Robotics and Computer Integrated Manufacturing 54 (2018) 133–144

Contents lists available at ScienceDirect

Robotics and Computer Integrated Manufacturing

journal homepage: www.elsevier.com/locate/rcim

Full length Article

Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform

Zhi Li[a,b], Ali Vatankhah Barenji[a,*], George Q. Huang[b]

[a] Guangdong Provincial Key Laboratory of Computer Integrated Manufacturing System, School of Electromechanical Engineering, Guangdong University of Technology, Guangzhou 510006, China
[b] HKU-ZIRI Lab for Physical Internet, Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong, Hong Kong, China

ARTICLE INFO

Keywords:
Blockchain
Cloud manufacturing
Peer to peer network
Security and scalability

ABSTRACT

New emerging manufacturing paradigms such as cloud manufacturing, IoT enabled manufacturing and service-oriented manufacturing, have brought many advantages to the manufacturing industry and metamorphosis the industrial IT infrastructure. However, all existing paradigms still suffer from the main problem related to centralized industrial network and third part trust operation. In a nutshell, centralized networking has had issues with flexibility, efficiency, availability, and security. Therefore, the main aim of this paper is to present a distributed peer to peer network architecture that improves the security and scalability of the CMfg. The proposed architecture was developed based on blockchain technology, this facilitated the development of a distributed peer to peer network with high security, scalability and a well-structured cloud system. The proposed architecture which was named as the "BCmfg" is made up of five layers namely; resource layer, perception layer, manufacturing layer, infrastructure layer and application layer. In this paper, the concept of its architecture, secure data sharing, and typical characteristic are discussed and investigated as well as the key technologies required for the implementation of this proposed architecture is explained based on demonstrative case study. The proposed architecture is explained based on a case study which contains five service providers and 15 end users with considering 32 OnCloud services. For evaluation purpose, the qualitative and quantitative methods are utilized and the results show that the proposed methodology can bring more advantages to CMfg than the security and scalability.

1. Introduction

In the twentieth century, a collaboration between the Internet of Thing (IoT) and information technology, was identified as the key technological and developmental trends that are necessary for remolding the global manufacturing enterprises [1]. Recently, IoT has been fussed into the manufacturing industry and has brought about a new type of manufacturing such as the IoT enabled manufacturing and one step forward to cloud manufacturing (CMfg) [2]. With respect to a recent scientific paper [3], IoT enabled manufacturing is explained as an advanced principle in which typical production resources are converted into smart manufacturing objects that are able to sense, interconnect and interact with each other in order to automatically and adaptively carry out manufacturing logics that are used in the cloud-based system. Recently, researchers have forecast that IoT will have a trillion-dollar impact in the industrial and manufacturing sectors. Therefore, on-demand usage and sharing of resources can be made possible by the use of the IoT technology in the manufacturing industry. The IoT enabled manufacturing was developed based on modern manufacturing concepts under the Industrial 4.0 standard and incorporated advanced technologies such as the multi-agent system, cutting-edge technology, service-oriented paradigm and other advances in artificial intelligence, and as such, highly influenced the outperformance of the manufacturing industry. The key advantages of this new manufacturing paradigm are real-time data gathering and data sharing amongst the enterprises and consumers [4].

In this way, the IoT connects more industrial equipment and parts together which leads to more data's generation; as a result, more comprehensive work data will help to ease the process of decision making within the factory. However, by expanding the boundaries of IoT and information technology-based manufacturing, an increase in connectivity will occur as well as a higher level of complexity in the computing infrastructure. As a result, many researchers have proposed CMfg as a measure to be used to cover existing drawbacks of manufacturing, this includes the complexity of computing infrastructure and service sharing by taking advantage of cloud computing, service-

* Corresponding author.
E-mail address: ali.vatankhah.b@gdut.edu.cn (A.V. Barenji).

https://doi.org/10.1016/j.rcim.2018.05.011
Received 20 January 2018; Received in revised form 2 May 2018; Accepted 29 May 2018
0736-5845/

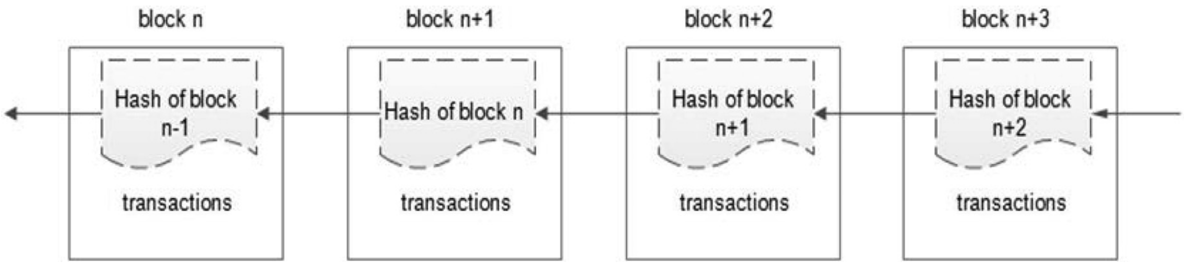

Fig. 1. Blockchain and hash of block.

oriented system and the IoT [5]. CMfg is a new service-oriented manufacturing mode that utilizes the internet and service platform to arrange manufacturing resource as well as provide service according to the end users demand [6]. Based on this definition, CMfg is a manufacturing paradigm that utilizes cloud computing and IoT to transfer manufacturing resources into the cloud environment, aiming to provide everything as a service. Therefore, on-demand service provision is a main advantage of CMfg [7]. However, this paradigm like the existing solutions uses a centralized network for communication purpose and third parts for managing. As a result, centralized network not only reduced the productivity of the CMfg but also bring flaws include scalability and a broken communication model and thus, opens the door for more vulnerabilities in the system such as cyber-attack [8]. On the other hand, in the manufacturing industry some of the physical devices are located in unsecured environments and as such, can easily be tampered with by hackers [9]. Also, data travels over a wireless network to the centralized based database which could also be a loophole in the architecture [10]. Moreover, the existing HPC and cloud-based manufacturing data sharing systems are very complex [11]; so existing HPC isn't feasible for the small and medium-size company. Hence, centralized based system support small-scale IoT networks in the manufacturing enterprise, which lack of answer to the emergent needs of an enormous IoT in the manufacturing ecosystems of tomorrow [12].

Therefore, in order to deal with these challenges, we proposed a decentralized network platfrom for a CMfg based on the blockchain technology (BC) which could be considered as the next generation of intelligent manufacturing. BC is a digital, decentralized ledger or in a simple way is peer to peer network. The concept of BC was proposed by Satoshi Nakamoto in 2008 [13]. This technology developed a distributed digital ledger of transactions that was shared amongst the nodes of a network instead of being stored on a central server. BC is capable of providing an effective solution to new manufacturing paradigms such as CMfg system, due to its abilities as follow [14,15]; A) BC stores data in the shared database as well as in the distributed and fault-tolerant database; based on these capabilities, participants in the manufacturing system are able to nullify their adversaries by harnessing the computational capabilities of the honest nodes. This makes the information that is exchanged between the parties to be resilient to foreign manipulation. B) BC is a robust architecture ward off attacks due to its decentralized network. C) BC relies on a public key infrastructure which allows the contents to be encrypted in such a way that is expensive to crack. Therefore, the proposed platform can be provided a secure and innovative data sharing solution by utilizing a decentralized and permission BC for CMfg which is accomplished by using a channel formation schema, enhanced service provision, systematic encryption and data sharing system with membership service support. The proposed methodology is developed based on the recent advancement in CMfg and fully supported to achieve a scalable, flexible and distributed network, in order to avoid the problems associated with a centralized framework. Furthermore, the proposed methodology can provide standards and protocols for implementing the new manufacturing approaches as well as resolves security and identity issues based on its advanced data cryptographic algorithms.

Therefore, this paper contributed to the following aspects: Firstly, a trusted and robust distributed network framework for whole product life cycle (PLC) was proposed; this robust distributed network framework would be used for future manufacturing systems, providing the ability for self-trust, data integrity audit and data resilience. Secondly, existing drawbacks on the new manufacturing paradigms and data sharing were highlighted. And thirdly, a secure data sharing by considering big-data in CMfg based on the proposed methodology explained and a key technology for implementation of the proposed system was defined.

In this paper, the sections are organized as follows: In Section 2, works related to the blockchain, IoT enabled manufacturing and cloud manufacturing will be discussed. Section 3 presents the proposed methodology and key characteristic of the system. While Section 4 presents the key implementation of the proposed system and example-based implementation. Section 5 focus on the evaluation of proposed methodology and last section conclusion and discussion.

2. Related work

2.1. Blockchain

A BC is a distributed data structure (ledger) which can hold any information (transaction, record and etc.) that is simulated and shared between the memberships of a network. BC created new types secure and trustable peer to peer communication platform. In the BC, each block is identified by its cryptographic hash and connected with another block for making chain [16]. Therefore, each block connected with other block based on hash information, which improves the security of BC [14]. This mechanism is illustrated in Fig. 1. As a matter of fact, any membership with access to the BC Network (BCN), block-linked list of blocks can read it and Figure out what is the world state of the data that is being exchanged on the network. Therefore, a block in the chain carries a list of transactions and a hash to the previous block [17].

