

E-Voucher System Development for Social Assistance with Blockchain Technology

Juniardi Akbar

School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, Indonesia
juniardiakbar@gmail.com

Rinaldi Munir

School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, Indonesia
rinaldi@informatika.org

Abstract— The system of providing social assistance in Indonesia is still far from perfect. One of the problems that will be discussed in this paper is the problem of distributing social assistance. In its implementation in the field, one of the alternative social assistance distribution systems is the electronic voucher system. However, this system still uses a centralized architecture which has several weaknesses, such as the existence of a single point of failure to transaction data that is still stored by one party, giving rise to potential fraud. Therefore, blockchain technology is used in an electronic voucher system for social assistance. By using blockchain technology, the electronic voucher system has data with integrity as a form of government accountability.

Keywords— *blockchain, integrity, social assistance, electronic voucher, decentralized system*

I. INTRODUCTION

Social assistance is the distribution of assistance from local governments to individuals, families and community groups that are unsustainable, selective, and aim to minimize the social risks. Social risks are events that can cause potential social vulnerabilities by individuals, families, groups and/or communities as a result of social crises, economic crises, political crises, and natural disasters that can cause people to live in unreasonable conditions.

Indonesia's geographical condition is in a disaster-prone area and the number of poor people of Indonesia which almost reached 10% according to data from Indonesia Statistic Centre (BPS) in 2020, has caused the government to create many social assistance programs. Based on its form, social assistance is generally divided into cash and non-cash. One example of non-cash social assistance is the groceries (*sembako*) program. In addition to cash and non-cash assistance, there are alternative forms such as electronic vouchers.

Indonesia's geographical condition in the form of islands demands that many stakeholders are required to take part in the distribution process of the non-cash social assistance program. Many stakeholders need coordination and supervision in this distribution. With so many stakeholders involved, the distribution system will require close coordination and supervision. An example is the involvement of the National Police as mentioned by the Minister of Social Affairs to oversee the process of distributing social assistance to make it more targeted, while ensuring that there are no irregularities in the field. This is the weakness of the non-cash assistance program where the large number of parties involved will increase the potential for dishonesty.

Social assistance in the form of vouchers can be used as a good alternative in preventing corrupt practices as well as

simplifying the process of providing assistance. One example of social assistance with the form of vouchers is Non-Cash Food Assistance (*Bantuan Pangan Non Tunai* also known as BPNT). BPNT is a social assistance in the form of non-cash food through the mechanism of electronic vouchers that are used only to buy foodstuffs at food vendors or *e-warong* in cooperation with banks. The flow in the BPNT system will be applied as a reference for the electronic voucher system that will be created. But of course, there are some limitations and simplifications.

According to Black's Law Dictionary 9th Edition, vouchers have the meaning as a confirmation to give the holder the right to make payments, repayment of a debt, or written authority. Because vouchers have a value equivalent to money, the ability to not be faked will be very important to have. In addition, vouchers for social affairs are only intended for eligible individuals who can receive and use the voucher. The voucher system must also be able to guarantee that every transaction recorded has integrity as a form of transparency and accountability from the government.

One of these problems can be solved by using blockchain technology. This technology has the main characteristic that the stored data is immutable so that it cannot be changed by anyone. So that it is almost impossible for anyone to change data such as the value in the voucher or the beneficiary data in the system.

Then, blockchain technology will reduce the need for a trusted third party to mediate in every transaction. In this way, the costs involved will also decrease. Having smart contracts in the blockchain eliminates the need for third parties. In addition, because of the decentralized network, the blockchain can eliminate dependence on one party.

II. RELATED WORK

The development of an electronic voucher system for social assistance with blockchain technology is still very rarely discussed. Even the development of electronic voucher systems in general with blockchain is still not much discussed. Blockchain technology has many benefits that are suitable for voucher systems such as solving the problem of proof of identity in transactions, anti-counterfeiting, transparency, and data immutability.

Because specifically the use of blockchain is still not widely applied to electronic voucher systems, we will discuss the related systems that use blockchain for electronic tickets. The electronic ticket system has properties that are almost like electronic vouchers so that it can be used as a comparison for related work.

