Copyright ⓒ 2023 KSII

A Novel Electronic Voting Mechanism Based on Blockchain Technology

Chuan-Hao Yang*, Pin-Chang Su, and Tai-Chang Su
Department of Information Management, National Defense University, Taiwan, R.O.C.
[e-mail: franky051205@gmail.com]
*Corresponding author: Chuan-Hao Yang

Received March 9, 2023; revised June 23, 2023; accepted October 8, 2023; published October 31, 2023

Abstract

With the development of networking technology, it has become common to use various types of network services to replace physical ones. Among all such services, electronic voting is one example that tends to be popularized in many countries. However, due to certain concerns regarding information security, traditional paper voting mechanisms are still widely adopted in large-scale elections. This study utilizes blockchain technology to design a novel electronic voting mechanism. Relying on the transparency, decentralization, and verifiability of the blockchain, it becomes possible to remove the reliance on trusted third parties and also to enhance the level of trust of voters in the mechanism. Besides, the mechanism of blind signature with its complexity as difficult as solving an elliptic curve discrete logarithmic problem is adopted to strengthen the features related to the security of electronic voting. Last but not least, the mechanism of self-certification is incorporated to substitute the centralized certificate authority. Therefore, the voters can generate the public/private keys by themselves to mitigate the possible risks of impersonation by the certificate authority (i.e., a trusted third party). The BAN logic analysis and the investigation for several key security features are conducted to verify that such a design is sufficiently secure. Since it is expected to raise the level of trust of voters in electronic voting, extra costs for re-verifying the results due to distrust will therefore be reduced.

Keywords: blind signature, blockchain, electronic voting, self-certification

http://doi.org/10.3837/tiis.2023.10.015 **ISSN : 1976-7277**

1. Introduction

The essence of democracy is majority rule. Deciding what the majority is will basically be carried out by a vote. Since the end of 2019, the influence of the coronavirus disease (namely COVID-19) has promoted the trend of legislation for absentee voting, so that voters can vote without returning to their registered domiciles. One of the approaches to conducting absentee voting is Internet voting (I-voting), which is one type of electronic voting (e-voting). However, while the advancement in information and communication technologies makes it possible to realize electronic voting, most countries still adopt paper voting and manual vote-counting procedures. The fundamental reason behind this phenomenon is that voters have concerns regarding the security of emerging techniques related to voting [1]. Furthermore, the transparency of the current voting procedures is often unable to make voters feel confident, no matter what type (i.e., paper or electronic) of voting it is [2] [3].

In recent years, with the increasing utilization in finance, medical care, and supply chains, blockchain technology has become famous. Through consensus, such a technology maintains a shared ledger and stores data distributedly over all nodes. In this way, if the data is tampered with, it will be detected immediately. Therefore, blockchain technology has the characteristics of decentralization, immutability, anonymity, etc. to ensure the transparency of the voting procedures. Because of these characteristics, researchers have begun to introduce this technology into electronic voting systems. In addition to process design using a blockchain, signature and encryption in cryptography are also techniques in electronic voting that are essential to addressing security issues of the system. In related researches, Chaum (1983) [4] first proposed the blind signature based on the RSA (short for Rivest-Shamir-Adleman, names of its inventors) encryption algorithm. Its concept is that the signature requester allows the signer to complete signing the unknown message content without revealing the information within it. It has the characteristics of protecting the privacy of the message content of the signature requester. However, it also causes security issues, such as insufficient integrity, untraceability, and non-repudiation. Jen et al. (2010) [5] proposed the blind signature based on the elliptic curve cryptography (ECC). The main feature is that it reaches a higher computational speed under the same circumstances achieving untraceability.

This research is motivated by resolving the above-mentioned issues associated with electronic voting. The main goal is to design a novel electronic voting mechanism with sufficient security and practicality, by utilizing the underpinning blockchain technology with the characteristics of decentralization, immutability, and trustworthiness, and adopting the theoretical bases of the elliptic curve cryptography, the blind signature, and the self-certification mechanism. Such a mechanism will have the following advantages:

- The electronic voting mechanism with blockchain technology provides decentralized services to ensure the transparency and fairness of voting procedures and thereby strengthens the level of trust of voters in such a mechanism.
- By applying the elliptic curve cryptography theory to the electronic voting system, the use of the blind signature technique meets the fundamental security requirements. Besides, the use of keys with shorter bit lengths effectively reduces the computational load of the system and still achieves the same security strength as the RSA encryption algorithm.
- The introduction of the self-certification mechanism prevents the certificate authority (CA) as a trusted third party from selecting the private key on behalf of the voter and counterfeiting the voter's identity in the process of creating and issuing the certificate, and it reduces the cost and risk of the overall certification system in storing, calculating, and managing public keys.

To prove that the proposed mechanism is sufficiently secure, the BAN logic analysis and the investigation for several key security features will be conducted. There will also be comparisons between the proposed mechanism and the ones designed by relevant studies. Furthermore, the feasibility of such a mechanism will be verified through simulations and demonstrations.

2. Related Researches

This section discusses the blockchain, cryptography, and electronic voting techniques which are adopted as the bases of this research, and categorizes, summarizes, and analyzes the related researches in the literature.

2.1 Blockchain Technology

Nakamoto (2008) published a white paper, "Bitcoin: A peer-to-peer electronic cash system" [6], in which the Bitcoin electronic currency and its algorithms were described, and the concept of blockchains was presented. Buterin (2013) proposed a next-generation smart contract [7]. The study described that the smart contract is based on blockchain technology and can be used to construct a trustless cryptocurrency and a decentralized application (Dapp) platform. This had made the applications of blockchain technology more diverse and freer.

The concept of smart contracts was proposed by Szabo (1996), an interdisciplinary legal scholar [8]. That is, in comparison with the traditional contracting method, a higher level of security will be achieved and the transaction costs associated with contracting will be reduced by programming relevant agreements and executing them on computers.

The programs of decentralized applications are deployed on peer-to-peer distributed blockchain networks, and all of the data are open, transparent, and immutable [9].

2.2 Cryptography

2.2.1 Elliptic Curve-based Blind Signature

The elliptic curve-based blind signature was proposed by Jeng et al. in 2010 [5]. With the characteristics of having a short elliptic curve key length, a fast processing speed, and the difficulty of solving an elliptic curve discrete logarithm problem (ECDLP) when trying to crack the encryption, this algorithm is computationally faster, less expensive, and harder to crack at the same key length than the RSA.

2.2.2 Self-certification Mechanism

Girault proposed a self-certification mechanism based on the RSA public key cryptosystem [10] in 1991. Its purpose is to allow the user to participate in the calculation of the public key at the authorization stage. At the subsequent usage stage, independent identity self-certification can be completed without the need for a trusted third party. This mechanism has a higher security level, a lower management load, and higher identity certification efficiency. For the security of the public key cryptosystem, Girault proposed three levels of security as shown in **Table 1**.

