sustainability

MDPI

Article

Design of an E-Voucher System for Supporting Social Welfare Using Blockchain Technology

Ching-Sheng Hsu [1], Shu-Fen Tu [2,*] and Zhao-Ji Huang [1]

[1] Department of Information Management, Ming Chuan University, 5 De Ming Rd., Gui Shan District, Taoyuan City 333, Taiwan; cshsu@mail.mcu.edu.tw (C.-S.H.); ahhjjgg55@gmail.com (Z.-J.H.)

[2] Department of Information Management, Chinese Culture University, No.55, Huagang Rd., Shihlin District, Taipei City 11114, Taiwan

* Correspondence: dsf3@ulive.pccu.edu.tw; Tel.: +886-2-28610511

Received: 21 February 2020; Accepted: 20 April 2020; Published: 21 April 2020

Abstract: Issuing vouchers is a means of implementing social welfare. There are some security concerns about paper-based vouchers, such as counterfeiting, reproducing, their low operating efficiency and so on. This study explores how to apply blockchain technology and cryptography to build a secure e-voucher system in order to solve various shortcomings of paper vouchers. A feasible application model is proposed that integrates blockchain technology in the context of vouchers to support the field of social welfare. In this study, we conducted an analysis to prove that the security requirements of the e-voucher system are met when applying this model. Subsequently, we used the Hyperledger Fabric blockchain platform and Kafka ordering services to implement the campus welfare meal voucher system. A large number of experimental data were obtained to show that the system has a satisfactory performance. In the conclusion section, we discussed the theoretical and management implications of this study, and how this study meets UN Sustainable Development Goals.

Keywords: blockchain; distributed ledger technology; e-voucher system; social welfare

1. Introduction

The 2030 Agenda for Sustainable Development and its Sustainable Development Goals set a series of key development goals for developed and developing countries to eliminate poverty, protect the planet and ensure the prosperity of all people. One of the priorities agreed by Member States is social protection, which has been repeatedly mentioned in the agenda as the main means of reducing poverty and eliminating inequality. The short-term goal of social protection is to help people meet basic needs, provide basic income levels for people living in poverty or prevent people from falling into poverty due to disease or drought. Long-term goals include increasing opportunities for inclusive growth, human capital development and social stability. Social protection appears in many targets in the Sustainable Development Goals (SDG), including Goals 1, 3, 5, 8 and 10 [1]. One of the types of social protection is social assistance, which is designed to help the most vulnerable individuals, families and communities to meet the social floor and improve living standards. The actions of social assistance may include welfare and social services to highly vulnerable groups, non-contributory transfers in cash, vouchers, or in-kind to individuals or households in need and temporary subsidies in times of crisis [2]. Therefore, social welfare is closely related to the social dimension of sustainability [3].

Issuing vouchers is one of the ways in which a government or non-profit organization can implement a social welfare program [4,5], as near-cash transfer has some benefits, such as increased income, consumption, expenditure and asset accumulations, and improved health outcomes [6]. A voucher is a kind of ticket which can be used instead of money to pay for something [7]. The person who receives the voucher can go to a certified store to purchase services or goods. The certified

stores then ask the government or non-profit organizations for money with the voucher received. Government or non-profit organizations may use cash vouchers to reach consumption incentives or public welfare. In Zambia, poverty is a challenge that this country has always faced. Since agriculture is the main economic body, the Zambian government launched the Farmer Input Support Program (FISP) to subsidize farmers' crop losses due to natural disasters. The government issued a physical pre-paid voucher card to the farmer, and the farmer can use the card to redeem agricultural input supply. Zambia expects farmers who have been subsidized for two years to leave the plan, but the government has no way to track who has reached the subsidy deadline, thus the cost of FISP has exploded. Later, Zambia decided to build an electronic voucher system to try to solve some problems [8,9]. However, the Zambian government still faced some problems, which we will discuss later in the next section.

Since a voucher is equivalent to proof of cash value and is not redeemable for cash, the anti-counterfeiting of vouchers is a very important issue. Because vouchers have a welfare purpose, only eligible individuals can receive and use vouchers. Therefore, preventing the transfer of vouchers is also a very important issue. Moreover, the relevant parties involved in the e-voucher system are more diverse than those involved in the general admission system, so mutual trust between groups is a key factor in the success of the e-voucher system. Recently, an emerging technology, called blockchain, has brought many new opportunities to the industry. Blockchain technology achieves trust among parties and fault tolerance through cryptography and decentralized architecture. The blockchain has evolved over several stages since its introduction. Virtual currency is the earliest application of blockchain technology. Gradually, it has been found that the special features of blockchain technology mean that it can be employed in many innovative applications in various industries. Nowadays, various products and services using blockchain technology have been proposed, including those in finance, agriculture, food and transportation. Some scholars have also begun to explore the application opportunities of blockchain technology in sustainable development [10]. So far, very few studies related to e-ticket systems have used blockchain technology [11,12]. Moreover, studies using blockchain technology have not proposed a system architecture for vouchers. A provable identity is necessary for accessing social benefits like vouchers, pensions or cash transfers. One of the remarkable properties of blockchain technologies is their ability to provide a provable identity [13]. Therefore, the purpose of our paper is to design a blockchain-based system for vouchers. By introducing blockchain technology, the proposed system can address the above issues related to vouchers.

The remainder of this paper is organized as follows: In Section 2, social protection instruments, legacy technology of ticketing systems, and prerequisite knowledge are reviewed; in Section 3, the general framework of the e-voucher system is described in detail; Section 4 presents a security analysis of the proposed e-voucher system; Section 5 provides a case study and implementation of the framework; and finally, conclusions are provided in Section 6.

2. Related Works

2.1. Social Protection Instruments

Social protection has received widespread attention worldwide. Extensive evidence over the past few years strongly suggests that social protection programs can be used to reduce poverty and inequality, increase human capital and protect people from risks. However, there is still much work to be done in social protection. Existing social protection procedures not enough because some groups are systematically left behind. Sustainability is a multiple concept covering social, economic and environmental aspects. It is committed to social integration and the elimination of obstacles for individuals to achieve their cherished lives. As countries around the world align their priorities with the Sustainable Development Goals (SDG), the 2030 Sustainable Development Agenda set social protection as a specific target (Target 1.3) and a feature in Goals 3, 5 and 10. Since social protection is one of the pillars of decent work, it is also a feature of Target 8.5 [6].

Various institutions and organizations use different organizational concepts to define social protection. What all these definitions have in common is that social protection provides a solution to the policy framework of poverty and vulnerability. Over the past 25 years, economic growth has been an important driver of poverty reduction worldwide. However, eradicating poverty by 2030 will require sustainable and inclusive growth, supplemented by interventions to ensure that those who cannot participate in and benefit from growth receive at least minimal well-being. The United Nations Development Programme (UNDP) categorized the social protection instruments into (1) non-contributory social transfers; (2) social insurance (fully or partially contributory); (3) social services; and (4) labor market policies. A social transfer is a benefit provided by the government or community donor to an individual (or household) in need of a specific type of social assistance. Social transfers can be short-term assistance in emergency situations or long-term and predictable support for people in trouble. At present, the interest of low-income countries in social transfer is concentrated on long-term predictable tools to address chronic poverty and its causes. The mechanism used to transfer the benefit to the beneficiary can be direct (cash, food, inputs, assets), voucher/coupon, subsidy/fee waiver or in-kind [14]. Vouchers or coupons are now mostly issued as electronic vouchers to increase convenience and facilitate the use of information technology for management and control. Take Zimbabwe for example—the 2011/2012 season is the second season in which voucher mechanisms are used in Zimbabwe. During the 2010/2011 cropping season, 339,000 households received inputs through voucher mechanisms. Following the national guidelines, Zimbabwe supports the 2011/2012 agricultural programme through electronic vouchers to provide inputs to 4100 farming households. Electronic vouchers can be redeemed at rural agricultural dealer outlets that have been identified to participate in the program. This enables farmers to choose the agricultural inputs they need during the growing season [15]. In a similar example, the Zambian government has implemented the Farmer Input Support Program since 2002 as part of its agricultural transformation agenda. In order to achieve the overall goal of the agricultural transformation agenda, the implementation form of the FISP plan undergoes several changes. One of the major changes is from traditional farmer input distribution systems to electronic voucher methods due to the poor effectiveness of traditional input allocation methods [16].

