A Study on Strengthening the Security of Grievance System Based on Smart Contract

Pin-Chang Su and Wan-Ling Huang*

Department of Information Management, Management College, National Defense University

ABSTRACT

In accordance with the goal of promoting digital transformation in advanced countries, we will continue to use forward-looking information technology and strive to build a smart government, which can provide secure and reliable digital services. However, the current grievance system lacks trust due to the lack of transparency in the process, concerns about the leakage of private information, and the protection measures for complainants in the complaint channel. However, the current grievance system lacks trust due to the lack of transparency in the process, concerns about leakage of private information, and the protection measures for complainants in the grievance channel, which in turn affects the sense of belonging between the organization and its members. This study uses smart contracts to automatically execute the terms of contract protocols, and constructs a self-authentication and blind signature mechanism based on elliptic cryptography. This mechanism can enhance the security of identity authentication, achieve intelligent and decentralized supervision and governance with emerging technologies in democratic countries, and enhance the trust of the existing grievance mechanism.

Keywords: Smart contract, grievance system, self-certification, blind signature

基於智慧合約強化申訴系統安全性之研究

蘇品長　黃琬玲*

國防大學管理學院資訊管理學系

摘　　要

配合先進國家推動數位轉型目標，持續運用前瞻資訊技術，致力於建構智慧化政府，提供安全可信任之數位服務，然而現行申訴系統由於過程不透明、隱私資料外洩疑慮及申訴管道中對於申訴者的保護措施等問題，導致系統缺乏信任，進而影響組織與成員之間歸屬感，本研究導入智慧合約自動執行合約協議條款，並建構以橢圓曲線密碼學為基礎之自我認證及盲簽章機制，提升身分認證安全性，運用新興科技達成民主國家智慧化、去中心化的監管和治理，並增強現行申訴機制之信任度。

關鍵詞：智慧合約，申訴系統，自我認證，盲簽章

文稿收件日期 112.1.6; 文稿修正後接受日期 112.5.18;*通訊作者
Manuscript received Jan 6, 2023; revised May 18, 2023; *Corresponding author

I. INTRODUCTION

With the emergence of the global financial tsunami in 2008, the role of third-party intermediaries in the financial industry has been doubted, unable to achieve trust in each other's transactions. In recent years, blockchain technology has been developing and evolving to overcome the problems of trust, privacy and information asymmetry, and has gradually developed into an independent research technology field. Smart contract can automate the computer program that performs the terms of the contract, building a decentralized system architecture. Social decentralization of supervision and governance to achieve the vision of smart city, smart governance and smart life [1-3].

In 2018, a student at Beijing University complained about the investigation of a professor's sexual assault case, however, the university refused and conceal the case. Therefore, netizens use blockchain technology to store the content of the complaint and publish the incident on the blockchain [4]. Through "decentralized ledger technology", grievance messages can be stored forever and cannot be deleted by anyone. In addition, the "nonrepudiation", "immutability" and "anonymity" characteristics of blockchain make it impossible to maliciously tamper with the content of grievance, and protect the real identity of the publisher, so as to achieve the electronic record of evidence [5]. However, the grievance filing procedure of existing grievance channels often fails to meet the requirements of openness and transparency. When filing grievances by paperwork, citizens are generally prone to deliberate obstacles, case dismissal, and case concealment. As for voice service hotlines, operators must manually judge, categorise, and deal with the cases, which may easily lead to untimeliness. Alternatively, online complaints may result in the leakage of private information, tampering of complaint data and file retention problems, causing applicants to lack trust in the grievance channel. A study on preventive measures and reporting systems of workplace bullying in Taiwan shows that victims do not trust grievance channels [6]. Multiple reasons exist for this phenomenon. One reason is that victims doubt about the protective measures for applicants in grievance channels. They doubt whether the grievances will affect their job and whether their privacy will be disclosed after grievances. A study on the effective factors influencing citizens' intention to use the complaint handling system in Mataram, Indonesia, shows that complaints can be completed quickly through the system, which helps save time and costs; among those effective factors, trust is a key factor affecting citizens' adoption of the complaint handling system [7]. Therefore, it is a topic worth studying how to establish a trustworthy complaint system to promote the trust between applicants and organisations.

This study plans to design a blockchain-based smart contract that combines an interplanetary file system with elliptic self-certification and blind signature technology to design a secure grievance mechanism with the following advantages.

- Programmatic mechanism protocols to be deployed on blockchain using smart contract. To allow the grievance file to be stored permanently and cannot be arbitrarily deleted or maliciously tampered with, and to achieve electronic records.
- Cryptography and blind signature mechanism using elliptic inverse elements and special point addition features to protect the privacy of grievances and file validity. Only a small key length is required under the same security as RSA, which can reduce the system load and enhanced the efficiency of the online grievance system.
- The self-certification method is used for identity verification to avoid the risk of forging user identities by the certificate authority centre during the creation and issuance of electronic certificates. It can also reduce the cost of storing, calculating, and managing the public keys in the authentication system.

II. RELATED WORKS

This chapter categorizes and analyzes the literature related to this study, and focuses on smart contract, cryptographic technology and recent research on grievance system, and compiles them as the basis of this study.

2.1 Smart Contract

The concept of a smart contract was first introduced in 1994 by Nick Szabo, and is defined as "a set of promises defined in digital form, including agreements on which contract participants can execute these promises." [8] Program protocols and write decentralized applications through smart contract, deploy them on the blockchain, and build a decentralized application platform that requires no trusted foundation. In a smart contract, the relevant agreements are programmed and executed by a computer, giving it higher security than the traditional contract method [9]. The current open source applications of blockchain such as ethereum which smart contract is written in four programming languages: Solidity, Mutan, LLL and Serpent. Compile and generate bytecode (binary code) and JSON format application binary interface (Application Binary Interface, ABI). Users can change the contract status by calling and using the functions provided by the smart contract through the contract address and the associated ABI.

2.2 Cryptography

Cryptography is an important security mechanism to ensure the security and correctness of messages. This section introduces the self-authentication mechanism and Blind Signature employed in this study.

