Journal of Manufacturing Systems 61 (2021) 338–350

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

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

Secure sharing of big digital twin data for smart manufacturing based on blockchain

Weidong Shen [a,b], Tianliang Hu [a,b,c,*], Chengrui Zhang [a,b], Songhua Ma [a,b]

[a] School of Mechanical Engineering, Shandong University, Jinan 250061, PR China
[b] Key Laboratory of High Efficiency and Clean Mechanical Manufacture at Shandong University, Ministry of Education, Jinan 250061, PR China
[c] Suzhou Institute of Shandong University, Suzhou 215123, PR China

ARTICLE INFO

Keywords:
Digital twin
Blockchain
Big data
Data sharing
Smart manufacturing

ABSTRACT

With the rapid development of digital twin technology, a large amount of digital twin data named as big digital twin data (BDTD), is generated in the lifecycle of equipment, which is supposed to be used in digital twin enabled applications. However, in the implementation of these applications, data sharing problem which is caused by the lack of data security as well as trust among stakeholders of equipment, limits data using value. It is a novel way to introduce blockchain technology into digital twin to solve the problem. However, current methods cannot fulfill the requirements of exponential growth and timely sharing of BDTD. Therefore, a blockchain-based framework for secure sharing of BDTD is proposed to solve the problems. Cloud storage is integrated into the framework, with which, BDTD is encrypted and stored in Cloud, while the hash of BDTD and transaction records are stored in blockchain. Some rules of generating new block are designed to improve the processing speed of blockchain. An algorithm for optimal sampling rate selection is presented to maximize total social benefits of the participants of BDTD sharing. Simulation results show that the algorithm is better than traditional method for maximizing the total social benefits. Furthermore, a protype system is developed and evaluated based on Fabric test network. Evaluation results show that BDTD can be shared securely multiple times per second through the framework, which demonstrates the feasibility of the framework in supporting timely sharing of BDTD.

1. Introduction

As one of the main developing trends of Industry 4.0, digital twin (DT) technology increasingly gains the attention of both academia and industry. As the precise virtual copy of product, digital twin almost mirrors every phases of product, such as design, manufacture, maintaining, and service [1]. The quality, cost, efficiency and life of product can be monitored, controlled, optimized, and predicted precisely by using DT with intelligent algorithms respectively [2]. In these applications, DT data is used to drive the self-updating of DT, train intelligent algorithms, and mine professional knowledge. In order to achieve high precision and high reliability of DT-based applications, DT data is collected from different equipment, different production line and even different plant. Furthermore, DT data usually has big volume, in order to meet the requirement of model training. Therefore, DT data sharing is required among different equipment, different lifecycle stages of equipment, different applications of equipment, and even different owners of equipment. On the one hand, because it is difficult for one equipment to gather enough data only by itself for DT-based application. On the other hand, DT data needs to be shared to promote lifecycle integration of equipment. For instance, DT data collected from using stage can be used to improve the design quality in design stage and make better manufacturing process in manufacturing stage. As shown in Fig. 1, the typical scenarios of DT data sharing include:

(1) Among different equipment with the same type

Because of the similarity of data in the same type of equipment, DT data can be shared to make DT-based services more precise. Data which is reusable and valuable for other equipment, needs to be shared. Such as the operation data before and after the failure of same type of bearings needs to be shared. On the contrary, business privacy data, useless data, and redundant data don't need to be shared. Such as the detailed normal operation data of bearing is redundant [3], and doesn't need to be shared completely. Only the data during a period of time before and after bearing failure is valuable and needs to be shared.

* Corresponding author at: School of Mechanical Engineering, Shandong University, Jinan 250061, PR China.
E-mail address: tlhu@sdu.edu.cn (T. Hu).

https://doi.org/10.1016/j.jmsy.2021.09.014
Received 15 June 2021; Received in revised form 8 September 2021; Accepted 21 September 2021
Available online 27 September 2021

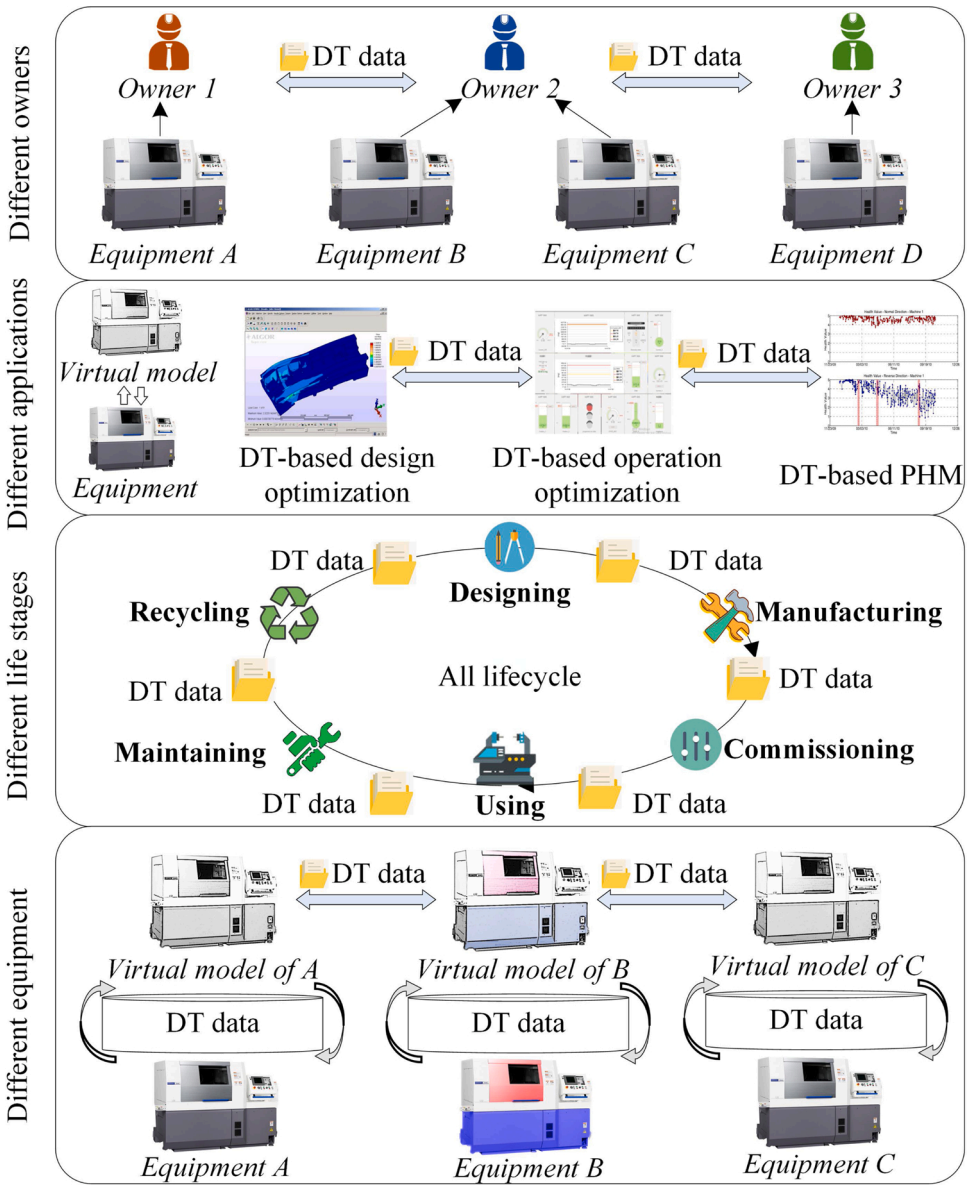

Fig. 1. The typical scenarios of DT data sharing.

(2) Among different lifecycle stages of equipment

There is time series relationship among DT data from different lifecycle stages of equipment. What's more, the ownership of equipment may change in different lifecycle stages (e.g. design stage, manufacturing stage, integration stage, using stage, recycling stage). It causes that data islands are formed between different lifecycle stages of equipment [4]. Therefore, DT data needs to be shared among all lifecycle of equipment to promote lifecycle integration of equipment.

(3) Among different applications of equipment

The DT data from different applications, such as the design optimization, the operation optimization, and the prognostics health management (PHM) based on DT of equipment, is useful to each other. Hence DT data can be shared among different applications of equipment to improve the service quality of DT-based applications.

(4) Among different owners of equipment

Due to privacy and security, there are data islands between different owners of equipment. In order to speed up DT data aggregation, DT data of different owners' equipment needs to be shared to fulfill the data requirements of DT-based applications.

With machine tool as an example, physical equipment data includes spindle speed, cutting tool vibration, temperature, and other various sensor data. These data are generated quickly and transferred to virtual space for updating virtual model or data analysis. Virtual equipment data refers to the simulation results and the results of data analysis. Such as simulation of gear wear based on virtual model, predictions of cutting tool life based on real-time data and huge amounts of historical data. Integrating the physical equipment data, virtual equipment data of machine tools as well as service system such as Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP), accurate production scheduling [5,6], efficient flexible production [7], and other higher value applications [8] can be realized. Therefore, the shared DT data has big volume, many varieties, fast generation velocity, and great value, which are named as 4 Vs characteristics of big data. In other words, the DT data gathered from various sources is a kind of big data [9]. Big data can also be regarded as an important part of digital twin. In

Table 1
Comparison of representative published researches related with blockchain and DT.

