 doi:10.20944/preprints201708.0002.v1

Article

M2M Security Technology of CPS Based on Blockchains

Shi-yong Yin [1], Jin-song Bao [1,*] , Yi-ming Zhang [2] and Xiao-di Huang [3]

[1] College of Mechanical Engineering, Donghua University, Shanghai 201620, China; ycfysjk@126.com (S.-Y.Y.); Bao@dhu.edu.cn (J.-S.B.)
[2] College of Literature, Science and the Arts, The University of Michigan, Ann Arbor, MI 48109, USA; yimingz@umich.edu
[3] School of Computing and Mathematics, Charles Sturt University, Albury, NSW, 2640, Australia; xhuang@csu.edu.au
* Correspondence: Bao@dhu.edu.cn; Tel.: +86-21-6779-2562

Abstract: As the core of intelligent manufacturing, CPS has serious security issues, especially for the communication security of its terminal M2M. In this paper, blockchain technology is introduced to address such a security problem of communications between different types of machines in CPS. According to the principles of blockchain technology, we design a blockchain for secure M2M communications. As a communication system of M2M consists of public network areas, equipment areas and private areas, we design a sophisticated blockchain structure between the public area and private area. For validating our design, we take cotton spinning production as a case study to demonstrate our solution to M2M communication problems under the CPS framework.

Keywords: blockchain; M2M; CPS; cotton spinning production

1. Introduction

Coming to the epoch of Industry 4.0, CPS, IIOT and M2M keep infiltrating into the realm of industry. CPS is a complex system combined of computation, networks, and the physical world. By using computing, communication and control technologies, CPS digitizes the physical world and realizes the unity of information world and physical world. Typically, CPS consists of two main parts: one is the physical world while another is an information system. Aiming to mine and analyze data of the physical world from the information world, CPS intelligently monitors actions of entities in the physical world, and takes actions to change their behavior to make the physical world entities work more efficiently. As a dynamic network, IIOT has physical and virtual bodies with their own identities and properties. It uses a smart interface to connect a physical world with a virtual world. Relying on a variety of technologies, including sensing, communication, computing, data processing and feedback control technology, M2M supports intercommunication of many heterogeneous devices. Nowadays, M2M has become an indispensable part in the next-generation network, with being widely applied to many new smart applications and services, such as CPS, M2H and M2S.

With the in-depth development and applications of CPS, its security issues are also of concern. Though related security issues are broadly studied and analyzed in the fields of Wireless Sensor Network (WSN), Ad-hoc network and Mobile Ad-hoc Networks (MANET) etc., they are barely applicable because CPS security covers a larger scope, contains much more content and requires higher levels of security. By investigating he CPS security issue, a content-aware security framework for generic CPS systems was proposed [1]. Several security problems along with the currently proposed solutions at different network layers of mobile ad hoc networks were presented and discussed based on the related studies before [2]. Through applications of current network security models to CPS, some flaws were found with the original model. So, it proposed a more appropriate model and explained the research challenges of CPS security [3]. The security design of IOT should be standardized to achieve an open, widespread and interacting fundamental security architecture [4]. On the basis of investigations of CPS security, a series of challenges urgent to resolve to boost the

 doi:10.20944/preprints201708.0002.v1

performance of CPS was also proposed [5]. Some security issues that may occur in CPS are discussed [6, 7].

A vast number of M2M intelligent devices are deployed in CPS. Thus, the security of M2M is decisive to performance of CPS. A simplified protocol stack was proposed and some important sections were introduced to provide secure transmission between M2M servers and its terminals [8]. M2M communication faces lots of security threats. For some unresolved security vulnerabilities, a dynamic-encryption authentication scheme was proposed, by which a mobile device could be authenticated by the network and a shared one-time-password could be generated. It can withstand Man-in-the-Middle attacks, impersonation attacks, reply attacks and DOS attacks [9]. Distributing trust building and enforcement tasks between device and network leads to scalable concepts, which can provide a flexible solution to the new threats that arise in M2M communications [10]. Combining with M2M characteristics, an improved direct anonymous authentication scheme was proposed [11]. To prevent accidents, a design of environmental monitoring platform of mines based on M2M technologies was also proposed [12].