Table 1. Three levels of security

Level	Description	Example
Level 1	The certificate authority knows the private and public keys of all users and can impersonate any user at any time without being detected.	Identity-based Certification System
Level 2	The certificate authority does not know the private keys of users, but can still forge an illegal user that is difficult to be detected.	Electronic Certificate Authentication System
Level 3	The private keys of users are self-selected, and the certificate authority cannot generate or even forge the public keys of users. The users can check the correctness of the public keys sent by the certificate authority on their own, and the certificate authority cannot dominate the generation and verification of the public keys for the users.	Self-certified Public Key Cryptosystem

2.3 Electronic Voting

Electronic voting refers to utilizing electronic equipment to assist in completing any part of the voting procedures. Generally, it is divided into two categories in correspondence with the different types of equipment used [11]. One category is implemented through the use of standalone electronic voting machines. In such a category, the voting personnel must be selected through a certain screening process, and the equipment cost may be fairly high. Furthermore, the voters are still required to go to a polling station to vote in person. The other category is Internet voting. Different from the category adopting electronic voting machines, the information exchange of this category is carried out exclusively through the Internet. In-person voting is no longer needed.

The representatives of recent studies regarding electronic voting are summarized as follows.

Song and Cui (2012) [12] presented an electronic voting algorithm by incorporating the ElGamal blind-signature algorithm in the Extensible Markup Language (XML). It was reported to have good security importance. However, the main issue with this algorithm is that it is categorized as a general centralized mechanism, which relatively lacks transparency and is prone to interventions of trusted third parties. Furthermore, when the algorithm is adopted, the voter identity may be traceable from the vote [13].

Waheed et al. (2021) [14] proposed a scheme using the elliptic curve-based blind signature. Compared with the ElGamal-based or RSA-based cryptosystems, the scheme is more efficient and secure. However, it is also categorized as a centralized mechanism. Its main issue is similar to the one proposed by Song and Cui (2012) [12].

Liu and Wang (2017) [15] presented a mechanism that incorporates blockchain technology and deploys the interactions among participants in the form of transaction records on the blockchain for verification. The mechanism provides relatively better transparency. However, their study did not describe how the participants generate public and private keys at the registration stage. If the public and private keys still need to be generated by relying on a trusted third party like the certificate authority, the mechanism may be prone to interventions of the third party. Besides, at the voting stage, the voter establishes voting information directly based on the voting options, not through the ballot sent by the organization, so the organization is not able to ensure non-repudiation of the voting behavior by the voter.

The mechanisms proposed by Dong et al. (2017) [16], Yu et al. (2019) [17], and Zhou and Yan (2020) [18] all incorporate blockchain technology for better transparency. However, the certificate authority is required in these mechanisms to assist in the public and private key

generation for conducting identity certification. They are prone to interventions of the certificate authority. Furthermore, the smart contract is used to provide a decentralized environment when there is not any trusted third party present. However, these mechanisms all deploy the public and private keys in the smart contract through the certificate authority. Since the smart contract is public and accessible to all participants, the information in it is not secure.

This research is to design a mechanism that is able to resolve the issues associated with the currently developed electronic voting mechanisms as discussed above.

3. Mechanism Design

This study proposes an electronic voting mechanism suitable for use through the Internet. First of all, the Ethereum blockchain [19] can be adopted to construct the development environment, and the smart contracts can be utilized for publishing the votes on the chain, which will allow the participants to conduct verifications from the hash values of the transactions on the blockchain and resolve the issue associated with the lack of transparency in the current electronic voting system. Furthermore, the blind signature algorithm based on the elliptic curve cryptography can be adopted to enhance the security of this mechanism to protect the privacy of the voters' identities and the content of ballots. For identity verification, the self-certification mechanism can be introduced to prevent untrustworthy certificate authorities from using the computed public and private keys during the process of certificate issuance to falsely act as the voters to vote. It can also reduce the load of certificate authorities to compute the public and private keys for all voters, so as to enhance the execution efficiency. The following describes the structure and operation process of the proposed electronic voting mechanism.

3.1 Operation Process and Symbols

The electronic voting process designed in this study is categorized into 5 stages, namely the initialization stage, the ballot collecting and voting stage, the blinding and signing stage, the unblinding stage, and the verifying and counting stage. The processes of all stages are shown in **Fig. 1**, and the parameters and symbols are shown in **Table 2**.

Table 2. System parameters

Item	Symbol	Description
1	$E(F_q)$	an elliptic curve in the finite field F_q
2	G	the base point on the elliptic curve
3	n	the order of the base point on the elliptic curve
4	q	a prime number greater than 2^{256}
5	$h_1(), h_2()$	the hash function (value-to-value), the hash function (point sequence-to-value)
6	id_z	the identity (ID) information of participant z (the voter, the election organization, or the time server)
7	r_z	a randomly-chosen value used in the computation process of the self-certification mechanism for participant z (the voter, the election organization, the time server, or the certificate authority)
8	SF_z	the signature file of participant z (the voter, the election organization, or the time server) computed by using id_z and r_z
9	VPK_z	the verification public key of participant z (the voter, the election organization, or the time server) obtained by registering with the certificate authority
10	SV_z	the signature for participant z from the certificate authority after generating VPK_z

Item	Symbol	Description
11	sk_z	the private key of participant z (the voter, the election organization, the time server, or the certificate authority)
12	PK_z	the public key of participant z (the voter, the election organization, the time server, or the certificate authority)
13	$options$	the collection of voting options
14	op_j	voting option j, where $j = \{1, 2, 3, \cdots, m\}$
15	bf	the blinding factor, representing a randomly-chosen value for the voter to conduct the blinding computation
16	w	the encrypted voting information
17	W	the blinded encrypted abstract document
18	R	the relationship value produced during the signing process of the election organization
19	$\mathcal{S}$	the signed document produced by the signing process of the election organization
20	wPK	the point produced by the unblinding computation of the voter
21	$addr$	the blockchain address produced during interaction with the smart contract
22	wPK'	the collection of points to be compared with each wPK
23	Sum	the collection of voting results

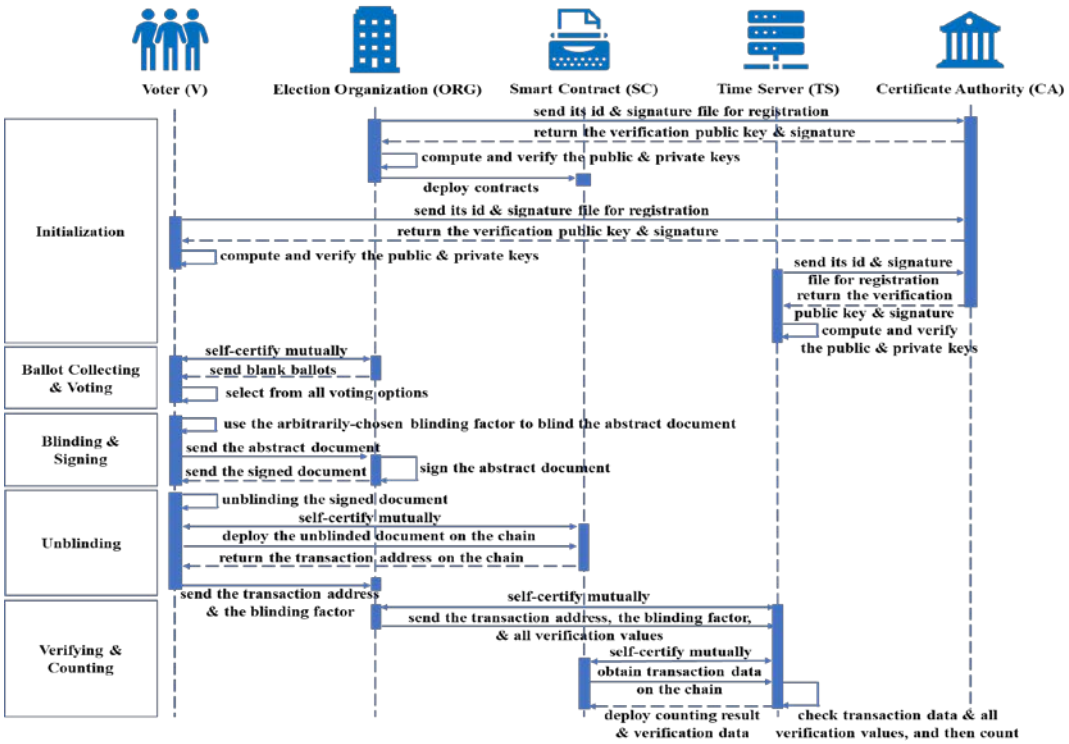

Fig. 1. Sequence diagram for the processes of all stages

3.2 Stages and Algorithms

This section describes the processes and algorithms of the 5 stages, namely the initialization stage, the ballot collecting and voting stage, the blinding and signing stage, the unblinding stage, and the verifying and counting stage.

