IADIS International Journal on Computer Science and Information Systems
Vol. 15, No. 2, pp. 29-43
ISSN: 1646-3692

RELIABLE ARCHITECTURE OF CROSS ORGANIZATIONAL WORKFLOW MANAGEMENT SYSTEM ON BLOCKCHAIN

Hirofumi Nagano[1], Taku Shimosawa[1], Atsushi Shimamura[2] and Norihisa Komoda[3]
[1]*Research & Development Division, Hitachi America, Ltd., 2535 Augustine Dr, Santa Clara, California, United States*
[2]*Research & Development Group, Hitachi Ltd., 1-280, Higashi-Koigakubo, Kokubunji-shi, Tokyo, Japan*
[3]*Code Solutions Co., Ltd., 1-2-11-9F, Edobori, Nishi-ku, Osaka, Japan*

ABSTRACT

Currently most of the workflows in enterprise business processes are implemented and managed as information system. However, workflows between organizations are still processed manually based on paper document because it is difficult for the organizations to trust the process and the result of workflow in the system which is provided by one of the organizations or a third-party organization. In this paper, a system architecture for cross organizational workflow management utilizing blockchain technology is proposed. It eliminates every Single Point of Trust (SPoT) which causes falsification risk of the process and data. Our proposed system architecture is considered to connect with internal workflow management system and accommodates two types of smart contracts for interorganizational workflow definition and interorganizational workflow processing, which validates related data in every transaction. By this architecture, each organization can be aware of the data falsification when the data on one of the organization nodes is falsified by a malicious workflow administrator or a system administrator. Through the implementation of the proposed system and evaluation of the falsification risks based on the attack scenarios along workflow life cycle, it is confirmed that all the risks are avoided by the proposed system architecture.

KEYWORDS

Business Process Management, Workflow, Blockchain, System Security, System Architecture

1. INTRODUCTION

Along with the improvement of information technology, business processes in enterprise have become to be managed by information systems. The method to describe and manage business process is called Business Process Management (BPM) and workflow management is one of

the key functions of BPM (van der Aalst, 2016), where remarkable progress has been made through application to practical use cases (Kumar & Zhao, 2002). The benefit of workflow management system is faster processing with less human effort (Reijers, et al., 2016). However, workflows between organizations are still document-based and are processed manually. This is because most of existing workflow management systems consist of a single workflow engine using a single database (Stohr & Zhao, 2001) assuming internal use in an organization. There have been several attempts to take advantage of distributed processing technologies such as WWW, CORBA, XML and Java to integrate systems in different organizations (Stohr & Zhao, 2001). However, the reliability of data and processing depends on the organization which own the system. Therefore, in order to secure the reliability of transactions between organizations which do not fully trust each other, it is imperative to provide immutable data sharing and reliable data processing among organizations.

Blockchain technology, which is originally introduced as a platform technology for Bitcoin (Nakamoto, 2008), presents a promising feature to provide immutable data store for multiple organizations that supports requirements of workflows management among organizations. Focused on this feature, companies have been working on many Proof-of-Concepts to evaluate the feasibility of this technology in supply chain management, trade finance, and other business cases (Hileman & Rauchs, 2017) (World Trade Organization, 2018) (World Economic Forum, 2018). One of the important features of blockchain is that it provides an immutable record among participants and it is valuable for the use cases such as traceability in supply chain where reliable record is required among trustless parties (Di Ciccio, et al., 2018). As one of the applications of blockchain technology in enterprise use, some approaches to implement workflow management systems among multiple organizations are proposed. For instance, the authors in (Alves, 2020) propose an architecture to integrate Business Process Management System (BPMS) and blockchain platform in order to guarantee transparency and tamper-proof information among participating parties. However, the intercommunication between BPMS and blockchain or the centralized BPMS can be a Single Point of Trust (SPoT) which a malicious user can attack to falsify related data. Another approach is to design specific workflow by designing method or tool and implement it as a smart contract on blockchain to secure that the workflow is processed as defined among untrusted organizations (Fridgen, et al., 2018) (Pintado, et al., 2019) (Weber, et al., 2016). However, workflow definition should be able to be modified dynamically based on changing business requirements of each organization and the workflow administrator should not be SPoT. Therefore, more holistic approach is required which securely manages whole process of workflow life cycle among trustless organizations.

In this paper, a system architecture of cross organizational workflow management which eliminates SPoT throughout the workflow lifecycle including defining, executing, and auditing process is proposed. This architecture avoids falsification risks of both process and data of workflow. Based on the implementation of the proposed system architecture, the security risks of the proposed system architecture are evaluated based on the attack scenarios along the workflow lifecycle and confirmed that the risks are avoided by the proposed architecture.

2. REQUIREMENT FOR CROSS ORGANIZATIONAL WORKFLOW MANAGEMENT SYSTEM

2.1 Definition of Workflow

This section describes the definition of workflow in this paper. Workflow is a part of enterprise business process and consists of several processes including creating, amending, rejecting, and approving a proposal among stakeholders to finally have an agreement on the proposal, while recording the whole process. Each workflow has a lifecycle which consists of three phases. Figure 1 shows the three phases of workflow and the relevant users in each phase. The first phase is the definition phase in which workflow administrators define the workflow definition based on the business rules. Based on the workflow definition, workflow processors initiate and process the workflow in the execution phase. The record of the workflow execution is stored in the workflow management system and referred by the auditors in the auditing phase. Workflow management system is the system to manage the whole lifecycle of these workflow processing phases which is managed by the system administrator.