Since the existence of many heterogeneous devices in CPS, current M2M security protocols are not capable of resolving the intercommunications of different devices. How to ensure the safety of communication of M2M is a question that is urgent to be solved. The main contributions of this paper are as follows: (1) introduced the blockchain technology to solve the security problems of M2M communication; (2) designed the block chain for safer M2M communication; and (3) applied blockchain technology to solve malleability and security issues of M2M system.

The rest of this paper is organized as follows. Part 2 introduces the block chain technology. It mainly presents the connotation and characteristics of the block chain, the nature of the block chain and its core technology. Part 3 discusses the safer M2M communication with the help of blockchain technology, and then presents our blockchain design, including the design of the overall structure, the public network area block chain, and private area block chain. Part 4 is a case study of applying blockchain technology into M2M communication of intelligent cotton production CPS to solve malleability and instant security issues of a M2M system. Finally, this paper concludes with the conclusion.

2. Introducing Blockchain Technology

2.1. The Connotation and Main Features of Blockchain

After the inventor of Bitcoin published a paper named "*Bitcoin: A peer-to-peer electronic cash system*" [13] in 2008, blockchain comes to publicity. Later, Swan claimed that blockchain is a transparent distributed database [14]. Ministry of Industry and Information technology of the People's Republic of China defines blockchain as a creative application of distributed storage, P2P transmission, consensus mechanism and encrypted algorithms. Despite being far from reaching consensus on definition of blockchain, the connotation is fairly clear. Using mathematics as its foundation, blockchain is a multidisciplinary technology that also combines cryptography, economic model, and network technology, into a distributed system that is established on distrust and indecent operations. The main features of blockchain are as follows:

(1) Rather than creating a system around a central server, blockchain utilizes p2p networking and a consensus mechanism to create the trust system between nodes, thus forming a decentralized system.

(2) Blockchain uses encryption especially asymmetrical encryption to protect transaction data. A consensus mechanism ensures that data cannot be modified or forged, guaranteeing a high level of security.

(3) Based on the chain structure, all data of a transaction are traceable. Blockchain utilizes special methods to motivate all nodes to cooperate in block verification and uses a consensus mechanism to choose specific nodes as new blocks [15].

2.2. The Working Mechanisms of Blockchain

Blockchain is an ordered chain of blocks. Blocks are containers of some related information and the data of transaction records. The different blocks may vary, but a normal block consists of a block

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

head, which contains metadata, and a block body, which records transaction process. The structure of a block is shown in Figure 1. A block head has three main parts except for its version number: ① a hash value linked to the previous block, which is essential to the chain structure; ②a hash function, timestamp and nonce related to transactions. Hash functions use to store blockchain data. Timestamp records time of generation of blocks. Nonce is a calculator used in proof of the work algorithm; and ③Merkle root is used to summarize all transactions in the block and to quickly check the existence and integrity of transaction data. A block body stores all verified transactions during the generation of a block. By linking blocks with hash values, a blockchain is created.

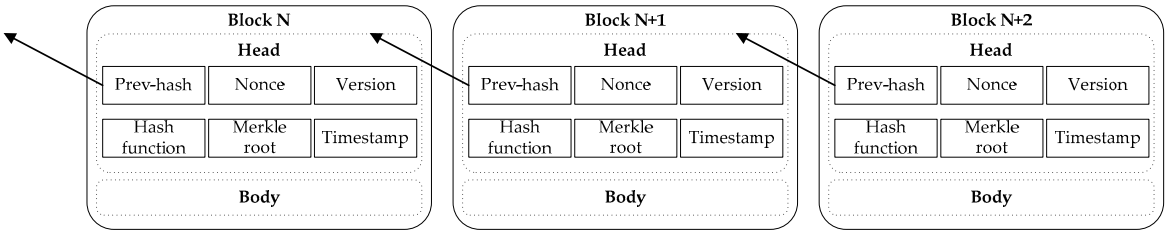

Figure 1. The structure of blocks

The working mechanism of a blockchain is illustrated in Figure 2. In a bitcoin network, if A wants to send a bitcoin to B, the following processes will be followed: ①Create a transaction order. Encrypt the previous transaction with B's public key, calculate the hash value, and then encrypt the hash value with its own private key to obtain its digital signature, and finally add the digital signature to the end of the bitcoin to create a transaction order. ②Broadcast the transaction order. Broadcast the transaction order to the Internet to inform other nodes about the transaction and each node incorporates received the transaction into a block. ③Verify transaction validity. All participants verify the validity of the transaction by searching for a solution x, which allows the hashed value computed from x, the hash value of the last block of the blockchain and transaction order using Hash256 algorithm satisfies certain conditions, for example, first 20 digits are 0. After the solution is found, the privilege of creating a new block is guaranteed and a bitcoin is rewarded. ④Transmit Verification results. The node that computes the solution firstly receives the bitcoin from the system and this piece of information is broadcasted to all the node through the Internet. ⑤Complete the transaction. A's and B's bitcoin are separately changed in the distributed ledger.