2.2. E-Ticketing Schemes

Vives-Guasch et al. [17] classified e-ticketing schemes into smart-card-based and non-smart-card-based systems. The smart-card-based systems use contact or contactless smart cards as the medium to offer limited ticketing services [18]. The non-smart-card-based systems use a mobile phone as the user-end device, which can perform more complicated operations than smart cards. The ticket system discussed in this study is the latter type of scheme. Generally, four participants are involved in the e-ticketing system: an issuer, user, collector and third-party provider [17,19,20]. An issuer creates and issues a ticket with specified contents. A user is the holder of the ticket and redeems the ticket via the collector, and the collector transfers the goods or renders services to the user. Sometimes, users may transfer the ticket to other users, and the collector and issuer can be the same individual. Because the transaction among the issuer, user and collector needs to be verified to prevent fraud, a third party trusted by each participant is necessary. The third party may be the provider of the trading platform or may only be responsible for authenticating the transactions. Hu et al. [19] proposed a universal e-ticket system, called Uniticket, which integrates all kinds of ticketing into one system. The Uniticket system has a trusted third-party platform and interfaces with personal and enterprise user ends. The personal users perform inquiries and bookings through their mobile phone, and the enterprise users issue and manage tickets by websites. All the transactions are processed by the central server and stored in the central database. If the central database fails, the entire system will not work. Moreover, malicious participants can achieve the purpose of fraud by invading the central database to tamper with the data.

Since there is no trust between participants, the ticket system requires a complicated verification process to confirm the identity of the participants and the tickets they hold. Tickets related to social

well-being will be verified by multiple parties, so that social welfare can be truly delivered to those in need. Government or non-profit organizations issue cash vouchers to people to redeem goods or services. The Zambian government is one such example. In 2002, the Zambian government started the Farmer Input Support Program to help people in rural areas eradicate poverty and food insecurity. Through this program, the government issues vouchers to eligible famers, who can use the vouchers to redeem goods at agro-dealers. In the beginning, the government intended to subsidize each beneficiary for two years. After two years, the beneficiary had to leave the project. However, none of the beneficiaries have graduated since the inception of the program because the program is operated manually, and no exit strategy has been designed [8,9]. As a result, the cost of FISP has increased so much that it has eroded the budget of other projects in the agricultural sector. In order to solve this dilemma, the Zambian government adopted an e-voucher system during the farming season in 2015 and 2016. After two years, a survey showed that the e-voucher system succeeded in terminating the subsidies for the same individual after three consecutive years and prevented the beneficiary from redeeming a given voucher multiple times. As we have mentioned in the above section, due to many organizations being involved in the system, how to build mutual trust between organizations is an important issue. In fact, there was a past event in which fake agro-dealers cheated the government's money system, which caused the payment to agro-dealers to be delayed [21]. In addition, the approved list needs to be passed between many different sectors, making the administrative process inefficient. One of the challenges of the e-voucher system is the delayed delivery and activation of e-cards caused by the delayed submission of beneficiary lists [9].

2.3. Security Requirements

For e-ticket systems, some security requirements need to be considered or met, as follows [17,22]:

1. Authenticity: The authenticity of the issuer of an e-ticket must be able to be verified;
2. Integrity: The e-tickets must be able to verify whether they are forged or altered;
3. Non-reproduced: There must only be one valid holder for a particular e-ticket at a particular time;
4. Non-repudiation: The issuance and redemption of e-tickets cannot be repudiated by relevant parties;
5. One-time redemption: An e-ticket cannot be redeemed again after it has been consumed;
6. Anonymity: This is an optional requirement. For non-anonymous e-tickets, the authorization of the holder must be able to be verified. On the other hand, for anonymous e-tickets, the holder must remain anonymous to the issuer or the service provider;
7. Transferability: This is also an optional requirement. If the e-ticket is transferable, anyone receiving the transferred e-ticket must be able to verify if this e-ticket is valid. Moreover, current and previous holders of this e-ticket should not be traceable. On the other hand, if the e-ticket is non-transferable, the e-ticket can only be held by a specific user.

This research proposes an electronic voucher system based on blockchain technology, and the system is mainly applied to the issuance and redemption of vouchers with social welfare purposes; that is, the issuer of vouchers may be the government or non-profit organization, and the holders of vouchers have specific qualifications, such as those who are economically disadvantaged or people with specific occupations. Therefore, the user must be able to be identified, and the voucher must not be transferred to someone who is not a qualified holder, otherwise the purpose of social welfare will be lost. In other words, for the last two optional requirements given above, the proposed system must make the issued e-vouchers non-anonymous and non-transferable. Needless to say, the first five requirements also need to be met.

2.4. Blockchain Technology

A blockchain is a decentralized ledger with a consistent protocol. Blockchain technology employs cryptographic techniques and a decentralized consensus mechanism to achieve trust and security. The main features of a blockchain can be summarized as follows [23].

2.4.1. Distributed Database

The transactions are recorded by multiple nodes, each of which records a complete transaction record. Therefore, each node can participate in monitoring the legality of the transaction and in verifying the validity of the transaction. Unless all the nodes are destroyed, the transaction record will not be lost [24]. Different from the centralized database, no node in the blockchain network has the right to record transactions separately, thus reducing the possibility of controlling a single node to record fake transactions.

2.4.2. Decentralization

Decentralization indicates that each participating node is equal and connected to each other to avoid a single individual obtaining an exclusive right to reviewing the transaction and occupying data resources [25]. For the blockchain, decentralization means decentralizing the data storage and transaction authentication process. The concept of data storage decentralization means that data are no longer centrally managed; instead, each participating node maintains the same information. The concept of the decentralizing transaction authentication process means that the transaction initiated by the participant is no longer approved by the regulatory agency. All participating nodes jointly verify the transaction and the transaction is only completed when all or most of the nodes approve the transaction.

2.4.3. Encryption

Blockchain technology combines the advantages of many encryption techniques, such as asymmetric encryption and hashing algorithms. In addition, a digital signature is employed to further protect the data integrity and identity verification.

2.4.4. Consensus Mechanism

The consensus mechanism is a method employed to reach consensus among the nodes in the blockchain system. There are various ways to implement the consensus mechanism, and the most appropriate depends on the necessity of the organization. The consensus mechanism not only needs to agree on the transaction verification, endorsement and order, but also requires the crash or Byzantine fault tolerance to be achieved. The most basic consensus is the consistency of the transaction order. For Hyperledger Fabric—an open source business blockchain framework hosted by The Linux Foundation—the consensus mechanism also includes verification of the transaction proposal, transaction approval and transaction confirmation, so that the correctness of a transaction can be fully inspected.

2.4.5. Smart Contract

The smart contract was proposed by Nick Szabo in 1997 [26]. The smart contract is like auto-executable program codes, which can be stored, delivered, controlled and managed via the blockchain [27]. The elements of a smart contract include the contract body, digital signature, contract terms and decentralized platform.

2.4.6. P2P Network Architecture

The blockchain network conforms to the P2P network architecture. In the P2P network architecture, multiple physical hosts are connected to each other and have the same computing functions. The P2P

network protocol defines the message exchange and task distribution among the peer-to-peer network of nodes.

There are two types of blockchain: permissionless and permissioned. A permissionless blockchain, also called a public blockchain, allows anyone to join the blockchain anonymously and to view the data without specific permissions. In order to maintain the security of the system, to encourage miners to package transaction data, and to ensure the activity of the system, a public blockchain often issues tokens to reward the miners responsible for packaging transactions. To address issues of trust and security, the efficiency of transactions is often sacrificed. On the contrary, any person or organization that wants to join a permissioned blockchain is restricted by permissions and must not be anonymous. Nodes must acquire an organization's licensors to join the blockchain network, and the visibility of data storage on the chain must be controlled via certain permissions. A permissioned blockchain can be divided into consortium and private blockchains. The consortium blockchain is composed of several trusted nodes, and the nodes trust each other, forming an alliance. Because the nodes are credible and have business relationships with each other, they are obliged to be responsible for joint packaging and recording transactions. Therefore, it is not necessary to reward the miners responsible for packaging by issuing tokens. As a result, the transaction efficiency of the consortium blockchain will be greatly improved. The private blockchain is an internal blockchain with no third-party participation, so trust and security are the highest compared to public and consortium blockchains, but decentralization is the lowest.

This study uses the architecture of the consortium blockchain to design the e-voucher system because the participants of the system are limited and need to register permissions. Regardless of the right of access to the data on the chain, or the right to participate in setting up nodes or to deploy smart contracts, everything can be designed within the alliance. There are currently several consortium blockchain frameworks, and Hyperledger Fabric is the most famous one. This study uses Hyperledger Fabric to develop the e-voucher system.

3. The General Framework of the E-Voucher System

For the convenience of explanation, let us first introduce the symbols that will be used:

- o: non-profit organization;
- b: beneficiary;
- d: dealer;
- V_i: e-voucher with number I;
- n: number of e-vouchers issued to the beneficiary;
- rsa_pk_u: Rivest–Shamir–Adleman (RSA) public key of user u;
- rsa_sk_u: RSA private key of user u;
- ecc_pk_u: Elliptic Curve Cryptography (ECC) public key of user u;
- ecc_sk_u: ECC private key of user u;
- DS_u: digital signature of user u;
- **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 a digital digest of message m;
- ||: concatenation operator.