3.2.1 The Initialization Stage

At the initialization stage, the certificate authority (CA) chooses one secure elliptic curve $E(F_q)$ in the finite field F_q, where $E(F_q)$: $y^2 = x^3 + ax + b\ (mod\ q)$, $4a^3 + 27b^2 \neq 0\ (mod\ q)$, and q is a prime number greater than 256 bits, and adopts a base point G with its order equal to n, so that

$$n \cdot G = O \tag{1}$$

where O is the infinitely-distant point of this elliptic curve. In addition, one-way collision-free hash functions, $h_1()$ and $h_2()$, are adopted at this stage. The public key is computed in the following equation.

$$PK_{CA} = sk_{CA} \cdot G \tag{2}$$

Subsequently, $E(F_q)$, G, q, PK_{CA}, $h_1()$ and $h_2()$ are published to allow the participants, namely the election organization, the voter, and the time server, to conduct the related computation when registering with the certificate authority.

For example, the election organization (ORG) uses its identity information id_{ORG} and a randomly-chosen secret value $r_{ORG} \in [2, n-2]$ to generate the signature file SF_{ORG}, and subsequently sends id_{ORG} and SF_{ORG} to the certificate authority. SF_{ORG} is computed in the following equation.

$$SF_{ORG} = h_1(r_{ORG} \parallel id_{ORG}) \cdot G \tag{3}$$

The certificate authority chooses a secret value $r_{CA} \in [2, n-2]$ to compute the verification public key VPK_{ORG} and the signature SV_{ORG} of the election organization as shown in the following equation, where (q_{ORGx}, q_{ORGy}) represents the corresponding point of VPK_{ORG} on the elliptic curve $E(F_q)$ in the x and y coordinates. After the computation, VPK_{ORG} and SV_{ORG} are sent to the election organization.

$$VPK_{ORG} = SF_{ORG} + \left(r_{CA} - h_1(id_{ORG})\right) \cdot G = \left(q_{ORGx}, q_{ORGy}\right) \tag{4}$$

$$SV_{ORG} = r_{CA} + sk_{CA} \cdot \left(q_{ORGx} + h_1(id_{ORG})\right) \tag{5}$$

The election organization uses the parameters (VPK_{ORG} and SV_{ORG}) returned by the certificate authority to compute the private key sk_{ORG} and to verify the computation accuracy of the certificate authority.

$$sk_{ORG} = \left(SV_{ORG} + h_1(r_{ORG} \parallel id_{ORG})\right) \tag{6}$$

The public key PK_{ORG} is computed by the election organization using the following equation.

$$PK_{ORG} = sk_{ORG} \cdot G \tag{7}$$

The verification is conducted as follows.

$$PK_{ORG} = \left(r_{CA} + sk_{CA} \cdot \left(q_{ORGx} + h_1(id_{ORG})\right) + h_1(r_{ORG} \parallel id_{ORG})\right) .\ \ G \tag{8}$$

$$PK_{ORG} = \left(\ r_{CA} + sk_{CA}\left(q_{ORGx} + h_1(id_{ORG})\right)\right) \cdot G + h_1(r_{ORG} \parallel id_{ORG}) \cdot G \tag{9}$$

$$\because PK_{CA} = sk_{CA} \cdot G \tag{10}$$

$$\therefore PK_{ORG} = \left(\ r_{CA} + h_1(r_{ORG} \parallel id_{ORG})\right) \cdot G + \left(q_{ORGx} + h_1(id_{ORG})\right) \cdot PK_{CA} \tag{11}$$

$$\therefore PK_{ORG} = r_{CA} \cdot G + h_1(r_{ORG} \parallel id_{ORG}) \cdot G + \left(q_{ORGx} + h_1(id_{ORG})\right) \cdot PK_{CA} \tag{12}$$

$$\because SF_{ORG} = h_1(r_{ORG} \parallel id_{ORG}) \cdot G \tag{13}$$

$$\therefore PK_{ORG} = r_{CA} \cdot G + SF_{ORG} + \left(q_{ORGx} + h_1(id_{ORG})\right) \cdot PK_{CA} \tag{14}$$

$$\because VPK_{ORG} = SF_{ORG} + \left(r_{CA} -\ h_1(id_{ORG})\right) \cdot G \tag{15}$$

$$\begin{aligned} \because SF_{ORG} &= VPK_{ORG} - \left(r_{CA} - h_1(id_{ORG})\right) \cdot G \\ &= VPK_{ORG} - r_{CA} \cdot G + h_1(id_{ORG}) \cdot\ G \end{aligned} \tag{16}$$

$$\therefore PK_{ORG} = r_{CA} \cdot G + VPK_{ORG} - r_{CA} \cdot G + h_1(id_{ORG}) \cdot G + \left(q_{ORGx} + h_1(id_{ORG})\right) \cdot PK_{CA} \quad (17)$$

$$\therefore PK_{ORG} = VPK_{ORG} + h_1(id_{ORG}) \cdot G + \left(q_{ORGx} + h_1(id_{ORG})\right). \ PK_{CA} \quad (18)$$

The registration processes of the voter and the time server with the certificate authority are the same as the process mentioned above. After registering with the certificate authority and receiving the exclusive verification public key VPK_z and signature SV_z (where z represents the participant), every participant can compute the private key by itself and verify the accuracy of the public key. It is also feasible to use identity-related parameters, such as id_z, VPK_z, and PK_z, to directly certify the identity of a participant without the need to rely on the certificate authority for conducting identity certification.

After completing registration, the election organization will incorporate the self-certification mechanism, the associated public parameters, and the voting functions in the smart contract and deploy the contract on the blockchain. As soon as the address of the contract is obtained, it will implement the decentralized voting and counting applications and publish them for the voters and the time server to use.

3.2.2 The Ballot Collecting and Voting Stage

All participants must mutually complete self-certification before interacting with each other. After the voter (V) and the election organization obtain valid identities from the certificate authority, as soon as the election organization receives the identity-related parameters (id_V, VPK_V, and PK_V) from the voter, it will conduct certification to make sure that the identity of the voter is valid. The associated computation is as follows.

$$PK_V{}' = VPK_V + h_1(id_V) \cdot G + \left(q_{Vx} + h_1(id_V)\right). \ PK_{CA} \quad (19)$$

$$PK_V{}' \stackrel{?}{=} PK_V \quad (20)$$

Similarly, the voter can use id_{ORG}, VPK_{ORG}, and PK_{ORG} sent by the election organization to certify its identity.

$$PK_{ORG}{}' \stackrel{?}{=} PK_{ORG} \quad (21)$$

After mutual identity certification, the election organization sends a ballot to the voter and puts the record on the blockchain to prevent the voter from repeatedly collecting ballots. The ballot contains the voting question and a collection of voting options (denoted by op_j, where $j = \{1, 2, 3, \cdots, m\}$) as shown in the following equation.

$$options = \{op_1, op_2, op_3, \cdots, op_m\} \quad (22)$$

The voter can mark an option after collecting the ballot.

