An On-Site Electronic Voting System Using Blockchain and Biometrics

Shu-Fen Tu
Department of Information Management, Chinese Culture University, Taiwan
dsf3@ulive.pccu.edu.tw

Ching-Sheng Hsu
Department of Information Management, Ming Chuan University, Taiwan
cshsu@mail.mcu.edu.tw

Bo-Long You
Department of Information Management, Ming Chuan University, Taiwan
wghl747pop9@gmail.com

Abstract: *Electronic voting (e-voting) improves the convenience of voting and the efficiency of vote counting. With the rise of blockchain technology, many studies have proposed e-voting systems using blockchain technology. Most of them consider the usage scenario of remote voting and pay less attention to that of voting conducted at polling stations. In view of this research gap, this study proposed a blockchain-based system for e-voting at polling stations. We designed a system process integrating blockchain technology and voter's biometrics to prevent data tampering and imposter voting. In addition, the blockchain platform adopted in our proposed system is Hyperledger Fabric (HF). Therefore, based on the HF framework, we specified how to deploy a blockchain network customized for this study. Finally, this study provided a property analysis of the proposed system and implemented a simulation system. In conclusion, the proposed system meets the requirements e-voting from two aspects. First, in terms of technology, our system adopted blockchain, digital signature, and biometric identification to achieve eligibility and immutability. Second, in terms of system process, the roles of government agencies and inspectors are incorporated to achieve transparency, receipt-freeness and accessibility.*

Keywords: *Blockchain, biometric, distributed ledger, e-voting.*

Received June 19, 2022; accepted February 26, 2023
https://doi.org/10.34028/iajit/20/5/13

1. Introduction

Voting is a way for citizens to express their opinions and to translate those opinions into results. Conventionally, voters need to collect and cast their paper ballots at the designated voting booth, and the number of votes each candidate receives is counted manually at the end of voting. Such paper-based voting system makes the voting procedure very time-consuming and is criticized for being error-prone and manipulation-prone as well. Therefore, more and more researchers have tried to use Information and Communication Technologies (ICT) to propose electronic voting (e-voting) systems [15]. With an e-voting system, the votes can be casted electronically and tallied automatically. Obviously, an e-voting system can enhance the efficiency of entire voting procedures. Moreover, automated vote counting is less likely to make mistakes than manual vote counting. Initially, most e-voting systems adopted centralized databases to record votes. However, a centralized e-voting system is vulnerable to attacks and manipulation, which makes voting results unreliable. Recently, an emerging blockchain technology has rapidly become a solution to unsolved issues with transparency, privacy, and data integrity of centralized e-voting systems. Blockchain is a decentralized and distributed digital ledger, and its data structure is a linked list of blocks. Each block contains transaction data and a cryptographic hash of the previous block. Such data structure and some cryptographic methods provide the ability for a blockchain to retain an unalterable history of transactions. Decentralization makes blockchain not vulnerable to attacks and manipulation, and immutability makes data stored in the blockchain trusted. Therefore, some studies make endeavors to design blockchain-based e-voting systems.

The model of e-voting can be classified into remote user interaction or voting station engagement [15]. The former model means that a voter can vote from anywhere using a digital device with a voting system installed, while the latter means that a voter needs to go to a designated polling station and cast their ballots using a machine prepared at a polling booth. It is usual that low turnout leads to a bias in electoral outcomes, and bias is considered as a serious democratic problem. Obviously, remote e-voting is convenient for voters and therefore may strengthen voter participation and increase voter turnout. Since ICTs enable anytime and anywhere access to information and resources, and blockchain technology facilitates online trust, there have been numerous efforts to develop remote e-voting systems based on ICTs and blockchain [2, 10]. However, an e-voting system that supports free and fair election should not only consider the integrity of ballots and accessibility to every eligible voter, but also other issues [13]. Summarizing several studies, the requirements that an ideal e-voting system should satisfy include [2, 7, 14, 16, 17, 22, 26, 30]:

1. Eligibility: only qualified voters can vote, and only valid ballots are counted.
2. Transparency: the whole process is clear and easy to understand for all stakeholders.
3. Immutability: the system should prevent ballots from being manipulated or tampered with.
4. Receipt-freeness: voters cannot be linked to their casted ballots so that they cannot show how they vote. This is a basic feature of realizing vote-selling and voter-coercion resistance.
5. Accessibility: all eligible voters can participate in voting.

Since remote e-voting allows voters to participate in voting from anywhere, it is difficult to ensure a secure physical environment and hence is vulnerable to vote-selling and vote-coercion. A few studies proposed a strategy to achieve receipt-freeness in remote e-voting [6, 26]. However, supervision is still a more effective means for the security of the physical environment. On the contrary, e-voting conducted from polling stations is easy to be supervised, thus reducing the chance of manipulation. Especially for large and important national elections, official supervision is very important to prevent vote-selling or coercion. The existing remote e-voting system may be portable to polling stations, but some security concerns may arise. For example, if voters use their mobile phones to vote, they inform the voting buyers of their vote. As another example, if voters use the officially approved *e-voting* machine at the polling booth, they may deliberately leave their ballot on the screen, so that the next person who enters the booth can vote for them. Therefore, using the existing remote e-voting system may not be appropriate because the process of voting at a polling station is not exactly the same as that of remote voting. In conclusion, conducting e-voting at voting stations is still necessary. However, research devoted to designing a blockchain-based system for e-voting with polling station engagement is not much. Another concern about security is voter impersonation. Whether it is paper-based voting or e-voting, voters need to rely on some kind of credentials or tokens to pick up their ballots. A vote may give the voting credential to someone else and let that person vote for him/her. In this study, anti-impersonation is classified as one of the eligibility criteria since impostors should be regarded as ineligible voters.

