IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2019, accepted April 28, 2019, date of publication May 1, 2019, date of current version May 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914223

BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT

LI BAI[1], MI HU[2], MIN LIU[2], (Member, IEEE), AND JINGWEI WANG[2]

[1]School of Accounting, Shanghai Lixin University of Accounting and Finance, Shanghai 201602, China
[2]College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China

Corresponding author: Min Liu (lmin@tongji.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant No. 61573257 and No. 71690234.

ABSTRACT Blockchain is experiencing rapid development and has the full potential of revolutionizing the IoT platform in the industrial field. In this paper, a light-weighted Blockchain-based platform for IIoT is presented to address security, trust, and island connection problem in the process of IIoT ecosystem construction. BPIIoT is comprised of the on-chain network and the off-chain network. All transactions are processed in the on-chain network such as including digital signature based on access control and programmable permission. The off-chain network deals with the storage, complex data processing, and other problems that blockchain cannot solve. The smart contract is utilized as the service contract of consumers and manufacture resources, providing on-demand manufacturing service. Two smart application cases, manufacturing equipment data sharing and maintenance service sharing from smart manufacturing, are implemented to explain the smart contract for equipment maintenance service and status data sharing service throughout maintenance, repair, and operation service network by the BPIIoT.

INDEX TERMS Smart manufacturing, Blockchain, IIoT, smart contract, on-demand.

I. INTRODUCTION

With the development of industrial production towards network and digitalization, smart factories are generating oceans of data from actuators, sensors and other devices. Gartner's IoT industry analysis report predicts that global access to the Internet will increase to 20 billion in 2020 [1]. As the number of connected devices in smart factories grows from billions to hundreds of billions, traditional centralized agent communication mode or Client/Server mode becomes unsuitable for the Internet of Things ecosystem construction. Many existing IoT solutions are expensive because of the high infrastructure (centralized clouds and large servers) and maintenance costs. Research firm Markets predicts that the global IoT market size is expected to grow from $170.57 billion in 2017 to $561.04 billion in 2020 [2]. In addition, all the connected devices have to be verified by the cloud server, and each connection between two devices is realized only through the Internet. As the number of IoT devices continuously increases, a large amount of information produced by these devices will also makes a higher cost. Besides, the connection of devices increases the risk of device manufacturers and smart factories, raising a significant challenge to the privacy, security and fault-tolerant of IoT.

The concept of Internet of Decentralized, Autonomous Things was presented in IBM Whitepaper [3]. IBM believes that a secure connection can be built among heterogeneous systems or open source systems, based on IoT solutions constructed by applying blockchain. Blockchain has been regarded as a disruptive innovation of computing mode after mainframe, personal computer, and Internet. As with cloud computing, Big Data and other new generation of information technology, blockchain is not a single information technology, but relies on existing technologies and ingenious composition and creation of them in order to realize new capabilities. Blockchain is an innovative application mode, in the Internet era, of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and etc. Currently, blockchain has some trial applications in some areas including Finance, Supply chain Management [4], Digital Asset Transaction [5], Internet of Things [6]–[8], and Smart Manufacturing [9].

The birth of blockchain brings about consensus mechanism and distributed network to IoT, which settles the cooperation problem of devices [10]. While distributed network helps nodes realize self-management, and centralized databases are

The associate editor coordinating the review of this manuscript and approving it for publication was Kuo-Hui Yeh.

no longer need, accordingly lower the operation costs of IoT. Furthermore, a peer-to-peer interconnecting provided by blockchain contributes to data communication for IoT, without CPU involved, this kind of distributed computation is able to process billions of transactions. Meanwhile, the computing power and storage capacity of geographically distributed idle devices can be fully utilized to process transactions.

In this paper, a light-weighted blockchain-based Platform for IIoT (BPIIoT) is presented to address security, trust, and island connection problem in the process of Industrial Internet of Things ecosystem construction, with blockchain techniques and smart contract introduced into IoT. Smart contract is utilized as the service contract of consumers and manufacture resources, providing on-demand manufacturing service. To be specific, BPIIoT, as a light-weighted blockchain network architecture, is comprised of the on-chain network and the off-chain network. All transactions are processed in the on-chain network, such as digital signature based on access control and programmable permission. The off-chain network deals with storage, complex data processing and other problems that on-chain cannot solved.

The rest of this paper is organized as follows: Section II introduces basics of blockchain. Section III descripts the relationship of blockchain and IoT. Section IV illustrates the proposed BPIIoT in detail. Section V shows two application cases, and Section VI concludes this paper and discusses the future work.

II. BASICS OF BLOCKCHAIN

Blockchain is the key technology of digital currency represented by Bitcoin, which was first proposed in 2008 by Satoshi Nakamoto [11]. However, there is currently no single definition of blockchain. Broadly speaking, blockchain is a new distributed infrastructure and computing paradigm in a trustless environment, which generates and updates data by using the distributed node and the distributed consensus algorithm, guarantees the security of data transmission and access through the cryptography theory, and has a work-operating mechanism based on the smart contract composed by automation scripts [7]. An integrated blockchain system covers some various technologies, such as data block, digital signature, and timestamp (for storing data), Peer-to-Peer (P2P) network, consensus algorithm (for maintaining the system), mining and proof-of-work mechanism, anonymous transaction mechanism and Bitcoin wallet, Merkle tree, Unspent transaction outputs (UTXO), double-spending and so forth [12]–[14].

A blockchain is a distributed data structure that is replicated and shared among the members of a network [7]. When a transaction begins, a data block is constructed firstly to record the content. Each block is verified by multiple nodes of the network, and the valid blocks are timestamped. A link is established between the blocks, thus generating a chain of blocks, i.e. *blockchain*. Each block in the chain is identified by its cryptographic hash, and each block references the hash of the block that came before it. The record of valid transaction is authenticated by other participants, and is replicated distributed across many nodes around the network. If someone intends to temper the data of a blockchain, more than 51% of the record of transactions need to be modified [15]. That is to say, it is hard to temper the data of blockchain when it reaches a certain size.

In a blockchain network, each user transacts through its own node, these nodes form a peer-to-peer network. Users interact with the blockchain by the use of asymmetric cryptography algorithm. Every signed transaction is broadcasted by a user's node to its one-hop peers. The valid transaction relays continually until it covers the entire network, while invalid transactions are discarded. In the mining process, the validated transactions are packaged into a timestamped candidate block during a certain time interval, the mining node broadcasts the block back to the network [16]. If the candidate block contains valid transactions, and references the correct previous block on the chain as well, then add the block to the chain. If not, the candidate block is discarded. Following elaborates some concepts and technologies of blockchain.

1) DATA BLOCK

All the transaction records are stored in data block, which is comprised of *header* and *body*. The *header* encapsulates the current version, address of the previous block, timestamp, random number, the hash value of current block, the root of Merkle tree (Merkle-root) and other information. The *body* mainly involves transaction counts and transaction details. Each transaction will be stored in block permanently, accordingly, transaction details can be queried. Every transaction is digitally signed by Merkle tree of *body*, thus the transaction is assured to be unforgeable and non-repetitive. Merkle root is generated via the hash process of Merkle tree, and stored in *header*.

