CBP2P: Cooperative Electronic Bank Payment Systems Based on Blockchain Technology

Zhao-Ping Peng[1], Mao-Lun Chiang[2], Iuon-Chang Lin[1], Chou-Chen Yang[1], Min-Shiang Hwang[3,4*]

[1] Department of Management Information System, National Chung Hsing University, Taiwan
[2] Bachelor Degree Program of Artificial Intelligence, National Taichung University of Science and Technology, Taiwan
[3] Department of Computer Science and Information Engineering, Asia University, Taiwan
[4] Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan
jpeng50204@gmail.com, mlchiang@cyut.edu.tw, iclin@nchu.edu.tw, cc.yang@nchu.edu.tw, mshwang@asia.edu.tw

Abstract

The most common consumer behavior was to pay in cash at a physical store in the past. However, with the rapid development and popularization of smart handheld devices and computers, merchants have had many innovative business models in recent years. For example, the digital cryptocurrency Bitcoin has the advantages of decentralization, anonymity, and the inability to tamper with data. If these benefits are combined with the current electronic payment financial operation model, they will be highly innovative. However, blockchain technologies have been applied to decentralized network architectures. As a result, the financial system will face anonymous crime, extensive data synchronization, and time-consuming transaction processes. This paper implements a P2P electronic payment system with a hierarchical structure based on the blockchain architecture, called CBP2P (Cooperative Bank Peer-to-Peer), to improve the defects and realize an accurate electronic payment system. Through the characteristics of the blockchain and cooperation between banks, we will enhance the security and availability of the system.

Keywords: Bitcoin, Blockchain, Peer-to-peer network, Electronic payment, Public key infrastructure, Consensus algorithm

1 Introduction

Bitcoin is a decentralized digital currency system proposed by Satoshi Nakamoto [1]. There is no existing central clearing unit or financial institution in the Bitcoin system. All system steps are performed by nodes in the P2P (peer-to-peer) network. The payment process between users can only be done through the network and wallet software. The system will create distributed data by downloading Bitcoin Core, and it must synchronize the previous data before it can use the transaction service. The wallet software will generate a public address and a private key to identify the user and sign the transaction. The protection of transaction data is achieved by calculating hash values. Then, the operating parameters are used to associate each data with forming a so-called blockchain.

Since Satoshi proposed the Bitcoin system in 2008, the total amount of data in the blockchain has reached about 71.8G. It continues to grow [2], which has caused users to consume a lot of storage space and network when synchronizing data. The private key created by the user is proof of ownership of the property in the wallet. Assuming that unbacked wallet files or local computers are threatened, it may result in theft or loss of Bitcoin. For example, James Howells of the United Kingdom claimed that he owned nearly 7,500 bitcoins between 2009 and 2013. Still, the house was cleaned one day and accidentally discarded the wallet file's hard drive, causing a considerable loss. To improve the time-consuming data synchronization of distributed users and maintain the responsibility of Bitcoin, the exchange mechanism has been developed. Users only need to go to the exchange to apply for an account and conduct various digital currency transactions without synchronizing large amounts of data. However, this method also has many security issues. For example, Coincheck in Japan was stolen by a hacker for virtual defects, while Binance stole many user accounts. The same problem occurs in South Korea, Hong Kong, and other places.

Furthermore, the exchange database is usually centralized. Therefore, if the system is vulnerable or hacked, it will cause huge losses and be difficult to track due to its anonymity. Therefore, we have listed some of the problems faced by the technology used by Bitcoin:

1) Blockchain data synchronization:

Users must spend huge time and network resources to synchronize past data before using the service, so they must provide effective storage space to store data [3].

2) Decentralized data storage:

The exchange database is usually centralized. If it is attacked or invaded, and there is no backup, it will cause huge losses. As far as Bitcoin is concerned, a peer needs to manage its currency and bear the risk of loss and theft.

3) The challenge of real-time trading:

In Bitcoin, the transaction will take about 30 minutes to make it legal because miners must find the appropriate nonce to mine the block on a certain difficulty and obtain proof of consensus POW. It is impossible to let the transaction wait for such a long time [4].

4) Anonymity and crime:

In the Bitcoin transaction process, the amount is transmitted through the address, and the generation of the address has nothing to do with the user's real identity.

*Corresponding Author: Min-Shiang Hwang; E-mail: mshwang@asia.edu.tw

DOI: 10.53106/160792642022072304004

Therefore, many black market transactions are carried out through this feature, making it difficult for law enforcement agencies to track [5].

