2018 IEEE 16th Int. Conf. on Dependable, Autonomic & Secure Comp., 16th Int. Conf. on Pervasive Intelligence & Comp., 4th Int. Conf. on Big Data Intelligence & Comp., and 3rd Cyber Sci. & Tech. Cong.

A Blockchain-based Risk and Information System Control Framework

Shenglan Ma[1], Hao Wang[2*], Hong-Ning Dai[3], Shuhan Cheng[1], Ruihua Yi[1], Tongsen Wang[1]
1. Division of Science and Technology, Fujian Rural Credit Union, Fujian, China
2. Department of ICT and Natural Sciences, Norwegian University of Sci. & Tech., Aalesund, Norway
3. Faculty of Information Tech., Macau University of Sci. and Tech., Macau, China
* Corresponding Author: Hao Wang, Norwegian University of Sci. & Tech., hawa@ntnu.no

***Abstract*—Risk and Information System Control Framework in business includes the methods and processes to manage risks and seize opportunities which involve identifying particular risk events relevant to the objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. In order to provide better support for the backtracking, traceability, irreversibility, and credible requirements of risk registration table data in the framework, this paper proposes a blockchain-based risk and information system control framework. A risk association tree is designed for combining summarized risk item ledgers with risk assessment ledgers and risk response ledgers based on the *Merkle Tree*. Three proposed smart contracts are used in risk identification, risk assessment, risk response and mitigation, and risk and control monitoring and reporting processes. We implement a prototype for this framework.**

***Keywords*—risk and information system control framework; blockchain; risk association tree; smart contract;**

I. INTRODUCTION

In today's business environment, enterprises need to innovate in order to survive and flourish. Innovation, however, almost always involves risk. To maintain or attain their competitiveness, future-thinking enterprise leaders are increasingly recognizing the need for how to implement and align effective risk management and control frameworks with their enterprise's business goals [1]. Risk is the combination of the probability of an event and its result. In the IT environment, risk is viewed as an unfavorable factor that may threaten the organization's assets or cause damage, with duality of good/bad [2]. Risk management can coordinate and guide the enterprises' coordination activities regarding related risks. Effective risk management helps maximize opportunities. The goal of Risk and Information Systems Control is to discover and mitigate all risks in an appropriate manner, and to ensure that the organization reduces the risks to an acceptable level that will not be harmed by the risks that should have been identified and mitigated. After identifying and assessing the risk, the risk owner selects the appropriate response plan and develops the risk action plan to be implemented, or modifies the control selected to mitigate the risk. The control must regularly monitor and report risk to management, and monitor risk-related trends, compliance and issues [3]. Meanwhile with the changes in external and internal environments, technological advances, the nature of attacks and the evolution of attackers, risk management needs to revisit risk management efforts and reassess risks while revising risk response plans. Continuously monitoring IT risks and controls and reporting to relevant stakeholders can ensure that IT risk management strategies are consistently effective and consistent with business goals. Due to the large number of risk data affiliates, the data of risk identification and response plans cannot be tampered with. Current risk management process mainly has three deficiencies. The first aspect is that data acquired are easy to miss. The risk staffs mainly copy and perform data preprocessing on the enterprise database, inevitably causing data loss damage. The second aspect is that electronic data are easy to tamper with and leaving no trace behind. Manual recording has been replaced by software monitoring, which has caused historical changes in the form of recording data, and electronic data have become the subject of audit verification. Compared with paper data, electronic data are easy to tamper with and no tampering marks remaining after tampering. The third aspect is that the data level security are low. Regardless of the cloud-based [4] or shared model is used to build real-time risk management platforms, business data have always been subject to greater security risks. Business data are the core secrets of the entity. Once the central database is attacked by hackers, business data are leaked.

In order to address these issues, a new blockchain-based risk and information system control framework is designed. A blockchain as a continuously growing list of records managed by a peer-to-peer (P2P) network is widely used in various application scenarios, and often combined with artificial intelligence [5], cloud computing [6], big data [7], the Internet of Things (IoT) [8] and other technologies [9-10]. Blockchain can run secure computations while no one but the data owner has access to the raw data [11]. In recent years, there have been a number of blockchain frameworks proposals appearing. Nowadays, scholars have done a lot of research on the application of blockchain [12-13], and have expanded and applied the technologies in government governance [14], medical treatment [15-16], electricity [17], digital storage [18], education [19] and other fields. The automatic execution is an important attribute for smart contracts [20]. Platforms running user-defined smart contracts and executing user-supplied transactions on their objects are also carried out [21-22].