We therefore reasonably conclude that an e-voting system customized for the voting process at polling stations is necessary. However, most recent research is devoted to remote e-voting systems. Considering transparency and immutability of e-voting, blockchain has been recognized as an ideal solution. Therefore, the aim of this paper is to propose a blockchain-based system to support e-voting at polling stations. The traditional centralized database may face the problem that a single node will be destroyed or tampered with and cannot be restored. The distributed database mainly provides a backup mechanism, but there is no mechanism to prevent data from being tampered. Therefore, using the traditional database management system in e-voting will cause security and trust problems. Blockchain is a decentralized ledger, and its storage structure is a linked list of blocks. In addition to recording data, each block also records a time stamp and the hash value of the previous block, so that the blocks have a strict order. Any newly generated block must be agreed by all nodes in the network before it can be written into the ledger. These features enable blockchain to replace traditional databases and provide the trust and security required by e-voting systems. There are various blockchain platforms, and this study adopted Hyperledger Fabric (HF) because HF has numerous features that benefit e-voting scenarios, which will be explained later. In addition, this study employed biometric authentication to prevent in-person voter impersonation. As a result, our system does not only satisfy the requirements of eligibility, transparency, immutability, and receipt-freeness, but also prevent the security flaws mentioned above. Narrowly speaking, our system also achieve accessibility because all eligible voters are allowed to vote at the polling station. There is an assumption to be made in our proposed system that every voter has a mobile phone. This is because voting credentials are electronic and need to be stored and carried using a mobile phone. Another research assumption is that all polling stations conduct e-voting. That is, the situation that e-voting and paper-based voting can be paralleled in the same polling station is not considered.

In this study, the general election in Taiwan is used as a scenario to illustrate our system process and architecture. Therefore, we give a brief snapshot of the election process and involved institutions in Taiwan. The current voting regulation in Taiwan is to use paper ballots and vote at polling stations in the place of residence. The regulations on voting are mainly based on “Presidential and Vice Presidential Election and Recall Act” [24], “Civil Servants Election and Recall Act” [4] and “Referendum Act” [25]. According to these laws and regulations, each eligible voter needs to collect the ballot with his or her identity card, personal chop, and voter notification at the designated polling station within the specified voting period. Then, the voter will secretly mark a candidate on the ballot paper in a polling booth with an officially prepared tool, and then put the ballot into the ballot box outside the polling booth to complete the voting process. Basically, there are two institutions involved in the election process: the Central Election Commission (CEC) and the Household Registration Authority (HRA). Roughly speaking, the tasks of the CEC include organizing election, sending voter notification and candidate information to voters, and announcing the result of election. The HRA is the institution that manages household registration records

of every citizen and governs household registration offices, which are responsible for issuing identity cards and citizen digital certificates. Citizen digital certificate is a smart Integrated Circuit (IC) card, which contains an algorithm to calculate digital signature and public key, and the private key is stored eternally in the IC chip.

The remainder of this paper is organized as follows. In section 2, the concept of blockchain and HF were introduced, and current blockchain-based e-voting systems were reviewed, especially those supporting e-voting at polling stations. In section 3, the general framework of the proposed e-voting system is described in detail. Section 4 is property analysis of the proposed e-voting system. Section 5 provides a case study and implementation of the framework. Finally, conclusions are provided in section 6.

2. Related Works

2.1. Blockchain Platforms

The concept of blockchain originally came from Satoshi Nakamoto's paper "Bitcoin: A Peer-to-Peer Electronic Cash system" [20]. Gradually, the blockchain technology attracts more and more attention due to the rise of Bitcoin. The blockchain can be regarded as a decentralized ledger composed of linked data blocks which are generated by cryptography technology. This decentralized ledger is shared by multiple participants, and each participant is responsible for maintaining and updating a synchronized copy of the data. So far, according to different degree of access restrictions, three blockchain platforms have been developed, which are public, private, and consortium blockchain. Public blockchain is completely decentralized and permissionless; thus, anyone can join the blockchain network without permission and participate in the process of transaction and consensus. To build trust, public blockchain uses a complex mathematical mechanism to make the ledger extremely difficult to tamper with, which limits its throughput. Openness can be a double-edged sword. Because everything recorded on the ledger is permanent and can be queried by any node of blockchain network, public blockchain is not suitable for storing private data. The classic representatives of public blockchain are Bitcoin and Ethereum. Private blockchain is in stark contrast to the public blockchain. Every node needs to get permission to join the private blockchain network. Since participation is restricted, its throughput is efficient. Private blockchain is not considered decentralized and is used in a single enterprise or organization.