3.1. Application Scenario

There are three roles involved in the voucher transaction, including the non-profit organization, the beneficiary, and the dealer. The non-profit organization issues a collection of vouchers to the qualified beneficiaries, and the beneficiaries use the vouchers to claim goods or services from the dealers approved by the non-profit organization. The main concerns of the non-profit organization are that the voucher must be issued to the appropriate beneficiary and cannot be transferred to another

non-beneficiary. With regards to the dealers, their concerns are that the vouchers received from the beneficiaries must be credible, so that they can successfully claim money from the non-profit organization. The only concern of the beneficiaries is that they can successfully claim goods or services from the dealer. Based on the above concerns, the whole process of the proposed e-voucher system is as shown in Figure 1, and the detailed procedures are explained below:

(1) Initially, a pair of public and private keys for the non-profit organization o, ecc_pk_o and ecc_sk_o, is generated. Then, ecc_pk_o is recorded in the blockchain, and ecc_sk_o is kept private by the non-profit organization o;
(2) Anyone who intends to apply for the e-voucher generates a pair of ecc_pk_b and ecc_sk_b. The ecc_pk_b and the application form are submitted to o, and the ecc_sk_b is stored in the mobile phone of the applicant;
(3) When o confirms that the applicant is a qualified beneficiary b, ecc_pk_b and a collection of e-vouchers, V_1 to V_n, belonging to b are recorded in the blockchain;
(4) Each time b wants to use an e-voucher, b must temporarily generate a pair of rsa_pk_b and rsa_sk_b and send a request with rsa_pk_b to o;
(5) When o receives the request from b, one unused e-voucher V_i belonging to b is read from the blockchain, and DS_o = **Enc**(**H**(V_i), ecc_sk_o) is calculated;
(6) Then, **Enc**(V_i || DS_o, rsa_pk_b) is sent to b. In addition, a record of V_i issuing to b is written into the blockchain;
(7) When b receives **Enc**(V_i || DS_o, rsa_pk_b), b calculates **Dec**(**Enc**(V_i || DS_o, rsa_pk_b), rsa_sk_b) to get V_i and DS_o. Then, b retrieves ecc_pk_o from the blockchain, re-hashes the received e-voucher V_i, and compares the re-hashing result with **Dec**(DS_o, ecc_pk_o). If the comparison displays no difference, the authenticity of the e-voucher and the issuer can be ensured;
(8) Before using V_i, b also generates DS_b = **Enc**(**H**(V_i), ecc_sk_b). Then, b creates the QR code for V_i, DS_o, and DS_b. Next, b presents the QR code to the dealer d to claim for the goods or service;
(9) The dealer d scans the QR code to read V_i, DS_o, and DS_b. Then, d retrieves ecc_pk_o and ecc_pk_b from the blockchain, re-hashes the received e-voucher V_i, and compares the re-hashing result with **Dec**(DS_o, ecc_pk_o) and **Dec**(DS_o, ecc_pk_b). If the comparison displays no difference, the authenticity of the e-voucher, the issuer, and the beneficiary can be ensured. At the same time, d will also check the usage history in the blockchain to confirm whether V_i has been used;
(10) If the verification is correct, d will deliver the goods or service to b. In addition, a record of V_i being used is written into the blockchain;
(11) Finally, the dealer d and the non-profit organization o should clear and deliver e-vouchers within the agreed period.

3.2. System Architecture

This research uses the Kafka and Zookeeper cluster network of Hyperledger Fabric to implement a blockchain-based e-voucher system. Kafka is an ordering service with crash fault tolerance. When there are multiple ordering service nodes (OSN), the OSN will directly forward the transaction TX to the Kafka node after receiving the TX from the client. Kafka will sort the TX and place it in the partition of Kafka. Note that all transactions in the partition are sorted and permanent records. After that, OSN can consume the data in the partition and obtain the sorted TX list. After this, the transaction is packaged into a block and passed to the committer peer to add the block to the blockchain. The responsibilities of the Zookeeper cluster is (1) to monitor Kafka nodes and to elect a control node during node failure, (2) to configure and manage topics and partitions, (3) to maintain the access control list of topics and (4) to maintain the Kafka cluster member list. Figure 2 depicts a general picture of the system architecture.

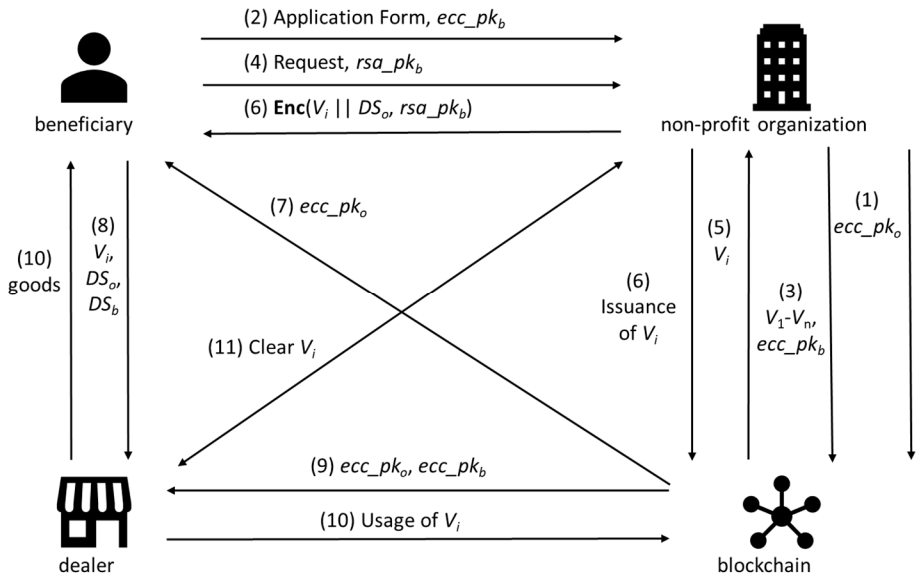


Figure 1. The whole process of the proposed e-voucher system.

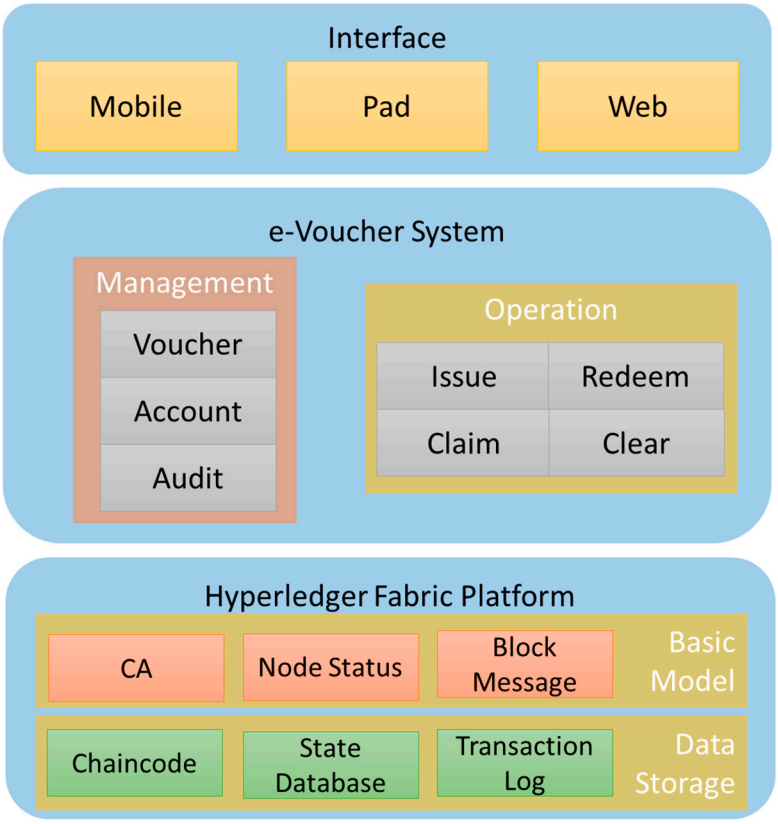


Figure 2. The system architecture.

3.2.1. Hyperledger Fabric Platform

The underlying technology is based on the Hyperledger Fabric platform. The data stored on the blockchain is irreversible and unmodifiable to ensure the security of e-voucher transactions. In addition, the issuance of e-vouchers is controlled and confirmed through smart contracts. All transaction information, such as e-voucher issuance and redemption, can be viewed through the state database

and transaction log. The basic model relates to the functions of blockchain network management, such as Certificate Authority (CA) management, and the user's public and private key generation. Moreover, all node states are monitored and managed through the Hyperledger Fabric platform.

3.2.2. E-Voucher System

The blockchain-based e-voucher system provides managers with necessary functions related to user account management; e-voucher management; and operations of issuance, checking, receiving and redemption.

3.2.3. User Interface

Users can apply for an account, submit a query, or redeem e-vouchers through the mobile application or web page.

4. Security Analysis

In Section 2.2, we proposed several security requirements for the e-voucher system. In this section, we will analyze how the system meets these security requirements.