There is a paper entitled “A Smart Contract-Based Mobile Ticketing System with Multi-Signature and Blockchain” [4] which discusses the implementation of blockchain in ticketing systems. This paper uses blockchain technology to be applied to a decentralized ticketing system. The system uses smart contracts on the blockchain to ensure the correct execution of transactions. A multi-signature mechanism is used to guarantee the authenticity and ownership of tickets. Money transfers involved in transactions are also multi-signature authorized.

In the proposed blockchain-based mobile ticketing system, event organizers sell tickets on the blockchain via smart contracts. Transaction integrity is ensured by smart contracts and multi-signature mechanisms, which protect consumers from counterfeit tickets and guarantee ticket validity. Digital signatures from event organizers and consumers are required to sign a QR code ticket for activation which guarantees ticket ownership.

Moreover, since all transactions are recorded on the blockchain which is traceable and immutable, in the event of a dispute over the use of the ticket, it can be resolved based on the information recorded on the blockchain. Apart from transaction integrity, blockchain platforms have an extra advantage in system stability. The mobile ticketing system used on a blockchain-based decentralized platform protects the system from a single point of failure.

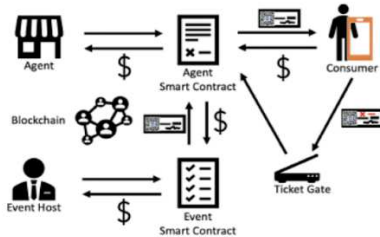


Fig. 1. Implemented system illustration

III. STUDY LITERATURE

A. Distributed System

Coloris (2005) describes a distributed system as a system that has hardware and software components located on a computer network and coordinates by conveying messages to each other. Meanwhile, Tanenbaum (2007) defines a distributed system as a collection of computers that are mutually independent and will be seen as a single computer by the client.

The main motivation in creating a distributed system is the ability between components (clients) to share resources without the need for a centralized server. This is an advantage of a distributed system, which eliminates the need for a centralized server. Distributed systems are considered to have the advantage of minimizing the risk of failure (fault tolerant). But of course, there are some challenges in building a distributed system such as failure, scalability, synchronization and replication. A good distributed system must be able to cope when part or all of the system fails. A distributed system is said to be scalable if the cost of adding nodes is directly proportional to the resources that must be added [1].

B. Cryptography

Cryptography is a science that studies the application of deep mathematical techniques related to information security aspects such as confidentiality, data integrity, authentication, and non-repudiation (anti-denial). The aim of cryptography is to apply these four fields in both theory and practice. Along with the times, the function of cryptographic algorithms is growing so that it is not only a method for hiding messages, but also as an effort to prevent and detect fraud or other malicious activities [2].

There are several cryptographic methods related to blockchain implementation such as symmetric key encryption, public key encryption, and hash functions.

1) Symmetric Key Encryption

In symmetric-key cryptography, the security is only held in the confidentiality of the key, while the algorithm itself does not need to be secret. The weakness of symmetric-key cryptography is that the recipient of the message must have the same key as the sender of the message so that the sender of the message must find a way to tell the key to the recipient of the message.

2) Public Key Encryption

In public key cryptography, there is no need to distribute the secret key (private key). Then with the presence of two keys (private key and public key), the number of keys can be pressed. To communicate secretly with many people, the process is only by declaring two keys, namely the public key to encrypt the message and the private key to decrypt the message received.

3) Hash Function

The hash function is a cryptographic algorithm that converts a plaintext message of arbitrary length to a short message of a fixed length (constant). The hash function is one-way, which means that a short message can no longer be decrypted into plaintext. Some examples of cryptographic hash algorithms are SHA-2, SHA-3, and MD5.

The most common cryptographic use of hash functions is as digital signatures. As a digital signature, long messages will be converted with a hash function and only the hash value will be signed. The receiving party then hashes the received message and verifies that the received signature is correct for this hash value [2]. One of the uses of hash functions is to ensure data integrity. Two plaintexts that differ only by 1 bit, will produce a short message that is significantly different.

C. Blockchain

Blockchain can be viewed as a distributed ledger scheme that is collectively managed and decentralized. This technical scheme consists of many blocks that pass through a number of nodes in the system that are secured using cryptography. Decentralized systems do not recognize a central server that has full access to all data. In a decentralized system, the data contained in the blockchain will be spread over many servers.

