An Architecture for Electronic Exchange of Official Document Based on Email and Blockchain

Chu-Mei Chiu[1], Fang-Ming Hsu[1], Meng-Hsiang Shen[1], Chun-Min Lin[2]*

[1] Department of Information Management, National Dong Hwa University, Taiwan
[2] Marketing and Distribution Management Department, Tzu Chi University of Science and Technology, Taiwan
point0614chiu@gmail.com, fmhsu@gms.ndhu.edu.tw, smc1025@smc.edu.tw, bagilu@gmail.com

Abstract

Official documents are considered as a critical communications channel among agencies, organizations, and the public. With the rise of e-government, most official documents have been evolved from printed to electronic form in recent decades. However, the convenience of electronic documents also brings higher security risks. Through the integration of email and blockchain technology, this study proposes an architecture for the electronic exchange of official documents to bridge the gap between convenience and security. With the verification of the proposed system, the findings provide a valuable reference for the governance of agencies.

Keywords: Document exchange, Blockchain, Email, Security, Convenience

1 Introduction

For the successful execution of public affairs, agencies need to exchange information with stakeholders. Official document is the most essential channel for exchanging information among agencies, organizations, and the public [1]. In general, agencies would implement the Official Document Management System (ODMS) to manage their official documents. To efficiently manage the sending and receiving of official documents among agencies, the System for Passing and Exchanging Electronic Document (SPEED) has been implemented by the central government in Taiwan.

The SPEED must have a confirmation mechanism for receiving of official documents. The trust for the assurance of the exchanged records is insufficient especially in the case of disputes. There were no transparent exchanging logs previously which resulted in a lack of trust between the sender and the receiver. Therefore, it is necessary to build a reliable and transparent environment for exchanging official documents. Users can trust that the exchanging logs which could not be tampered with. The sender and receiver access logs any time.

There are 35,000 users which belong to 26 exchange centers in the SPEED. Even though every exchange center has a backup system, it takes much time to recover system when encounters failure. Before the system is recovered, users in the failed center cannot send or receive documents. Owing to their responsibility, exchange centers have low willingness to expand its size. Therefore, the mechanism for easily increasing the scalability is required.

Email becomes a convenient communication channel between users and is widely used in modern society. SPEED is a proprietary system. It can effectively transmit official documents but it not popular to the public. If the exchange center can be replaced by email, it is not necessary to build exchange centers in the SPEED. Official documents will be easy to transmit to the public by email. However, the security of email is weak such as spam, phishing, spoofing, or no confirmation from receivers. These weaknesses of email will affect the effectiveness of communication among agencies. Blockchain technology which is useful in creating a trustworthy system can bridge the defect of email. Therefore, this study integrates email and blockchain to build a new architecture for exchanging official documents. The architecture can ensure the security and convenience in electronic exchange of official documents.

2 Literature Review

2.1 Deficiency of SPEED

The Taiwanese government began promoting electronic official documents in 1993 and has been committed to making it the main channel between agencies and organizations [2]. Via the Internet instead of postal mail, SPEED became the most important platform for exchanging official documents among agencies and improving the efficiency of government affairs [3-4]. The exchange process of SPEED identifies users and ensures the integrity and authenticity of data which cannot be counterfeited, intercepted, or tampered by others [5].

SPEED contains four layers which are described as follows [6].

(1) Management layer: This layer prompts users to register in the address book which is similar the “Contacts” of an email system through which users can exchange information.
(2) Exchange layer: This layer undertakes the electronic exchange task. It serves as a centralized exchange center for affiliated agencies and executes the exchange to external agencies. This layer resembles an email system that sends documents from the sender

*Corresponding Author: Chu-Mei Chiu; E-mail: point0614chiu@gmail.com
DOI: 10.53106/160792642023032402012

to the receiver. Figure 1 depicts the workflow of this layer.

(3) Agency layer: This layer provides an application programming interface (API), i.e., sending and receiving module (S&R Module) for official documents, also named "jAgent" in Figure 1. This API becomes a component of ODMS for interfacing with exchange layer of SPEED.

(4) Terminal layer: This layer allows user to send and receive electronic documents via browser linked to ODMS without having to install any software on the user's site.

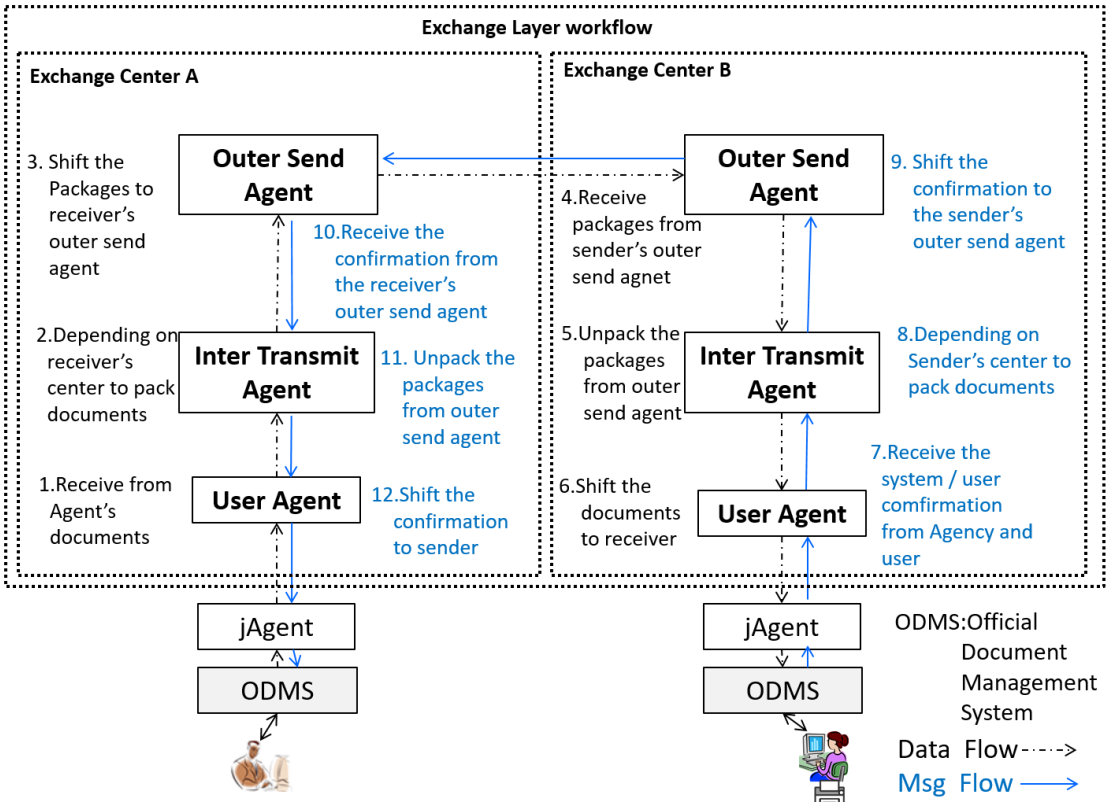

Figure 1. Workflow of exchange layer

There are three issues within SPEED that can be improved.