Proposition 1. *The proposed e-voucher system preserves the authenticity of the e-voucher.*

There are two roles that are required to verify the authenticity of the e-voucher issuer, i.e., the non-profit organization o. One is the beneficiary b, and the other is the dealer d. Each e-voucher sent to b or d is accompanied by the digital signature of o, DS_o. Both b and d can read the public key of o, ecc_pk_o, from the blockchain, to verify the e-voucher and DS_o. Moreover, only o has the right to write its ECC public key into the blockchain. Therefore, we can ensure that the proposed system has the property of verifying the authenticity of the issuer of the e-voucher.

Proposition 2. *Modification of the e-voucher can be discovered.*

As we mentioned above, both b and d receive the e-voucher V_i with DS_o. To verify V_i and DS_o, b and d re-hash the V_i and decrypt DS_o with the public key of o, ecc_pk_o, retrieved from the blockchain. If the content of the e-voucher is modified, the re-hashing result and the decrypting result must be different because SHA-256 is believed to have a very high collision resistance. This means that the probability of two different messages being calculated to output the same digest is extremely low. Therefore, forgery or alteration of the e-voucher can be discovered immediately.

Proposition 3. *The proposed e-voucher system prevents anyone from reproducing the e-voucher.*

Because of the nature of the consortium blockchain, only the non-profit organization has the right to write issued e-vouchers into the blockchain. Moreover, the issuance and redemption of the e-voucher will also be recorded in the blockchain. Whether any e-voucher has been issued or redeemed can be verified through the records of the blockchain. Moreover, the voucher V_i and digital signatures DS_o sent to the beneficiary b will be encrypted with the b's RSA public key rsa_pk_b. Even if other people intercept the transmitted message, they cannot recover V_i and DS_o without the matched RSA private key rsa_sk_b. Therefore, it is meaningless and not profitable to reproduce the e-voucher.

Proposition 4. *The non-profit organization cannot deny the emission of the e-voucher, and the beneficiary cannot deny the usage of the e-voucher.*

When issuing the e-voucher, the non-profit organization o signs the e-voucher with its private key ecc_sk_o. The public key ecc_pk_o that matches ecc_sk_o is recorded in the blockchain. If DS_o is verified using ecc_pk_o, the non-profit organization o cannot repudiate the issuance of the e-voucher because

ecc_pk_o and ecc_sk_o match. Moreover, once ecc_pk_o is written into the blockchain, o cannot deny the authenticity of ecc_pk_o due to the undeniable nature of the blockchain.

Proposition 5. *The beneficiary cannot redeem the same e-voucher repeatedly.*

Because our system uses the consortium blockchain architecture, only trusted members can join the alliance, and only the dealer has the right to write the blockchain with e-voucher usage records. Once the dealer verifies that the e-voucher is correct and delivers the goods to the beneficiary, the usage of the e-voucher will be recorded in the blockchain. If an e-voucher exhibits repeated consumption, the dealer can immediately detect this from the blockchain record.

Proposition 6. *The authorization of the holder can be verified.*

A qualified beneficiary b needs to provide the ECC public key ecc_pk_b to the non-profit organization o to write it into the blockchain. Once ecc_pk_b is written into the blockchain, ecc_pk_b and ecc_sk_b are bound together, so that b cannot re-generate another pair of ECC private keys to sign the e-voucher; otherwise, b will not be able to use the e-voucher. It is reasonable to say that ecc_sk_b must be kept privately. Therefore, as long as the digital signature can be verified with ecc_pk_b, the identity of the holder can be confirmed.

Proposition 7. *The beneficiary cannot transfer the e-voucher to others.*

Before using the e-voucher, the beneficiary b needs to sign the e-voucher with ecc_sk_b. As we have mentioned above, ecc_pk_b and ecc_sk_b are bound together, and reasonably, ecc_sk_b must be kept privately. Even if the e-voucher is transferred to another person, this e-voucher is not useful to others because others do not have the private key ecc_sk_b paired with the public key ecc_pk_b. Consequently, it is impossible for others to generate the correct digital signature. Therefore, the e-voucher is not transferable.

5. Implementation Details and Experimental Results

5.1. E-voucher System Development and Configuration Details

This research uses a university student's meal voucher subsidy as a system implementation scenario. For any student who applies for a meal voucher subsidy, the school will review their eligibility to see if the student meets the financially disadvantaged conditions, and qualified students will receive a collection of meal vouchers from the school. Subsequently, students can redeem meals from the cafeterias on campus with the meal vouchers. As can be seen in Figure 1, the school plays the role of the non-profit organization, the student plays the role of the beneficiary, and the cafeterias on campus play the role of the dealer. The system implementation interface is described below.

5.1.1. Student Side

The student-side interface of the system is mainly based on mobile applications. Students can register and log in through the login interface (see Figure 3a) and submit personal information to apply for a meal voucher subsidy (see Figure 3b). After the student's application is approved, the student can view the e-vouchers (see Figure 3c). Then, the student can click on one of the e-vouchers to generate a QR code (see Figure 3d).

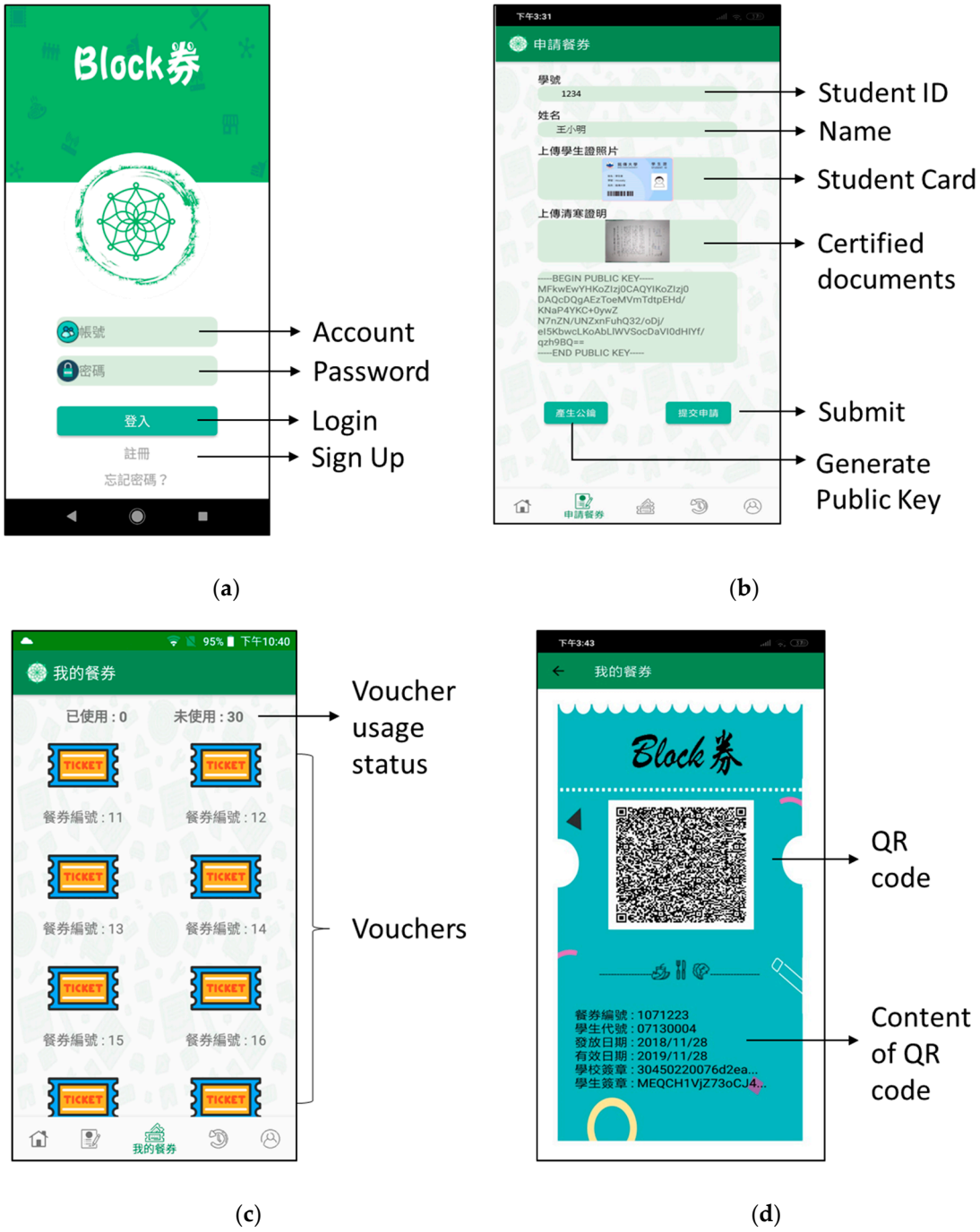
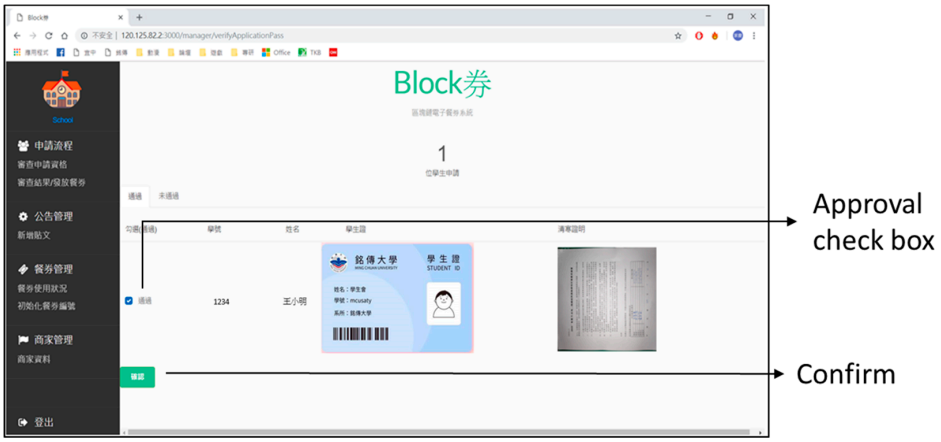