2) MINING AND FORK

Data block is generated in the process of mining. Hash of pre-block and total transactions within 10 minutes compose a 256-bit string, and if a random number (nonce) were found in that the hash of string meets a certain condition, the miner achieves the right of accounting of the block, the so-called *proof-of-work* (PoW). Newly generated block broadcasts on the network, other nodes can easily verify the block. Through the PoW, miners compete the accounting right of block and link the block to the main chain, finally miners receive economic incentives as compensation. In this way, the main chain of blockchain is updated. When a fork happens, the fork problem is resolved automatically by the next block. Miners will compute and compare the workload of candidate forks. The nodes adopt the fork that carries the greatest amount of work.

3) TIMESTAMP

Timestamp is the total number of seconds from 00:00:00, 1970/01/01 (GMT) till now. It is usually a character sequence

which denotes uniquely a certain time moment. Blocks of the main chain on the network are strictly chronological. Any node has accounting right of a certain block should attach timestamp to the *header* of the block, accordingly the time of data writing in the block is recorded. Timestamp is the proof of existence of data stored in block, and it guarantees the database of blockchain not to be tampered. Besides, timestamp provides time dimension for the applications based on blockchain.

4) MERKLE TREE

Merkle tree is a data structure of blockchain, which can summarize and verify the existence and integrity of data in block quickly. Merkle tree involves the bottom database in *body*, the Merkle root in *header*, and all branches from the bottom data to the Merkle root. The computing process of Merkle tree is, handling the data of *body* by hash computing, and inserting the generated new hash into Merkle tree, repeating to do so until there is only one root hash left which is denoted by Merkle root.

5) P2P NETWORK

Each node stores a full blockchain and performs data transmission and interaction according to the P2P (Peer-to-Peer) protocol [17]. Different from the centralized network mode, there is no server end, centralized service, and hierarchical structure in the P2P network. Each node has equal status, no specificity, and each node provides services together.

6) CRYPTOGRAPHY

In the definition and construction of block and blockchain, cryptography techniques such as Hash algorithm and elliptic curve public key cryptography are used to ensure the security and integrity of information [18]. These cryptographic techniques are also used to design consensus algorithms based on workload proofs and to identify users.

7) CONSENSUS MECHANISM

In the blockchain, the nodes compete for accounting and the criterion for competition is called the consensus mechanism [19]. The consensus mechanism refers to the algorithms, protocols, and rules that define the consensus process, which includes PoW workload proof, PoS (*Proof of Stake*) equity certificate, DPoS (*Delegated Proof of Stake*) share authorization certificate, distributed consistency algorithm, etc. [20], [21].

The mainstream consensus mechanism of the alliance chain is mostly based on PBFT and its variants, and the rights control of *joining* has greatly improved performance, but at the expense of some of the consensus efficiency, constraints, fault tolerance and other aspects of performance. The choice of consensus algorithm is related to the specific application scenario. Paxos or Raft is applicable to the trusted environment, PBFT is applicable to the license alliance chain, and PoW, PoS, Ripple consensus is applicable to the non-licensed chain [22]. The best design of consensus mechanism is modular (like Notary).

8) SMART CONTRACT

Smart contracts are commitments defined in digital form and agreements by contract participants to enforce these commitments. The essence of the contract terms embedded in hardware and software was first proposed by cryptographer Nick Szabo in 1997 [23]. A smart contract is a stateful computer script running on a blockchain data block. It is event-driven and can process data actively or passively to control and manage smart assets on various chains, accept, store and send value. The combination of blockchain and smart contract is becoming a current research hotspot, such as Ethereum, Codius, and Hyperledger, which have their own programmable contract language and executable infrastructure, and smart contracts are stored on blockchains. Scripts are executed in a distributed manner through blockchain nodes. A state machine system is built by the blockchain consensus algorithm to support the efficient operation of smart contracts [24].

III. BLOCKCHAIN AND IIOT

A. THE PROBLEMS OF IIOT

As an integrated architecture for manufacturing IoT technologies and models, IIoT uses IP-based networks and cloud connectivity to describe machines and product networks that can communicate and share intelligence in industrial environments to optimize relevant industrial operations to eliminate uncertainty and safety in industrial processes. The core of IIoT is to use good data to drive the fusion of the physical world and the virtual world. Digital Twins is a ''secondary world'' composed of physical entities and digital virtual bodies [25]. Through the virtual factory, it can monitor the production capacity, operational efficiency and equipment operation status of the manufacturing site, and manage the plant operation in real time and effectively; in addition, it can also develop, manufacture, sell and analyze the product performance throughout the product life cycle.

The development phase of IIoT includes data collection and storage, production management and analysis, business intelligence and decision making, and business model change [26]. For the IIoT implementation, the most critical issues are the security of the data [27], the trust of network [28], and isolation connection [29].

1) SECURITY OF THE DATA

The seismogenic virus exposed in 2010 caused massive damage to industrial and public infrastructure such as multinational nuclear power plants, dams, and national grids [30]. A reliable IIoT infrastructure ensures that critical computing, network and storage resources are up and running, avoiding unplanned downtime of the equipment. Security means that data is not damaged, not lost, and is not stolen or tampered with. However, most manufacturers believe that additional

security measures will not increase the market value of the device itself, only increase its production costs [31]. As a result, existing IoT devices have long-standing high-risk vulnerabilities such as default passwords and plaintext transmission key. In 2016, the Mira botnet launched a DDOS attack on Dyn, a US domain name resolution service provider, by controlling a large number of IoT devices, causing a large-scale network disconnection in the eastern United States [32]. Such attacks greatly threaten the security of user data and could cause data leakage. Therefore, solving the security of existing IIoT architecture is an urgent matter.

2) TRUST OF NETWORK

After Edward Snowden leaks [33], [34], it is difficult for IIoT adopters to trust technological partners who may give device access and control to certain authorities (i.e., governments, manufacturers or service providers), allowing them to collect and analyze user data. Therefore, trust and anonymity should be at the core of future IoT solutions.

3) ELIMINATION OF THE ISOLATED CONNECTIONS

The interconnected devices inside the plant do not work in isolation, but need to interact with the entire ecosystem. The depth and breadth of the interconnection determine the pattern of the IIoT ecosystem. The connection mode of the Industrial Internet of Things includes device to device, device to cloud platform, device to gateway, cloud platform to cloud platform [35]. Elimination of the isolated connections is a major problem that needs to be solved.

B. APPLICATIONS OF BLOCKCHAIN IN IIOT

In the past decade, with the emergence of blockchain, the idea of combining blockchain and IIoT has gained considerable interest [36]. In fact, there are many similarities between the IIoT and the blockchain, such as a tremendous number of different nodes, frequent and volatile heterogeneous data exchange, high security and privacy requirements, etc. Hence, it is feasible to utilize the blockchain technology to the IIoT system to improve the underlying architecture and solve the above-mentioned issues [37].