(1) A centralized exchange center has the risk of single node failure. In other words, the failure of a node in the center may affect the availability of the whole system [7]. All the agencies covered by the center must wait for the system to be recovered or switched to the backup system before they can resume working properly.

(2) The convenience of the system is limited. The public has not been included in SPEED. The sending and receiving of official documents between agencies and the general public are still in the form of hard copies.

(3) The trust for the evidence of the exchanged records is insufficient especially in the case of disputes. A trustworthy mechanism is required to provide sufficient evidence for persuading users to accept it.

2.2 Threat of Security for Email

Email technology can strengthen communication between government agencies and the public [8]. Email increasingly replaces paper and is used in every working space [9] with the advantage of timeliness and flexibility [10]. While email has been widely used in government agencies for communication, the security of email has been problematic [11]. There are a lot of threats such as malware, social engineering, counterfeit, spam, and phishing. Those threats are increasing which in turn threatens the security of personal data [12]. While email servers provide filters to protect users from attacks, threat issues still exist [13]. For data protection, encryption and steganography methods are used frequently [14]. The encryption method scrambles information so that it cannot be understood by unauthorized users. The steganography method hides the information in diverse forms [15]. Thus, they prevent others from doubting the authenticity of the information [16]. Since the encryption method requires lots of computations, authentication is needed to enhance the protection of encrypted files [17]. Email is an effective communication tool, but it is prone to overload [18]. There are many studies discussing issues of interruption and efficiency caused by email [19]. The United States government promises to improve the service of email as a way of communication [20].

In order to prevent malicious mail and attacks from hackers and thus improving the security of email, many studies discuss the development of document encryption, digital signature and blockchain. If related technologies are integrated, the security of data and the authentication and

non-repudiation for user identification can then be ensured [21-24].

2.3 Credibility of Blockchain

The characteristics of blockchain technology include decentralization, integrity, reliability, traceability, and non-repudiation of users [25]. Blockchain technology was first applied to the Bitcoin cryptocurrency [26-27], and has since been applied to fraud detection, identity management, document verification, and rights protection [28-33]. Via private key signature, transaction blocks and consensus of ledger are constructed to achieve the validity and authenticity of transactions [34]. The transaction records of the blockchain are based on a decentralized network ledger with many copies. The ledger will not be tampered with when one node is under attack [35]. Blockchain can behave as a tracking system which provides information to users regarding their transactions [36-37]. The Estonian government integrated the blockchain with digital ID to provide services for e-Residency. Blockchain has been used in the U.S. and E.U. to enhance the security of agencies' online services [38]. Using blockchain technology, the Chinese government launched one-stop services to keep the changes of citizens' records in their e-government system [39]. Blockchain has gradually affected the relationship among organizations [40].

Blockchain provides users with enhanced security by way of a mechanism which prevents data from being tampered with. However, blockchain still encounters challenges, such as privacy, complexity, throughput, and capacity [41]. Public service is a good opportunity for blockchain [42]. There are three types of blockchain: public blockchain, consortium blockchain, and private blockchain. The electronic exchange of official documents requires the management of authority. In addition, the users' address book and transaction records are opened under permission. Consortium blockchain integrates certificates to verify the identification of users and achieve a secure and trustworthy setting for the exchange of official documents. Therefore, this study used registered consortium blockchain to achieve the goal of security.

3 Overview of the Proposed Architecture

Through the integration of email and blockchain, this study proposed an architecture for the electronic exchange of official documents to achieve its intended objectives, i.e., convenience in usage, security in exchanging information, and lower cost in implementing and maintaining system. The popularity of email makes it easy for users to join the proposed system. Figure 2 demonstrates the framework of the proposed architecture. In this architecture, the sending and receiving module (srAgent) of the web server and smart contract of the blockchain server are used as the core. In the meantime, it follows the regulation of the contract to write the exchanged logs into the blockchain ledger. This architecture provides users a secure and trustworthy environment for exchanging official documents electronically. All subsystems of this architecture are depicted in Figure 2. Application subsystem, email subsystem, blockchain subsystem, certificate authority (CA) subsystem, and the message queuing telemetry transport (MQTT) subsystem are shown in the corresponding sever.

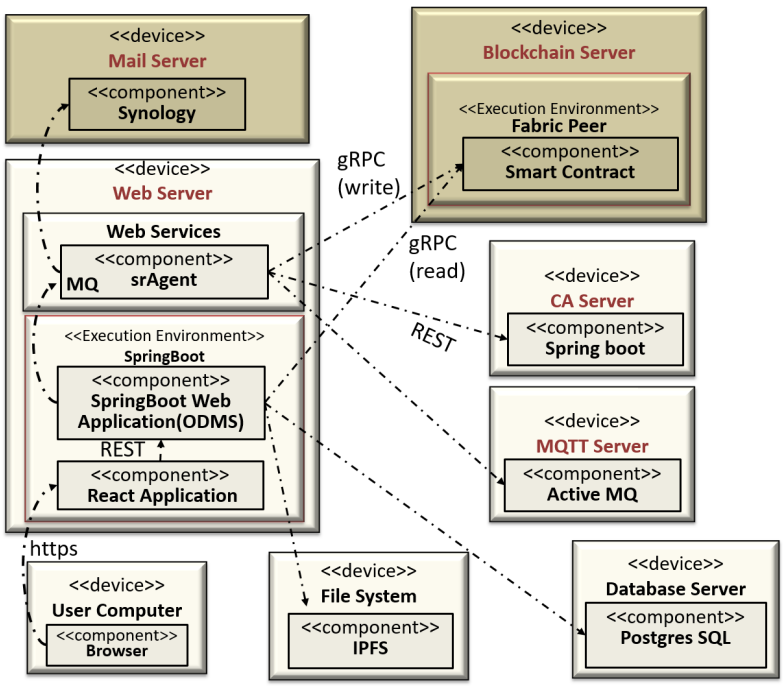

Figure 2. Framework of the proposed architecture

The subsystems in the proposed architecture are described as follows.

3.1 Application Subsystem

This subsystem has the following roles.

(1) Front-end service (React Application): It provides the interface for users to log in the system, verify the identification, upload and download official documents, and inquire simply by web browser and https protocol.