Figure 3. User interface of the student side. (**a**) Login interface; (**b**) E-voucher application form; (**c**) E-voucher status; (**d**) The QR code of an e-voucher.

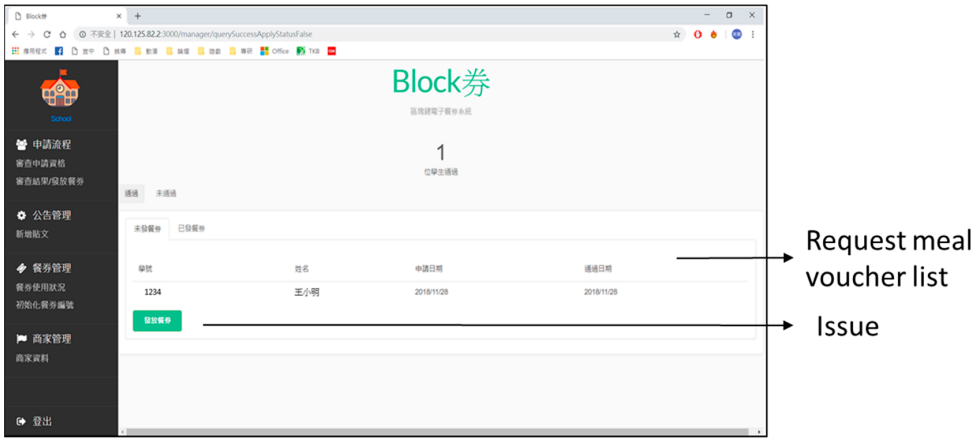
5.1.2. School Side

The school-side system uses the web browser as an interface. After login, the school administrator can view the applications pending approval (see Figure 4a). Then, the administrator can click on the applicant record to view the documents provided by the student (see Figure 4b). If the applicant qualifies for the subsidy, the administrator can check the box and confirm approval. Once a student requests a meal voucher, the administrator will be notified and issue a meal voucher to the student (see Figure 4c).

(**a**)



(**b**)



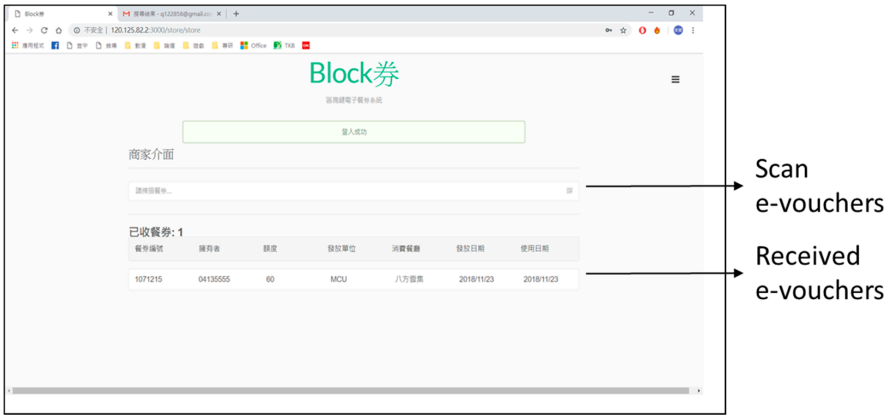
(**c**)

Figure 4. School-side interfaces. (**a**) School login interface; (**b**) Interface for an examination of pending applications; (**c**) Interface for issuing meal e-vouchers.

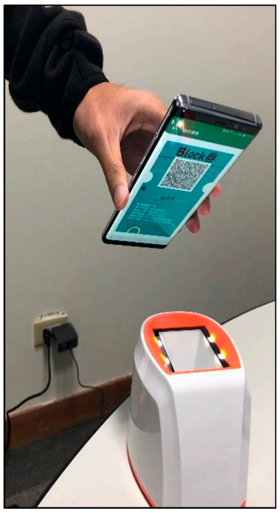
5.1.3. Cafeteria Side

The cafeteria-side system also uses the web browser as an interface. After login, the webpage will display summary information on the e-vouchers received (see Figure 5a). The cafeteria selects the scan e-voucher function to open the bar code scanner and scans the QR code presented by the student

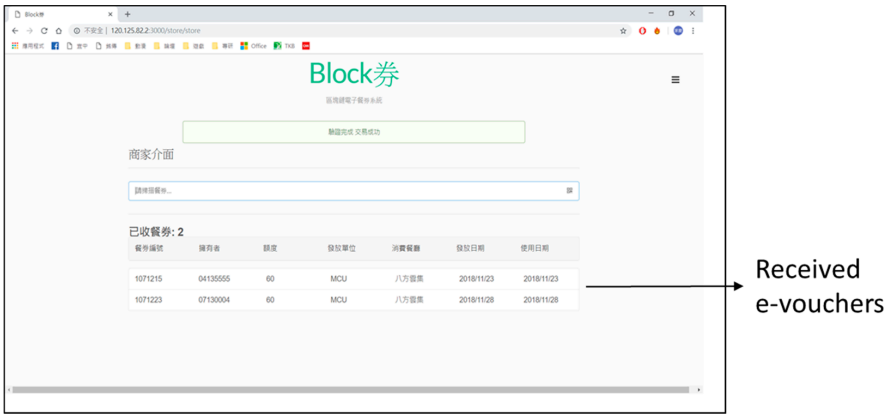
(see Figure 5b). The system will automatically upload the data and complete the transaction after verification. From the webpage, the cafeteria can see that the e-voucher just scanned has been added to the list of received e-vouchers (see Figure 5c).



(**a**)



(**b**)



(**c**)

Figure 5. Cafeteria-side interfaces. (**a**) Cafeteria login interface; (**b**) Students pay with a meal voucher; (**c**) Cafeteria receives the meal voucher.

5.2. System Performance Analysis

This research uses Hyperledger Fabric 1.4.1 (LTS) and the Kafka cluster multi-machine deployment mode for system development. The parameter configuration of Kafka deployment is shown in Table 1. There are 10 hardware devices, and the hardware device specifications and configurations for multi-machine deployment are shown in Tables 2 and 3, respectively.

Table 1. Kafka deployment parameter configuration table.

Parameter	Value
BatchTimeout	100 ms
MaxMessageCount	10
AbsoluteMaxBytes	99MB
PreferredMaxBytes	512KB

Table 2. Hardware specifications.

Component	Specification
CPU	CORE I7 4790 3.6 GHz
Memory	8GB DDR3L
HDD	1TB

Table 3. Configurations for multi-machine deployment.

Host	Name of the Peer Node
Host 1	Kafka1, Zookeeper1, Orderer1
Host 2	Kafka2, Zookeeper2, Orderer2
Host 3	Kafka3, Zookeeper3, Orderer3
Host 4	Kafka4
Host 5	Peer0.Org1
Host 6	Peer1.Org1
Host 7	Peer0.Org2
Host 8	Peer1.Org2
Host 9	School-side HTTP application server
Host 10	Cafeteria-side HTTP application server

This research carried out a system test for three parties, namely, a student-side app, a school-side webpage, and a cafeteria-side webpage.

