A Study on the Process of Claiming Casualty Insurance based on Smart Contracts

Shun-Yuan Ho[1], Tsung-Che Wu[2], Bo-Yu Chen[2], Tzer-Long Chen[3], Hsiu-Chia Ko[1]*

[1] Department of Information Management, Chaoyang University of Technology, Taiwan
[2] Department of Banking and Finance, National Chiayi University, Taiwan
[3] Department of Healthcare Administration and Medical Informatics, Kaohsiung Medical University, Taiwan
s10614902@gm.cyut.edu.tw, tcwujeff@mail.ncyu.edu.tw, s1111175@mail.ncyu.edu.tw, tlchen@kmu.edu.tw, hcko@cyut.edu.tw

Abstract

The insurance claim process is quite cumbersome; it is time-consuming, with high personnel costs from manual review. It may even take several months to complete the entire process. Therefore, how implementing insurance claim settlement automation to reduce costs, improve efficiency, reduce claim processing time, and increase client satisfaction is a common issue the insurance industry must face. This study explores the application of smart contracts in the casualty insurance settlement process to achieve the effect of automatic claim settlement and double protection for special accidents. When the insurance industry conducts insurance claim reviews through the characteristics of blockchain and smart contracts, such as openness and transparency, anonymity, and automation, the review process can be curtailed, and the premium can be directly transferred to the bank account of the insured. Thus, the purpose of automating casualty insurance claims is achieved through smart contracts.

Keywords: Casualty insurance, Blockchain, Smart contract, Automation, Efficiency

1 Introduction

1.1 Research Purpose and Issues

Regarding handling casualty insurance, insurance claim settlement is the issue the public is most concerned about, for it is often very time-consuming to process the claim application and benefit judgment in the case review. Because of the definition of the principle of compensation for damages, the insured cannot obtain profits exceeding the losses due to the onset of the insured event. To prevent money laundering or fraud, the insurance industry must undergo repeated audits to confirm that it is authentic before compensating the insured. The lengthy claim settlement process means not only increased labor costs but also causes a delay in the allocation of insurance benefits, and the insured cannot immediately obtain the rights and interests of insurance compensation.

To improve these problems, the insurance industry has begun to promote the automation of insurance claims, hoping to shorten the review process of claims and reduce the manpower and time spent on review; so that the progress of the claim process can be completed in a short time to improve customer service satisfaction. There are already cases of claim automation; for example, Taiwan Life Insurance launched the claim settlement service of "Scan QR code for instant health check fees". When the policyholders receive the notice, they need to scan the exclusive QR Code inside and enter the relevant information for the payment. If the receiving bank has participated in the eACH (Enhanced Automated Clearing House) system, an e-remittance system mechanism with 21 banks currently registered, the policyholders can receive health check premium within 2 minutes at the fastest and 30 minutes at the latest. This practice makes it easy for policyholders to complete the application easily and changes the passive way policyholders receive the premium. Currently, this service is limited to health insurance only. In recent years, financial technology has become more mature. If this technology can be combined and applied in the insurance industry, the automation of insurance claims for other types of insurance is just around the corner. Therefore, this study explores how to integrate smart contract technology with the insurance industry to achieve automation of insurance claims.

1.2 Research Purpose and Issues

This study explores the application of smart contracts in casualty insurance. Blockchain technology and smart contract features, such as openness and transparency, non-tampering, automation, etc., will prompt insurance companies to review casualty insurance claims and shorten the overall time of claim processing. At the same time, it reduces the time and labor costs required and reduces human error through electronic system services; victims of accidents can get compensation for losses as soon as possible. Therefore, smart contracts combined with casualty insurance claims benefit the insurance industry and can safeguard customers' rights and interests. This study assumes that the casualty insurance's proposer, insured, and beneficiary are all the same person; therefore, the insured will be discussed as the subject of insurance.

Issues to be discussed:

(1) How to sign a smart contract between the insurance company and the insured so that it can be applied to

*Corresponding Author: Tzer-Long Chen; E-mail: tlchen@kmu.edu.tw
DOI: https://doi.org/10.70003/160792642024122507005

casualty insurance claims.
(2) How to apply digital signature technology to the settlement of casualty insurance claims.
(3) Explore the differences before and after the application of smart contracts in the claims process.

2 Literature Review and Exploration

2.1 Casualty Insurance

Injuries caused by accidents are often unpredictable. For example, conditions like death, disability, and food poisoning have been combined with casualty insurance claims, which is also the basic norm for emergencies and external injuries.

In accordance with Article 131 of the Insurance Act, "a personal accident insurer is obligated to pay the insured amount when the insured suffers injury by accident, or becomes disabled or dies on account of such injury. The term "injury by accident" as used in the preceding paragraph refers to physical harm caused by unforeseen external events other than illness." Accidents are defined on the premise of "accident" excluding external, sudden, and non-disease causes. It protects the insured from the outpatient and hospitalization medical losses the insured have to bear due to accidents. The payment of expenses is divided into full reimbursement and rationed payment. There are four types of casualty insurance [1-2]: 1) Whole life casualty insurance: All irreversible injuries, such as hospitalization, surgery, disability, and death of the victim due to accidents, which are approved under the procedures of the insurance company; 2) disability insurance: A kind of care insurance when certain parts of the body losses function due to accident or disease resulting in the loss of work and living ability; 3) medical insurance: An insurance covers the expenses during hospitalization when the insured is under medical care. There are two types of payment for medical insurance: full reimbursement and rationed payment; 4) major burn insurance.

Table 1 shows a summary of casualty insurance claims and coverage items.

Table 1. Items covered in casualty insurance

Items covered in casualty insurance		
Items	Coverage	Descriptions
Accidental death & Dismemberment	Death	Return paid premium plus interest for the insured under age 15
	Dismemberment	Based on the proportion listed in the disability level table
Hospital income benefit	Accidental hospital costs	The actual Number of days of hospitalization multiplied by the daily amount
	Fracture outpatient	Including days of non-hospitalization and days of hospitalization with less than complete fracture
Accident full reimbursement	The actual amount spent within the coverage	Difference from medical insurance: outpatient medical treatment can apply for claims.

2.2 Blockchain

Blockchain is a technology that uses cryptography to connect and copy data. With the help of algorithms and cryptography, the transaction records on the blockchain are encrypted and then copied and stored in miners' computers all over the world [3, 22].