3.2.3 The Blinding and Signing Stage

After marking an option op_j, the voter adopts a random value $bf \in [2, n-2]$ as the blinding factor and uses the public key PK_{TS} of the time server (TS) and the one-way collision-free hash function $h_2()$ to generate the encrypted voting information w. The encrypted voting information w is then blinded to generate the encrypted abstract document W. After mutual identity certification, W is sent to the election organization.

$$w = h_2\left(bf \cdot PK_{TS} \parallel op_j\right) \quad (23)$$

$$W = w \cdot G \quad (24)$$

As soon as the election organization receives the blinded encrypted abstract document W, it uses a random value $r_{ORG} \in [2, n-2]$ and its private key sk_{ORG} to sign the document W

and to generate the relationship value R and the signed document S. Subsequently, R and S are returned to the voter.

$$R = r_{ORG} \cdot W \tag{25}$$

$$S = (sk_{ORG} + r_{ORG}) \cdot W \tag{26}$$

3.2.4 The Unblinding Stage

After receiving the relationship value R and the signed document S, the voter uses the public key PK_{ORG} of the election organization to compute the unblinding point wPK for the encrypted voting information w, and then deploys such a point along with R and S on the blockchain through the smart contract (SC). In the meantime, the smart contract will enable its functions to verify whether or not the 3 parameters (wPK, R, and S) and the same transaction address $addr$ already exist on the blockchain. If they do exist, such a vote will be nullified. In this way, repeated voting by the voter can be avoided.

$$wPK = w \cdot PK_{ORG} \tag{27}$$

After the parameters are deployed on the blockchain, the participants can conduct the verification on their own. The equations are as follows.

$$R \stackrel{?}{=} R' = S - wPK \tag{28}$$

$$\because R = r_{ORG} \cdot W \tag{29}$$

$$\because S = (sk_{ORG} + r_{ORG}) \cdot W \tag{30}$$

$$\therefore r_{ORG} \cdot W \stackrel{?}{=} (sk_{ORG} + r_{ORG}) \cdot W - wPK \tag{31}$$

$$\therefore r_{ORG} \cdot W \stackrel{?}{=} sk_{ORG} \cdot W + r_{ORG} \cdot W - wPK \tag{32}$$

$$\because wPK = w \cdot PK_{ORG} = W \cdot sk_{ORG} \tag{33}$$

$$\therefore r_{ORG} \cdot W \stackrel{?}{=} wPK + r_{ORG} \cdot W - wPK \tag{34}$$

$$\therefore r_{ORG} \cdot W = r_{ORG} \cdot W \tag{35}$$

$$\therefore R = R' \tag{36}$$

As the final step, the voter sends the election organization the transaction address $addr$ obtained after deploying the parameters on the blockchain along with the encrypted blinding factor BF computed by the following equation.

$$BF = bf \cdot G \tag{37}$$

3.2.5 The Verifying and Counting Stage

After mutual self-certification with the time server, the election organization sends the time server the transaction address $addr$, the encrypted blinding factor BF, and the verification values of all voting options ($options = \{op_1, op_2, op_3, \cdots, op_m\}$). Subsequently, the time server uses the transaction address $addr$ to obtain the unblinding point wPK of each vote through the smart contract and uses the private key sk_{TS} of the time server and the public key PK_{ORG} of the election organization to compute a collection of points $wPK' = \{wPK'_1, wPK'_2, wPK'_3, \cdots, wPK'_m\}$ to be compared with and to verify each wPK. Taking voting option 1 op_1 as an example, the computation is as follows.

$$wPK = w \cdot PK_{ORG} \tag{38}$$

$$wPK'_1 = h_2(BF \cdot sk_{TS} \parallel op_1) \cdot PK_{ORG} \tag{39}$$

The verification process is as follows.

$$wPK \stackrel{?}{=} wPK'_1 \tag{40}$$

$$w \cdot PK_{ORG} \stackrel{?}{=} h_2(BF \cdot sk_{TS} \parallel op_1) \cdot PK_{ORG} \quad (41)$$

$$\because w = h_2(bf \cdot PK_{TS} \parallel op_j) \quad (42)$$

$$\therefore h_2(bf \cdot PK_{TS} \parallel op_j) \cdot PK_{ORG} \stackrel{?}{=} h_2(BF \cdot sk_{TS} \parallel op_1) \cdot PK_{ORG} \quad (43)$$

$$\because bf \cdot PK_{TS} = bf \cdot sk_{TS} \cdot G = BF \cdot sk_{TS} \quad (44)$$

$$if\ op_j = op_1 \quad (45)$$

$$h_2(bf \cdot PK_{TS} \parallel op_j) \cdot PK_{ORG} = h_2(bf \cdot sk_{TS} \cdot G \parallel op_1) \cdot PK_{ORG} = h_2(BF \cdot sk_{TS} \parallel op_1) \cdot PK_{ORG} \quad (46)$$

$$wPK = wPK'_1 \quad (47)$$

When $wPK = wPK'_1$, it indicates that the vote is for option 1. Such a result will be added to the collection of voting results, $Sum = \{sum_{op1}, sum_{op2}, sum_{op3}, \cdots, sum_{opm}\}$. That is $sum_{op1} + 1$. On the other hand, when $wPK \neq wPK'_1$, the other results $wPK'_j, j \in 2 \cdots m$ will be compared to decide which option the vote is for.

When all the votes are compared and the results are counted, the collection of voting results Sum, the product of the encrypted blinding factor and the private key $BF \cdot sk_{TS}$, and the verification values of all voting options ($options = \{op_1, op_2, op_3, \cdots, op_m\}$) will be deployed on the blockchain to allow all participants to verify the counting results on their own.

4. Security Analysis and Evaluation

This section verifies the security of the proposed mechanism through the analysis using the BAN logic and the investigation of relevant security regulations.

4.1 The BAN Logic Analysis

The Burrows-Abadi-Needham logic (BAN logic) was proposed by Burrows, Abadi, and Needham in 1990. It is a security analysis that specifically focuses on examining whether or not the identities of two parties in the transaction can be certified in the network security protocol. The representation of a general security protocol includes the subjects, the keys, and the formulas. The combination of them will represent all of the inference processes. The BAN logic has 5 inference rules, namely the message-meaning rule, the nonce-verification rule, the jurisdiction rule, the receiving rule, and the freshness-conjuncatenation rule.

Participants in this study mutually certify whether or not the identities of each other are authorized users through the proposed self-certification mechanism before transactions. Taking the voter (V) and the election organization (ORG) as an example, the BAN logic analysis is used to prove that through such a mechanism, each party trusts the public key (S) sent by the other with which it communicates, so as to ensure the correctness and security of the mechanism. First, the goals to be achieved through the BAN logic analysis are as follows.