Three types of BCN exist namely public BC, consortium BC and private BC which are explained and follow:

- Public BC: is a BCN that anyone in the world can access, and send transactions to network expect to see them included if they are valid, and anyone in the world can participate in the consensus process. The main disadvantages of public BC are public but no means isn't secure, it is secure by the power of cryptography. The public blockchain is considered to be a fully decentralized blockchain. Bitcoin is an example for public BC.
- Consortium BC: in this type preselected a set of nodes control the consensus process in the system. So consortium BC is partly private. For an instant, ten manufacturing industries created one BCN for communication between members, each of members must control a node and for block validation at last five members must be validated of that block. The right to read the BC may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API.
- Private BC: is BCN where write authorizations are kept centralized to one organization. Read authorizations may be public or limited to

a random level. Such as application auditing, database management etc.

Recently, many researchers have tried to develop BC based industrial application in order to take advantages of this technology. For example, Li et al. [18] introduced across enterprises knowledge and services exchange framework based on BC, they used BCN for exchanging knowledge between enterprise via edge computing. Sikorski et al. [19] proposed toward machine to machine communication via blockchain technology and used proof of concept for illustration of implementation in the electrical grid system. Tian [20] has proposed an agri-food supply chain traceability system based on the BC. The system used the radio-frequency identification (RFID) to keep track of the agri-food in the supply chain and adopted the BC in order to ensure that the data utilized is correct and reliable. This system is capable of preventing fraud, corruption, tampering and the falsification of information. Oliveir et al. [21] introduced a novel platform for decentralized logistics based on the BC and IoT. BC and IoT were used as basic building blocks, which were able to create a trusted and integrated platform for managing logistics operations in a fully decentralized way. Liang et al. [15] used BC for integrating data sharing and collaboration amongst healthcare application, they proposed a user-centric health data sharing solution by utilizing a decentralized and permission BC to protect privacy by utilizing a channel formation scheme as well as an enhanced identity management system with membership service. Therefore BC has the advantage of security, irreversibility, distributability, transparency, and accuracy [16]. This technology is utilized mining and trading of bitcoin by constructing the data structure and encrypting the transmission of transaction information [22]. The data block in the system is maintained by the nodes with the aid of the maintenance function. There are no centralized management agencies, and the rights and obligations of each node are equal. This technology is suitable for the storage of data that requires identification and verification. It enables participants to establish a decentralized consensus on the sequence of events as well as in the current status of the transaction [23]. The advantage of decentralization means that no central authority is required, and also, the trust between the parties concerned are still maintained. It enables the exchange of data autonomously and securely in the untrusted environment [24]. Once the information is verified and added to the BC, it will be permanently stored. The openness and unchangeability of the BC ensure that high transparency, stability, and reliability are feasible. Moreover, it offers liquidity, more accurate record-keeping, and transparency of ownership [25].

2.2. IoT and CMfg

The idea of IoT was developed in this book ``The Road Ahead" that was printed in 1995. Due to lack of high tech information and equipment such as high-speed network, sensor and smart thing, the IoT wasn't given proper attention at that time. However, with the fast development of RFID technology in the 21st century, IoT has been given much more attention. Recently, it has been shown that IoT was capable of providing a promising opportunity to developed and make a new type of industrial systems based on the application of RFID, wireless sensor network and cloud computing [26]. Therefore, it has attracted much attention both from the industrial and academic spectrum, and many technical studies have been conducted in this field due to the many application of this technology. For example, IoT enabled smart factory visibility and traceability system by using Laser scanners was developed [27]. Yang et al. [4] proposed IoT enabled dynamic service selection across multiple manufacturing clouds, the proposed method used IoT's real-time sensing ability on service execution, Big data's knowledge extraction ability on services in manufacturing clouds, and event-driven dynamic service selection optimization to deal with disturbances from the users and service market as well as to continuously adjust service selection to be more effective and efficient. RFID enabled multi-agent based control system for flexible manufacturing system was presented [28,29] and authors used RFID technology to share data between the system level. Recently [30] developed an IoT based tracking and tracing platform for prepackaged food supply chain which used a cloud-based storage for the data store.

Nowadays, IoT is key components of new manufacturing model known as the cloud manufacturing. CMfg is defined as a new paradigm which is developed and model based on existing advanced manufacturing technology (e.g., application service provider, manufacturing grid, additive manufacturing and etc.) with considering and supporting cloud computing, IoT and service-oriented technologies. The main aim of this paradigm is shifting manufacturing resources and capabilities to services and define manufacturing service which managed and operated in an intelligent and unified way, in order to arrive full allocation and socializing of manufacturing resources and capabilities [27]. CMfg has been of prime focus for a great deal of research interest and suggested applications in recent years i.e. by both the industrial and academic communities. And so a vast number of papers were published in the different sections [31] which include architecture, platform, framework, model, and application. in this respect, Bo-Hu et al. [32] defined the concepts of CMfg and identify between CMfg and grid manufacturing. Xu [11] presented four layer based architecture for CMfg by shifting cloud computing to CMfg. Tao et al. [33] defined a typical characteristic of CMfg and introduced key characteristic of this IT structure in the manufacturing industry. Lihui and Vincent [34] developed the application of cloud-based distributed process planning by considering multi-task machining. Ocatavian et al. [35] focused on shop level and presented the vMES virtualization layer for manufacturing executing systems. Vatankhah [36] design cloud-based manufacturing execution system for flexible manufacturing system via model driven architecture.

CMfg brings many advantages to the manufacturing industry [31,37,38]. However, the centralized network was used for the implementation of this architecture in the industrial environment. Centralized network suffers from flexibility, efficiency, availability, security, and scalability. Recently, many researchers have highlighted that distributed network is a great solution for improving the centralized network in the manufacturing system, for example Skulj et al. [39] developed decentralized network architecture for CMfg, based on autonomous work systems for use as service providers. But the proposed architecture suffer from standardization and implementation protocol. Therefore, there are huge academic gaps in this field for overcome existing gaps in the CMfg. Only some research papers and academic website have been able to recognize the advantage of this distributed network for the industrial application. Also the literature referred by the authors indicate that there are some valuable efforts being made on the design and development of the distributed network and data sharing system which is based on BC. Therefore, in this paper, we introduced a methodology for trustable and secure distributed network and service sharing for manufacturing industry based on the BC and CMfg, which was named as the BCmfg.

3. Proposed architecture for BCmfg

We present an architecture based on the BC and CMfg, for a secure and distributed service sharing, and the trustable connection between end users and service providers. This architecture is depicted in Fig. 2. BCmfg consists of five main layers which are the resource layer, perception layer, manufacturing service provider layer, infrastructure layer, and application layer. Each layer is explained as follow;

1. Resource layer: This is the physical manufacturing resource as well as the capabilities of the manufacturing layer. The main components of this layer are divided into two parts which are: the hardware resources and software resources. Hardware resources are made up of machines, robots and the material handling system. And, software

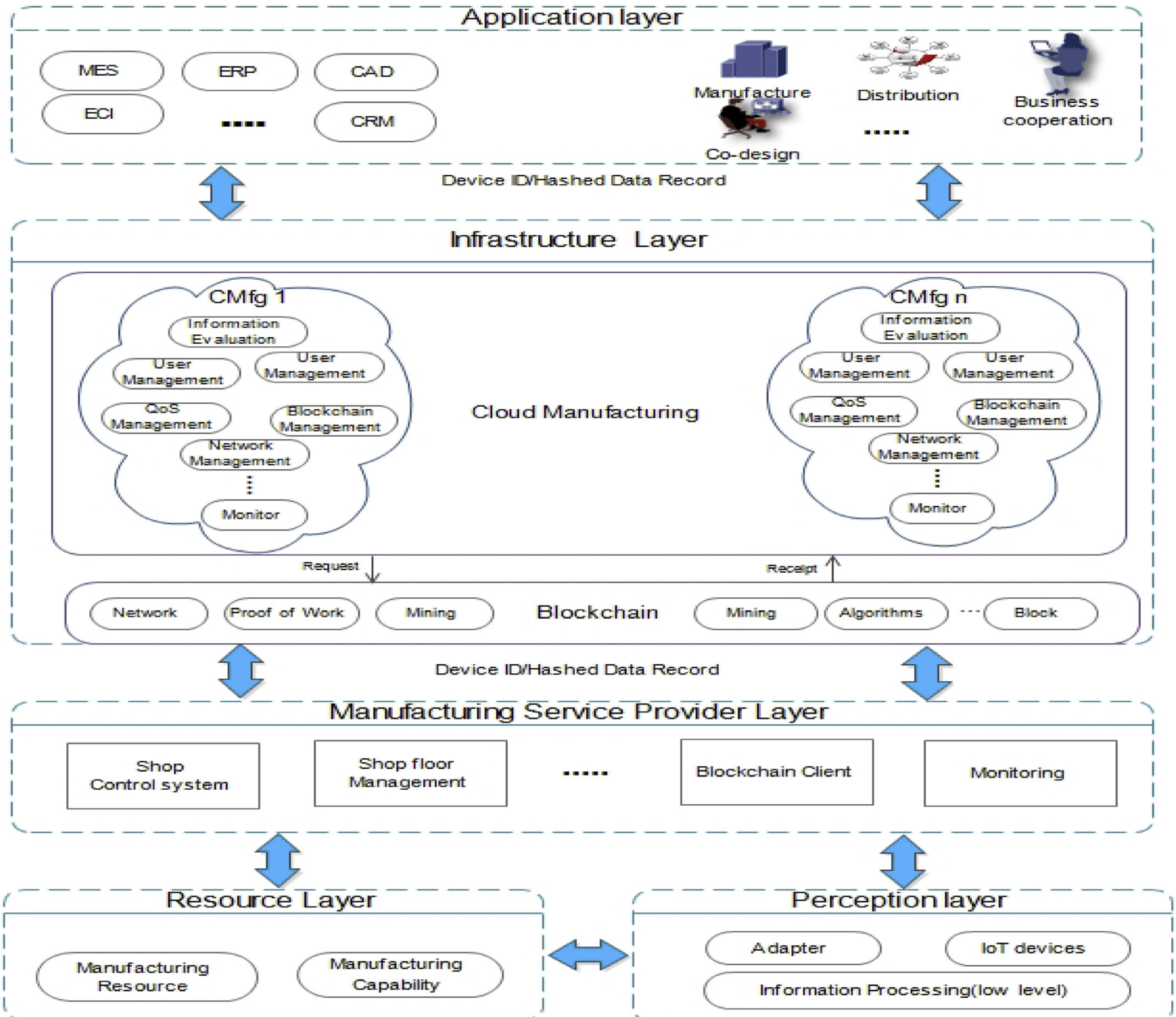

Fig. 2. Proposed architecture for BCmfg.

