ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20180621055030
Preliminary communication

CPS Information Security Risk Evaluation Based on Blockchain and Big Data

Yonggui FU, Jianming ZHU, Sheng GAO

Abstract: CPS (Cyber Physical Systems) have got wide application and research, and information security risk evaluation became the key for CPS greatly developing. In view of the physical structure and business characteristics of CPS, this paper constructs an information security risk evaluation system for CPS. In the process of risk evaluation, colligating the analysis results from experts and the analysis results of external data sources' related big data for information security risk evaluation of CPS, by experts confirming the index system and indexes' weight values for CPS information security risk evaluation, further through using evaluation model to realize the quantitative calculation to CPS information security risks. This paper proposes using blockchain technology to construct the data's authenticity and reliability guarantee system for CPS and CPS related external systems, and constructing blockchain's layered model structure based on CPS. In the part of case analysis, comparing and analysing the evaluation system based on blockchain and big data and the evaluation system based on traditional mode, to confirm the research value of this paper.

Keywords: Big Data; Blockchain; CPS; Information Security Risk Evaluation

1 INTRODUCTION

The deepening of the integration for Informationization and Industrialization, and the development of cloud computing, real-time transmission, credible service, network communication and control technology, artificial intelligence technology etc., promote the traditional physical systems gradually integrate the functions of control, computing, communication, remote collaboration etc., and form the Cyber Physical Systems (CPS) that integrate 3C technology (Control technology, Computation technology, and Communication technology) as a whole [1-3].

As the proposer of CPS, Helen Gill thought: Cyber-Physical Systems were physical, biological, and engineered systems whose operations were integrated, monitored, and/or controlled by a computational core. Components were networked at every scale. Computing was deeply embedded into every physical component, possibly even into materials. The computational core was an embedded system, usually demanding real-time response, and was most often distributed [4]. The National Natural Science Foundation Committee (NSF) of United States thought: CPS were engineered systems that were built from, and depended upon, the seamless integration of computational algorithms and physical components [5]. After colligating and analyzing the classical CPS definitions, this paper thinks: CPS are complex integrated systems, that not only are technology systems, but also management and control systems. For the technology systems, CPS integrate network and information technology, control technology, communication technology, storage technology, etc. For the management and control systems, CPS integrate management science, decision analysis, control method, etc. The construction objects of CPS are real-timely and dynamically realizing high integration and interaction among computing and control units and embedded physical devices. So, with the change of network environment and information technology level, CPS will also appear in different application modes.

Comparing with other network systems or information systems, CPS embody more complexity in physical structure and technology constitution, at the same time, because data communication and processing are the important contents of CPS operating, so it is not feasible for using service isolation method to implement the security management to CPS' data. In fact, because of using traditional information and network security management measures, CPS had encountered more prominent security threats than other information systems, that brought great troubles to the application and development of CPS. For these, CPS' research and application experts all over the world paid high attention to the information security problems of CPS. In the process of integration of informationization and industrialization, the authenticity and reliability of information, the security and supervisability of information transmission, and the stability of information resource and information service operation are the premise and foundation for the good application and development of CPS. Therefore, information security is the key problem needed to be solved in the development of CPS. While to measure the information security level of CPS operation, it is necessary to establish a proprietary information security risk evaluation system based on CPS architecture, business characteristics and data flow, and the evaluation system not only needed to make the existing information security risk evaluation criteria and methods as the foundation, but also needed to embody the characteristics of CPS themselves.

As CPS have got wide attention from all the world, and China is a classical application and research country, so, in the following research, we mainly make the CPS information security risk evaluation in China the object to expand research, and the research results have the same guidance significances to the other countries.

2 APPLICATION AND RESEARCH ON INFORMATION SECURITY RISK EVALUATION

Information security risk evaluation includes analyzing information system's important assets, assets facing threats, assets' vulnerability, adopted protection measures, etc., testing the effectiveness of adopted safety protection measures, comprehensively analyzing and judging the probability of security incidents and the losses that may be caused, judging information system facing security risks, proposing risk management suggestions, providing reference basis for improving system security protection measures [6].

At present, information security risk evaluation criteria can be mainly divided into two series: CC and ISO17799, the two series' emphasis is different. CC series evaluate information security risk from two angles as technology and management, while ISO17799 mainly evaluates information security risk from the angle of management. GB/T20984-2007 from China are the basis criteria for the country's information security risk evaluation, the criteria set content, structure, and process for information security risk evaluation, which belong to the CC series, at the same time cite some of the clauses in ISO17799 series.

According to GB/T20984-2007, the content of information security risk evaluation mainly includes three parts: asset identification, threat identification, and vulnerability identification. Information system asset's security attributes include availability, integrity, confidentiality, and information system asset facing threats, asset's vulnerability, and adopted security measures directly influence the asset's security attribute reached degree.

In academic circles, the research results on information security risk evaluation mainly include information security risk evaluation's theory discussion, architecture design, value analysis and evaluation model construction, etc.

Because at present information security risk evaluation has already formed a relatively complete theoretical system, so, in recent years, information security risk evaluation's theoretical discussion, architecture design, value analysis aspects' research results are relatively less, but these research results still have very important promotion function to information security risk evaluation implementation and theoretical perfection.