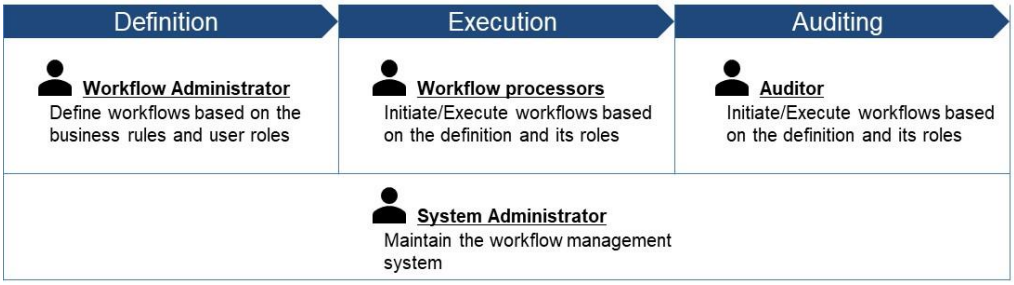

Figure 1. Workflow lifecycle and the relevant users

Figure 2 shows the overview of conventional workflow management system. It is composed of client applications for workflow processors and auditors, workflow designing tool for workflow administrator, and the workflow engine which controls the workflow execution process based on the workflow definition using workflow state management function and stores the execution result as the audit trail. In the definition phase, the workflow administrator creates a workflow definition using workflow design tool and it is stored in the workflow management system. In the execution phase, a processor can select one of the definitions and initiate a workflow which is processed by other processors through client application. The processing of a workflow is controlled by the state management function in the workflow engine using stored workflow state in the database. The execution result is stored in the database by the execution record management function which also provide referring function for auditors through client application.

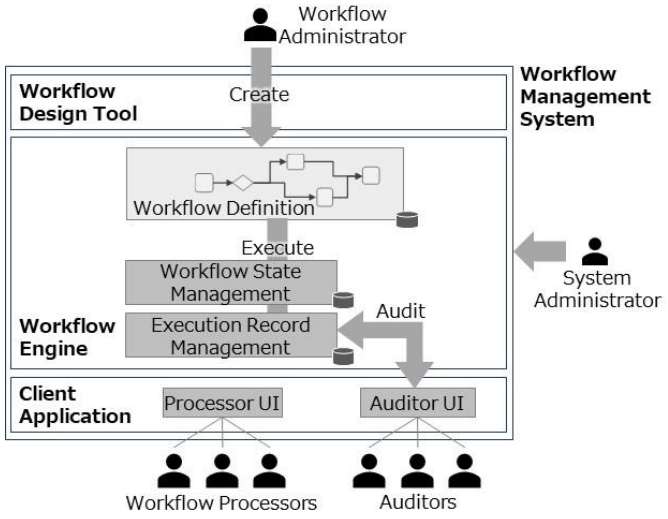

Figure 2. Overview of Workflow Management System

There are many patterns of workflow structure (van der Aalst, et al., 2003) in practical business processes and it is defined as a data structure as shown in Table 1. In this example, the workflow consists of five steps and the sequence of the workflow shown in Figure 3 is defined as a relationship between steps defined in “precondition” and “next step” field.

Table 1. Example of workflow definition

Step	Role	Operation	Precondition	Next step
Initiate Request	Initiator	set “Item 1” and “Item 2”	-	Update Request
Update Request	Approver1	approve “Item 1” and “Item 2”, set “Item 3” and “Item 4”	Initiate Request	Approve Request1 Approve Request2
Approve Request1	Approver2	approve “Item 1”, “Item 2”, “Item 3”, and “Item 4”	Update Request	Approve Request3
Approve Request2	Approver3	approve “Item 1”, “Item 2”, “Item 3” and “Item 4”	Update Request	Approve Request3
Approve Request3	Apprver4	approve “Item 1”, “Item 2”, “Item 3”, and “Item 4”	Approve Request1 Approve Request2	

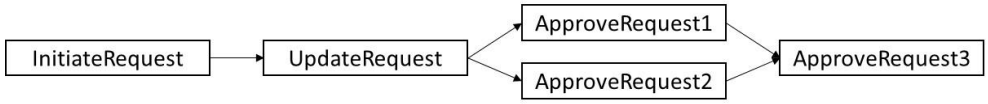

Figure 3. Example of workflow sequence

When this workflow is processed in the execution phase, the transaction record should be recorded as Table 2 to know the status of the workflow and to be audited in the auditing phase.

Table 2. Example of transaction record

Date	Operator	Step	Action
8/9/2020 09:05	AAA	Initiate Request	Initiated
8/9/2020 10:12	BBB	Update Request	Approved
8/9/2020 11:23	CCC	Approve Request1	Approved
8/9/2020 13:41	DDD	Approve Request2	Rejected

The conventional workflow management system is designed for internal use in a single organization in order to improve the efficiency of business process and reduce the cost of workflow management. Therefore, it works on a single server with a single database which should be managed by the system administrator of the organization.