Similar to private blockchain, consortium blockchain is also permissioned but governed by a group of organizations rather than a single entity, like in the case of private blockchain. As a result, consortium blockchain has a greater degree of decentralization than private blockchain, resulting in stronger security. In addition, since the participants are limited to a group of organizational alliances, consortium blockchain can adopt a more efficient consensus mechanism than that of public blockchain. These characteristics make the consortium blockchain very suitable for applications in business scenarios, so it is increasingly valued by enterprises. HF, one of enterprise-grade blockchain software projects hosted by The Linux Foundation, is a well-known consortium blockchain platform. There are several features, as explained below, to make HF achieve efficient performance and can be customized to suit various business scenarios. The traditional consensus model of blockchain platforms is "order-execute", which means that all nodes first reach a consensus on the order of transactions and then execute transactions in order. Such sequential execution style usually causes significant impact on latency of confirmation. Different from the traditional, HF uses execute-order-validate model, in which transactions are executed and endorsed before ordering and confirming whether there is a conflict. As long as there is no conflict, the status of the ledger will be updated. Such model is more effective than the traditional model, and it can support flexible trust assumptions. International Business Machines Corporation (IBM) has demonstrated that HF can reach a maximum transaction throughput of 2000 transactions per second [31]. Moreover, HF provides pluggable consensus modules, so that enterprises or organizations can choose appropriate modules according to their application needs. In addition, HF does not require native cryptocurrency, and hence can get rid of cumbersome mining operations [7]. Furthermore, HF provides the channel mechanism to make transactions private between designated parties. Each channel has its own ledger, and there may be multiple channels between consortium members connected to the same network [11]. Finally, HF enables the use of smart contracts to define and perform business logic in blockchain networks and provides smart contract APIs for various general-purpose programming languages. That means most developers already have the ability to write smart contracts. As a consequence, HF is a suitable blockchain platform for developing e-voting systems in terms of confirmation latency, privacy, confidentiality, and smart contracts [7].

2.2. Blockchain-based E-Voting System

E-voting means that marking ballots, casting, or counting are conducted in an electronic way with the aid of digital devices. The digital device may be a standalone voting machine, a computer or mobile device connected to the Internet. The degree of automation may at least facilitate vote casting or encompass the full function of casting, counting, and tabulating results. With the rapid development of ICT, full automation of voting is easily realized. Voters can vote from anywhere and anytime using their mobile device with the required

voting system and Internet connection. Khan *et al*. [15] classified such scenario of e-voting as remote user interaction, and the opposite is voting station engagement, in which voters go to the polling station to vote using the deployed voting system. Since remote e-voting can best reflect the merits of ICT, many researchers have devoted themselves to the study of remote e-voting. Early studies of remote e-voting systems adopted a centralized system architecture, whose privacy and availability were a concern. Once the single central server fails or suffers an attack, the whole system will not work correctly, and the system storage will be at high risk of information leakage. When blockchain appears, its decentralization characteristics improved the shortcomings of the centralized architecture, and its immutability and traceability make blockchain a trust mechanism of e-voting. Therefore, blockchain has gained more and more adoption in studies related to an e-voting system. Various types of blockchain platforms were adopted in blockchain-based e-voting systems [2], among which Ethereum and HF are the two most popular. However, conducting transactions on Ethereum needs to be charged in gas, which causes potential expenses or additional overhead from managing virtual currency. Su and Su's e-voting system used Ethereum to build a private blockchain network [29]. Although a private Ethereum blockchain may be more efficient than a public Ethereum blockchain, Schäffer et al.'s study has shown that due to the bottleneck of the design architecture of the private Ethereum blockchain, the scalability of the Ethereum private chain is limited [28]. Thus, Ethereum may not be suitable for large scale elections [23]. We have also observed that there are many recent blockchain-based e-voting studies adopting HF [3, 7, 9, 18, 19, 22].

Remote e-voting can facilitate voters to vote but also challenges fair and free elections due to unsupervised. In the absence of supervision, some illegal behaviors, such as vote-selling or vote-coercion, are difficult to prevent. Receipt-freeness is an essential property for a remote e-voting system to prevent vote-selling and vote-coercion [6, 26]. Receipt-freeness means that an e-voting system leaves no clue to voters to demonstrate their voting strategies to others. Although some studies related to remote e-voting have proposed various methods to prevent vote-selling or vote-coercion, it is reasonable to assume that the most effective way against vote-selling or vote-coercion is to provide a secure physical voting environment. As long as voters do not use the preventive mechanism of the e-voting system and are willing to let others monitor their voting process, receipt-freeness will be difficult to achieve. Yu *et al*. [30] utilized cryptographic techniques, such as Paillier encryption, proof-of-knowledge, and linkable ring signature, to deal with issues of security and coercion-resistance. However, their security analysis is based on the assumption that the physical environment is secure. That is, no one stands by voters to watch, and voters do not let others vote for them. Clark and Hengartner [6] adopted a 5-Dictionary panic password system [5] to resist vote-coercion. A panic password is not the true password but is indistinguishable from the true password from the user's view. Therefore, voters can give a panic password to a coercer, and the coercer has no idea whether the password is true or not. Before a voter can be recognized as eligible by the system, a one-time registration process needs to be completed in person at a private booth. During registration, the true password and its corresponding panic passwords for a voter are decided. The above studies have shown that a secure physical environment still needs to be involved in the e-voting system processes.