(2) Back-end service (Application): It manages the users' registration information and saves them into the Postgres SQL. The registration information includes primary and auxiliary information. The primary information includes user's code, name, object identifier (OID), email account, status, certificate information and MQTT account. The auxiliary information includes backup email account, postal address, and phone number. The subsystem saves the uploaded official documents in IPFS first and then uses message queue to activate the srAgent.

(3) Sending and receiving module for official documents, S&R Module (srAgent): This is the core of the application subsystem in change of the following actions.

A. The srAgent interfaces with the CA subsystem and verifies the identification of users via REST protocol.

B. The srAgent interfaces with the email subsystem. On the sender side, the srAgent uploads the data regarding official documents to email subsystem. On the receiver side, the srAgent downloads the data regarding official documents from the email subsystem.

C. The srAgent interfaces with the blockchain subsystem and writes the logs sent/received into the ledger.

D. The srAgent interfaces with the MQTT subsystem and sends a brief message regarding official documents to receiver.

3.2 Email Subsystem

The email subsystem is used as the platform for electronic exchange of official documents. The application subsystem packs and uploads the signed and encrypted official documents in SMTP format to the registered email account. And then the email subsystem passes the documents to the designated receiver for replacing the exchange layer of the SPEED. When the user's email account or server is abnormal, the srAgent will switch to the auxiliary account of the user. In short, this mechanism prevents the problem of SPEED where a single node failure will damage the execution of the exchange center. Therefore, it will enhance the robustness of the system.

3.3 Blockchain Subsystem

The blockchain subsystem is constructed upon consortium blockchain which stores all exchanged logs, receipts and user registration information in a fixed and traceable way. It generates a block via consensus algorithm to attach to ledger. The same ledger is distributed in every node so that the ledgers get consistency. The smart contracts established in this study are:

(1) Write exchange information when sending documents (wSendmsg): The wSendmsg writes all information related to the successful sending into the transaction ledger via gRPC (write) after the certificate and private-key signature from the sender received. Information written includes the number of documents, code and name of the sender, time of sending, code and name of the receiver, and subject of the official documents. The wSendmsg responds success or failure message back to the web application.

(2) Write confirmation message when receiving documents (wRecemsg): The wRecemsg writes all information related to the successful receiving of an official document into the transaction ledger via gRPC (write) after the certificate and private-key signature from the receiver are received. Information written includes time of receiving, code and name of the receiver. The wRecemsg responds success or failure message back to the web application.

(3) Access the transaction ledger records (rSendmsg): Authorized users are allowed to inquire the electronic official documents exchange records via gRPC (read).

(4) Read confirmation message after delivered documents are written (rRecemsg): After the wRecemsg writes the confirmation message, the web application sends inquired results via gRPC (read) to the sender. The sender might need to re-send the electronic official document or send hard copies if confirmation message could not be found after the predefined time limit.

(5) Write the registration information of the user (wReg): The wReg writes the code and name of user, and the email accounts into the registration ledger via gRPC (write) to write into the user's address book.

(6) Synchronize the registration information of the user (synReg): To save users inquiring about users who can be exchanged electronically, gRPG (read) is used to synchronize the address book to the web application server.

3.4 Certificate Authority (CA) Subsystem

In PKI mechanism, the certificate issued by the CA is used for user identity verification, document encryption and signature. This mechanism achieves the security and non-repudiation of the sender and the receiver, and the confidentiality of the document. It prevents the official document from being stolen or leaked by others, also the email accounts from being counterfeited. Through certification, the proposed system can block spam mails by using web application.

3.5 MQTT Subsystem

The mechanism of MQTT broker is implemented by sending an extra message upon delivery of the email to notify the receiver for double check. Since the proposed architecture doesn't need to change the protocols of the email subsystem, the web application might fail to receive the official document

if the user receive email through specific client software such as Outlook. Therefore, the proposed architecture adds the MQTT subsystem to assist the user's obtaining every official document surely.

4 Experiment and Verification

This study implements a prototype to verify the feasibility of the proposed architecture. The environment and the result of execution for sending and receiving official documents are as follows.

4.1 Prototype System

Both the virtual machine and the container technology have been incorporated into the implementation of the prototype system. The prototype system includes subsystems which are shown in Table 1, and the system deployment is shown in Figure 3.

Table 1. Major components of the prototype system

Subsystem	Physical machine	Virtual machine	Number	Software
Email	Format: DS918+, OS: DSM 6.2.4, RAM: 4G, HD: 4T x4 =16T	None	2	Synology
Blockchain	Intel NUC x 2, 8 core x 2, RAM: 32G, SSD: 1T, OS: ubuntu 20.04, divided to 8 VMs	VM Manager 1.5.1, OS: CentOS 7.8, @VM: CPU 2, RAM 8G, HD 200G, Docker-ce 19.03.5	5	Hyperledger Fabric 1.4.8
Application (Including srAgent)			2	JAVA JVM: openjdk 1.8 Tomcat ActiveMQ Artemis
CA				
MQTT			1	Mosquitto MQTT v3.1