resources are made up of computational models, low-level control software, data gathering software etc. The manufacturing capabilities are formed with resources, people (or organization) and knowledge, which reflects its ability to complete a manufacturing task or experiment supported by the related manufacturing resources and knowledge [40]. The main purpose of this layer is to provide manufacturing as a service for end users for example machining as a service.

2. Perception layer: This layer is responsible for sensing the physical manufacturing resources and virtualization and so, it follows the concept of cloud manufacturing [41]. The main purpose of this layer is to create a connection within the network and process the related data and information by using the IoT to realize the overall connection of various manufacturing resources and capabilities.
3. Manufacturing service provider layer (MSPL): this layer not only responsible for service providing (catalyzing, definition and etc.) but also has two main responsibility: Firstly, it is responsible for changing data type to hash and storing on the generated block. Secondly, it is responsible to establish a connection with the BCN, which exists in the subsequent layer (i.e. the infrastructure layer). A key component of this layer is the blockchain client which is responsible for connecting to the network and monitoring the note and block. Possibility to make a communication with different service providers and end users via indirect manner and distributed system is started from this layer which is the main difference between CMfg and BCmfg. In the proposed architecture blockchain client establish a peer to peer communication with other parts and, started to change the format of data to hash data and encapsulate hash data to created block on the BCN for broadcasting on the network. For a better understanding of this section, the connection of all parts in the proposed platform is illustrated via sequence diagram in Fig. 3. In this Figure machine level sends data to perception layer via IoT and after preprocess and generation of capability by perception layer, data send to MSPL, based on this information existing service on the MSPL modify and blockchain client developed a connection between cloud provider and manufacturing service provider for sending modify service to the cloud. This is long time connection which is generated by BCN by considering private key and membership verification. Communication between resource layer and perception layer explained in the detail in next section.

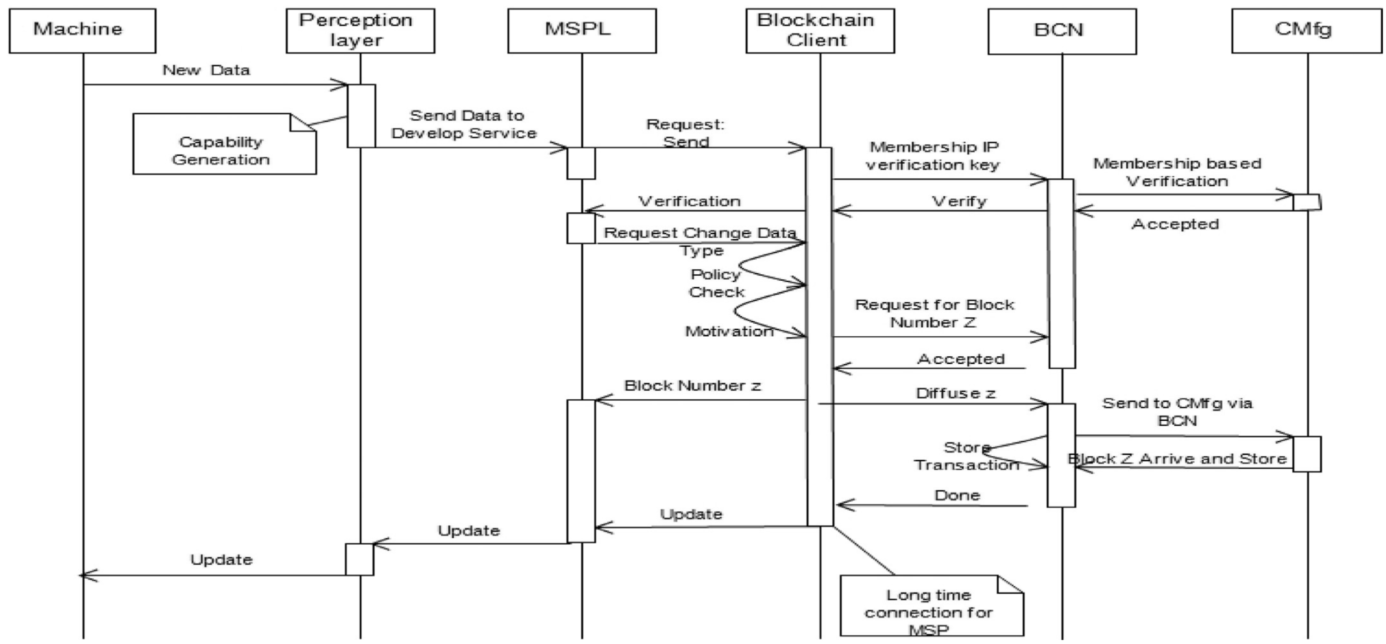

Fig. 3. Communication of layers based on blockchain client.

4. Infrastructure layer: It is responsible for providing the infrastructure that supports the different layers, this consists of two parts which are the cloud manufacturing and BCN. The cloud manufacturing is responsible for providing core functions and service for the operation of the manufacturing system and customers, which includes knowledge management, cloud data storage and cloud services [4]. This part can be consist of more than one CMfg providers, this is one of the main advantages of the proposed platform and illustrated the ability to collaborate. On the other hand, the BCN which is developed based consortium BC is responsible for developed a peer to peer network between the end users and service providers as well as to develop a secure collaboration platform between cloud infrastructure providers. It is consist of two type nodes, controller/verification nodes and request/response nodes. Therefore in the proposed platform CMfg providers play as controller node and end user play as request node on the system, so more than one CMfg collaborate and cooperate together for developing and managing BCN without considering third part and each CMfg responsible to membership verification and network maintenance which is improve the security of the platform and also responsible for own data sharing and storing which is reduced the complexity of the whole system.
5. Application layer: It is responsible for providing different specific application interfaces and related end-interaction equipment. The applications can be categorized into two parts i.e. the PLC application and the end user application. Both are web applications that use BCN and cloud environment for service provision. The main duty of web application creates a wallet for each user, for example end user create wallet via a web application, and connected to BCN based on the wallet number for a sending request or using services. In the case of service request connection is a short time, because short time connection improves the security and latency of the BCN.

In the proposed architecture, blockchain client exists in different layers; within the layers, the blockchain clients take up the responsibility of encapsulating data to generated blocks and registering the key for each block in the BCN. In the next section, this concept is explained in more details. Moreover, several specific features and characteristic of the proposed framework including on-demand services and secure data sharing model, are explained in the following section.

3.1. Typical characteristic of BCmfg

3.1.1. On-demand secure services

BCmfg was proposed based on the CMfg which is on-demand IT service (storage, network and etc.) provider for PLC. The main advantages of the proposed system with comparing by CMfg is the use of the BCN for data sharing and service exchange in the whole life cycle, this function provide on-demand secure service for the whole system by taking into account that in the BCN originality of data is defined in a deterministic way and used symmetric encryption for data sharing on the network [24]. This is done so as to know which user sent the data to the system and where the user is, and confidentiality of network was guaranteed by encryption process. Therefore, the proposed system provides a secured platform for on-demand secure service.

3.1.2. Supports secure data exchange

Big-data is the foundation of CMfg [42]. Due to the usage of the IoT and computer-based machines in the manufacturing system, there has been a large number of data generated in the CMfg. These data can be sensed and collected over the internet to be processed in the cloud. Data exchange plays a crucial role of service exchange in the CMfg; in this respect, secured data has become one of the important issues that need to be taken care of [43]. As mentioned previously, data sharing in the existing system suffers from security and scalability issues which lack in a centralized system. A secured data sharing process in the PLC components is illustrated in Fig. 4. This was developed based on the BCN and big-data on new manufacturing paradigms (CMfg, IoT enabled manufacturing) [44].

The process is mainly composed of eight parts, which are the Data source (DS), Data Acquisition (DA), Data preprocessing (DP), Cloud database (CD), Data analysis and mining (DAM), decision data (DD), Cloud-based application (CBA) and blockchain network (BCN).