The research results on evaluation model construction are relatively numerous. This aspect's research results include the research based on situational awareness theory, the research based on neural network model, support vector machine model, the research based on fault tree, fault graph method, the research based on ANP+DEMATEL method, the research based on Markov chain, the research based on Delphi method, the research based on fuzzy theory, the research based on entropy weight theory, the research on evaluation model index construction, etc.

Some of the existing literature researches are to analyze from qualitative point of view, and some of the existing literature researches are from quantitative point of view to construct operational model, and more researches are from the view of combining qualitative analysis and quantitative model to implement. Most of the world countries' research focused more on the concrete fields' application. The research of China focused more on making GB/T20984-2007 the theory and technology basis, making asset identification, threat identification, and vulnerability identification as the subjects of research. The research methods and contents are suited to most of the existing information systems. In this paper, we also make GB/T20984-2007 the research basis.

3 THE SYSTEM FOR CPS INFORMATION SECURITY RISK EVALUATION

At present, the research and application on CPS information security risk evaluation embody the following deficiencies: blindly copying the traditional information risk evaluation system, insufficiently understanding the characteristics of CPS, inadequately describing the generation and correlation of CPS information security problems, and not ensuring the authenticity and security of data related to CPS information security risk evaluation, etc.

The complexity of the structure and business content of CPS leads to the complexity of information security problems of CPS. Therefore, the generality of qualitative analysis cannot accurately reflect the specific content of information security risks of CPS. At the same time, quantitative analysis also cannot well reflect the forming causes, casual relationships, and the characteristics of information security risks of CPS. So, it is necessary to combine qualitative analysis with quantitative calculation to comprehensively evaluate the information security risks of CPS.

Petri net is used to describe the causality relationships of asynchronous and concurrent computer system events. Petri net model has strong simulation ability to complex system events, so it is widely used in the fields of workflow management, data analysis and fault diagnosis, etc. The proposer of Petri net was Dr. Carl A. Petri, and the proposed year was 1962 [7]. Petri net model consists of Place, Transition, Connection and Token, etc. Petri net has the characteristics of dynamicity, extendibility, time series and logicality etc., and can describe the correlation among system events well. So, it is suitable for accurately describing the rich business and data relationships with Petri net. For the definition and principle of Petri net, the readers can see the related literature; in here we don't discuss it any more.

So, this paper proposes to use Petri net model to describe the evaluation process of the internal information security risks of CPS, and the formed initial index system and the indexes' initial weights, and combines the evaluation results from the external related multi data sources' big data for information security risk evaluation of CPS, by experts discussing, analyzing and finally confirming the structure of evaluation index system and each index's weight value. Here, it needs to be emphasized, each index value and different layered (corresponding to system, subsystem, asset, etc.) risk values for CPS sample are got through colligating the analysis results from Petri net and the analysis results from CPS' external related multi data sources' big data. For the quantitative calculation of the information security risks of the evaluated CPS, this paper proposes to use RBF (Radial Basis Function) neural network model, because RBF neural network model has strong evaluation ability to information systems' information security risks and has got wide application. For further ensuring the reliability and authenticity of the analysis results of CPS' internal data and external related multi data sources' big data, we introduce blockchain technology into CPS. In view of CPS' layered structure characteristics and each layer's function characteristics, blockchain's layered structure in

CPS is constructed and blockchain's each layer's function analyzed. The architecture for CPS information security risk evaluation is shown in Fig. 1.

Due to the diversity and greatness of CPS data, in Fig. 1, we also applied big data technology to CPS. In Fig. 1, after analyzing and confirming each risk evaluation element of each asset for each subsystem of each sample, CPS will compose the initial index system for CPS information security risk evaluation (Gotten by evaluation experts evaluating CPS (embodied in Petri net model)), while the corresponding weight values (provided by evaluation experts colligating the results for evaluation experts evaluating CPS information security risks, the results for data analysis experts analyzing CPS' external related multisource big data, and the results for evaluation experts carrying out fuzzy comprehensive evaluation), the final index system (Provided by evaluation experts colligating the initial index system, and the results for data analysis experts analyzing CPS' external related multisource big data), and the evaluation results (Provided by evaluation experts colligating the results for evaluation experts evaluating CPS information security risks, the results for data analysis experts analyzing CPS external related multisource big data) will become the basis for constructing quantitative model for calculating other CPS information security risk evaluation results. In Fig. 1, the analysis results from Petri net model for the CPS information security risk evaluation system to be evaluated include the preliminary evaluation results for CPS information security risk evaluation, but the terminal evaluation results need be confirmed by RBF neural network model calculating.