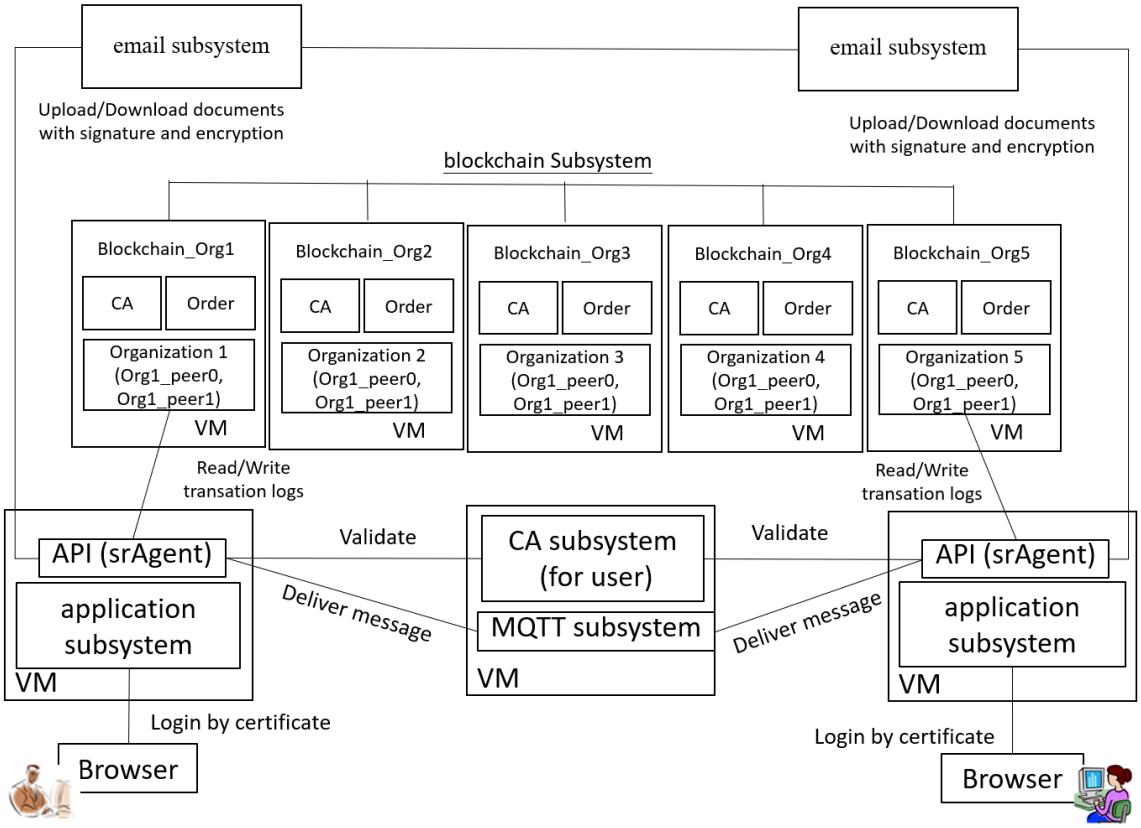

Figure 3. Deployment of prototype system

This prototype system is constructed as below:

(1) The email subsystem: Two physical email servers are used. For managing email server by its owner, the open-source Synology is used as the email subsystem to simulate the exchange center of official documents.

(2) The blockchain subsystem: The blockchain subsystem is deployed on 5 VMs as 5 organizations (Orgs). For cost saving, system portability and efficient use of resources, a container management program (Docker-ce) is imported. We use Hyperledger Fabric platform which is a consortium blockchain and allows developers to choose a consensus algorithm. Fabric has many plug-and-play components such as modular architecture and membership services. Fabric features include minority execution, majority verification / permission, fast processing and smart contract. These features meet the security requirements of electronic exchange system for official documents. Fabric peer is used to form a channel of registered users. The basic entity contains three types of nodes and Gossips, i.e., CA, Orderer, and Peer. The roles and tasks of all three nodes and Gossips are explained below [43].

A. CA is responsible for (A) registering, (B) submitting registered certificates (ECerts), (C) submitting transaction certificates (TCerts) and assuring the anonymity of blockchain transactions, and (D) extending and revoking the certificates.

B. Orderer is responsible for ensuring the exchanged transaction records are packed in a certain order and forming a sorted cluster with other Orderers. Furthermore, since the design of Fabric relies upon deterministic consensus algorithm, the blocks eventually verified by the Peer will be consistent. Thus, the ledgers will be free from having forks.

C. Four roles of Peer

- The Endorsing Peer is responsible for (A) submitting a proposal for endorsement, and responding to allow or reject endorsement, (B) maintaining smart contracts, (C) verifying whether or not the proposal of transaction follows the smart contract, and (D) asking the Endorser to sign the proposal.
- The Committing Peer is responsible for (A) verifying whether or not a transaction is legal, (B) submitting the blockchain, and (C) maintaining the current status of ledgers and the storage of local database.
- The Leader Peer is responsible for connecting the Orderer to download new blocks when they appear.
- The Anchor Peer is responsible for enabling its organization to communicate with another organization via Gossip.

D. Three tasks of Gossip

- It manages the Peers by constantly exploring new nodes and discovering new memberships of the channel.
- It passes ledger data to all Peers within the Channel. When one Peer receives a new ledger, it must update the ledger on the host and broadcast the most updated ledger to the other Peers as well.
- Through P2P, the nodes with old version ledger must update their ledger by Gossip.

(3) The application subsystem and S&R Module (srAgent): The application subsystem and srAgent are built on 2 VMs for sender and receiver respectively. We adopt spring boot framework to develop web application program and use Tomcat for web services. The application subsystem serves as the interface to simulate the host connecting the senders and receivers. The srAgent serves as the interface among CA, email, blockchain, MQTT and application subsystem.

(4) The CA Subsystem: The CA subsystem was installed on one VM. This CA subsystem uses certificates conforming to X.509 regulation for web application users to verify their identity. These certificate authorities include GCA for government agencies, MOEACA for organizations, XCA for institutes, and MOICA for citizens. This implementation is helpful for practical integration.

(5) The MQTT subsystem: The MQTT subsystem is established on the same VM of CA. The subsystem sends an extra message to the receiver for informing received documents. The delivery of this message will alert the receiver for checking the receiving of official documents in application subsystem.

4.2 Requirement of System Security and Experiment Setting

An experiment setting is developed according to the architecture in Figure 2. The email subsystem is responsible for the exchange mechanism. The security and trust mechanism are provided by blockchain, CA certificate and the MQTT subsystem. The user interface is responsible for the application subsystem. The procedures where a sender sends a document, and the receiver receives it are shown in Figure 4.

Before sending, the sender must log in to the web application and pass the identity verification. The system will (1) request CA then CA responds true or false, (2) use the sender's private key to sign and receiver's public key to encrypt the document if CA responds true, (3) pack the document with SMTP and upload to the email subsystem, (4) send a short message to the receiver with the MQTT protocol, and (5) write the relevant transaction log into the blockchain. The sender can check the received status from the blockchain at any time. If the receiver has no confirmation, the system will obey the time schedule to start the task of re-sending the document. If the confirmation message has not been received on schedule, the sender must manually intervene.

The receiver can log in the web application any time to receive the latest official documents. Even if the user does not log in the web application, srAgent still polls the mail server, receives new mails, disassembles the mail packets, and puts

them into the file system periodically.

After verifying the identity of receiver, the system will get the receiver's private key to decrypt and use the sender's public key to verify the signature and write the received time stamp into the blockchain. Thus, the sender can obtain the proof that the receiver has received the document already.