Related works	Putz et al. [22]	Suhail et al. [23]	Zhang et al. [24]	Huang et al. [25]
Year	2021	2021	2020	2020
Objects	Industrial asset	Industrial internet of things	Intelligent manufacturing systems	Product
Purpose	Secure data sharing	Data management	Configuration of digital twin manufacturing cell	Data management of digital twin
Blockchain	Ethereum	DAG-based blockchain	Fabric	Unknown
DT data storage	Off-chain storage (Swarm)	On-chain storage	Off-chain storage (Edge)	On-chain storage
Implementation	●●●● (Fully)	○○○○ (None)	●●○○ (Partially)	○○○○ (None)
Test items	Latency and cost for interaction	None	Throughput and latency of Ethereum and Fabric	None
Test results	Swarm is restricted to one update per second.	None	Fabric could achieve higher throughput and lower latency than Ethereum.	None

order to describe the DT data gathered from different equipment, different lifecycle stages of equipment, different applications, and different owners of equipment, big digital twin data (BDTD) is proposed to describe the above characteristics.

Although many DT-based applications have been studied, it can be observed that, for BDTD, as the impetus of DT-based applications, there is lack of a method to make BDTD be shared securely. Security is crucial for interested parties which want to share their data with trustless others. If the shared data is leaked, it might cause huge losses for the party. In addition, because of the lack of trust, the operations of payment and sending data involved in BDTD sharing cannot be implemented safely. Therefore, a secure method for BDTD sharing is required to promote BDTD sharing among trustless parties.

The first possible method is to design access control mechanism which relies on a third party. For instance, a service-oriented security architecture for access control in semantic data federations was presented to solve the problem of satisfying the confidentiality requirement of various stakeholders in product lifecycle [10]. A pull mode industrial solution was designed to enable data sharing between original equipment manufacturers and their suppliers by using a combination of PTC PDMLink and Microsoft SharePoint technologies [11].

The second probable method is to depend on Cloud/Fog computing. For instance, a secure online/offline data sharing framework was proposed to solve the problems of online/offline encryption, outsourced decryption, and fine-grained keyword search in Cloud [12]. A fog-computing-based approach was proposed to share industrial big data with high security by moving the integration task from the Cloud to the edge of networks [13].

However, the two methods both depend on centralized third party that is vulnerable to malicious attacks, such as single node invalidation and data tampering. It lacks a secure and decentralized method for data sharing among all parties in lifecycle of equipment.

In order to solve the problem, blockchain is introduced into industrial filed to improve the security of data sharing. For instance, a blockchain-based distributed peer to peer (P2P) network architecture was proposed to solve the problem of centralization in Cloud manufacturing [14]. Blockchain-based data sharing techniques were proposed to address the security problems of data transmission in Industrial Internet of Things (IIoT) [15,16]. A blockchain-enabled efficient data collection and secure sharing scheme combining Ethereum and deep reinforcement learning was proposed to ensure security when sharing data among smart mobile terminals [17]. Blockchain-based architectures combining RFID and IoT technology were proposed to provide a chain of immutable transactions of supply chains in multi-company project environments [18,19]. An industrial blockchain-based framework for product lifecycle management was proposed to fulfill the requirements of the openness, interoperability and decentralization [20]. Moreover, in order to support the application of CPS and DT, blockchain-based resource sharing architectures were proposed to improve the security and efficiency of data management [21]. The representative latest published researches related with blockchain and DT are compared as shown in Table 1.

As described in Table 1, Huang et al. proposed a blockchain-based method for data management of digital twin of product [25]. Zhang et al. proposed a blockchain-based architecture for the configuration of intelligent manufacturing systems [24]. Suhail et al. discussed the blockchain-based framework for the data management and security of Industrial Internet of Things (IIoT) [23]. Putz et al. proposed a blockchain-based sharing model for the management of digital twin components and associated information [22].

To the data sharing problems of DT, the time latency of data sharing is a very important factor. However, in the researches listed in Table 1, Putz et al. fully implemented their method which is based on Ethereum and Swarm, and evaluated the latency and cost for interaction [22]. Because Swarm is restricted to one update per second, timely DT data sharing, which need to support sensor data to be updated several times per second, might not have been considered in their research. In addition, Zhang et al. evaluated the throughput and latency of Ethereum and Fabric, which showed that Fabric could achieve higher throughput and lower latency than Ethereum [24]. But the time latency of the combination of Fabric and Cloud for data sharing has not been evaluated. If blockchain technology and Cloud technology are applied to DT data sharing, the evaluation of time latency is indispensable.

To this end, our goal is to design a blockchain-based framework which can support the secure sharing of BDTD, fulfill the processing speed requirement of time-sensitive data, and maximize the total social benefits of BDTD sellers and BDTD buyers. The main contributions of this paper are as follows.

(1) A framework for secure sharing of BDTD is proposed by combining blockchain with Cloud technology. Channel is used to achieve business isolation and data confidentiality for the participants of BDTD sharing. The hash of BDTD and transaction records are stored in blockchain. But original BDTD are encrypted, encapsulated, and stored in Cloud.
(2) The implementation method of the framework is presented. In order to fulfill the requirement of time-sensitive data, some rules of generating new block are designed to improve the processing speed of blockchain. Evaluation results demonstrate that BDTD can be shared securely multiple times per second through our framework.
(3) An algorithm for optimal sampling rate selection of BDTD is proposed to maximize the total social benefits of BDTD sellers and BDTD buyers. Simulation results show that our algorithm has better performance than traditional method in terms of maximizing the total social benefits.

The rest of this paper is organized as follows. Requirements for secure sharing of BDTD are analyzed in Section 2. A framework of blockchain enabled secure sharing of BDTD is proposed in Section 3. Section 4 describes the implementation method of secure sharing of BDTD based on blockchain. An algorithm for optimal sampling rate selection of BDTD is presented in Section 5. The framework and algorithm are evaluated in Section 6. Section 7 is discussion. Finally,

conclusions are summarized in Section 8.

2. Requirements for secure sharing of BDTD

2.1. Characteristic of BDTD

DT data mainly consists of physical device data, virtual device data, service system data, and fused data [26]. Along with the application of DT technology, the volume of BDTD becomes big while gathering data from various sources, which makes it cannot be stored, analyzed, managed, and shared by regular tools within a tolerable time. The characteristics of BDTD are summarized as follows.

(1) Huge data volume. With the operation of equipment, the volume of BDTD generated by the equipment grows exponentially, which makes BDTD cannot be stored in blockchain which has limited storage ability.
(2) Wide type variety. BDTD generated in lifecycle of equipment includes designing data, manufacturing data, commissioning data, using data, maintaining data, and recycling data. So there is a wide variety of data in BDTD.
(3) High generation velocity. In order to reflect the state of physical equipment in real time, the sampling rate of sensors in physical equipment is high generally. As the main component of BDTD, sensor data makes the generation velocity of BDTD high.
(4) Big using value. DT data works as the "driver" for physical equipment, virtual equipment, and service system. Since BDTD is accumulated by a large amount of DT data. BDTD has big value for all participants in lifecycle of equipment. For instance, the designer of equipment can improve the design scheme according to BDTD. The users of equipment can implement real-time operation optimization based on BDTD.

2.2. Requirements analysis

The requirements for secure sharing of DT data, which include multi-party sharing, data variety support, data velocity support, data integrity, data confidentiality mechanism, as well as read and write operations, were presented by Dietz et al. [27]. However, with respect to secure sharing of BDTD, these requirements are not enough and lack consideration of exponential growth of data volume and efficiency of data sharing. In order to provide a feasible solution for secure sharing of BDTD, the essential requirements for the solution are analyzed and summarized as follows.

(1) Supporting multi-party sharing of BDTD. In order to create more value for all parties related to equipment, BDTD needs to be shared among different parties.
(2) Supporting exponential growth of BDTD. BDTD has a big volume and cannot be stored by regular database. The solution should support the exponential growth of BDTD.
(3) Supporting the sharing of BDTD which has high sampling rate. As an important part of BDTD, sensor data from physical equipment has high sampling rate generally. The sensor data accrues in intervals ranging from minutes to milliseconds [27]. Therefore, the solution should support the sharing of BDTD such as sensor data.
(4) Supporting the sharing of BDTD which includes a wide variety of data. The data types of BDTD include structured data (e.g., symbols and digit), semi-structured data (e.g., trees and graphs), and unstructured data (e.g., images and audios) [9].
(5) Supporting verification of BDTD integrity. For a party that wants to purchase BDTD from the others, BDTD integrity must be taken into consideration. Because incomplete or falsified data cannot be tolerated by any party.
(6) Supporting confidentiality of BDTD. In general, BDTD is only shared with someone who has the permission of BDTD owner. Therefore, the confidentiality of BDTD needs to be fulfilled for the safety of BDTD.

In order to fulfill the requirements, there are two typical solutions for secure data sharing. One is the centralized solution which needs an authoritative third party to be an intermediary. Transactions between owners and consumers of BDTD depend on the third party. However, with respect to the integrity, traceability, and confidentiality of BDTD, a centralized third party usually cannot be trusted by all stakeholders. The other is the distributed solution known as blockchain, which provides a secure way for data sharing among parities which do not trust each other. Tamper proof, traceability, and collective maintenance are the main features of blockchain. Tamper proof means that after transaction information is added to blockchain, the difficulty and cost of tampering transaction information are very high. Traceability is that any piece of transaction information on the blockchain can trace its origin through the chain structure. Collective maintenance means that blockchain is maintained by all nodes with maintenance function.

Taking the tamper proof, traceability, and collective maintenance of blockchain into consideration, a distributed solution is more suited for BDTD sharing. Therefore, a blockchain-based solution for secure sharing of BDTD is selected to solve the trust problem in this study.