The three major features of blockchain are 1) Decentralization: also known as "Trust Machine". It is a data structure that emphasizes sharing of recorded data. By storing data on different cloud systems and combining point-to-point network relationships, it can establish the trust effect without routing through and controlled by the third-party central organization; it can operate in a decentralized system to ensure the security and traceability of the transaction data. 2) Immutability: Once the transaction data is recorded in each block, no user can change or delete it; it can only be corrected by adding new data. After the data is verified, it will be permanently written into the block, co-existing with the records entered in the past. Through the one-on-one function technology of the algorithm, the data is prevented from being artificially tampered resulting in a lack of accuracy in the transaction records. Complex and difficult-to-crack functions are used to ensure data security. 3) Traceability: When the transaction data has been placed on the block, the data and input records cannot be tampered with, and any past transaction records can be checked at any time. If any problem occurs during the data transmission process, the process of each system can be traced to find the source of the error [4, 18].

The construction types of blockchain applications are divided into 1) Public chain: a completely open and transparent blockchain, such as Bitcoin and Ethereum, allowing everyone to edit, read, verify, and freely participate in the consensus mechanism, which is the major type of the current blockchain type. 2) Alliance chain: combining the features of both public and private chains, it retains decentralization, but consensus verification needs to be completed for some nodes. Compared with the public chain, the alliance chain is slightly better at reducing the number of nodes and improving operational efficiency; compared with the private chain, it has the advantage of reducing the counterparty risk. It is common in the same type of enterprises or different enterprises with cooperative relations [5]. 3) Hybrid chain: a combination of multiple different blockchain types. According to different needs, such as the concatenation of alliance chain information by enterprises to improve operational efficiency, the e-fingerprint data is written into the public chain, and the integration of multilateral information is achieved [6, 17].

Blockchain technology is well known in today's society; it can be combined with the fields such as finance, agriculture, education, etc. Blockchain can improve transaction efficiency and maintain user privacy simultaneously; it executes automation through established rules and improves the scale between various nodes [7].

2.3 Digital Signature

A digital signature is an electronic encryption verification seal that can confirm digital information such as e-documents, macros, or e-mails. The technology it provides can be used to maintain the security of -documents and confirm whether the information comes from the signer and whether the content has been tampered with.

A digital signature made with "asymmetric" encryption technology uses technology in the field of public key encryption to open e-documents through a pair of keys – a private key and a public key, where the private key is privately owned and the public key is public [8]. Based on the existing file content, an encrypted verification value is calculated by a mathematical algorithm or other methods so that the data receiving end can successfully verify it, which can ensure the correctness of the source of the file and the integrity of the content [8].

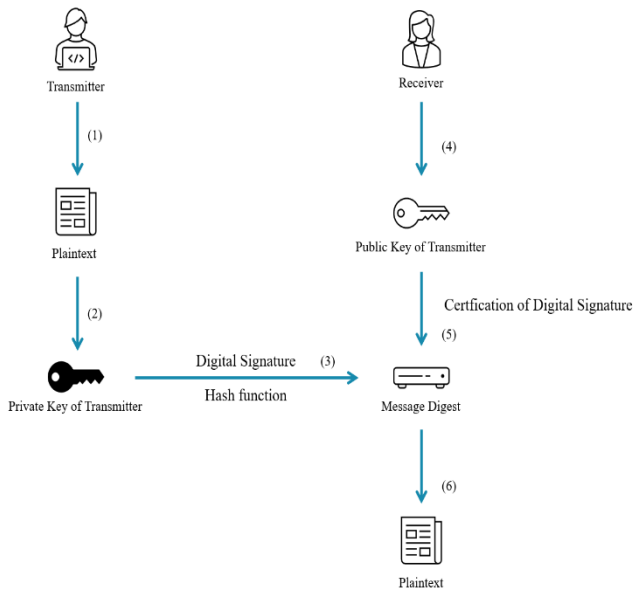

Figure 1. The schematic diagram of the digital signature operation process

The elements of a digital signature are 1) public key: encryption calculation and verification of the signature value; 2) private key: decryption calculation and calculation of the signature value; 3) digital fingerprint: one-way verification of information content irreversible hash calculation [9]. The characteristics of digital signatures ensured by the above elements include 1) Unforgeability: The signer uses his private key to sign the document. If a blocker other than the signer and verifier wants to block the document, he must first obtain the signature of the document and all the split messages before execution. Those who want to engage in improper conduct cannot block and forge information if they do not have the private key. 2) Privacy: Modified files will not leave any clues of hidden information, and the subsequent blockers will not be able to learn the hidden content. This is also true for third parties so that they can achieve the goal of not leaking the information. 3) Unlinkability: The same original document has different signatures after being processed by different blockers, which means that others cannot learn any hidden information from the signatures of each document. If the signer wants to hide part of the information, in addition to removing the part of the content, the original signature must be divided into a new signature so that those who are interested will not be able to know the hidden content [10, 21]. Figure 1 shows the process of the digital signature operation.

2.4 Smart Contract

Smart contract is an important technology for formulating special agreements for contracts in blockchain. It is a program stored on blockchain, which can perform logical judgment and execution of the contract [11]. Nick Szabo, an expert in computer and cryptography, proposed the concept of smart contracts in 1994, advocating that transaction terms can be implemented through computerization. Smart contracts follow the principle of "If-Then", for example: (If) only when the agreed amount is sent to the system, then the ownership of the goods will be automatically transferred to the buyer. In the application of smart contracts, the ownership of money and objects can also be stored in the blockchain system; so that each transaction can be witnessed and verified by hundreds of people to ensure the success of the transaction and the accuracy of the information, and also reduce intermediary agency payroll costs.

In recent years, the application of blockchain technology in the financial and real estate fields has been changing dramatically; in addition to improving work efficiency, it can also improve the existing difficulties in the business process [12]. A smart contract is a string of codes running on the blockchain. Taking Ethereum as an example, imagine that while every miner runs this code simultaneously, the code will not be tampered with and is completely open and transparent. No one changes the content and execution of the smart contract; thus, it can provide better protection and enforcement for both parties [13, 19].

Nowadays, there are many smart contract applications and virtual token systems on Ethereum, which has been a well-known blockchain platform in recent years [14]. Smart contracts may have uncertainties and exceptional situations when processing contracts. A mechanism called "supervisory sandbox" can be used to test the compensation mode. This mechanism allows companies to conduct real tests within a certain regulatory scope without fully complying with existing strict regulations, thus avoiding legal and regulatory issues in the insurance smart contract field [20, 23].