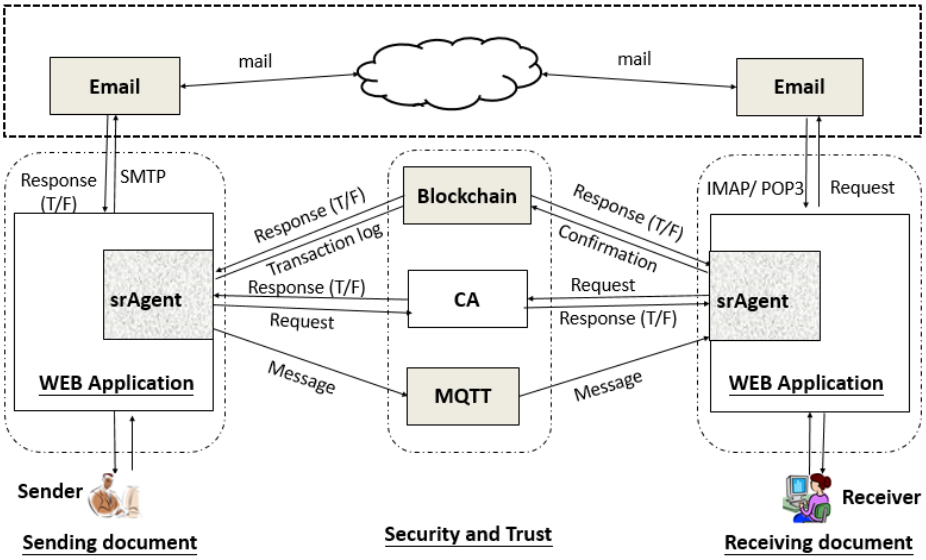

Figure 4. Data flow of proposed system

4.3 Test of Sending and Receiving Document

Once the user logs in the web application successfully with their certificates by verifying the identification through the CA of the S&R Module, they can use the sending function and upload the signed and encrypted document to the email subsystem. When the upload is completed, all related information, such as the amount of the documents sent, the sender, time of sending, etc., will be written into the blockchain subsystem and sent via MQTT as a brief message to the receiver. In Figure 5, there are three documents sent by sender U001. Documents whose ID are 10983570018 and 11059367811 have been received while the document with ID 10957477555 has not been received. When receiver U002 received the document with ID 10957477555, the sender U001 can see its received time stamp as shown in Figure 6.

If the receiver logs in successfully, s/he can use the receiving function to download documents and acquire all related information including the amount of the documents received, the subject, the sender, and the time that the sending and the receiving were completed, etc. (see Figure 7).

Document ID	Subject	Receiver	Sent time(MQTT)	Received time(MQTT)	Sent time(BC)	Received time(BC)
10957477555	Test 333	U002	2020-12-31 10:09:24		2020-12-31 10:09:24	
10983570018	Test 222	U002	2020-12-30 17:44:58	2020-12-30 17:45:55	2020-12-30 17:44:58	2020-12-30 17:45:55
11059367811	Test 111	U003	2020-12-30 17:25:19	2020-12-30 17:26:07	2020-12-30 17:25:19	2020-12-30 17:26:07

Figure 5. Sender U001's queried list with document (ID 10957477555) unreceived

Document ID	Subject	Receiver	Sent time(MQTT)	Received time(MQTT)	Sent time(BC)	Received time(BC)
10957477555	Test 333	U002	2020-12-31 10:09:24	2020-12-31 10:10:11	2020-12-31 10:09:24	2020-12-31 10:10:11
10983570018	Test 222	U002	2020-12-30 17:44:58	2020-12-30 17:45:55	2020-12-30 17:44:58	2020-12-30 17:45:55
10959367811	Test 111	U003	2020-12-30 17:25:19	2020-12-30 17:26:07	2020-12-30 17:25:19	2020-12-30 17:26:07

Figure 6. Sender U001's queried list with document received

Document ID	Subject	Sender	Sent time(MQTT)	Received time(MQTT)	Sent time(BC)	Received time(BC)
10957477555	Test 333	U001	2020-12-31 10:09:24	2020-12-31 10:10:11	2020-12-31 10:09:24	2020-12-31 10:10:11
10983570018	Test 222	U001	2020-12-30 17:44:58	2020-12-30 17:45:55	2020-12-30 17:44:58	2020-12-30 17:45:55

Figure 7. Receiver U002's queried list

Once an official document has been uploaded to the email system by the web application via the S&R Module, all related information, such as the code of the sender, the date and time of sending, the code of the receiver, the amount of the documents, the subject, etc., will be written into the transaction ledger via the smart contract of the blockchain system. When the receiver has downloaded official documents from the email subsystem, the date and time of receiving will be written into the transaction ledger of the blockchain subsystem (see Figure 8). Once the ledger has been written by the sender, the S&R Module will send a brief message via MQTT (see Figure 9) to double check that an official document is coming for collection.

```
type Message struct {
    IndexID          string `json:"indexID"`                    # Document ID
    SendOrgUnitID    string `json:"sendOrgUnitID"`              #Sender code
    SendTime         string `json:"sendTime"`                   # Sent date & time
    ReceiveOrgUnitID string `json:"receiveOrgUnitID"`           #Receiver code
    UserConfirmTime  string `json:"userConfirmTime"`            # Received date & time
    ApplicationID    string `json:"applicationID"`              # Application ID
    Topic            string `json:"topic"`                      # Subject
}
```

Figure 8. Content of blockchain record

```
private ExMsg build() {
    return ExMsg.builder()
            .author("U001")                                  # Sender code
            .serial("10957477555")                           # Document ID
            .title("Test 333")                               # Subject
            .type(ExMsg.Types.FROM_SENDER)                   #Upload message
            .time(Timestamp.valueOf(LocalDateTime.now()).getTime()) # sent  date& time
            .build();
}
```

Figure 9. Content of MQTT message

4.4 Evaluation of the Proposed System

This study conducts the evaluation of an experiment when sending and receiving a document in the proposed system. The evaluation results of security, performance and convenience are as follows.

(1) Evaluation of Security

A. Preventing from the tamper of blockchain ledger

The ledger with blocks 50-52 is shown in Figure 10. The linked block of ledger makes it uneasy to tamper with the blockchain. When an unauthorized modification of blockchain ledger occurs, the system will post error messages. The ledger will be locked before the recovery by the system. The error logs and denial of access are shown in Figure 11 and Figure 12 which proved the record of the blockchain ledger cannot be tampered with. Even if it has been tampered with, the system can detect the tamper, make the ledger unworkable, and recover the data. The test has successfully proven that the transaction of exchange is secure and trustworthy.