With blockchain technology, risk register tables (including the risk identification, assessment and response plans) that are changed and modified in risk identification, risk assessment, risk response and risk control can be stored in blockchains, enabling the sharing of risk among organizations, personnel

978-1-5386-7518-2/18/$31.00 ©2018 IEEE
DOI 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00031

and equipment. Risk register table data cannot be tampered with, and can be traced. The framework uses multi-level risk association tree to track different risk management modules in risk smart ledgers, and designs smart contracts to automate the calculation of key performance indicators (KPIs) and key risk indicators (KRIs) [23] to improve risk early warning and risk response automation capabilities. A concrete blockchain-based risk and information system control framework technical implementation is fulfilled. This paper is divided into five sections. Section II analyses risk and information system control framework. Section III proposes three types of risk smart ledgers combined with different risk management modules and also proposes risk association tree to establish the relationship among ledgers. In addition, it also proposes risk contracts to improve risk management and automation control capabilities. While Section IV uses the proposed framework to design and fulfill the blockchain-based technical implementation. Finally, we draw our conclusion in Section V.

II. Risk and Information System Control Framework

Risk management can be seen as an activity that needs to be performed to predict the challenges and reduce their probability and impact. Effective risk management can help maximize the use of opportunities. Risk is a factor that must be assessed at all levels of the organization: the strategic level, the business unit level and the information system level. IT risk management refers to the implementation of risk strategies that reflect the organizational management culture, preferences and tolerances, and considers technology and budgets as well as addressing regulatory and compliance requirements. An effective IT risk management strategy is critical to the organization's ability to effectively implement its overall business strategy.

Risk and information system control framework is a periodic process. The first step in the IT risk management process is to identify IT risks, including confirming risk scenarios and risk frameworks, and the process of identifying and documenting risks. The risk identification generates a risk list and documents (mainly risk register table) as the basis for IT risk assessment in the next phase of the process. Assessing risks and prioritizing them can provide management with the data needed for risk response and mitigation (phase 3 of the cycle) to seek and implement cost-effective ways to eliminate risks that have been identified and assessed. The final phase is risk and control monitoring and reporting. This phase will monitor the implementation of the controls, risk management tools and current status, and then report the results back to top management. This process repeats as the risk environment changes with the result of internal or external factors.

Fig 1 shows the life cycle of the risk and information system control framework.

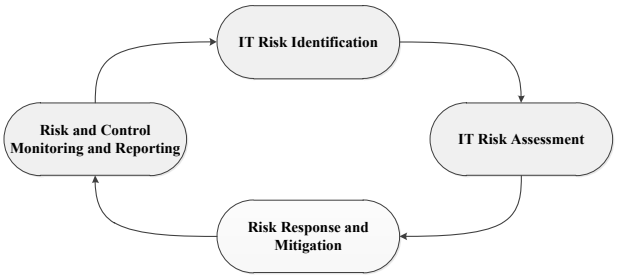

Fig. 1. Life Circle of Risk and Information System Control Framework Figure

The framework is based on the complete cycle of all elements. Failure to perform any one of these phases in a complete and comprehensive manner may result in defects in the next phase, resulting in inefficiencies in the overall process. From the perspective of risk management, members in risk and information system control include senior management, IT departments, risk practitioners, auditors, etc., and the associated systems include BCP operating system (including IoT monitoring equipment) ,project management system and internal information management systems, etc. Through risk management, organizations try to reduce IT risk to an acceptable level, identify possible threats, and implement appropriate mechanisms to detect, control negative events, and recover from incidents.

1. Risk identification is the process of discovering, identifying, and documenting the risks faced by the organization. It is the first of four processes in the life cycle. Risk identification includes not only the organization itself, but also its external dependencies and assumptions, such as the availability of contract workers or the timely delivery of materials.

2. After identifying and recording risks on the risk register table, the phase is assessing the level of IT risk. When calculating or evaluating IT impact it must consider the dependencies of other systems, departments, business partners, and users on the affected IT systems. Sometimes the assessment includes: the critical functions required for a company to continue operations; the risks associated with each key function; the control based on the likelihood that the risk is extremely high; the prioritization of risks based on the likelihood and potential impact of the risk; risk and corporate risk; the relationship between preference and tolerance.