1) Blockchain Architecture

Blockchain is a data structure that allows the creation of an immutable ledger of transactions spread across multiple servers. This technology uses public key cryptography to sign

transactions between parties. The data on each transaction will be stored in a distributed ledger. The distributed ledger will consist of cryptographically linked transaction blocks [3]. The transaction blocks will be connected to each other in a chain which defines the blockchain literally as a chain or chain of blocks.

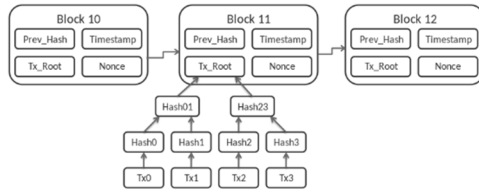


Fig. 2. Blockchain architecture

2) Blockchain Characteristic

First, blockchain is decentralized. The decentralized system on the blockchain means that transactions do not need to be validated by a single party. A consensus algorithm will be used in the blockchain to maintain data consistency in a distributed network. The distributed system will avoid a single point of failure situation when a server fails and results in paralysis [5].

Second, blockchain is persistent. The system on the blockchain guarantees transactions can be validated quickly so that corrupt transactions (changed or invalid) will not be accepted. This makes it almost impossible to tamper with transactions that have been recorded on the blockchain because blocks with invalid transactions can be easily found.

Last, blockchain is secure. All information on the blockchain is secured using cryptographic algorithms. In theory, it is almost impossible to hack a blockchain network, or at least it takes a very large effort with a very high level of complexity to do so.

3) Blockchain Classification

Blockchain can be classified into public blockchain and private blockchain. The public blockchain system allows everyone to join which means that everyone can read and write transactions, perform audits on the blockchain, and review the blockchain network. The weakness of public blockchains is vulnerability to attacks. Attackers can do damage to transactions that will be recorded in the block as well as damage to transactions that have already been recorded. Therefore, a strong consensus mechanism is needed to validate each new block that you want to [5].

In a private blockchain system, a node must first get approval to be able to join the blockchain network. The participation of a party will be determined by the nodes that control the access of the blockchain network. The presence of a central node on the blockchain network will reduce the decentralized nature of the blockchain. Once nodes become part of the network, they can contribute to a decentralized network. Each node must maintain a copy of the ledger and collaborate to reach consensus each time a block is added [5].

IV. DESIGN AND IMPLEMENTATION

The following is the flow of the e-voucher system for social assistance that has been implemented in the BPNT.

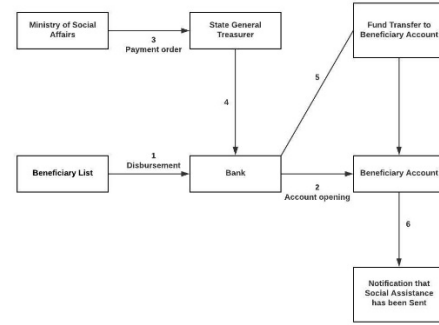


Fig. 3. Illustration of BPNT distribution mechanism

- The bank opens an electronic account for each Beneficiary Family (KPM) based on the Beneficiary List (DPM) from the Ministry of Social Affairs.
- The transfer of aid funds will be transferred from the Ministry of Social's account to the bank to the KPM assistance electronic account.
- The channelling bank provides notification that the funds have been transferred to the KPM account (can be in the form of SMS to KPM's cellular phone number).
- Beneficiaries come to *e-warong* who have collaborated with local banks by bringing their IDs.
- KPM then selects the type of assistance according to the quota and buys the desired food.

It can be seen from the mechanism of the electronic voucher system that is already running at BNPT, blockchain technology can be applied to the creation of electronic accounts, the creation of electronic vouchers, and recording transactions when the voucher has been used. The system created will also adopt the BNPT system with the flow made as similar as possible. But of course, there are simplifications such as in the bureaucratic process between government institutions (Ministry of Social Affairs, State General Treasurer, and Banks).

Then in the implementation of the electronic voucher system, the process of transferring aid funds will be simplified. As a substitute for transfers of aid funds from banks to KPM accounts, the prototype system will implement tokens in the blockchain network that will replace the money function of currency in conducting transactions between social assistance recipients and shop owners.