There are various existing researches on blockchain-based solutions for IIoT. Considering the security and privacy of data, Wu et al. proposed a new two-factor authentication scheme based on the Blockchain technology to ensure data security [38]. Further, in [39], IoT was combined with the open source Blockchain platform to realize data exchange, and a distributed method was created to improve the security on the equipment level. Based on the Blockchain and Smart Contract, a point-to-point IIoT platform called the BPIIoT was created in [8] to realize data exchange without trusted intermediaries. However, the major drawback that those researches have is that the introduction of the Blockchain technology increases the transmission and computing burden of the IIoT architecture, but the impact on the real-time capability of the industrial environment is not taken into deep consideration. Novo [36] proposes an access control system based on the blockchain technology to manage IoT devices. However, the system is not fully built on a distributed architecture because of the usage of the central management hub. Once the management hub is failed or attacked, IoT devices connected to it become unavailable. Yang *et al.* [40] exploit the consortium blockchain technology to propose a secure energy trading system. But they do not consider privacy issues such as the sensitive data disclosure risk, and thus it cannot guarantee sensitive data confidentiality. The aforementioned systems all adopt chain-structured blockchains in IoT systems, which are overloaded for power-constrained IoT devices. Xiong *et al.* [41] introduce edge computing for mobile blockchain applications and present a Stackelberg game model for efficient edge resource management for mobile blockchain. They reduce computational requirements of mobile devices by leveraging edge computing. Furthermore, [42] describes how the integration of IIoT and blockchain will improve the security and efficiency of various industrial sectors such as supply chain, autonomous vehicle and manufacturing plant equipment. Based on blockchain technology, Liang *et al.* [43] present a trusted and resilient communication architecture for IIoT applications, which can achieve data assurance, resilience and accountability. To ensure the security and privacy of trading data and consumption in the smart grid energy trading scenario, blockchain is used together with several other technologies including multi-signatures, and anonymous encrypted messaging streams in [44]. All of the above works have pointed out that the scalability is a major concern of blockchain-enabled IIoT systems. However, the performance of blockchain systems (scalability, decentralization, security or latency) hasn't been well investigated in these works.

IV. A LIGHT-WEIGHTED BLOCKCHAIN-BASED PLATFORM FOR INDUSTRIAL IOT (BPIIOT)

A. OVERVIEW OF BPIIOT

As shown in IV-B, the light-weighted blockchain-based platform for Industrial IoT (BPIIoT) is based on a blockchain network embedded with smart contracts. Smart contracts serve as an agreement between service consumers and manufacturing resources, who provide the on-demand manufacturing services, to support the development of Decentralized end-to-end manufacturing Applications (DApps). We aim to build a decentralized system with nodes supervising each other, create a trusted data resource trading platform.

The deployment and implementation of blockchain technology requires the participation of multiple nodes. Under the conditions of the Internet of Things, the computing power of each intelligent device is very limited. Compared with the traditional blockchain mining nodes, the Hash computing capability is even Less than one thousandth of the GPU system. In practical applications, the power consumption of IoT devices is also a difficult problem. The existing blockchain technology cannot be directly applied to the industrial Internet of Things, the BPIIoT platform is

designed as a lightweight network architecture consisting of an On-Chain network and an Off-Chain network to reduce network load and latency. All transactions are carried out in the on-chain network, such as digital signatures based on admission control, programmable licenses, etc. Correspondingly, some problems, such as storage, complex data processing, etc., can be solved under the off-chain network. The on-chain network avoids the participation of third parties by introducing Secure Multi-Party Computation (SMPC). Data query and calculation are distributed on different nodes, which participate in the calculation without leaking information. In addition, each node in the sub-network is not required to repeat the calculation and storage of data to meet higher computing requirements.

B. ON-CHAIN NETWORK

The on-chain network consists of a normal node and a verification node. Normal nodes do not participate in the bookkeeping record, that is, they do not participate in the calculation of the PoW. They only encrypt and transmit the data and broadcast the data as a transaction to the entire blockchain network. The verification node is specially deployed for the calculation of PoW, and has strong computing power. It is responsible for access control management and clearing payment of normal nodes. These verification nodes can be composed of multiple different objects. Networked service providers can use mainstream PC servers to build these nodes. Since these verification nodes themselves do not store user data, there is no possibility of user data leakage and exploitation.

The primary function of the on-chain network is to provide communication services, and the data transmission between the nodes through the blockchain. There are two ways to store data on a blockchain, one is to add data to a transaction, such as bitcoin, and the other is to write data into a contract, such as Ethereum. Both store data by sending transactions to the blockchain, and these transactions include transferring information and any other data. When the transaction is completed, the data contained in the transaction is open to the blockchain network. The on-chain network supports multiple blockchain services, such as incentives, right management, transaction verification, asymmetric encryption, and so on.

C. OFF-CHAIN NETWORK

In the off-chain network, data storage and calculation processing are mainly performed. The blockchain is not a general-purpose database. The off-chain network has a decentralized off-chain database, namely Distributed Hash-Table (DHT) [45], which can be accessed by the blockchain. Blockchain save the data's references instead of the data itself. The data is encrypted in the blockchain and stored in the DHT, and the access control protocol is written on the blockchain to ensure the security, and the off-chain network provides an API interface to read the data in the DHT.

The nodes in the off-chain network form a distributed database. Each node allocates a certain percentage of

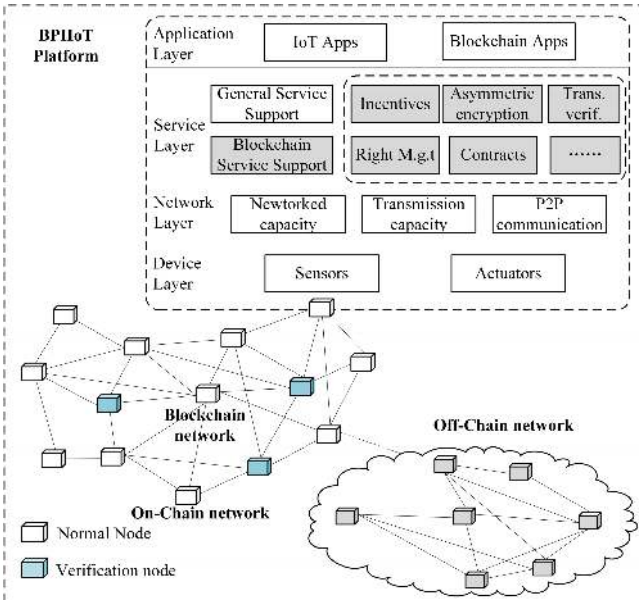


FIGURE 1. The light-weighted blockchain-based platform for industrial IoT (BPIIoT).

encrypted data according to shares, thus ensuring the confidentiality and fault tolerance of the calculation process. Kademlia DHT protocol [46] based distributed storage can help the storage of shares.

In terms of computational processing, the off-chain network ensures the correctness of code execution and does not leak raw data to any nodes. In addition to the superiority of privacy, the off-chain computing network can be broadcasted through the blockchain after complex calculations.

D. IOT UNIT

The IoT unit, a node in on-chain network, is the most important component of BPIIoT, which provides a plug-and-play solution as a bridge between machine/equipment and blockchain networks. Through the IoT unit, the machine/equipment can upload operation data to the blockchain, send transactions to the related smart contracts, and receive transactions from other nodes in the blockchain. Each IoT unit consists of four layers, namely the device layer, the network layer, the service layer, and the application layer. The device layer includes mainly sensors and actuators deployed in the industrial field, and is connected to the machine or equipment through the interface board. The node communicates with the blockchain through the network layer. The service layer consists of General Service Support and Blockchain Service Support. GSS includes device manager, I/O interface, controller service, and the functionality of the microcontroller. BSS covers incentives, asymmetric encryption, transaction verification, rights management, contracts, and so on.

E. DISCUSS

The proposed BPIIoT can address the three major issues of IIoT presented in section III. A. We will discuss as follows.