2.2.1 Self certification

Girault proposed the RSA-based self-certified public key cryptosystem in 1991 [10]. In the registration stage, the user participates in the public key calculation by the CA. In the verification stage, the participant can complete identity verification by itself. The algorithm of each stage is as follows.

- Initial stage：The CA generates public and private key with the RSA method. First, choose two large prime numbers p and q, and calculate $n = p \cdot q$. Next, calculate the public key $e \cdot gcd(e,\ \emptyset(n)) = 1$. Next, calculate the private key d, $ed = 1\ mod\ \emptyset(n)$. And g is the integer of the largest order in the group of multiplications Z_n^*. Finally, expose e and n, and preserve d.
- Registration Stage：For example, the user M is identified by ID_M. M select their own private key S_M, and calculate $V_M = g^{-S_M}(mod\ n)$ .Then transfer ID_M and V_M to the CA, and calculate the public key $P_M = (V_M - ID_M)^d\ (mod$ n) of M, and send P_A back to M. M verify ${P_M}^e + ID_M \stackrel{?}{=} V_M$, if it is true then P_M is the public key of M, and S_M is the private key.
- Verification Stage：When the user M and R communicate with each other after registering their identities, M transfers its ID_M and P_M to R, and the user R calculates $V_M = {P_M}^e + ID_M\ (mod$ n). M chooses a random parameter value x, and calculates $t = g^x\ (mod\ n)$, then transfer t to R.；R selects a random parameter value C and transfers it to M. M calculates$Y = x + S_M \cdot C\ (mod\ n)$, and transfers Y to R, Finally R is verified using the equation${g^Y \cdot {V_M}^C \stackrel{?}{=} t\ (mod\ n)}$, and if the equation validates then the M identity can be prove. In the same way M can verify the identity of R in this way.

2.2.2 Blind signature

Chaum proposed a blind signature based on RSA in 1983 [11]. Let the signatory complete the message signature without knowing the contents of the signature. The verifier can verify the correctness of the signature through the signer's public key and protect the privacy of the signature requestor. The algorithm of each stage is as follows.

- Initial stage：The signer randomly selects 2 large prime numbers p and q and calculates $n = p \cdot q$ and $\emptyset(n) = (p - 1)(q - 1)$. Select two very large numbers e and d, and calculate $ed \equiv 1\ (mod$ c) and $\gcd(e, \emptyset(n)) = 1$ where $1 < e < \emptyset(n)$. d as the private key, and e and n as the public key of the signatory.
- Blinding Stage：The signature requester randomly selects a random number r as the blind factor. Blinding the message m to $m' = r^e \cdot m\ (mod\ n)$, and transfer the m' to the signatory, and when the

signatory receives the m', he does not know what its content is.

- Signature Stage：After the signatory receives the message m', the private key d is used to calculate $s' = m'^{d} \ (mod \ n)$. Then send the signed blind message back to the signature requestor.
- Unblinding stage：After the signature requester receives s', and calculate $s = s' \cdot r^{-1} \ (mod \ n)$ for unblinding, and s is the signature of the signatory to the message m.
- Verification Stage：The verifier can use the signer's public key e to calculate whether $s^{e} \equiv m \ (mod \ n)$ is valid and verify the correctness of the signature.

2.3 Grievance System Related Research

In order to overcome the difficulties and challenges faced by the grievance system, this study collects the relevant researches proposed by scholars in recent years to integrate smart contracts through blockchain.

2.3.1 Blockchain-based grievance system for police agencies

In 2020, Hingorani et al. proposed a Blockchain-based grievance system for police agencies. The system is conceived to operate on a public chain developed by Ethereum, using the decentralized system of blockchain, decentralized ledger technology and immutable, data integrity characteristics to save all types of criminal records, to avoid the tampering and loss of evidence data [12]. The system protocol is shown in Fig. 1.

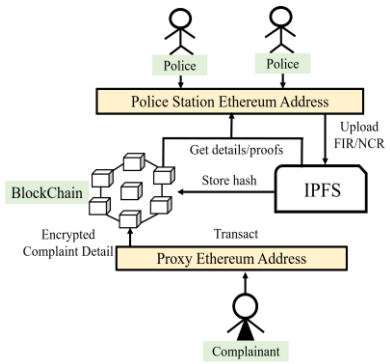

Fig.1. The grievance system protocol proposed by Hingorani et al[12]

2.3.2 Blockchain-based grievance management system for students

In 2021, Shettigar et al. proposed a blockchain-based student grievance management system. The system is conceived to operate on a Consortium Chain developed by Hyperledger Fabric Composer. Using the verifiable, decentralized and immutable characteristics of blockchain data to solve the cost of single point of failure and backup of centralized server databases, and to eliminate the opportunity for abuse of power by school authorities. If students are not satisfied with the solution, they can exercise their rights and file a grievance again [13]. The system protocol is shown in Fig. 2.

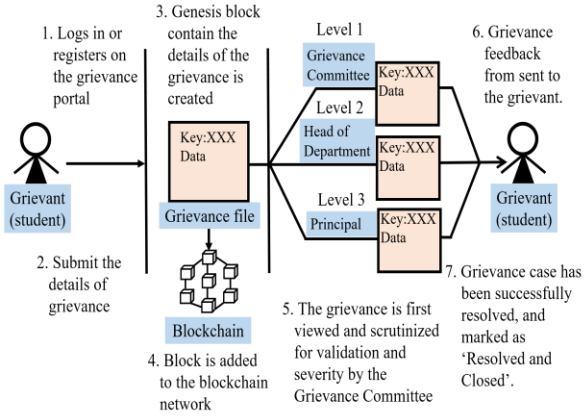

Fig.2. The grievance system protocol proposed by Shettigar et al[13]

2.3.3 Blockchain-based grievance management system for national and social welfare

In 2021, Rahman et al. proposed a blockchain-based national and social welfare grievance management system. ，The system architecture uses Hyperledger Aries and Hyperledger Indy to create a platform for national and social welfare complaints. Using the transparency, and decentralisation features of blockchain to solves the traditional problems of complex, opaque, and untrustworthy complaint procedures. The platform uses the Interplanetary File System to store and share files to avoid tampering [14]. Its system protocol is shown in Fig. 3.