2.2 Assumption of Cross Organizational Workflow

Cross organizational workflow is assumed as a combination of internal and interorganizational workflows as depicted in Figure 4. Each step in interorganizational workflow should be processed based on the internal workflow in corresponding organization. The internal workflow is managed in the way as described in Section 2.1. However, the interorganizational workflow should be managed in a different manner. It should be defined by the workflow administrators from multiple organizations based on an agreement between organizations, processed by the workflow processors from multiple organizations, and audited by third party auditor.

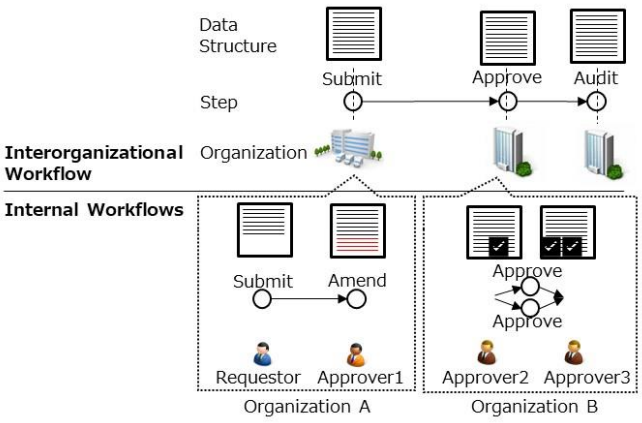

Figure 4. Overview of cross organizational workflow

2.3 Requirement for Cross Organizational Workflow Management System

As described in section 2.2, the interorganizational workflow in the cross organizational workflow is defined, processed, and managed among organizations which do not fully trust each other. Therefore, the system needs to be designed to accommodate some additional feature in order to securely process workflow among trustless organizations.

There are two additional requirements for the cross organizational workflow management system. One is to secure that the workflow is processed as agreed among the organizations beforehand. The other is to store and provide immutable audit trail of transactions which include the set of proposed data and the approvers. However, if the cross organizational workflow management system is implemented as a centralized system as shown in Figure 2, there are three falsification risks as shown in Table 3.

Table 3. Falsification risks on a workflow management system

Target	Risk	Caused-by
Workflow Definition	Alter Definition	**Workflow Administrator**
Workflow State	Skip step	**System Administrator**
	Alter State	**System Administrator**
Execution Record	Alter Record	**System Administrator**

These falsification risks are caused by two SPoT in the system. One is the workflow administrator. If the workflow definition is managed by a single responsible administrator from one of the organizations, the administrator can falsify the definition on their own decision. The other is the system administrator. If the system is managed by a single responsible administrator from one of the organizations which own the system, they can falsify the state of workflow or the proposal data (Figure 5).

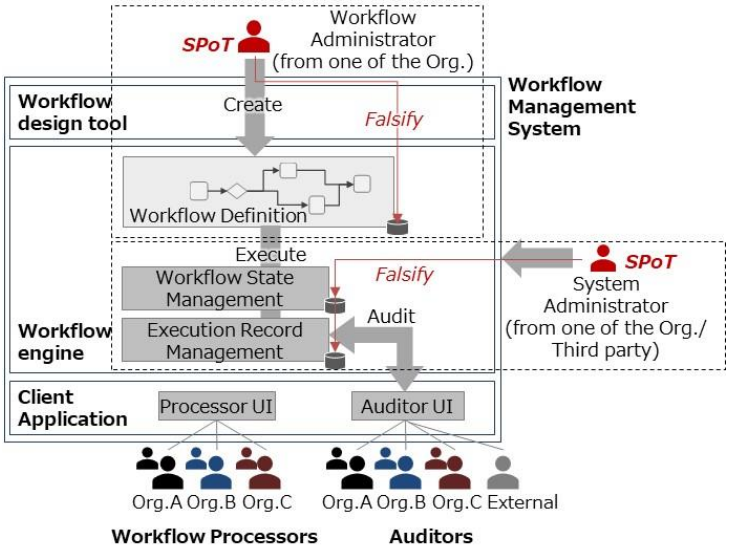

Figure 5. Single Point of Trust in Workflow management system

The cross organizational workflow management system should satisfy these two additional requirements described above by eliminating the two SPoT throughout the lifecycle of workflow processing in order to avoid the three falsification risks.

3. OUTLINE OF CROSS ORGANIZATIONAL WORKFLOW MANAGEMENT SYSTEM

3.1 System Architecture

As described in section 2.2, cross organizational workflow consists of two parts, internal workflow and interorganizational workflow. Currently conventional workflow management system as shown in Figure 2 is widely used for internal workflow in enterprise. Therefore, cross organizational workflow management system should consider the connectivity with the internal workflow management system. And also, the two SPoT should be eliminated in the interorganizational workflow part as described in 2.3. In order to eliminate the two SPoT, we utilize blockchain technology where a consensus mechanism and immutable data store are accommodated for secure processing and secure data sharing among participant organizations.

Figure 6 and 7 shows the two types of system architecture for cross organizational workflow management considering the connectivity with the internal workflow management system in each organization. The Architecture (I) utilizes a conventional workflow management system as a workflow execution engine for cross organizational workflow and stores the execution record in blockchain. In this architecture, the execution records are immutable. However, the workflow management system is managed as a centralized system which consists of single engine and single database. Therefore, it should be managed by one of the organizations or a third-party vendor. In this case, the system administrator of the workflow management system is the SPoT. The system administrator can falsify the workflow definition or falsify the executed record before it is submitted to the blockchain nodes.