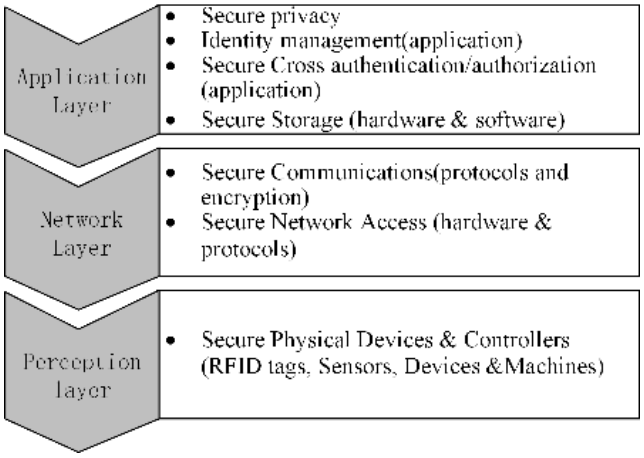


FIGURE 2. The threat of the IIoT mainly comes from the application layer, the network layer, and the perception layer.

In terms of security, the threat of the IIoT mainly comes from the application layer, the network layer and the perception layer, as shown in Figure 2. The blockchain will have an important impact on the IIoT by virtue of its peer-to-peer, open and transparent, secure communication, difficult to tamper with and multi-party consensus. Multi-center features will reduce the high cost of operation and maintenance of the centralized architecture. The characteristics of information encryption and secure communication will help protect privacy. Identity, rights management and multi-party consensus can help identify illegal nodes and prevent malicious attacks in time. We will present the data security and privacy strategies in detail in section IV.

In traditional IIoT, the trust problem between components can be solved with the help of digital signature and access control mechanisms. Control over resources distribution and finished products can be carried out using a database accessible to all components. However, those solutions are quite complex and require the deployment of complex infrastructure to provide fault tolerance, performance and availability. The BPIIoT provides a simpler solution for this problem, which uses smart contracts for processing and storing information related to the interaction between all components, eliminating mistrust between the parties.

For the communication problem between IoT heterogeneous devices, the blockchain uses P2P networking technology and hybrid communication protocol to establish a decentralized trust and autonomous system between devices, which greatly improves the stability and reliability of the Internet of Things.

V. DATA SECURITY AND PRIVACY

According to CIA requirement [47], we need to make sure that our architecture have to meet three requirements: confidentiality, integrity and availability. In this section, we consider secret sharing mechanism, data access based on the Secure Multi-Party Computation to guarantee data security and privacy.

A. THE SECURE MULTI-PARTY COMPUTATION

The growth of the Internet has triggered tremendous opportunities for cooperating computation that could occur could occur between mutually untrusted parties [48]. SMPC refers to the problem that two or more users can cooperate to perform a certain computing task under the premise of ensuring to protect the private information in an untrusted network. SMPC is the basis for cryptographic protocols such as electronic elections, threshold signatures, and electronic auctions. Scholars have done a lot of research on the efficiency of secure multi-party computing protocols, the formal definition of secure multi-party computing, the expansion of new application environments, and the construction of new secure multi-party computing protocols.

Equation (1) represents the mathematical model of SMPC, which includes k users who do not trust each other in the distributed network. The secret input corresponding to user U_j is represented by x_i, and the corresponding output is represented by y_i. These k users perform function F together.

$$F : (x_1, x_2, \ldots, x_n) \rightarrow (y_1, y_2, \ldots, y_n) \tag{1}$$

In the calculation process, for any user U_i, in addition to obtaining the output y_i, no information can be obtained from other $U_j (j \neq i)$ users. Generally exist $y_1 = y_2 = \ldots = y_n$, Thus the function can be simplified, expressed as $k : (x_1, x_2, \ldots, x_n) \rightarrow y$.

The SMPC basic protocol consists of a basic functional security protocol that could be called frequently by higher layer protocols as an underlying tool, such as Oblivious Transfer Protoco (OTP), Multiplication Protocol (MULP), Secure Two-Party Scalar Product Protocol (STSP), Permutation Protocol and Secure Comparing.

B. SECRET SHARING MECHANISM

Secret sharing is a common cryptographic technique that separates secrets and stores them separately. This concept was first proposed by Shamir [32] and Blakley [49]. We consider using the Threshold Secret Sharing to prevent the secret from being too concentrated in the hands of one party, and to reduce the risk of secret disclosure. Assume that in a threshold cryptosystem, n represents the number of all participants, and t+1 represents the minimum number of participants required to decrypt a secret processed with threshold encryption. For example, for a secret s, shared by n participants, at least t+1 participants can recover the shared secret s, and any subset of t participants cannot know the secret. The Linear Secret-Sharing Scheme (LSSS) divides a secret into multiple shares, and these shares constitute a linear combination of the secret. The Shamir Secret Sharing (SSS) [12] uses polynomial interpolation to ensure its safety on a finite field.

For the secret s, it can be represented by the t-degree polynomial$f(x)$:

$$f(x) = l_0 + l_1 x + \cdots + l_t x^t \tag{2}$$

$$l_0 = s, l_i \sim U(0, p-1) \tag{3}$$

Then the shares can be expressed as:

$$\forall i \in \{1, \ldots, n\} : [s]_{p_i} = f(i) \tag{4}$$

Given t+1 shares, you can use Lagrangian interpolation to reconstruct $f(x)$, if $= f(0)$, the secret s recovery. Since the SSS is linearly homogeneous, the scalar operation of adding and multiplying the shares are directly performed. Taking the addition operation as an example, the process is expressed as follows:

$$\mathrm{c} \times \mathrm{s} = \text{ reconstruct } \left(\left\{c[s]_{pi}\right\}_{i\in n}^{t+1}\right) \tag{5}$$

$$s_1 + s_2 = \text{reconstruct}\left(\left\{[s_1]_{pi} + [s_2]_{pi}\right\}_{i\in n}^{t+1}\right) \tag{6}$$

The multiplication of the two secrets s_1 and s_2 is more complicated. If a participant tries to calculate the multiplication of two secrets, a 2t degree polynomial will be obtained, which requires a polynomial reduction step (2t→t), and adds a constraint that majority users are honest to ensure the privacy and correctness of the results (i.e. t<n/2).

C. DATA ACCESS

In the BPIIoT system, the off-chain network and the on-chain network are interconnected. Data access is achieved through a global dictionary, three different decentralized databases that can be accessed through the global dictionary, Public Ledger, DHT and MPC. Identities are stored on the Public Ledger, and the off-chain database (DHT) storage and computing(MPC) requests are routed through the blockchain. The data query and calculation are distributed. The data is stored on different nodes. These nodes participate in the calculation, and the introduction of Secure Multi-Party Computation (SMPC) in the blockchain network can avoid leaking information.

The definition of shared identity is an extension of multiple identifiers and their semantics, defining access control rules for metadata and the nature of data (public or private data) represented by 2n+1 tuples.

$$\text{SharedIdentity}_p = \left(\text{addr}_p, p\, k_{sig}^{(p_1)}, p\, k_{s(g,\ldots,}^{(p_2)}, \ldots, p\, k_{sig}^{(p_n)}\right) \tag{7}$$

The public transaction is stored on the public ledger after blockchain verification. Since the predicate with the shared identifier and management access control is stored on the ledger, the blockchain can access any off-chain resources. For metadata involving privacy, the under-chain network can act as a trust validator. For example, Bob needs to use Alice's height data. Alice allows Bob to use her height information for joint query calculations, not knowing her specific height. At this point Alice can call a smart contract, using the MPC Predicate, MPCl['alice_height']=alice_height to share her height data, and Bob refers to the data for calculation without knowing Alice's specific height. The MPC predicate creates a data owner Alice, and a data user Bob with restricted access rights. The MPC predicate is stored on the blockchain, which defines the identity-related information (the address of the shared identity list and the reference permissions of the data) that can be used to verify access rights. Other private metadata is stored in the off-chain network via DHT.