5) Consume huge system resources:

Because only the fastest miner can get a block and reward, the mining done by other miners is useless and needs to be discarded, resulting in a waste of resources [6].

To solve the previous problems and take the current electronic payment model as a scenario, we propose a hierarchical peer-to-peer system, which divides the decentralized system into banks, as a super-peer layer and a user layer. A consensus is reached through rapid mining at the bank level to generate a blockchain, speed up transactions, and store the entire blockchain data at the bank level. As a result, bank cooperatives maintain blockchain data and greatly reduce system costs [7]. Furthermore, there is no need to download and store synchronized blockchain data for users, which is convenient and does not waste space. At the same time, through the operation of the bank layer, the transaction speed is fast, and no third-party intermediary is required.

2 Overview of Blockchain Technology

Blockchain technology provides users with a decentralized way to maintain and store data. The architecture is shown in Figure 1.

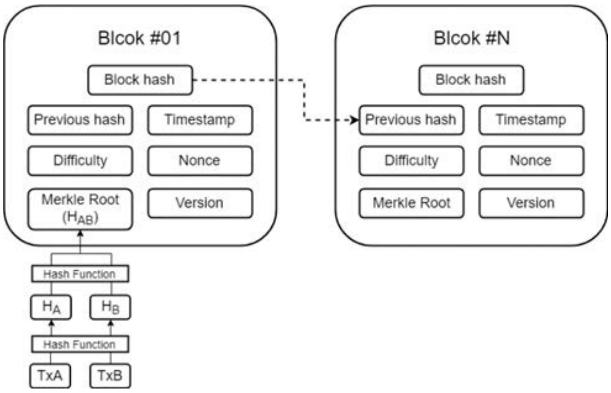

Figure 1. Blockchain data architecture

The generated data is stored in blocks. Each new block is generated by adding the previous block's hash to form a chained data structure to ensure the integrity of the data so that all network members can participate in the verification of data. Once the data has been verified and synchronized, it cannot be modified or deleted [8]. The data fields in the block are described in the following:

- Number of Transactions: The total number of transactions in this block.
- Timestamp: Unique number generated when the block is created [9].
- Difficulty: The difficulty when the block was created.
- Hash and Previous Block: The hash value of the block and the previous block. And the blockchain is also used to make each block interlock, so the blockchain has traceable and untampered features.
- Merkle Tree: All transaction information in this block.

Blockchain has brought great changes to the security of data and traditional system architecture. For example, the bitcoin system protects transaction data integrity through cryptography, decentralized data storage, and network structure without a centralized institution. The following will introduce blockchain core application technologies.

A. Decentralized Architecture

Blockchain is the technology used in underlying Bitcoin, and the network architecture is fully decentralized. When new users want to use Bitcoin's transaction-related functions, they must download and install the wallet software. At last, the system will request all of the previous blockchain data from the neighboring nodes for synchronization. Through the p2p network structure, each node will back up the raw data. As long as there are more nodes, the backup of the data will be more needed. Unlike the traditional client-server architecture, it effectively avoids catastrophic attacks and malicious tampering and has no central control unit. Each node maintains the entire decentralized ledger and network operation according to the agreed consensus [10]. However, the blockchain data is continually growing, so a new user who wants to use the service must use a huge amount of resources to synchronize the data to use the service. Thus, although the decentralized architecture greatly enhances security, it also sacrifices performance.

B. Public-key Cryptography

When a user sends a transaction, the other party's address must be specified and signed with its private key before sending it. In contrast, other users can confirm the correctness of the transaction data through the encryption and the decryption relationship between the public key and private key [11]. Although public-key cryptography ensures the wallet's security and data transmission, it also increases the risk because the generation of the address is not directly related to the user's identity, so the criminal often uses the bitcoin as a medium to conduct illegal transactions. On the other hand, if the user loses its private key and does not properly back it up, there will be no other way to retrieve the wallet. In 2020, Liu *et al.* proposed an ECC-based digital currency anonymous transaction scheme to ensure the anonymity of the sender and receiver [12].