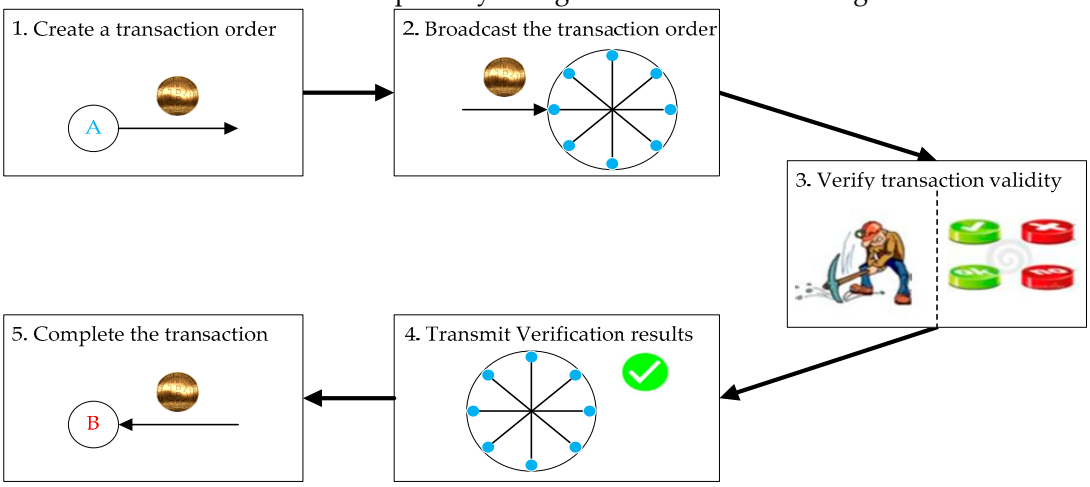

Figure 2. The working principle of a blockchain

2.3. The Utilization of Blockchain of CPS in M2M

Features of a blockchain and M2M technology in CPS are compatible to some extent. For example:

(1) Blockchain technology and M2M both utilize the idea of distributed and decentralized computing. There is no centralized database in a blockchain, with each network node storing its own copy of the blockchain. The physical level of CPS contains energy/environment, personnel and various types of physical equipment and other elements. The interconnection between machines and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

equipment (M2M) is a key technology in CPS, and it can take the form of machine to machine, machine to cluster and even cluster to cluster. But no matter which form of M2M takes, they all exhibit the nature of decentralization.

(2) A Blockchain and M2M both require high levels of security. Other than a system being built on dependency and trust, a blockchain uses encryption and digital signature to secure information. While in a M2M system, the transmission and storage of information also require high confidentiality, integrity and validity, authenticity. In addition, M2M has the nature of non-repudiation. Despite some level of variation in different systems, for example military, electrical, medical and manufacturing systems, the security of information is generally the first priority of such systems.

(3) A Blockchain and M2M reach the high level of harmony in the traceability and sharing of information. Providing effective sharing of historical information, Blockchain technology uses a hash value, which is connected to the previous block, to track information of transactions throughout the whole blockchain. In M2M systems, especially in the area of manufacturing, tracing historical data is crucial. For instance, by reviewing data, we can identify key factors that might impact product quality. By improving processes, a higher quality will then be achieved. By filtering through the data, we can discover weak spots in production. The rate of machine breakdowns will be then lowered considerably by optimizing maintenance methods. Also, through data sharing, those unnecessary processes can be easily spotted. Then cutting or reducing expenses of these processes on the supply chain will help cut production costs.