Block Details	
Channel name:	mychannel
Block Number	52
Cerate at	2021-02-25T07:38:08.508Z
Number of Transactions	1
Block Hash	c8e01d47dd3bfa3449e2b66f4474b0725f74b90f5b9a157711300e54d375f8a5
Data Hash	6b18e89dcc0977fbf02d494729decafda65633ae4894f6e289e8307d28d64f41
Prehash	7ba8fb048e2732670d31ad6808a7aac006eb6cd61609fec17e39fe028b7ef048

Block Details	
Channel name:	mychannel
Block Number	51
Cerate at	2021-02-25T07:21:36.113Z
Number of Transactions	1
Block Hash	7ba8fb048e2732670d31ad6808a7aac006eb6cd61609fec17e39fe028b7ef048
Data Hash	bd0487e966bed65520904bd4635c57bac75d653d864da01dece7ea2b3e8ac43d
Prehash	f5bdce9fef8543a66972b84b23cdcc14f2de84f2ec49dc3d4cec2c3a2680feff0

Block Details	
Channel name:	mychannel
Block Number	50
Cerate at	2021-02-25T07:38:08.508Z
Number of Transactions	1
Block Hash	f5bdce9fef8543a66972b84b23cdcc14f2de84f2ec49dc3d4cec2c3a2680feff0
Data Hash	ee324c5176ca164b4724f4faefa1ffa95ea004710be59c2e39d4cd77f6d2ce89
Prehash	55dda4eb149dfea8298bc5c553e20fae93045aa74428eb0de3bf910922c5ae4e

Figure 10. Link of ledger blocks

```
2021-03-12 09:58:08.786 CST [comm.grpc.server] 1 -> INFO 858a unary call completed grpc.service=discovery.Discovery grpc.method=Discover grpc.pe
er_address=172.243.2.1:48080 grpc.peer_subject="CN=Admin@org1.naadx.org,OU=admin,L=San Francisco,ST=California,C=US" grpc.code=OK grpc.call_dura
tion=317.618µs
2021-03-12 09:58:08.990 CST [fsblkstorage] nextBlockBytesAndPlacementInfo -> ERRO 858b Error reading next block bytes from file number [0]: unex
pected end of blockfile
2021-03-12 09:58:08.991 CST [common.ledger.blockledger.file] Next -> ERRO 858c unexpected end of blockfile
2021-03-12 09:58:08.991 CST [common.deliver] deliverBlocks -> ERRO 858d [channel: mychannel] Error reading from channel, cause was: SERVICE_UNAV
AILABLE
2021-03-12 09:58:08.991 CST [comm.grpc.server] 1 -> INFO 858e streaming call completed grpc.service=protos.Deliver grpc.method=Deliver grpc.peer
_address=192.168.62.1:63846 grpc.code=OK grpc.call_duration=3.806825ms
2021-03-12 09:58:09.301 CST [fsblkstorage] nextBlockBytesAndPlacementInfo -> ERRO 858f Error reading next block bytes from file number [0]: unex
pected end of blockfile
2021-03-12 09:58:09.301 CST [common.ledger.blockledger.file] Next -> ERRO 8590 unexpected end of blockfile
2021-03-12 09:58:09.301 CST [common.deliver] deliverBlocks -> ERRO 8591 [channel: mychannel] Error reading from channel, cause was: SERVICE_UNAV
AILABLE
2021-03-12 09:58:09.301 CST [comm.grpc.server] 1 -> INFO 8592 streaming call completed grpc.service=protos.Deliver grpc.method=Deliver grpc.peer
_address=192.168.62.1:63847 grpc.code=OK grpc.call_duration=1.09145ms
2021-03-12 09:58:09.582 CST [fsblkstorage] nextBlockBytesAndPlacementInfo -> ERRO 8593 Error reading next block bytes from file number [0]: unex
pected end of blockfile
2021-03-12 09:58:09.582 CST [common.ledger.blockledger.file] Next -> ERRO 8594 unexpected end of blockfile
2021-03-12 09:58:09.582 CST [common.deliver] deliverBlocks -> ERRO 8595 [channel: mychannel] Error reading from channel, cause was: SERVICE_UNAV
AILABLE
2021-03-12 09:58:09.582 CST [comm.grpc.server] 1 -> INFO 8596 streaming call completed grpc.service=protos.Deliver grpc.method=Deliver grpc.peer
_address=192.168.62.1:63848 grpc.code=OK grpc.call_duration=2.615412ms
2021-03-12 09:58:09.692 CST [fsblkstorage] nextBlockBytesAndPlacementInfo -> ERRO 8597 Error reading next block bytes from file number [0]: unex
pected end of blockfile
2021-03-12 09:58:09.692 CST [common.ledger.blockledger.file] Next -> ERRO 8598 unexpected end of blockfile
2021-03-12 09:58:09.693 CST [common.deliver] deliverBlocks -> ERRO 8599 [channel: mychannel] Error reading from channel, cause was: SERVICE_UNAV
AILABLE
```

Figure 11. System error logs

```
[fabric@org1 javascript]$ node query.js
Wallet path: /home/fabric/archives/message/javascript/wallet
user1 ok
Failed to evaluate transaction: Error: EACCES: permission denied, scandir '/var/lib/docker/volumes/net_peer0.org1.naadx.org/_data/ledgersData/ch
ains/chains/mychannel/'
[fabric@org1 javascript]$ node invoke.js
Wallet path: /home/fabric/archives/message/javascript/wallet
```

Figure 12. Denial of access

B. Preventing from counterfeited identity

All users must register with a certificate before they use the system. When any unregistered user logs in the system, it will fail. Therefore, it is difficult for users to forge one's identity. When an unspecified receiver catches someone's document, the document cannot be decrypted and read to ensure the confidentiality of the document. The use of PKI upon the management of users makes counterfeiting identity impossible. After sending an email, there is information with certificate and time stamp to ensure security, to prevent receiver from receiving counterfeited email.

C. Preventing from tampered document

If the document was tampered with before the email was received, the verification of signature will fail when the receiver received it. It means that the document has been tampered with. The document sent by email acquires certificate and signature which were encrypted by both the sender and receiver. The integrity and authenticity of the document are secured.

D. Preventing from missed email

When the document was uploaded into an email, the system will automatically send a message to the receiver. If

the receiver's email was thrown into spam, the receiver could receive the message from MQTT still. Then, the receiver can ask the sender to resend the document. When the time stamp received is not written into the blockchain database within time schedule, the system will automatically resend the document. Therefore, the system can ensure the arrival of documents from sender to receiver.

E. Preventing from single node failure

The node service will be stopped when the node fails. The entire system can keep running without its availability being affected.

(2) Evaluation of Performance

A. Response time and latency

The transaction logs of blockchain ledger shows that the time for signing and encrypting a document is close to that of SPEED. However, the email's response time is quicker than that of exchange center. In case of a single user, the bottleneck of sending and receiving a document in the proposed system is in card readers instead of software. The response time is acceptable.

B. System capacity

In the case of multiple users, the capacity of the proposed system depends on that of the mail server. Since the users are distributed in different mail servers, the capacity of the proposed system is better than that of SPEED.