In this system, when the voucher is generated, the role of the bank is to send the token to the voucher. The role of banks can be eliminated to facilitate the process of forming vouchers by seeing vouchers as a medium of exchange circulated by the government. However, to make the system as similar as possible to the BPNT system, the author decided to still involve the bank by assuming that this electronic voucher is the currency or exchange rate issued by the bank.

Then the electronic voucher system using blockchain technology to be implemented must meet the following criteria.

- The system can guarantee data integrity because the data cannot be modified after being stored.
- No one party has complete control over the stored transaction data.
- The system can defend against single point of failure attacks.

In point a, the use of a hash function makes the blockchain immutable. This means that no one party can change the data to minimize fraud that can occur. Each party must honestly and transparently report the value of the assistance received and sent so that fraud tracking can be easily carried out.

Then on the next two points, the decentralization of the blockchain has an important role. In point b, the nature of decentralization will protect against single point of failure attacks. As for point c, the nature of decentralization also eliminates the need for parties to be in control of all data.

The system must be able to meet the functional requirements to manage the lifecycle of an electronic voucher. The electronic voucher lifecycle can be divided into 4 parts, namely voucher creation, token transfer, voucher exchange, and voucher exchange confirmation. Although the use of blockchain in theory will guarantee data integrity, a system will be designed that will ensure data integrity by accompanying digital signatures on every transaction that is accompanied by financial transactions such as money transfers to vouchers and voucher exchanges.

To meet some of the criteria above, the Hyperledger Fabric framework will be used. This framework has been designed to have smart contracts that can be used. In addition, Hyperledger Fabric is designed as a permissioned blockchain so that every participant in the network is a participant who has been recognized and has access permission. Hyperledger Fabric is more suitable to be used as a tool for system prototype development.

As for this prototype, there are several non-functional requirements which can be seen in the following table.

TABLE I. NON-FUNCTIONAL REQUIREMENT

Code	Parameter	Requirement
NF01	Availability	The prototype must continue to run even if a peer dies.
NF02	Integrity	Prototypes can prevent transaction data from being altered in an unwanted way.
NF03	Security	The ability of the system to handle security threats.

While some security threats that may be experienced by system that has been built can be seen in the following table.

TABLE II. SECURITY THREATS

Threat	Attacker's Action	Example
Device theft	The beneficiary's device was stolen.	A beneficiary's phone was stolen, and he exchanged his voucher at one of the stalls

Tampering data on nodes	Changing the data on the node that the attacker is running on.	Someone changes the balance data held by a voucher and exchanges the voucher beyond the proper limit
-------------------------	--	--

In the electronic voucher system architecture using blockchain technology, there are three main parts, including the Hyperledger Fabric blockchain layer, the frontend layer that directly interacts with users, and the last is the backend layer that interacts directly with the blockchain. The general architecture of this prototype electronic voucher system can be seen in figure below which illustrates the relationship between the blockchain, frontend, and backend layers.

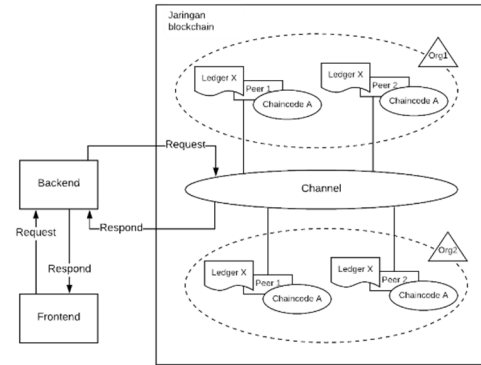


Fig. 4. System prototype general architecture

A. Blockchain

The blockchain layer is the most important part in this prototype system. The blockchain technology that will be used is Hyperledger Fabric which has smart contracts that will be installed in each peer in several organizations in the blockchain network. In figure above, the general components contained in the Hyperledger Fabric blockchain network have the following components.

- There is a channel that will bridge between the backend and the blockchain network.
- There are two organizations in the blockchain network namely government and bank.
- There are multiple peers within an organization in a blockchain network.
- Ledger held by each peer that contains transaction data that occurs in the blockchain network.
- There is a chaincode which is a smart contract in the blockchain network that provides some of the functionality of this prototype system.