3. M2M-Security-Oriented Blockchain Design

3.1. Overall Design

On the foundation of ensuring data throughput and extensibility, to achieve validity of data, which means that data are usable, reliable, integral, safe and manageable, senders of data are required to send real, legal and standardized data. The transmission must be covert, recorded, queryable, and traceable. The receivers can only receive the data sent from the senders which cannot be forwarded. The process of receiving data can be recorded and queryable. In a M2M transmission system of CPS, The design of blockchain in this paper is illustrated in Figure 3.

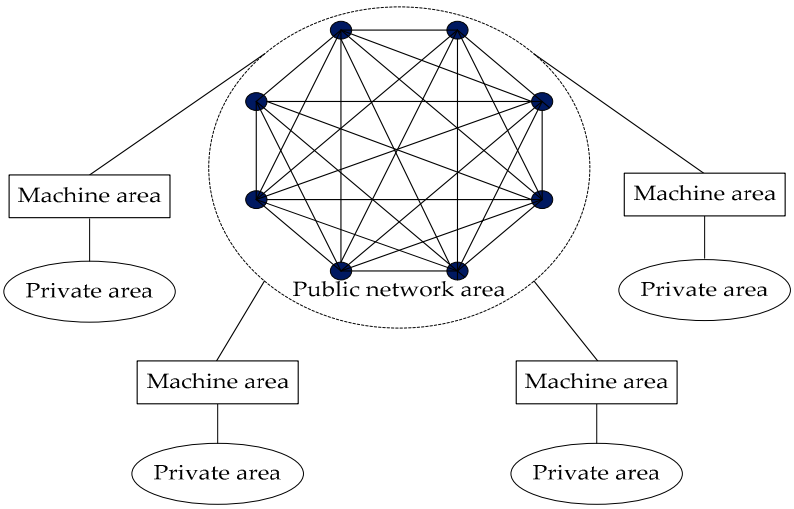

Figure 3. Our overall design of the Blockchain for M2M Security

(1) Public network area. Based on the industrial Internet of things, the public network area builds machine communication platforms. This ensures the normal communication of various types of machines, audits registration of machines and accesses authentication to achieve connection and communication among machines, unifies data format and communication rules, maintains the blocks of public network area and queries communication records.

(2) Device area. The device area is the channel connecting the public network area and the private area. It receives messages from the public network area, passes the query requests and query results to and from the private area.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

(3) Private area. The private area establishes and records the blocks of communication process among machines, saves data of the communication process, accepts the external query, or obtains external related data by querying.

3.2. Design of Machine-Equipment Blockchain in Public Network Area

In CPS, if devices must be replaced due to malfunctioning or other reasons, the new device will have to be connected to the production line by registration. Every new device has a piece of information that marks its own identity, e.g. digital certificate, which needs to be sent to the public network to register. It will be successfully registered after approval. Then the public network will create an equivalence between the certificate and its identity, and store the public key of this device into the key pool. At the same time, the device is added as a new blockchain into Machine-Equipment Blockchain (M-EB). The structure of M-EB is shown in Figure 4. After a public area has accepted and registered a new device, M-EB will use the public key to verify the encrypted digital certificate, confirm the identity of the device and finally authorize access into this area. Up until now, the new device can participate in M2M communication.

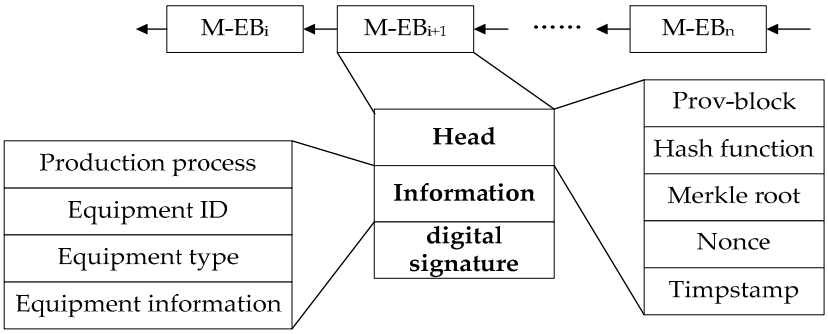

Figure 4. The structure of the machine & equipment blockchain

M2M technology uses a communication mechanism, which aims to empower all machines with the ability of communication, to realize the smart and interactive connections between machines and systems. To maintain data integrity and reduce data redundancy, the public network can standardize the format of communication among any M2M terminals of CPS. Here we also reach a consenses on types of communication data: uploading information refers to the collection of local data, and downloading information refers to the communication protocol, orders of networks and settings of parameters.