C. Consensus Algorithm

Proof of work (POW) is a consensus algorithm used on Bitcoin. In this session, the nodes responsible for processing the transaction data into blocks are called miners. By setting the nonce and using the CPU or GPU, it computes a data-generated hash value to get rewards, and this hash must meet the difficulty condition to be a legal block hash, which is also commonly known as "Mining." The difficulty of Bitcoin is dynamic, and it can generate a block in about 10 minutes. The most widely discussed security issues are 51% of attacks. Once an attacker has mastered a calculated ability of more than 50% of the entire network, it can reverse or rewrite blockchain data. Ghash.io is currently the most powerful mine, with overall computing power accounting for more than 42% of the entire network. This highly centralized computing power is a concern about the security of bitcoin networks [13]. In 2019, Li *et al.* proposed a more efficient intra-committee consensus algorithm than Byzantine Fault Tolerance (BFT) [14]. In 2021, Navaro *et al.* proposed an adaptive and practical

BFT algorithm in the authority blockchain. They divided the nodes into trusted and failed nodes, in which nodes with defective reputations are excluded from voting [15]. Recently, Wen *et al.* proposed a consensus mechanism of quantum blockchain based on the randomness and irreversibility of quantum measurement and zero-knowledge proof [16].

3 CBP2P Architecture

To solve massive data synchronization and excessive resource consumption in the Bitcoin blockchain, we propose a hierarchical structure CBP2P in a real financial environment. As shown in Figure 2, the trusted bank is a super-peer in the alliance blockchain, used to maintain transaction data security.

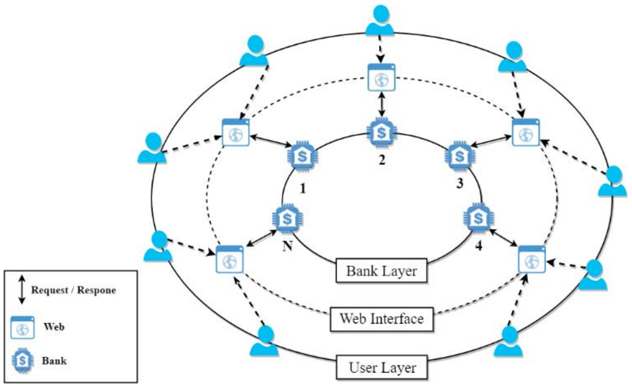

Figure 2. CBP2P system architecture

The system is divided into a user layer, a Web interface layer, and a bank layer. The functions and descriptions of each layer are as follows.

3.1 User Layer

Users do not have to retain the risk of losing their currencies and wallets, nor worry about data synchronization time, storage devices, and network resources, but apply to register an electronic wallet with a real identity so that they can transact with other users [17]. Transaction data is generated by the trusted bank layer and stored in the distribution to ensure its integrity and undisturbed. The benefits are as follows:

- No need to waste time and resources to synchronize data;
- Transactions do not have to be processed by traditional third parties;
- User data is stored in decentralized super peers to prevent malicious attacks.

3.2 Web Interface

The web interface architecture is shown in Figure 3. To solve the customer ownership problem of each bank, when using the electronic wallet, the user must first register on the designated bank page, as shown in Figure 4.