3. Framework of blockchain enabled secure sharing of BDTD

Our blockchain-based framework for secure sharing of BDTD is illustrated as shown in Fig. 2. The framework comprises multiple organizations, client, physical equipment, and Cloud storage. The components of our framework are described in the following sections. Section 3.1 explains the organizations. Section 3.2 focuses on the client and Cloud storage.

3.1. Organizations of blockchain

The organizations include the stakeholders of physical equipment and the orderer of blockchain in our framework. The stakeholders generally involve designer, manufacturer, owner, user, maintainer, etc. related with equipment. They are not only the main participants in BDTD sharing, but also the main members of consortium blockchain network which only allow authorized nodes to join. Except *orderer* organization, which is composed of certificate authority and orderer peers, every organization contains certificate authority, leader peer, endorse peer, anchor peer, committer peer, and several ledgers of which number is equal to the number of channels the organization joins. The channel is a kind of communication link with confidentiality, which is used to achieve business isolation and data confidentiality. Channel 1 is a communication link that serves *Designer* and *Manufacturer* only. Channel 2 is a communication link for all organizations. Channel 3 is a communication link only for *Designer* and *Owner*. Channel 4 is a communication link that serves *Manufacturer* and *Owner* only. Channel 5 is a communication link only for *User A* and *User B*. Channel 6 is a communication link only for *User A* and *Maintainer*. Channel 7 is a communication link only for *User B* and *Maintainer*. *User A* joins channel 2, channel 5, and channel 6. Channel 2 provides a communication mechanism for *User A* to share BDTD data with all other organizations. Channel 5 provides a communication mechanism for *User A* to share BDTD data with *User B* and prevent unauthorized other organizations from viewing their transactions. Channel 6 provides a communication mechanism only for *User A* to share BDTD data with maintainer.

The peers in an organization are responsible for different tasks. Orderer peer is responsible for receiving the transactions with endorsement signature from other organizations, sorting the unpacked transactions, generating blocks, and broadcasting them to the other peers. Lead peer can communicate with the orderer peer, and is responsible for getting the latest block from the orderer peer and synchronizing them within the organization. Endorse peer is responsible for

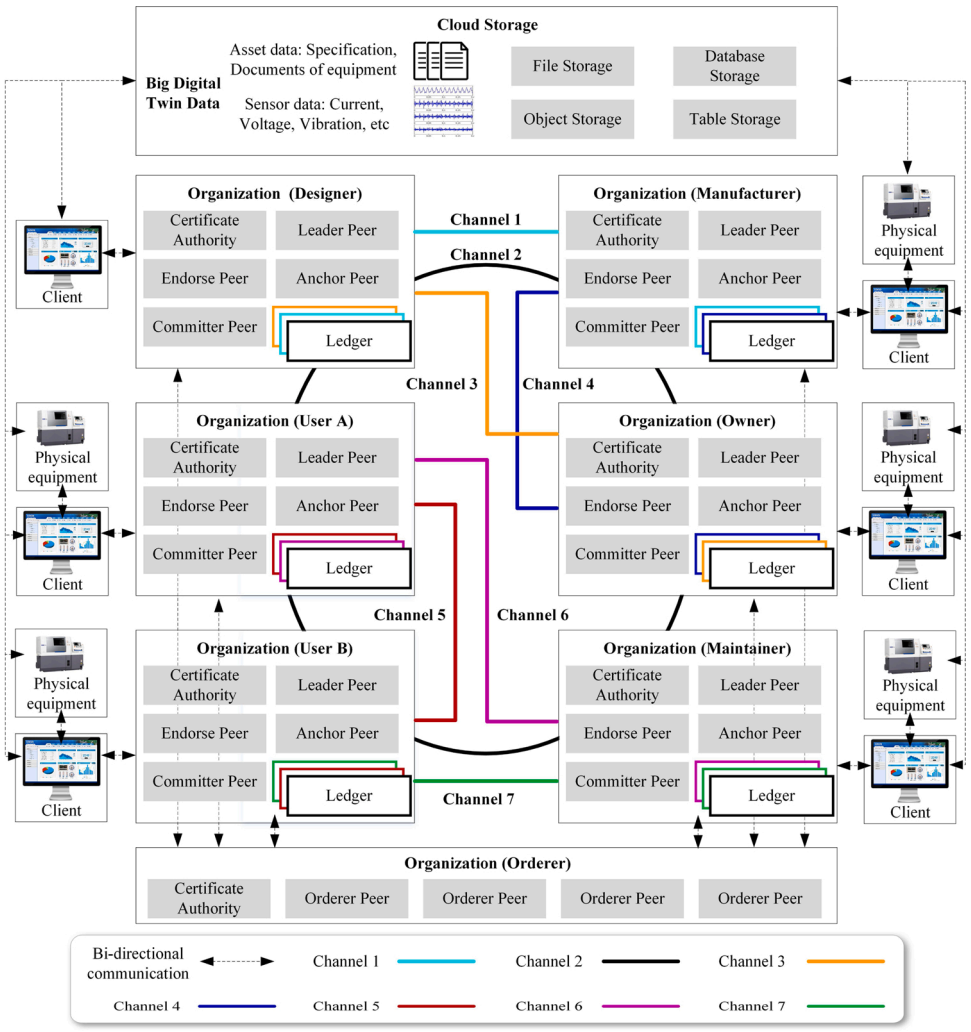

Fig. 2. The blockchain-based framework for secure sharing of BDTD.

executing transaction and signing the result. Anchor peer is responsible for exchanging information with other organizations on behalf of the organization. Committer peer is responsible for verifying the transactions in the block sent from orderer peer, as well as maintaining the replication of ledger which comprises world state and blockchain [28]. World state is the state of ledger after the last transaction is completed. Blockchain stores the history of all transactions.

The basic structure of blockchain is shown in Fig. 3. Except for genesis block, the head of every block contains the hash of its previous block, the hash of current block, transactions and metadata. Based on the connection mechanism, every transaction can be recorded in an immutable way.

3.2. Client and cloud storage

Clients are responsible for constructing transaction proposal, generating transaction, and broadcasting transaction to orderer peers in our framework. Application program for sharing BDTD runs on the client and is connected to a peer of the organization to communicate with the blockchain network. Moreover, clients are responsible for managing the data upload, data preprocessing, and data encryption of the physical equipment. Through the connection with Cloud, clients manage and share the DT data of the physical equipment.

Cloud storage provides storage service that includes file storage, objects storage, database storage, and table storage, for physical

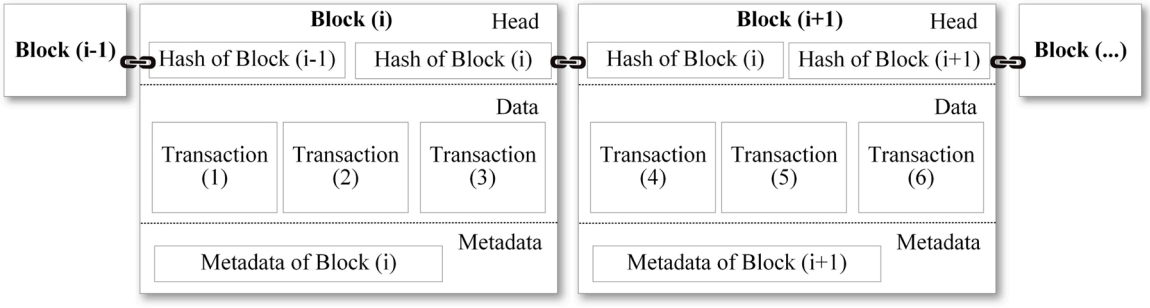

Fig. 3. The basic structure of blockchain.

equipment and clients. Cloud database refers to the database deployed in a virtual computing environment by Cloud providers as well as provides online database services for users through database as a service paradigm or data storage as a service paradigm. Compared with local storage, the advantages of Cloud storage include pay-as-you-go manner, scalability, network connectivity, rapid deployment, etc. With respect to security problem brought by Cloud storage, several publications had given some feasible encryption schemes for Cloud [29]. In this paper, Proxy Re-Encryption (PRE) is combined with Cloud storage to guarantee the confidentiality of BDTD. PRE is proposed by Blaze, Bleumer and Strauss and can be used to achieve secure public Cloud data sharing [30, 31]. The detailed implementation method of encrypting BDTD is presented by using PRE in Section 4.

4. Implementation method of secure sharing of BDTD based on blockchain

4.1. Workflow

Based on the framework proposed in Section 3, the workflow of secure sharing of BDTD enabled by blockchain is described as shown in Fig. 4. The interactions between the components of proposed framework are divided into five steps, which are determining ownership of BDTD, storing BDTD, BDTD tokenization, designing smart contract, and operation of smart contract. Firstly, the ownership of BDTD is determined by sending hash of BDTD, timestamp, and signature of BDTD owner to consortium blockchain network which is responsible for auditing information and packaging information into new block of blockchain. Then BDTD are uploaded and stored in Cloud. BDTD owner can price BDTD by BDTD tokenization. Finally, BDTD are shared based on Proxy Re-Encryption and smart contract which is designed by both parties involved in the sharing of BDTD. The detailed implementation procedure of each step is described in following sections.