III. MECHANISM PROTOCOL DESIGN

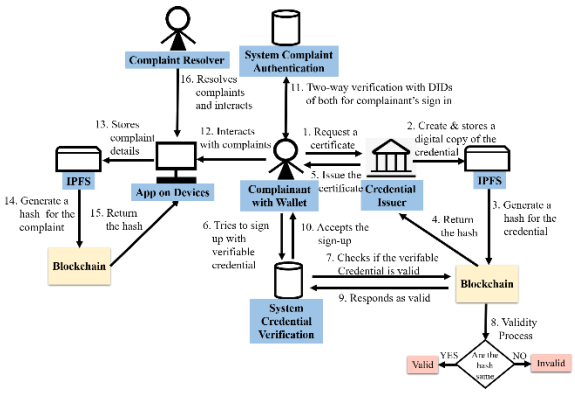

Fig.3. The grievance system protocol proposed by Rahman et al[14]

3.1 System Architecture

The conceptual diagram of the designed protocol and flowchart proposed in this study are illustrated in Fig. 4 and Fig. 5. Participants include the person filing the grievance, the grievance center responsible for receiving and distributing the grievance, and the unit responsible for investigating the grievance. First, the service developer designs a smart contract to be deployed on the blockchain. Each participant completes identity registration with the CA and confirms its identity through the self-certification mechanism before transaction to ensure that it is a legal user. The complainant then sends the grievance case to the grievance center through blind signature and encryption technology, and uploads it to the blockchain to ensure the confidentiality and privacy of the information. After receiving the case, the investigating unit verifies the validity of the signature and unblinded grievance case to implement the investigation. Finally, the investigation unit completes the complaint closure in the same way and uploads it to the blockchain. The complainant downloads the grievance closure case through the smart contract for verification and decryption.

3.2 System Algorithm

The core technology of this research system design first is to use the self-authentication method of elliptic cryptographic system for identity registration and authentication. Second, the complainant applies for a complaint case through a blind signature and encryption mechanism. This chapter describes the process of transmission and the algorithm respectively, and the system parameters are described in Table 1.

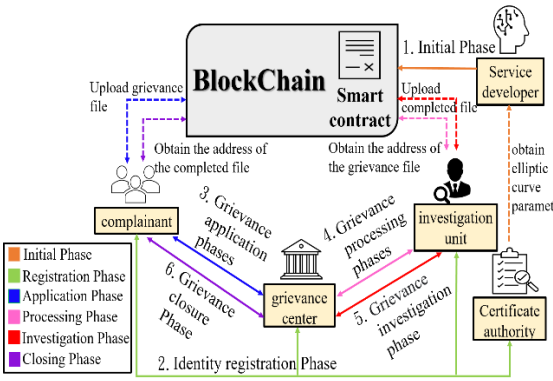

Fig.4. Conceptual diagram of the protocol

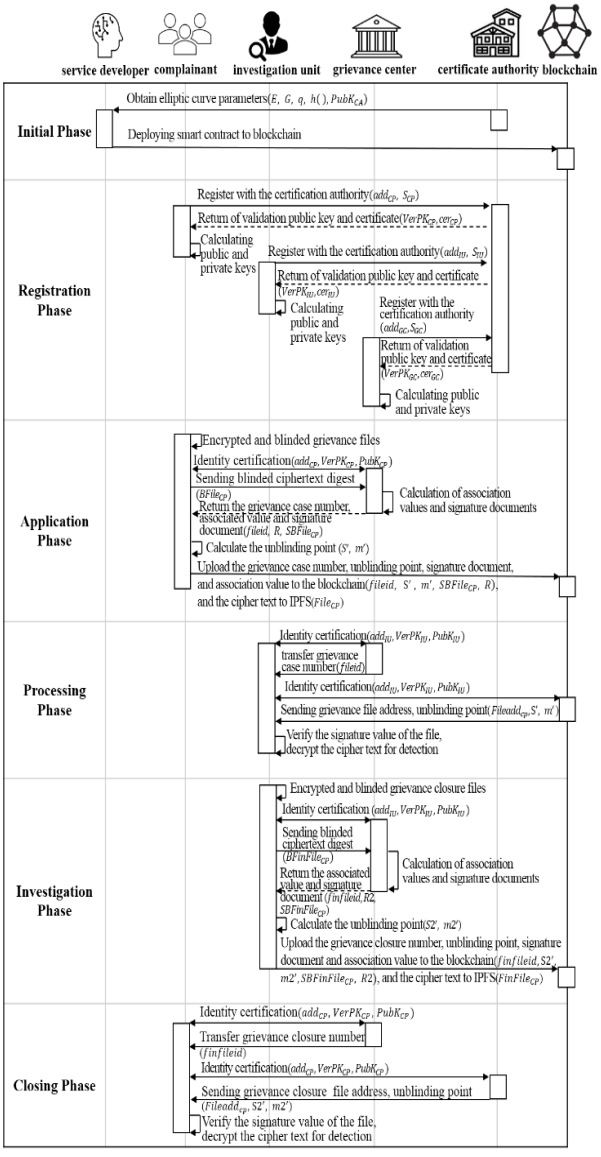

Fig.5. The flow chart of our proposed system

Table 1. Description table of symbols

No	Symbol	Description
1	SD, CA, CP, GC, IU	service developer, certificate authority, complainant, grievance center, investigating unit
2	SC	Smart contract designed by service developer.
3	S_i	The signature file of the participant, i∈$\{CP, GC, IU\}$
4	add_i	The address of the participant, i∈$\{CP, GC, IU\}$
5	$PubK_i, prik_i$	The public keys and private key of the participant, i∈$\{CA, CP, GC, IU\}$
6	$VerPK_i$	The public key for participant verification, i∈$\{CP, GC, IU\}$
7	cer_i	Certification signature of the participant, i∈$\{CP, GC, IU\}$
8	$fileid$	Grievance case number
9	m	Digest of encrypted grievance messages
10	R	The association value is calculated by the grievance center according to the signed blind grievance case.
11	S', m'	The unblinding point of the complaint application is calculated by the complainant according to the associated value and the signature document.
12	$File_{cp}$	The grievance file encrypted by the complainant.
13	$BFile_{cp}$	Digest of the grievance ciphertext blinded by the complainant.
14	$SBFile_{CP}$	A file of blinded grievance information signed by the grievance center.
15	$Fileadd_{cp}$	The IPFS system returns the address of the grievance file
16	d_i	The secret parameter values of the participant, i∈ $\{CP, GC, IU\}$
17	t, bf	The secret parameters value of the complainant.
18	r_{GC}, k_{GC}	The secret parameters value of the grievance center.
19	r, gf	The secret parameter value of the investigation unit.