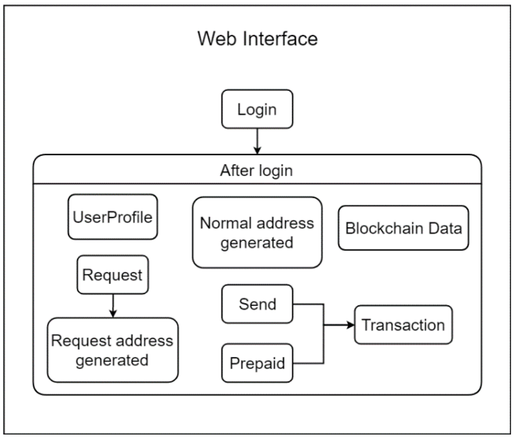

Figure 3. CBP2P system architecture

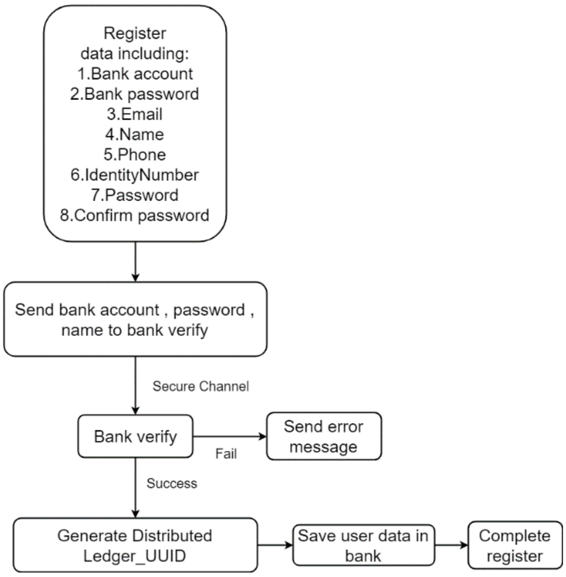

Figure 4. Registration process

This mechanism ensures that bank customers can use p2p blockchain transactions; even if the system is attacked, the user's data is stored in each bank's super-peer to ensure that the user's data and property will not be stolen or lost. The transaction is conducted on the bank's blockchain to ensure the normal execution of the transaction. When registering, the user must enter the bank account number and password, e-mail, real name, phone number, ID number, and set the password to log in to the electronic wallet system. The data will then be sent to the bank for verification through a secure channel. If the verification is completed, the system will generate a code called Universal Unique Identifier (UUID), which contains 32 hexadecimal digits and is divided into five parts with hyphens. The code is the account that the user logs into the wallet. After logging in, users can use various services of the system:

1) User Profile: Users can query users' profiles and depositor and transaction amount;
2) Normal address: This address is used to send or receive payment;
3) Request: Generate a request address with a specified amount;
4) Prepaid: Add assets to users' wallets through prepaid services;
5) Send: Send the transaction to others;

6) Blockchain Data: It can query the data in the verified blockchain.

According to the above description, the benefits are as follows:

- Maintain a sense of belonging among bank customers.
- Real name registration can prevent crime and money laundering activities.
- UUID can improve the security of user accounts.
- Nodes can be added and adjusted flexibly.
- The data is stored in super peers, which can ensure the security of user data.
- The transaction was conducted in the bank's consortium chain, and even if it is attacked, it will not affect its operations.

3.3 Bank Layer

The bank layer is a set of reliable banks, where each bank acts as a miner to create blockchain blocks that are maintained together. Data is distributed and stored in each bank, so users do not need to spend many resources to use the service to calculate or synchronize data based on data security. In addition, each reliable bank will verify whether the information generated by others is fraudulent and supervise each other. In terms of data privacy, verification only needs to calculate the hash value of the consensus algorithm so that the block will be generated quickly.

The CBP2P Bank architecture is shown in Figure 5, and its functional description is as follows:

1) Join or Leave CBP2P Network: Banks can join or leave the CBP2P network through this function.
2) Block Generated: Nodes perform mining through this function to generate blocks.
3) Block Verification: After receiving the block, the bank verifies the transaction through the Merkle tree and checks the legality of the block hash.
4) Block Synchronization: Synchronize the verified blocks to the database.
5) Data Broadcasting: Banks on the network have their IP/port to broadcast data to each other.

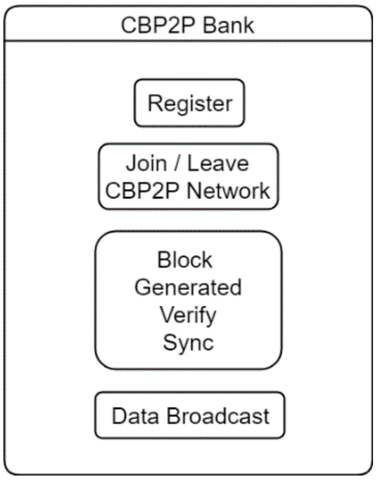

Figure 5. Bank layer architecture

Through the layered architecture of the above system, it can bring some goals and advantages:

- Reduce the development cost of back-end systems: Blockchain data is stored in members of trusted banks of super peers. This is different from the traditional structure, and there is a risk of owning its data and possibly losing and stealing it.
- Users do not have to synchronize large amounts of data: Users need to synchronize large amounts of data in the Bitcoin system. In the development of electronic payment, synchronization is not convenient for users, but banks replace the Bitcoin method by synchronizing blockchain data.
- The transaction process does not require a third party: Users can directly conduct transactions without a third party, and the bank will generate block data.
- Reduce the cost of traditional electronic payment architecture: In electronic payment, there are many third parties in the transaction process between buyers and sellers, which will cause buyers and sellers to spend more costs. In this article, we will simplify the transaction process.
- Real-time transactions: Transaction data is stored in the blockchain for quick inventory and authentication.
- Data confidentiality and integrity: Each bank's customer data will be encrypted, so when other banks receive the transaction data generated by the bank, they will not know the meaning of the message and cannot tamper with it.