4.2. Determining ownership of BDTD

BDTD owner needs to determine the ownership of BDTD through sending hash of BDTD, timestamp, and its signature to consortium blockchain network. Once the hash of BDTD is stored in blockchain, BDTD cannot be falsified. BDTD are classified into time-sensitive data and non time-sensitive data. The time-sensitive data mainly refer to the data collected by various sensors. The non time-sensitive data include production tasks, equipment specification, process plans, etc. In order to fulfill the transaction requirement of time-sensitive data, three rules of generating new block are defined to improve the efficiency of determining ownership of BDTD.

Rule 1: BDTD should be divided into two levels, which are high level and low level. High-level data refer to the time-sensitive data. Low-level data refer to the non time-sensitive data. BDTD owner can customize the level of BDTD to fit its needs.

Rule 2: BDTD owner can mark high-level data with service fee that it is willing to pay. The orderer peer can gain the service fee. It is not allowed for low-level data to be marked with service fee.

Rule 3: The orderer peer can give priority to high-level data which have higher service fee. Low-level data recorded in the new block of blockchain should be specified to be no less than a certain proportion.

As a BDTD owner, *User A* sends a transaction about determining the ownership of BDTD to consortium blockchain network. The transaction is denoted as

$$Transaction(Hash, Timestamp, High, Fee, Sign_A)$$

Hash is the hash of BDTD from *User A*. *Timestamp* indicates the time when the transaction takes place. *High* refers to high level. *Fee* is service fee that *User A* is willing to pay. $Sign_A$ is the signature of *User A*.

4.3. Storing BDTD

Cloud provides storage service for BDTD owners as well as charges according to the size and using time of storage space occupied by BDTD owners. The transaction procedure between BDTD owners and the Cloud based on blockchain is presented as follows.

(1) *User A* sends a transaction about paying for its BDTD storage to consortium blockchain network. The transaction is denoted as

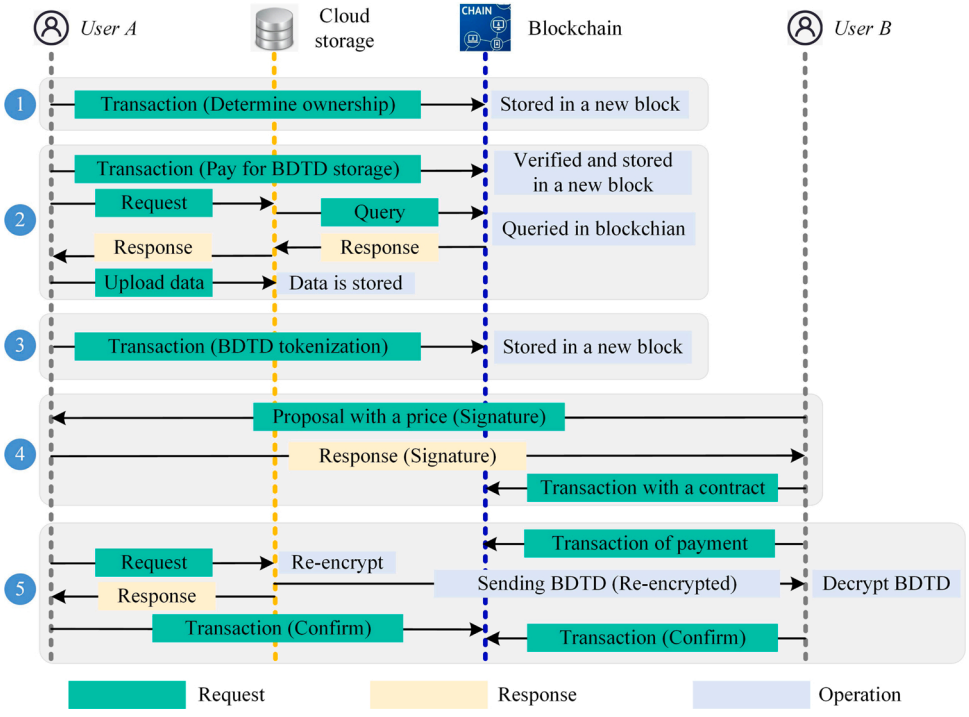

Fig. 4. Workflow of BDTD secure sharing based on blockchain.

$$Transaction(PubK_A, PubK_{DB}, Size, Time, Token, Timestamp, Sign_A).$$

$PubK_A$ is the account of *User A*. $PubK_{DB}$ is the account of Cloud. *Size* and *Time* is the size and using time of storage space respectively. *Token* is the amount of payment. *Timestamp* indicates the time when transaction takes place. $Sign_A$ is the signature of *User A*.

(2) The transaction sent from *User A* is audited, verified, and packaged into a new block. When the new block is connected to blockchain, it can be considered that the transaction has been recorded in an immutable form.
(3) When the Cloud receives the request of BDTD storage from *User A*, it needs to communicate with the consortium blockchain network for querying whether *User A* has paid for occupying storage space. If the response of the consortium blockchain network shows that *User A* has already paid, *User A* will be allowed to upload its BDTD.
(4) The original BDTD of *User A* are fragmented locally into lots of fragmentations. Then the fragmentations of BDTD are encrypted by using cryptography algorithm, e.g. Elliptic Curve Cryptography (ECC), which is an asymmetric cryptography algorithm [32]. Finally, the encrypted BDTD are uploaded to Cloud.

The confidentiality of BDTD is guaranteed by using cryptography algorithm. For instance, through using ECC, a user can obtain a pair of keys, which are a private key and a public key. After the original BDTD are encrypted by using the public key, the encrypted BDTD can only be decrypted by using the private key which is only known to the user.

4.4. BDTD tokenization

Data tokenization is the process that data are tokenized as on-chain assets for sale and transaction [33]. In order to facilitate BDTD sharing, BDTD need to be converted into data asset with a specified price. The procedure of BDTD tokenization is presented as follows.

(1) *User A* sends a transaction about BDTD authorization to the consortium blockchain network. The transaction is denoted as

$$Transaction(PubK_A, Address_C^A, Hash_C^A, Token_C^A, Timestamp, Sign_A).$$

$PubK_A$ is the account of *User A*. $Address_C^A$ is the address of BDTD stored in the Cloud. $Hash_C^A$ is the hash of BDTD from *User A*. $Token_C^A$ is the price of BDTD. *Timestamp* indicates the time when transaction takes place. $Sign_A$ is the signature of *User A*.

(2) Then the consortium blockchain network audits the transaction by interacting with Cloud. If the transaction is verified, it is packaged to a new block by orderer peer.
(3) After the transaction is stored in blockchain, it can be considered that the BDTD of *User A* is converted to data asset.

Moreover, in order to protect the interest of BDTD owner, the openness of BDTD is classified as complete openness, partial openness, and no openness. Complete openness means that anyone has access to BDTD without restriction. Partial openness means that BDTD is only shared with a few parties authorized by BDTD owner. No openness means that BDTD owner is not willing to share data with anyone. The openness of BDTD can be specified in the transaction about BDTD tokenization.

4.5. Designing smart contract

The concept of smart contract was defined as "a digital transaction protocol within which the parties execute the terms of a contract" by Nick Szabo [34]. Smart contract includes codes translated from contractual terms. The process of designing smart contract by BDTD owner and BDTD consumer is presented as follows.

(1) The agreement about the price of BDTD is reached through the consultations between BDTD owner and BDTD consumer. They also need to design the steps of BDTD transaction.
(2) Then the steps of BDTD transaction are converted into codes that have certain outcomes of execution.
(3) Finally, smart contract is inspected and signed by BDTD owner and BDTD consumer. Smart contract is deployed in blockchain.

4.6. Operation of smart contract

The operation of smart contract is performed automatically and cannot be interfered by anyone. The inputs of smart contract are the transactions generated by BDTD owner and BDTD consumer, e.g. transaction about paying for BDTD, transaction about sending BDTD, etc. The outputs of smart contract are the state change of smart contract. The operation process of smart contract is presented as follows.

Firstly, *User B* sends a transaction about paying for BDTD to consortium blockchain network. With the transaction as input, the state of smart contract is changed, which means that smart contract has been executed partially.

Secondly, *User A* sends BDTD to *User B* through Cloud. In order to guarantee the confidentiality of BDTD, the transmission process of BDTD is based on PRE as shown in Fig. 5. *User A* has a private key named $PriK_A$ and a public key named $PubK_A$. *User B* has a private key named $PriK_B$ and a public key named $PubK_B$. *C* denotes the original BDTD that generated by *User A*. The transmission process of BDTD is presented as follows.

(1) *C* is encrypted as C_{PubKA} by *User A* using its public key $PubK_A$.
(2) *User B* sends a request of data sharing to *User A*. The request including the address and hash of *C* is denoted as

$$Request(PubK_B, Address_C, Hash_C, Timestamp, Sign_B)$$

(3) If *User A* agrees with the request from *User B*, a re-encryption key $Rk_{A\text{-}B}$ is generated by *User A* using $PriK_A$ and $PubK_B$. Then $Rk_{A\text{-}B}$ is sent to Cloud where C_{PubKA} is stored.
(4) C_{PubKA} is re-encrypted as C_{PubKB} by Cloud using $Rk_{A\text{-}B}$. Then C_{PubKB} is sent to *User B*.
(5) Finally, C_{PubKB} is decrypted as *C* by *User B* using its private key $PriK_B$.

Throughout the transmission process of BDTD, Cloud cannot read the plaintext of BDTD.

Thirdly, when *User B* receives re-encrypted BDTD from Cloud, *User B* sends a transaction about receiving BDTD to consortium blockchain network. After the transaction is verified and recorded in blockchain, payment operation in the smart contract is executed automatically.