In the prototype system that was built, some of the operations implemented in the chaincode are as follows.

1. CreateVoucher

This operation will create a voucher by receiving data such as owner's name, phone number, identity number (NIK), category, and date expired. When the voucher has been successfully created, the voucher will have a default value that is still blank. Then after the voucher is successfully created, a token request will be made to the bank.

2. TransferToken

This operation will send the token to the selected voucher. After the token for a voucher has been successfully processed, the voucher now has a value that is ready to be exchanged.

3. RedeemVoucher

This operation is the first step to send tokens from vouchers to stalls. This operation will first check whether the value of the token to be exchanged does not exceed the nominal amount of the balance on the voucher and ensure that the voucher has not expired. The purpose of this operation is to generate an OTP code which is used to confirm whether the token is suitable to be sent or not.

4. ConfirmRedeemVoucher

This operation is the final step to send tokens from vouchers to stalls. This operation will receive an OTP code to be matched. If it is appropriate, the nominal voucher balance will decrease, and the shop token will increase.

B. Backend

The backend layer is the bridge between the frontend and the blockchain network. One of the advantages of Hyperledger Fabric is that it has provided an SDK to send transaction requests from clients to a blockchain network that already supports many programming languages such as Java, JavaScript, and Golang.

The backend layer will receive requests from the frontend layer via REST API communication. This request will then be sent to a channel on the blockchain network. The response results will then be received by the backend layer and then will be forwarded back to the frontend layer.

C. Frontend

The frontend becomes the interface of the system prototype that interacts directly with the user. At the frontend layer, processes such as receiving user input, verifying user input will be carried out, and displaying response data obtained from the blockchain. There are two interfaces in this prototype system, including SMS-based and the web-based. SMS-based will be the interface for the social assistance recipients. The next form of frontend that will be implemented is a website which is a form of interface for shop owners and the government.

One of the pages created is the voucher registration. Admin will register the voucher number by filling in the identity number (NIK), phone number, recipient name, assistance category, voucher value, and voucher expiration date.



Fig. 5. Create new voucher page

Another page that will be explained is voucher redemption. Vouchers are redeemed by the store by filling in the voucher id and the items to be spent. Then to confirm, an OTP code will be sent to the social assistance recipient's SMS




Fig. 6. Voucher redemption



Fig. 7. Voucher redemption confirmation

V. EXPERIMENT AND ANALYSIS

In implementing the prototype system, it was found that Hyperledger Fabric is suitable for use as a framework for electronic voucher systems in government environments. This is because Hyperledger Fabric is designed as a permissioned blockchain so that every participant in the network is only an identified participant and has access permission. In this case, only the government, banks and shops will gain access to the network.

The proposed system prototype architecture can also be implemented and function well in processing the voucher life flow. In the prototype architecture, there is a channel that will bridge between the backend and the blockchain network. The blockchain network will be run by two organizations namely the government and the bank. Each organization in the blockchain network will have multiple peers. The interaction will be carried out on the frontend and will be forwarded with a REST API to the backend which will forward the interaction to the Hyperledger Fabric blockchain network.

Then to test availability requirements, we can kill one or more nodes of the blockchain on the docker container. To perform availability testing, one of the nodes of the blockchain in the docker container will be shut down. It turns out that the system continues to run as usual even though there are dead nodes.

```
peer node start -- About an hour ago Up About an hour 0.0.0.0:7051->7051/tcp peer0.org1.example.com
peer node start -- About an hour ago Up About an hour 7051/tcp, 0.0.0.0:9051->9051/tcp peer0.org1.example.com
peer node start -- About an hour ago Up About an hour couchdb:3.1.1 couchdb0
peer node start -- About an hour ago Up About an hour 4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp couchdb1
peer node start -- About an hour ago Up About an hour 0.0.0.0:7050->7050/tcp orderer.example.com
peer node start -- About an hour ago Up About an hour 4369/tcp, 9100/tcp, 0.0.0.0:7984->7984/tcp couchdb1
peer node start -- About an hour ago Up About an hour 7054/tcp, 0.0.0.0:8054->8054/tcp ca_org1
peer node start -- About an hour ago Up About an hour 7054/tcp, 0.0.0.0:9054->9054/tcp ca_orderer
peer node start -- About an hour ago Up About an hour 0.0.0.0:7054->7054/tcp ca_org1
```