4 CBP2P Transactions

In CBP2P, the user exchanges currency by entering an address, which is divided into the following two addresses:

Normal address (***Address$_n$***): It can freely specify the address to send and receive money;

Request address (***Address$_r$***): It can set the amount and fixed goods.

In addition to payment and collection, if the user requires prepayment, they can request their bank to store the value. All the above transactions will be sent to the transaction pool, and all super peers will perform mining tasks. For the generation of blocks, we will introduce the complete transaction process and the implementation of the blockchain in the following subsections.

4.1 Transaction Process

The process of system transactions is shown in Figure 6. The transactions in the transaction pool will cooperate with the bank to generate the block to be verified. The operation steps are as follows:

Step 1: When the Web service is running, the transaction pool will be activated. As a result, transactions sent by users will be temporarily stored in the pool.

Step 2: When the transaction pool has been activated for 15 seconds, or the transaction capacity reaches 2500 times, the network will broadcast to all banks in the network to generate blocks.

Step 3: Each bank processes the data in the transaction pool. First, the node will set a current value to compete and obtain the block hash value. Then, each bank cooperates to calculate the hash value that meets the difficulty and does not repeatedly calculate the same Nonce value to improve mining efficiency.

Step 4: When the calculated block hash meets the difficult conditions, the task bank will immediately generate the block and broadcast it to other banks. When other banks receive the block, they will verify the block and transaction data.

Step 5: After each node confirms and verifies the data, each node synchronizes the block data to the database.

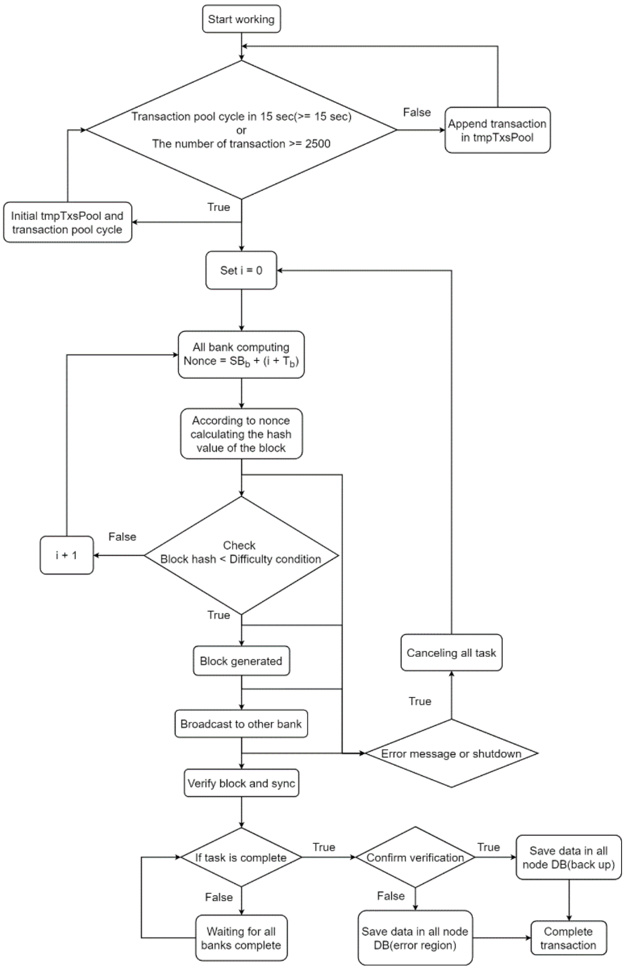
Start working
Transaction pool cycle in 15 sec(>= 15 sec)
or
The number of transaction >= 2500
False
Append transaction in tmpTxsPool
True
Initial tmpTxsPool and transaction pool cycle
Set i = 0
All bank computing
Nonce = SB$_b$ + (i + T$_b$)
According to nonce calculating the hash value of the block
Check
Block hash < Difficulty condition
False
i + 1
True
Block generated
Broadcast to other bank
Canceling all task
True
Error message or shutdown
Verify block and sync
If task is complete
True
Confirm verification
True
Save data in all node DB(back up)
False
Waiting for all banks complete
False
Save data in all node DB(error region)
Complete transaction

Figure 6. Transaction works

4.2 Block Generated

Figure 7 shows the bank's process of generating blocks. It contains the mining process and its calculation formula. Proceed as follows:

Step 1: When the **bank** collaborates to generate blocks, it will generate the Merkle tree of the transaction first.

Step 2: The block data includes:

1). height: Current chain length;
2). packing time: Packing time label;
3). previoushash: The hash value of the previous block;
4). merkleroot: The root value obtained after classifying the transaction;
5). difficulty: Current difficulty value;
6). version: Blockchain technology version.