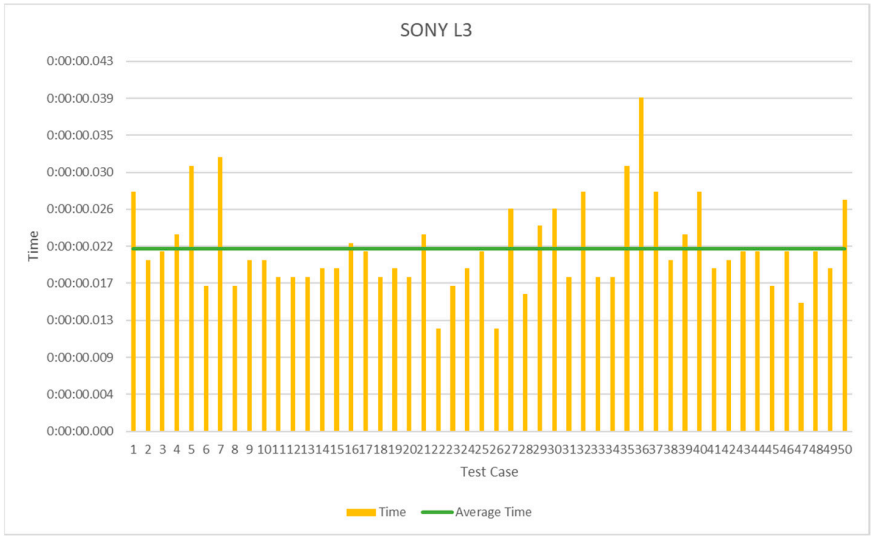
5.2.1. Student-Side App

The test item on the student side is the time from submitting a request for a meal voucher to generating the QR code. This research wrote automated scripts and used the automated testing tool "monkeyrunner" [28] to test the status while students using the app. Two mobile phones were tested in this study, as shown in Table 4.

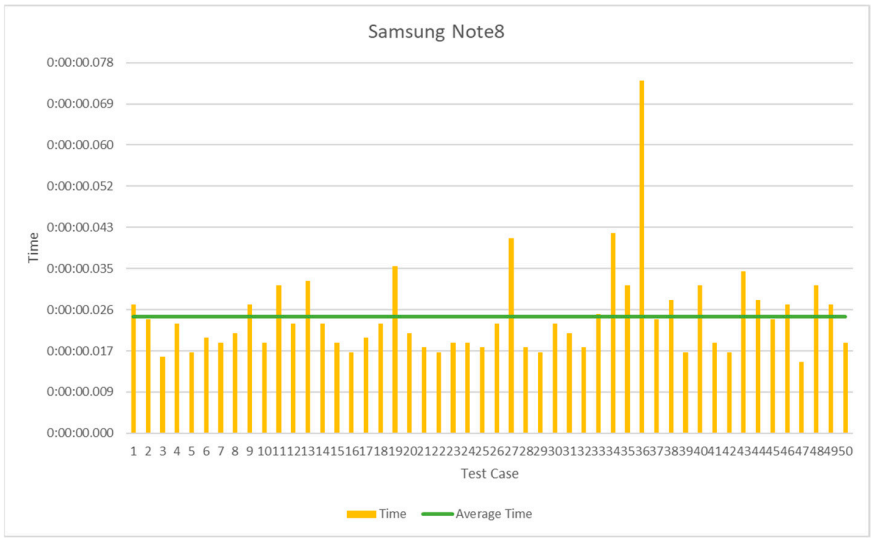
Table 4. Hardware specifications for the two mobile phones.

Phone	Sony L3	Samsung Note8
OS	Android 8.1	Android 7.0
CPU	MTK MT6762/2 Ghz	Exynos 8895/2.3 Ghz
CPU Cores	8	8
RAM	3GB	6GB

A total of 50 test data were prepared in this study. A bar chart of the test results of the two phones is shown in Figure 6, and the summary values of the test results are shown in Table 5.



(**a**)



(**b**)

Figure 6. A bar chart of the test results. (**a**) The test result of SONY L3; (**b**) The test result of Samsung Note8.

Table 5. Hardware specifications for the two mobile phones.

Phone	Sony L3	Samsung Note8
maximum	0.032	0.095
minimum	0.012	0.010
standard deviation	0.005	0.018
average	0.021	0.019

5.2.2. School-Side Webpage

The test items on the school side include the time required for checking the student's qualification and the time from issuing meal e-vouchers to completing writing the data into the blockchain. The issuance of meal vouchers is divided into two test cases: issuing 30 e-vouchers at a time and issuing one e-voucher at a time. A total of 30 test data were prepared in this study. A bar chart of the

times required for checking qualifications is shown in Figure 7, where the maximum value is 0.551 s, the minimum value is 0.383 s, the standard deviation is 0.043 s, and the average value is 0.451 s.

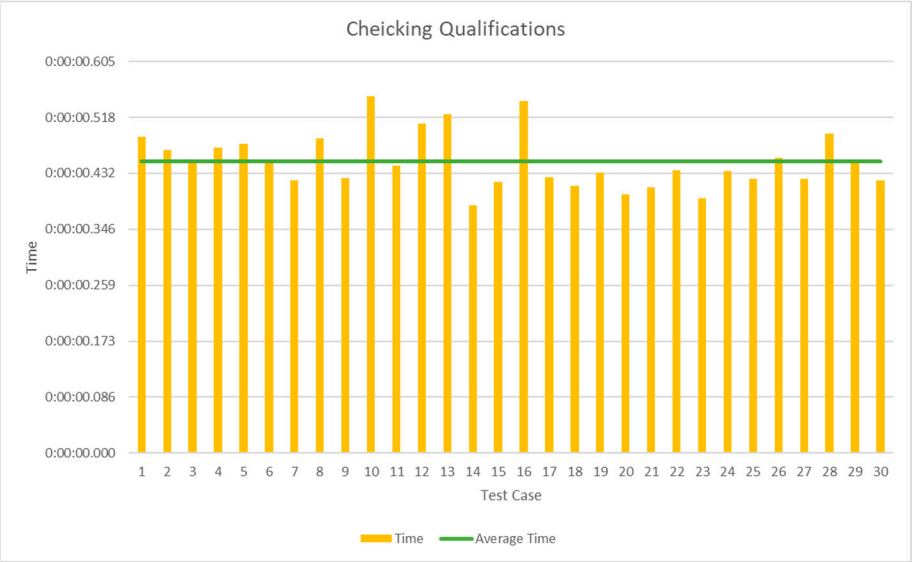
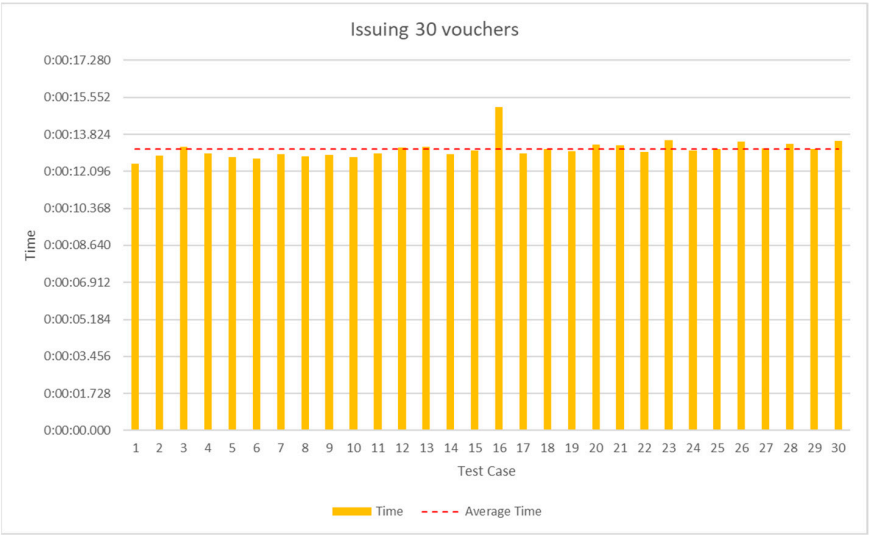


Figure 7. The test results for checking qualifications.

Bar charts of the times required for issuing e-vouchers and writing data into the blockchain are shown in Figure 8, and the test results are summarized in Table 6.

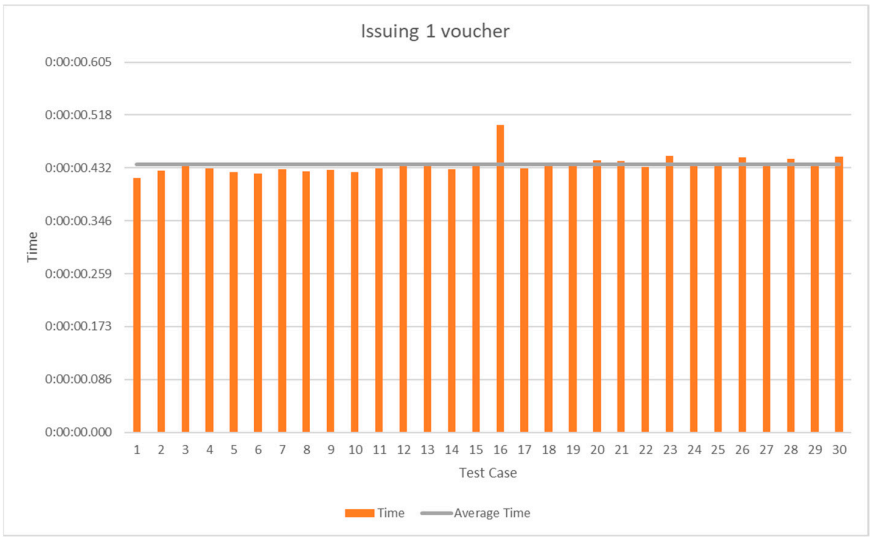
Table 6. Summary of test results of issuing e-vouchers (unit: second).