Through determining ownership of BDTD, storing BDTD, BDTD tokenization, designing smart contract and operation of smart contract, secure sharing of BDTD based on blockchain is implemented in Section4. Moreover, in order to maximize total social benefits of BDTD sellers and BDTD buyers, an algorithm for optimal sampling rate selection of BDTD is proposed in Section 5.

5. Algorithm for optimal sampling rate selection of BDTD

5.1. Problem formulation

In the proposed framework of blockchain-based BDTD sharing, BDTD buyer purchases BDTD from BDTD sellers. Then BDTD are processed and analyzed by the BDTD buyer to develop advanced models, e.g. life prediction model of cutting tool. The volume of BDTD is an

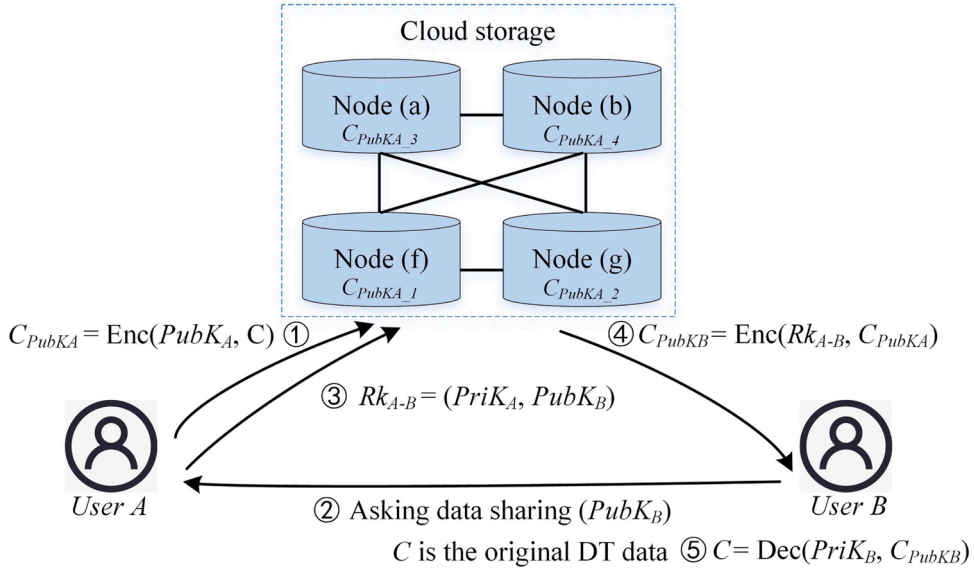

Fig. 5. DT data sharing scheme based on Proxy Re-Encryption.

important intrinsic characteristic that affects the performance of model developed by the BDTD buyer. In order to obtain the higher performance of advanced model, the bigger volume (V) of BDTD gathered in a fixed period of time (T) needs to be bought. The time (T) is divided into $(t_1, t_2, \ldots, t_i, \ldots, t_n)$ based on the requirement of BDTD buyer. The corresponding BDTD volume (V) is denote as $(v_1, v_2, \ldots, v_i, \ldots, v_n)$. The budget ($B$) of BDTD buyer is divided into $(B_1, B_2, \ldots, B_i, \ldots, B_n)$.

The sampling rate (r_{ij}) of sensor system of the j_{th} BDTD seller directly affects its BDTD volume (v_{ij}). The BDTD volume acquired in a period of time (t_i) is calculated as (1).

$$v_{ij} = r_{ij} \cdot t_i \tag{1}$$

The energy consumption of sensor system is known to be linearly proportional to sampling rate (r_{ij}) [35,36]. Given hardware constants α_1 and α_2, we assume that the energy consumption cost (C_{eij}) of sensor system during a unit time is calculated as

$$C_{eij}(r_{ij}) = \varepsilon(\alpha_1 r_{ij} + \alpha_2) \tag{2}$$

where ε is the price of per unit electricity.

What the BDTD seller cares about is to gain more revenue with as little cost as possible. The utility function of the j_{th} BDTD seller is given as

$$U_{ij}(r_{ij}) = p_{ij} - C_{eij} \tag{3}$$

where p_{ij} is the revenue of the j_{th} BDTD seller through selling BDTD. The revenue p_{ij} depends on the satisfaction degree that BDTD bring to BDTD buyer. The higher the satisfaction degree of BDTD buyer, the more the revenue of BDTD seller.

For the advanced model developed by BDTD buyer, the higher the data volume or sampling rate, the higher the model performance (e.g. accuracy of life prediction model of cutting tool) [37]. For rational BDTD buyers, the higher the model performance, the higher the satisfaction degree. Therefore, the satisfaction degree function of BDTD buyer is monotonically increasing and follows the diminishing marginal utility [38]. The satisfaction degree function is defined as

$$\xi(r_{ij}) = \beta_1 + \beta_2 log(1 + r_{ij}) \tag{4}$$

where β_1 and β_2 are the curve fitting parameters of the satisfaction degree function $\xi(\cdot)$ to real-world data.

The optimization problem for BDTD sharing is defined as

$$\begin{aligned} &\max_{r_{ij}} U_{ij}(r_{ij}) = \frac{\beta_1 + \beta_2 \log(1 + r_{ij})}{\sum_{j=1}^{m}(\beta_1 + \beta_2 \log(1 + r_{ij}))} B_i - \varepsilon(\alpha_1 r_{ij} + \alpha_2) \\ &s.t.\ (1) C_{eMin} \le \varepsilon(\alpha_1 r_{ij} + \alpha_2) \le C_{eMax} \\ &(2) U_{ijMin} \le U_{ij}(r_{ij}) \end{aligned} \tag{5}$$

where C_{eMin} denotes the minimum of energy consumption cost during a unit time. C_{eMax} denotes the maximum of energy consumption cost during a unit time. The first constraint indicates that the energy consumption of the BDTD seller is in a certain range when the sampling rate changes. In order to inspire BDTD sharing, U_{ijMin} is the minimum reward for the BDTD seller.

5.2. Algorithm for optimal sampling rate selection

In order to solve the optimization problem for BDTD sharing, the optimal sampling rate (r_{ij}) of BDTD seller need to be determined. The sampling rate of each BDTD seller is denoted as $R = (r_{i1}, r_{i2}, \ldots, r_{ij}, \ldots, r_{im})$. R^* denotes the optimal sampling rate of each BDTD seller and can be defined as a Nash Equilibrium (NE) [37]. For each BDTD seller following optimal sampling rate, as long as others do not change their sampling rate R_{-ij}, one BDTD seller cannot improve its own revenue. The existence of NE in the presented problem is proved as follows. Φ_{-ij} is the total satisfaction degree provided by BDTD sellers where the j_{th} BDTD seller is excluded.

$$\frac{\partial U_{ij}(r_{ij})}{\partial r_{ij}} = \frac{\beta_2 B_i \Phi_{-ij}}{ln10\left(1 + r_{ij}\right)\left(\Phi_{-ij} + \beta_1 + \beta_2 log\left(1 + r_{ij}\right)\right)^2} - \varepsilon\alpha_1 \tag{6}$$

$$\frac{\partial^2 U_{ij}(r_{ij})}{\partial^2 r_{ij}} = -\frac{\beta_2 B_i \Phi_{-ij}\left(\Phi_{-ij} + \beta_1 + \beta_2 \log\left(1 + r_{ij}\right) + \frac{2\beta_2}{\ln 10}\right)}{\ln 10\left(1 + r_{ij}\right)^2\left(\Phi_{-ij} + \beta_1 + \beta_2 \log\left(1 + r_{ij}\right)\right)^3} \tag{7}$$

According to (6) and (7), the secondary-order derivative of $U_{ij}(\cdot)$ with respect to r_{ij} is negative, i.e. $\frac{\partial^2 U_{ij}(r_{ij})}{\partial^2 r_{ij}} < 0$. Therefore, $U_{ij}(\cdot)$ is a strictly concave function. The optimization problem for BDTD sharing is a convex optimization problem where NE among BDTD sellers exits.

Since (5) is a convex optimization problem with inequality constraints, the Lagrangian dual function of (5) is defined as

