Blockchain based Mechanism for Cross-departmental Workflow Collaboration

Zhengwei Che, Zongshui Xiao, Lanju Kong, Zhongmin Yan and Qingzhong Li

School of Software, Shandong University, China
Dareway Software Co., Ltd.

Abstract

There are some shortcomings in the process of cross-regional, cross-domain, and cross-department collaboration in the current process instance: 1. the overall operational status of the process is missing, making it impossible for any of these departments to obtain a global view of the process operation; 2. the process data of the workflow is missing and cannot be obtained from any business area; and 3. when the business process is complex, people may be unaware of the business of a certain department and affect the follow-up business process. In order to solve the above problems, we introduce blockchain technology, which puts information that needs to be shared and transferred on the blockchain. Then we use the blockchain to carry out message transfer and control data storage for workflow engines of various departments in the new registration process.

Keyword: blockchain, distributed workflow, inter-department cooperation.

I. Introduction

In the past, when people deal with complicated business processes, they usually need to shuffle back and forth between departments and windows. Some people do not understand the process, and might even encounter staff that is unable to explain procedures clearly. There might be delays before these processes are accepted, this leads to repeated, redundant workflows. This greatly reduces the work efficiency and make handling business process more difficult.
If the system of every department designed for student registration is integrated into a large comprehensive system, namely a centralized workflow system, the information of every department is then stored in this system. This increases the accessibility of information shared by departments and improves interdepartmental the operability. However, it also has many disadvantages such as threats to the internal information security of the system. Using the central database to store data does not guarantee the security of the data and it is vulnerable to attacks. Data can be lost, changed, or compromised. In addition, a centralized system cannot guarantee system trust. For example, financial departments has very high requirements on information and operation security. Once the data is maliciously modified, it will cause catastrophic consequences. As a result, there will still be people running back and forth between departments.

A centralized workflow management system usually uses a workflow engine to control the execution of workflow on all computers [1]. This requires the person setting the process definition to fully understand the processes within all departments. The user can only execute in the order set by the process definition tool, and cannot freely choose the execution order of parallel nodes according to their own preferences. In executed processes, the temporary and unstructured execution process is often encountered. In this case, due to the centralization of model definition, the process of definition is separated from the process of execution, and the whole workflow becomes rigid and inefficient. When the whole process needs to be executed across regions, organizations and departments, it becomes more difficult. First of all, it is time-consuming and laborious for the staff working on the process of definition to understand the business processes of all the participating departments, because some of the department specific business processes are closed and confidential. In addition, sometimes the departments are not in the same organization, and the departments are in a reciprocal state of collaboration throughout the workflow Hence there may not be an organization ultimately responsible for the management of the entire process.

In addition to centralized workflows, we can also choose to use distributed workflow management systems. In the distributed workflow management system, the execution of a process
instance often requires the cooperation of multiple workflow engines, which in turn requires the guarantee that each workflow engine accesses the same control data. Therefore we put all the control data on a single host for shared use. However in this mode, each department can access the Shared data without restriction, which will compromise the security and confidentiality of the data [2].

At present, when there is a new student registration in the school, various departments need to coordinate and cooperate to handle the new student registration procedures. However there are many departments in the school. For security reasons, the systems of each department are independent and cannot communicate with each other. When registering, it is often necessary for the registrant to handle business in each department. When the business of each department is completed, the corresponding department will stamp the seal to prove that the registrant has visited the department and completed all business of the department.

During the entire registration process, the following problems exist: 1. the overall running state of the process is missing, and departments cannot obtain the global situation of the process operation; 2. the process of data is missing, and the data of the whole process cannot be obtained from any business domain; 3. when the business process is relatively complex, the staff may not be clear or may miss the business of a certain department and as a result affecting the subsequent business procedures; and 4. each department delivers the message by stamping on the paper, which has low security and credibility. Once the stamped paper is lost, the registrant will be in great trouble.