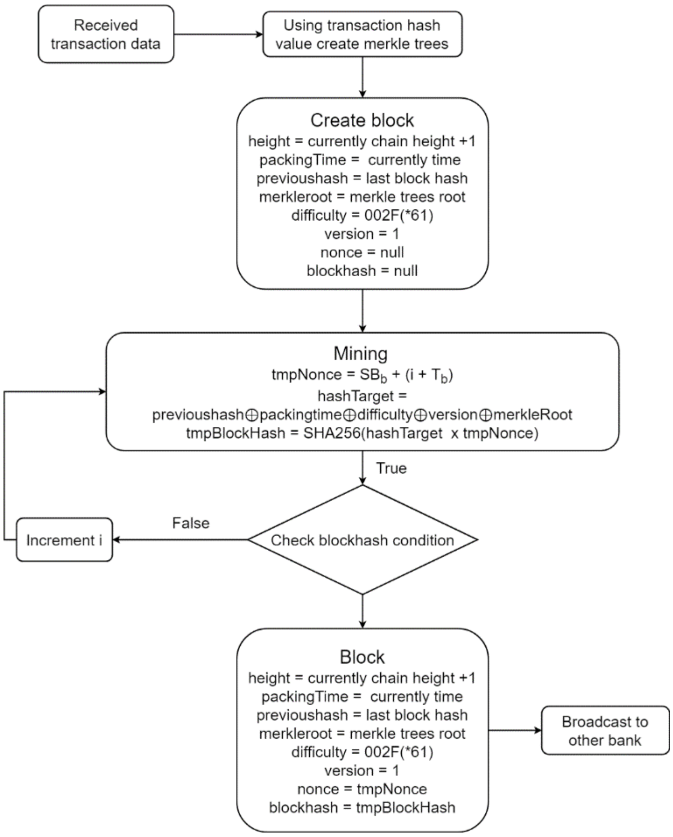
Received transaction data
Using transaction hash value create merkle trees
Create block
height = currently chain height +1
packingTime = currently time
previoushash = last block hash
merkleroot = merkle trees root
difficulty = 002F(*61)
version = 1
nonce = null
blockhash = null
Mining
tmpNonce = SB$_b$ + (i + T$_b$)
hashTarget =
previoushash⊕packingtime⊕difficulty⊕version⊕merkleRoot
tmpBlockHash = SHA256(hashTarget x tmpNonce)
True
False
Increment i
Check blockhash condition
Block
height = currently chain height +1
packingTime = currently time
previoushash = last block hash
merkleroot = merkle trees root
difficulty = 002F(*61)
version = 1
nonce = tmpNonce
blockhash = tmpBlockHash
Broadcast to other bank

Figure 7. The process of a block generated

Step 3: The calculation formulas for starting mining and block hashing are as follows:

$$SHA526(previoushash \oplus packingtime \oplus difficulty \oplus version \oplus merkleRoot \times nonce$$

The calculation of random numbers is as follows:

$$Nonce = SN_b + (i \times T_b)$$

where SN_b is the serial number of the bank; i is the number of computations, the initial setting is 0; T_b is the total number of banks.

Step 4: Check whether the block hash value meets the difficulty condition. If they do not match, continue to increase the random number until a valid block hash value is calculated.

Step 5: Store the block data.

4.3 Block Verification and Storage

Figure 8 shows the process of verifying the block. For example, when a bank quickly generates a block and broadcasts it, the bank receiving the data will synchronize the transaction and synchronize the block after verifying all nodes. The verification steps are as follows:

Step 1: The bank has the original data of the user's transaction. After receiving the block, the bank will use the original transaction data to generate a Merkle tree to obtain the Merkle root. It then compares with the Merkle root of the received block to verify the integrity of the transaction.

Step 2: Use the Merkle root calculated in the previous step to verify the block hash.

Step 3: If the above steps are met, the bank will return the delivery with a verification success message. After other banks complete the data verification, the bank synchronizes the block data to its own blockchain.

