.1109/TII.2019.2894573

[16] Li, Zhi, Ali Vatankhah Barenji, and George Q. Huang. "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform." *Robotics and computer-integrated manufacturing* 54 (2018): 133-144. https://doi.org/10.1016/j.rcim.2018.05.011

[17] Zhang, Yongping, Xiwei Xu, Ang Liu, Qinghua Lu, Lida Xu, and Fei Tao. "Blockchain-based trust mechanism for IoT-based smart manufacturing system." *IEEE Transactions on Computational Social Systems* 6, no. 6 (2019): 1386-1394. https://doi.org/10.1109/TCSS.2019.2918467

[18] Kapitonov, Aleksandr, Ivan Berman, Vitaly Bulatov, Sergey Lonshakov, and Aleksandr Krupenkin. "Robonomics based on blockchain as a principle of creating smart factories." In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pp. 78-85. IEEE, 2018. https://doi.org/10.1109/IoTSMS.2018.8554864

[19] Khattak, Muhammad Adil, Jun Keat Lee, Khairul Anwar Bapujee, Xin Hui Tan, Amirul Syafiq Othman, Afiq Danial Abd Rasid, Lailatul Fitriyah Ah

[20] Mengelkamp, Esther, Benedikt Notheisen, Carolin Beer, David Dauer, and Christof Weinhardt. "A blockchain-based smart grid: towards sustainable local energy markets." *Computer Science-Research and Development* 33 (2018): 207-214. https://doi.org/10.1007/s00450-017-0360-9

[21] Mollah, Muhammad Baqer, Jun Zhao, Dusit Niyato, Kwok-Yan Lam, Xin Zhang, Amer MYM Ghias, Leong Hai Koh, and Lei Yang. "Blockchain for future smart grid: A comprehensive survey." *IEEE Internet of Things Journal* 8, no. 1 (2020): 18-43. https://doi.org/10.1109/JIOT.2020.2993601