3.3. Design of Communication Blockchain in Private Area

Private sectors are in charge of recording communications between blocks, storing data and querying the relevant information. Since information about communication proocess can be shared, private sectors ensure that it is difficult to be tampered with.

The blocks of a communication blockchain (BC) are composed mainly of header information and communication information. Header info includes：①a hash value that links to the previous block; ② a target hash; ③ Merkle root; ④ nonce; ⑤ timestamp; and other components. While communication information consists of ①sender ID,to identify the initiator; ②receiver ID, to identify the receiver; ③information type, to embody the data type of communication and tell whether it is uploaded data or downloaded data; ④data size, to specify the total number of bytes of the data unit; ⑤data, to be stored for specific communication data required; ⑥encryption type, to specify the type of encryption; and⑦information varification, to verify the accuracy of the data after transmission. The structure of the communication blockchain is illustrated in Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

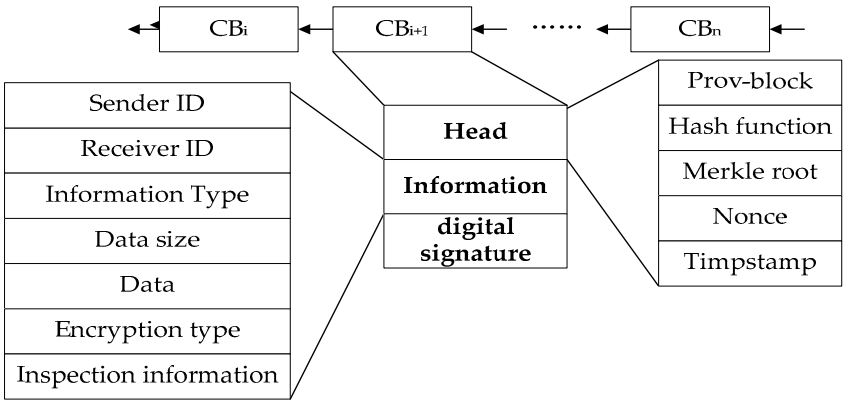

Figure 5. The structure of the communication Blockchain

Communication blockchain mainly records the communications between devices. Each communication is linked to the blockchain as a separate block. The data in the interworking process, including the ID of the communication, the type of information, the size of the data, and the encryption mode, are saved to the block.

Suppose device M1 wants to search for its communication record with a certain device M2, it can send a query packet to the public network area in the form shown in Figure 6. If the query is succesful, M2 returns the packet of the query result to M1 through the public network area. The format of the packet is shown in Figure 7. Otherwise, the public network area returns the query failure message back to M1.

Receiver ID	Sender ID	Digital signature of Sender	Data to be inquired	Inspection information

Figure 6. The data format of a query packet

Receiver ID	Sender ID	Digital signature of Sender	Encrypted data	Inspection information

Figure 7. The data format of an information packet

The whole process of query communication is illustrated in Figure 8. The step-by-step descriptions are detailed as follows:

Step 1: M1 sends a query packet to the public network area.

Step 2: After receiving the query packet, the public network area resolves the query packet and checks whether it is complete or not, according to the data check information. If not, M1 is required to resend the packet and the system re-enters Step 1; Otherwise , the system enters Step 3.

Step 3: According to the ID of M2 in the query packet, the public network area checks whether M2 exists in the machine-equipment blockchain or not. If not, a null value from the public network area is sent to the query sender, and the query fails; Otherwise, the system enters Step4.

Step 4: The public network area delivers the query packet to the private area of M2 through the equipment sector.

Step 5: The private area of M2 analyzes the query packet to decide if the digital signature of packet is legal. If not, the service request will be denied. And, a denial of service information will be sent to M1 through the public network area. System re-enters step 1. Otherwise, it goes directly to Step 6.

Step 6: The private area of M2 searches for the query packet in the history. It encrypts results using M1's public key and then encapsulats them into a packet, which is later sent to the public network area.

Step 7: After receiving the packet, the public network area checks whether or not it is complete according to the inspection information in the packet. If not, M2 is required to resend the packet.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

Otherwise, the system goes to Step 8.

Step 8: The information packet is sent to the private area of M1 through its device area.