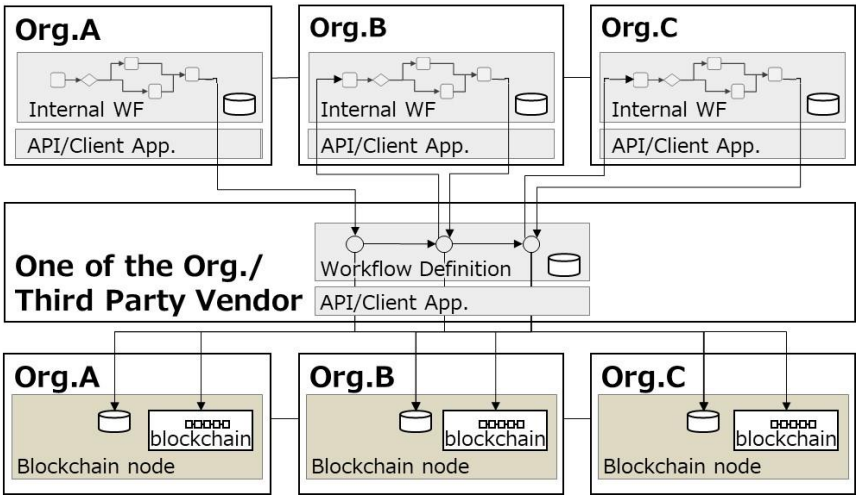

Figure 6. System architecture of cross organizational workflow on blockchain (I)

In order to eliminate this SPoT, we propose the Architecture (II) depicted in Figure 7. In this architecture, workflow definition is implemented as a smart contract on blockchain and it can't be modified without agreement of participant organizations. Also, the data submission to the storage is managed by this smart contract. The only risk of falsification is that the internal user

or system administrator of internal workflow management system is able to falsify the execution record before it is submitted to the cross organizational workflow management system implemented on blockchain. However, this is an internal issue and should be managed by each organization.

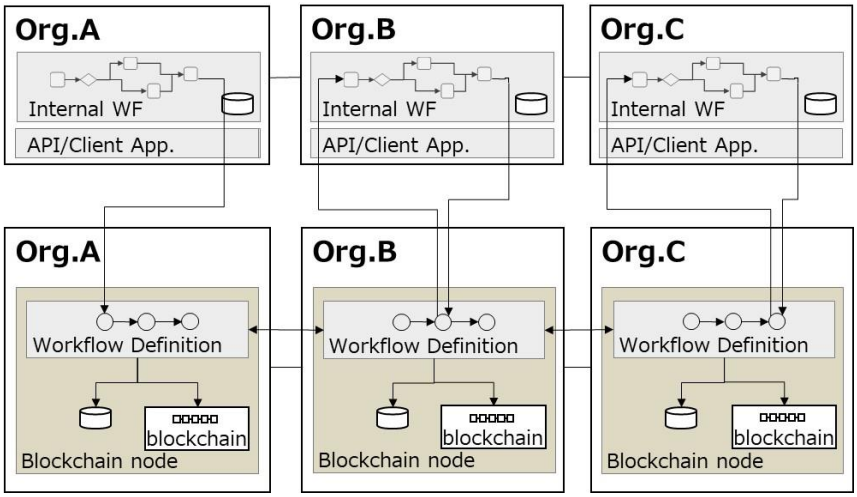

Figure 7. System architecture of cross organizational workflow on blockchain (II)

Figure 8 depicts the components of blockchain node in which the workflow lifecycle from definition to execution is managed by the two types of smart contracts. One of the smart contracts is to manage workflow definition and the other is to manage workflow processing. The smart contract to manage workflow definition accept requests from workflow administrators of each organization through the workflow admin web application. This smart contract manages the requests for workflow definition from the viewpoint of each organization, such as requirements for data items, steps, and approvers. The request is sent to other nodes and the smart contract on each node validates the data format and the user privilege and checks conflicts between requests. If the result of this validation is the same as each other, then the smart contract writes the result into the workflow definition store on each node. Thus, workflow definitions are organized by the smart contract based on the requests from the workflow administrators and it is impossible to alter the definitions in all nodes by one of the workflow administrators. The first SPoT of workflow administrator is thus eliminated by this smart contract.

The other smart contract is to manage workflow processing. This smart contract processes the workflow based on the workflow definition which an initiator indicates in the first step. Each request to process workflow is accepted by the smart contract for workflow processing and it validates the results from each of the nodes and store the result into workflow state database on each node. In this architecture, the system administrator of each organization manages their own node. They can alter the state of workflow in their own node, but as described above, the smart contract validates the result in each node and if the results are different from the one by other node, it will be rejected, and the user can be aware of the falsification. Thus, the second SPoT of system administrator is eliminated in the proposed system architecture.