Before signing a contract, you must first register as a user on a platform mutually recognized by both parties to the contract to mutually confirm whether the overall procedure is legal and use your personal public and private keys as the identity authentication of the contract signer. When a contract is produced according to the transaction conditions, all the content in the contract must be agreed upon and signed

by both parties before it becomes effective; then the smart contract is placed on the decentralized blockchain platform and distributed among the nodes; when the set conditions are met, the contract is executed automatically. There are four elements in a smart contract: 1) Contract subject: used to automatically execute pre-established operations, such as: opening related services, locking restrictions in the contract, etc.; 2) digital signature: using the communicator's private key to carry out transactions certification, the transaction will be recognized only after the certification operation is completed; 3) contract terms: the operations formulated in the smart contract and all its contents are public information, and can only be executed after the participants agreed and signed; 4) decentralized platform: the smart contract will be placed on a specific decentralized platform, and when the set conditions are met, it will be distributed among the nodes for execution [15-16]. The review process of casualty insurance claims application is shown in Figure 2.

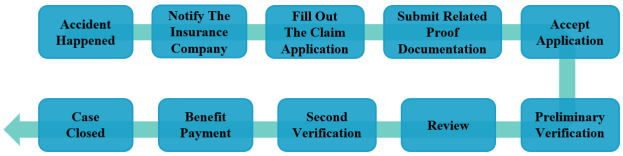

Figure 2. Review and claim application process for casualty insurance

3 Methodology

Before the contract is formally signed, the main stakeholders or units of the claim settlement process must first register as legal users on the approved blockchain website; the relevant eight parties include the insured, hospitals, police, arbitration associations, pharmacies, third-party units, court, and the insurance company. When the registration is completed, all parties concerned will jointly own a shared ledger, which has the characteristics of a blockchain, including immutable data, decentralization, and traceability of records which can protect the rights and interests of all parties. When smart contracts complete the review of insurance claims, the benefit will be automatically transmitted to the insured's bank account to complete the automatic claim settlement process for casualty insurance, which can improve the speed of claim settlement and customer satisfaction. The research framework is shown in Figure 3. Finally, this study assumes that the proposer, insured, and beneficiary of casualty insurance are all the same person; therefore, the insured will be discussed as the main body of insurance.

Integrating technology and claim process through the parametric equations of smart contract, this study explores how to use smart contracts in the casualty insurance claims process to shorten the claim review process, speed up claim payments, reduce labor costs and reduce human-induced errors while improving information security.

The equations established in this study will be encrypted and decrypted in combination with e-technologies such as digital signatures and blockchains. The blockchain has the characteristics of decentralization, non-repudiation, and stability; therefore, the smart contracts deployed in blockchains also meet the above conditions. The information in the blockchain is open and transparent; users' basic rights and interests can be protected against the risks at the information level.

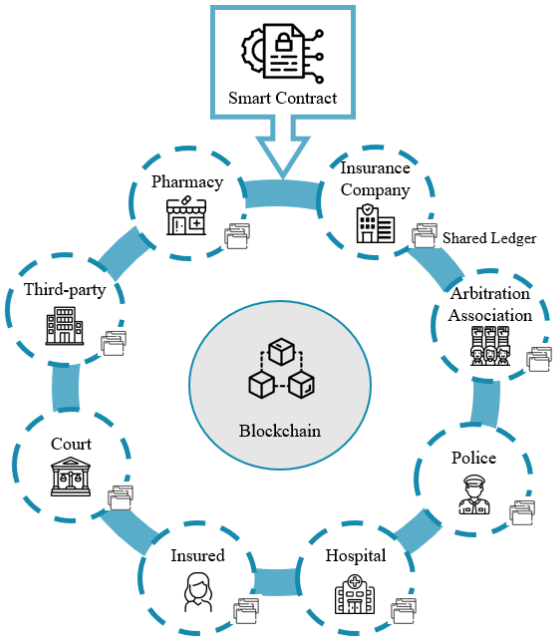

Figure 3. Research framework for claim settlement

The procedure is divided into registration and claim settlement processes. The persons and units related to this process include the insured, the police, hospitals, courts, pharmacies, arbitration associations, banks, and third-party institutions. When an accident occurs, the procedure for insurance claims will involve all relevant people and units in this process. The hospital will issue the pharmacy the patient's drug quota and the medical group key; the third-party agency will issue the police service certificate key; the insurance company will issue the group signature to the authorized sales representatives and issue a certification card to the insured. The insured then has the rights covered by the casualty insurance contract. When the claim is approved, the claim will be automatically transmitted to the insured's bank account.

In terms of protecting the privacy of customers' rights and interests, the private key of the insured will be stored in the certification card signed by the insurance company; the hospital will apply to the pharmacy for the key to be signed by the medical group to store the drug quota in the medical records; the arbitration association applies to the court for a key to sign the arbitration case and the judgment to be stored in the judgment document; and the policy applies to a third party to sign the key and store it in the police service card under the condition of anonymity. Except that the original applicant can check the real identity of the signer, the others can only check the accuracy and completeness of the signature through a public key without knowing the real identity of the signer, providing a comprehensive mechanism for privacy protection.

When an accident occurs, the insured will receive the case certificate after reporting the case and the diagnosis certificate issued by the hospital, and the medicine from the pharmacy based on the prescription issued by the doctor. When the insured applies to the insurance company for compensation, the police pass the case certificate to the insurance company through a private key as an accident certificate for authenticity. The hospital passes the diagnosis record to the insurance company through a private key to verify the trauma of the insured. The insurance company then approves the amount of benefit to be paid that meets the claimed standard. The arbitration association transmits the judgment to the court through a private key. When the insurance company receives the information, it will first check the authentication card of the insured stored in the insurance company's system as a basis for confirming whether the insured meets the coverage of the insurance contract. If the information is verified through the automatic appropriation system, the insurance benefits will be remitted to the insured's bank account, and automatic claim settlement for casualty insurance implementation will be completed through smart contracts. Table 2 describes the process from application registration to claim settlement in a parameter comparison table.