Unlike remote-e-voting, supervision e-voting constraints voters to cast only under oversight at a designated location, i.e., polling station [21]. There is not much recent research on supervision e-voting systems. De los Santos *et al*. [8] developed an e-voting system, called e-voting kiosk, to support election for the Supreme Student Government in the university. However, their system was implemented in a centralized network architecture, where multiple voting kiosks are connected to a single database and application server. To improve the existing paper-based voting in Poland, Pawlak and Poniszewska-Maranda [22] employed the HF to design an auditable system architecture to support supervised e-voting at polling stations. The voting applications are installed in polling stations, and voters use the application to vote with their own tokens. Before voting, voters need to obtain a voting credential from local offices, which is a one-time numerical code, called Vote Authentication Token (VIT). With their VIT, voters use the certified voting application at a polling station to select a candidate. All votes are transmitted to blockchain and recorded. Pawlak and Poniszewska-Maranda's scheme allowed voters to vote again, as long as they get an unused authorized VIT. However, voters are identified only when obtaining voting credentials from local offices. If someone gives the VIT to others, others can vote for that person with this VIT. Even if the VIT is not given to anyone else, the voter may deliberately leave the ballot on the screen, and the next person using the app can vote for the voter as well. Adewale Olumide *et al*. [1] proposed an e-voting system to prevent voters from impersonation and multiple voting by using the voter identification number card and fingerprint for authentication and as voting credentials. However, their system adopted a centralized database to store all relevant data. Ruparel *et al*. [27] adopted Ethereum to build a secure and transparent e-voting system. In the registration phase, the personal details and biometrics of voters are verified by the Electronic Registration Officer (ERO) and then stored on blockchain. Afterwards, voters will obtain a vote-token as a voting credential so that they can cast ballots through their mobile wallet application. Ruparel *et al*. [27] said that voters can vote at polling stations as well,

but detail voting process at polling stations was not specified in their paper. In addition, Ruparel *et al*. [27] designed a multi-signature authentication to provide additional security for votes. Before recording on blockchain, every vote was encrypted with the voter's private key and public keys of Polling Office (PO) and all candidates. Therefore, before tallying, every vote is required to be decrypted with the voter's public key and private keys of PO and all candidates. However, such multi-signature authentication violates the rule of receipt-freeness because each ballot is linked to the voter through the public key. Indrason *et al*. [12]'s e-voting system used fingerprints to authenticate voters and required facial recognition to complete ballot submission. Although Indrason *et al*. [12] utilized biometrics to prevent impersonations, their scheme is put forward for voting scenes without polling stations. It is not easy to prevent voters from being monitored and hence leaves a loophole for vote-selling or vote-coercion. Besides, Indrason *et al*. [12] did not clearly specify which blockchain platform was adopted in their system.

3. The Proposed System

In the case of e-voting, ballots are electronic; so, inside the booth, there is a voting machine provided by CEC instead of the seal. Voters use the voting machine to select and submit their preferred candidates.

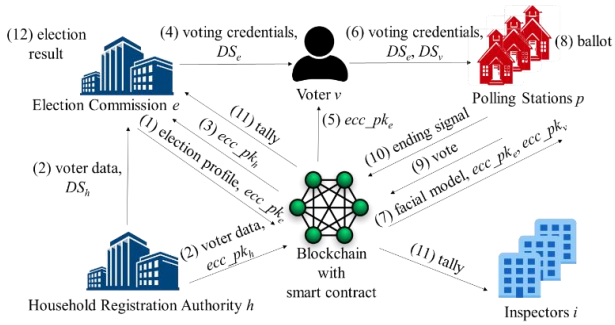

Figure 1. The whole process of the proposed e-voting system.

3.1. System Process

Before explaining the proposed e-voting system, we make some assumptions about our system. Firstly, every citizen has their own public and private key, and the HRA keeps a copy of public keys of citizens. Secondly, the HRA can build facial models of voters because, in Taiwan, every citizen has a headshop on their own identity card. For the sake of explanation, let us first introduce the symbols to be used.

e: CEC which is responsible for various election affairs
h: HRA which is responsible for managing personal data of the whole nation
p: polling stations, in which qualified staffs are put on duty to assist with on-site affairs and voting machines are prepared inside the voting booths
i: any institution that has the right or is allowed to inspect the process of election, such as congress or the media
v: a voter
ecc_pk_u: ECC (Elliptic Curve Cryptography) public key of role *u*
ecc_sk_u: ECC private key of role *u*
DS_u: digital signature of role *u*, and DS_u=Enc(H(*m*), ecc_sk_u)
TS: a timestamp
Enc(*m*, *k*): encryption function, which encrypts message *m* with key *k*
Dec(*m*, *k*): decryption function, which decrypts message *m* with key *k*
H(*m*): SHA-256 hash function, which generates digital digest of message *m*

Figure 1 depicts the entire election process with the involvement of the proposed e-voting system. The whole process can be divided into three phases, and the details of each phase are illustrated as follows.

a. Before voting

1. The CEC *e* is responsible for initiating the election and writes the election profile and its public key ecc_pk_e on blockchain. The election profile records all the information that needs to be known by voters, such as candidate lists, type of the election, and where and when to hold the election.
2. The HRA *h* provides data of eligible voters along with its digital signature DS_h to *e* and, at the same time, writes the data and its public key ecc_pk_h on blockchain. The voter data include necessary personal information and voters' public keys and facial models.
3. After receiving the data of voters, *e* reads ecc_pk_h from blockchain to verify the data and DS_h. If verification is successful, *e* will produce the voting credentials for each voter, which records the voter's ID and the designated polling station.
4. Election Commission (EC) *e* delivers each voting credential along with its digital signature DS_e to respective voter.
5. A voter *v* can verify the voting credential and DS_e with ecc_pk_e stored on blockchain upon receiving.

b. During voting

6. Voter *v* brings the voting credential along with DS_e and DS_v to the designated polling station. Precisely speaking, it is the QR code containing the voting credential, DS_e and DS_v that *v* brings to the polling station. The QR code is generated and kept using the mobile app.
7. To be eligible to vote, *v* is required to show the QR code and face to be checked against the voter data stored on blockchain.
8. Once *v* passes the verification, the poll worker will generate a new electronic ballot and randomly

assigns it to a voting machine. Note that *v*'s mobile phone will be temporarily kept at the receipt desk to prevent *v* from taking photos at the voting booth.