3. The risk response focuses on the correct response to risk-related decisions. This phase requires the rationality of making risk-response decisions, and provides plans to implement changes to the agreement based on a reasonable timetable.

4. The organization relies on its monitoring and reporting capabilities to identify the risks which have been assessed and mitigated. The best way to risk monitoring and management is to monitor a reasonable condition that is wide enough to provide a risky environment without losing the results in the data flood. Identifying and using key risk indicators (KRIs) and key performance indicators (KPIs) can greatly improve the continuous monitoring process. Continuous monitoring is a necessary step in the risk management life cycle.

As the IT risk management procedure should be comprehensive, complete, auditable (available for independent third party review), justified (for reasonable reasons), compliant (in line with policies, laws or regulations), monitored (restricted to review and accountability), enforcement (consistent, mandatory and necessary), timely updating (followed by changed business processes, technology and law) and managed (with sufficient resources, supervision and support), the use of blockchain technology can well support the requirements of backtracking, tracking, falsification and multi-trust in the risk and information system control framework.

III. SMART LEDGERS, RISK ASSOCIATION TREE AND SMART CONTRACTS

This section designs corresponding risk smart ledgers, risk association tree based on Merkle Tree [24] and smart contracts based on Risk Blockchain.

A. Risk Smart Ledgers

In the risk smart contracts, the risk register table formed in the process of risk identification is kept. The contracts are updated according to the process of risk analysis and control. Risk smart contracts are divided into three types. First is the summarized risk item ledger, which holds a complete account of risk from identification to response. Second is a risk assessment ledger, which holds account information for different assessment situations for one of the risk items. Third is the risk response ledger, which saves the account for the different response program under one of the identification items. Fig 2 shows three types of ledgers.

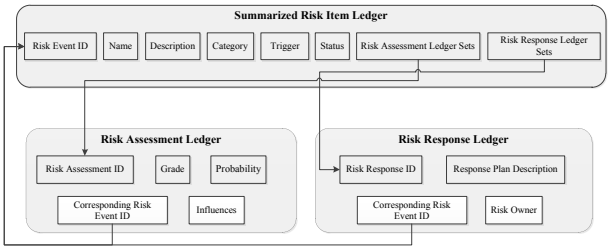

Fig. 2. Three Types of Smart Ledgers

The following explains the key attributes in the ledgers:

Risk Event ID. Risk managers need to quickly find a specific risk event, so they need to use a unique sign to identify each risk, such as giving a number.

Name. A brief name is descripted for risk such as a server failure, a test that cannot be completed on time, a reduced consulting cost or a good reputation.

Description. Because the name of a risk event is often too short, it also provides a more detailed description.

Category. The enterprises classify the risks. E.g., server failures can fall into the category of technology or hardware technology.

Trigger. A trigger is a sign or symptom of the actual occurrence of a risk event. E.g., cost overflows from early activities may be a symptom of poor cost estimates; defective products may be a sign of low quality of supply materials. Documenting the potential symptoms of project risks also helps the project team identify more potential risk events.

Status. Status is the current formation of a risk, such as the occurrence of a risk event and the corresponding countermeasure execution. E.g., after the related clauses in the contract are executed, the risk status of server failure has been set ‘dealt with’.

Grade. A grade is often a number. E.g. one indicates the highest level of risk.

Probability. Risk events always have different potentiality to happen. E.g. the server may have a lower probability of failure.

Influence. If a risk event really happens, it will always have a big or medium, or small impact on achieving the aim . E.g., a failed server may have a big impact on completing projects on time and successfully.

Response Plan Description. A detailed response plan is formulated. E.g., a possible response to a server failure risk event is to replace the defective server within the negotiated cost range and within a certain period of time in compliance with the relevant clauses in the contract with the supplier.

Risk Owner. Someone who is responsible for any related risk events and implements a strategy for coping.

B. Risk Association Tree

Since a complete risk register table has three types of ledgers, and the risk assessment ledger and the risk response ledger sets are subsets of the summarized risk item ledger, it is necessary to use the Merkle Tree to establish the relationship among the ledgers in order to quickly and cost-freely locate the latest information on the corresponding risk register.