Main contributions: (1) we use blockchain to prevent information from being tampered with while still keeping the traceability, thereby ensure that information can be trusted based on strong security features such as [3] and PBFT [4] (Byzantine fault tolerance) consensus mechanism; and (2) blockchain technology can enable departments to audit results in the transfer of information [5], so that each workflow engine can have access to data while also ensuring data security. In this way, it not only guarantees that the transaction will not be tampered, but also improves the security of information enables the secure sharing of audit results among departments.
II. Background Knowledge

A. Registration process

As shown in Figure 1, the general registration process at enrolment is as follows:

1. The registrant goes to the academic affairs office of the department and present the ID card, admission notice, admission ticket, file and other materials for the qualification examination of freshmen;
2. The registrant goes to the dormitory administrator's centre to check in, and get the dormitory number, bed number, dormitory key, etc.;
3. Then he goes to the logistics department to handle meal card, recharge, change password, etc.;
4. Pay the tuition and accommodation fees at the financial department, and get the receipt through bank card;
5. Students who need to transfer their household account should submit their household account transfer certificate to the security office to handle the transfer procedures;
6. Apply for insurance at the school office;
7. Finally, he goes to the youth league committee of the school department, submit the letter of introduction for party and league organization, and handle party and league relations.

A collection of all department business activities throughout the registration business process is represented as Set $D = \{d_1, d_2, d_3, ..., d_7\}$. Registrants need to go to each department for registration according to the registration process. Some of the processes are in sequence. For example, passing the first step of freshman qualification audit is the precondition for all subsequent registration businesses. Similarly, the fourth step requires the registrant to not only have completed the step one, but also the second step, i.e., the first and the second step business to deal with is the prerequisite of the fourth step.
In Figure 2b, all the operation transactions on the blockchain can be divided into six types: sealed by trading \((T_{pass})\), audit failed transactions \((T_{unpa})\), authorized transactions \((T_{auth})\), to check the record transactions \((T_{review})\), invalid transactions \((T_{invalid})\), notification transactions \((T_{inform})\), namely \(T = \{T_{pass}, T_{unpa}, T_{auth}, T_{review}, T_{invalid}, T_{inform}\}\). The data structure of transactions on blockchain is shown in Figure 3, Transaction \(Tx=(\text{From}, \text{To}, \text{Data}, \text{Operation type}, \text{Pre-hash})\), that is, each transaction consists of five parts: From (address account of sent trading on blockchain), To (account address of trading the receiver on blockchain), Data (the detailed content of trade, based on different role of the From and To, can define different operating custom and different Data structure, including the type of Operation (e.g., affix one's seal), time, sending department or personal information, such as in JSON format), the Operation type (Operation type classification, such as seal through the verification, not through, authorization,
and check the records, etc.), Pre - hash (pointing to the registrants blockchain accounts on a trading transaction code, This makes it easy for enrollees to find all their transactions.

### B. Blockchain

Blockchain technology creates a decentralized environment where transactions and data are not controlled by any third-party organization. Any transactions are recorded in the open ledger in a verifiable and permanent manner after completion. Blockchain is a distributed database, the user data is stored in the form of a security and cannot be changed on the block, the new piece will continue to increase at the end of the chain block, and every block size are saved in a piece of the hash value, so that can be traced back to the previous block. Finally these blocks link to each other to form a chain, that is the blockchain[7]. The prominent advantage of blockchain is that it is a decentralized, untamable, traceable and jointly maintained distributed ledger.

As our blockchain system does not allow all department, organization or individual to join in, and only some selected departments are allowed to join as nodes, it is more suitable to use an alliance chain. The whole blockchain system does not involve tokens. On the blockchain, information is simply stored, and messages are transmitted. Therefore, we choose the PBFT consensus mechanism with higher consensus efficiency. PBFT algorithm is divided into three stages: pre-preparation, preparation and confirmation. The advantage of this method is that consensus delay is short and consensus efficiency is high.

### III. System Model

#### A. Department collaboration workflow model based on blockchain

The traditional workflow model is shown in Figure 2a. The internal business processes of the department can be processed through the workflow engine of the department, but the information cannot be directly transmitted and shared between departments. The interfaces of the corresponding departments need to be invoked. In order to break the barrier of information sharing and improve the
security and reliability of information transmission, as shown in Figure 2b, each department has a complete distributed ledger by introducing blockchain technology.