9. Voter *v* enters the voting booth where the machine is located, chooses a candidate, and casts the ballot by using the machine. Once *v* has cast the ballot, the vote and its associated polling station code will be written on blockchain. If *v* does not select any candidate, the casted ballot will certainly be regarded spoiled and will not be tallied at the end of voting. Note that *v* may leave the booth without casting the ballot on purpose. If the ballot is left on the machine, it will give the next voter in the booth a chance to vote instead. To prevent such a situation, any ballot left on the machine will be automatically casted and recorded on blockchain once a new ballot is assigned to this machine or the ending signal of the polling station is sent. If no candidate is selected on this ballot, it is also certainly considered spoiled. By doing so, we can prevent probable vote selling and buying and, at the same time, ensure that the number of casted ballots matches that of issued ballots. In addition, when a vote is recorded on blockchain, the total votes received by each candidate are tallied automatically by the smart contract.
10. A polling station *p* sends an ending signal to blockchain when times up or all voters inside the polling station area at the time of close of voting complete voting.

c. After voting

11. When all ending signals from polling stations are collected, the smart contract closes the voting, and EC *e* reads the tally sheet from blockchain. Some institutions, which are allowed to inspect the tally sheet, can query the tally sheet from blockchain as well.
12. EC *e* announces the election result in accordance with the tally sheet.

3.2. System Architecture

The proposed e-voting system adopted HF as the underlying blockchain platform. HF provides a number of Software Development Kits (SDKs) for several general-purpose programming languages. As shown in Figure 2, front-end users interact with HF through applications, and applications send requests to and receive responses from HF blockchain network via various Application Programming Interfaces (APIs) provided by client SDK. Figure 3 shows the multi-host deployment of HF blockchain network, which includes a cluster of orderers and an organization consortium composed of EC, HRA, and Inspector. Currently, there are several released ordering services, and this study adopted Raft, which is officially recommended by HF. Each node in the HF architecture plays different roles, including endorsers, committers, orderers, and Certificate Authorities (CAs). Orderers receive transactions from different application clients and are responsible for arranging them, packaging them into blocks, and providing crash-tolerant services. CAs are responsible for registration of identities and the renewal and revocation of certificates. The client application generates and signs a transaction proposal and then submits it to the endorser. The endorser verifies the identity and authority of the client, approves the execution result of the chaincode, and then returns the verification output to the client. Each peer node is default to be a committer and is responsible for submitting transactions and maintaining the ledger and state. Generally speaking, endorsers and committers are provided by the organizations in the consortium. Besides various service nodes, HF also contains a communication mechanism called application channel, which is used to keep a group of organizations private. Organizations in the same application channel can communicate privately and share the same ledger and chaincode for specific business purposes.

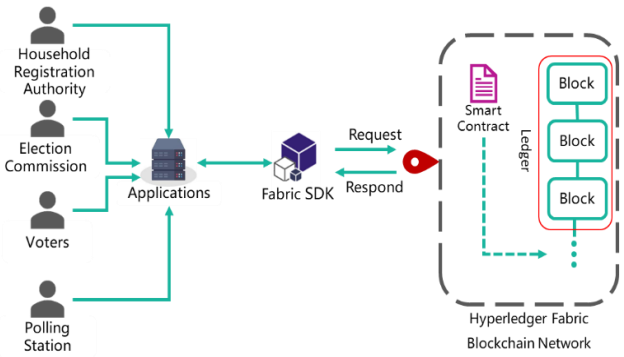

Figure 2. Illustration of interactions between users and the blockchain.

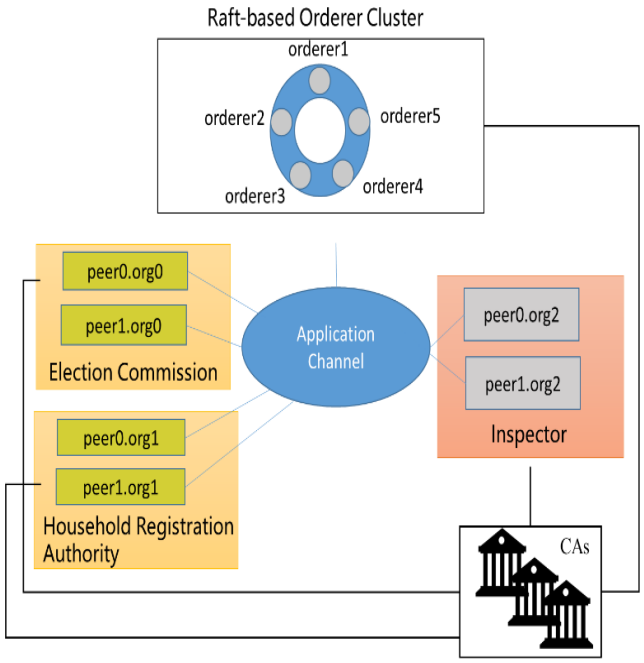

Figure 3. The multi-host deployment of HF blockchain network.

4. Property Analysis

In this section, we will analyze our proposed system based on the properties of an ideal e-voting system mentioned in the first section.