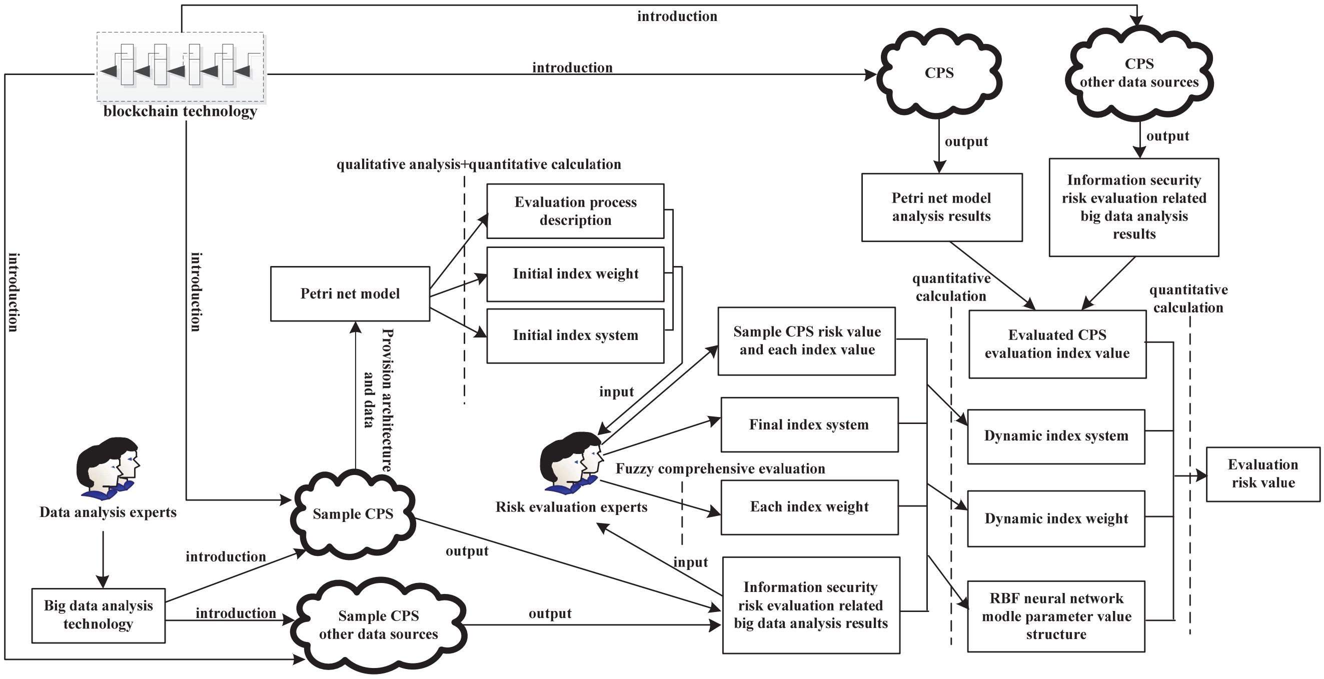
introduction
introduction
CPS
CPS
other data sources
blockchain technology
output
output
qualitative analysis+quantitative calculation
Evaluation process description
Initial index weight
Initial index system
Petri net model
Petri net model analysis results
Information security risk evaluation related big data analysis results
introduction
introduction
Provision architecture and data
quantitative calculation
quantitative calculation
Sample CPS risk value and each index value
Evaluated CPS evaluation index value
input
Final index system
Dynamic index system
Fuzzy comprehensive evaluation
Evaluation risk value
Data analysis experts
Sample CPS
Risk evaluation experts
Each index weight
Dynamic index weight
introduction
output
input
Big data analysis technology
introduction
Sample CPS other data sources
output
Information security risk evaluation related big data analysis results
RBF neural network modle parameter value structure

Figure 1 The architecture diagram for CPS information security risk evaluation

CPS information security risk evaluation not only includes CPS interior evaluation, but also includes evaluation of other systems related to CPS, that is, CPS information security risk evaluation element index system not only includes CPS internal elements, but also includes CPS related other systems' elements. In Fig. 1, Petri net model is used to describe the correlation and concrete state of CPS internal elements (CPS internal elements' risk values need be confirmed by comprehensively analyzing CPS' internal data and CPS' external related multi data sources' big data), CPS external risk elements' information need be gotten by analyzing CPS external related big data. Blockchain technology is used for providing guarantee to the authenticity and reliability of CPS data and CPS external related systems' data.

3.1 Index System Construction and Evaluation Realization

3.1.1 Index System Construction

In Petri net model, CPS information security risk evaluation process has been described. Through analyzing the evaluation process, the initial index system for evaluation can be constructed, according to the structure characteristics of CPS, the indexes can be constructed with layered structure as "subsystem → asset → element", next the experts will confirm, analyze and revise the initial index system, and create the revised index system, continue through CPS external related multisource big data analysis results to validate the revised index system, further creating the final index system.

The index weight can be obtained by colligating the analysis results from Petri net model, and the importance level of each subsystem, each risk asset, each element index that is provided by experts using fuzzy comprehensive evaluation method, on this basis further with the reflection of CPS external data source information security risk evaluation related big data to each element information security risk importance, to verify and adjust each asset's evaluation index element weight (External data sources reflected risk evaluation index weight values are gotten by experts using fuzzy comprehensive evaluation method, on this basis further with the analysis results of external multisource big data to verify and adjust.). The variability of big data results in the variability of the information content contained in big data, because the variation of big data is dynamic and real-time, so the evaluation index system and each index weight for CPS are also varying with the variation of big data dynamically and real-timely, which are conforming to the different demands for different phases of CPS information security risk evaluation.

In the process of constructing risk element indexes of each asset, we can get risk correlations among each element index of CPS through the information in Petri net model, and we can also get the risk correlations among each element index of CPS through analyzing a certain number of same profession's same type of CPS' risk evaluation related external multisource big data (In general, different CPS have large differences in the aspects of structure and information interaction, and the differences of their risk evaluation external related multisource big data are also large, so, we need consider cautiously before using this method.), as the basis of adjusting the evaluation weight values.