Table 2. Parameter comparison

Person	Secret key	Public key
Insured	SK_{INS}	PK_{INS}
Hospital	SK_{HP}	PK_{HP}
Insurer	SK_I	PK_I
Police	SK_P	PK_P
Arbitration Association	SK_{AA}	PK_{AA}
Hospital Group signature	GSK_{HP}	GPK_{HP}
Police Group signature	GSK_P	GPK_P
Other		
Insured proposes for Insurer		P_{INS}
Detailed items to apply for casualty insurance		Pci
Insured's key certificate		CFC_{INS}
Code number		CN_{INS}
Insured's payment for Life Accident and Dismemberment Insurance expenses' certificate		Doc
Insured's public key certificate		$PCFC_{INS}$
Insurer Group authorized public key to Salesperson		APK_{SP}
Signature		S
User		U
Prime number		p, n
Group public key		GPK
Group secret key		GSK
Hash function		H
Group Manager		GM
Mediation Server		MS
Verifier		Ver
User identify information		ID_U
User secret key		GSK_U
Group Manager secret key		GSK_{GM}
Group Manager public key		GPK_{GM}
Group Mediation Server secret key		GSK_{MS}
Group Mediation Server public key		GPK_{MS}
Information		i
Time random number		t
Hospital identity		ID_{HP}
Police's service certificate		ID_{PS}
Arbitration Association case		ID_{AA}
Hospital key certificate		KC_{HP}
Police's key certificate		KC_P
Arbitration Association key certificate		KC_{AA}
Hospital application for group signature from Pharmacy		S_{HP}
Police's application for group signature from Independent Agency		S_P
Arbitration Association application for key signature from Courthouse		S_{AA}
Diagnosis of proof certificate		PC_D
Diagnosis fee data		FD_D
Medicine tagged prescribe		GP_{HP}
Case certificate		PC_C
Arbitration Association verdict		PC_{AA}
Electronic payment details		$E\text{-}Pay$
Equation of Group signature key		E_{GK}
Master Key		MK
Decrypting with secret key of Insurer		D_{SK_I}
Encrypting with public key of Insurer		E_{PK_I}
Verifying the correctness of medical Group group public key		$V_{GPK_{HP}}$
Verifying the correctness of the police's group public key		V_{GPK_P}
Verifying the correctness of arbitration group public key		$V_{PK_{AA}}$
Audit Injured Standard		AU_{IS}
Pharmacy		$PHAR$
Courthouse		CH

3.1 Registration Procedure for the Insured

Initially, the insured needs to apply for an anonymous authentication card from the insurance company to protect the privacy of the insured and, at the same time, store the private key and other relevant information of the insured in the authentication card. First of all, the insured needs to send the casualty insurance application details (Pci), and the insured's key certificate (CFC_{INS}) to the insurance company through a personal private key (SK_{INS}) using a secure channel. The application for registration (P_{INS}) of the parametric equation of the insured is shown in Eq. (1).

$$INS \to I : P_{INS} = \left\{ Pci, Sig_{SK_{INS}}(Pci), CFC_{INS} \right\} \quad \textbf{(1)}$$

After the insurance company receives the registration application (P_{INS}) from the insured, it uses the public key (PK_{INS}) of the insured in the key certificate (CFC_{INS}) to verify the accuracy of the signature ($Sig_{SK_I}(PK_{INS})$). If confirmed, the insurance company authorizes the public key for the handling business (APK_{SP}). If all procedures are correct, the insurance company will give the insured a coded serial number (CN_{INS}), which is the authentication card. Its function is to record relevant information about the insured; only the insurance company and the handling business can obtain the real name of the insured from the key or authentication card, and other people cannot obtain relevant personal information about the insured through the authentication card, which is composed of a coded serial number with anonymous protection characteristics. The recorded information of the insured is the proof of insurance premium paid by the insured for accidental injury insurance (Doc), which can be considered as proof of the right of the insured to have accidental injury insurance

coverage. The parametric equation with which the insurance company replied to the registration application from the insured is (2), and the parametric equation with which the insurance company authorizes the business is (3). In addition, the insurance company will combine the public key (PK_{INS}) of the insured and the private key (SK_I) of the insurance company to form the public key certificate ($PCFC_{INS}$) of the insured, which is stored in the authentication card and then passed to the insured. The authentication card, besides containing the public key certificate ($PCFC_{INS}$) of the insured, also contains the personal private key of the insured. The insured registration procedure is shown in Figure 4.

$$I \to INS : PCFC_{INS} = \{CN_{INS}, Doc, PK_{INS}, Sig_{SK_I}(PK_{INS})\} \quad \textbf{(2)}$$

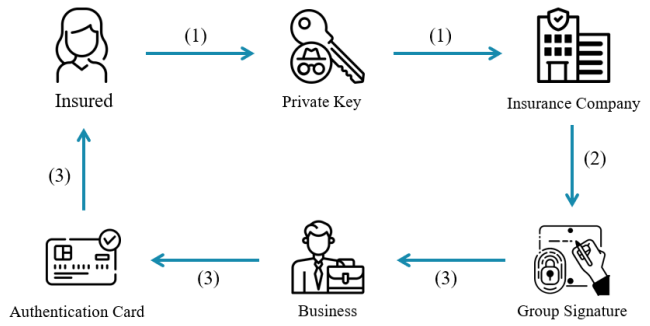

Figure 4. The registration procedure for the insured

Before the insurance company authorizes the business, it must first construct a group signature (S). This technology allows any authorized group member to sign group documents anonymously. After signing, any verifier can verify the group signature through the group public key (GPK). The system process for group signature includes six stages setting, joining, signing, verification, tracking, and revocation, which is the complete process of group signature.

In the setting stage, the secure prime number (p, n) will be used to calculate $n = p*q$, and then the group public key (GPK) and group signature private key (GSK) will be set. Then set the group signature private key as group signature private key (GSK) = group administrator private key (GSK_{GM}) + arbitrator server private key (GSK_{MS}), and then determine the group administrator public key (GPK_{GM}) and the arbitrator's server public key (GPK_{MS}) and make $GSK_{TM} * GPK_{TM} + GSK_{MS} * GPK_{MS} = 1$. After the above steps are completed, the hash function (H) is determined.

If the user (U) wants to become a signed member, he must upload the user identity information (ID_U) to the group manager (GM). After the group manager agrees to accept the user as a new member, the user identity-related information will be sent to the arbitrator server (MS) to generate the parameters. Then the arbitrator server will calculate the group manager public key (GPK_{MS}) and store the user identify information (ID_U) and the arbitrator server private key (GSK_{MS}) in the database.