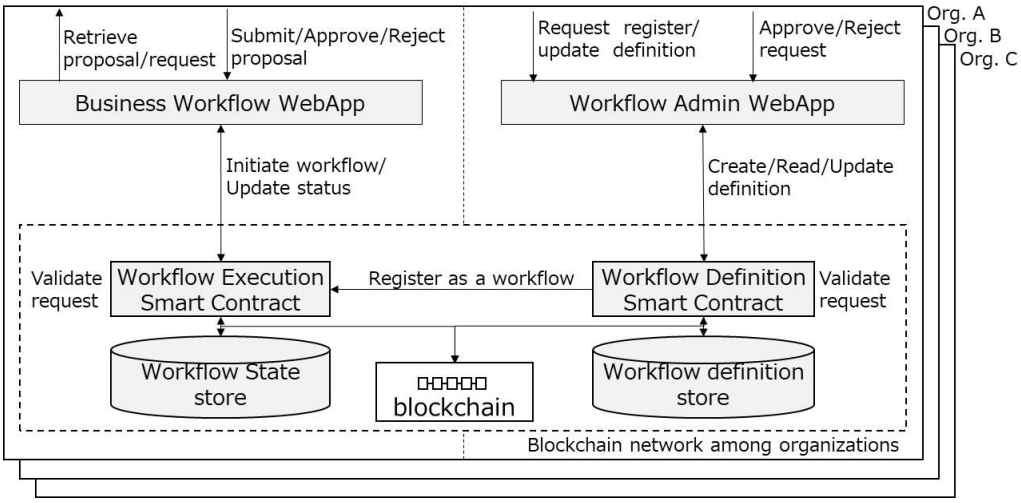

Figure 8. System components in blockchain node

3.2 Transaction Flow

This section describes how a workflow transaction is processed and the data is stored while eliminating SPoT by the architecture described in section 3.1. Figure 9 shows the transaction flow when a workflow processor submits a transaction to initiate a workflow. First the web application on the blockchain node in one of the participating organizations shows the list of workflow templates that the processor can initiate. The processor selects one of the templates, set required values and submit the proposal. Then the smart contract on the node distributes the proposal to other nodes and each node validates the proposal including the user authority, processes the code for proposal and creates a read/write set to be stored in state database. This read/write set includes the proposal data itself and the result of the processed code. If the returned read/write set from other nodes are the same as the result of this node, then the node requests other nodes to write the result. In the state database, the workflow proposal is stored with the request ID and the action which is created in the smart contract as the next step to be processed by an approver or a reviewer.

Figure 10 shows the transaction flow of the audit process. In case a user requests to refer a record to know the status of a proposal or to audit a proposal after the case is closed, the smart contract processes the request in the same way as a processing request as described above. And the smart contract on each node write the result of the reference request into the state database in order to verify that the results among state databases on each node are consistent through the validation process by smart contract. Thus, the transaction flow of the proposed system architecture keeps the consistency of the stored record even in the audit phase after the case is closed.

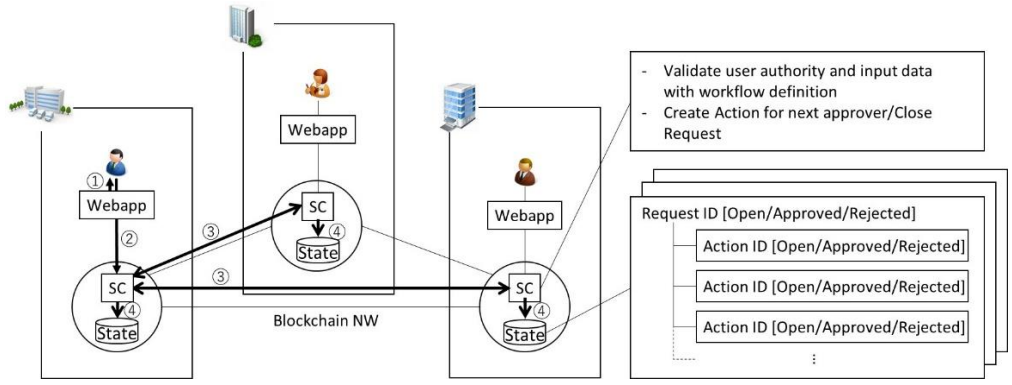

Figure 9. Transaction flow of create/update process

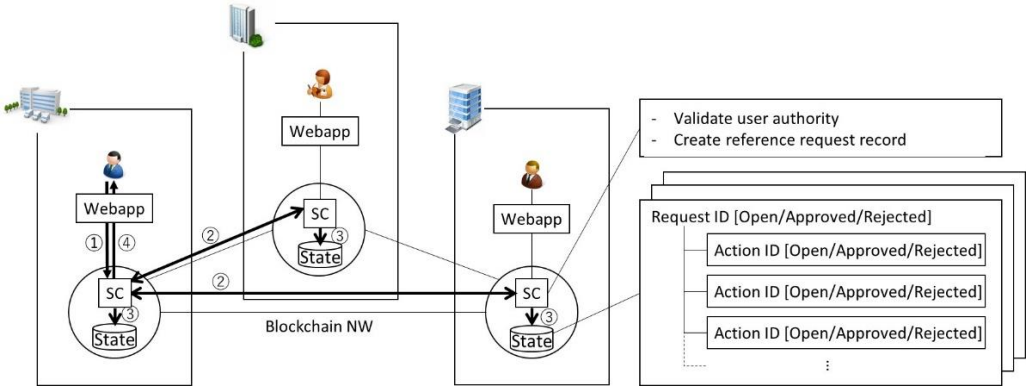

Figure 10. Transaction flow of reference process

4. IMPLEMENTATION AND EVALUATION OF PROPOSED SYSTEM ARCHITECTURE

4.1 Use case of Cross Organizational Workflow

As described in (van der Aalst, et al., 2003), there are many patterns of workflow structure and control, however all the patterns are composed by the combination of proposing, approving, reviewing, and rejecting transactions. In order to demonstrate the feasibility of the transaction flow on the proposed system architecture, a simple use case of interorganizational workflow is implemented which processes a cross organizational workflow among three organizations for customer onboarding (Figure 11). In this use case, the requestor in one of the organizations submits a proposal with related information and then other organizations approve or reject the proposal in sequence.