In a simple scenario, DS sends data to the DP via an IoT device which is used a machine to machine (M2M) connection; after being processed in the DP, the final hash data (HD) is created with the appropriate key and block for sharing in the BCN via blockchain client which is located on MSPL. The generated block contain HD and send it to the cloud environment via a BCN. Always first note which verifies all

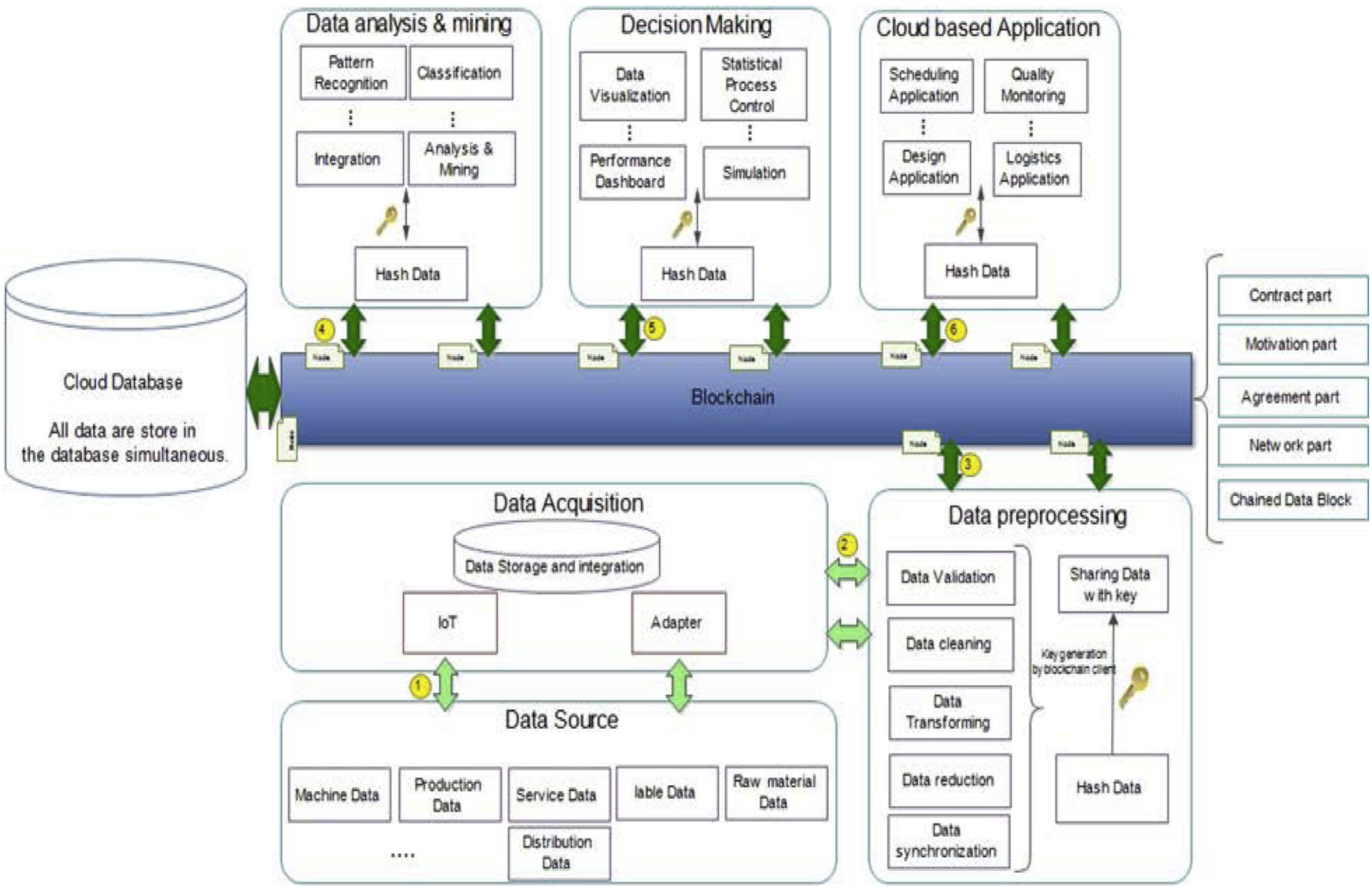

Fig. 4. Schematically explanation of data sharing in the BCN by considering all parts of the big-data.

Table 1
Components of blockchain network.

Part	Responsibility and purpose	Main modules
CDB	It is responsible for providing the chained data blocks in the system with the related techniques, which is used for transferring data to HD.	Hash algorithms, asymmetric encryption and merkle tree and time stamping.
NP	It specifies the mechanisms of distributed networking, represents the data forwarding peer to peer communication and verification of the communication. It is responsible for verifying the legality of the broadcasted message as well as the management of the peer connection.	Data forwarding, peer management, and data verification.
AP	Also called the consensus or handshake part. It provides decentralized communication within the network and helps to develop trust between the unknown users in the communication environment.	Proof of Work (PoW) based algorithm, Proof of Stake, Delegated Proof of Stake algorithm and Proof of Movement algorithm.
MP	It is responsible for making a motivation on the network by generating a reward for new block i.e. appreciated the effort for data verification.	Crypto data.
CP	It is responsible for serving as activators for the static data by using various scripts, algorithms and smart contracts.	Script and algorithms.

blocks in the BCN is a CBA, which is responsible for saving all HD and transaction on the CD. After that, other parts based on the note information and block information can have access to HD. All other parts use a similar mannerism and process for sending data to the system. The main part of this system is the BCN and how the network acts as a distributed network for the system. As illustrated in Fig. 4, BC consist of five parts, namely chained data block (CDB), network part (NP), agreement part (AP), motivation part (MP) and contact part (CP). Table 1 summarizes the purpose and components of BCN.

In the BCN, each note after winning the consensus competition, created a new block and set all related HD on the block based on the Merkle tree with time stamps, indicating the creation time of the block. The developed block by blockchain client consists of two parts i.e. the header which contains Meta information and a body part which contain all the verified data that is stored in form of a hash; this is accomplished by using a specific algorithm such as the SHA256 [45]. The header part contains the Merkle tree and its root. After the generation of the block, it's broadcast to the BCN where all the nodes keep searching. Each node can verify a block on the BCN according to the defined specification (key), if the key is invalid, it is sent to other neighboring nodes for data sharing. This means that blocks undergo verification from all of the nodes. The nodes use a mutual trust between the nodes which creates a form advantage by promoting all the decentralized nodes reaching consensus on the data's validity. This mutual trust between the nodes is developed by many types of consensus algorithm which is located on the AP. After creating the new block, the motivation of network is done by MP; this improves the data verification process on the network. In the last part, CP packages various scripts, algorithms, and smart contracts, which serve as important activators to the block in the blockchain as play the key on each block. Blocks and notes used the smart

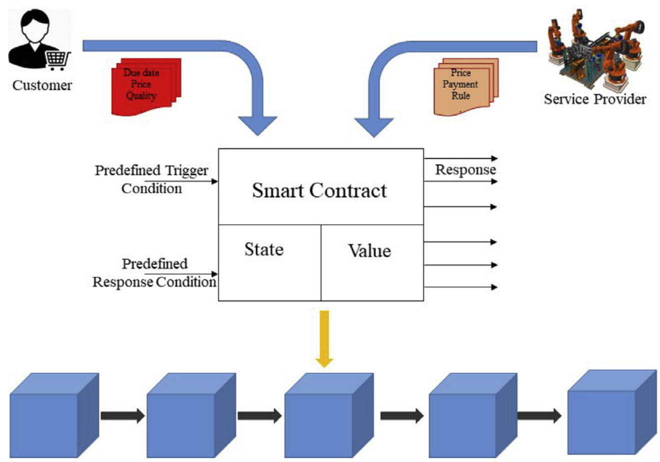

Fig. 5. Smart contact in the blockchain.

contact for verification and access for HD on the block, Fig. 5 illustrates the smart contacts on the chains of blocks through the BCN.

Smart contracts have gained prominence due to their use on distributed ledger infrastructures based on BC, which have overcome the need for trusted third parties to implement and take responsibility for automated transactions. Therefore, in the proposed platform smart contracts act as agreements between the end users and the service providers to provide on-demand manufacturing services and encapsulated on the block. A smart contract is an executable software module that is developed by the blockchain owners, installed into the BCN itself and then enforced when pre-defined rules are met [46]. When smart contracts are run on a distributed ledger, the execution and recording of transactions are provided by a cryptographically enabled decentralized infrastructure. Therefore smart contracts in BC are typically programmed in a procedural language. For example on the platform Ethereum, developers can encode smart contracts in a procedural language called Solidity [47]. In the proposed platform the rules of the smart contacts are developed based on agreement provided by end users and service providers these rules can contain due date, quality payment method and etc. in the simple explanation, when end user request service from service provider, also provided some information regarding due data, quality and payment method, in this time service provider negotiated with end user for decide about this rules and make it this rules as smart contact and deploy on the BCN via block.

By considering proposed data sharing mechanics and smart contact, the developed architecture can provide a secure transaction ledger database through a decentralized network. It has the potential to reduce the operational costs and frictions, create transaction records that are secure and immutable, enable transparent ledgers with nearly instantaneous updates and open up new opportunities for growth.