4.1. Eligibility

An ideal e-voting system should only allow eligible voters to participate in voting and only count valid ballots. A person is considered an eligible voter if he/she is listed on the electoral roll and can only vote with his/her own voting credential. That is, if someone on the electoral roll votes with other people's voting credentials, then that person is not an eligible voter. Our system protects against ineligible voters in many ways. First of all, the voter credentials are produced according to the voter data, and the voter data sent to the EC from the HRA, which is an official organization that records personal information across the country. Second, besides using digital signature to identify the voter credential, the proposed system also uses facial recognition to confirm that the holder of the credential is not an imposter. Third, the public keys and facial models are stored on blockchain to ensure the authentication is trustable. With regards to ballots, our system ensures that only valid ballots are counted in the following manner. First, ballots are sent to voting machines by the poll worker based on valid voting credentials, and the current ballot of a voting machine is uploaded to the blockchain as soon as the ballot is casted by the voter, or the next blank ballot or the ending signal of the polling station is sent. As a result, the final number of ballots sent out and the number of ballots collected must be kept in balance. Second, vote counting is performed by the smart contract, and only valid votes recorded on blockchain will be counted. In addition, the execution result of the smart contract needs to be validated by the service nodes of HF blockchain network.

4.2. Transparency

All transactions made on blockchain will be retained, and HF provides APIs for members of the consortium to read the transaction history. Generally speaking, in a democratic country, the actions of the government are scrutinized by public opinion and the media. Therefore, our system also includes the role of inspectors in the consortium, so that the overall voting operations can be supervised by external institutions and become more transparent.

4.3. Immutability

The immutability of the proposed system is mainly guaranteed by digital signatures and blockchain. All entities need to attach their digital signatures to the transmitted data so that the receivers can verify the sender and the data. In addition, all relevant data and public keys are stored on blockchain, which is recognized as a trusted and immutable platform.

4.4. Receipt-Freeness

After the voter's identity is verified by the poll worker, a blank ballot will be delivered to the voting machine. The proposed system does not and need not to record the voter's identity on the ballot. As the voting at polling stations is officially supervised, it can be ruled out that someone is watching behind the voters. In addition, at the end of voting, the voter's public key or private key is not required to unlock the voting. Therefore, each ballot has no connection with the voter.

4.5. Accessibility

The electoral roll is made by the CEC, and voting credentials are issued accordingly. That is to say, no eligible voters are excluded from our system. Therefore, as long as they can reach the polling place, every eligible voter can participate in voting.

5. System Implementation

According to the system process proposed in this study, we have implemented a simulation system, and some user interfaces are displayed below. The user interface of the electoral agency side is web-based, while that of the electoral side is a mobile application.

1. Before voting

Figure 4 shows the user interface of the electoral agencies to complete the pre-voting operations, including creating a voting event, uploading voter data, and delivering vote credentials to voters.

Figure 4. User interface for the pre-voting operations.

2. During voting

When the voter enters the polling station to prepare to vote, they need to use the mobile application to show the QR code to the poll worker, as shown in Figure 5. As mentioned earlier, the QR code contains personal information such as voter's voting credential and public

key. The poll worker uses the interface shown in Figure 6 to scan the QR code to verify the identity of the voter.

Figure 5. User interface of the voter's QR code.

Figure 6. User interface of scanning QR code.

3. After voting

Figure 7 shows the interface for the electoral agencies and inspectors to check the result of vote counting at the end of voting. Voters can use the mobile app to see the announcement from the EC about the voting result as shown in Figure 8.

Figure 7. User interface for querying the vote result.

Figure 8. User interface of the announcement of the vote result.

6. Discussions and Conclusions

Voting is the way for people to express their opinions, and it is also an important activity for democratic elections. Initially, people must go to a designated polling station to pick up their paper ballots with identification, choose a candidate on the paper ballots, and then cast the ballots into a ballot box. Later, with the maturity of information and communication technology, many researchers put forward various e-voting systems so that voting is not be limited by time and space. The emergence and launch of blockchain has overcome some shortcomings of traditional e-voting systems. At present, most blockchain e-voting systems mainly focus on the remote voting scenario. Although a remote voting system can facilitate voting, without official supervision, it is still difficult to prevent someone from monitoring voters and intending to influence their voting intentions. Because the procedure of remote voting is different from that of polling stations, it is not suitable to apply the remote voting system to polling stations. In this study, we designed a blockchain e-voting system for voting at polling stations based on the voting procedures of general election in Taiwan. The main characteristics of the system proposed in this study are summarized as follows. First, our system adopted HF as the blockchain platform, which is designed for use in enterprise contexts and recognized to be suitable for applying in e-voting. In addition, we explicitly mapped out the implementation framework of HF, which is rarely mentioned in other researches. Second, this study ensures the integrity and immutability of the data and prevents imposter voting from the perspectives of technology and system process. On the technical side, digital signature is adopted, so that everyone can verify the received data, and all relevant data were stored on blockchain, so that it is difficult for the data to be

tampered with. Besides, voter authentication not only relies on voting credentials, but also relies on biometric comparison to prevent others from fraudulent using voting credentials. In terms of system process, each ballot is either submitted by the voter or forcibly returned by the system if the voter does not submit it, so that no one has the opportunity to access the other's ballot. Third, the results of electoral votes must be credible before it can be accepted by the public. This study not only uses the blockchain as the trust mechanism of the system, but also adds the role of the inspectors in the process of the system, making the election results more credible.