When the user wants to generate a signature on the information (i), the user's identity-related information (ID_U) and other information must be transmitted to the arbiter server (MS) for verification, and the arbiter server will determine the user's signature information whether it meets the standard; if not, the signing request will be rejected. If it is qualified, it will determine a time random number (t) and calculate the hash function (H) of information (i) and time random number (t) and then send the calculated data to the user. After receiving it, the user will sign it using their individual signature secret key (SIG_U), then return it to the mediation server. The mediation server will first verify if it is a valid signature by checking if it meets the calculated hash data and if it has been personally signed by the user. If it is verified, it will be sent to the group manager (GM) and the user. When the group manager receives the valid signature from the mediation server, it will use the group manager secret key (GSK_{GM}) to calculate if it matches and return the result to the mediation server and the user. After receiving the responses from both, the mediation server will first calculate if they are the same as the original calculation. If they are the same, it means that both have used the correct group manager secret key (GSK_{GM}) and user secret key (GSK_U), and it will store the group manager secret key and user secret key in the database. If the calculation result is different from the original, the user's request will be rejected. After the user receives the final data from the mediation server, the time signature (t, S) of the information (i) is generated.

Next, to verify whether the user's groups signature (i, (t, S)) is a legal one, the signature verifier (Ver) first calculates $i^* = H(i, t)$ and then calculates whether $S^{GPK} = i^*$ is established, where GPK is the group public key.

If there is a dispute over the group signature (i, (t, S)), the identity of the original signer can be found out with the assistance of the group manager (GM) and the arbiter server (MS). The steps are: The group manager (GM) sends the group signature (i, (t, S)) to the moderator server (MS). After the arbiter server receives it, it searches for records in the database according to the information (i) and time random number (t) and then checks whether $i^* = H(I, t)$ is established. If it is established, the original signer's user identity-related information (ID_U) and the user's personal key (GSK_U) are sent back to the group manager.

When the group manager (GM) wants to delete the identity of the user's signing membership, the group manager (GM) must send the user identity-related information (ID_U) to the arbiter server (MS). After the arbiter server (MS) receives it, the process of revoking the signing member's qualification from the database is complete; i.e., the arbiter server will no longer accept any signature request from the user after cancellation. The above is the complete process of group signature.

$$\begin{aligned} &U \to MS : SIG_U = \{ID_U, i, t, E, H, GPK_{MS}, GSK_{MS}\} \\ &U \to MS : SIG_U = \{ID_U, i, t, E, H, GPK_{MS}, GSK_{MS}\} \\ &MS \to GM : S = \{GSK_{GM}, GSK_U, t, S\} \\ &Ver \to I = \{i^*, S^{GPK}, H\} \end{aligned} \quad \textbf{(3)}$$

3.2 Hospital Registration Procedure

To protect the privacy of the hospital, the hospital applies to the pharmacy for the medical group signature key and saves the drug quota in the medical records. Everyone can use the public key signed by the medical group (GPK_{HP})

to verify whether it is correct and whether the records are complete. However, to meet the conditions of anonymity and privacy protection, only the pharmacy can know the hospital's signature, and other people and units cannot know the owner's signature. The initial step is that the hospital signs the hospital's private key (SK_{HP}) with the hospital's identification card (ID_{HP}) and, at the same time, sends the hospital's key certificate (KC_{HP}) to the pharmacy in a secure manner and the group signature registration application (S_{HP}) that the hospital applies to the pharmacy is described in Eq. (4).

$$HP \rightarrow PHAR : S_{HP} = \left\{ ID_{HP}, Sig_{SK_{HP}}(ID_{HP}), KC_{HP} \right\} \quad (4)$$

The pharmacy uses the hospital public key (PK_{HP}) to verify the correctness of the signature. If it is correct, the group signature key equation (E_{TK}) is combined with the master key (MK) and the hospital's identification card (ID_{HP}) to form a medical group signature private key (GSK_{HP}) and stored in the hospital identification card. Finally, the parameter equation of pharmacy's response to the hospital's application for registration is listed in Eq. (5). The hospital registration process is shown in Figure 5.

$$HAR \rightarrow HP : E_{TK}(MK, ID_{HP}) = GSK_{HP} \quad (5)$$

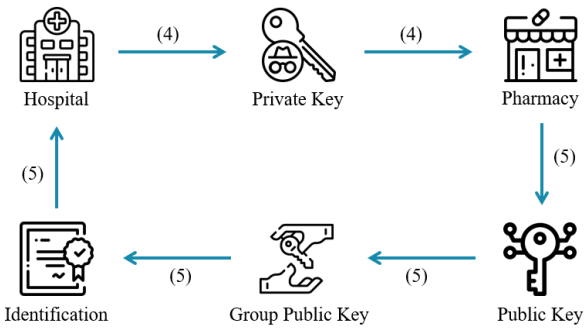

Figure 5. Hospital registration procedure

3.3 Police Registration Procedure

The police application registration process is similar to the hospital registration process. In order to maintain the privacy of the police, the police need to apply to a third-party organization for a police service card to sign the police group key and, at the same time, save the signature key in the service card. Anyone can perform signature verification through a list of police group public keys (GPK_P), but except for third-party organizations, no one else can learn the owner's real signature through the public key, which is in line with anonymity and security. First, the police use the service certificate (ID_{PS}) to sign the police private key (SK_P), and then transmit the police key certificate (KC_P) to a third-party organization in a secure manner. The parameter equation for police application registration (S_P) is given in Eq. (6).

$$P \rightarrow GP : S_P = \left\{ ID_{PS}, Sig_{SK_P}(ID_{PS}), KC_P \right\} \quad (6)$$

To verify the accuracy of the signature, the third-party organization uses the police public key (PK_P) as the identification method. If the identification result is correct, the group signature key equation (E_{TK}) will be combined with the master key (MK) and the service certificate of the police (ID_{PS}) to form the private key signed by the police group (GSK_P) and then deliver the service certificate storing the private key signed by the police group to the police. The parameter equation for the third-party organization to reply to the police application for registration is listed in Eq. (7). The police registration process is shown in Figure 6.