The department collaboration workflow model based on the blockchain consists of the registrar, each department workflow engine involved in the registration business, and the blockchain system. Department workflow engine is responsible for managing the registration in the department of internal business process, and each department in the workflow engine defines its process[8], and can make use of the system of the department internal data. Inter-departmental call information needed typically will be link through the registration in the first audit round, and provide the authorization code in the chain of blocks of each audit within a workflow engine through parameter \( k_i = \{k_1, k_2, k_3, \ldots \} \) which is used to pass the audit information and only send the final result of the department audit to the blockchain in the form of transaction \( Tx \). The blockchain system of user workflow engine is responsible for transmitting the shared information between departments. It only provides the data result information needed by users to transact business across departments and does not provide the detailed data of users in a department system to protect users' privacy. The department collaboration workflow model based on blockchain is shown in Figure 2.

![Diagram](image_url)

**Figure 2: Departmental collaboration workflow model**
In Figure 2b, all the operation type of transactions on the Blockchain can be divided into six types: sealed by trading \( (T_{\text{pass}}) \), audit failed transactions \( (T_{\text{unpa}}) \), authorized transaction \( (T_{\text{auth}}) \), to check the record transactions \( (T_{\text{review}}) \), invalid transaction \( (T_{\text{invalid}}) \), notification transactions \( (T_{\text{inform}}) \), namely \( T = \{ T_{\text{pass}}, T_{\text{unpa}}, T_{\text{auth}}, T_{\text{review}}, T_{\text{invalid}}, T_{\text{inform}} \} \). The data structure of transactions on blockchain is shown in Figure 3. Transaction \( Tx = (\text{From}, \text{To}, \text{Data}, \text{Operation type}, \text{Pre}-\text{hash}) \), that is, each transaction consists of five parts: From (address account of sent trading on blockchain), To (account address of trading the receiver on blockchain), Data (the detailed content of trade, based on different role of the From and To, can define different operating custom and different Data structure, including the type of operation (e.g., affix one's seal), time, sending department or personal information, such as in JSON format), the operation type (operation type classification, such as seal through the verification, not through, authorization, and check the records, etc.), Pre - hash (pointing to the registrants Blockchain accounts on a trading transaction code, This makes it easy for enrollees to find all their transactions.

![Transaction Table]

**Figure 3 Data structure of the transaction**

### B. New nodes join the blockchain

Current users of the blockchain system have enrollees and departments, who can join the blockchain network as nodes. Since the alliance chain only allows selected people or departments to join, when
a new node wants to join the blockchain network, it should first submit user information to the corresponding certificate authority and seek approval to join.

As a trusted third party, the school's academic affairs office is the Certification Authority, which is responsible for managing and issuing digital certificates. All departments involved in student registration shall apply to the school office to join the blockchain network. The school office shall check whether the information is legal. If it is not legal, the department is not allowed to join the blockchain network. Otherwise, admission is allowed, and the school office will issue a CA certificate to the department. The certificate contains department information, public key, date of validity, etc., and is signed by the school's academic affairs office. The user can use the public key of the school office to verify the signature on the certificate. Users can join the blockchain network according to the issued CA certificate and generate their own private key wallet and blockchain address.

When new students who want to apply for enrollment registration, that is, when registrants join the blockchain network, they need to pass the examination and approval of the office of academic affairs of the department. After the examination and approval, the office of academic affairs of the department will issue the CA certificate to the registrants. The CA certificate contains the public key and the registry's identity information, such as name, student number, department, class, etc., and has been signed by the department's academic affairs office. Registrants apply to join the blockchain network based on their CA certificates, and generate their own blockchain accounts.

When departments and enrollees join the blockchain network, they have their own identity accounts in the blockchain, each of which corresponds to an ID and a blockchain wallet containing a pair of public and private keys. ID is the blockchain address, which represents identity. The public or private key should be kept securely, the private key is used to sign transactions, and the public key is used to verify that the signature of a transaction is valid.

Since it takes large hard disk space to synchronize all of the data on the blockchain to the local location, light node wallets are used on the registry's mobile and department's web ends. As the light
node does not need to download and store all the blockchain data, it only acquires and stores the transaction data related to itself on the blockchain after analyzing the data.