3.2. service execution

Once the end users connecting to the BCN and used services, services will be running via hypervisor mechanism. There are two types of service modes exit during the execution, OnCloud (OC) service and OffCloud (OFFC) service. OC service is completely under the control of the cloud platform which provided by the CMfg and used BCN for connection with end users. These services mainly involve computing resources. OFFC service means that some manufacturing task should be performed by humans or physical resources outside the cloud platform, which is located in the resource layer. In the case of service execution at the proposed platform end user need to create wallet via a web application and send a service request to the BCmfg this request and service execution illustrated in Fig. 6. End users used specific wallet number which is generated by BCN for requesting service, after creating a wallet, end user provided detail information regarding request service, therefore block is created based on this information and broadcasted on the BCN. The first rules of the smart contact between end user and service provider developed in this step by considering end user information regarding services such as quality and due date. For improving the security of the platform after generating a black used symmetric encryption method for data transferring between the end user and service provider. Symmetric encryption is a form of computerized cryptography utilized a singular encryption key to guise an electronic message [48]. For arriving this goal Fig. 6 shown how encryption and decryption is used for data in the proposed platform. also connection between end user and service provider is short time connection which improves the latency of the proposed system, it means that after sending request to end user via BCN, automatically end user disconnected until the service provider accepted the request and send it service to the end user, but end user can monitor its request as guest on the system but cannot change or add new data to system.

In the case of providing services to end users process is similar, but in this case service provider after accepting the request and updating smart contact with modify rules used the longtime connection, therefore membership verification is a need for improving the security of the network. It means that for providing service need to verify this service with others service providers.

4. Key implementation and case study

To evaluate the concept of the BCmfg and its related technology for implementation and verification, in this paragraph firstly we focused on developing BCN after that we explained our case study with detail implementation.

Fig. 7 shows the key component of the BCN which follows the consortium BC. The main components of the BCN are a regulator, BC developer, participant, operator, traditional data source, CD, certificate authority and old processing platform. All these components can be explained as follow:

- The regulator performs oversight for the BCN and usually is granted permission to see all the transactions that occur within the network.
- The BC developer is responsible for creating applications and solutions, which include smart contacts, transaction etc.
- The certificate authority creates security certificates and provides privacy and cryptography within the network.
- The participant is made up of two parts i.e. the end user and industrial participants; the end user participant users operate in a business network, while the industrial participant users operate in the industrial network. However, both networks interact with the BCN via an interface agent.
- The operator is responsible for defining, creating, managing, and monitoring the BCN. Each business in the network has a BCN operator.
- The traditional data source is an existing data system which may provide data to influence the behavior of smart contracts.
- The old operation platform is an existing computer system which may be used by the BCN to augment processing. This system may also need to initiate requests into the BC.

As we mention before this research paper as one of the first research paper in the field of manufacturing system and blockchain technology, therefore in this part we are going to implemented proposed system in the demonstrative scenario which is consist of five industries that are provided manufacturing as a service and 15 end users with considering 32 OC services. Manufacturing service providers can use existing methods for the perception of manufacturing resources and access to computational resources [49]. As simple scenario we consider each manufacturing service provider can provide three types of service namely; machining as a service, technical issue as a service and welding as a service also each customer can send one request to the system at

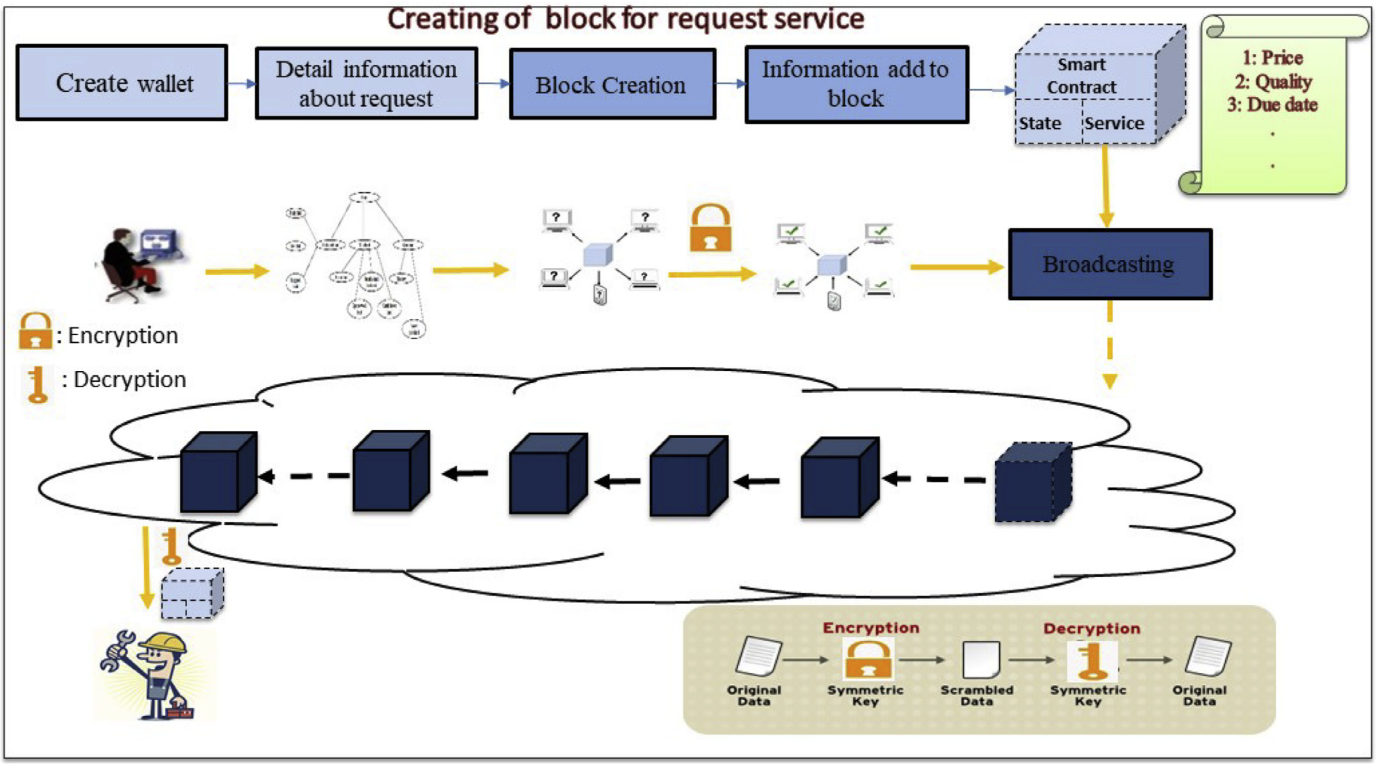

Fig. 6. End user and service provider connection.

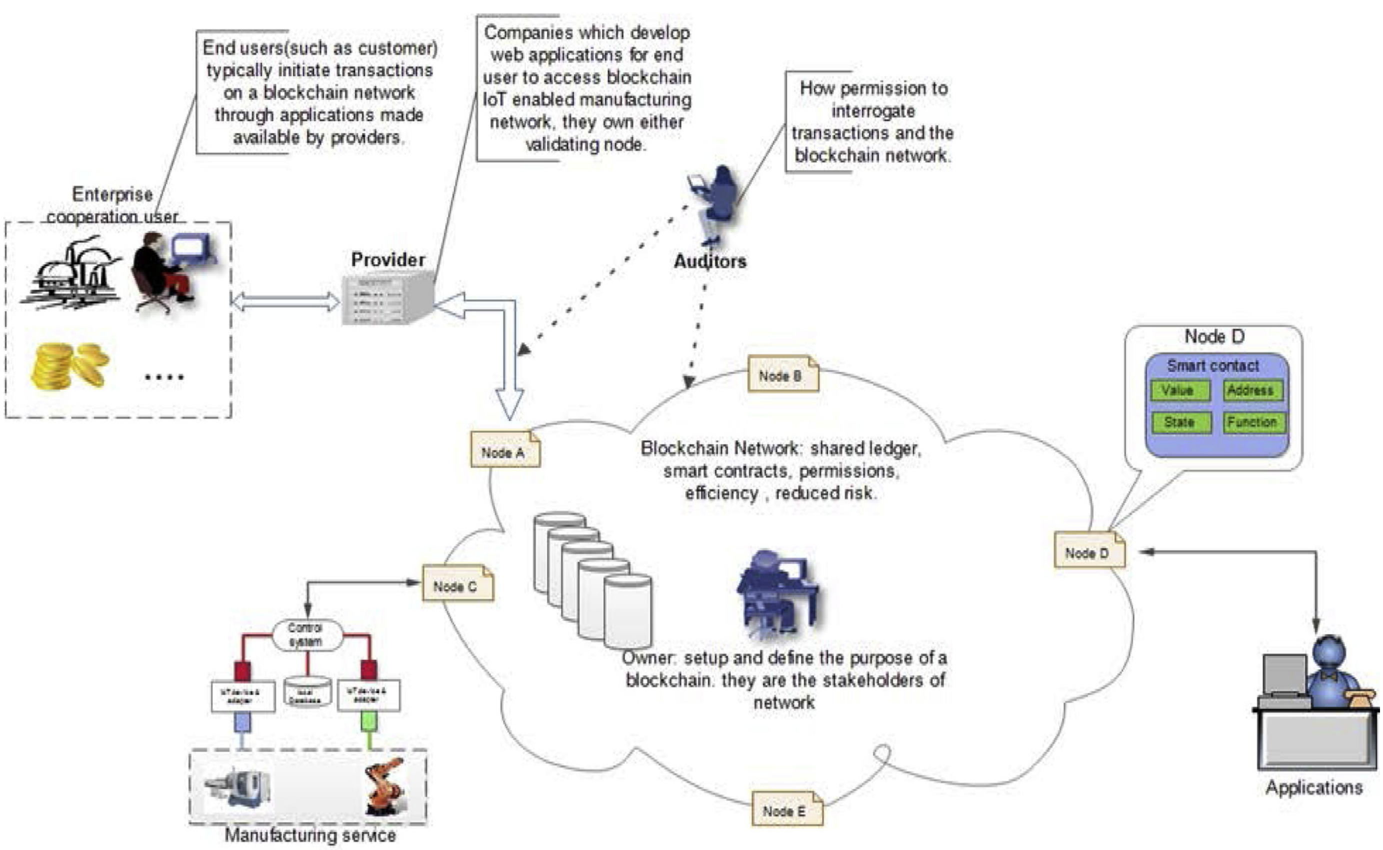

Fig. 7. Key components of BCN and proposed system for implementation.