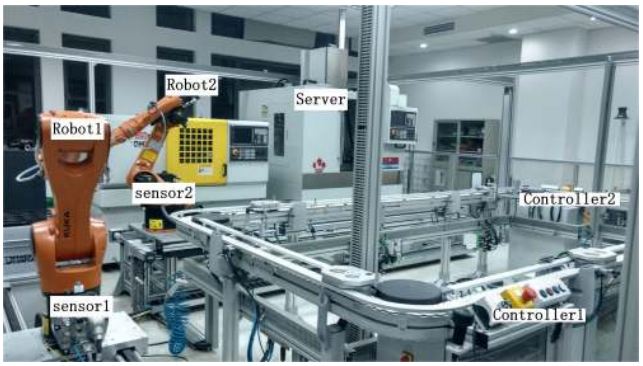


FIGURE 3. An automatic packaging platform based on the proposed BPIIoT.

The data under the chain is stored in the DHT, and its data access mode is similar to that of the public ledger. By default, data is locally encrypted and only signed entities can request to send back data. Otherwise, use $DHI'.\,\text{set}(l\varepsilon, v, p)$, where k is the key, v is the value of the data, and p is the predicate, Data access via key k is only possible when p is satisfied.

The usage of MPC is similar to DHT. Share data v when $MPC \cdot \text{set}(k, v, p)$ is executed, where k is the key, v is the value of the data, and p is the predicate, shares are allocated to potential computing parties and stored locally. The predicate p is used to determine which participant can reference the data for calculation without leaking v, which is $v_{Twf} \leftarrow MPC|k|$. By default, only the original owner can request the original data via $v \leftarrow MPC$. declassif $y(k)$ request. Any participant can reference the data for calculation.

VI. APPLICATION CASES

Figure 3 shows an automatic packaging platform based on the proposed BPIIoT architecture. There are two sensors connected with two robots to collect state data, such as temperature, vibration frequency and so on. The server is responsible for verifying transactions on the blockchain, and the verified transactions are packaged to form new blocks. The following application cases are implemented on this platform.

A. BPIIOT FOR SMART PREDICTIVE MAINTENANCE

In the field of smart manufacturing, the predictive maintenance service application with smart contract in a smart factory, as shown in Figure 4, can be developed based on the BPIIoT platform to record and manage the equipment information and the maintenance process, such as equipment type, equipment details, production dates, parts information, status data, maintenance records and inventory.

Sensors with different functions and types are installed on the production equipment. Through the Prognostic and

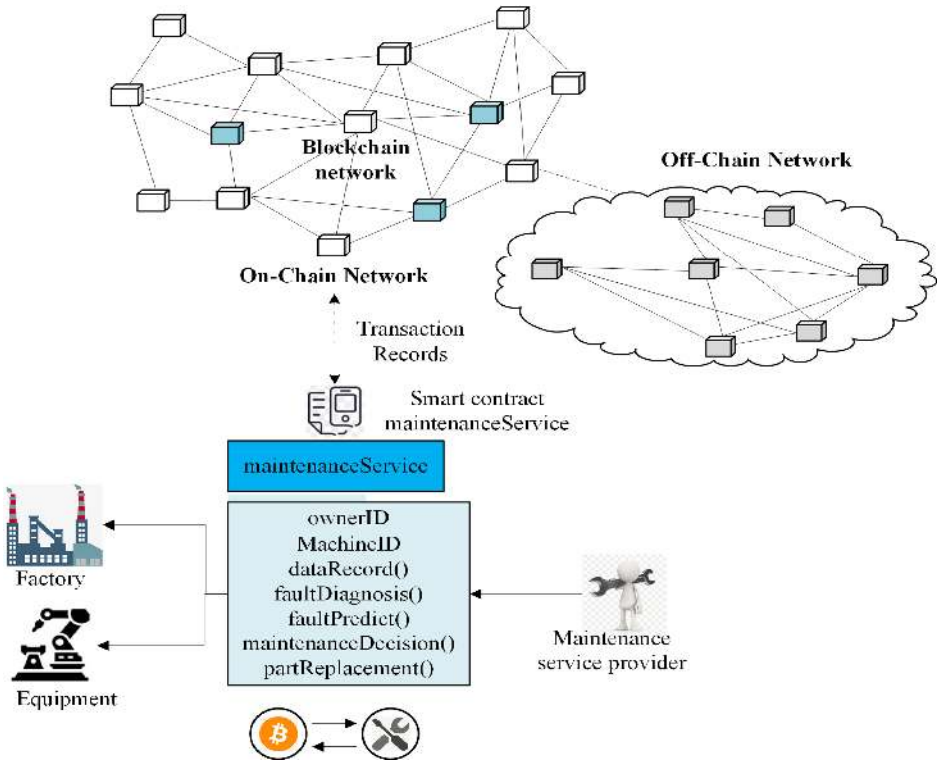


FIGURE 4. The predictive maintenance service application with smart contract in a smart factory.

Health Management (PHM) and self-service application of the BPIIoT platform, the equipment state parameters can be online monitored at different positions such as the temperature, vibration frequency, pressure, displacement. The state parameters and maintenance data are recorded in a node from the on-chain network. The equipment can request for maintenance services, replenishment or replacement of spare parts issued by the service provider/supplier. As shown in Table 1, by creating a smart contract maintenanceService, the equipment maintenance transaction between the manufacturer and the service provider is automatically executed, and the smart contract as an agreement between the device and the maintenance service provider, can process the maintenance service request or process part replacement instructions

In the case of Ethereum, the smart contract is the code stored in the blockchain. The contract state is stored in the blockchain. The contract code is executed through the blockchain node, which is equivalent to the enforcer of laws and regulations in the process of commercial transaction and supervision and management. And store the contract calculation result through the distributed consistency algorithm in the blockchain to update the contract status. The blockchain is equivalent to a transaction-based state machine that changes the state of the state machine through transactions from the initial state. State refers to any data that can be represented by the computer. The state transition can be expressed as follows: $\sigma_{t+1} = \gamma\ (\sigma_t, T)$.

Where γ is the state transfer function of the blockchain; σ_t is the state of the blockchain at time t; and T is the transaction. In the blockchain system, transactions are collected into blocks, each of which can be replaced by its own hash value. Each block contains the hash of the previous block, the set of transactions, and the state of the block itself. The block is connected to the chain by storing the hash of the previous block. Overall, $\sigma_{L+1} = \gamma\ (\sigma_L, B)$ B $= (T_0, r_1, \ldots)$, $\sigma_{t+1} = \gamma\ (\ldots \gamma\ (\gamma\ (\sigma_2, T_0)\ , T_1)\ , \ldots)$.

The blockchain stores all transactions in the block for easy traceability. Like Ethereum, the latest state of the blockchain is stored in the MPT (Merkle Patricia Tire), which instantly generates a summary of the latest status. You can quickly find the needed information based on Key.