**IV. Business workflow**

In the whole process of registering business workflow, the interaction between department workflow engine and blockchain system can be divided into two types: the workflow where the registrant carries out registration business and the workflow for information update.

**A. Department registration business process**

Definition 1: in the process of executing business by the user, if the execution of the current department node depends on one or several executed nodes, the current department node being executed is called Cur-node, and the dependent executed node is called Pre-node. For example, after the registration of the dormitory administrator department, the registrar shall execute the registration of the finance department. There is a strict sequence of execution of the business process between the finance department node and the dormitory administrator department. In this business scenario, the dormitory administrator department is Pre-node, while the finance department is Cur-node.

![Diagram of registration process transaction process](image)

Figure 4: Registration process transaction process

First, the registrant needs to send an authorization transaction $T_{auth}$ on the blockchain. The purpose is to allow the current department node Cur-node to check the pre-node stamp on the blockchain to pass the transaction and confirm whether it has passed the Pre-node audit. If the cur-node has multiple Pre-node, it needs to send multiple $T_{auth}$ correspondingly.

Next, Cur – node will parse out which contains sealed $H_{pass}$ hash value of the deal according to the authorization code sent by the registrar, and send $T_{review}$ on the blockchain according to the hash value in the chain of blocks needed to find $T_{pass}$. This keeps a record of all view trading department
in order to protect the registrants information security and the right to freedom of control of their information.

Finally, Cur-node conducts a series of audits on the register in its own system. If the register passes these audits, the Cur-node can register its business. After that, in order to prove to the later department that it has registered the business for the registrant, Cur-node needs to send the transaction $T_{pass}$ on the blockchain.

If the registrant fails to pass the audit of Cur-node, it needs to send $T_{unpass}$ on the blockchain.

B. Information updates the workflow

Definition 2: the update of a transaction not only causes the update of the transaction information in this article, but also leads to the invalidation or update of the transaction information in other departments. In this case, the department that is responsible for the update is called Rel-node. For example, when the freshman asks to change the dormitory, the number of the dormitory will change, and even the type of dormitory will change sometimes. The four-room dormitory will be replaced by a single room. In this case, it is necessary to go to the financial department to pay the accommodation fee.

Transactions on the blockchain cannot be modified directly. When the information of a transaction needs to be updated, an invalid transaction needs to be sent first, so that the old or wrong information is marked as invalid transaction, and then a new transaction is sent, and the updated information is written into the new transaction.

![Figure 5: Update the transaction process](image)

Figure 5 shows the transaction model of information update. As the information of Cur-node changes, relevant information of Rel-node also needs to change. First, Cur-node sends the transaction $T_{invalid}$ on the blockchain, marking the stamped transaction previously sent on the
blockchain as invalid. The hash value of the transaction to be invalidated is stored in the data, and the declaration of invalid transaction sealed, and the reason for its invalidation; Service type is invalid.

Then, after the re-audit of the modified information, the transaction \( T_{pass} \) is sent after the passage of Cur-node, the sender of the modified transaction is Cur-node, the receiver is the registrar, the updated information of the registrar is stored in the data, and the service type is still sealed.

Meanwhile, Cur-node will also send a notification of invalid transaction of the department stamp \( T_{inform} \) to Rel-node on the blockchain, to notify Rel-node that the information of the registered person has changed through this transaction, and the data of the notification transaction is the specific changed information. Once this type of message is captured by the workflow engine of Rel-node, the stamped transaction that caused the change is marked as invalid by sending the transaction \( T_{invalid} \) on the blockchain. Then the registrant is to re-enroll to complete the registration business.