$$GP \rightarrow P : E_{TK} = (MK, ID_{PS}) = GSK_P \quad (7)$$

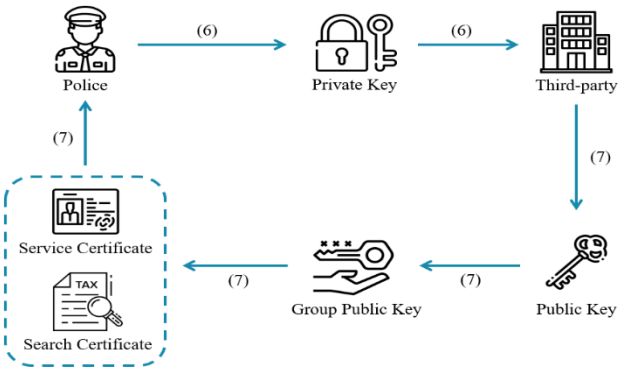

Figure 6. Police registration procedure

3.4 Arbitration Association Registration Procedure

The arbitration association transmits the arbitration case to the court and signs the key. Only the insured, the arbitration association, and the court can verify the record. As the third party cannot learn the detailed information and the signature of the owner, it has the characteristics of privacy protection. The initial step is to sign the private key of the Arbitration Association (SK_{AA}) through the arbitration case (ID_{AA}); then transmit the key certificate (KC_{AA}) of the Arbitration Association to the court in a secure manner. The procedure for Arbitration Association's registration application to the court for key signature is in Eq. (8).

$$AA \rightarrow CH : S_{AA} = \left\{ ID_{AA}, Sig_{SK_{AA}}(ID_{AA}), KC_{AA} \right\} \quad (8)$$

If it is necessary to determine whether the signature is correct, the court needs to use the public key of the Arbitration Association (PK_{AA}) to verify it. If it is correct, the master key (MK) will be combined with the arbitration case (ID_{AA}) to form a judgment (PC_{AA}). Its legal content includes arbitration cases and judgments, which are finally sent back to the Arbitration Association for the record. The parametric equation of the court's response to the registration application filed by the Arbitration Association is provided in Eq. (9). The registration process of the Arbitration Association is shown in Figure 7.

$$CH \rightarrow AA : E_{GK} = (MK, ID_{AA}) = PC_{AA} \quad (9)$$

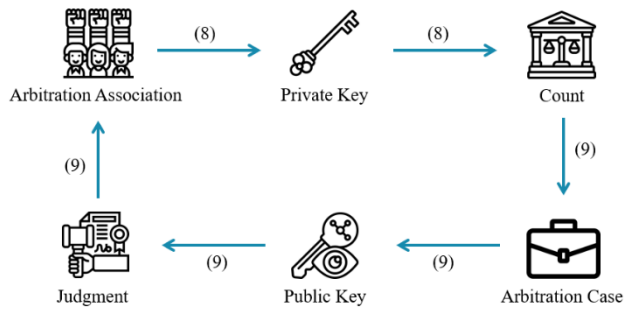

Figure 7. Arbitration association registration procedure

3.5 Claims Procedure

When an accident against casualty insurance occurs, the insured will receive the case certificate, the diagnosis certificate from the hospital, and the arbitration report after reporting the case. These records will be stored in third-party agencies, pharmacies, and courts to be used as verification data for insurance claim review and settlement in the future. When the insured applies to the insurance company for compensation for casualty insurance, the certificate of diagnosis (PC_D), diagnostic cost data (FD_D), and drug prescription (GP_{HP}) will be combined through the signature of the medical body (GSK_{HP}). Through the police body, the case certificate (PC_C) is signed by the signature private key (TSK_P), while the judgment (PC_{AA}) is combined with the Arbitration Association private key (SK_{AA}). Then, encrypt (E) all the data, including the public key certificate of the insured ($PCFC_{INS}$) and the public key of the insurance company (PK_I), and send it to the insurance company after the procedure is complete. The parametric equations for the insured to apply for claims are listed in Eqs. (10), (11), and (12).

$$HP \to I : E_{PK_I} = (PC_D, FD_D, GP_{HP}, Sig_{GSK_{HP}}(PC_D, FD_D, TP_{HP}), PCFC_{INS}) \quad (10)$$

$$P \to I : E_{PK_I} = (PC_C, Sig_{GSK_P}(PC_C), PCFC_{INS}) \quad (11)$$

$$AA \to I : E_{PK_I} = (PC_{AA}, Sig_{SK_{AA}}(PC_{AA}), PCFC_{INS}) \quad (12)$$

When the insurance company receives the claims application materials, it will first decrypt (HP) the diagnosis certificate sent by the hospital, the case certificate sent by the police, and the judgment of the arbitration association and then obtain the group signature of the private key of the doctor and the police and the private key of the arbitration association. According to the public key signed by the medical group (GPK_{HP}), the public key signed by the police group (GPK_P), and the public key of the arbitration association (SK_{AA}), the insurance company then verifies (V) whether the group signatures are correct. After the inspection, this record will be kept in the insurance institution for insurance dispute prevention and data storage. The parametric equations for the insurance company to respond to the insured's claim application are given in Eqs. (13), (14), and (15).

$$I \leftrightarrow HP : D_{SK_I} = \left(E_{PK_I}\left(Sig_{GSK_{HP}}(PC_D, FD_D, GP_{HP})\right)\right),$$
$$V_{GPK_{HP}}\left(Sig_{GSK_{HP}}(PC_D, FD_D, GP_{HP})\right) \stackrel{?}{=} PC_D, FD_D, GP_{HP} \quad (13)$$

$$I \leftrightarrow P : D_{SK_I} = \left(E_{PK_I}\left(Sig_{TSK_P}(PC_C)\right)\right), V_{TPK_P}\left(Sig_{TSK_P}(PC_C)\right) \stackrel{?}{=} PC_C \quad (14)$$

$$I \leftrightarrow AA : D_{SK_I} = \left(E_{PK_I}\left(Sig_{SK_{AA}}(PC_{AA})\right)\right), V_{PK_{AA}}\left(Sig_{SK_{AA}}(PC_{AA})\right) \stackrel{?}{=} PC_{AA} \quad (15)$$

After the insurance company confirms that each signature is correct and complete, it will execute the claim amount audit procedure (AU_{IS}) according to the trauma condition recorded in the medical diagnosis certificate and remit the claim amount to the insured's bank account after confirming that the claim amount is correct to complete the application procedure, while updating the insured's authentication card information as a basis for future traceability. The parametric equation of the claim payment procedure is listed in Eq. (16). The claim process is shown in Figure 8.