In maintenanceService, two state parameters of pressure and vibration frequency are selected. The controller service monitors the temperature and vibration frequency at each critical position of the equipment, and defines different rules to determine whether to execute the maintenance service request or component replacement instruction. When the vibration frequency of the device exceeds a given threshold a certain number of times, the controller service sends an equipment service request, that is, the transaction is sent through the *requestService* function of the *maintenanceService* (between the device and the service provider). Similarly, when the temperature of a component on the device exceeds a given threshold a certain number of times, the spare part replacement command is triggered, and the device sends the

TABLE 1. Smart contract: Maintenance service.

Smart contract: maintenanceService

Input: addr1 - unit public address
addr2 - public machine address
addr3 - public serviceProvider address
T - temperature
V - vibration frequency

Output: call transaction

```
1: TempCount = 0
2: TempThreshold = 200
3: TempCountThreshold = 1000
4: VibraCount = 0
5: VibraThreshold =100
6: VibraCountThreshold = 1000//initialization
7: if (V > VibraThreshold) then
8:     VibraCount = VibraCount+1;
9: end if
10: if (T > TempThreshold) then
11:    TempCount = TempCount+1;
12: end if
13: if (VibraCount > VibraCountThreshold) then
14:     call_transaction with addr2
15:     VibraCount = 0; //reset the VibraCount
16: end if
17: if (TempCount > TempCountThreshold) then
18:     call_transaction with addr1
19:     TempCount = 0; //reset the TempCount
20: end if
21: end
```

transaction through the *orderPart* function of the smart contract *maintenanceService* (between the equipment and the service provider), and passes the token to pay for spare parts.

The transaction is stored in a member variable, and the contract method can be called to query the contract or change the state of the contract. Through the Ethereum client (geth) deploying the smart contract maintenanceService on the blockchain network and assigning an address to it, a private blockchain network is established, and any user in the network who knows the contract address and interface can send transaction through the contract. All operations that change the state of the contract require the creation of a transaction in the blockchain. When the transaction is sent to the blockchain network, it is written to a block along with other outstanding transactions. After the miners verify the validity of the transaction, they form a consensus in the block and broadcast the new block to the entire network. When the transaction is ''mining'', the contract is executed

B. BPIIOT FOR SHARING SERVICE OF EQUIPMENT STATUS DATA

In the traditional production environment, the status data of manufacturing equipment is complex and stored in independent systems [50]. These systems may belong to the different service providers. Manufacturing companies maybe have no direct control over these equipment status data and cannot understand true value of the massive amount of data. For example, equipment operation data and maintenance records are stored in the equipment manufacturer or maintenance service provider's server. Once the service provider is replaced, historical data is lost and broken, which is not conducive to continuous supervision of the manufacturing equipment and management and maintenance of the whole life cycle. The E-chain can support manufacturing companies to achieve multi-party coordination of supply chain, intelligent production management and distributed production collaboration, and promote the sharing of research and development technology, production equipment and manufacturing services. Among them, the sharing of equipment includes not only the sharing of equipment capacity, but also the sharing of equipment status data. Status data sharing makes research and development technology, manufacturing and distribution audits more effective, which helps production companies reduce operating and manufacturing costs.

In the blockchain-based manufacturing equipment data sharing model shown in Figure 5, the manufacturing equipment in the factory is registered after the Ethereum smart contract registration; the data is verified using multi-point consensus and encryption technology to ensure data consistency and security; the validated data, which are organized into a standardized readable and writable data format by big data and AI technology, are stored in the off-chain database, while a summary index is generated and be sent to the on-chain network. The contents of the block record information such as data ownership and browsing permissions. In the BPIIoT, the access rights of different nodes are defined through the blockchain, smart contracts are applied to send transactions, which support the equipment nodes to share data with other nodes (service providers, smart factories or third-parties). PoW is introduced to incentives in the form of tokens, the transaction can contain binary data and tokens to form a peer-to-peer network with private, central, open, transparent and other features.

1) NODES AND TRANSACTION

Network nodes are divided into two categories: equipment nodes (data contributors) and service provider nodes (data beneficiaries). The software components of each node are the same, including administrator, back-end API library, Ethernet client and database, Ethernet client provides functions such as account management, mining, transfer, smart contract deployment and execution. After registering through a smart contract, the node participates in the network activity as a unique digital identity. It has an external account and a contract account that stores the code (shares an address space). The address of the external account is determined by the public key. The address of the contract account is determined when the contract was created. Each account has a token balance that can be changed by sending it a transaction with a token.

The equipment status data and the digital asset record are stored in the blockchain network. The transaction information includes the registration alias of the equipment (for

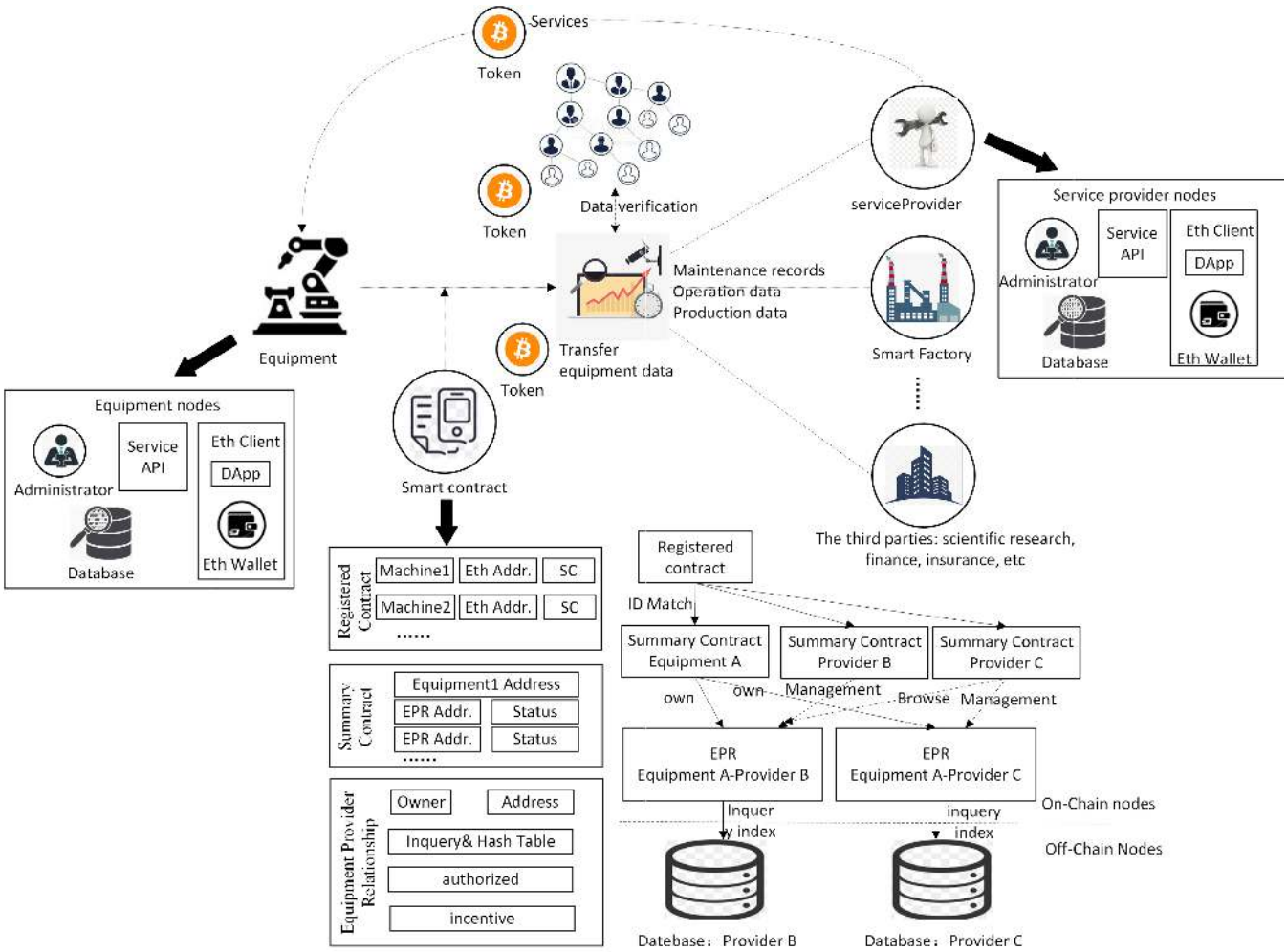


FIGURE 5. The blockchain-based manufacturing equipment data sharing model.

privacy protection), the data type, the metadata tag of the original transaction data, the complete metadata index, and the transaction record, transaction encrypted link, timestamp generated by the transaction. All information is encrypted and digitally signed to ensure authenticity and accuracy.