3.2.1 Initial phase

A secure elliptic cryptographic system should follow international standards, such as ISO 1177-3, ANSI X9.62, IEEE P1363, FIPS 186-2, etc. Certificate Authority (CA) selects a security ellipse curve $E(F_q)$ on finite field F_q. $E(F_q): y^2 = x^3 + ax + b$ and $4a^3 + 27b^2 \neq 0$ Choose a base point G with order n on $E(F_q)$, such that $n \cdot G = O.O$ is the infinity point of this ellipse curve, Then CA chooses a one-way, collisionless hash function $h()$, and calculate its public key. Finally, publish the parameters $E, G, q, h(), \ and \ PubK_{CA}$.

$$PubK_{CA} = prik_{CA} \cdot G \tag{1}$$

Example:CA select the Secp256k1 ellipse curve parameter value. The service developer deployed the designed smart contract on the Ganache test chain with his metamask wallet address “0x3736B620d4D8B81e258D550Fabd94BFb3f6D7298” through the browser extension MetaMask and received the contract address 0xCFa3Fbce802a99e99588580fC190713343ed8C71”. The parameters are shown in Table 2, the process of smart contract deployment is shown in Figure 6, and the record of contract deployment is shown in Figure 7.

Table 2. Description table of the parameters of the initial phase

Type	Parameters
E	$y^2 = x^3 + 7$
G	55066263022277343669578718895168534326250603453777594175500187360389116729240,32670510020758816978083085130507043184471273380659243275938904335757337482424
q	11579208923731619542357098500868790785326998466564056403945758400790883467166 3
$h()$	SHA-3
$PubK_{CA}$	13792973388884037743091314079033130149476045026226023504209066894062002766801,5955640910787099522438595119385713023364817756396330262037850157918946165845 9

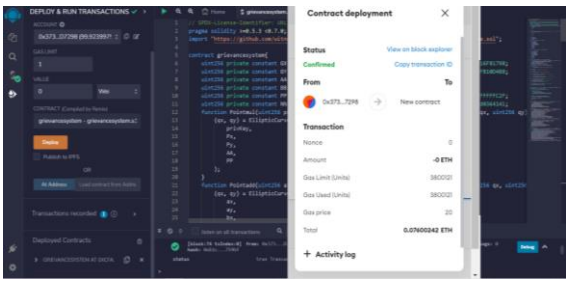

Fig.6. The process of smart contract deployment

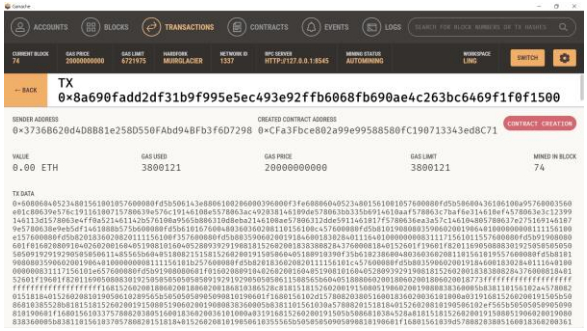

Fig.7. The record of contract deployment

3.2.2 Identity registration phase

The participant (take the complainant CP as an example) chooses a random secret parameter value $d_{CP} \in [2, n-2]$. Generate signature file S_{CP} by calculating identity address add_{CP} and secret parameter value d_{CP} on the block chain and deliver S_{CP} and add_{CP} to CA for registration. The calculation steps are as follows:

$$S_{CP} = h(d_{CP} \parallel add_{CP}) \cdot G \tag{2}$$

Table 3. Description of the parameters of the first stage of identity registration

Type	Parameters
add_{CP}	0x394e356AFcdC0f43aD60501524F89 80a983d5F40
d_{CP}	13322245678953221112345 67
S_{CP}	90578744662287318359762450173732 66392564336429581275282069036725 802867005260,10655837899047040547 81605017753293271714316028956281 79617733604224308219058664

After CA receives the complainant CP application registration information, CA randomly selects a secret parameter $k_{CP} \in [2, n-2]$ and calculates the complainant's verification public key $VerPK_{CP}$ and signature value cer_{CP} together with the application registration information. After completing the calculation, the CA will return the verification public key $VerPK_{CP}$ and signature value cer_{CP} to the complainant CP, and the calculation is as follows:

$$VerPK_{CP} = S_{CP} + \left(k_{CP} - h(add_{CP})\right) \cdot G$$

$$= (q_{CPx}, q_{CPy}) \tag{3}$$

$$cer_{CP} = k_{CP} + prik_{CA}(q_{CPx} + h(add_{CP})) \tag{4}$$

Table 4. Description of the parameters of the second stage of identity registration

Type	Parameters
k_{CP}	73732663925643364295812752820690367258028670055562 60
$VerPK_{CP}$	41954928986989083531380503529009400582079960769593241027565033333764797508356,1145784701268988946522814090628675234287737350196023589655972220097241544695649602358965597222009724154469564
cer_{CP}	83440481651591938623985816144406537082631484721429080829719088246275721221889

The complainant CP receives the verification public key $VerPK_{CP}$ and signature value cer_{CP} from CA and calculates the public and private key ($PubK_{CP}$, $prik_{CP}$) by itself, and the calculation is as follows:

$$prik_{CP} = cer_{CP} + h(d_{CP} \parallel add_{CP}) \tag{5}$$

$$PubK_{CP} = prik_{CP} \cdot G \tag{6}$$

Table 5. Description of the parameters of the third stage of identity registration

Type	Parameters
$prik_{CP}$	11485126005298576759006993592742 21221049159242599739439641412116 40251847985649
$PubK_{CP}$	45440428325685024798784595134370 25076096298827859374672736342140 1276767654342,507787315568264933 47641730406444407757973285439859 00766789227676375735325727