Step 9: The private area analyzes the digital signature of M2 to identify its legitimacy. If it is illegal, M2 will be required to resend the packet and system re-enters Step 6. Otherwise, the private area of M1 uses its private key to obtain the data and the whole query completes.

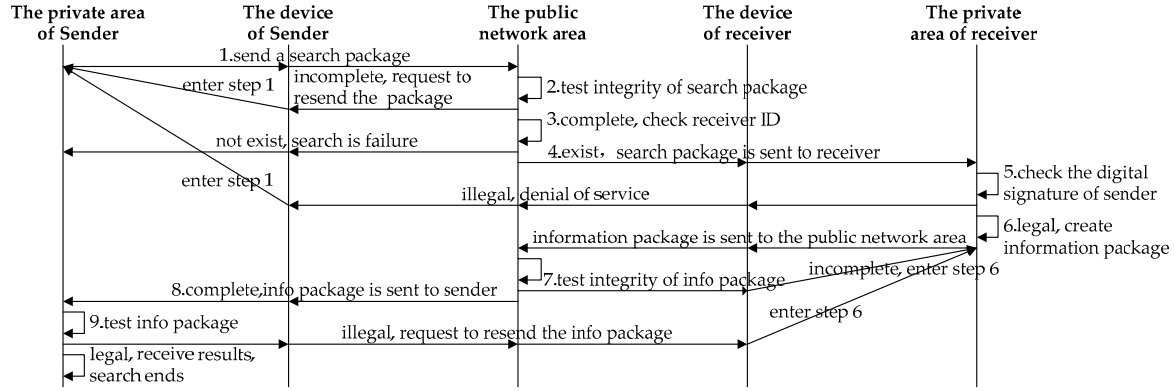

Figure 8. The communication process for search

4. A Case Study: Cotton-production-oriented security of M2M under CPS architecture

In this section, we present a case study to exemplify our design of the Blockchain under CSP architecture.

4.1. Problem Description

Traditional cotton production is a quite complicated process. As illustrated in Figure 9, cotton spinning involves a few key processes: blow room opening, cleaning and mixing, carding, drawing, lap forming, combing, carded yarn, combed yarn, packing palletizing, etc.. The processes are complex and continuity demanded.

The cotton-production-oriented CPS architecture involves a bottom physics layer of machines, devices, energy, environment and workers, and a middle layer of industrial network based on various types of smart sensors, FRID, Wi-Fi and Tag. In our design, hundreds of high-performance sensors will need to be deployed in one single cotton production workshop to differentiate machines, equipment or raw materials. By then each device will record enormous amount of real-time data, e.g. quality data of cotton yarn during each processes and status data of operation devices . With the proceeding of production, a cotton bale becomes cotton slivers, carded yarns and finally combed yarns. It's whole transformation processes will also establish a lot of data. Therefore, in the large data environment, intelligent cotton production will encounter: First, though the size of cotton-production-oriented CPS is huge in size, and M2M technology is increasingly mature, CPS itself is growing. To put it more specifically, the equipments will increase or decrease in number according to the actual needs of production without sacrificing the satbility of M2M communication. Second, say a carding machine sends a query requrest to a lap forming machine layed on its previous process for information reagrding lap forming status and quality so as to adjust its own setting accrodingly; due to suddenly incerase of the order quantity, M2M system will have to send an instruction to extend the working hours to realated machines; a carding machine conveys quality information of carded yarn to combing machine as a reference to adjust a proper parameter to continue. How can these information or instructions be transmitted safely to its target device? This case is to discuss how to ensure communication scalability in the dynamic change of M2M system under the CPS architecture for cotton spinning and timeliness and safety of multipoint-to-multipoint communication in data environment.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2017 doi:10.20944/preprints201708.0002.v1