2) SMART CONTRACT TYPE AND FUNCTION

Node management and API applications are implemented through smart contracts that automatically track specific state changes, such as changes in access rights, and updates to data records. A generic smart contract template is formed based on common business models and processes in different business areas. This article defines the Register Contract (RC), the Summary Contract (SC), and the Equipment Provider Relationship (EPR). Use smart contracts as assets on the chain to achieve process management over the life cycle of the contract (submission, deployment, use, cancellation).

The RC maps the participant's identity string to the corresponding Ethereum address, supports registration of a new identity or changes an existing mapping relationship; causes the identity string to form a mapped address with the blockchain, finds and matches the corresponding SC contract.

The SC contains a list of EPR contract indexes, indicating that all nodes participate in the business with the history of other nodes. For device nodes, the SC contract stores all service provider indexes that have business relationships with the node; for service provider nodes, SC contracts are stored an index of a device that has provided a service or an index of a third-party organization that the device has authorized to share data. An SC contract supports a user notification function; a state variable of a device-server relationship indicates a status of the relationship, such as "whether newly established," Waiting for update", "Device authorization"; device nodes can accept, reject, delete relationships, decide which data records to authorize to share.

The EPR contract defines a data pointer combination and its associated access permissions to identify data records held by the service provider. each pointer consists of a query string that returns a subset of the data, the query string is labeled the hash of the data subset ensures that the data is not tampered with; the hash table can match the query address with the list of additional query strings to share data records with other nodes.

Use the MPR contract to build the relationship between the device and the service provider, correlate the device's data records with licenses, data pointers, and enter them on an external database. Service providers can add new data records to devices, and devices can authorize sharing of data records between service providers. Participants will automatically receive notifications and verify before operating changes, ensuring that each participant is informed and involved in the maintenance of data records. The public key encryption algorithm is used to perform digital identity management on the network node, and the digital identity of the node is matched with the Ethereum Address. After the blockchain network confirms the command, the Off-Chain devices and service providers' respective databases are updated synchronously to ensure data consistency.

3) INCENTIVE MECHANISM

Introduce the mining and reward mechanism of blockchain, and encourage data beneficiaries such as service providers or third-party organizations to contribute computing power as miners, use workload proof mechanism to build consensus, and form a trusted blockchain data sharing network. The service provider or third-party organization participates in the management of the blockchain network, and can obtain the corresponding reward, that is, the device grants its data access authority. The MPR contract has a built-in mining bonus function, and the service provider adds a bonus query to all transactions that are sent out to update the MPR contract.

If the block containing the record of the updated transaction is dug out, the mining bonus function assigns ownership of the reward query to the miner, after which the miner receives the award by sending a request to the corresponding service provider database administrator. The distribution of data and value in the network is achieved by issuing Token tokens, as shown in table 2 for an example of a Token issuance contract. After authorization by the device, the authorized party obtains read and write access to the device data. For example, the device node obtains the Token reward by uploading the data; the service provider node and other nodes can also obtain the Token reward by verifying the uploaded device data; the Token obtained by the device node can be used to purchase the maintenance service, etc.

4) SERVICE PROVIDER

Service providers include equipment manufacturers and maintenance service providers. The maintenance service provider can provide a more complete equipment health management plan, formulate a more efficient and reasonable maintenance scheduling plan and establish a complete evaluation and evaluation standard system. For equipment manufacturers, analyzing equipment operating data and production data can help improve the process and accelerate the development cycle, which can bring about the improvement of the efficiency of the whole life cycle, which can bring about the transformation of business models from selling machines to selling services, personalization and industrial chain finance.

TABLE 2. Contract token: Data sharing.

Contract token: data sharing

```
Input: Addr1 - address public miner
       Addr2 - address receiver
       Amount – transaction amount
Output: Balance - mapping (address => unit) public balances
1: Addr1 = msg. sender//initialization
2: if (msg. sender!= Addr1) then
3:   return
4:     else if
5:       balances[receiver] += amount// mint function
6: end if
7: if (balances [msg. sender] < amount) then
8:    return
9:     else if
10:      balances [msg. sender] -= amount
         balances[receiver] += amount
          event transfer (address from, address to, unit amount)//
          transfer function
11: end if
12: end
```

5) SMART FACTORY

Through the internal information system (such as SCADA, ERP, PDM, CRM, etc.) and the device data sharing network for API docking, you can master all the data of the equipment in the factory, realize online operation and monitoring; machine equipment networking can provide real-time feedback Data, and use the computing power of the cloud to optimize equipment operations, adjust production schedules in a timely manner, improve efficiency and reduce costs.

6) THIRD-PARTY

Blockchain and multi-party computing support sharing production data of factories without leaking secrets, providing data foundations for statistical research for universities and research institutions, helping government departments to coordinate production resources, plan production capacity, and provide production plans and recommendations.

The device data sharing model keeps the private information in the account of the device node. The running data, maintenance records and production data of the device are stored in the database under the chain. After the anonymization process, the data index is extracted and transmitted to the blockchain network. Other nodes use smart contracts to capture relevant information and perform intelligent big data analysis and mining through big data and artificial intelligence.

VII. CONCLUSION AND FUTURE WORK

This paper elaborates the concept definition, technical principle and infrastructure of blockchain, and proposes a light-weighted BPIIoT to support the development of

decentralized, end-to-end manufacturing applications. The BPIIoT platform is based on a blockchain network embedded with smart contracts. Smart contracts serve as an agreement between service consumers and manufacturing resources to provide on-demand manufacturing services. In order to reduce the load and delay of the network, the BPIIoT platform is designed as a light-weighted network architecture consisting of an on-chain network and an off-chain network. All transactions are carried out on the on-chain network, such as digital signature based on admission control, programmable licenses, etc., the off-chain network handles problems that cannot be solved by blockchain technology, such as storage, complex data processing, and so on. Several basic protocols for secure multi-party computing are described, and data sharing mechanisms and data access methods are studied. Aiming at the interconnection problem between the on-chain network and the off-chain network, the identification management method of the blockchain and the corresponding link protocol are proposed. Through the BPIIoT platform, smart devices in smart factories can perform decentralized, trusted, end-to-end network interactions and transactions, helping to open up the data channels of the IoT horizontal industry chain and vertical IoT devices, establish and maintain the consensus of the industrial IoT ecosystem, promote the use of data throughout the ecology. Finally, taking the smart maintenance and data sharing of the equipment as two use cases, the application of BPIIoT is verified and analyzed.