Test Cases	Issuing 30 E-Vouchers	Issuing One E-Vouchers
maximum	15.078	0.503
minimum	12.465	0.415
standard deviation	0.448	0.015
average	13.129	0.438



(**a**)

Figure 8. *Cont.*



(**b**)

Figure 8. The test results for issuing e-vouchers. (**a**) Issuing 30 e-vouchers at a time; (**b**) issuing one e-voucher at a time.

5.2.3. Cafeteria-Side Webpage

The test item on the cafeteria side is the total time from scanning the QR code, to writing the data into the blockchain, until refreshing the webpage. A total of 30 test data were prepared in this study. Figure 9 shows the test results. We divided the test results into two parts: one was the time from scanning the QR code to writing into the blockchain, and the other is the total time. It can be observed from Figure 9 that a larger proportion of the total time is spent on writing data into the blockchain. Table 7 shows a summary of the test results of the cafeteria-side system.

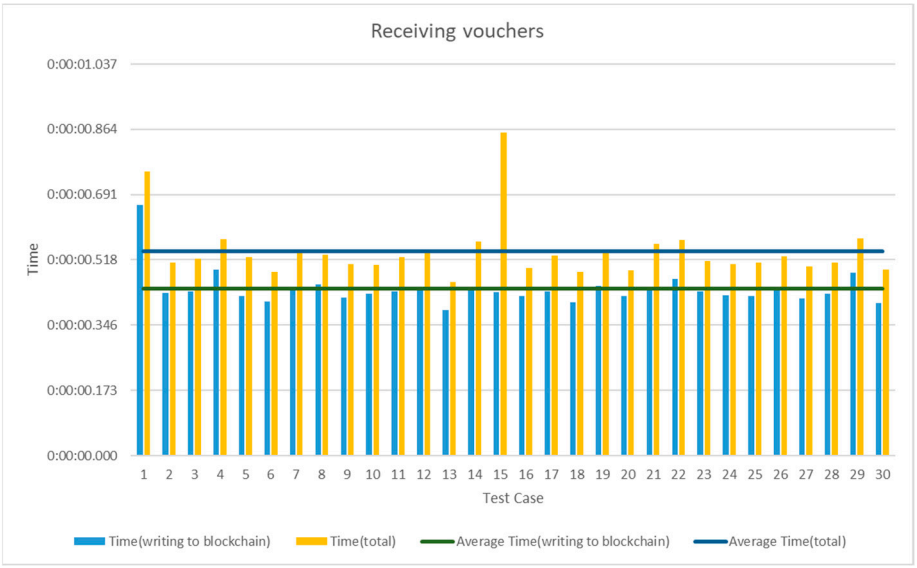


Figure 9. The test results for the cafeteria side.

Table 7. Summary of test results of the cafeteria-side webpage (unit: second).

Test Cases	Writing to Blockchain	Total Time
maximum	0.333	0.423
minimum	0.283	0.356
standard deviation	0.015	0.022
average	0.300	0.402

6. Conclusions

This research proposes an e-voucher system using the architecture of the consortium blockchain. A voucher in this study refers to a kind of ticket that can be used to pay for goods or services, and the issuance of the voucher has social welfare purposes. The so-called social welfare purpose means that the voucher is mainly used to subsidize specific groups, such as low-income households or unemployed workers. Therefore, the voucher is not only an asset, but its use and flow must be able to be monitored; otherwise, it may not be possible to subsidize those who really need it. The characteristic of the consortium blockchain is that it can monitor and track the use and flow of valuable assets. Anyone who wants to use a voucher must be audited to join the alliance.

In addition, this research uses Hyperledger Fabric, which has the characteristics of identity management, a high performance, privacy protection, etc., and enables the complete and secure transfer of assets between organizations. In other words, Hyperledger Fabric is very suitable for business transaction scenarios with permission control and involving multiple roles. The voucher issuance and redemption of this study involves members of different parties, including the non-profit organization, the beneficiaries, and the dealers. At the same time, different permissions must be set for different members. Through security analysis, we have shown that the proposed system can confirm the identity of the issuer, ensure the authenticity of the e-voucher, and achieve non-anonymity and non-transferability. Because the proposed system automates the issuance and redemption of vouchers and can achieve security, this system does not only enable mutual trust without a third party, but also improves the efficiency of the entire process. Finally, this study shows that the system has a good performance through a large amount of experimental data.

6.1. Theoretical Implications

As e-tickets are valuable assets, there must be a trustworthy mechanism supporting the transaction of e-tickets. The traditional e-ticket system introduces a trusted third party (TTP) to verify the transactions to achieve mutual trust among the parties involved in the transactions [17,19,20]. A trusted third party may be an independent agency or a trading platform. Any transaction, such as the issuance or redemption of a ticket, must be sent to the TTP for verification. It can be seen that a TTP is a centralized agent. Once this single, centralized TTP collapses, it represents the collapse of the trust mechanism of the e-ticket system. TTP has been criticized, in fact, for being a security hole [29]. Unlike traditional electronic tickets, this research introduces blockchain technology as the trust mechanism of the system. The blockchain network itself is a decentralized trust mechanism. Any transaction that needs to be written into the decentralized ledger must obtain the consensus and endorsement of nodes over the blockchain network. Instead of relying on the central institution, this study can avoid the system risk caused by the collapse of the central agent.

The implementation of social welfare policies must ensure that beneficiaries truly benefit from social welfare. Therefore, e-voucher systems with social welfare purposes need to provide an identity authentication mechanism. In the e-voucher system under the Farmer Input Supply Program (FISP), the Zambian government delivers the beneficiary a physical card, called a Voucher Scratch Card (VSC), which is linked to the beneficiary's national registration card (NRC) number. The beneficiaries enter the VSC number and NRC number using their mobile phone to redeem the goods. The e-cards are issued by the Zambia National Farmers Union (ZNFU), and the beneficiaries are approved by the Farmer Organization. However, the approved beneficiary list is not directly sent to ZNFU,

but passed to ZNFU through three units, which are the Camp Agricultural Committee (CAC), District Agricultural Coordinator (DACO) and Ministry of Agriculture (MoA); the e-card is not directly issued to the beneficiary, but sent to the beneficiary through DACO. This process delays the delivery of the approved beneficiary list, which in turn leads to the delayed submission and activation of e-cards [9]. The beneficiaries must show the physical VSCs to verify their identity, and a delay in getting the card means that they cannot get the subsidy on time. This research uses digital signatures and asymmetric cryptography as the identity authentication mechanism. The private key is stored privately on the beneficiary's phone, and the public key paired with it is recorded in the blockchain. This study does not include the delivery of physical cards and generates a QR code with an e-voucher and digital signature on the beneficiary's mobile phone. The beneficiary only needs to show the QR code to the dealer, and the e-voucher and identity are verified promptly since all data are digitized. As a result, the entire process can be simplified without layer-by-layer transfer. Even if the process is simplified, this research still maintains the security and trust mechanism because the blockchain is introduced.

6.2. Managerial Implications

Considering fairness, the implementation of social welfare often needs to add some additional conditions or restrictions. Zambia's FISP originally set the beneficiary's benefit period to be two years so that FISP could take care of more beneficiaries without adding a large financial burden. However, the government has failed to remove any beneficiaries from the plan. Consequently, the number of beneficiaries is growing rapidly, and the costs of FIST are becoming higher and higher, which impacts other agricultural budgets. Nevertheless, even since the implementation of the e-voucher system, the government has not established and enforced graduation conditions [9]. From the example of Zambia's FISP, if restrictions cannot be properly set and enforced, it will have a serious impact on the fairness and costs of social welfare. This study can help non-profit organizations to enforce the restrictions of social welfare. All the restrictions can be programed as a secured stored procedure, called a smart contract, and the smart contract enables the blockchain to enforce these restrictions in an automated way and without third parties. It is of great significance not to rely on the implementation of social benefits by third parties. If there must be a TTP trusted by all participants, the TTP essentially becomes an arbiter to decide who may or may not follow the protocol [29]. As a result, social welfare resources may be deliberately manipulated, which makes the restrictions meaningless. Because this study introduces the blockchain without relying on TTP, the implementation of restrictions can be prevented from being manipulated. In addition, human resources can be saved due to the automated execution of restriction.