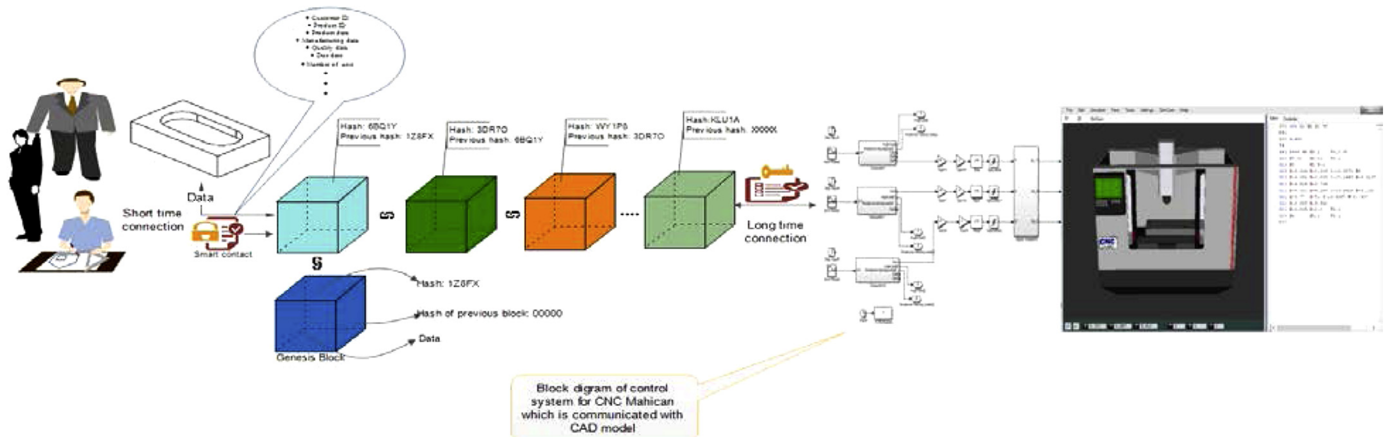

Fig. 8. Schematic explanation of case study with considering blocks in the chain.

Table 2
Manufacturing service providers.

Service providers	Location	Services	Capability	Types	Numbers of services
A	Guangzhou	Machining	3-Axis CNC milling	Machining and technical issue	3
B	Shenzhen	Machining & welding	3-Axis CNC milling, turning machine, and Arc welding machine	Welding, machining and technical issue	5
C	Foshan	Machining	Multi-Axis CNC machine. Traditional machining	Machining and technical issue	10
D	Guangzhou	Machining,welding and technical issue	3-Axis CNC milling and turning machine. Arc welding machine. Technician	Machining, welding and expert human service	15
E	Foshan	Machining, and technical issue	3-Axis CNC machine and machine tools	Machining and technical issue	5

the same time, Fig. 8 illustrated case study by considering BCN, customers and service providers. Table 2 explained manufacturing service providers in the detail by highlighting existing services on each industry. As an example a customer wants to produce a part which is needed to have an ellipse in the middle of the cube that can be done with CNC milling machine (Fig. 8) which need two type services first one technical issue as s service such as “G Code” and machining as a service. The end user publishes the information related to part for service providers via BCN based on the function as a publishing board. The service providers reads the offers, analyses them and send an offer to the customer (product cost and due date). The customer reads the offers than decided to select service (minimum cost, due date and quality). When customer accepted an offer from the service provider, it is executed as an atomic exchange. For realistic implementation and consider detail information from manufacturing service providers such as machine level and software level. We virtualized each services (machining service) via Matlab Simulink [50], with advanced of Sim Scape Toolbox which is allowed us to use the complete computer aided design (CAD) model of the geometry of the machine tool, for this proposed we used Solid Work software for developed CAD model of machine tool (Fig. 8) and control system of machine tools is developed for controlling of CAD models (block diagram) [51]. Therefore manufacturing service providers virtualized in the both physical and software level. After virtualization of the existing manufacturing service providers we used VMware [52] for developed cloud environment and encapsulation of developed services on the cloud then communication between the encapsulated services on cloud created based on blockchain client which isn't short time communication, it is long time communication by considering private key and membership approval. Fig. 8 shown the case study by considering BCN and virtualization of service providers and end users.

Therefore, the proposed architecture was implemented on Dual Booting Fedora 25 and Windows 10 with UEFL firmware virtual machine and VMware is used for developed cloud providers. We used

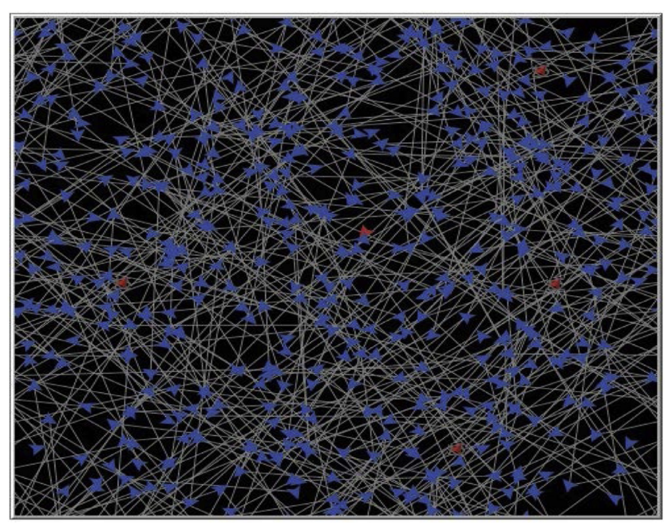

Fig. 9. Schematic of Blockchain Network with five controller nodes and 1000 request nodes.

MultiChain [53] to build a distributed BCN with five controller/verification nodes and 1000 request/response nodes, the schematic representation of this network is depicted in Fig. 9, red color nodes are controller and blue color nodes are request. All data transfers to a cloud environment for interpretation and analysis of the posted offers. All code for developing BCN and geniuses block is done by Python 3.6 and Solidity language used for developed simple smart contact between end users and service providers. Also Javascript used for developed web interface for users.

5. Results and discussion

For evaluation and verification of proposed architecture we firstly focused on qualitative evaluation method after that we provided security evaluation and highlighted the requirements of security evaluation on the proposed system, and how our proposed system provided these requirements. Then quantitative evaluation based on BCN was provided for illustrated capability of developed network.

5.1. Platform evaluation

In this section based on the prototype implementation of proposed architecture, we presented a series of figures and try to explain workflow of the proposed platform via a case study. The first step is a login to the system each end user must sing up and developed a valid wallet with 2-step verification (2FA) which is acts as an extra layer of security for wallet [54]. After registration and getting wallet number, customer can publish request on the system, based on the case study end user prepare data and published request for production of part via manufacturing service providers, after publishing and considering smart contract, manufacturing service providers can fine new request for production of part in the system, after decoding product data such as manufacturing data, quality data, due date and etc. Each manufacturing service provider send offer based on its capability to system with new production cost, due date and payment method, by considering that manufacturing service providers used private key technology for sending offers to end users so customers just can be accessed for this offer, therefore customer selected the best offer and send acceptance to selected manufacturing service provider. In this system, smart contact is simple code regarding payment between customers and manufacturing service provider. Fig. 10 shown this process and interface of system for end user and manufacturing service provider. As illustrated in Fig. 10 each user have specific wallet number.

For a better understanding of system Fig. 11 illustrated the detail information of transaction for end user request and accepted offers by manufacturing service provider. End user accepted the offer of manufacturing service provider C because the production cost is less than others service providers.

In the Fig. 11 can find that wallet number of end user send it acceptance to wallet number manufacturing service provider A. Also the gas price is considered as tax and maintenance fee of the whole platform, each end user needs to pay regarding of services.

5.2. Security evaluation

There are three main security requirements that need to be addressed by our proposed architecture, namely: confidentiality, integrity and availability [55]. These three equipment named as CIA trial is a model to guide policies for information security within a system. In the following section we exampled how our proposed platform can cope with these requirements.