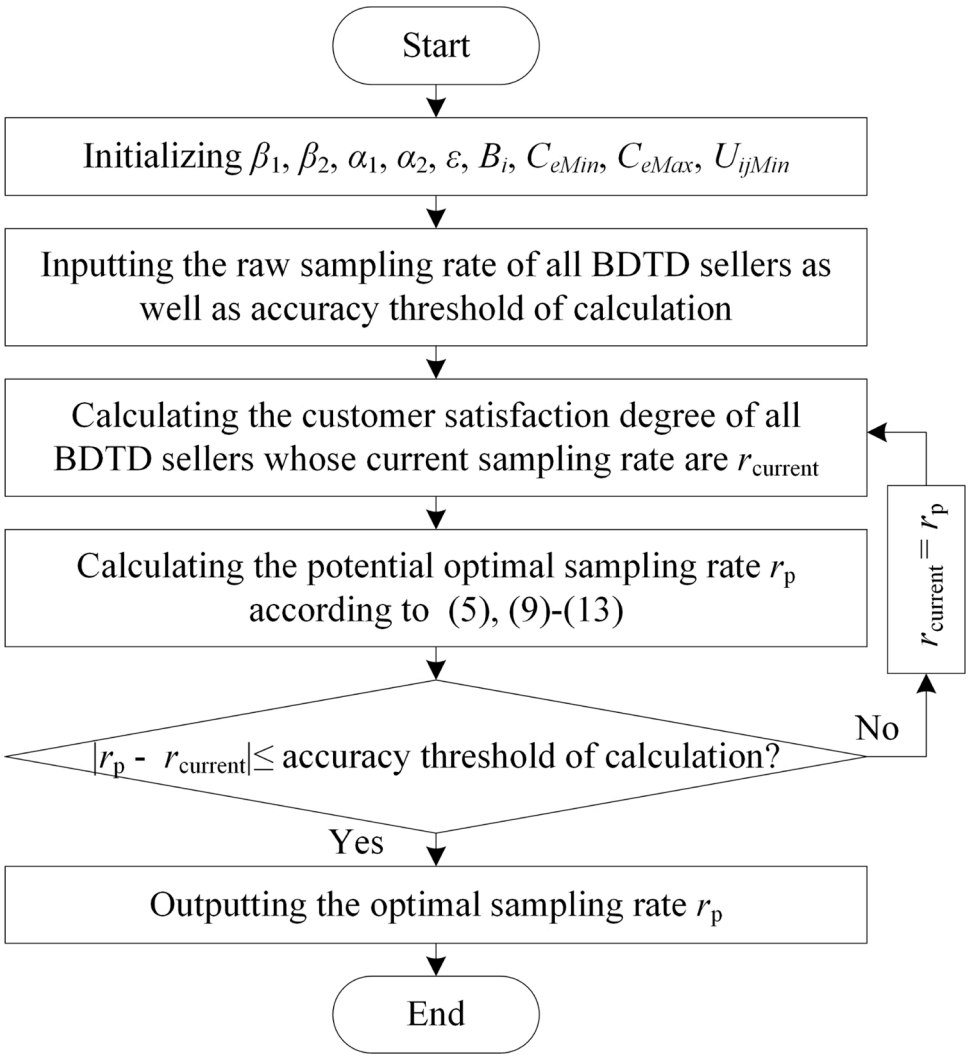

Fig. 6. The flow chart of algorithm for optimal sampling rate selection.

$$L_{ij}(r_{ij},\mu_1,\mu_2,\mu_3)=U_{ij}(r_{ij})+\mu_1(C_{eMax}-\varepsilon(\alpha_1 r_{ij}+\alpha_2))+\mu_2(\varepsilon(\alpha_1 r_{ij}+\alpha_2)-C_{eMin}) +\mu_3(U_{ij}(r_{ij})-U_{ijMin}) \tag{8}$$

where μ_1, μ_2, and μ_3 are Lagrange multipliers. Karush-Kuhn-Tucker (KKT) conditions for the optimization problem for BDTD sharing are set up as (9)–(13).

$$\frac{\partial L_{ij}(r_{ij},\mu_1,\mu_2,\mu_3)}{\partial r_{ij}} = (1+\mu_3)\frac{\partial U_{ij}(r_{ij})}{\partial r_{ij}} + \varepsilon\alpha_1(\mu_2-\mu_1) = 0 \tag{9}$$

$$\mu_1(C_{eMax} - \varepsilon(\alpha_1 r_{ij} + \alpha_2)) = 0 \tag{10}$$

$$\mu_2(\varepsilon(\alpha_1 r_{ij} + \alpha_2) - C_{eMin}) = 0 \tag{11}$$

$$\mu_3(U_{ij}(r_{ij}) - U_{ijMin}) = 0 \tag{12}$$

$$\mu_1,\mu_2,\mu_3 \geq 0 \tag{13}$$

Finally, iteration method is used to obtain the point $(r_{ij}^*,\mu_1^*,\mu_2^*,\mu_3^*)$ satisfying the KKT conditions and the constrain conditions of (5). $(r_{ij}^*,\mu_1^*,\mu_2^*,\mu_3^*)$ is the optimal solution of optimization problem for BDTD sharing. r_{ij}^* is the optimal sampling rate of BDTD seller. μ_k^* for $(k=1,2,3)$ is the optimal shadow variable associated with the optimal solution. The optimal sampling rate selection algorithm is presented in Fig. 6.

6. Evaluation

In order to verify the feasibility of the proposed framework and algorithm, the time sensitivity of our framework is evaluated in Section 6.1 by developing and using an evaluation system which combines Hyperledger Fabric and Cloud. The effectiveness of the algorithm proposed in this paper is evaluated in Section 6.2 through a simulation about selecting sampling rate of welding robot BDTD.

6.1. Time sensitivity evaluation

In order to achieve intelligent process planning of welding robots, which is designed to autonomously select the optimal welding sequence and welding parameters according to welding task [39], a large amount of DT data is required for training algorithm and mining professional knowledge. However, it is difficult for single welding robot to gather enough data only by itself. Welding robots need to share DT data with each other to obtain enough data for training algorithm and mining professional knowledge. For welding robots owned by different users, a secure method is essential for them to share their data with trustless others, which can avoid possible data leakage and reduce transaction risk. In order to evaluate the time sensitivity of our framework, an evaluation system of our framework is developed and used to share BDTD of welding robots, as shown in Fig. 7.

Because we mainly focus on the feasibility of applying our

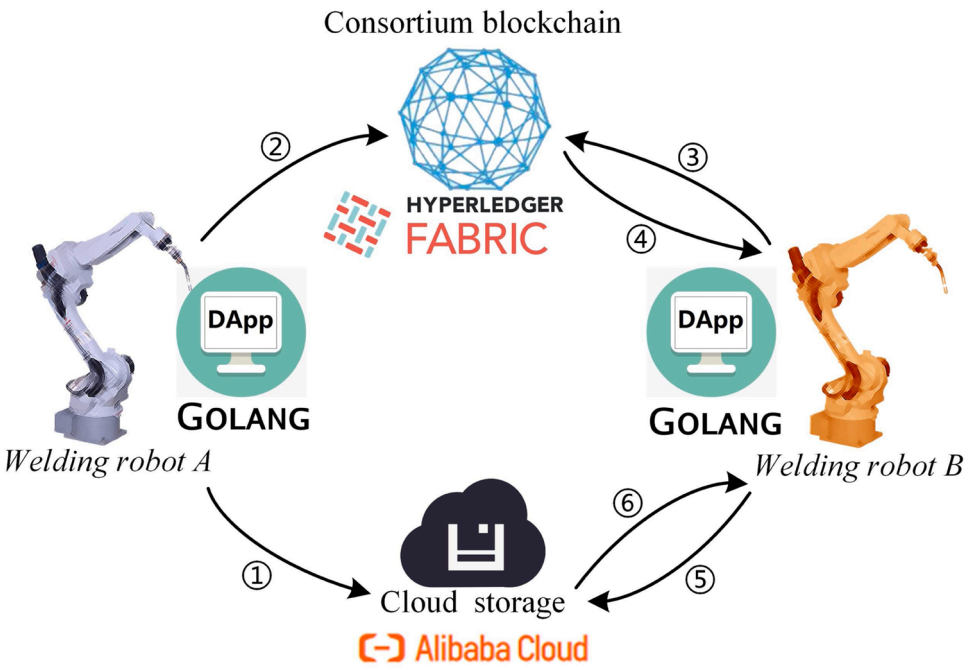

Fig. 7. Evaluation system for secure sharing of BDTD of welding robots.

framework to timely data sharing, the evaluation system is simplified compared with the implementation method in Section 4. The BDTD generated by *welding robot A* are shared with *welding robot B* through DApp developed by using Golang, consortium blockchain based on Hyperledger Fabric [28], as well as Cloud storage based on Alibaba Cloud. The process of BDTD sharing of *welding robot A* is described as follows.

Step 1: The DApp of *welding robot A* generates data file to simulate the sensor data of *welding robot A*. After the hash value of sensor data is calculated, sensor data is uploaded to Alibaba Cloud.

Step 2: A transaction about the timestamp, hash value, and storage location of sensor data is generated and sent to Hyperledger Fabric by the DApp of *welding robot A*. The transaction is recorded in blockchain after endorsing, sorting, packaging and verifying of the peers of Hyperledger Fabric.

Step 3: A transaction about querying the status of the sensor is generated and sent to Hyperledger Fabric by the DApp of *welding robot B*.

Step 4: The latest status which includes the timestamp, hash value, and storage location of the sensor is retrieved in blockchain and sent to *welding robot B*.

Step 5: According to the hash value and storage location of sensor data, the download request of data file is sent to Alibaba Cloud by the DApp of *welding robot B*.

Step 6: The data file of the sensor is sent to *welding robot B*. It is completed that the latest data of sensor of *welding robot A* is shared securely with *welding robot B*.

We tested the the latency of sensor data sharing by recording the time of process from *step 1* to *step 6* takes. The test network of Hyperledger Fabric 2.3.2 [40] was run on virtual machine (ecs.g6.8xlarge, 32 vCPU) of Alibaba Cloud. *Max Message Count* [41], i.e. the maximum number of messages to permit in a batch, was set to 5. Cloud storage was set by using Object Storage Service (OSS) of Alibaba Cloud. The DApp was developed by using Golang 1.16.5.

The latency of sensor data sharing when there are one to ten sensors sharing data at the same time is shown in Fig. 8. The results show that when the number of sensors increases, the latency of sensor data sharing increases. Sub-second latency demonstrates that sensor data can be shared securely multiple times per second.