3.1.2 Evaluation Realization

This paper proposes using the current popular evaluation model-RBF neural network model to calculate the risk values of evaluated CPS, in view of the weighted RBF neural network model is more accurate to approach the true value of the evaluated object in evaluation calculation [8], this paper proposes introducing risk element weight value in model construction. Because the research on RBF neural network is very mature, so in here we don't discuss more.

In the process of using RBF neural network model to calculate the risk evaluation values of CPS, we need select multiple CPS with same hardware composition and function construction, and use the CPS' risk evaluation values and the corresponding evaluation element index values of the same period in history as the training data (We can also use multiple periods of system risk evaluation values and the corresponding evaluation element index values of some a CPS as the training data, but this method also needed to be considered cautiously before using.), to get the parameter constitution and parameter values of RBF neural network for calculating the risk evaluation values of CPS. Due to CPS have complex physical and function structure, so, sometimes we need construct different RBF neural network evaluation models for different subsystems, and even sometimes we also need construct different RBF neural network evaluation models for different assets, then further to summarily calculate these evaluation result values.

3.2 Information Quality Guarantee System

CPS information security risk evaluation's basis mainly sources of expert evaluation results and the related information security risk big data, so the authenticity and reliability of CPS information security risk evaluation related data resources also determine the credibility of CPS evaluation result. However, the traditional information management methods are unable to ensure the authenticity and the reliability of CPS information.

Blockchain is the decentralized distributed account issued by Satoshi Nakamoto with bitcoin in January 9, 2009, in Blockchain, using hash algorithm, digital signature, time stamping technology and consensus mechanism to realize data non repudiation proof [9]. Therein, the hash algorithm is a method for mapping arbitrary length binary value to a shorter and fixed length binary value, for a piece of data information, the hash value is exclusive, the hash value is equivalent to the data abstract for this piece of data information. Digital signature is a technology for the information sender using asymmetric encryption technology to encrypt data abstract and verify the authenticity of the sent information. Time stamping technology is used for ensuring the time traceability of information. Consensus mechanism is used for realizing authentication to the authenticity of business data and electing the business accounting subject. The work principle of blockchain is shown in Fig. 2.

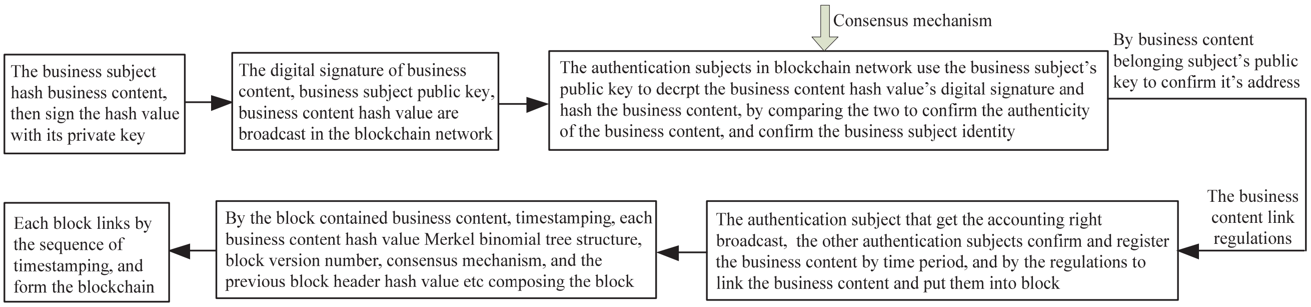
Consensus mechanism
The business subject hash business content, then sign the hash value with its private key
The digital signature of business content, business subject public key, business content hash value are broadcast in the blockchain network
The authentication subjects in blockchain network use the business subject's public key to decrpt the business content hash value's digital signature and hash the business content, by comparing the two to confirm the authenticity of the business content, and confirm the business subject identity
By business content belonging subject's public key to confirm it's address
The business content link regulations
The authentication subject that get the accounting right broadcast, the other authentication subjects confirm and register the business content by time period, and by the regulations to link the business content and put them into block
By the block contained business content, timestamping, each business content hash value Merkel binomial tree structure, block version number, consensus mechanism, and the previous block header hash value etc composing the block
Each block links by the sequence of timestamping, and form the blockchain

Figure 2 The work principle of blockchain

At present, as a data authenticity guarantee technology system, blockchain has already achieved wide attention from academic circles and industry circles, and having generated a large number of research and application results, the research contents include value analysis (such as [10, 11]), architecture design (such as [12, 13]), and product introduction (such as [14, 15]), etc., and the research fields include finance, education, medical treatment, intellectual property, etc. Although at present very successful blockchain products have not appeared in the field of CPS, and the academic research results on blockchain applying in CPS have not formed, but the products of blockchain related to Internet of things have got attention and debugging from academic circles and industry circles. So, this paper proposes applying blockchain technology to CPS and other information security risk related data's network systems, for ensuring CPS information security risk evaluation data sources are true and reliable. The logic structure of blockchain technology applying in CPS information security risk evaluation system is shown in Fig. 3 (Fig. 3 is an abstract graph, in fact, the blockchain for CPS can be different from the blockchain for Intranet or other network systems.).