C. System availability

At present, there are 26 exchange centers and 35,000 users in the SPEED. The daily number of documents exchanged by agencies exceeds 6.58 million [44], and each exchange center has an average of up to 1,400 users. When an exchange center fails, users registered in that center cannot exchange documents. The proposed system replaces the centralized exchange center by email server. Therefore, when the email server of an agency fails, only the users registered in that server are affected and cannot operate properly. In other words, this proposed system can improve overall usability and availability.

D. System reliability:

The transaction logs are stored in a centralized database of each exchange center in SPEED. These records may be tampered with unauthorized actions. Sometimes users questioned/unquire about the time of sending and receiving the document. This proposed system replaces the centralized database by the decentralized blockchain ledger. Once the transaction log is completed, it cannot be modified. Therefore, this proposed system can improve the reliability of the system.

(3) Evaluation of Convenience

Any organization can establish its own web application which integrates S&R Module provided by the proposed system. Unlike S&R Module, the proposed system also provides a web application or APP for general public. Through digital certificate, email, and appropriate device, individual user can communicate with agencies anytime and anywhere without passing a piece of paper. Smartphones, tablets, laptops or desktop computers with a browser can be used in the proposed system. Therefore, the proposed system is more convenient than before.

5 Conclusion

Openness and trust are crucial elements of agency for successful communication with other agencies and the public. API creates openness and blockchain builds up trust. Using API and blockchain can help agencies to reach their goals toward innovation and transformation. Thus, blockchain, API and email with digital certificate are used to create a new channel for government affairs which becomes open and trustworthy.

5.1 Research Contribution

The architecture proposed by this study has the following contributions.

(1) Secure and trustworthy network: The proposed system provides a ledger which cannot be tampered with. This system can also operate when a single node fails. The system provides high availability and reliability. The ledger of the system increases security and credibility. The digital certificate verifies user's identity so that it can prevent counterfeited identity. Furthermore, the digital signature and encryption not only help the non-repudiation of users but also enhance the confidentiality and security of documents. It can be extended to connect individuals or worldwide organizations. Therefore, the proposed architecture indeed has its extension for users.

(2) Transformed government service: Any individual can use email to receive documents from agencies anytime and anywhere. Comparing to conventional paper document, the proposed system is free from the limits of space and time. Therefore, this system can provide the benefit of energy saving by reducing the use of paper.

(3) Open and transparent data governance: There were large numbers of documents exchanged among agencies [44]. Through the integration of these related data into the blockchain ledger, it provides innovation to the public by adding value to the data.

(4) Lower Cost of Maintenance: Since email is a necessity to agencies, they don't need to implement another dedicated system for document exchange. Besides, almost citizens have their own email accounts. There is no extra cost for the training of the public. Therefore, the cost is low.

5.2 Future Research

Based on the email and blockchain technologies, this study proposes an architecture for electronic exchange of official documents. The evaluation of security, performance and convenience have shown that the architecture is feasible and efficient. Nonetheless, there are still related issues which can be incorporated into follow-up research in the future. For instance, researchers can use a business-oriented email system with open API to integrate web application of the proposed architecture. Besides, this architecture can be extended to other fields such as commercial transaction application.

References

[1] Y. F. Lin, I. H. Yeh, The Discussion the Strategy of Improving Government Effectiveness from the Deficiency of Official document Process Management, *Archives Semiannual*, Vol. 19, No. 1, pp. 24-35, June, 2020.

[2] K. W. Su, H. Y. Chang, K. C. Wang, A Practical Approach for User Interface Design of a G2B Based Official Document Exchange System in Taiwan, *International Journal of Innovative Computing*, Information and Control, Vol 7, No. 11, pp. 6423-6436, November, 2011.

[3] S. H. Weng, *A Study on Enhancing Electronic Document Exchange System Security Mechanisms with Digital Watermarking Technology*, Master Thesis, Management College National Defense University, Taoyuan, Taiwan, 2019.

[4] R. Y. Gu, *Open Document Format Promotes Acceptance Research through the Electronic Official Document Exchange System*, Master Thesis, Chinese Culture University, Taipei, Taiwan, 2020.

[5] C. H. Wu, *A Study of the Implementation for a High-Secure Cloud-Based Exchange Model of Electronic Medical Records in Conformity with IHE Framework*, Master Thesis, National Kaohsiung First University of Science and Technology, Kaohsiung, Taiwan, 2016.

[6] C. M. Chiu, C. F. Lin, The Policy Development and Promotion Strategy of the Service for Passing and Exchanging Electronic Documents System, *Archives Semiannual*, Vol. 19, No. 2, pp. 4-23, December, 2020.

[7] K. Y. Yang, Using Blockchain Technology to Improve Digital Services in the Public Sector: a New Opportunity for Electronic Official Document Interchange Mechanism, *Archives Semiannual*, Vol. 18, No. 2, pp. 106-117, December, 2019.

[8] C. R. Neu, R. H. Anderson, T. K. Bikson, E-Mail Communication Between Government and Citizens-Security, Policy Issues, and Next Steps, *Issue Paper, RAND Science and Technology*, pp. 1-9, January, 1998.

[9] S. Whittaker, V. Bellotti, J. Cwizdka, *Everything through e-mail, Personal information management*, University of Washington Press, Settle and London, 2007, pp. 167-189.

[10] M. Sampson, Electronic Mail, *Encyclopedia of Information Systems*, dblp computer science bibliography, 2003.

[11] H. A. Aldawood, G. Skinner, A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications, *26th International Conference on Systems Engineering*, Sydney, Australia, 2018, pp. .

[12] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, A. Martin, Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues, *IEEE Communications Surveys & Tutorials*, Vol. 21, No. 3, pp. 2886-2927, Third Quarter, 2019.

[13] J. C. González, V. García-Díaz, E. R. Núñez-Valdez, A. G. Gómez, R. G. Crespo, Replacing email protocols with blockchain-based smart contracts, *Cluster Computing*, Vol. 23, No. 3, pp. 1795-1801, September, 2020.

[14] R. Kumar, A. J. Singh, Understanding steganography over cryptography and various steganography techniques, *International Journal of Computer Science and Mobile Computing*, Vol. 4, No. 3, pp. 253-258, March, 2015.

[15] A. Alsaidi, K. Al-lehaibi, H. Alzahrani, M. AlGhamdi, A. Gutub, Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding, *Journal of Computer Science & Computational Mathematics*, Vol. 8, No. 3, pp. 33-42, September, 2018.

[16] A. Malik, G. Sikka, H. Verma, A high capacity text steganography scheme based on LZW compression and color coding, *Engineering Science and Technology*, Vol. 20, No. 1, pp. 72-29, February, 2017.