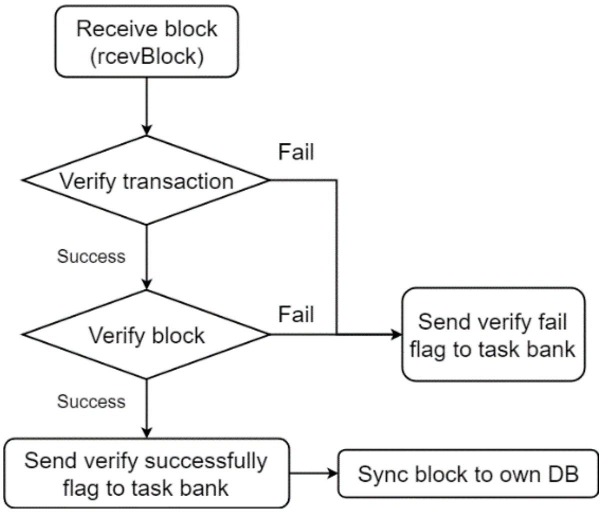

Figure 8. The process of verifying the block

5 Analysis

In this section, we will analyze system performance and security-related issues on the blockchain.

5.1 Performance Analysis

We used a 4-core 2.6GHz Intel i7 processor and 16 GB DDR3 RAM device to perform the performance measured on the MSI GP62 6QF and simulated the time taken by 15 banks to process each of the 500 transactions. The unit is milliseconds.

The performance of mining is shown in Figure 9. The performance of mining is shown in Figure 9. When there are more repositories, the present value of mining can be calculated faster—conversely, the fewer nodes, the more time it takes to calculate the present value of mining. Table 1 shows detailed information about mining performance. By the experimental results, the proposed scheme is feasible.

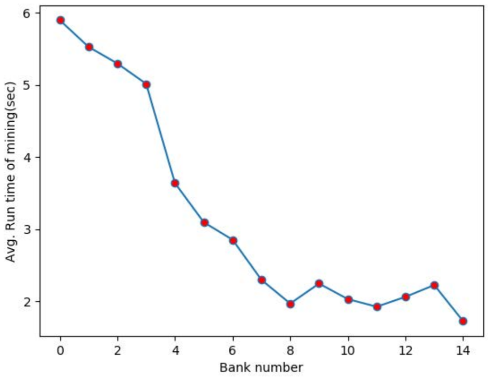

Figure 9. The performance of mining

Table 1. The run time of mining

Number of banks	Avg. Time (sec)
1	5.898860
2	5.527680
3	5.297480
4	5.015420
5	3.638620
6	3.095900
7	2.853180
8	2.298100
9	1.968660
10	2.245940
11	2.030480
12	1.924979
13	2.061480
14	2.225265
15	1.724780

5.2 Security Analysis

This section will analyze the blockchain architecture and possible attacks and use these cases to design the CBP2P system security mechanism to prevent these attacks.

A. Bank Distributed Architecture

In Bitcoin's architecture, the entire system and blockchain operate in a pure P2P manner (also known as a public chain). These methods bring many advantages, such as complete decentralization, data security, and user privacy. However, the entire financial operation and mechanism cannot avoid supervision [18-19]. Therefore, we propose the alliance chain CBP2P network based on the principle of financial supervision. The blockchain consists of trusted super peers, and if members want to join, they must obtain permission. As a result, users do not need to spend resources to participate in the past block synchronization, block verification, and mining.

B. Blockchain Architecture

Banks use the POW consensus algorithm to generate blocks and further ensure the security of data through calculations. The blockchain architecture is shown in Figure 10. In the hash algorithm, we use the secure hash algorithm 256 (SHA256) for hashing, and when performing mining tasks, the random number will increase when the block hash value meets difficult conditions.

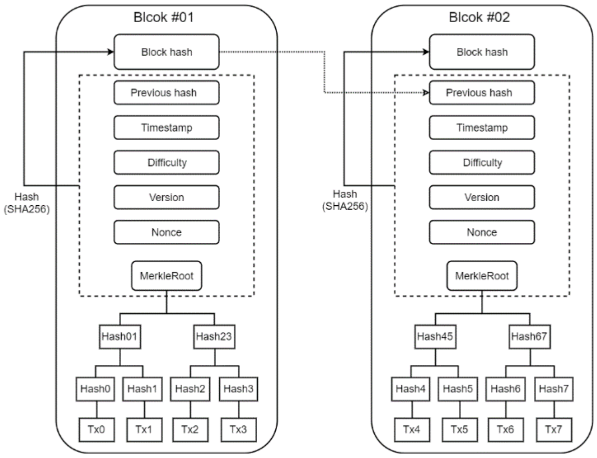

Figure 10. Blockchain architecture

C. Insider Attack

The bank's database stores information about each user's electronic wallet, including account number, password, and personal data. If the original data is stored in the database without encryption, insiders may illegally embezzle the currency. To avoid the risk of stealing user accounts by looking at the database, the system will store data after SHA256 encryption. Because the database is stored using data hashes, internally related staff only view a series of encrypted data, not the original data (such as account passwords or other important data). When the user logs in, the system only needs to hash the input data and then compare the databases for verification [20].