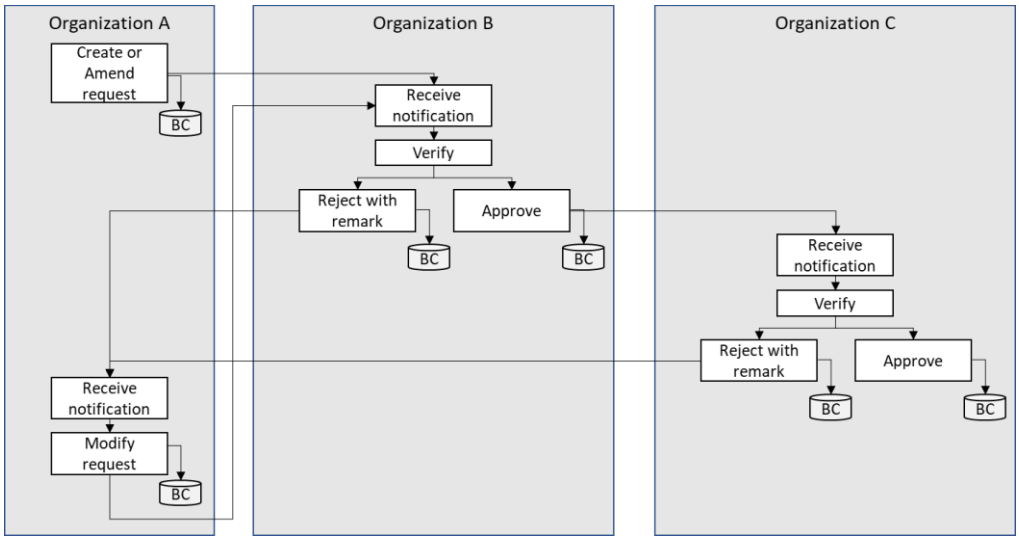

Figure 11. Use case of implemented workflow

4.2 Implementation on Hyperledger Fabric

The use case described above is implemented on Hyperledger Fabric (The Linux Foundation, online) which is one of the major implementations of the consortium blockchain as a platform to implement the smart contract. The implemented system provides the client application for the workflow processors where they can submit a proposal or approve/reject the proposal. Each action is processed by the workflow smart contract as described in section 3.2 and the execution result is stored in the state database, and the state of designated workflow is updated. The workflow smart contract validates the signature and input values based on the workflow definition and if it is passed, it creates a read/write set to be stored in the state database as a new state with the inputs and it is shared among all nodes. Even if a malicious system administrator of one of the organizations alters the data on their own node, it is not reflected to other nodes and it can be found when the next transaction is processed by the smart contract because the organizations cannot agree on the result for the next transaction. The executed result stored in the state database can be referred by the workflow processers and the auditors using the client application. Figure 12 shows the screen images of the audit trail views for auditors. The left image shows the request and approval history and the proposal content of a workflow. The right image shows the transaction record on blockchain. These data are also processed by workflow execution smart contract and displayed after the comparison among participant nodes as described in section 3.2. Therefore, the auditors can trust the data that it is not falsified by malicious users.

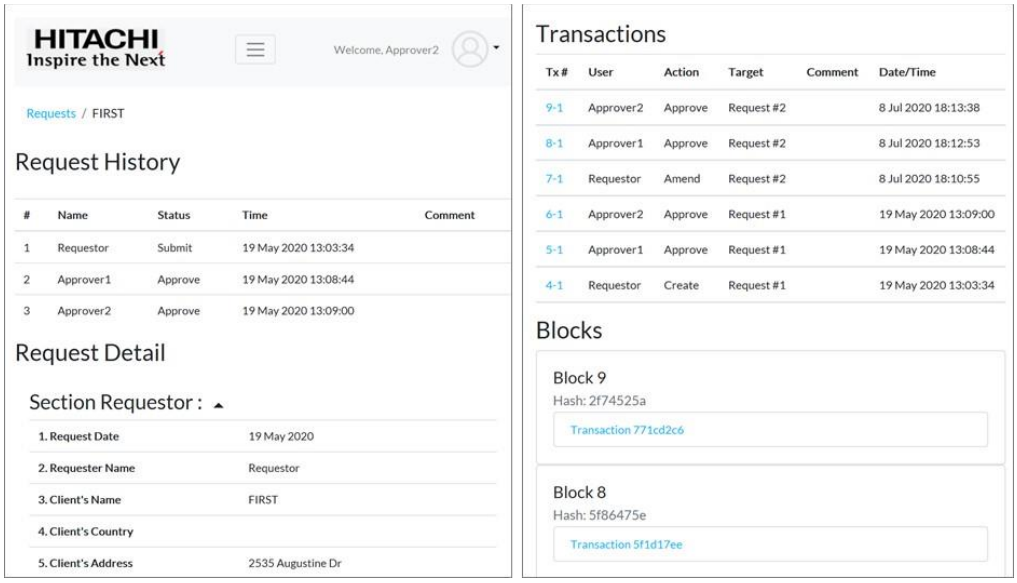

Figure 12. Screen image of the implemented system

4.3 Security Evaluation of Proposed System Architecture

This section evaluates the proposed system architecture from the security perspective. Figure 13 shows the attack target assets of two architecture. The client application at the internal workflow management system (a) can be the attack target because the malicious user may alter the transaction data before it is submitted to the interorganizational workflow management system. The client application at the interorganizational workflow management system in architecture (I) can be the attack target in the same way. Workflow definition (b), state database (d), and blockchain (e) can be also the attack targets if the malicious user aim to alter the definition or result of workflow.