- Confidentiality: it is a set of rules for make sure that only the authorized user is able to used service in the network, for arriving confidentiality in the proposed architecture this rules guaranties by using symmetric encryption. As illustrated in Fig. 6 data transferring between the end user and service providers done based on encryption and decryption. In this process encryption is the process of transforming data so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again.
- Integrity: Make sure that the sent data such as end user request is received at the destination without any change. In the proposed architecture hash mechanism between blocks is guarantee the

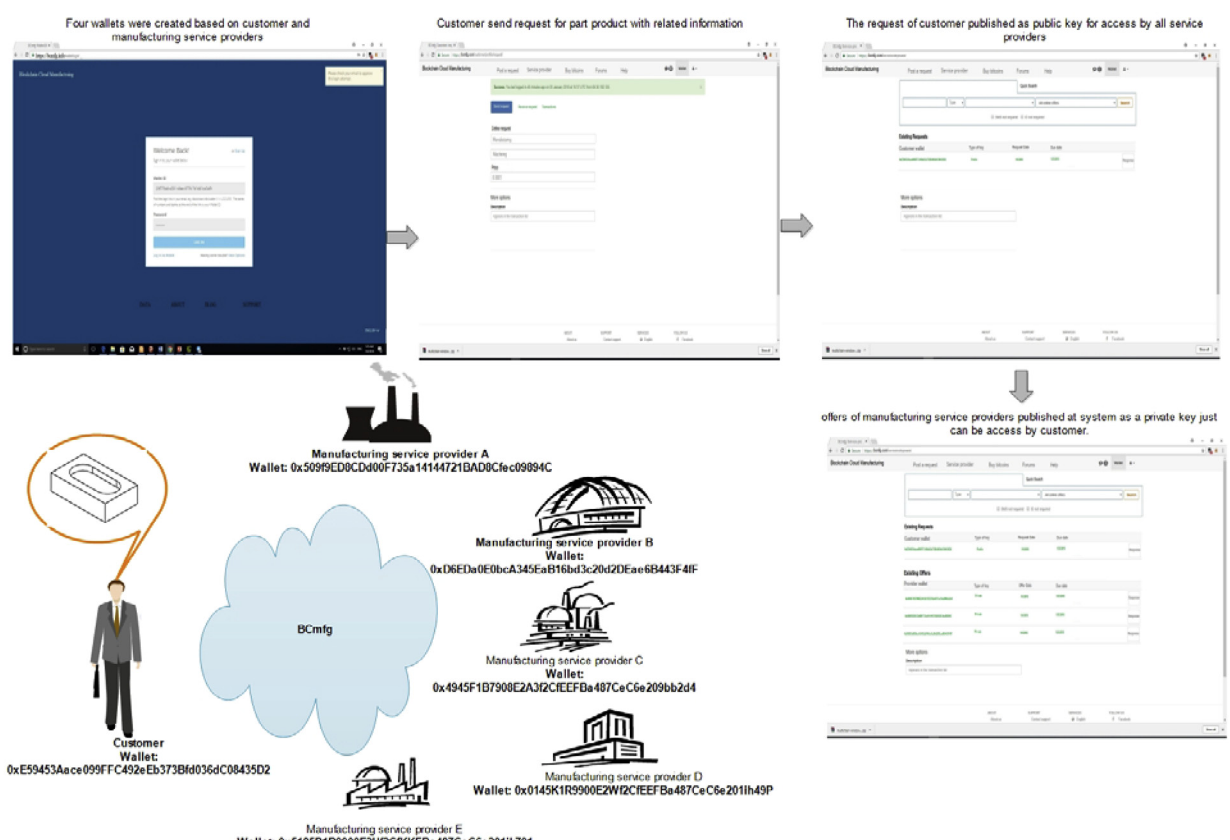

Fig. 10. Workflow and interface of proposed system, it is offer web based interface for users and have many type of user interface for example interface for customer with manufacturing service provider is different.

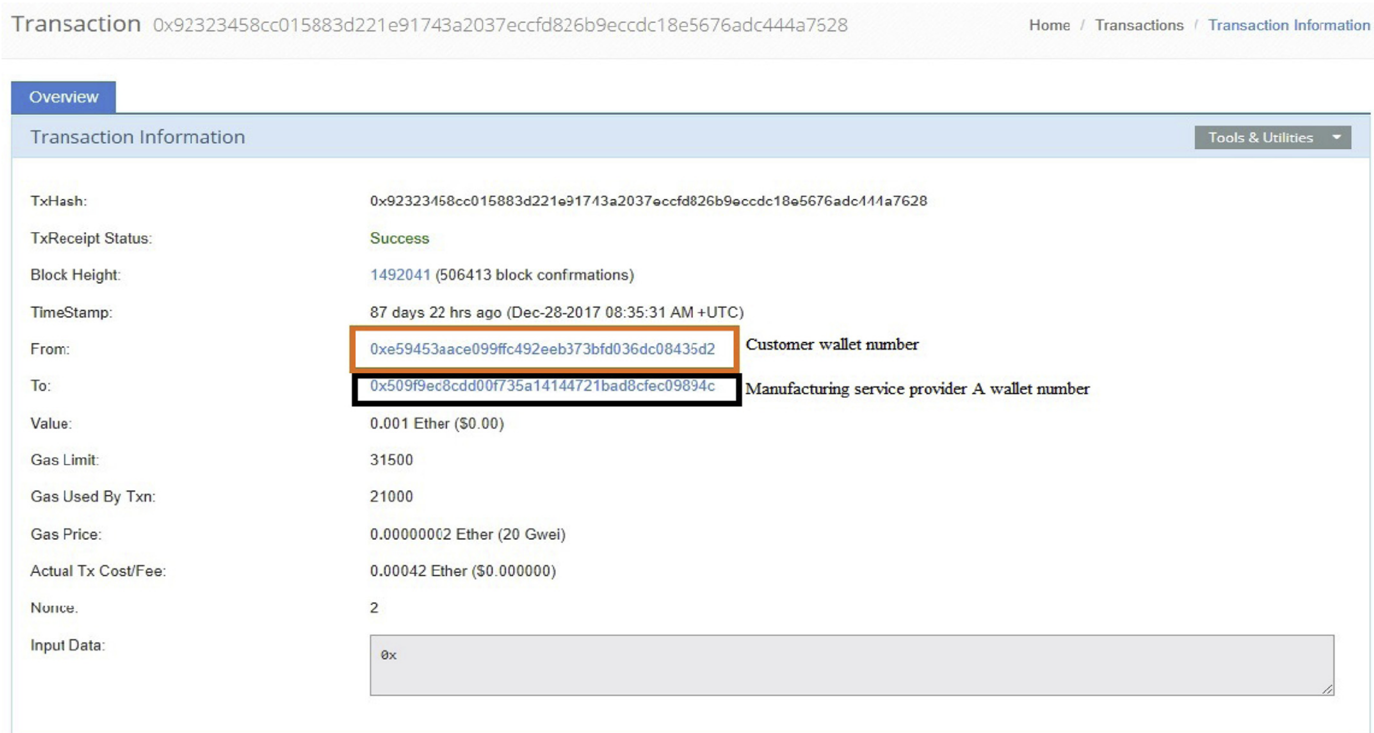

Fig. 11. Process of transaction and it essential information for each transaction.

integrity. As shown in Fig. 8 each block connected via other black based on a hash function which is the beauty of the BCN and guarantee the integrity of the platform.

- Availability: It is a guarantee of reliable access to the information by authorized people. In the proposed architecture, we used short time connection for end users which improve the availability of the platform and membership verification for longtime connection which improves both availability and security of the peer to peer network.

5.3. BCN performance evaluation

For performance evaluation of proposed architecture in this study, we focused on BCN therefore based on case study developed BCN via OC services and 15 customers is evaluated. This evaluation is done based on wallet creation and data encapsulation operation on the BCN. The wallet creation perfume based on random wallet names and each wallet size ranges between 0.5 kb and 1 MB. Via the time command we measured each step needed in the entire process to create a test network, including wallet create, block create, miners create, distribute to users, network connect, network stop and network delete. Therefore after running our tests, we developed Table 3 based on 5, 10 and 15 end users. The first conclusion drawn from these test results is that the values of all indicators linearly related to numbers of end users for example wallet create for five end user is 2.1 and this value linearly increased until 6.87 for 15 end users. Also based on miners create with increasing number of end users this value linearly decreased therefore developed BCN is stable and is illustrated high scalability.

Table 3
Average time based on seconds, three test was done by considering 5, 10 and 15 end users.

Test time	End user 5	End user 10	End user 15
Wallet create	2.1	3.8	6.87
Block create	0.18	0.23	0.29
Miners create	1.5	1.46	1.42
Distribute to users	1.88	2.22	3.62
Network connect	0.21	0.35	0.58
Network stop	1.3	1.9	2.77
Network delete	3.4	3.3	3.2

6. Conclusion

The complexity of manufacturing industry has increased to unprecedented levels with a wide variety of new technologies such as IoT, Cloud manufacturing and etc. CMfg try to play an important role in addressing this challenge by introducing everything as a service with numerous autonomous and cooperative entities. But existing developed CMfg architecture suffering from centralization. Therefore this article demonstrates that how possible to successfully employ the blockchain technology to facilitate of cloud manufacturing and establish a new type of trustable platform as blockchain cloud manufacturing with aiming to developed peer to peer and decentralized network infrastructure for CMfg. Therefore we proposed an architecture based on BCN and CMfg which explained in the detail by considering key components. The implementation of proposed architecture explained based on a case study which includes five manufacturing service providers and 15 end users.

As mentioned before, the main aim of this research paper was to integrate BC into the manufacturing industry and highlight peer to peer communication between different parts of manufacturing sectors, in order to improve the trust and flexibility of the cloud manufacturing. Therefore in evaluation of old cloud manufacturing models, end user could not connect with a finite set of standard and data sharing and service sharing follow the centralized based system which are used third parts for this purpose but in the proposed BCmgf not only customer could be connected to specific service but also can be share data and information in the distributed manner which is improve the security of system.

In the future works, the agent based modeling simulation platform will be developed in order to realistic evaluation of proposed architecture. Also we will focus developed IoT based blockchain platform for supporting decentralized communication of manufacturing shop floor, by aiming to improve the flexibility and agility of the manufacturing system and introduced blockchain industry to smart manufacturing.