According to the literature review in section 2.2., some studies designed a system to support on-site voting, but used a centralized database. Some blockchain-based systems did not support on-site voting or did not use voter biometrics to prevent imposter voting. Some blockchain-based on-site voting systems authenticated voters with their biometrics but adopted Ethereum, which is less suitable than HF for e-voting systems [7]. Based on the characteristics of the proposed system mentioned above, our study makes up for the deficiency of existing research. The comparison was summarized in Table 1.

Table 1. Comparison with other studies.

	Remote/On-Site	Blockchain-based	With Biometric
Ours	On-Site	Yes (HF)	Yes (Facial)
[1]	On-Site	No	Yes (Fingerprint)
[6]	Remote	No	No
[8]	On-Site	No	No
[12]	On-Site	Yes (N/A)	Yes (Fingerprint +Facial)
[27]	On-Site	Yes (Ethereum)	Yes (N/A)
[30]	Remote	Yes (HF)	No

There are some suggestions regarding future directions of research related to this work. First of all, we can set up an oracle inside the smart contract to connect blockchain with the real world. By doing so, smart contracts can obtain data from the real world, thus enhancing the credibility of the data input into the smart contract. Second, the biometric identification in this study is mainly based on the voter's face, but there are various biometrics modalities, and the feasibility of other biometrics can be explored in the future. Third, the layout of the reception desk and polling stations can be redesigned to ensure smooth traffic flow in the polling station. Fourth, we assume that every voter has his/her own mobile phone used to carry on the vote credentials, and the situation of which the voter does not have a mobile phone is not considered in this study. Therefore, in the future, a system that allows e-voting and traditional voting to be cooperate at the same time can be considered.

References

[1] Adewale Olumide S., Boyinbode Olutayo K., and Adekunle S., "An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram," *International Journal of Information Engineering and Electronic Business*, vol. 13, no. 5, pp. 24-37, 2021. DOI: 10.5815/ijieeb.2021.05.03

[2] Alvi S., Uddin M., Islam L., and Ahamed S., "Classification of Blockchain Based Voting: Challenges and Solutions," *in Proceedings of the IEEE Asia-Pacific Conference on Computer Science and Data Engineering*, Gold Coast, pp. 1-6, 2020. doi: 10.1109/CSDE50874.2020.9411598.

[3] Carcia J., Benslimane A., and Boutalbi S., "Blockchain-Based System for E-Voting Using Blind Signature Protocol," *in Proceedings of the IEEE Global Communications Conference*, Madrid, pp. 1-6, 2021. doi: 10.1109/GLOBECOM46510.2021.9685189.

[4] Civil Servants Election and Recall Act. https://glrs.moi.gov.tw/EngLawContent.aspx?lan=E&id=658, Last Visited, 2023.

[5] Clark J. and Hengartner U., "Panic Passwords: Authenticating under Duress," *in Proceedings of the 3rd USENIX Workshop on Hot Topics in Security*, San Jose, pp. 1-6, 2008. https://dl.acm.org/doi/abs/10.5555/1496671.1496679#sec-recommendations

[6] Clark J. and Hengartner U., "Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance," *in Proceedings of the 15th International Conference on Financial Cryptography and Data Security*, Gros Islet, pp. 47-61, 2012. https://doi.org/10.1007/978-3-642-27576-0_4

[7] Denis González C., Frias Mena D., Massó Muñoz A., Rojas O., and Sosa-Gómez G., "Electronic Voting System Using an Enterprise Blockchain," *Applied Sciences*, vol. 12, no. 2, 2022. https://doi.org/10.3390/app12020531

[8] De los Santos G., De los Santos J., and De los Santos L., "E-Voting Kiosk: A Network Architecture School-based Registration and Voting System," *in Proceedings of the IEEE 12th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management*, Manila, pp. 1-5, 2020. doi: 10.1109/HNICEM51456.2020.9400135.

[9] Díaz-Santiso J., and Fraga-Lamas P., "E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts," *Engineering Proceedings*, vol. 7, no. 1, 2021. https://doi.org/10.3390/engproc2021007011

[10] Huang J., He D., Obaidat M., Vijayakumar P., Luo M., and Choo K., "The Application of the

Blockchain Technology in Voting Systems: A Review," *ACM Computing Surveys*, vol. 54, no. 3, pp. 1-28, 2021. https://doi.org/10.1145/3439725

[11] Iftekhar A., Cui X., Tao Q., and Zheng C., "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications," *Entropy*, vol. 23, no. 8, pp. 1054, 2021. https://doi.org/10.3390/e23081054

[12] Indrason N., Khongbuh W., and Saha G., "Blockchain-Based Boothless E-Voting System," *in Proceedings of the 3rd International Conference on Innovative Computing and Communications*, Delhi, pp. 779-788, 2020. https://doi.org/10.1007/978-981-15-5113-0_64

[13] Kaudare A., Hazra M., Shelar A., and Sabnis M., "Implementing Electronic Voting System with Blockchain Technology," *in Proceedings of the International Conference for Emerging Technology*, Belgaum, pp. 1-9, 2020. doi: 10.1109/INCET49848.2020.9154116.