Fig. 8. Stopping one of the nodes in the docker container

In the picture above, there are several nodes running on top of the docker container. Furthermore, a command has been executed to stop one of the nodes in the docker container i.e., *peer0* in *organization1*. After stopping the peer, the blockchain operation will be called. The operation that is run on the test is the operation to get all data on the ledger and the result is that the system continues to run well. Since the

system can run even if one of the peers dies, the system satisfies the availability point for the non-functional requirements.

The next test is integrity that will be carried out through several experiments to change the data that enters the network which should not happen. This test is carried out with the following experiments:

- Change your own transaction data.
- Trying to enter a new transaction into your own transaction history.

The two experiments above were carried out by direct invoke chaincode. Neither can be done because it is already handled on the chaincode side.

As for system security testing, there are two threats to be analysed.

1) Device theft

To mitigate the threat of device theft, the recipient of the social assistance must immediately report to the relevant operator to gain access to his or her mobile number. In addition, the problem of device theft will lead to the potential for the voucher to be used by other people (thief). The process that requires a social assistance recipient device is a voucher exchange confirmation process in which the system will send an OTP code via SMS to the social assistance recipient's mobile number.

This problem can be solved non-technically by adding regulations to the voucher exchange confirmation process. The shop owner will be notified with brief information such as name and identity number (NIK) from the recipient of the social assistance on the voucher exchange confirmation page. The shop owner must verify the social assistance recipient manually to be able to process the voucher redemption.

2) Tampering data on nodes

To perform this test, we will use an API specifically found on the Hyperledger blockchain. The Hyperledger blockchain itself has a special function that makes a request targeting only one node on the blockchain.

By sending a request, the transaction created will only be committed to the node with the id peer0.org1.example.com. Whereas in a blockchain network a transaction must have the approval of every peer0 on org1 and org2. Therefore, this transaction will be rejected because it does not meet the number of approved nodes.

The electronic voucher system created still has several weaknesses that require several assumptions to be fulfilled. The first assumption is that the system is assumed to be

running on a very secure server. This is because there are several certificate authorities on the backend that contain the private key.

The second assumption is that the implementation is tested on a single local machine with multiple peers running with a docker container. Systems in a production environment may require implementation on more than one machine thus requiring additional test scenarios.

From the whole test, it can be concluded that this prototype has been running quite well. Non-functional testing has been fulfilled quite well. However, there are still shortcomings in the security requirements of the security threat of device theft.

VI. CONCLUSION

Electronic voucher systems using blockchain technology can guarantee data integrity and accountability. The system has successfully met all requirements and its integrity has been met. The Hyperledger Fabric is suitable for developing electronic voucher systems. This technology was chosen because it is designed as a permissioned blockchain so that every participant in the network is a participant who has been recognized and has access permission. In addition, Hyperledger Fabric is also designed to have a smart contract that can facilitate the development process.

The prototype of the electronic voucher system already has the functionality to manage the life flow of electronic vouchers, from voucher creation, token transfer, to voucher exchange. However, improvements in system security and system scalability testing are needed if the system is to be used in a production environment.

ACKNOWLEDGMENT

The author would like to express gratitude to Dr. Ir. Rinaldi Munir, M.T. as the thesis advisor for the author's final project in Bandung Institute of Technology (ITB) for giving much helpful advice, knowledge, and guidance that helped the author to present this paper properly and correctly. The author would also like to thank the author's family and friends that helped motivate and gave support so that the author can finish the thesis and this paper with passion.

REFERENCES

- [1] Coulouris, G. F., Dollimore, J., & Kindberg, T. (2005). Distributed systems: concepts and design
- [2] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography.
- [3] Kshetri, N. (2017). Can blockchain strengthen the internet of things?
- [4] K. Lin, Y. Chang, Z. Wei, C. Shen and M. Chang. (2019). A Smart Contract-Based Mobile Ticketing System with Multi-Signature and Blockchain
- [5] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems.private