Funding

This work was supported by the National Natural Science Foundation of China under Grant (51405089), the Science and Technology Planning Project of Guangdong Province under (2015B010131008) and (2015B090921007) and China Postdoctoral Science Foundation under (2018M633008).

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.rcim.2018.05.011.

References

[1] X. Yang, G. Shi, Z. Zhang, Collaboration of large equipment complete service under cloud manufacturing mode, Int. J. Prod. Res. 52 (2014) 326–336.
[2] F. Tao, Y. Cheng, L. Da Xu, L. Zhang, B.H. Li, CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system, IEEE Trans. Ind. Inf. 10 (2014) 1435–1442.
[3] R.Y. Zhong, X. Xu, E. Klotz, S.T. Newman, Intelligent manufacturing in the context of industry 4.0: a review, Engineering 3 (2017) 616–630.
[4] C. Yang, W. Shen, T. Lin, X. Wang, IoT-enabled, dynamic service selection across multiple manufacturing clouds, Manufact. Lett. 7 (2016) 22–25.
[5] D. Wu, M.J. Greer, D.W. Rosen, D. Schaefer, Cloud manufacturing: strategic vision and state-of-the-art, J. Manuf. Syst. 32 (2013) 564–579.
[6] L. Zhang, Y.-L. Luo, F. Tao, L. Ren, H. Guo, Key technologies for the construction of manufacturing cloud, Comput. Integr. Manuf. Syst. 16 (2010) 2510–2520.
[7] L. Ren, L. Zhang, L. Wang, F. Tao, X. Chai, Cloud manufacturing: key characteristics and applications, Int. J. Computer Integr. Manuf. 30 (2017) 501–515.
[8] D.-G. Feng, M. Zhang, Y. Zhang, Z. Xu, Study on cloud computing security, J. Softw. 22 (2011) 71–83.
[9] P. Radmand, A. Talevski, S. Petersen, S. Carlsen, Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries, Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, IEEE, 2010, pp. 949–957.
[10] A.V. Barcnji, R.V. Barenji, B.L. Sefidgari, An RFID-enabled distributed control and monitoring system for a manufacturing system, Innovative Computing Technology (INTECH), 2013 Third International Conference on, IEEE, 2013, pp. 498–503.
[11] X. Xu, From cloud computing to cloud manufacturing, Rob. Comput. Integr. Manuf. 28 (2012) 75–86.
[12] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H. Park, DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (2017) 78–85.
[13] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Bitcoin (2008).
[14] X. Liang, J. Zhao, S. Shetty, D. Li, Towards data assurance and resilience in IoT using blockchain, Military Communications Conference (MILCOM), MILCOM 2017–2017 IEEE, IEEE, 2017, pp. 261–266.
[15] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on, IEEE, 2017, pp. 1–5.
[16] M. Iansiti, K.R. Lakhani, The Truth About Blockchain, Harv. Bus. Rev. 95 (2017) 118–127.
[17] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inf. Syst. Eng. 59 (2017) 183–187.
[18] Z. Li, W. Wang, G. Liu, L. Liu, J. He, G. Huang, Towards open manufacturing: a cross-enterprises knowledge and services exchange framework based on blockchain and edge computing, Ind. Manage. Data Syst. (2017) 303–320.
[19] J.J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: machine-to-machine electricity market, Appl. Energy 195 (2017) 234–246.
[20] F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, Service Systems and Service Management (ICSSSM), 2016 13th International Conference on, IEEE, 2016, pp. 1–6.
[21] O. Gallay, K. Korpela, N. Tapio, J.K. Nurminen, A Peer-to-Peer Platform for Decentralized Logistics, epubli, 2017.
[22] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu, The blockchain-based digital content distribution system, Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on, IEEE, 2015, pp. 187–190.
[23] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015.
[24] G. Zyskind, O. Nathan, Decentralizing privacy: using blockchain to protect personal data, Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, 2015, pp. 180–184.
[25] R. Wattenhofer, The Science of the Blockchain, CreateSpace Independent Publishing Platform, 2016.
[26] R.V. Barenji, A.V. Barenji, M. Hashemipour, A multi-agent RFID-enabled distributed control system for a flexible manufacturing shop, Int. J. Adv. Manufact. Technol. 71 (2014) 1773–1791.
[27] R.Y. Zhong, X. Xu, L. Wang, IoT-enabled smart factory visibility and traceability using laser-scanners, Procedia Manufact. 10 (2017) 1–14.
[28] A.V. Barenji, R.V. Barenji, M. Hashemipour, A frameworks for structural modelling of an RFID-enabled intelligent distributed manufacturing control system, S. Afr. J. Ind. Eng. 25 (2014) 48–66.
[29] A.V. Barenji, R.V. Barenji, M. Hashemipour, Flexible testing platform for employment of RFID-enabled multi-agent system on flexible assembly line, Adv. Eng. Softw. 91 (2016) 1–11.
[30] Z. Li, Z. Li, G. Liu, G. Liu, L. Liu, L. Liu, X. Lai, X. Lai, G. Xu, G. Xu, IoT-based tracking and tracing platform for prepackaged food supply chain, Ind. Manage. Data Syst. 117 (2017) 1906–1916.
[31] G. Adamson, L. Wang, M. Holm, P. Moore, Cloud manufacturing–a critical review of recent development and future trends, Int. J. Computer Integr. Manuf. 30 (2017) 347–380.
[32] B.-H. Li, L. Zhang, S.-L. Wang, F. Tao, J. Cao, X. Jiang, X. Song, X. Chai, Cloud manufacturing: a new service-oriented networked manufacturing model, Comput. Integr. Manuf. Syst. 16 (2010) 1–7.
[33] F. Tao, L. Zhang, V. Venkatesh, Y. Luo, Y. Cheng, Cloud manufacturing: a computing and service-oriented manufacturing model, Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 225 2011, pp. 1969–1976.
[34] L. Wang, X.V. Wang, Cloud-Enabled Distributed Process Planning, Cloud-Based Cyber-Physical Systems in Manufacturing, Springer, 2018, pp. 105–123.
[35] O. Morariu, T. Borangiu, S. Raileanu, vMES: virtualization aware manufacturing execution system, Comput. Ind. 67 (2015) 27–37.
[36] A.V. Barenji, Cloud based manufacturing execution system: case study FMS, Int. J. Ind. Syst. Eng. 29 (2018) 115–121.
[37] X.V. Wang, L. Wang, A cloud-based production system for information and service integration: an internet of things case study on waste electronics, Enterprise Inf. Syst. 11 (2017) 952–968.
[38] X.V. Wang, L. Wang, A. Mohammed, M. Givehchi, Ubiquitous manufacturing system based on Cloud: a robotics application, Rob. Comput. Integr. Manuf. 45 (2017) 116–125.
[39] G. Škulj, R. Vrabič, P. Butala, A. Sluga, Decentralised network architecture for cloud manufacturing, Int. J. Computer Integr. Manuf. 30 (2017) 395–408.
[40] L. Zhang, Y. Luo, F. Tao, B.H. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, Y. Liu, Cloud manufacturing: a new manufacturing paradigm, Enterprise Inf. Syst. 8 (2014) 167–187.
[41] F. Tao, Y. Cheng, L.D. Xu, L. Zhang, B.H. Li, CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system, IEEE Trans. Ind. Inf. 10 (2014) 1435–1442.
[42] A. Kumar, R. Shankar, A.K. Choudhary, L.S. Thakur, A big data MapReduce framework for fault diagnosis in cloud-based manufacturing, Int. J. Prod. Res. 54 (2016) 7060–7073.
[43] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (2011) 1–11.
[44] B. Esmaeilian, S. Behdad, B. Wang, The evolution and future of manufacturing: a review, J. Manuf. Syst. 39 (2016) 79–100.
[45] N.T. Courtois, M. Grajek, R. Naik, Optimizing sha256 in bitcoin mining, International Conference on Cryptography and Security Systems, Springer, 2014, pp. 131–144.
[46] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, Security and Privacy (SP), 2016 IEEE Symposium on, IEEE, 2016, pp. 839–858.
[47] C. Dannen, Introducing Ethereum and Solidity, Springer, 2017.
[48] Y. Zhang, J. Wen, The IoT electric business model: Using blockchain technology for the internet of things, Peer Peer Netw. Appl. 10 (2017) 983–994.
[49] F. Tao, Y. Zuo, L. Da Xu, L. Zhang, IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing, IEEE Trans. Ind. Inf. 10 (2014) 1547–1557.
[50] C. simulator, CNCSimulator Pro, CNCSimulator Pro, (2001) https://cncsimulator.info/download.
[51] Z. Pandilov, A. Milecki, A. Nowak, F. Górski, D. Grajewski, D. Ciglar, M. Klaić, T. Mulc, Virtual modelling and simulation of a CNC machine feed drive system, Trans. FAMENA 39 (2016) 37–54.
[52] B. Ward, The Book of VMware, No Starch Press, 2002.
[53] G. Greenspan, MultiChain Private Blockchain, White Paper, 2015, http://www.multichain.com/download/MultiChain-White-Paper.pdf.
[54] J. Hruska, Consumer, Merchant and Mobile Device Specific, Real-Time Dynamic Tokenization Activation within a Secure Mobile-Wallet Financial Transaction System, Google Patents, (2013).
[55] R.L. Krutz, R.D. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010.