The public key $PubK_{CP}$ obtained by the participant through the above equation is compared with the $PubK_{CP}$ calculated by the verified public key $VerPK_{CP}$ for its correctness, and the calculation is as follows:

$$PubK'_{CP} = VerPK_{CP} + h(add_{CP}) \cdot G + [q_{CPx} + h(add_{CP})] \cdot PubK_{CA} \tag{7}$$

Table 6. Description of the parameters of the fourth stage of identity registration

Type	Parameters
$PubK'_{CP}$	45440428325685024798784595134370 25076096298827859374672736342140

	401276767654342,5077873155682649 33476417304064444077579732854 39 85900766789227676375735325727

3.2.3 Grievance application phase

The complainant randomly selects a parameter value $t \in Z_q$ as the secret parameter and encrypts it with the public key $PubK_{IU}$ of the investigation unit to generate the ciphertext $\mathrm{C} = \{C_1, C_2\}$. The complaint random secret parameter value $bf \in [2, n-2]$ is used as a blind factor with the public key $PubK_{IU}$ of the investigating unit, and hash function $h(\ )$ to blind the encrypted grievance message summary m, and send the blinded ciphertext summary $BFile_{cp}$ to the grievance center. The calculation is as follows:

$$C_1 = \mathrm{t} \cdot G \tag{8}$$

$$\mathrm{F}=(f_1, f_2)= t \cdot PubK_{IU} \tag{9}$$

$$C_2 = (c_{2x}, c_{2y}) = (f_1 \times m_1, f_2 \times m_2) \tag{10}$$

$$m = h(\mathrm{C}) \tag{11}$$

$$BFile_{cp} = m \cdot bf \cdot PubK_{CP} \tag{12}$$

Table 7. Description of the parameters of the first stage of grievance application phase

Type	Parameters
t	1124567890643211345
C_1	95856789024910179311156751475847 02252488343620195156952508699 49 79896394029404,65309781896873347 37231472152901215202806793667 16 23578652302877008150777423 36
$PubK_{IU}$	39133464524558521781757027165 85 48143564181063036270151453216 26 82324669321602,11032460681111918 58296633541039688807632369164 66 12248706553542595457051127582 1
C_2	79947290257316257295208011014 16 65663681156556070458401033782 61 550768561653385,6088801314895494 32451172807068572872450714915 61 00969950737364719427150270160
m	59963371158773892517253217489 39 84073226452920899248831452208 27 633746287900559
bf	43333226674567893456443 56

$BFile_{cp}$	58517402480454485973434760956 03 37470725650564270900930621965 37 936142898159070,5893212818859418 81360906620311929155759744002 97 43374680448404100445022407461 7

After receiving the blinded ciphertext summary $BFile_{cp}$, the grievance center uses the random secret parameter value $r_{GC} \in [2, n-2]$ and the private key $prik_{GC}$ for digital signature. Calculate the association value R and the signature file $SBFile_{CP}$. Then send the association value R, and the signature file $SBFile_{CP}$ back to the complainant.

$$R = r_{GC} \cdot BFile_{cp} \tag{13}$$

$$SBFile_{CP} = (prik_{GC} + r_{GC}) \cdot \ BFile_{cp} \tag{14}$$

Table 8. Description of the parameters of the second stage of the grievance application phase

Type	Parameters
r_{GC}	60687753605678673608386871614 0
R	64823418211476544993230442950258 54539802388864145062963616840525 969801125515,2158228130537476026 08846200647857342132691255469160 01767913705261048659497264
$SBFile_{CP}$	39740222649059378357179436921399 88512261288683747686438339238001 4562714781660,114488028782396320 04151143940976683548077393205885 37373587813031803081462337 90

After the complainant receives the association value R and the signature file $SBFile_{CP}$, the complainant uses the public key of the grievance center $PubK_{GC}$ to calculate the value of unblinding, and upload the grievance application case onto the blockchain.

$$\mathrm{S}' = SBFile_{CP} - m \cdot prik_{CP} \cdot PubK_{GC} \tag{15}$$

$$m' = m \cdot prik_{CP} \cdot (bf - 1) + m \tag{16}$$

Table 9. Description of the parameters of the third stage of the grievance application phase

Type	Parameters
S′	27175385443208040839670411387866 82 27445393569587306579092146701362 72 10133453,65798292866737920186991032 87067810592642756061352826161211 13 20959347665719709

m'	298430243954851717221949442433549092935320431159906420302037716632252400813303748366992012237723936550273152808068643142643218380574909937198133202758563340392285688745640129203 64

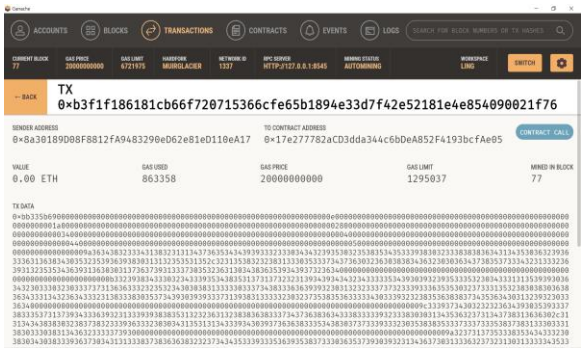

Fig.8. The transaction records for grievance applications

3.2.4 Grievance processing phase

The investigating unit will first complete the identity self-certification with the complainant, and the complainant will send the unblind point S', m', signature file $SBFile_{CP}$, association value R and cipher text C to the investigating unit for investigating operation.

$$R - h(C) \cdot PubK_{GC} \stackrel{?}{=} S' - m' \cdot PubK_{GC} \quad (17)$$

Table 10. Description of the parameters of the first stage of the grievance processing phase

Type	Parameters
$R - h(C) \cdot PubK_{GC}$	63102965822358290672363580746469449799735206245476413917156611567817176692176,76919515314797925968921472254381763410738213895825547850934470459477016632 81
$S' - m' \cdot PubK_{GC}$	63102965822358290672363580746469449799735206245476413917156611567817176692176,76919515314797925968921472254381763410738213895825547850934470459477016632 81