Goal 1: $ORG| \equiv S_V$

Goal 2: $V| \equiv S_{ORG}$

Before conducting the analysis, the message exchange process of this study is transformed into the expressions defined by the BAN logic format. The transformed messages are as follows.

Message 1: $V \rightarrow ORG: (VPK_V, PK_V, ID_V)$

Message 2: $ORG \rightarrow V: (VPK_{ORG}, PK_{ORG}, ID_{ORG})$

Subsequently, the assumptions regarding the mechanism proposed in this study are stated as follows for further inference and analysis.

Assumption 1: $V| \Rightarrow r_V$

Assumption 2: $ORG| \equiv V| \sim (ID_V, r_V)$

Assumption 3: $ORG| \Rightarrow r_{SC}$

Assumption 4: $ORG| \equiv CA| \sim SV_V$

Assumption 5: $V| \equiv CA| \sim SV_{ORG}$

Assumption 6: $V| \equiv ORG| \sim (ID_{ORG}, r_{ORG})$

Assumption 7: $V| \equiv ORG| \equiv (sk_{ORG}, CA| \sim VPK_{ORG})$

Assumption 8: $ORG| \equiv V| \equiv (sk_V, CA| \sim VPK_V)$

Assumption 9: $V| \equiv ID_{ORG}$

Assumption 10: $ORG| \equiv ID_V$

According to the assumptions regarding the proposed mechanism and the rules of the BAN logic, it is proven that the voter and the election organization can trust the messages sent by each other after mutually certifying their identities through the self-certification mechanism. The proofs are described as follows.

When the election organization receives Message 1, it is proven that the election organization can see the message sent by the voter.

$$ORG \lhd (VPK_V, PK_V, ID_V)$$

According to the jurisdiction rule, the following is inferred.

$$ORG^{\lhd}(PK_V)$$

Based on the formulas $sk_V = \left(SK_V + h_1(r_V \| id_V)\right)$ and $PK_V = sk_V \cdot G$, and Assumptions 1, 2, and 4, the following conclusions are drawn.

$$ORG| \equiv V| \Rightarrow PK_V \text{ and } ORG| \equiv V| \equiv PK_V$$

Therefore, according to the jurisdiction rule, the following is proven.

$$ORG| \equiv PK_V \text{ (Goal 1)}$$

Furthermore, according to Assumptions 3, 5, and 6, when the election organization receives Message 2, the following conclusions are drawn.

$$V| \equiv ORG| \Rightarrow PK_{ORG} \text{ and } V| \equiv ORG| \equiv PK_{ORG}$$

According to the jurisdiction rule, the following is proven.

$$V| \equiv PK_{ORG} \text{ (Goal 2)}$$

At the initialization stage, the registration process of the smart contract is the same as the other participants. Therefore, they can trust the $VPKs$, PKs, and IDs sent by each other through the self-certification mechanism without relying on the certificate authority for identity certification. Besides, the participants have jurisdiction over the chosen random value r to prevent the third party from impersonating their identities. Therefore, the security of the proposed self-certification mechanism is verified.

4.2 Security Analysis

This study summarizes the security regulations defined in the voluntary voting system guidelines (VVSG) 2.0 and conducts verification for a list of security aspects of the proposed electronic voting mechanism. These aspects include transparency, confidentiality, integrity, authentication, anonymity, non-repudiation, untraceability, and minimum third-party participation [20].

4.2.1 Transparency

The proposed electronic voting mechanism is developed based on blockchain technology. A blockchain is a decentralized, immutable, and credible distributed ledger that provides a secure, stable, transparent, verifiable, and efficient transaction record. As its extensions, the smart contract and the decentralized applications are developed and deployed on a distributed blockchain network, on which all data are open, transparent, and immutable. Therefore, transparency in the voting operation is ensured. Visitors on the blockchain are allowed to examine the voting processes and transactions at any time to verify the operation of the voting mechanism.

4.2.2 Confidentiality

The voter uses a randomly-chosen secret value bf and the public key PK_{TS} of the time server to encrypt the vote (as shown in (23)). The secret value bf is owned by the voter, and the private key sk_{TS} is owned by the time server. Therefore, even if a third party steals the encrypted information of the vote, without the associated secret value bf and private key sk_{TS}, decrypting the information will require facing the difficulty of solving a problem with elliptic-curve discrete logarithmic complexity. This means that the proposed mechanism ensures the confidentiality of the vote.

4.2.3 Integrity

The encrypted abstract document W to be signed by the election organization is computed by the voter using the one-way collision-free hash function $h_2()$ (as shown in (23) and (24)). Even if a third party intercepts the encrypted document sent by the voter and falsifies it before deploying it on the blockchain, the produced encrypted abstract document will not be the same because of the irreversibility characteristic associated with the hash function $h_2()$, and therefore signature verification will fail. It is evident that when verification at the time server finally succeeds, it means that the same hash value of the encrypted abstract document is produced and that the content of the vote is correct and intact. This indicates that the proposed mechanism ensures the integrity of the vote.

4.2.4 Authentication

Through the proposed self-certification mechanism, two parties confirm the identities of each other before transmitting data. Taking the voter as the sender and the election organization as the receiver as an example, the voter sends id_V, VPK_V, and PK_V for identity certification, and the election organization uses (19) and (20) to certify the identity of the voter. A third party intending to impersonate the identity of the voter will face the difficulty of solving a problem with elliptic-curve discrete logarithmic complexity. Therefore, the proposed mechanism ensures the authentication of the participants' identities.

4.2.5 Anonymity

In the proposed mechanism, the blind signature technique is adopted to allow the voter to use a randomly-chosen value bf as the blinding factor and to incorporate the public key PK_{TS} of the time server for encrypting and blinding operations to generate an encrypted abstract document that is blinded (as shown in (23) and (24)). In this way, the election organization can only process the vote, and will not be able to access its content. Through the use of a random value bf, the produced encrypted abstract document will not be deterministic, so the election organization will not be able to determine which content of a vote will generate which

kind of encrypted abstract document. Therefore, the voter does not need to worry that the document may be exposed during the signing process. Besides, when submitting the vote, the voter deploys the unblinding point wPK, the relationship value R, and the signed document S on the blockchain through the smart contract for verification. The process of deployment is accomplished by using the public and private keys stored at the transaction address to complete the transaction with the smart contract. No one will know who the owner of the private key is as long as it is not disclosed to anyone. Therefore, the proposed mechanism ensures the anonymity of the voter identity.

4.2.6 Non-repudiation

Because the associated certificate is only owned by a specific voter, the behavior of such a voter collecting a ballot after mutual self-certification with the election organization will be regarded as a transaction record and deployed on the blockchain through the smart contract, which makes the fact that the voter has already collected a ballot undeniable and prevents the voter from repeatedly collecting ballots. As for whether or not to cast a vote after collecting a ballot, it depends on the voter to exercise the voting right. Besides, when the voter deploys the information regarding the vote on the blockchain, the smart contract will verify whether or not the information and the same transaction address already exist on the blockchain. If they exist, such a vote will be nullified and not deployed on the blockchain to ensure that the voter can only cast a vote once. As for the process of the blind signature, the election organization signs the document as the operation shown in (26). Since the private key sk_{ORG} is only owned by the election organization, and the time server can verify the validity of the transaction record by using the public key PK_{ORG} of the election organization (as shown in (40)), it can prevent the election organization from denying the signing behavior. Therefore, the proposed mechanism ensures non-repudiation of the ballot collecting, voting, and signing behaviors.