6.2. Algorithm effectiveness evaluation

The simulation about selecting sampling rate of welding robot's

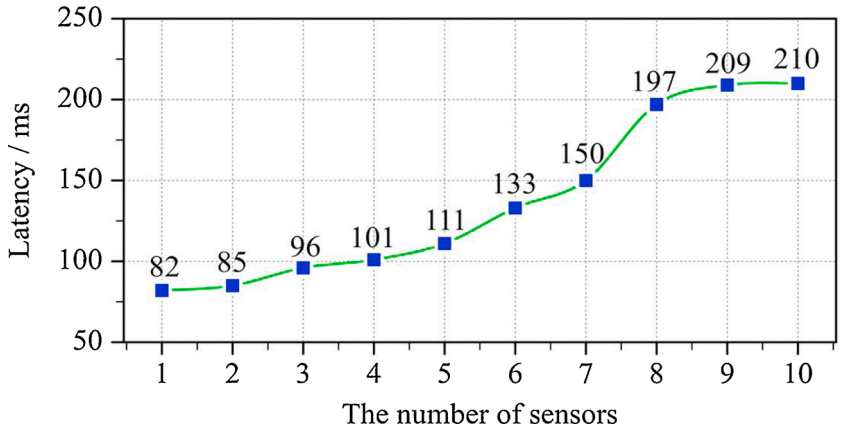

Fig. 8. Latency of sensor data sharing when there are one to ten sensors.

BDTD based on the proposed algorithm is carried out, in which the initial parameters of the simulation are set as β_1=0.7, β_2=0.1, α_1=0.01, α_2=10, ε=1, C_{eMin}=10, C_{eMax}=20, U_{ijMin}=1, respectively. The raw sampling rate R of BDTD sellers are set to different values, R=(100, 200, 1000, 500, 800, 300, 600, 700, 400, 900, 750, 250, 450, 650, 150).

In order to verify the advantages of our algorithm, the comparison with uniform pricing algorithm (UPS) [42], which is a common pricing strategy, is completed. The price of BDTD is set at a uniform value p_i in UPS. p_i is the BDTD price of unit satisfaction degree. Therefore, the satisfaction degree $\xi(r_{ij}) = \frac{B_i}{(n_i \cdot p_i)}$, the max sampling rate $r_{ijMax} = \xi^{-1}(r_{ij})$. The simulation of the optimal sampling rate and profit using our algorithm and UPS when B_i=200, 300, and 400 are carried out respectively.

The optimal sampling rate comparison between our algorithm and UPS is shown in Figs. 9 and 10 . When there are few BDTD sellers, the sampling rate of BDTD sellers using UPS is higher. However, when there are more than six BDTD sellers, the sampling rate of BDTD sellers using our algorithm is higher. With respect to the efficiency of promoting BDTD sellers to choose higher sampling rate, our algorithm is better than UPS in general.

The optimal profit comparison of BDTD sellers using our algorithm and UPS is shown in Figs. 11 and 12 . It can be found that the optimal profit of BDTD seller is steady with the increase of the number of BDTD sellers in UPS. It is caused by very low sampling rates as shown in Figs. 9 and 10. On the contrary, the optimal profit of BDTD sellers using our algorithm decreases gradually with the number of BDTD sellers increases. In the meantime, the optimal sampling rate of BDTD sellers is

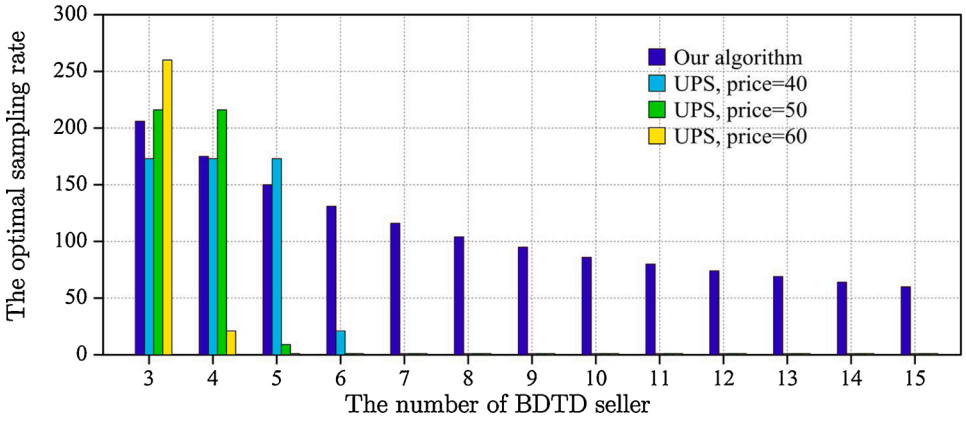

Fig. 9. The optimal sampling rate comparison of our algorithm with UPS in different price.

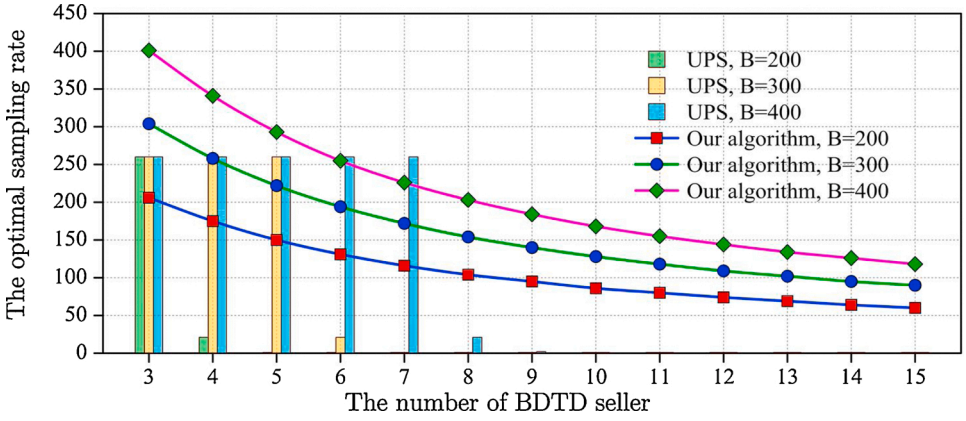

Fig. 10. The optimal sampling rate comparison of our algorithm with UPS in different budget.

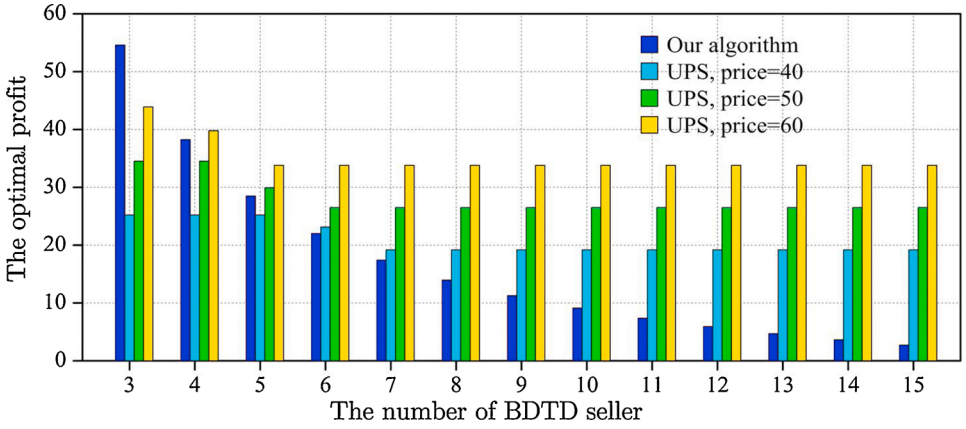

Fig. 11. The BDTD seller's optimal profit comparison of our algorithm with UPS in different price.

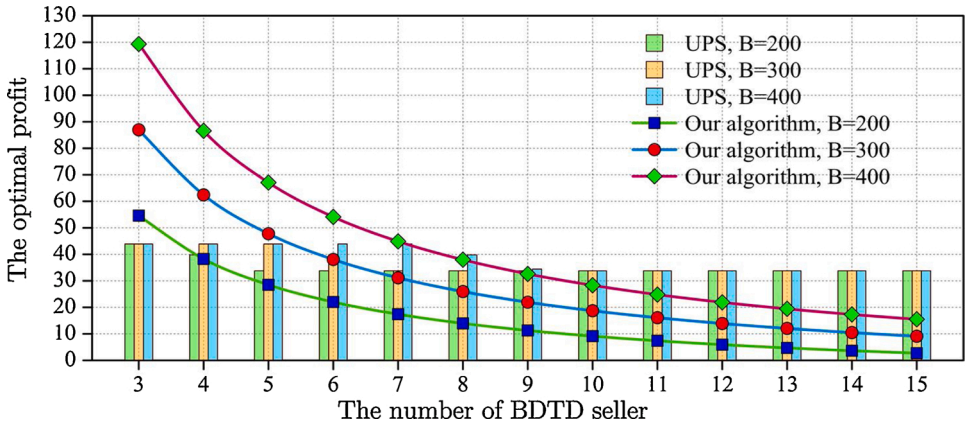

Fig. 12. The BDTD seller's optimal profit comparison of our algorithm with UPS in different budget.

Table 2
Analysis on the satisfaction of essential requirements for secure BDTD sharing.

No.	Essential requirements for secure BDTD sharing	Solutions in our framework
1	Supporting multi-party sharing of BDTD.	Channel is used to achieve business isolation for the participants of BDTD sharing.
2	Supporting exponential growth of BDTD.	BDTD are stored in Cloud which has massive storage space.
3	Supporting BDTD sharing which has high sampling rate.	The rules of generating new block are defined to fulfill transaction speed requirements.
4	Supporting BDTD sharing which includes a wide variety of data.	Original BDTD is stored in Cloud which can provide file storage, objects storage, database storage, and table storage.
5	Supporting verification of BDTD integrity.	The hash of BDTD and transaction records are stored in blockchain.
6	Supporting confidentiality of BDTD.	BDTD are encrypted through cryptography algorithm ECC and PRE.

still at a high level as shown in Figs. 9 and 10.