### C. Mapping of workflow logs to blockchain

Table 1 is extracted from the workflow log important fields of each record represents an event \( e \), is composed of the attributes in table 1, the \( e = (e_{user}, e_{start}, e_{end}, e_{type}, e_{bc}) \). In the upper chain attribute, 0 represents the information that is not required to be sent to the blockchain, and 1 represents the information that needs to be passed across departments to be sent to the blockchain. Therefore, there is a mapping between the workflow log and the data structure of the blockchain. Algorithm 1 realizes the mapping between the data with the upper chain attribute of 1 in the workflow log and the state and the data structure of the blockchain.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>registrant</th>
<th>Start Time</th>
<th>End Time</th>
<th>operation type</th>
<th>Co-chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Johnny</td>
<td>2016/09/07 09:27:00</td>
<td>2016/09/07 09:30:00</td>
<td>d1s1 internal audit</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Johnny</td>
<td>2016/09/07 09:32:00</td>
<td>2016/09/07 09:35:00</td>
<td>d1s2 internal audit</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Johnny</td>
<td>2016/09/07 09:38:00</td>
<td>2016/09/07</td>
<td>Sealed by</td>
<td>1</td>
</tr>
</tbody>
</table>
Algorithm 1:  Mapping from workflow log to blockchain

initialize: (From,To,Data,Operation type,Pre-hash)

  // Initialize the data in the blockchain
(from,to)←search(MyA,A1)

  // Map your address to “from”, destination address maps to “to”
Operation type←search(type)

  // Map the types in the log to “Operation type”
switch Operation type

  // Different Data structures are defined according to type.
Case pass:Data←search(t,d)

  // T_pass, Map the log’s timestamp t and department d to Data
Case unpa:Data←search(t,d,r_unpa)

  // T_unpa, Map the log’s timestamp t, department d, and unpassed reason runpa to Data
Case auth:Data←package(t,H_pass)

  // T_auth, The timestamp t and stamped transaction hash values calculated by the package(.) algorithm are mapped to Data
Case review:Data←review(t,H_pass,H_auth)

  // T_review, The timestamp t, stamped transaction hash value H_pass and
authorized transaction hash value Hauth calculated by the review (.)
algorithm are mapped to Data

**Case invalid:** \((Data, T_{\text{inform}}) \leftarrow \text{invalid}(t, H_{\text{invalid}})\)

// \(T_{\text{invalid}}\). Enter a timestamp \(t\), an invalid trade hash value \(H_{\text{invalid}}\), and use
the invalid(.) algorithm to generate Data and Tinform

\(T_{\text{inform}}, Data \leftarrow \text{inform}(r_{\text{invalid}}, info, d)\)

// The input is timestamp \(t\) and the invalid trade hash value \(H_{\text{invalid}}\), use
the invalid(.) algorithm to generate Data and the reason that Tinform input
is the trade invalid \(r_{\text{invalid}}\), notify the content info and department \(d\), and
output the Data of Tinform

Pre-hash \leftarrow \text{Get hash(from)}

Upload(From, To, Data, Operation type, Pre-hash)

V. Experiment

The mapping performance between the event log \(e\) in the workflow engine and the transactions of
the blockchain directly affects the efficiency of the entire business process. As the concurrency of
event \(e\) increases in the departmental workflow engine, the computational efficiency of the mapping
algorithm and the ability of the workflow engine to handle congestion also increases.

According to the demand analysis on student registration business, the mapping should reach the
maximum concurrent number of about 800, and the maximum response time should be controlled
within 3 seconds to meet the real-time requirement of cross-department information sharing. As seen
from the performance indicators obtained from the performance test in table 2, when the number of
concurrency reaches 1000, the response time is also controlled within 3 seconds, indicating that the
actual response results can meet the current requirements.

<table>
<thead>
<tr>
<th>concurrency</th>
<th>System normal response time</th>
<th>Actual response time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mapping algorithm at present is mainly extracted in the event log need to pass the business flow of information is mapped to $T_{pass}, T_{unpass}, T_{auth}, T_{review}, T_{invalid}, T_{inform}$, the six types of transactions on blockchain. After a period of using these transactions, it is found that the information extracted and mapped to the blockchain transactions can meet the requirements of cross-departmental information transmission and sharing.

**VI. Discussion and summary**

All departments and registrants involved in the registered business can join the blockchain system after the authentication and have their own blockchain accounts. Using blockchain in the distributed workflow system of student registration business departments for data and information transmission between the workflow engine, users can view their business at any time by using light node client to handle the process and results.

However, the system still has the following shortcomings: when the information update of one department causes the information modification of another department, then the department causing the modification needs to send a notification transaction to all departments causing the modification on the blockchain. In this link, we believe that all departments involved in the registration process trust each other, there is no malicious deception, and intentionally send false notice transactions.

**References**