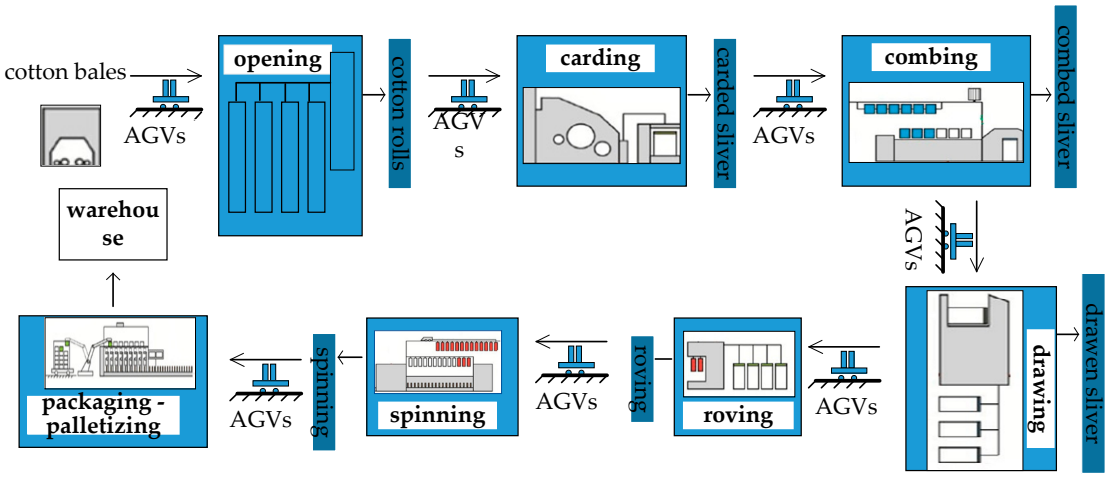

Figure 9. The process flow diagram of cotton spinning

4.2. Solutions

4.2.1. Maintenance of Extensibility of M2M

If a production line is built, new devices must be added to the industrial network. Things will happen when the production line has to be modified or updated according to needs. Some devices must be substituted. In a word, M2M systems are dynamic and must be extensible. Then how to maintain the extensibility of M2M systems?

M2M systems of CPS use blockchain technology to maintain its extensibility. Industrial IOT platforms recognize the IDs of new devices and timestamp them before adding them to the blockchain as a new block. See Fig.10. For a changing scenario, the information of the replaced parts is still stored in the equipment blockchain as historical data for later querying and analyzing. If a lot of devices are to replace, the whole production line must be re-deployed and blockchain must be reestablished. This situation will be discussed otherwise.

Furthermore, similar to M2M systems, raw materials are dynamic as well. That is to say, the forms of materials are different in each step of production. For example, cotton is diplayed in bales before opening and cleaning, and roll forms after this step. It will become cotton strips after combing. Cotton is finally presented as combed yarn after all of processes. The dynamic maintenance of raw materials can also be achieved through blockchain technology. Industrial IOT platforms recognize the IDs of new forms of the material, stamp them with verification time, and then add them to the material blockchain as a new block, as shown in Figure 10. The forms of materials have undergone physical changes in production, but all the tramformation data during their entire life cycle are stored in the blockchain. This will be helpful for future data analysis and quality tracing of raw materials and finished yarns.

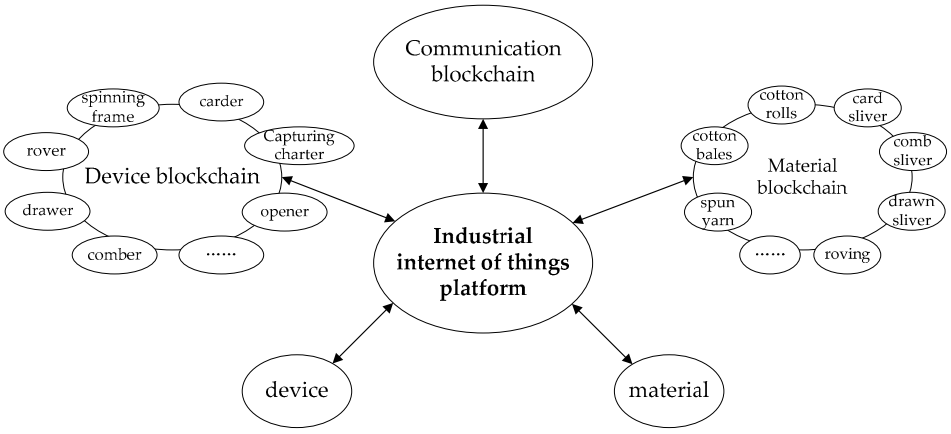

Figure 10. Create device, material and communication blockchains

 doi:10.20944/preprints201708.0002.v1

4.2.2. Maintenance of Timeliness and Security

In cotton production process, machines, materials and environment all produce enormous amount of real-time data. Under such large date environments, the request information of any devices in the M2M system, or the operation instructions of the system itself, or how relevant information is transmitted to the target device within specified time all relect security and timeliness demand for M2M systems.