Then three risk Merkle Trees are designed based on the characteristics of the blockchain:

1. Transaction tree (tx), which holds transactions in specific blocks;

2. Receipts tree, which are essentially multiple pieces of data that show the impact of each transaction;

3. Risk association tree (RAT), which holds the relationship among the three types of ledgers.

Among them, the first two trees are commonly used in the blockchain to reduce the client's saving data and ensure data consistency. The risk association tree establishes the association relationship among the three types of ledgers that are rapidly related to each other through the hash relationship.

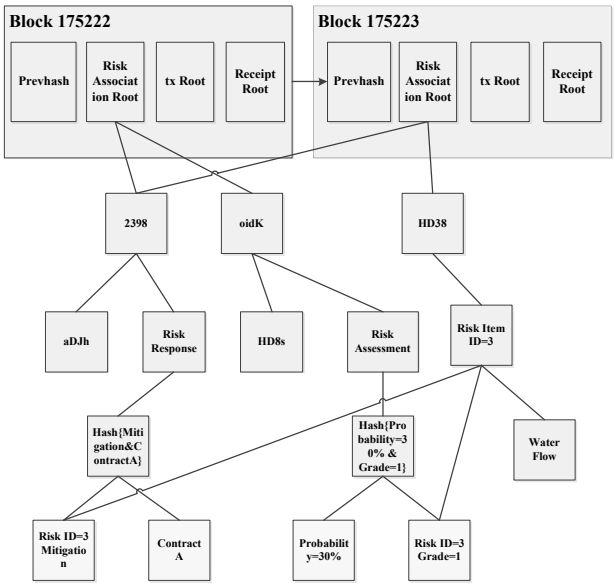

Fig. 3. Risk Association Tree Figure

As shown in Fig 3, Block 175222 writes risk identification ledger and risk response ledger, and risk item ledger is written in Block 175223. The risk item, risk assessment and risk response are utilized by the hash values. Establish an association relationship ('Risk Item ID=3' establishes a relationship with 'Grade=1' and 'Mitigation' through the tree node relationship), and then each block chain agent only needs to download the corresponding block header. E.g., using the hash value of risk assessment id and risk response id in the 'Risk Item ID=3' ledger on the Block 175223, it can quickly find the risk response and risk assessment data in the Block 175222 by the Merkle Tree. Similarly, for the known corresponding risk item ID in the risk assessment ledger in the Block 175222, the hash value can be used to locate the data in the 'Risk Item ID=3' ledger on the Block 175223.

C. *Risk Smart Contracts*

Due to risk control, regular assessments and tests are necessary to effectively identify new risks and emerging risks. Since the constantly changing nature of risks and related controls, continuous monitoring is a necessary step in the risk management life cycle.

To this end, when building smart contracts for risks, three types are mainly implemented. The first contract is based on the risk identified and evaluated data, and automatically calculates the KPIs and KRIs. The second contract is dynamically adjusting the risk approval level according to the risk appetite, agreement SLA and the implementation of response plans in the risk ledger, increasing or decreasing the approval level while automatically modifying the status according to the risk response plan ledger. The third contract is required after the modification of the risk register table. The risk status should be updated only after the corresponding decisions of managements.

Smart Contract 1: KPIs and KRIs Automatically Calculation

1. Getting corresponding *Risk Event ID* for the type of blockchain transaction ledger is risk identification ledger or *Risk Response Ledger*;

2. Obtaining the corresponding *Summarized Risk Item Ledger* from the *RAT* according to the *Corresponding Risk Event ID* to obtain the latest Item value;

3. Calculating the index value of the KPI and KRI indicators;

4. Generating the new *Summarized Risk Item Ledger* transaction block, put on the chain and wait for consensus confirmation.

Smart Contract 2: Approval Level Dynamic Adjustment

1. Getting corresponding *Risk Event ID* for the type of blockchain transaction ledger is *Risk Response Ledger* or *Risk Response Ledger*;

1.1 Obtaining the corresponding *Summarized Risk Item Ledger* from *RAT* according to the *Corresponding Risk Event ID* to obtain the latest Item value;

1.2 Calculating the influences of changed status of the risk response;

1.3 Generating the new approval level for influence rules;

1.4 For the change of risk status, then prototype generates a new *Summarized Risk Item Ledger* transaction block, and calls *Smart Contract 3* for consensus.