It is important for the organizations to comply with government regulations. According to Taiwan's Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions, RSA 2048 bits and ECC 256 bits are suggested for ensuring confidentiality, integrity and authentication, and SHA256 and ECC 256 bits are suggested for digital signature to ensure non-repudiation [30]. In this study, the e-voucher and digital signature of the non-profit organization are encrypted using RSA 2048 bits, and the digital signatures of the non-profit organization and the beneficiary are generated using SHA256 and ECC 256 bits. Therefore, the system processes and architectures proposed in this study are feasible and compliant with regulations.

6.3. Socio-Political Implications

In September 2015, the UN Sustainable Development Summit released the 2030 Agenda for Sustainable Development and proposed 17 Sustainable Development Goals (SDG). Goal 1 is to eradicate poverty for all people everywhere and promote equality. Goal 10 is to reduce inequality within and among countries, and one of the targets of Goal 10 is to adopt universal policies and pay attention to the needs of disadvantaged and marginalized populations [31]. The government can implement social welfare policies via issuing vouchers to help those disadvantaged and marginalized populations. However, the government must attract more dealers to participate in the redemption of

vouchers to facilitate the implementation of this policy. The proposed system enables the government and dealers to trust each other, so dealers may be more willing to cooperate with the government. As a result, the policy can benefit more people in need. In addition, beneficiaries may be reluctant to apply to the government agency in person because they fear discrimination from others. Vouchers can be applied for online to avoid the psychological burden and possible discrimination of applicants who apply to social welfare agencies in person. The proposed system allows beneficiaries to complete voucher applications online, which can reduce their psychological burden.

6.4. Limitations

This study does not consider cash flow between the non-profit organization and the dealers. The clearance of vouchers is handled separately by the non-profit organization and dealers. In fact, the complete process should include the participation of financial institutions. The non-profit organization places funds in financial institutions, and the funds can immediately be remitted to the dealer once the e-voucher is redeemed. In future works, the process and system should be further re-designed to consider the role of the financial institution. In addition, this study lacks a reward mechanism for dealers. Although this study can ensure that the dealers do not suffer from financial losses due to illegal tickets or illegal users, it only prevents dealers from excluding cooperation with the government. Strong economic incentives are key to drawing dealers into actively participating in the cooperation. Therefore, future research could design tokens as a mechanism for rewarding each redemption provided by dealers.

Author Contributions: Conceptualization, formal analysis, and methodology, C.-S.H. and S.-F.T.; software, validation, data curation, and investigation, C.-S.H. and Z.-J.H.; writing—original draft preparation, and writing—review and editing, S.-F.T. and C.-S.H.; resources, supervision, and project administration, C.-S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Carter, B.; Roelen, K.; Enfield, S.; Avis, W. *Social Protection Topic Guide*; K4D Emerging Issues Report; Institute of Development Studies: Brighton, UK, 2019.
2. Wikipedia. Social Protection. Available online: https://en.wikipedia.org/wiki/Social_protection (accessed on 17 April 2020).
3. Mendoza-Cavazos, Y. Social Welfare and Sustainability. In *Encyclopedia of Sustainability in Higher Education*; Leal Filho, W., Ed.; Springer: Cham, Switzerland, 2019.
4. Parker, M.D. Social service vouchers: Issues for social work practice. *J. Soc. Soc. Welf.* **1991**, *18*, 39–55.
5. Vace, L.M. Vouchers, Thy Name Is Welfare. 2017. Available online: https://www.fff.org/explore-freedom/article/vouchers-thy-name-welfare/ (accessed on 15 February 2020).
6. United Nations Development Programme. Leaving No One Behind: A Social Protection Primer for Practitioners. 2016. Available online: https://www.undp.org/content/undp/en/home/librarypage/poverty-reduction/-leaving-no-one-behind--a-social-protection-primer-for-practitio.html (accessed on 17 April 2020).
7. Collins Online Dictionary. Available online: https://www.collinsdictionary.com/dictionary/english/voucher (accessed on 15 February 2020).
8. Mofya-Mukuka, R.; Kabwe, S.; Kuteya, A.N.; Mason, N.M. How Can the Zambian Government Improve the Targeting of the Farmer Input Support Program? In *Food Security Collaborative Policy Briefs 146939*; Indaba Agricultural Policy Research Institute: Lusaka, Zambia, 2013; Volume 59, pp. 1–7.
9. Siame, M.; Lichilo, I.; Siame, N. An Assessment of FISP e-voucher Performance. *Int. J. Innov. Res. Dev.* **2017**, *6*, 188–212. [CrossRef]
10. Voshmgir, S. Blockchain & Sustainability. Available online: https://medium.com/crypto3conomics/blockchain-sustainability-7d1dd90e9db6 (accessed on 25 February 2020).

11. Cha, S.C.; Peng, W.C.; Hsu, T.Y.; Chang, C.L.; Li, S.W. A Blockchain-Based Privacy Preserving Ticketing Service. In Proceedings of the 2018 IEEE 7th Global Conference on Consumer Electronics, Nara, Japan, 9–12 October 2018; IEEE: Nara, Japan, 2018; pp. 585–587.
12. Erdenebold, T.; Park, J.Y. Proposing Conceptual Platform for Air Ticketing System Using Blockchain Technology. In Proceedings of the International Conference on Future Information & Communication Engineering, Pattaya, Thailand, 27–30 June 2018; The Korea Institute of Information and Communication Engineering: Busan, Korea, 2018; pp. 5–8.
13. Galen, D.; Brand, N.; Boucherle, L.; Davis, R.; Do, N.; El-Baz, B.; Kimura, I.; Wharton, K.; Lee, J. Blockchain for Social Impact: Moving beyond the Hype. Center for Social Innovation, RippleWorks. Available online: https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf (accessed on 25 February 2020).
14. Moderating Team ROSA. Policy Briefs on Social Transfers—What are Social Transfers? 2013. Available online: https://europa.eu/capacity4dev/hunger-foodsecurity-nutrition/documents/policy-briefs-social-transfers-what-are-social-transfers (accessed on 17 April 2020).
15. Mazvimavi, K.; Murendo, C.; Minde, I.J.; Kunzekweguta, M. Assessing the impacts of Zimbabwe's agricultural vouchers input program. In Proceedings of the 4th International Conference of the African Association of Agricultural Economists, Hammamet, Tunisia, 22–25 September 2013.
16. Kasoma, A.C. Implementation of the e-voucher in Zambia; challenges and opportunities. *PMRC E-Voucher Res. Rep.* **2018**. [CrossRef]
17. Vives-Guasch, A.; Payeras-Capellà, M.M.; Mut-Puigserver, M.; Castella-Roca, J.; Ferrer-Gomila, J.L. A secure e-ticketing scheme for mobile devices with near field communication (NFC) that includes exculpability and reusability. *IEICE Trans. Inf. Syst.* **2012**, *95*, 78–93. [CrossRef]
18. Karaiskos, D.C.; Kourouthanassis, P.E.; Giaglis, G.M. User acceptance of pervasive information systems: Evaluating an RFID ticketing system. In Proceedings of the Conference European Conference on Information Systems, St. Gallen, Switzerland, 7–9 June 2007; Österle, H., Schelp, J., Winter, R., Eds.; Association for Information Systems AIS Electronic Library (AISeL): Atlanta, GA, USA, 2007.
19. Hu, L.; Wang, Y.; Li, D. Uniticket: A third party universal e-ticket system based on mobile phone. *Wirel. Eng. Technol.* **2011**, *2*, 157–164. [CrossRef]
20. Fujimura, K.; Terada, M. Trading among untrusted partners via voucher trading system. In *Towards the E-Society: E-Commerce, E-Business, and E-Government*; Schmid, B., Stanoevska-Slabeva, K., Tschammer, V., Eds.; Springer: Boston, MA, USA, 2001; pp. 445–457.
21. Lusakatimes.com. The FISP E-Voucher Program has been Infiltrated by Fake Agro Dealers. Available online: https://www.lusakatimes.com/2019/06/02/the-fisp-e-voucher-program-has-been-infiltrated-by-fake-agro-dealers/ (accessed on 15 February 2020).
22. Fujimura, K.; Eastlake, D. Requirements and Design for Voucher Trading System (VTS). In *RFC 3506*; RFC Editor: Fairfax, VA, USA, 2003.
23. Eyal, I. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer* **2017**, *50*, 38–49. [CrossRef]
24. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology, Zug, Switzerland, 20–22 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 45–54.
25. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data, Honolulu, HI, USA, 25–30 June 2017; Karypis, G., Zhang, J., Eds.; IEEE Computer Society: Washington, DC, USA, 2017; pp. 557–564.
26. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
27. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
28. Monkeyrunner Reference. Available online: https://developer.android.com/studio/test/monkeyrunner (accessed on 15 February 2020).
29. Szabo, N. Trusted Third Parties are Security Holes. Available online: http://nakamotoinstitute.org/trusted-third-parties (accessed on 2 April 2020).

30. Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions. Available online: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380243 (accessed on 2 April 2020).
31. Sustainable Development Goals. Available online: https://www.un.org/sustainabledevelopment/sustainable-development-goals/ (accessed on 29 March 2020).