The architecture of CPS includes application layer, collaborative processing layer, network layer, and physical layer [16]. The characteristics of CPS as complex, layered structure, and integration make we can construct blockchain's layered function system architecture in CPS to achieve blockchain's application. Combining the system architecture characteristics of CPS to construct blockchain's layered function system, in CPS, the blockchain's layered function architecture is shown in Fig. 4.

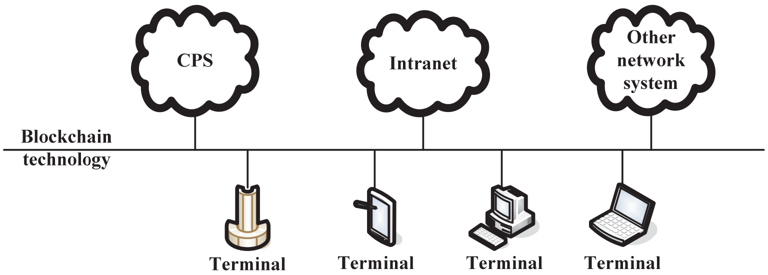

Figure 3 The CPS information security risk evaluation system logic structure based on blockchain

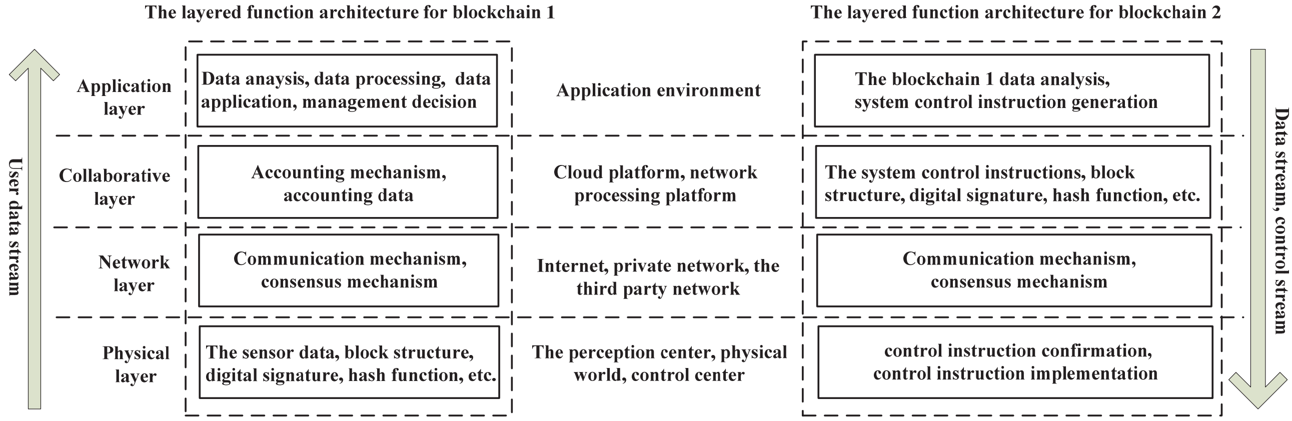
The layered function architecture for blockchain 1
The layered function architecture for blockchain 2
User data stream
Application layer
Data anaysis, data processing, data application, management decision
Application environment
The blockchain 1 data analysis, system control instruction generation
Collaborative layer
Accounting mechanism, accounting data
Cloud platform, network processing platform
The system control instructions, block structure, digital signature, hash function, etc.
Network layer
Communication mechanism, consensus mechanism
Internet, private network, the third party network
Communication mechanism, consensus mechanism
Physical layer
The sensor data, block structure, digital signature, hash function, etc.
The perception center, physical world, control center
control instruction confirmation, control instruction implementation
Data stream, control stream

Figure 4 The blockchain layered function architecture in CPS

From Fig. 4 we can see, the data stream, control stream, and layered system structure of CPS make CPS' business can be divided into two parts, so we built two blockchains (blockchain 1 and blockchain 2) to correspond to the two parts of businesses. The data characteristics, block structure, digital signature algorithm, hash function, communication mechanism, consensus mechanism, and accounting mechanism (control instruction confirmation) for the two blockchains can be different, the corresponding business subjects and authentication subjects (Because of the openness and transparency of blockchain, in CPS the blockchain system's authentication subjects' selection should meet the confidentiality requirements to the related data that risk evaluation process involving.) can also be different. The layered structure characteristics of CPS not only can meet the realization of blockchain technology route (business data generation → digital signature → business data and signed related data network broadcast → consensus authentication → distributed accounting → accounting data application), but also can make full use of the advantage characteristics of the network layer providing service to data broadcast and consensus authentication, and cloud platform or network processing platform providing service to data storage and management. In addition, in view of the confidentiality requirements to the related data that risk evaluation process involving, we can also adopt the corresponding encryption measures to the blockchain data in CPS.

For the blockchain 1, perception center digitally signs the perceived sensor data, then broadcasts through the network layer. The subjects that joined blockchain 1 in CPS may authenticate the sensor data's authenticity and source according to the blockchain 1 system granted permissions, the authenticated data would be respectively stored in the cloud platform space by each authentication subject. For the subjects that joined in the blockchain 1 in CPS, if needing to use the data of the blockchain 1, they can analyze and manage the specific data of the blockchain 1 which are owned by themselves, and apply the data analysis results to other environment or guide their management decision activities.