2. Getting corresponding *Risk Response Ledger Sets* for the type of blockchain transaction ledger is *Summarized Risk Item Ledger*;

2.1 Obtaining the risk response plans in the corresponding *Risk Response Ledger* according to each ID in the sets;

2.2 Calculating the approval level by the changed risk response plans summarized in the sets;

2.3 Updating the approval level in the *Summarized Risk Item Ledger* and submit a consensus.

2.4 For the change of risk status, prototype generates a new *Summarized Risk Item Ledger* transaction block, and calls *Smart Contract 3* for consensus.

Smart Contract 3: Status Changing Confirmation

1. Getting corresponding *Risk Event ID* for the type of blockchain transaction ledger is *Risk Assessment Ledger* or *Risk Response Ledger* and risk status changed;

1.1 Obtaining the corresponding *Summarized Risk Item Ledger* from the *RAT* according to the *Corresponding Risk Event ID* to obtain the latest Item value;

1.2 Judging whether it needs approval to modify the status;

1.3 If it is not allowed to modify the status, a new pending status is generated and a new *Summarized Risk Item Ledger* transaction block is generated for consensus. If it is allowed, then put on the chain and wait for consensus confirmation.

2. Getting corresponding *Risk Event ID* for the type of blockchain transaction ledger is *Summarized Risk Item Ledger* and risk status changed;

2.1 Judging whether it needs approval to modify the status;

2.2 If it is not allowed to modify the status, a new pending status is generated and a new *Summarized Risk Item Ledger* transaction block is generated for consensus. If it is allowed, then put on the chain and wait for consensus confirmation.

IV. A Prototype Blockchain-based System

This section describes the realizations of blockchain-based risk and information system control framework. First, the architecture of the information system is designed, and the network structure diagram covering various participants is given. Then it describes the sharing of risk information and the application process of smart contracts in combination with the four processes of the life cycle.

A. System Architecture

This section describes the realizations of blockchain-based risk and information system control framework. First, the architecture of the information system is designed, and the network structure diagram covering various participants is given. Then it describes the sharing of risk information and the application process of smart contracts in combination with the four processes of the life cycle.

The framework is mainly divided into four layers, such as Portal Layer, Platform Layer, Integrated Platform Layer and Blockchain Agents, as shown in Fig 4. Portal Layer provides risk management personnel, auditors and management within the organization with an intuitive risk management process sights. Platform Layer provides blockchain-based risk management, including indicator setting (KPI and KRI), risk identification, risk assessment, risk response plan and risk reporting. Integrate Platform Layer connects with multiple systems within the enterprise and obtains corresponding risk data, including risk response plan project execution status and server risk monitoring data. Blockchain Agents provide access to the risk blockchain.