4.2.7 Untraceability

In this study, the blind signature mechanism is incorporated. The voter uses a randomly-chosen value bf as the blinding factor for blinding the encrypted abstract document (as shown in (23) and (24)). The election organization can only sign the encrypted abstract document (as shown in (26)), and will not be able to access its content to know its voting option. Furthermore, the time server uses its private key sk_{TS} to check the vote (as shown in (40)) during the counting process. Although the time server eventually learns the content of the vote, it will not be able to make a connection with the voter. Even if any third party tries to trace the voter through the published verification parameters on the blockchain, it will still need the private key sk_{TS} of the time server (as shown in (29)). Therefore, the proposed mechanism ensures untraceability of the voter identity.

4.2.8 Third-party Participation

A decentralized blockchain does not rely on any trusted third party, thereby enhancing data verifiability and maintaining voting transparency. Therefore, the voter can still count the votes and verify the election result by itself even when there are no trusted third parties present [21]. As for identity certification, the participant in this study uses its own identity information and a random value to generate the signature file (as shown in (3)). After registering with the certificate authority and receiving the verification public key and the signature, it produces the public and private keys by itself and verifies the correctness of the public key (as shown in (19)). As soon as all participants complete registration, identity certification between any two

parties of the transaction will no longer need to go through the certificate authority. Instead, they self-certified mutually. The proposed mechanism satisfies the security requirements of the Level 3 public key cryptosystem proposed by Girault (1991) [11] and ensures minimum third-party participation.

4.3 Comparison Between Security Alternatives

The comparison between the proposed mechanism and security alternatives proposed by relevant studies is shown in **Table 3**.

Table 3. Comparison between the proposed mechanism and alternatives by relevant studies

Security Characteristics	Song & Cui (2012) [12]	Waheed et al. (2021) [14]	Liu & Wang (2017) [15]	Dong et al. (2017) [16]	Yu et al. (2019) [17]	Zhou & Yan (2020) [18]	Proposed Mechanism
Transparency	✕	✕	○	○	○	○	○
Confidentiality	○	○	○	✕	✕	✕	○
Integrity	○	○	○	○	○	○	○
Authentication	○	○	○	✕	✕	✕	○
Anonymity	✕	○	○	○	○	○	○
Non-repudiation	○	○	✕	○	○	○	○
Untraceability	✕	○	○	○	○	○	○
Minimum Third-party Participation	✕	✕	△	△	△	△	○
○ : Satisfied △ : Partially Satisfied ✕ : Not Satisfied							

The electronic voting mechanisms proposed by Song and Cui (2012) [12] and Waheed et al. (2021) [14] are both categorized as general centralized mechanisms. Compared with the blockchain-based electronic voting mechanisms, they relatively lack transparency and are prone to interventions of trusted third parties. Furthermore, when the mechanism proposed by Song and Cui is adopted, the voter identity may be traceable [13], so the vote does not satisfy the security requirements of anonymity and untraceability. The mechanism proposed by Liu and Wang (2017) [15] further incorporates blockchain technology and deploys the interactions among participants in the form of transaction records on the blockchain for verification. However, their study did not describe how the participants generate public and private keys at the registration stage. It merely explained that the individual participant submits the identity information and the public key to the organization for registration. If the public and private keys still need to be generated by relying on a trusted third party like the certificate authority, the mechanism does not completely meet the security requirement of reducing third-party participation. Besides, at the voting stage, the voter establishes voting information directly based on the voting options, not through the ballot sent by the organization, so the organization is not able to ensure non-repudiation of the voting behavior by the voter.

The electronic voting mechanisms proposed by Dong et al. (2017) [16], Yu et al. (2019) [17], and Zhou and Yan (2020) [18] also incorporate blockchain technology. However, the certificate authority is required in these mechanisms to assist in the public and private key generation for conducting identity certification. Unlike the self-certification mechanism proposed in this study, in which the participants produce the public and private keys on their

own and certify the identities of each other mutually, these mechanisms only partially meet the security requirement of minimum third-party participation. Furthermore, the main goal of the smart contract is to provide a decentralized environment when there is not any trusted third party present, and it will automatically carry out the processes according to the corresponding triggering inputs. However, these mechanisms all deploy the public and private keys in the smart contract through the certificate authority. Based on the fact that the smart contract is public and accessible to all participants, this means that everyone can access all information stored in the smart contract. As a result, counterfeiting may occur during the signing, and direct deciphering may be possible during encrypting the votes. Therefore, these mechanisms do not meet the security requirements of confidentiality and authentication.

On the other hand, the proposed mechanism meets all the listed security requirements and is proven to be feasible. Further verification of the feasibility of such a mechanism will be conducted through simulation and demonstration in the next section.

5. Simulation and Demonstration

This study proposes an electronic voting mechanism. In this section, the feasibility of the proposed mechanism will be verified through simulation and demonstration. The testing blockchain environment was established by using the Truffle Suite Ganache tools. The smart contract was developed by using the Solidity scripting language in the Remix online development environment. Subsequently, the MetaMask crypto wallet was registered and the smart contract was deployed on the Ganache simulated blockchain. Finally, the decentralized application (Dapp) for voting was developed by utilizing the Web3.js libraries for interacting with the Ethereum network. The following subsections describe the implementation of simulations for the 5 stages of the proposed voting mechanism.

5.1 The Initialization Stage

The initialization stage includes two parts, deploying the smart contract and registering the voting participants. For deploying the smart contract, the following steps are completed.

- Start Ganache to establish the testing blockchain, and set the network name and port number on the setting page,
- Use Remix and Solidity to implement the contract of the election organization,
- Select “Injected Web3” in the environment column of the deployment function settings and select the contract name to be deployed in the contract column, and
- Deploy the contract on the Ganache testing blockchain through the browser extension program MetaMask.

For registration, all participants register with the certificate authority through the decentralized application. A screenshot of the simulated registration process is shown in **Fig. 2**.

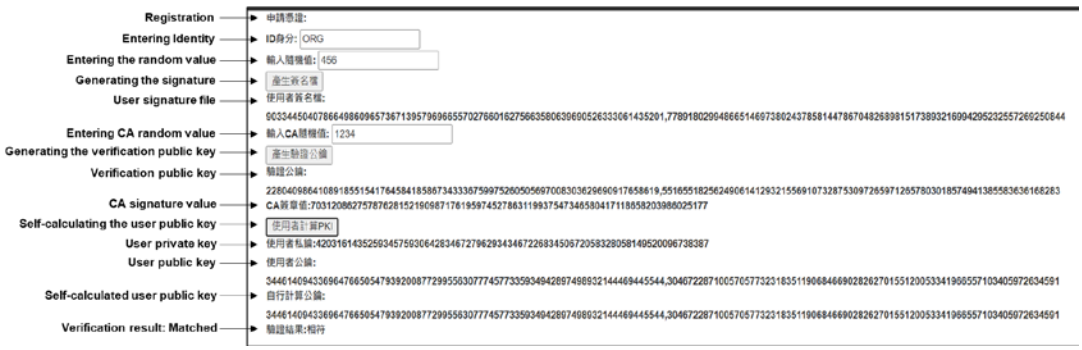

Fig. 2. A screenshot of the simulated registration process

5.2 The Ballot Collecting and Voting Stage

All participants need to mutually self-certify the identities of each other before interactions. Taking the voter and the election organization as an example, the voter first sends the identity id_V, the verification public key VPK_V, and the public key PK_V to the election organization for identity certification. After the process succeeds, the election organization similarly sends the identity id_{ORG}, the verification public key VPK_{ORG}, and the public key PK_{ORG} to the voter for identity certification. The mutual identity certification process is shown in **Fig. 3**. Subsequently, the voter collects the ballot and enters the voting page. After the randomly-chosen blinding factor is generated and an option is selected, the vote is submitted and the process is completed (as shown in **Fig. 4**).