For the blockchain 2, the application subjects of CPS analyze the corresponding data of blockchain 1 which are owned by themselves, then produce the control instructions for CPS, the application subjects digitally sign the control instruction data in the corresponding cloud platform or other network processing platform, then broadcast through the network layer; the subjects that joined blockchain 2 in CPS may authenticate the control instruction data's authenticity and source according to the blockchain 2 system granted permissions. The authenticated data will be respectively stored in the cloud platform space by each authentication subject. After CPS application subjects' instruction data are being confirmed, the control instruction will implement the corresponding control to CPS through control center.

So, although the blockchain technology is complex, the CPS' layered structure and intelligent data interaction processing technology can achieve the seamless grafting between CPS and blockchain technology. Under the support of blockchain technology system, CPS information security risk evaluation data can be dynamically, real-time, and safely achieved from CPS, and the cloud platform or other network processing platforms which CPS rely on can also meet the strong computing power and data storage capacity requirements that were required by the blockchain technology applications.

4 CASE ANALYSIS

In this part, from a concrete situation to analyze the application of combining blockchain technology and big data. For the case construction, based on the temperature and humidity monitoring system of the Internet of things laboratory of shanxi university of finance and economics, and the gas monitoring and controlling system of tunlan mine of shanxi coking coal group, on the basis of analyzing the structure and function of the two systems, a total of 20 experts from shanxi university of finance and economics and shanxi coking coal group together constructed a case system on CPS, and intelligent home management system was a subsystem of this CPS. Using situational analysis method to evaluate and analyze the information security risks of this case system. The topology structure for this case system is shown in Fig. 5.

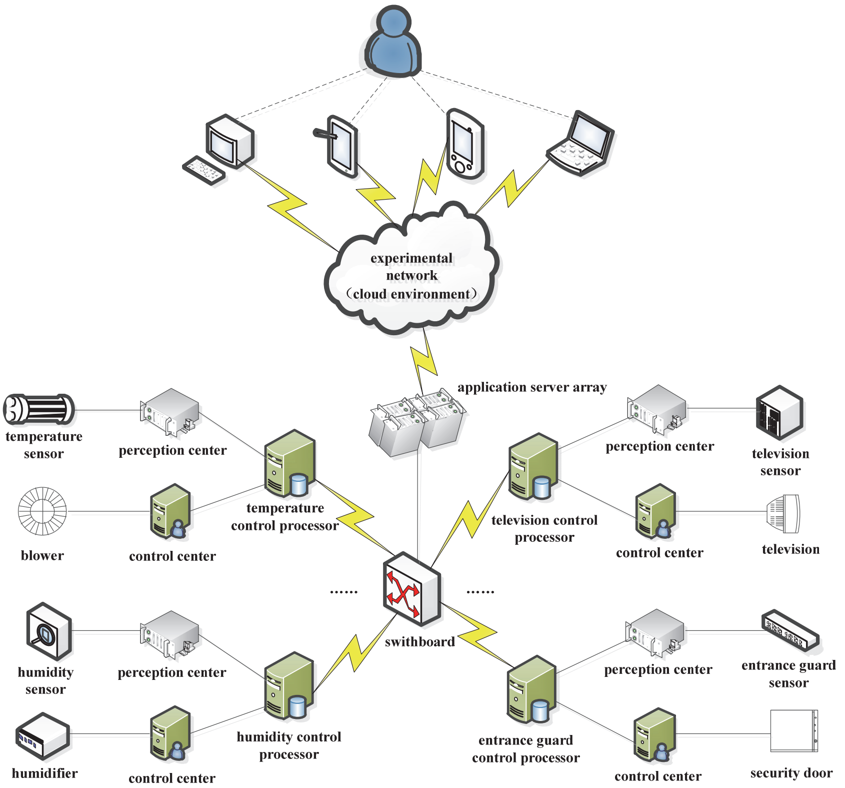

Figure 5 The topology structure for the case system

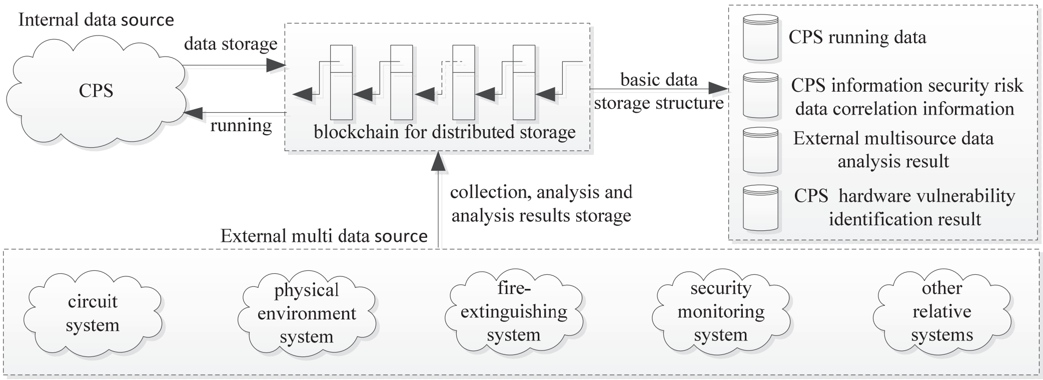
Internal data source
CPS
data storage
running
blockchain for distributed storage
basic data
storage structure
CPS running data
CPS information security risk data correlation information
External multisource data analysis result
CPS hardware vulnerability identification result
collection, analysis and analysis results storage
External multi data source
circuit system
physical environment system
fire-extinguishing system
security monitoring system
other relative systems