As illustrated in Fig.10, all data of machinary and materials in yarn production are stored in the equipment blockchain and raw material blockchain respectively. If intercommunications happen between devices or mutual visits occurred between euipments and materials, all communication or access process data will be stored in the communication blockchain. At the same time, equipment information of the two communication sides, material information of the accessed materials will be timely backed up to the in the communication blockchain. A blockchain has an important feature of keeping multiple backups. If some devices have malfunctions, their own data will be thus backed up not only in the device blockchain but also in its communication blockchain and in those of devices they've been contacted with previously. Even if the IIOT is attacked, data are hard to be tamperted with due to the existence of multiple copies. All of these ensure the high security and timeliness of data.

5. Conclusions

This paper has introduced blockchain technology to the security of communication under CPS architecture. The meaning, main features and working principles of blockchains are presented under such an architecture. In particular, we have presented our design of the three-area-blockchain, mainly the public network area and private area, for resolving the M2M security problem. For validating our design, we take cotton spinning as an example to explore the possibility of applying blockchain technology to resolve the expansibility of M2M system and the timeliness and security of M2M communication in CPS architecture for cotton spinning.

Acknowledgments: This study was supported by The Fundamental Research Funds for the Central Universities, China and National Natural Science Foundation of China (51475301).

Author Contributions: Shi-yong Yin and Jin-song Bao conceived this study and wrote the paper; Yi-ming Zhang conceived and designed the case; Xiao-di Huang performed the case.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wang, E. K.; Ye, Y. M.; Xu, X. F.; Yiu, S. M.; Hui, C. K.; Chow, K. P. Security issues and challenges for cyber physical system. In Proceedings of the IEEE/ACM International Conference on Green Computing and Communications & Cyber, Physical and Social Computing, Hangzhou, China, 733-738 December 2010.
2. Djenouri, D.; Khelladi, L.; Badache, A. N. A survey of security issues in mobile ad hoc and sensor networks. *IEEE Commun. Surveys Tuts.* 2005, 7, 2-28.
3. Anand, M.; Cronin, E.; Sherr, M.; Blaze, M.; Ives, Z.; Lee, I. Security challenges in next generation cyber physical systems. In Processdings of Beyond SCADA: Network Embedded Control for Cyber Physical Systems, Washington, D. C., USA, March 2006.
4. Lee, E. A. Cyber physical systems: design challenges. In Processdingd of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing, Washington, D. C., USA, 363-369, May 2008.
5. Cardenas, A. A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Processdings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 495-500, June 2008.
6. Medaglia, C.; Serbanati, A. An overview of privacy and security issues in the internet of things. In Processdings of the 20th Tyrrhenian International Work-shop on Digital Communications, Sardinia, Italy, 389-395, September 2009.
7. Weber, R. Internet of things-new security and privacy challenges. *Computer Law & Security Review*, 2010, 6, 23-30.

8. Saedy, M.; Mojtahed, V. Ad hoc M2M communications and security based on 4g cellular system.*Wireless Telecommunications Symposium*, 2011, 1-5.
9. Chen, S.; Ma, M. D. A dynamic-encryption authentication scheme for m2m security in cyber-physical systems. In Processdings of the Global Communications Conference, Atlanta, GA, USA, 2897-291, December 2013.
10. Inhyok, C.; Shah, Y.; Schmidt, A. U.; Leicher, A.; Meyerstein, M. V. (M.). Trust in M2M communication. *IEEE Veh. Technol. Mag.*, 2009, 4, 69-75.
11. He, Y. Y.; Chen, L. Q.; Wang, L. L. An improved direct anonymous atteatation scheme for m2m network. *Procedia Engineering*, 2011, 15, 1481-1486.
12. Zhang, K. S.; Chen, M.Z. Research of environment monitoring platform of mine area based on M2M. *Industry and mine automation,* 2013, 39, 63-67.
13. Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system. *Consulted*, 2009, 1-8
14. Swan, M. *Blockchain: blueprint for a new economy*. O'Reilly Media, USA, 2015.
15. Yuan, Y.; Wang, F. Y. Blockchain: the state of the art and future trends. *ACTA automatica sinica,* 2016, 42, 481-494.