7. Discussion

Compared with traditional centralized solution, our framework has a higher level of security. On the one hand, due to the distributed mechanism of blockchain, there is no single party that can control the total process of transaction. On the other hand, because of the application of cryptography algorithm, such as ECC and PRE, the confidentiality and privacy of BDTD can be guaranteed in our framework. In terms of essential requirements for secure BDTD sharing presented in Section 2, our framework is analyzed as shown in Table 2. It can be found that all the requirements of secure BDTD sharing listed in Section 2 are fulfilled in our framework.

Compared with the methods presented in [22–25], the advantages of our framework include supporting the exponential growth of BDTD volume, and the sharing of BDTD which need to be shared multiple times per second. The evaluation results demonstrate the potential of our framework in supporting timely data sharing. The simulation results show that our algorithm has better performance than UPS in terms of maximizing the total social benefits, which means that not only BDTD seller can gain a certain profit, but also BDTD buyer can purchase high-quality BDTD.

8. Conclusion

As the impetus of DT, BDTD can promote the application of DT in all lifecycle of equipment. However, due to the lack of secure sharing method, BDTD cannot be widely shared among trustless parties. To solve the problem, this paper integrates blockchain and Cloud technology into secure sharing of BDTD. A framework of blockchain enabled secure sharing of BDTD is proposed, where the hash of BDTD and transaction records are stored in the blockchain, but original BDTD is encrypted, encapsulated and stored in the Cloud. It can relieve the pressure of data storage of blockchain and support the exponential growth of BDTD. The implementation method of the framework is presented, where some rules of generating new block are designed. It can improve the processing speed of blockchain to fulfill the requirement of time-sensitive data. For maximizing the total social benefits of BDTD sellers and BDTD buyers, an algorithm for optimal sampling rate selection of BDTD is presented to solve NE problem. The performance evaluation of our framework demonstrates that BDTD can be shared securely multiple times per second. The simulation results show that our algorithm has better performance than UPS which is a common pricing strategy. The proposed algorithm not only makes BDTD sellers gain most revenue, but also makes BDTD buyers obtain high quality of data which have high sampling rate.

There are still some problems need to be studied in the future. For sensors with sampling rate of one thousand or even more times per second, the throughput and latency of current solutions need to be improved to fulfill the requirements of the real-time sharing of BDTD. Moreover, the process of controlling equipment through DT and BDTD needs to ensure safety with blockchain, which requires less data latency.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 51875323 and Key R&D Program of Shandong Province (Major scientific and technological innovation project) under Grant No. 2019JZZY010123.

References

[1] Tao F, Qi Q. Make more digital twins. Nature 2019;573(7775):490–1.
[2] Lu Y, Liu C, Wang KIK, Huang H, Xu X. Digital Twin-driven smart manufacturing: connotation, reference model, applications and research issues. Robotics Comput-Integr Manuf 2020;61.

[3] Mao W, Tian S, Fan J, Liang X, Safian A. Online detection of bearing incipient fault with semi-supervised architecture and deep feature representation. J Manuf Syst 2020;55:179–98.
[4] Liu M, Fang S, Dong H, Xu C. Review of digital twin about concepts, technologies, and industrial applications. J Manuf Syst 2021;58:346–61.
[5] Liu Z, Chen W, Zhang C, Yang C, Cheng Q. Intelligent scheduling of a feature-process-machine tool supernetwork based on digital twin workshop. J Manuf Syst 2021;58:157–67.
[6] Zhang M, Tao F, Nee AYC. Digital twin enhanced dynamic job-shop scheduling. J Manuf Syst 2021;58:146–56.
[7] Fan Y, Yang J, Chen J, et al. A digital-twin visualized architecture for flexible manufacturing system. J Manuf Syst 2021;60:176–201.
[8] Glatt M, Sinnwell C, Yi L, et al. Modeling and implementation of a digital twin of material flows based on physics simulation. J Manuf Syst 2021;58:231–45.
[9] Gandomi A, Haider M. Beyond the hype: big data concepts, methods, and analytics. Int J Inf Manage 2015;35(2):137–44.
[10] Fabian B, Kunz S, Konnegen M, Muller S, Gunther O. Access control for semantic data federations in industrial product-lifecycle management. Comput Ind 2012;63 (9):930–40.
[11] Shehab E, Fowler C, Gil AR, et al. Enhancement of product information collaboration and access in the aerospace industry. Int J Prod Res 2013;51(11): 3225–40.
[12] Miao YB, Tong QY, Choo KKR, et al. Secure online/offline data sharing framework for cloud-assisted industrial internet of things. IEEE Internet Things J 2019;6(5): 8681–91.
[13] Wang J, Zheng P, Lv Y, Bao J, Zhang J. Fog-IBDIS: industrial big data integration and sharing with fog computing for manufacturing systems. Engineering 2019;5 (4):662–70.
[14] Li Z, Barenji AV, Huang GQ. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Robot Comput Integr Manuf 2018;54: 133–44.
[15] Liang W, Tang MD, Long J, et al. A secure FaBric blockchain-based data transmission technique for industrial internet-of-things. IEEE Trans Industr Inform 2019;15(6):3582–92.
[16] Liu MT, Yu FR, Teng YL, Leung VCM, Song M. Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: a deep reinforcement learning approach. IEEE Trans Industr Inform 2019;15(6):3559–70.
[17] Liu CH, Lin QX, Wen SL. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. IEEE Trans Industr Inform 2019; 15(6):3516–26.
[18] Helo P, Shamsuzzoha AHM. Real-time supply chain—A blockchain architecture for project deliveries. Robot Comput Integr Manuf 2020;63:101909.
[19] Venkatesh VG, Kang K, Wang B, Zhong RY, Zhang A. System architecture for blockchain based transparency of supply chain social sustainability. Robot Comput Integr Manuf 2020;63:101896.
[20] Liu XL, Wang WM, Guo H, et al. Industrial blockchain based framework for product lifecycle management in industry 4.0. Robot Comput Integr Manuf 2020;63: 101897.
[21] Yu C, Jiang X, Yu S, Yang C. Blockchain-based shared manufacturing in support of cyber physical systems: concept, framework, and operation. Robot Comput Integr Manuf 2020;64:101931.
[22] Putz B, Dietz M, Empl P, Pernul G. EtherTwin: blockchain-based secure digital twin information management. Inf Process Manag 2021;58(1).
[23] Suhail S, Hussain R, Jurdak R, Hong CS. Trustworthy digital twins in the industrial internet of things with blockchain. IEEE Internet Comput 2021.
[24] Zhang C, Zhou G, Li H, Cao Y. Manufacturing blockchain of things for the configuration of a data- and knowledge-driven digital twin manufacturing cell. IEEE Internet Things J 2020;7(12):11884–94.
[25] Huang S, Wang G, Yan Y, Fang X. Blockchain-based data management for digital twin of product. J Manuf Syst 2020;54:361–71.
[26] Tao F, Zhang M. Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing. IEEE Access 2017;5:20418–27.
[27] Dietz M, Putz B, Pernul G. A distributed ledger approach to Digital Twin secure data sharing. IFIP Annual Conference on Data and Applications Security and Privacy 2019:281–300.
[28] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the 13th EuroSys Conference, EuroSys 2018; 2018.
[29] Ferretti L, Pierazzi F, Colajanni M, Marchetti M. Performance and cost evaluation of an adaptive encryption architecture for cloud databases. IEEE Trans Cloud Comput 2014;2(2):143–55.
[30] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. Lecture notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Berlin, Germany: Springer-Verlag; 1998. p. 127–44.
[31] Liang K, Au MH, Liu JK, et al. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Trans Inf Forensics Secur 2014;9(10): 1667–80.
[32] He D, Zeadally S. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE Internet Things J 2015;2(1):72–83.
[33] Zhou T, Li X, Zhao H. DLattice: a permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization. IEEE Access 2019;7:39273–87.
[34] Szabo N. Formalizing and securing relationships on public networks. First Monday 1997;2:9.
[35] Tobola A, Streit FJ, Espig C, et al. Sampling rate impact on energy consumption of biomedical signal processing systems. 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks, BSN 2015 2015.
[36] Kurp T, Gao RX, Sah S. An adaptive sampling scheme for improved energy utilization in wireless sensor networks. 2010 IEEE International Instrumentation and Measurement Technology Conference, I2MTC 2010 - Proceedings 2010:93–8.
[37] Lin X, Li J, Wu J, Liang H, Yang W. Making knowledge tradable in Edge-AI enabled IoT: a consortium blockchain-based efficient and incentive approach. IEEE Trans Industr Inform 2019;15(12):6367–78.
[38] Jiao Y, Wang P, Feng S, Niyato D. Profit maximization mechanism and data management for data analytics services. IEEE Internet Things J 2018;5(3): 2001–14.
[39] Shen WD, Hu TL, Zhang CR, Ye YX, Li ZY. A welding task data model for intelligent process planning of robotic welding. Robot Comput Integr Manuf 2020;64:101934.
[40] Available from: https://github.com/hyperledger/fabric.
[41] Available from: https://hyperledger-fabric.readthedocs.io/en/release-2.2/config_update.html.
[42] Liu M, Liu Y. Price-based distributed offloading for mobile-edge computing with computation capacity constraints. IEEE Wirel Commun Lett 2018;7(3):420–3.