The investigation unit uses the private key $prik_{IU}$ to decrypt the ciphertext C_1, and calculate $Z = (z_1, z_2)$. Then use the inverse element of the Z-point to decrypt the message and restore it to the plain text M'.

$$Z = (z_1, z_2) = prik_{IU} \cdot C1$$

$$= prik_{IU} \cdot \mathrm{t} \cdot G = \mathrm{t} \cdot PubK_{IU} \quad (18)$$

$$M' = \left(c_{2x} \cdot {z_1}^{-1}, c_{2y} \cdot {z_2}^{-1}\right)$$

$$= (f_1 \times m_1 \cdot {z_1}^{-1}, f_2 \times m_2 \cdot {z_2}^{-1}) \quad (19)$$

$$\because \mathrm{F} = (f_1, f_2) = t \cdot PubK_{IU} \quad (20)$$

$$\therefore M' = (f_1 \times m_1 \cdot {z_1}^{-1}, f_2 \times m_2 \cdot {z_2}^{-1})$$

$$= (m_1, m_2) = \mathrm{M} \quad (21)$$

Table 11. Description of the parameters of the second stage of the grievance processing phase

Type	Parameters
m_1	7332119971101163211611132991111091121089710511 0
m_2	8411410110132991111081089711211510110032111110321161041013211411

IV. SECURITY ANALYSIS AND EVALUATION

This study uses blockchain technology as a framework to design a grievance mechanism through smart contract. Achieve security key assignment at the time of identity registration. Self-authentication is an effective way to resist man-in-the-middle attacks when both parties conduct transactions. During the grievance application and closing process, the grievance files are encrypted and blinded through blind signature and encryption based on the elliptic curve cryptosystem to ensure the confidentiality, authentication and untraceability of the files.

This chapter first verifies the logic of this study's self-certification mechanism by the BAN-Logic analysis of the identity authorization protocol. Analyze the security expected to be achieved and compare it with recent research proposals by scholars.

4.1 BAN-Logic

BAN-Logic is a type of formal security analysis method based on the logical derivation, which was proposed by Burrows, Abadi and Needham in 1990 [15], and is widely used in the

analysis of identity authentication protocols [16]. In this section, we verify the logical analysis proof of participant self-certification in this study mechanism through this method.

4.1.1 BAN-Logic objective

In the study framework, participants verify their identity as legal users through a self-certification mechanism. Since each participant (complainant, grievance center, and investigation unit) is registered in the same way. Take the complainant's application process to the grievance center as an example, using BAN-Logic logic analysis to prove whether both parties trust the public key $PubK_i$ transferred to each other to ensure the correctness and security of the mechanism. The following are the objectives to be achieved as proved by the study mechanism in the BAN-Logic analysis:

- Objective 1：$GC| \equiv PubK_{CP}$
- Objective 2：$CP| \equiv PubK_{GC}$

4.1.2 BAN-Logic message assumption

According to the message representation method defined by BAN-Logic, the following messages are transferred by the complainant to the grievance center in this study mechanism.

- Message 1：CP → GC：(add_{CP}、$VerPK_{CP}$、$PubK_{CP}$)
- Message 2：GC → CP：(add_{GC}、$VerPK_{GC}$、$PubK_{GC}$)
- Message 3：$CP \rightarrow CA$：(add_{CP}, S_{CP})
- Message 4：$CA \rightarrow CP$：($VerPK_{CP}$, cer_{CP})
- Message 5：$GC \rightarrow CA$：(add_{GC}, S_{GC})
- Message 6：$CA \rightarrow GC$：(VPK_{GC}, cer_{GC})

The following assumptions about the mechanism of this study are proposed for deriving further argumentation analysis.

- Assumption 1：CP| ⇒ (d_{CP} , add_{CP})
- Assumption 2：GC| ⇒ (d_{GC} , add_{GC})
- Assumption 3：CP| ≡ GC| ~ (d_{GC} , add_{GC})
- Assumption 4：GC| ≡ CP| ~ (d_{CP} , add_{CP})
- Assumption 5：CP| ≡ CA| ~ (cer_{GC})
- Assumption 6：GC| ≡ CA| ~ (cer_{CP})
- Assumption 7：CA| ⇒ $PubK_{CA}$
- Assumption 8：$GC| \equiv CA$
- Assumption 9：$CP| \equiv CA$

4.1.3 BAN-Logic deduction

In accordance with the BAN-Logic rules and the message transfer and proposed assumptions of the research mechanism, it can be proven that the participants trust both parties as the legal identity authorized by the CA through the self-certification mechanism designed by the institute. The proof process is as follows:

- In the registration phase, in accordance with the message sent by the complainant, it can be proved that the grievance center GC can see the message sent by the complainant CP.

$$GC \triangleleft (add_{CP} 、 VerPK_{CP} 、 PubK_{CP}) \quad (22)$$

- Based on the message-meaning rules, the following conclusion can be inferred.

$$GC^{\triangleleft}(PubK_{CP}) \quad (23)$$

- Based on equation (5) $prik_{CP} = cer_{CP} + h(d_{CP} \parallel add_{CP})$, equation (6) $PubK_{CP} = prik_{CP} \cdot G$ and assumptions 1, 4 and 6 of this study, we can conclude the following inferences.

$$\text{GC}| \equiv \text{CP}| \Rightarrow PubK_{CP} \quad (24)$$

$$\text{GC}| \equiv \text{CP}| \equiv PubK_{CP} \quad (25)$$

- According to the jurisdiction rule applies, and yields the following：

$$GC| \equiv PubK_{CP} \text{（Objective 1）} \quad (26)$$

- The registration process of the participants in this study is same and therefore it can be proved that the complainant CP can read the message sent by the grievance center GC when the complainant receives Message 2.

$$CP^{\triangleleft}(add_{GC} 、 VerPK_{GC} 、 PubK_{GC}) \quad (27)$$

- Based on the message-meaning rules, the following conclusion can be inferred.

$$CP^{\triangleleft}(PubK_{GC}) \quad (28)$$

- Based on equation $prik_{GC} = cer_{GC} + h(d_{GC} \| add_{GC})$, equation $PubK_{GC} = prik_{GC} \cdot G$ and assumptions 2, 3 and 5 of this study, we can conclude the following inferences.

$$\mathrm{CP}| \equiv \mathrm{GC}| \Rightarrow PubK_{GC} \quad (29)$$

$$\mathrm{CP}| \equiv \mathrm{GC}| \equiv PubK_{GC} \quad (30)$$

- Based on the message-meaning rules, the following conclusion can be inferred.

$$CP| \equiv PubK_{GC} \text{（Objective 2）} \quad (31)$$

Through the theory of logic above, it can be deduced that the complainant and the grievance center both trust the public key transferred by each other and can verify the identity of the participant without the certificate authority.