[14] Kamran., Nasir M., Imran M., and Yang J., "Study on E-Voting Systems: A Blockchain Based Approach," *in Proceedings of the IEEE International Conference on Consumer Electronics-Asia*, Gangwon, pp. 1-4, 2021. DOI: 10.1109/ICCE-Asia53811.2021.9641914

[15] Khan K., Arshad J., and Khan M., "Investigating Performance Constraints for Blockchain based Secure E-Voting System," *Future Generation Computer Systems*, vol. 105, pp. 13-26, 2020. https://doi.org/10.1016/j.future.2019.11.005

[16] Kirillov D., Korkhov V., Petrunin V., Makarov M., Khamitov I., and Dostov V., "Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain," *in Proceedings of the 19th International Conference on Computational Science and Its Applications*, Saint Petersburg, pp. 509-521, 2019. https://doi.org/10.1007/978-3-030-24296-1_40

[17] Kyazhin S. and Popov V., "Yet Another E-Voting Scheme Implemented Using Hyperledger Fabric Blockchain," *in Proceedings of the 20th International Conference on Computational Science and Its Applications*, Cagliari, Italy, pp. 37-47, 2020. https://doi.org/10.1007/978-3-030-58808-3_4

[18] Mookherji S., Vanga O., and Prasath R., *Blockchain Technology for Emerging Applications*, Academic Press, 2022. https://doi.org/10.1016/B978-0-323-90193-2.00006-5

[19] Mustafa M. and Waheed S., "An E-Voting Framework with Enterprise Blockchain," *in Proceedings of the 1st Advances in Distributed Computing and Machine Learning*, Vellore, pp. 135-145, 2020. DOI:10.1007/978-981-15-4218-3_14

[20] Nakamoto S., "Bitcoin: A Peer-to-Peer Electronic Cash System," *Decentralized Business Review*, pp. 1-9, 2008. https://bitcoin.org/bitcoin.pdf

[21] National Democratic Institute, "Common Electronic Voting and Counting Technologies," Available at: https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies, Last Visited, 2023.

[22] Pawlak M. and Poniszewska-Marańda A., "Implementation of Auditable Blockchain Voting System with Hyperledger Fabric," *in Proceedings of the 21st International Conference on Computational Science*, Kraków, pp. 642-655, 2021. https://doi.org/10.1007/978-3-030-77961-0_51

[23] Pawlak M. and Poniszewska-Marańda A., "Trends in Blockchain-Based Electronic Voting Systems," *Information Processing and Management*, vol. 58, no. 4, pp. 102595 2021. https://doi.org/10.1016/j.ipm.2021.102595

[24] Presidential and Vice Presidential Election and Recall Act. https://glrs.moi.gov.tw/EngLawContent.aspx?lan=E&id=659, Last Visited, 2023.

[25] Referendum Act. https://law.cec.gov.tw/EngLawContent.aspx?lan=E&id=4, Last Visited, 2023.

[26] Ruan Y. and Zou X., "Receipt-Freeness and Coercion Resistance in Remote E-Voting Systems," *International Journal of Security and Networks*, vol. 12, no. 2, pp. 120-133, 2017. https://core.ac.uk/download/pdf/146989105.pdf

[27] Ruparel H., Hosatti S., Shirole M., and Bhirud S., "Secure Voting for Democratic Elections: A Blockchain-Based Approach," *in Proceedings of the 2nd International Conference on Communication, Computing and Electronics Systems*, Coimbatore, pp. 615-628, 2020. https://doi.org/10.1007/978-981-33-4909-4_47

[28] Schäffer M., Di Angelo M., and Salzer G., "Performance and Scalability of Private Ethereum Blockchains," *in Proceedings of the International Conference on Business Process Management: Blockchain and Central and Eastern Europe Forum*, Vienna, pp. 103-118, 2019. https://doi.org/10.1007/978-3-030-30429-4_8

[29] Su P. and Su T., "Secure Blockchain-Based Electronic Voting Mechanism," *The International Arab Journal of Information Technology*, vol. 20, no. 2, pp. 253-261, 2023, doi: 10.34028/iajit/20/2/12.

[30] Yu B., Liu J., Sakzad A., Nepal S., Steinfeld R., Rimba P., and Au M., "Platform-Independent Secure Blockchain-Based Voting System," *in Proceedings of the 21st International Conference on Information Security*, Guildford, pp. 369-386, 2018. https://doi.org/10.1007/978-3-319-99136-8_20

[31] Yuan P., Xiong X., Lei L., and Zheng K., "Design and Implementation on Hyperledger-Based Emission Trading System," *IEEE Access*, vol. 7, pp. 6109-6116, 2019. doi: 10.1109/ACCESS.2018.2888929.

Shu-Fen Tu received the Ph.D. degree from the Institute of Information Management, National Central University, Taiwan in 2005. From 1998 to 1999, she is a software engineer of the Syscom Group Co., Taiwan. From February 2005 to July 2005, she is an assistant professor of Department of Information Management, Chaoyang University of Technology. Currently, she is a professor of Department of Information Management, Chinese Culture University, Taiwan. Her current research interests include Blockchain, sentiment analysis, steganography, and secret sharing.

Ching-Sheng Hsu received his Ph.D. degree from the Institute of Information Management, National Central University, Taiwan, in 2005. From 1998 to 1999, he was a software engineer at the Syscom Group Co., Taiwan, where his work focused on Web-based stock trading systems. Currently, he is a professor of the Department of Information Management, Ming Chuan University, Taiwan. His research interests include Blockchain, e-Learning, Data Mining and Big Data, Information Hiding, and Secret Sharing.

Bo-Long You received his master's degree from the Department of Information management, Ming Chuan University, Taiwan, in 2021. From 2016 to 2020, he was a teaching assistant and a part-time employee at Ming Chuan University. His research interests are Blockchain and Android Apps development.