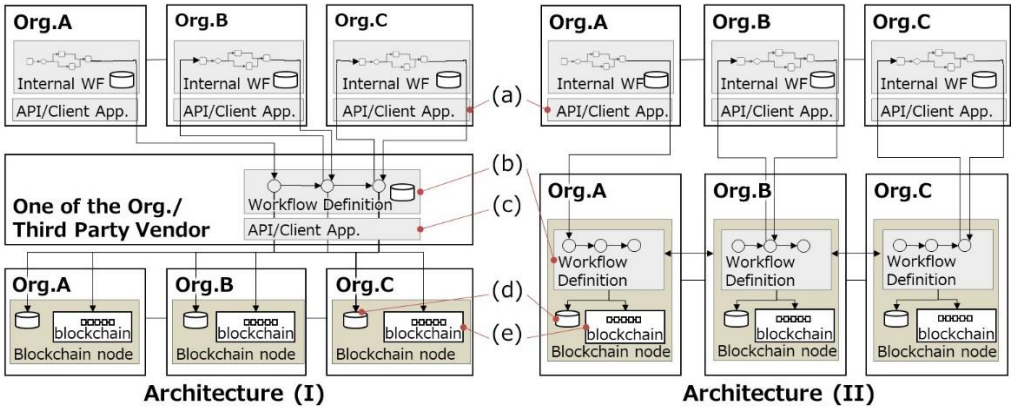

Figure 13. Attack target assets from the data integrity perspective

Figure 14 shows the attack scenarios based on the attack target assets and the workflow lifecycle. In the definition phase or before opening a workflow case, the workflow definition can be the attack target. In the execution phase, all the target assets can be the attack target. In the audit phase, state database and blockchain can be the attack target as the execution result.

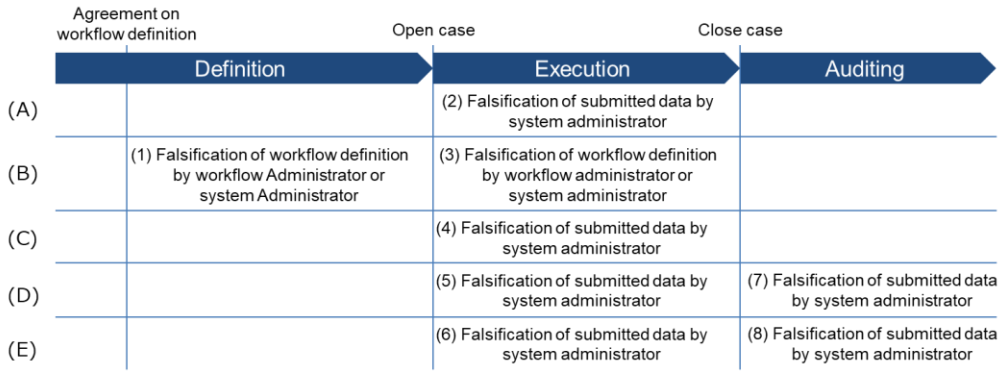

Figure 14. Attack scenarios in workflow lifecycle

The proposed system architecture (II) avoids the falsification risk in each scenario as follows.

(1) The first scenario is the falsification of workflow definition by one of the workflow administrators among participating organizations before opening a case. They may falsify the definition to skip the step of approval. In the proposed system architecture, the workflow definition is implemented as a smart contract and it is distributed into every processing node. And the smart contracts send the read/write set of the transaction each other to be processed in other nodes. If one of the smart contracts on the processing node is falsified by the administrator, the validation does not pass, and the transaction will be rejected. Thus, the first falsification risk is avoided in the proposed system architecture.

(2) The second scenario is the falsification of submitted data at the interface between internal WfMS and cross organizational WfMS. This is an internal issue and should be managed by internal compliance.

(3) The third scenario is the falsification of workflow definition by one of the workflow administrators among participating organizations during a case is open. The motivation of malicious user is the same as the first scenario and this is avoided as same as the first scenario in the proposed system architecture.

(4) The fourth scenario is the falsification of submitted data between cross organizational WfMS and blockchain datastore. In the architecture A, the WfMS is managed by third party or one of the organizations and there is a falsification risk. But in the proposed system, these are processed in the blockchain node and there is no risk of falsification.

(5) The fifth scenario is the falsification of the proposal data by a system administrator while a case is open. They may falsify the data after another administrator approved the proposal. In the proposed system architecture, each node executes the smart contract and validate the results each other. If the proposal data in one of the nodes is falsified, the result will be different from the result of other nodes and the validation fails. Thus, this risk is avoided in the proposed system architecture.