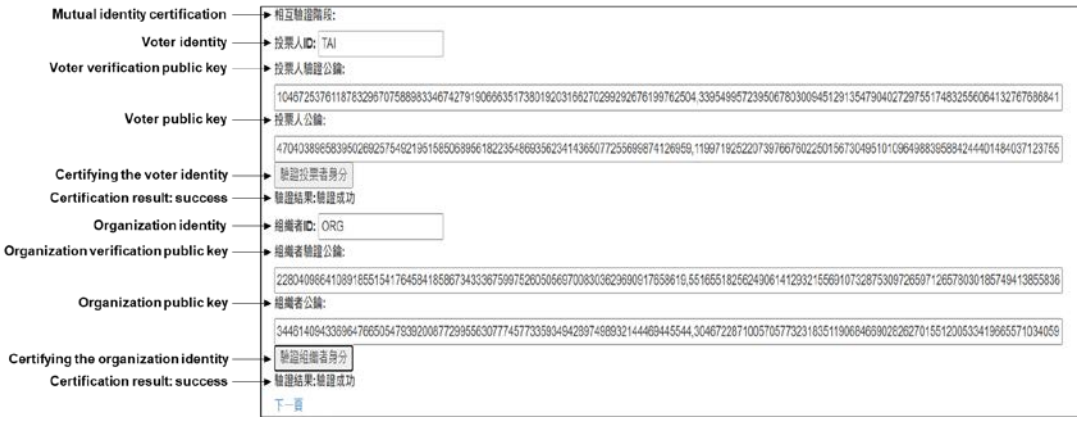

Fig. 3. A screenshot of simulated mutual identity certification between the voter and the election organization

Fig. 4. A screenshot of simulated voting

5.3 The Blinding and Signing Stage

After the voter clicks "submit" at the previous stage, the blinding factor bf, the public key PK_{TS} of the time server, and the one-way collision-free hash function $h_2()$ are used to generate the encrypted voting information w and to conduct the blinding process. The program for the blinding process is shown in **Fig. 5**. The blinded encrypted abstract document W is then sent to the election organization for signing. The program for the signing process is shown in **Fig. 6**. After signing, the election organization sends the relationship value R and the signed document S back to the voter.

```
//投票選用盲因子bf，盲化投票訊息w，產生盲化後之密文摘要W ←— Adopts a blinding factor bf to blind the voting information w,
                                                            and produces the blinded encrypted abstract document W
function CastVote(){
    var S_option = get_SelectOption(document.querySelector('input[name="candidate"]:checked').value);
    var blind = get_ng(bf, PKts, 0n, secp_p);
    //w = hash(k * PKts || S_option)，hashFunction : web3.utils.soliditySha3
    var W = BigInt(web3.utils.soliditySha3({t:'string', v:blind.x.toString(16)}, {t:'string', v:blind.y.toString(16)}, {t:'string', v:S_option}));
    var W = get_ng(w, secp, 0n, secp_p);
```

Fig. 5. The program for the blinding process

```
//ORG簽章產生關聯值R，簽章文件S ←— Signs the document W, and produces the relationship value R
var R = Sign_W(W)[0];                and the signed document S
var S = Sign_W(W)[1];
function Sign_W( W ){
    return [get_ng(random_org, W, 0n, secp_p), get_ng((sk_org+random_org),  W, 0n, secp_p)];
}
```

Fig. 6. The program for the signing process

5.4 The Unblinding Stage

After receiving the relationship value R and the signed document S, the voter uses the public key PK_{ORG} of the election organization to generate the unblinding point wPK for the voting information w. The program for the unblinding process is shown in **Fig. 7**. Subsequently, the unblinding point wPK, the relationship value R, and the signed document S are deployed on the Ganache testing blockchain through the use of Web3.js and MetaMask to summon the smart contract for providing the voting participants to conduct the verification on their own. A screenshot of the simulated deployment process is shown in **Fig. 8**.

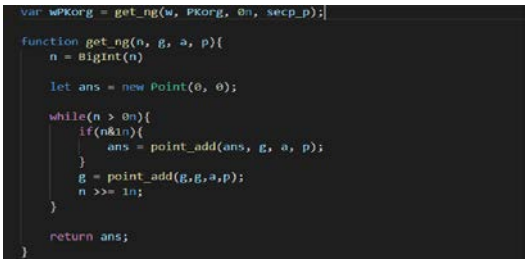

Fig. 7. The program for the unblinding process

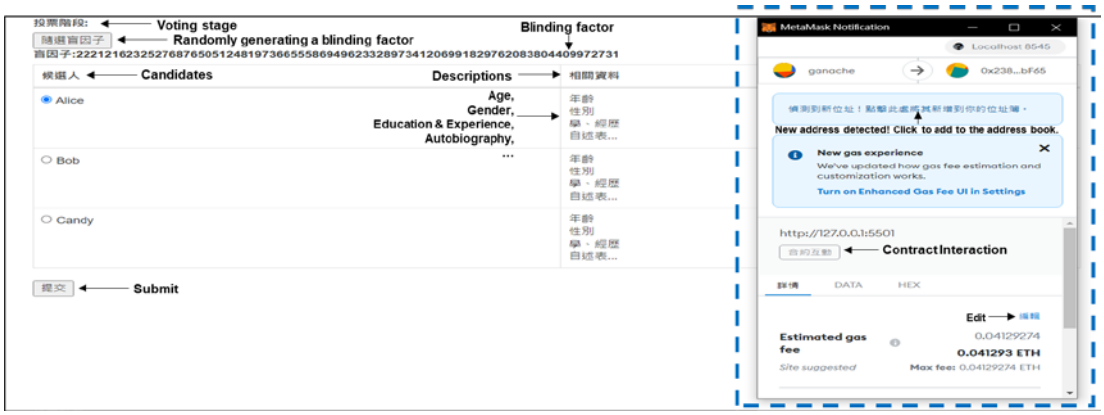

Fig. 8. A screenshot of the simulated data deployment on the blockchain after voting

5.5 The Verifying and Counting Stage

At the verifying and counting stage, after the time server and the election organization mutually self-certify the identities of each other (as shown in **Fig. 9**), the election organization sends the transaction address $addr$, the encrypted blinding factor BF, and the verification values of all voting options $options$ to the time server. Subsequently, the time server uses the transaction address $addr$ to obtain the unblinding point wPK from the blockchain through the smart contract and uses its private key sk_{TS} and the public key PK_{ORG} of the election organization to compute a collection of points wPK' to be compared with and to verify each wPK. A screenshot of the simulated counting process is shown in **Fig. 10**.