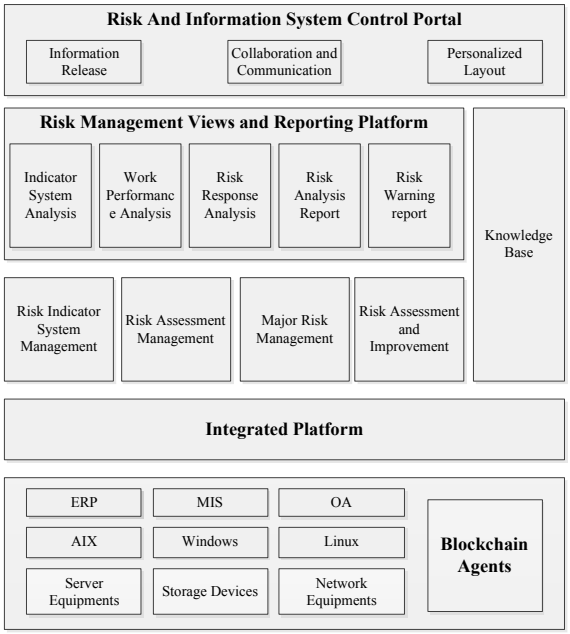

Fig. 4. Framework Prototype Figure

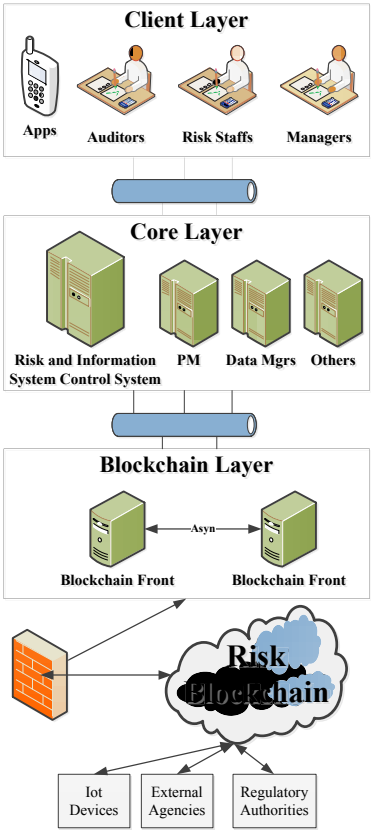

Fig. 5. Network Structure Figure

Fig 5 shows the network structure. Risk and information system control prototype does internal risk services to personnel, auditors, management personnel, associated IoT devices and internal management systems while does external services to external auditors and regulatory agencies (E.g., our banks, Fujian rural credit union (FRCU), are supervised by the China Banking Regulatory Commission) by spreading the own data via blockchain.

Based on blockchain the enterprise can build a trusted risk blockchain information flow. And outside the enterprise, the participants cover the IoT devices, external agencies and regulatory authorities. IoT devices (mainly equipment room, waterproof, electrical and etc.) automatically obtain blockchains and dynamically adjust their own risk warning and response strategies. External agencies automatically trigger corresponding risk response services based on the SLA agreement with the enterprise. Regulatory Authorities is mainly responsible for the supervision of risk management and regulated companies by analyzing the risk information in the blockchain.

B. Blockchain based Risk and Information System Control Prototype

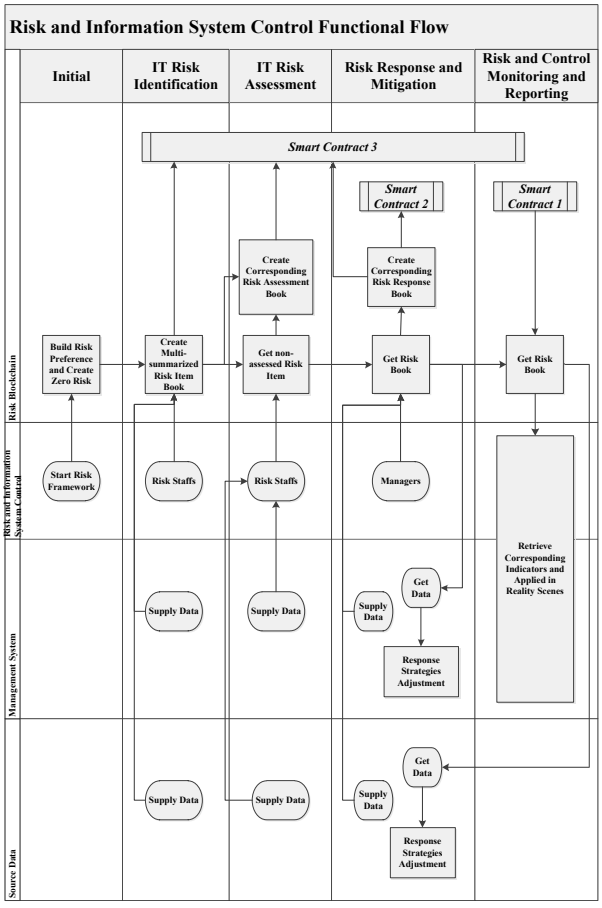

Fig. 6. The Overall Prototype Flow Procedures Figure

The blockchain-based risk and information system control prototype procedures are mainly divided into risk identification, risk assessment, risk response and mitigation, and risk and control monitoring and reporting. When the enterprise establishes the risk management framework at its earliest stage, a risk appetite is formed according to the enterprise's strategy, market environment, regulatory requirements and internal conditions, meanwhile the initial risk ledger is written (zero risk initial). Functional flows is shown in Fig 6.

1. Risk Identification

In this process, identification risk data are generated mainly through artificial identification of risk personnel and automated monitoring of machines or data centers. These identifications include software or platform auto-detection servers or desktop operating systems, middleware vulnerabilities, and environmental controls (e.g., power outages, insufficient generator capacity, HVAC overheating, lack of water and safe operating areas). The source of the collected risk data is shown in Table I.