(6) The sixth scenario is the falsification of submitted data in blockchain in execution phase. But it is almost impossible to falsify blockchain data because of the nature of data structure.
(7) The seventh scenario is the falsification of proposal data by a system administrator after a case is closed. They may falsify the data after all the approvers approved the case. In the proposed system architecture, each node executes the smart contract and validate the results each other even if this case is already closed and it is just a reference transaction. Thus, this falsification risk is also avoided in the proposed system architecture.
(8) The eighth scenario is the falsification of submitted data in blockchain in the audit phase. But as same as the sixth scenario, it is almost impossible to falsify.

Table 4 shows the comparison result of two system architectures from the perspective of security in audit phase. Both architectures are secure in terms of immutability of audit trail as the data is stored in blockchain. However, the architecture (I) is not secure in terms of adherence of workflow definition because the definition is managed by one of the organization or third party and can be falsified by malicious user. On the other hand, the proposed architecture (II) is secure regarding this point as the definition is managed as a smart contract and can not be falsified without agreement among participant organizations. The architecture (I) is not also secure in terms of consistency of records between internal workflow and interorganizational workflow because of the vulnerability of client application in internal workflow management system (a) and interorganizational workflow management system (c). Especially, the attack target (c) is not under the control of each organization. On the other hand, the risk is limited to the attack target (a) and it can be controlled within each organization.

Table 4. Security comparison of two system architectures

	Architecture (I)	Architecture (II)
Adherence of workflow definition	Not Secure	Secure
Immutability of audit trail	Secure	Secure
Consistency of records	Not Secure	To be secured by internal control

Thus, our proposed system architecture avoids all the falsification risks regarding interorganizational workflow part by eliminating the SPoT in cross organizational workflow management system and provide reliable workflow management system for every participant organizations.

5. CONCLUSION

In this paper, a reliable architecture of cross organizational workflow management system is proposed. Conventional workflow management system is designed for internal use and there are two SPoT where malicious user may attack to falsify the workflow definition or the execution result if it is applied to cross organizational use. Our proposed system utilizes blockchain as the secure data store among trustless organizations and also utilizes smart contract on blockchain as the secure workflow processing engine. It is also considered to connect with internal workflow management system as most of the cross organizational workflow is assumed

to be a combination of internal workflow and interorganizational workflow. Through the implementation of the workflow processing smart contract and the evaluation of the falsification risks based on the attack scenarios along the workflow lifecycle, it is confirmed that our proposed system architecture avoids all the falsification risks by eliminating the two SPoT in cross organizational workflow management system. It provides reliable and efficient processing for cross organizational workflow in enterprise use.

REFERENCES

Alves, P. et al, 2020. Exploring Blockchain Technology to Improve Multi-party Relationship in Business Process Management Systems. *ICEIS 2020 - 22nd International Conference on Enterprise Information System*.

Di Ciccio, C. et al, 2018. Blockchain-based traceability of inter-organisational business processes. *International Symposium on Business Modeling and Software Design*. Vienna, Austria, pp. 56-68.

Fridgen, G. et al, 2018. Cross-Organizational Workflow Management Using Blockchain Technology – Towards Applicability, Auditability, and Automation. *Proceedings of the 51st Hawaii International Conference on System Sciences.* Hawaii, USA, pp. 3507–3516

Hileman, G. & Rauchs, M., 2017. *2017 Global Blockchain Benchmarking Study*. [Online] Available at: https://ssrn.com/abstract=3040224 (last visited Oct. 12, 2020)

Kumar, A. & Zhao, J.L., 2002. Workflow support for electronic commerce applications. *Decision support systems*, Vol. 32, No. 3, pp. 265-278.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online] Available at: https://bitcoin.org/bitcoin.pdf (last visited Oct. 12, 2020)

Pintado, O., et al, 2019. Caterpillar: A business process execution engine on the Ethereum blockchain. *Journal of Software: Practice and Experience*, Vol.49, No. 7, pp. 1162-1193.

Reijers, H. et al, 2016. The effectiveness of workflow management systems: A longitudinal study. *International Journal of Information Management*, Vol.36, pp 126-141.

Stohr, A. E. & Zhao, J.L., 2001. Workflow Automation: Overview and Research Issues. *Information Systems Frontiers*, Vol. 3 No. 3, pp 281-296.

The Linux Foundation, online. Hyperledger Fabric - Hyperledger. [Online] Available at: https://www.hyperledger.org/use/fabric (last visited Oct. 12, 2020)

van der Aalst, W. et al, 2016. Business Process Management Don't Forget to Improve the Process!. *Business & Information Systems Engineering*, Vol. 58, No. 1, pp 1-6.

van der Aalst, W. et al, 2003. Workflow Patterns. *Distributed and Parallel Databases*, Vol. 14, No. 1, pp 5-51.

Weber, I. et al, 2016. Untrusted Business Process Monitoring and Execution Using Blockchain., *International Conference on Business Process Management*., s.l.

World Economic Forum, 2018. Trade Tech - A New Age for Trade and Supply Chain Finance. [Online] Available at: http://www3.weforum.org/docs/White_Paper_Trade_Tech_report_2018.pdf (last visited Oct. 12, 2020)

World Trade Organization, 2018. Can Blockchain revolutionize international trade?. [Online] Available at: https://www.wto.org/English/res_e/booksp_e/blockchainrev18_e.pdf (last visited Oct. 12, 2020)