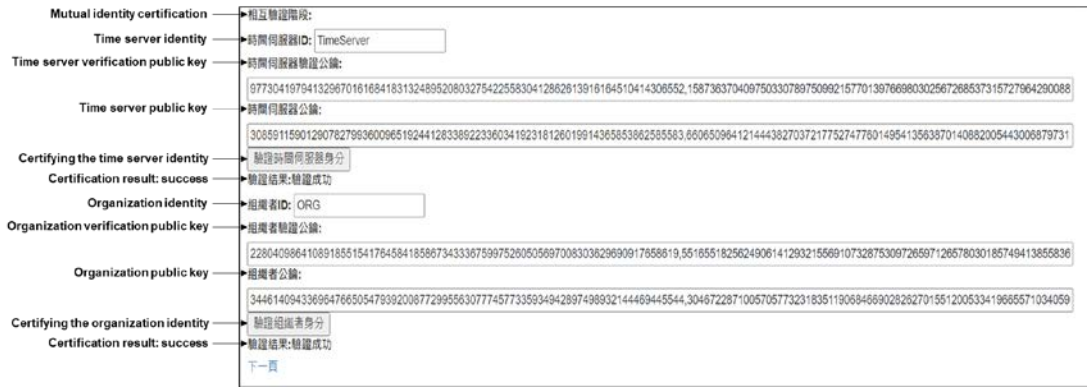

Fig. 9. A screenshot of simulated mutual identity certification between the time server and the election organization

Fig. 10. A screenshot of the simulated counting process

6. Conclusion

The main contribution of this study is the design of an electronic voting mechanism that meets all security requirements discussed in Section 4. The specific features of the mechanism are briefly described as follows. (1) Blockchain technology is incorporated to avoid the issues associated with the verification of the voting process through a trusted third party. (2) The elliptic curve cryptography is adopted to provide higher efficiency on the premise that the same level of security is reached (compared with the RSA cryptography). (3) A self-certification mechanism is introduced for identity certification to prevent the certificate authority as a trusted third party from selecting the private key on behalf of the voter and counterfeiting the voter's identity, and to reduce the cost and risk of the overall certification system in storing, calculating, and managing public keys.

A consideration for future work may be conducting extensive analyses and validation of the proposed mechanism by testing and evaluating its performance and limitation with the real-life numbers of participants as well as different voting scenarios to ensure that it serves its purpose.

References

[1] J. W. Liu, "Opportunity, Challenge and Future of Promoting Electronic Voting in Taiwan," *Taiwan Democracy Quarterly*, vol. 16, no. 1, pp. 155-162, 2019. Article (CrossRef Link)

[2] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in *Proc. of the 18th Annual International Conference on Digital Government Research*, pp. 574-575, 2017. Article (CrossRef Link)

[3] W. J. Juang, "Does technology promote democracy? Analysis of the public's perception of the relevance of democratic development with adopting electronic voting," *Taiwan Democracy Quarterly*, vol. 18, no. 1, pp. 83-140, 2021. Article (CrossRef Link)

[4] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, Springer, Boston, MA, 1983, pp. 199-203. Article (CrossRef Link)

[5] F. G. Jeng, T. L. Chen, and T. S. Chen, "An ECC-based blind signature scheme," *Journal of Networks*, vol. 5, no. 8, pp. 921-928, Aug. 2010. Article (CrossRef Link)

[6] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008. Article (CrossRef Link)

[7] V. Buterin, "A next-generation smart contract and decentralized application platform," 2013. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[8] N. Szabo, "Smart contracts: building blocks for digital markets," 1996. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[9] D. Johnston, S. O. Yilmaz, J. Kandah, N. Bentenitis, F. Hashemi, R. Gross, S. Wilkinson, and S. Mason, "The general theory of decentralized applications, DApps," 2014. [Online]. Available: https://cryptochainuni.com/wp-content/uploads/The-General-Theory-of-Decentralized-Applications-DApps.pdf

[10] M. Girault, "Self-certified public keys," in *Proc. of EUROCRYPT 1991: Advances in Cryptology — EUROCRYPT '91*, pp. 490-497, 1991. Article (CrossRef Link)
[11] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system" *Future Generation Computer Systems*, vol. 105, pp. 13-26, Apr. 2020. Article (CrossRef Link)
[12] F. Song and Z. Cui, "Electronic voting scheme about Elgamal blind-signatures based on XML," *Procedia Engineering*, vol. 29, pp. 2721-2725, 2012. Article (CrossRef Link)
[13] B. C. Xie and Z. W. Luo, "On the anonymity of Song and Cui's electronic voting scheme," in *Proc. of Symposium on Enterprise Architecture and Information Technology*, New Taipei, Taiwan, 2012.
[14] A. Waheed, N. Din, A. I. Umar, R. Ullah, and U. Amin, "Novel blind signcryption scheme for e-voting system based on elliptic curves," *Mehran University Research Journal of Engineering & Technology*, vol. 40, no. 2, pp. 314-322, Apr. 2021. Article (CrossRef Link)
[15] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," *Cryptology ePrint Archive: Report 2017/1043, International Association for Cryptologic Research*, 2017. Article (CrossRef Link)
[16] Y. K. Dong, D. W. Zhang, Z. Han, and L. Chang, "Board voting system based on the consortium blockchains," *Chinese Journal of Network and Information Security*, vol. 3, no. 12, pp. 31-37, 2017. Article (CrossRef Link)
[17] T. Yu, C. Cao, L. Wang, and L. Xu, "An anonymous electronic voting scheme based on alliance chain," *Cyberspace Security*, vol. 10, no. 12, pp. 22-29, 2019.
[18] Z. Zhou and G. L. Yan, "An anonymous electronic voting protocol design," *Software Guide*, vol. 19, no. 1, pp. 229-233, 2020.
[19] G. Wood, "Ethereum: A secure decentralized generalised transaction ledger," 2014. Article (CrossRef Link)
[20] Election Assistance Commission, "Voluntary voting system guidelines," 2021. [Online]. Available: https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines
[21] K. T. Sri, K.R. Sri, and N. Pedamallu, "E-voting system using blockchain," *Journal of Xi'an University of Architecture & Technology*, vol. 13, no. 5, pp. 527-533, May 2021.

Chuan-Hao Yang currently serves as an Assistant Professor with the Department of Information Management, National Defense University, Taiwan, and as a Lieutenant Colonel with the Taiwan Army. He received his B.S. degree from the National Defense University, Taiwan in 1991 and his M.S. and Ph.D. degrees from the Naval Postgraduate School, Monterey, CA, US, in 2005 and 2014, respectively. His original research interests include Virtual Reality, Modeling and Simulation, Mobile Robots, and Human-body-motion Tracking using inertial/magnetic sensors. Currently, he is also working in the fields of Information Technology (e.g., Information Security, Data Hiding, Blockchain Technology, etc.)

Pin-Chang Su currently serves as a Professor with the Department of Information Management, National Defense University, Taiwan. He received his Ph.D. degree in Electrical Engineering from Chang Gung University, Taiwan in 2007. His research mainly focuses on Algorithm Design in Error-Control Coding, Information Security, Cryptographic Systems, and E-Commerce Technologies. His published articles can be found in most academic journals like KSII Transactions on Internet and Information Systems, Computers and Electrical Engineering, Security and Communication Networks, Applied Mathematics and Computation, Journal of e-Business and so forth.

Tai-Chang Su is a young researcher, currently serving as a MIS Manager at the National Defense University, Taiwan. He received his master's degree in management science from the Department of Information Management, National Defense University, Taiwan in 2022. His major research interests include Blockchain Technology, Algorithm Design, and Cryptographic Systems.