We describe two applications of the proposed BPIIoT platform based on smart contract and blockchain. We look forward to focusing on research in the use of blockchain to meet the legislative standards for industrial application.

ACKNOWLEDGMENT

(Li Bai and Mi Hu are co-first authors.)

REFERENCES

[1] M. Hung. *Leading the IoT*. [Online]. Accessed: Feb. 21, 2019. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[2] *Internet of Things (IoT) Market*. Accessed: Feb. 22, 2019.[Online]. https://www.marketsandmarkets.com/PressReleases/iot-m2m.asp

[3] *Device Democracy: Saving the Future of Internet of Things*. Accessed: Feb. 21, 2019. [Online]. Available: https://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/

[4] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[5] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[6] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *Proc. 21st Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2018, pp. 321–329.

[9] L. Du, L. Chen, L. Zhang, L. Dai, and Y. Shen, "Security architecture based on blockchain for smart cloud manufacturing," *Inf. Technol. Netw. Secur.*, vol. 37, no. 11, pp. 34–38, 2018.

[10] F. Zhang, M. Liu, Z. Zhou, and W. Shen, "An IoT-based online monitoring system for continuous steel casting," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1355–1363, Dec. 2016.

[11] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Feb. 21, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[12] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*, 1st ed. Berkeley, CA, USA: Apress, 2018.

[13] M. Turkanović, M. Hölbl, K. Koši , M. Heri ko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[14] Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain," *IEEE Access*, vol. 6, pp. 31077–31087, 2018.

[15] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.

[16] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Int. Cryptol. Conf.*, 2017, pp. 357–388.

[17] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robot. Comput.-Integr. Manuf.*, vol. 54, pp. 133–144, Dec. 2018.

[18] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[19] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Gener. Comput. Syst.*, to be published. doi: 10.1016/j.future.2017.09.023.

[20] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, to be published.

[21] W. Wang *et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2018.

[22] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, *Ripple: Overview and Outlook*. 2015. [Online]. Available:http://www.ghassankarame.com/ripple.pdf

[23] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, pp. 469–548, 1997.

[24] F. Daniel and L. Guida, "A service-oriented perspective on blockchain smart contracts," *IEEE Internet Comput.*, vol. 23, no. 1, pp. 46–53, Jan./Feb. 2019.

[25] A. Canedo, "Industrial IoT lifecycle via digital twins," in *Proc. Int. Conf. Hardw./Softw. Codesign Syst. Synth. (CODES+ISSS)*, Oct. 2016, p. 1.

[26] J. Wan, I. Humar, and D. Zhang, *Industrial IoT Technologies and Applications: International Conference, Industrial IoT 2016, GuangZhou, China, March 25-26, 2016, Revised Selected Papers* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). 2016.

[27] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[28] S. Jeong, W. Na, J. Kim, and S. Cho, "Internet of things for smart manufacturing system: Trust issues in resource allocation," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4418–4427, Dec. 2018.

[29] M. Banerjee, J. Lee, Q. Chen, and K.-K. R. Choo, "Blockchain-based security layer for identification and isolation of malicious things in IoT: A conceptual design," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul./Aug. 2018, pp. 1–6.

[30] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

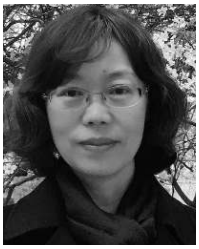
[31] A. Wright, "Mapping the Internet of Things," *Commun. ACM* , vol. 60, no. 1, pp. 16–18, Jan. 2017.

[32] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

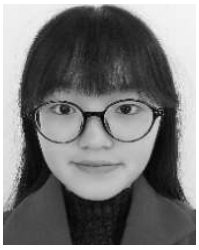
[33] L. Li, M. Liu, W. Shen, and G. Cheng, "A discrete stress–strength interference theory-based dynamic supplier selection model for maintenance service outsourcing," *IEEE Trans. Eng. Manage.*, vol. 63, no. 2, pp. 189–200, May 2016.

[34] L. Li, M. Liu, W. Shen, and G. Cheng, "An expert knowledge-based dynamic maintenance task assignment model using discrete stress–strength interference theory," *Knowl.-Based Syst.*, vol. 131, pp. 135–148, Sep. 2017.

[35] J. Lee, H. D. Ardakani, S. Yang, and B. Bagheri, "Industrial big data analytics and cyber-physical systems for future maintenance & service innovation" *Procedia CIRP*, vol. 38, pp. 3–7, Jan. 2015.
[36] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[37] J. Wan, J. Li, M. Imran, D. Li, and F. E-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, to be published. doi: DOI 10.1109/TII.2019.2894573.
[38] L. Wu, X. Du, W. Wei, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 769–773.
[39] M. Samaniego and R. Deters, "Internet of smart things—IoST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Jun. 2017, pp. 9–16.
[40] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, to be published.
[41] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
[42] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.
[43] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 261–266.
[44] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[45] M. Caesar, M. Castro, E. B. Nightingale, and G. O'Shea, and A. Rowstron, "Virtual ring routing: Network routing inspired by DHTs," in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun.*, Sep. 2006, pp. 351–362.
[46] S. Rhea *et al.*, "OpenDHT: A public DHT service and its uses," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 4, pp. 73–84, Oct. 2005.
[47] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.
[48] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in *Proc. Workshop New Secur. Paradigms*, Sep. 2001, pp. 13–22.
[49] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS Conf.*, Las Vegas, NY, USA, 1979, pp. 313–317.
[50] L. Li, M. Liu, W. Shen, and G. Cheng, "Product deterioration based demand forecasting and service supply model for MRO service chain," *IEEE Trans. Eng. Manag.*, to be published.



LI BAI received the bachelor's degree from the Xi'an University of Technology, Xi'an, in 1995, and the master's degree from the Shanghai University of Finance and Economics, Shanghai, in 2006. She has published over 20 journal papers in his research-related areas. She is currently an Associate Professor with the Accounting and Finance Department, Shanghai Lixin University of Accounting and Finance, Shanghai, China. She was involved in the Internet accounting and finance analysis for about 15 years.



MI HU received the B.E. degree in control science and engineering from Shandong University, Jinan, China, in 2017. She is currently pursuing the M.S. degree with the College of Electronics and Information Engineering, Tongji University, Shanghai. Her research interests include blockchain and machine learning, and their applications in the industrial IoT.

MIN LIU received the bachelor's degree from the China University of Geosciences, Wuhan, in 1993, and the master's and Ph.D. degrees from Zhejiang University, China, in 1996 and 1999, respectively. He is currently a Full Professor with the College of Electronic and Information Engineering, Tongji University, Shanghai, China. He has published over 100 papers in scientific journals in his research related areas. He was a Postdoctoral Fellow of the Computer Science and Engineering Department, Shanghai Jiao Tong University, from 1999 to 2001. As a Product Architecture Engineer, he has developed an enterprise resources management system with Asia-Bridge Software Co., Ltd., from 2001 to 2004. He was involved in system engineering to collaborative MRO and smart manufacturing for about 20 years.

JINGWEI WANG received the B.E. degree in control science and engineering from Shandong University, Jinan, China, in 2016. He is currently pursuing the Ph.D. degree with the College of Electronics and Information Engineering, Tongji University, Shanghai. His research interests include graph data mining, big data analytics, and machine learning.