$$E - Pay, Sig_{SK_I}(AU_{IS}, E - Pay) \quad (16)$$

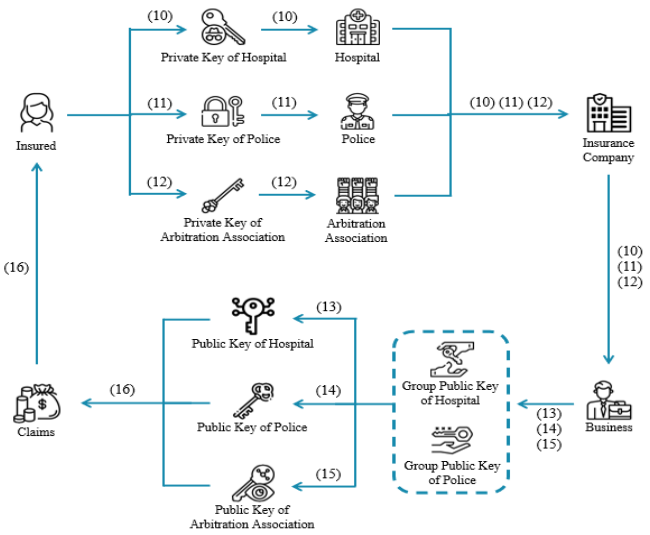

Figure 8. Claim process of the insured

4 Comparison of Traditional Casualty Insurance Claim vs. Using Smart Contract

This section compares the existing disadvantages of traditional claims procedure cited in extant literature with the improvements in claims procedure through smart contracts:

(1) Muromskaya, A. A. (2021). [21] The Probability of Ruin of a Joint-Stock Insurance Company in the Sparre Andersen Risk Model. Muromskaya (2021) believes that the claims review standards vary due to the different judgment methods of insurance companies. For example, each insurance company has different standards for measuring the degree of trauma, and there is a gap in the amount of benefit, which affects the amount of money paid. Therefore, setting

a set of evaluation standards through smart contracts can not only improve the impact of differences in the evaluation of various insurance companies but also protect the rights of the insured and improve customer satisfaction.

(2) Shuang, W., Yi, L. (2021). [22] Impact of the Business Structure on Solvency of Property-Liability Insurance Companies and Its Mediating Effect. Shuang (2021) mentioned that the details of claims are closely related to the success of the application. Human error or process errors will lead to failure. This problem can be improved by using smart contracts to perform audits. The smart contract includes parameter setting and system automation review, which can avoid the above-mentioned mistakes and reduce human error rate.

(3) Grebeniuk, N. V., Riznyk, N., Zhurylo V. V., Tymoshyk, N. S., Dobizha N. V. (2021). [23] Interaction of banks and insurance companies in the context of the sale of insurance products. Grebeniuk (2021) mentioned that any operational process of an insurance company interacts with other departments, which means that each operational process cannot exist independently. The division of labor in the insurance process is transmitted from department A to department B, and from department B to department C… etc. It is evident that time-consuming is a problem in the transmission process. Once there is an error midway, it will take additional time and manpower to trace the source of the error, which leads to low work efficiency and delay in the review time. Therefore, adding smart contracts to the review process can reduce time and labor costs and maximize review efficiency, thereby speeding up the payment of claims to protect the insured's rights.

(4) In the overall standardization of claims settlement operations, such as data access and modification, and personnel deployment must keep detailed records. Smart contracts have the characteristics of the blockchain, such as openness and transparency, non-repudiation, inability to tamper with, etc. In the claim process, not only can the information of each transaction be recorded, but it also ensures that the data has not been tampered with and is stored properly, which is conducive to the use of retrospective data in the future.

The comparison between the smart contract claims procedure and the traditional claims procedure is shown in Table 3.

Table 3. Comparison between smart contract claims procedure and the traditional claim procedures

	Smart contract claims procedure	Traditional claims procedure
Review efficiency	better	poor
Human review error rate	low	high
Openness and transparency	high	low
Payment speed	fast	slow
Customer satisfaction	high	low
Degree of data preservation	better	poor

5 Conclusions

This study is based on the research of applying smart contracts in the casualty insurance claim process, combining the characteristics of smart contracts and blockchain. When the insurance company conducts the audit of accidental injury insurance claims, it can shorten the time and personnel costs of the claims audit and reduce the human error rate, thereby improving the audit efficiency and the speed of claim payment; so that the insured can get the due claims as soon as possible compensating for personal losses incurred when risks occur which in turn can also increase customer satisfaction.

The smart contract described in this study is applied to the automation of casualty insurance. If it can be officially implemented in the future, through the maturity of the system technology and the participation of insurance companies, the expected benefits will be as follows:

(1) Combining e-policies with smart contracts can speed up claims settlement and maximize benefits for customers. The lengthy process in the past, such as contract signing, reviewing medical records, claims settlement, etc., can all be completed on the platform, and at the same time it increases people's willingness to take out the insurance.

(2) The signing of the contract is carried out in the form of a smart contract, not a traditional paper contract. Smart contracts allow transactions without a third party. At the same time, these transactions are traceable but irreversible, so they have the characteristics of decentralization and non-tampering. As a result, there will be no tempering of contract content or loss of data so that the insured can sign the insurance contract with peace of min.

(3) The blockchain records every transaction. If the insured suffered physical injury due to an accident, he can automatically complete the claim settlement process through smart contracts, reduce other transaction costs related to the contract, and quickly make up for irreversible losses. In addition, based on the openness of transparency of the smart contract, the insured can track the progress of claims payment at any time through the smart contract.

(4) Combining distributed ledgers with casualty insurance can not only improve audit efficiency but also reduce time costs and error rates, etc., so that the insured can get compensation in a short time when an accident occurs, thereby improving customer trust. If smart contracts can be practically applied to the insurance industry's claims process, insurance companies and their customers will benefit. At the same time, insurance companies can combine financial technology to avoid being eliminated by the rapidly changing market competition.

Research Contribution:

(1) This study is of great significance to the trend of insurance technology innovation as it uses smart contracts for claims processing.
(2) Through cryptography and blockchain characteristics, this study can ensure the security and privacy of claims data transmission.

Research Limitations:

(1) This study did not collect relevant claims data to explore the feasibility of the proposed claims automation method.
(2) This study did not include other insurance types or variables for discussion, and the research results may be biased.