TABLE I. RISK FACTORS

Factors	Detailed factors
External Environment	Market and economic factors Market/product life cycle replacement frequency Industry and competition Geopolitical situation Regulatory environment Technical status and development Threat panorama
Internal Environment	Business goals and objectives IT's strategic importance to the business IT complexity Physical complexity and degree of change Change management capabilities Operational model Strategic priority company culture Financial ability
Risk Management Capabilities	Risk Governance Risk Management
IT Related Capabilities	Assessment, Guidance, and Monitoring Adjustment, Planning and Organization Build, Buy, and Implement Delivery, Service, and Support Monitoring, Evaluation and Evaluation

For identified risk items, a general ledger of risk items is constructed, different risks are distinguished by different identification ID, written in the blockchain, and the Smart Contract 3 is triggered.

2. Risk Assessment

In this process, risk personnel obtain the identified but not yet assessed risks in the blockchain, the existing control values (control status) and risk appetite in the blockchain, then perform risk assessments (assessing the current risk level exceeds all situations where risk levels are acceptable). In addition, the Integrated Platform can also use data analysis methods to evaluate the risk rating results by extracting the business system data within the enterprise. The results are

written into the blockchain in the form of risk assessment ledger and trigger simultaneously Smart Contract 3 Risk. These results are sometimes shown as 'risks within the risk appetite range are acceptable', 'risks outside the risk appetite but within risk tolerance are not acceptable' and 'risks outside the risk tolerance range are totally unacceptable'. Through the blockchain, it can ensure that all IT risks are evaluated and not deliberately bypassed, reducing the risk of being missed.

3. Risk Response and Mitigation

The management is responsible for assessing and responding to the risk register tables and risk assessment reports in the blockchain, generating risk response plans (risk acceptance, risk mitigation, risk transfer and risk avoidance) after execution of the approval. The response plans are in the form of Risk Response Ledger to consensus in the blockchain.

Risk mitigation is a mode of use control. It can be either an active attempt to prevent an accident or a passive permission to detect, contain and recover from an accident. To this end, three common blockchain-based risk mitigation responses are listed below:

(1) For HVAC and other data center control equipment, it is possible to obtain a risk response ledger corresponding to its own equipment ID, for example, when a certain type of risk occurs, the response of the spray system is used, thereby the control strategy of its own equipment for automatic monitoring and operation is changed.

(2) The project management platform acquires the data in the risk response ledger in the blockchain that needs to establish the corresponding projects. The progress of the risk control test and the achievement of the milestones obtained during the mitigation in the project progress are also written in the risk register table to maintain the accuracy and timeliness of the data in the blockchain, ensuring that the risk ledgers are always available.

(3) Any change to the risk environment may affect the accuracy and appropriateness of the plan associated with continuity or recovery. For example, the risk previously accepted by management may now need to be eased. Therefore, after the changing of risk response ledgers, business continuity plan (BCP) and disaster recovery plan (DRP) need to be adjusted accordingly, and sent to the appropriate person for approval and processing, triggering Smart Contract 2 and Smart Contract 3.

In the process of risk response, the OA system can obtain the ledgers through the blockchain for the processes that require approval, thereby generating an approval flow to the corresponding responsible persons.

4. Risk and Control Monitoring and Reporting

In this process, Smart Contract 1 is used to automatically calculate KRI and KPIs from various data sources and reporting risks. In addition to conventional project documents, changed documents, problem logs, and configuration, now historical risk assessment ledger data (previous risk assessment results) and risk response ledger data (security and test reports) can provide more comprehensive control services.

In addition, the experience based in the risk management prototype can directly obtain the historical risk chain items in the blockchain as processed or responded, and the corresponding risk assessment ledger and risk response ledger as the historical experience through the risk association tree.

V. CONCLUSIONS

Risk management refers to the processes of how to minimize risks in a sure-risk environment. Risk and information system control refers to the method of management that takes the initiative to deal with risks proactively, purposefully and programmatically through the recognition, measurement and analysis of risks, and strives to obtain maximum security guarantees with minimal costs. Current systems of risk and information system control cannot guarantee continuous tracking and tamper-proof of risk information, which often leads to lack of risk identification and solutions, especially significant risks to the company. This paper establishes a mechanism for sharing risk information among insiders, IoT devices and information systems based on the risk and information system control framework, and uses blockchain technology to ensure that information can be tracked and tampered with. This paper designs three kinds of risk intelligent ledgers and establishes the relationship through the risk association tree. The paper also designs three kinds of risk smart contracts for automatic risk calculation and approval flow control during risk identification, risk assessment, risk response and mitigation as well as risk and control monitoring and reporting. A blockchain-based system prototype is designed to realize risk data sharing with information systems, IoT devices and management personnel on the information chain.