Figure 6 The application case architecture

4.1 The Application Case

The hardware environment of case system includes circuit system, fire control system, security monitoring system, CPS network system, physical environment system, etc. Therefore, the data sources for the hardware vulnerability identification in the case of system's information security risk evaluation not only include the interior of CPS, but also include the Intranet network of the organization and other related network systems. In view of the limited data capacity of the case system, taking the multisource data analysis instead of the big data analysis, and simulating the data acquisition and storage management for intelligent home management subsystem's hardware environment vulnerability identification process, as shown in Fig. 6.

In Fig. 6, blockchain runs in CPS, and stores all the CPS running data, at the same time links with multi data sources outside CPS, for the information security risk evaluation of CPS, basing on evaluation requirements, the multisource data will be collected, analyzed, and the analysis results will be distributed stored in the blockchain system. Because of the greatness and complexity of the data in the whole evaluation process, we store the basic data and blockchain in different storage spaces, respectively. The basic data are classified (Classified as CPS running data, external multisource data analysis results, data correlation information, and CPS hardware vulnerability identification results, etc.), and stored respectively.

For CPS external related systems (such as circuit system, fire control system, security monitoring system, etc.), we can construct blockchain system other than CPS' blockchain system respectively, and the other systems' blockchain system's structure and work principle can refer to Bitcoin blockchain and Ethereum blockchain, and these blockchains will link with the blokchain for CPS, here we don't discuss more.

4.2 Efficiency Calculation and Analysis

The main traits of the information security risk evaluation system are the application of external related big data to realize the integrity of risk acquisition and the accuracy of risk identification, and the application of blockchain technology to insure the data reliability and authenticity. Colligating the information system evaluation index system inferred in reference [17-20], and discussing by 20 experts from shanxi university of finance and economics and shanxi coking coal group, and proposing intelligent home management subsystem information security risk evaluation index system R should include: the integrity of risk acquisition (R_1), the accuracy of risk identification (R_2), the guarantee degree of data security (R_3), the adaptability of evaluation system (R_4), the cost of evaluation system (R_5), the profit of evaluation system (R_6). Colligating the experts' opinions, and giving the weight of each evaluation index as: $W = [W_1, W_2, W_3, W_4, W_5, W_6] = [0.25, 0.25, 0.2, 0.15, 0.1, 0.05]$. Therein, W_1, W_2, W_3, W_4, W_5, W_6 correspondingly represent the weight of R_1, R_2, R_3, R_4, R_5, R_6.

Limiting the score value of each expert giving to each index from low to high to interval [0,1], and giving the score values of R_1, R_2, R_3, R_4, R_5, R_6 in intelligent home management subsystem based on blockchain and big data as C_A, and based on traditional system as C_B, computing the average value of the score values of R_1, R_2, R_3, R_4, R_5, R_6 given by each expert as $\overline{C}_A$ and $\overline{C}_B$, the results are shown in Tab. 1.

Table 1 The score values of each index evaluation value

$\overline{C}$	R_1	R_2	R_3	R_4	R_5	R_6
$\overline{C}_A$	0.95	0.95	0.96	0.86	0.42	0.96
$\overline{C}_B$	0.59	0.69	0.66	0.95	0.25	0.84

Taking the cost as negative value and calculating the expected efficiency values under different evaluation systems, the expected efficiency value of intelligent home management subsystem information security risk evaluation based on blockchain and big data can be calculated as:

$$\begin{aligned}&\overline{E}_A = W \times (\overline{C}_A)^{\mathrm{T}}\\&= (0.25\ 0.25\ 0.20\ 0.15\ 0.10\ 0.05)\\&\times (0.95\ 0.95\ 0.96\ 0.86 - 0.42\ 0.96)^{\mathrm{T}}\\&= 0.802\end{aligned}$$

The expected efficiency value of intelligent home management subsystem information security risk evaluation based on traditional system can be calculated as:

$$\begin{aligned}&\overline{E}_B = W \times (\overline{C}_A)^{\mathrm{T}}\\&= (0.25\ 0.25\ 0.20\ 0.15\ 0.10\ 0.05)\\&\times (0.59\ 0.69\ 0.66\ 0.95 - 0.25\ 0.84)^{\mathrm{T}}\\&= 0.6115\end{aligned}$$

From Tab. 1 we can see, the experts generally recognize the guarantee function of blockchain in data security, the value of big data analysis to the integrity of risk acquisition and the accuracy of information security risk evaluation, but the experts also recognize the application of blockchain and big data will bring challenge and cost increase to actual operation,. So, promoting the application of blockchain technology and big data technology in the field of CPS, and saving the application cost, are the important problems needed to be solved in the future of blockchain and big data technology extensively applied in CPS information security risk evaluation.

By comparing $\overline{E}_A$ with $\overline{E}_B$ we can see, the experts have recognized the value of blockchain and big data application in CPS information security risk evaluation.