4.2 Security Analysis

By referring to the ISO information security management requirements, we present a security analysis of the proposed blockchain-based solution, how it addresses core security issues. Here, the definitions of various security indicators and solutions are discussed as follows:

4.2.1 Authenticity

Authenticity is the characteristic of ensuring that a subject or resource is identified as the person it claims to be. The receiver of the message may confirm the identity of the network user or data transmitter and ensure that the message is from the claimed transmitter.

- Malicious behavior:
  The attacker or illegal participant impersonates a legitimate user and sends the grievance case to the investigating unit.
- Solution:
  In this study, participants were able to verify their own identities. When a malicious third party wants to impersonate a person, it will face the problem of a discrete logarithm of the elliptic curve. In this way, authenticity can be achieved.

4.2.2 Integrity

Integrity means ensuring that the identity of a subject or resource is the same as the identity of the person it claims to be. This means that the receiver of the message can confirm the identity of the network user or data sender, and ensure that the message is sent by the purported sender.

- Malicious behavior:
  The attacker or illegal participant attempts to intercept the grievance file and tamper with the content of the grievance transmitted by the complainant.
- Solution:
  The grievance file encryption is generated based on the elliptical curve method. The complainant will calculate the hash value of the ciphertext file, as in equation (11) $m = h(C)$. Therefore, the grievance center receives the grievance files and compares the hash values as in equation (17) $R - h(C) \cdot PubK_{GC} \stackrel{?}{=} \mathrm{S}' - m' \cdot PubK_{GC}$. If the file is tampered with by an attacker or illegal participant, the hash value will be different and thus discovered.

4.2.3 Confidentiality

Confidentiality means that information cannot be accessed by unauthorized persons during transmission which can protect the confidentiality of information.

- Malicious behavior:
  Attacker or illegal participant intercepts grievance messages, and intended to obtain the content of the grievance.
- Solution:
  In this study, the grievance content is encrypted by the complainant based on the elliptic curve cryptography. The complainant randomly selects a secret parameter and encrypts it with the public key $PubK_{IU}$ of the investigation unit, such as in equation (8) $C_1 = \mathrm{t} \cdot G$ and equation (10) $C_2 = (c_{2x}, c_{2y}) = (f_1 \times m_1, f_2 \times m_2)$. Since the private key is only owned by the receiver, if the attacker or illegal participant intercepts the encrypted grievance file, there is no corresponding private key. If a malicious third party attempts to calculate the private key, it will face the problem of a discrete logarithm of the elliptic curve.

4.2.4 Resist man-in-the-middle attack

A man-in-the-middle attack is when an

attacker impersonates or fakes a person's identity and joins the system to disrupt the entire operational process without being identified by others.

- Malicious behavior:
  The attacker or illegal participant intercepts the closing file sent to the grievance center by the investigation unit. He attempted to impersonate a participant to tamper with the contents of the grievance case, disrupting the operation of the system and tampering with the case information.
- Solution:
  This study was designed using a self-certification approach. The participants have both completed the authentication of their identities prior to the transaction, as in equation (7) $PubK_{CP} \stackrel{?}{=} VerPK_{CP} + h(add_{CP}) \cdot G + [q_{CPx} + h(add_{CP})] \cdot PubK_{CA}$. To ensure that each other is legitimate before executing transactions, we can effectively resist man-in-the-middle attacks.

4.2.5 Unforgeability

Unforgeability means that an attacker or illegal participant attempts to forge a document or signature, and anyone can verify whether the document or signature is forged. Only authorized parties can sign grievance cases.

- Malicious behavior:
  The attacker or illegal participant attempted to forge the signature of the grievance center. He intercepted the grievance cases, forged a signature, and returned it to the complainant.
- Solution:
  In this study, the blind signature method based on elliptic curves was used. The grievance center signs the grievance case and generates the associated value R and the signature document $SBFile_{CP}$. The verifier can verify the validity of the signature by using the public key of the grievance center $PubK_{GC}$ as in equation (17) $R - h(C) \cdot PubK_{GC} \stackrel{?}{=} S' - m' \cdot PubK_{GC}$. In this way, unforgeability can be achieved.

4.2.6 Immutability

Information and data cannot be tampered with by anyone.

- Malicious behavior:
  The attacker or illegal participant attempts to tamper with the records on the blockchain and uploads the tampered messages.
- Solution:
  In this study, the complainant completes the complaint application through a blockchain smart contract. Data on the block chain is linked to each block chain by a hash function. Therefore, when an attacker or illegal participant attempts to tamper with the data content, the Hash value will be changed accordingly, which will affect the data in the whole chain. In addition, if the attacker attempts to tamper with the information on the blockchain, due to the self-certification method used in this research, the participant must verify whether the identity is authorized by the CA before the transaction, otherwise no transaction can be executed. Therefore, this study is immutable.

4.2.7 Untraceability

Untraceability means that the content of the transmission is not traceable by an object during the attacker's monitoring process.

- Malicious behavior:
  After receiving a grievance case, the grievance center attempts to steal the content of the grievance from the complainant.
- Solution:
  In this study, the blind signature mechanism based on elliptic curves was used. The complainant uses the random secret parameter value bf as the blind factor and generates the blinded ciphertext digest with the public key $PubK_{IU}$ of the investigation unit as in equation (12) $BFile_{cp} = m \cdot bf \cdot PubK_{CP}$ The grievance center only knows that the signature to be signed is a blinded grievance ciphertext digest $BFile_{cp}$, but does not know its content. This mechanism ensures the untraceability of grievance content.