Research Suggestions:

(1) It is recommended to include other insurance variables for discussion to improve the claims automation framework.
(2) It is recommended to conduct a thorough analysis of the security level of the claims automation framework proposed in this study.

References

[1] K. R. Petroni, Optimistic reporting in the property-casualty insurance industry, *Journal of Accounting and Economics*, Vol. 15, No. 4, pp. 485-508, December, 1992.

[2] K. Epermanis, S. E. Harrington, Market discipline in property/casualty insurance: Evidence from premium growth surrounding changes in financial strength ratings, *Journal of Money, Credit and Banking*, Vol. 38, No. 6, pp. 1515-1544, September, 2006.

[3] D. Fu, S. Hu, L. Zhang, S. He, J. Qiu, An intelligent cloud computing of trunk logistics alliance based on blockchain and big data, *Journal of Supercomputing*, Vol. 77. No. 12, pp. 13863-13878, December, 2021.

[4] J. Xu, W. Zhou, S. Zhang, J. Fu, A review of the technology and application of deposit and *traceability* based on blockchain, *Journal of High Speed* Networks, Vol. 27, No. 4, pp. 335-359, November, 2021.

[5] Z. Zheng, S. Xie, 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.

[6] J. Zhang, L. Guo, T. Lyu, An enhanced personal credit identification coin-day destruction model based on blockchain technology fuzzy sets for *region* of China pearl river delta, *Journal of Intelligent and Fuzzy Systems*, Vol. 41, No. 3, pp. 4519-4525, January, 2021.

[7] Z. Yang, X. Zheng, Sports training big data *integration* and optimization based on block-chain technology, *Journal of Intelligent and Fuzzy Systems*, pp. 1-7, June, 2021.

[8] A. Buldas, D. Firsov, R. Laanoja, H. Lakk, A. Truu, A new approach to constructing digital signature schemes, *Advances in Information and Computer Security*, Tokyo, Japan, 2019, pp. 363-373.

[9] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, G. Wang, Digital signature scheme for *information* non-repudiation in blockchain: a state of the art review, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2020, No. 1, pp. 1-15, March, 2020.

[10] M.-S. Hwang, S.-M. Chen, C.-Y. Liu, Digital signature with message recovery based on factoring and discrete logarithm, *IETE Journal of Research*, Vol. 62, No. 3, pp. 415-423, 2016.

[11] N. P. Sheppard, Can smart contracts learn from digital rights management, *IEEE Technology & Society Magazine*, Vol. 39, No. 1, pp. 69-75, March, 2020.

[12] D. Perez, B. Livshits, Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited, *30th USENIX Security Symposium*, Vancouver, B.C., Canada, 2021, pp. 1325-1342.

[13] K. Wrona, F. M. Scharf, M. Jarosz, Security accreditation and software approval with smart contracts, *IEEE Communications Magazine*, Vol. 59, No. 2, pp. 56-62, February, 2021.

[14] T. Dickerson, P. Gazzillo, M. Herlihy, E. Koskinen, Adding concurrency to smart contracts, *Distributed Computing*, Vol. 33, No. 3-4, pp. 209-225, June, 2020.

[15] M. D. Turjo, M. M. Khan, M. Kaur, A. Zaguia, Smart supply chain management using the blockchain and smart contract, *Scientific Programming*, Vol. 2021, pp. 1-12, 2021.

[16] D. Li, R. Hu, Z. Lin, Vocational education platform based on block chain and IoT technology, *Computational Intelligence and Neuroscience*, Vol. 2022, pp. 1-10, 2022.

[17] H. Xiong, T. Dalhaus, P. Wang, J. Huang, Blockchain Technology for Agriculture: Applications and Rationale, *Frontiers in Blockchain*, Vol. 3, pp. 1-7, February, 2020.

[18] F. Serpush, M. B. Menhaj, B. Masoumi, B. Karasfi, Wearable sensor-based human activity *recognition* in the smart healthcare System, *Computational Intelligence and Neuroscience*, Vol. 2022, pp. 1-31, February, 2022.

[19] H. Mhamdi, B. O. Soufiene, A. Zouinkhi, O. Ali, H. Sakli, Trust-based smart contract for automated agent to agent communication, *Computational Intelligence and Neuroscience*, Vol. 2022, pp. 1-11, 2022.

[20] J. J. Goo, J. Y. Heo, The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation, *Journal of Open Innovation: Technology, Market, and Complexity*, Vol. 6, No. 2, pp. 1-18, June, 2020.

[21] A. A. Muromskaya, On the Probability of Ruin of a Joint-Stock Insurance Company in the Sparre Andersen Risk Model, *Journal of Mathematical Sciences*, Vol. 254, No. 4, pp. 574-581, April, 2021.

[22] S. Wu, Y. Li, Impact of the Business Structure on Solvency of Property-Liability Insurance Companies and Its Mediating Effect, *Discrete Dynamics in Nature and Society*, Vol. 2021, No. 1, pp. 1-17, 2021.

[23] N. V. Grebeniuk, N. Riznyk, V. V. Zhurylo, N. S. Tymoshyk, N. V. Dobizha, Interaction of Banks and Insurance Companies in the Context of the Sale of

Insurance Products, *Journal of the Balkan Tribological Association*, Vol. 27, No. 4, pp. 697-710, 2021.

Biographies

Shun-Yuan Ho is currently a doctoral candidate in the Information Management Department of Chaoyang University of Science and Technology. His research interests include enterprise resource planning, information security, technology acceptance model, and supply chain.

Tsung-Che Wu received Finance Ph.D. in Mississippi State University. Currently he is an assistant professor in National ChiaYi University and Chairman of Cameo Communications Inc. With research interest includes corporate governance, financial markets, and ESG, he has published articles in journals such as Sustainability and Emerging Markets Finance and Trade.

Bo-Yu Chen is currently a master's student in the Department of Banking and Finance at National Chiayi University. His research interests include Insurance, Information Security and Financial Technology.

Tzer-Long Chen received his Ph.D. Degrees from the Department of Information Management, National Taiwan University, Taiwan. Currently he is an assistant professor in Kaohsiung Medical University, Taiwan. His research interests are in Information Security, Internet of Things, and Blockchain.

Hsiu-Chia Ko holds a PhD degree from National Sun-Yat-Sen University, Taiwan. She is currently an Associate Professor of Information Management at the Chaoyang University of Technology, Taiwan. Her research interests include social commerce, on-line communities, knowledge management, and electronic commerce.