[17] M. Almazrooie, A. Samsudin, A. A. A. Gutub, M. S. Salleh, M. Omar, S. A. Hassan, Integrity verification for digital Holy Quran verses using cryptographic hash function and compression, *Journal of King Saud University - Computer and Information Sciences*, Vol. 32, No. 1, pp. 24-34, January, 2020.

[18] S. Whittaker, C. Sidner, Email overload: Exploring personal information management of email, *Proceedings of the SIGCHI conference on Human factors in computing system*, Vancouver, BC, Canada, 1996, pp. 276-283.

[19] B. V. Hanrahan, M. A. Pérez-Quiñones, Lost in email: Pulling users down a path of interaction, *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea, 2015, pp. 3981-3984.

[20] M. Ferris, New Email security infrastructure, *Proceedings of the 1994 workshop on new security paradigms*, Little Compton, RI, USA, 1994, pp. 20-27.

[21] M. F. Hinarejos, J. L. Ferrer-Gomila, A Solution for Secure Multi-Party Certified Electronic Mail Using Blockchain, *IEEE Access*, Vol. 8, pp. 102997- 103006, May, 2020.

[22] K. Elmaghraby, T. Dimitriou, Blockchain-Based Fair and Secure Certified Electronic Mail Without a TTP, *IEEE Access*, Vol. 9, pp. 100708-100724, July, 2021.

[23] M. F. Hinarejos, J. L. Ferrer-Gomila, L. Huguet-Rotger, A Solution for Secure Certified Electronic Mail Using Blockchain as a Secure Message Board, *IEEE Access*, Vol. 7, pp. 31330-31341, February, 2019.

[24] X. L. Bao, A Decentralized Secure Mailbox System based on Blockchain, *2020 International Conference on Computer Communication and Network Security*, Xi'an, China, 2020, pp. 136-141.

[25] M. D. Juan, R. P. Andrés, P. M. Rafael, R. E. Gustavo, P. C. Manuel, A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain, *International Journal of Modeling and Optimization*, Vol. 8, No. 3, pp. 160-165, June, 2018.

[26] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, Accessed 2 January 2021.

[27] R. Rivera, J. G. Robledo, V. M. Larios, J. M. Avalos,

How digital identity on blockchain can contribute in a smart city environment, *2017 International Smart Cities Conference*, Wuxi, China, 2017, pp. 1-4.
[28] S. Figorilli, F. Antonucci, C. Costa, F. Pallottino. L. Raso, M. Castiglione, E. Pinci, D. Vecchio, G. Colle, A. R. Proto, G. Sperandio, P. Menesatti, A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain, *Sensors*, Vol. 18, No. 9, Article No. 3133, September, 2018.
[29] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, *Journal of medical systems*, Vol. 40, No. 10, Article No. 218, October, 2016.
[30] C. Esposito, A. D. Santis, G. Tortora, H. Chang, K. R. Choo, Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, Vol. 5, No. 1, pp. 31-37, January-February, 2018.
[31] D. Kumar, D. Chandini, B. Reddy, D. Bhattacharyya, T. H. Kim, Secure Electronic Voting System using Blockchain Technology, *International Journal of Advanced Science and Technology*, Vol. 118, pp. 13-22, 2018.
[32] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, A. Kamišalić, EduCTX: A Blockchain-Based Higher Education Credit Platform, *IEEE Access*, Vol. 6, pp. 5112-5127, January, 2018.
[33] A. Poller, U. Waldmann, S. Vowé, S. Turpe, Electronic identity cards for user authentication-promise and practice, *IEEE Security and Privacy*, Vol. 10, No. 1, pp. 46-54, January-February, 2012.
[34] M. E. Peck, Blockchains: How they work and why they'll change the world, *IEEE Spectrum*, Vol. 54, No. 10, pp. 26-35, October, 2017.
[35] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, *IEEE Access*, Vol. 4, pp. 2292-2303, May, 2016.
[36] T. Bocek, B. B. Rodrigues, T. Strasser, B. Stiller, Blockchains everywhere - a use-case of blockchains in the pharma supply-chain, *2017 IFIP/IEEE Symposium on Integrated Network and Service Management*, Lisbon, Portugal, 2017, pp. 772-777.
[37] J. Zhang, S. Zhong, T. Wang, H. C. Chao, J. Wang, Blockchain-Based Systems and Applications: A Survey, *Journal of Internet Technology*, Vol. 21, No. 1, pp. 1-14, January, 2020.
[38] H. Hou, The Application of Blockchain Technology in E-Government in China, *26th International Conference on Computer Communication and Networks*, Vancouver, BC, Canada, 2017, pp. 1-4.
[39] F. M. Hsu, T. F. Ho, The Challenges of Blockchain Applications on Administrative Innovation in Government, *Archives Semiannual*, Vol. 20, No. 1, pp 4-15, June, 2021.
[40] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, J. Han, When Intrusion Detection Meets Blockchain Technology-A Review, *IEEE Access*, Vol. 6, pp. 10179-10188, January, 2018.
[41] T. V. Le, C. L. Hsu, A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges, *Journal of Internet Technology*, Vol. 22, No. 4, pp. 789-802, July, 2021.
[42] Z. Zheng, S. Xi, H. N. Dai, X. Chen, H. Wang, Blockchain Challenges and Opportunities: A Survey, *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp. 352-375, October, 2018.
[43] *A Blockchain Platform for the Enterprise*, https://hyperledger-fabric.readthedocs.io/en/release-2.2/, Accessed 16 June 2021.
[44] National Archives Administrator, official document e-web, *Statistics of document exchanged in June 2022*, https://www.good.nat.gov.tw/download.php?area=5&page=1, Accessed 5 August 2022.

Biographies

Chu-Mei Chiu is a Ph.D. candidate of Department of Information Management at the National Dong Hwa University, Taiwan. She worked at Information Technology Division at the National Archives Administration for 20 years. Her research interests include blockchain, information management, and electronic records management, digital archives.

Fang-Ming Hsu is a professor of Department of Information Management and Dean of College of Management at the National Dong Hwa University, Taiwan. He is also a member of the committee of national archive management in Taiwan Government. His areas of interest include knowledge management, data mining and business intelligence.

Meng-Hsiang Shen is a Ph.D. candidate in the Department of Information Management at the National Dong Hwa University. He also serves in the Department of Information Management at St. Mary's Junior College of Medicine, Nursing, and Management. His research interests include information management and data mining**.**

Chun-Min Lin is an assistant professor at the Marketing and Distribution Management Department, Tzu Chi University of Science and Technology in Hualien, Taiwan. He is currently a member of The Association for Computational Linguistics and Chinese Language Processing. He received his Ph.D. degree in National Dong Hwa University, Taiwan.