VI. ACKNOWLEDGEMENT

This work is partially funded by the Fujian Fumin Foundation and partially supported by the National Natural Science Foundation of China under Grant No. 61672170 and the Science and Technology Planning Project of Guangdong Province under Grant No. 2017A050501035.

REFERENCES

[1] Purdy G. ISO 31000: 2009—setting a new standard for risk management[J]. Risk analysis, 2010, 30(6): 881-886.

[2] ISO P N. IEC 27005 Information technology[J]. Security techniques. Information security risk management, 2011.

[3] Fraser J R S, Simkins B J, Fraser J. Enterprise risk management: An introduction and overview[M]. John Wiley & Sons, Inc., 2010.

[4] Horwath C, Chan W, Leung E, et al. Enterprise risk management for Cloud Computing[J]. COSO.[Online]. Available: http://www. coso. org/documents/Cloud\% 20Computing\% 20Thought\% 20Paper. pdf, 2012.

[5] Omohundro S. Cryptocurrencies, smart contracts, and artificial intelligence. AI matters, 2014, 1(2): 19-21.

[6] Gaetani E, Aniello L, Baldoni R, et al. Blockchain-based database to ensure data integrity in cloud computing environments. 2017.

[7] Liu P T S. Medical record system using blockchain, big data and tokenization//International Conference on Information and Communications Security. Springer, Cham, 2016: 254-261.

[8] Conoscenti M, Vetro A, De Martin J C. Blockchain for the Internet of Things: A systematic literature review//Computer Systems and

Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of. IEEE, 2016: 1-6.

[9] Hou H. The Application of Blockchain Technology in E-Government in China//Computer Communication and Networks (ICCCN), 2017 26th International Conference on. IEEE, 2017: 1-4.

[10] Frey R, Wörner D, Ilic A. Collaborative Filtering on the Blockchain: A Secure Recommender System for e-Commerce. 2016.

[11] Manset D. Big Data and Privacy Fundamentals: Toward a "Digital Skin"//The Digitization of Healthcare. Palgrave Macmillan, London, 2017: 241-255.

[12] Gatteschi V, Lamberti F, Demartini C, et al. Blockchain and smart contracts for insurance: Is the technology mature enough?. Future Internet, 2018, 10(2): 20.

[13] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts//Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016: 839-858.

[14] Atzori M. Blockchain technology and decentralized governance: Is the state still necessary?. 2015.

[15] Yue X, Wang H, Jin D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 2016, 40(10): 218.

[16] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management//Open and Big Data (OBD), International Conference on. IEEE, 2016: 25-30.

[17] Sikorski J J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy, 2017, 195: 234-246.

[18] Sreehari P, Nandakishore M, Krishna G, et al. Smart will converting the legal testament into a smart contract//Networks & Advances in Computational Technologies (NetACT), 2017 International Conference on. IEEE, 2017: 203-207.

[19] Sharples M, Domingue J. The blockchain and kudos: A distributed system for educational record, reputation and reward//European Conference on Technology Enhanced Learning. Springer, Cham, 2016: 490-496.

[20] B. Egelund-Müller, M. Elsman, et al. Automated Execution of Financial Contracts on Blockchains. Business & Information Systems Engineering,(2017):1-11.

[21] Liang J, Han W, Guo Z, et al. DESC: enabling secure data exchange based on smart contracts[J]. Science China Information Sciences, 2018, 61(4): 049102.

[22] Corrales M, Jurcys P, Kousiouris G. Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework[J]. 2018.

[23] Beasley M S, Branson B C, Hancock B V. Developing key risk indicators to strengthen enterprise risk management[J]. ERM Initiative at North Carolina State University and the Committee of Sponsoring Organizations of the Treadway Commission, Raleigh, NC, 2010.

[24] Merkle R C. A digital signature based on a conventional encryption function[C]//Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1987: 369-378.