5 CONCLUSIONS

Comparing to traditional information systems, the information security risk evaluation for CPS is more complex, so, the traditional information security risk evaluation methods are also unsuitable for efficiently describing the evaluation process and evaluation results of CPS. For improving the integrity and accuracy of CPS information security risk evaluation, this paper proposes to introduce CPS external risk evaluation related big data to perfect the evaluation process. Aiming at the characteristics of data sources are numerous, data capacity is huge, data structure is alienation for CPS information security risk evaluation related big data, and the authenticity, reliability requirement for information, this paper proposes the thought of applying blockchain technology to CPS information security risk evaluation system. In the part of case analysis, we calculated and analyzed the efficiency of the evaluation system for this paper.

By using Petri net model, big data technology, blockchain technology, RBF neural network model, etc., this paper constructs an information security risk evaluation system for CPS, but we do not go a step further to research the realization process of the evaluation system. In view of the characteristics of CPS, some difficulties can occur in the risk evaluation realization process, the prominent difficulties are:

(1) The definition for CPS external information security risk evaluation related multi data sources, the collection, management and analysis to the risk evaluation related big data.

(2) The construction and operation of blockchain in the physical environment of evaluation system.

Hereafter, we will implement the risk evaluation system, comprising the construction of data processing environment, the realization of evaluation model and evaluation process model, and the application of blockchain technology. Because CPS and blockchain technology both are new products, existing application and research results are very rare, so the difficulties and challenges are much in the course of implementation.

Acknowledgements

This work was supported by the National Social Science Fund of China under Grant 18BTQ083.

This paper is a revised and expanded version of a paper entitled [CPS Information Security Risk Evaluation System Based on Petri Net] presented at [2017 IEEE Second International Conference on Data Science in Cyberspace, Shenzhen, China, 26 June 2017].

6 REFERENCES

[1] https://baike.baidu.com/ (05.05.2018)

[2] https://ptolemy.berkeley.edu/projects/cps/ (03.04.2018)

[3] Wang, Z. J. & Xie, L. L. (2011). Cyber-physical Systems: A Survey. *Acta Automatica Sinica*, *37*(10), 1157-1165.

[4] http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Publikation_Medien/Vortraege/download//CPS_27Feb2013.pdf. (01.10.2016)

[5] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286. (01.10.2016)

[6] http://www.cstc.org.cn/templet/default/show_zyfw.jsp?id=1293. (01.10.2016)

[7] Jiang, Z. B. (2004). *Petri net and its application in modeling and control of manufacturing system*, Beijing, China: Machinery Industry Press, 21.

[8] Fu, Y. G. & Zhu, J. M. (2016). Network Supplier Credit Evaluation Model Based on Big Data. *Journal of Central University of Finance and Economics*, 348, 74-83.

[9] Nakamoto, S. (2009). Bitcoin: a peer-to-peer electronic cash system. https//bitcoin.org/bitcoin.pdf. (11.11.2016)

[10] Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *Journal of Financial Perspectives*, 33, 92-113. https://doi.org/10.2139/ssrn.2646618

[11] Goertzel, B., Goertzel, T., & Goertzel, Z. (2016). The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons. *Technological Forecasting and Social Change*, (4), 1-9.

[12] Zhu, J. M. & Fu, Y. G. (2016). Supply chain dynamic multi-center coordination authentication model based on blockchain. *Chinese Journal of Network and Information Security, 2*(1), 27-33.

[13] Tsai, W. T., Yu, L., Wang, R., Liu, N., & Deng, E. Y. (2017). Blockchain Application Development Techniques. *Journal of Software, 28*(6), 1474-1487.

[14] Morselli, R., Bhattacharjee, B., Katz, J., et al. KeyChains: A decentralized public-key infrastructure. https://www.researchgate.net/publication/228714967_Keychains_A_decentralized_public-key_infrastructure. (10.10.2016)

[15] Kuo, T. T., Hsu, C. N., et al. ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. http://8btc.com/doc-view-838.html. (12.12.2017)

[16] Zhang, K., Zhang, G. Q., & Zhang, M. T. (2011). A Preliminary Framework for Designing the Trusted Cyber-Physical Systems. *Journal of Computer Research and Development*, 48, 242-246.

[17] Chen, J. (2009). *Course for Information System Development Method* (*the third edition*). Beijing: Tsinghua University Press, 242-243.

[18] Liu, K., Guo, Y., & Pan, Y. (2012). Information System Evaluation Research Based on Multidimensional utility coalition. *Information Studies: Theory and Application, 35*(3), 103-108.

[19] Chen, J. M. & Zhang. Z. Y. (2000). Application of fuzzy method in information system evaluation. *Chinese Journal of Management Science, 8*(1), 75-80.

[20] Xu, B. X. & Wang, X. (2007). *Information System Development Method*. Beijing: Machinery Industry Press, 190-200.

Contact information:

Yonggui FU, Associate Professor
(Corresponding author)
School of Information Management,
ShanXi University of Finance and Economics,
696 Dock City Road, Xiaodian District, Taiyuan 030006, Shanxi Province, China
E-mail: fygzcd@163.com

Jianming ZHU, Professor
School of Information, Central University of Finance and Economics,
39 South College Road, Haidian District, Beijing 100081, China

Sheng GAO, Associate Professor
School of Information, Central University of Finance and Economics,
39 South College Road, Haidian District, Beijing 100081, China