4.3 Comparison Of Benefits

We discuss the proposed grievance system in Chapter 2. Based on the advantages and characteristics of the technology used in this study, the security analysis was conducted as follows. The Comparison of benefits between the proposed mechanism and other grievance mechanisms are shown in Table 12.

Table 12. Comparison of benefits between the proposed mechanism and other grievance mechanisms

Security analysis comparison items	Hingorani et.al [11]	Shettigar et.al [12]	Rahman et.al [13]	This study
Authenticity	╳	╳	○	○
Integrity	○	╳	○	○
Confidentiality	○	╳	△	○
Resist man-in-the-middle attack	╳	╳	○	○
Unforgeability	○	○	○	○
Immutability	○	○	○	○
Untraceability	△	△	△	○
○：fully in line with the characteristics △：partly in line with the characteristics ╳：not in line with the characteristics				

In the grievance mechanism proposed by Hingorani, Shettigar and Rahman, although the blockchain technology combined with smart contract, to achieve the permanent preservation of data, can not be tampered with and can not be counterfeited characteristics. In addition, since identities are anonymous on the blockchain, attackers cannot predict user information through grievance information and achieve identity untraceability. However, the untraceability of the content of the grievance, after it has been signed by the signatory, is not stated.

In the study by Hingorani et al, Diffie-Hellman key exchange was used for encryption of grievance files to achieve data confidentiality and integrity. However, the study did not mention the identity registration mechanism, which may lead to man-in-the-middle attacks due to the lack of confirmation of the identity of the communicating party. It is also unable to identify the purported sender of the message.

In the study by Shettigar et al, the grievance files were not encrypted and the identity registration and authentication methods were not described. As a result, data may be altered, tampered with and traced by unauthorized persons during transmission, and may lead to man-in-the-middle attacks. It is also unable to identify the purported sender of the message.

In the study by Rahman et al. the grievance files were stored in the Interplanetary File System and encrypted, Self-Sovereign Identity (SSI) and Zero Knowledge Proof are used to manage digital identity in a decentralized manner to achieve identity autonomy. Avoid man-in-the-middle attacks by zero knowledge proof to verify identity. However, the encryption method was not described and the confidentiality of the data was only partially achieved.

V. CONCLUSION

This study designs a smart contract grievance system, which is deployed on a blockchain. Through the participants to trigger the smart contract, the pre-defined rules and conditions are automatically executed to achieve the characteristics of "untraceable", " immutable", " unforgeable", etc. Maintain the grievance process and data intact, this will eliminate the risk of deliberate obstacles, case dismissal, or case concealment upon grievance filing, and reduce applicant's questioning, trust, and privacy protection issues in the grievance case. Use the blind signature based on the elliptic curve cryptosystem mechanism to protect the privacy of the complainant, achieve untraceability of the grievance content, and improve the complainant's trust in the system. In addition, authentication protocols are the foundation of security for distributed systems, we use the self-certified public key system can eliminate the risk of counterfeiting user identities in the certificate centre, ensuring the authenticity, integrity, and non-repudiation of the identity data of the participants, and effectively resist middleman attacks. In this manner, the system has high security and can effectively reduce the public key storage and management burden.

REFERENCES

[1] Swan, M., Blockchain Blue print for a New Economy, O'Reilly Media Publishing, United States, 2015.

[2] Sun, J., Yan, J., and Zhang, K. Z., "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, 2016.

[3] Efanov, D., and Roschin, P., "The all-pervasiveness of the blockchain technology," Procedia computer science, Vol. 123, pp. 116-121, 2018.

[4] Li, C. C., “The Peking University scandal that was written into the blockchain: School Ignores Professor's Sexual Assault, Lies to Persecute Solidarity Students,” 2018/04/26, Retrieved from:https://www.storm.mg/article/429991?page=1

[5] Hu, Z. X., “Blockchain breaks through national power Sexual assault case at Peking University will stay on the internet forever,” 2018/04/27, Retrieved from:https://cnews.com.tw/124180427a02/

[6] Yeh, C. L., “The Study on Preventive Measure and Reporting System of Workplace Bullying in Taiwan,” Master's thesis, Department of Labor Relations, National Chung Cheng University, 2021.

[7] Meutia, N. S., and Subriadi, A. P., “Effective Factors Influencing the Intention to Use Citizens Complaint Handling System,” Journal of Computer Science and Informatics Engineering (J-Cosine), Vol. 5, No. 2, pp. 120-129, 2021.

[8] Szabo Nick. “Smart Contracts.” [Online forum comment]. 1994. Retrieved from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[9] Ouyang, L., Zhang, W., and Wang, F. Y. “Intelligent contracts: Making smart contracts smart for blockchain intelligence.” Computers and Electrical Engineering, Vol.104, 108421, 2022.

[10] Girault, M., “Self-certified public keys,” In Workshop on the Theory and Application of of Cryptographic Techniques,” Springer, Berlin, Heidelberg, pp. 490-497, 1991.

[11] Chaum, D., “Blind signatures for untraceable payments,” In Advances in cryptology, Springer, Boston, MA, pp. 199-203, 1983.

[12] Hingorani, I., Khara, R., Pomendkar, D., and Raul, N., “Police complaint management system using blockchain technology,” In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) IEEE, pp. 1214-1219, December 2020.

[13] Shettigar, R., Dalvi, N., Ingale, K., Ansari, F., and Maheshwar, R. C., “Blockchain-Based Grievance Management System,” In Evolution in Computational Intelligence, pp. 211-222, 2021.

[14] Rahman, M., Azam, M. M., and Chowdhury, F. S., “An Anonymity and Interaction Supported Complaint Platform based on Blockchain Technology for National and Social Welfare,” In 2021 International Conference on Electronics, Communications and Information Technology (ICECIT) IEEE, pp. 1-8, September 2021.

[15] Burrows, M., Abadi, M., and Needham, R. M., “A logic of authentication,” ACM Transactions on Computer Systems (TOCS), Vol.8, Issue. 1, pp. 18-36, 1990.

[16] Zhang, X., Wang, B., and Zhang, W., “A Robust Authentication Protocol for Multi-server Architecture Using Elliptic Curve Cryptography,” Int. J. Netw. Secur., Vol. 21, No. 2, pp. 191-198, 2019.