D. Guessing Attack

The system will generate a UUID after the user successfully registers to prevent attackers from using brute force methods or other methods to crack the user's e-wallet account or password. The group ID is like a password that only the user knows. It contains 32 hexadecimal digits, which are divided into five parts by hyphens, as shown below:

4c2eb93a-fe44-56b6-ba4a-6e3d8624e834

The total of all combinations is about 2^128. Assuming that the user attempts to log in with more than three consecutive errors by entering an account or password when logging in, the system will freeze for 60 minutes, so this method can only prevent online attacks. However, in an offline guess attack, because the UUID has enough bits and combinations, it is difficult for an attacker to spend a long time cracking the user account [21].

E. Offline Guessing Attack

In the case of a guessing attack, an attacker usually performs an online operation to crack a password or data. This method is straightforward to prevent and detect. The offline guess attack allows the attacker to contact the target host directly or offline to force the software to crack. Offline guessing attacks can be divided into three types: 1). Dictionary attacks: crack data through a specific dictionary. 2). Brute force attack: Use the computing power of the machine to force crack. 3). Hybrid: Mixed-use of Dictionary Attack and Brute Force to crack. When designing this article's e-wallet account number and password, the account number is a set of UUIDs that only know oneself. With the advantages of long bits, it is difficult for an attacker to crack user accounts to log in illegally [22].

F. Replay Attack

When a user submits a request for authentication, login, registration, transaction, etc., the bank will record the time stamp and generate a secret random number to execute the challenge response. If a malicious attacker intercepts the user's data and sends it, the bank will confirm the validity of its timestamp and the secret random number to prevent the attacker from carrying out the attack.

G. Eavesdropping Attack

AES encrypts the transmission of Web and bank data in the system. Therefore, if a malicious attacker wants to eavesdrop on the data transmitted between the user and the bank, the transmitted data cannot eavesdrop because the attacker has no secret key.

H. 51% Attack

There are some security issues when using POW as a consensus algorithm. First, if the attacker has more than half of the nodes or computing power, it may prevent other miners from putting the generated blocks into the chain. Second, its computing power allows the consensus to discard blocks of lower length and difficulty. Finally, it can even put fake blocks into the main chain. In this article, we still maintain the mechanism of mining blocks. Instead, supernodes act as miners and assemble a mining pool. All super nodes collaborate to mine to generate blocks, and other nodes can verify the blocks generated by other nodes [23-24]. Therefore, if a bank manipulates one or more banks, the proposed scheme is secure and can avoid 51% attacks.

6 Features Comparison

This section will compare the features between CBP2P and the current digital cryptocurrency system and payment. In 2021, Song & Chen proposed the security of digital financial transactions based on blockchain technology. They analyzed DoS attacks, the attacks that a single character might launch, and the attacks that multiple characters colluded to launch [25].

6.1 Current Digital Cryptocurrency System

We compare the system with the digital cryptocurrencies Bitcoin and Ethereum, as shown in Table 2. In the following, we will describe the differences between CBP2P and the above two cryptocurrency systems:

- Transaction time: Anyone can become a node of Bitcoin and Ethereum by downloading a wallet and synchronizing historical blockchain data, but only some super peers can be trusted. Therefore, to ensure data integrity, blocks are generated through difficult calculations. However, in CBP2P, nodes are composed of trusted banks, so we can quickly generate transactions through lower-level calculations to ensure data integrity.
- The amount of data synchronized by users: The historical data of Bitcoin and Ethereum is huge and growing; this is a big burden for users. In CBP2P, users do not need to synchronize data, but the bank alliance chain will synchronize.
- Data storage location: Bitcoin and Ethereum historical blockchain data are stored in each node, a big burden for ordinary users. In CBP2P, these data are only stored in the repository.
- Mining pool distribution: ghash.io is currently the largest mining pool in Bitcoin, and its computing power accounts for 48% of the network. In Ethereum, it is f2pool, and its computing power accounts for 27.4% of the network. A highly concentrated mining pool may cause 51% attacks. Therefore, in CBP2P, we evenly allocate computing power to avoid such risks.
- Identity: In Bitcoin and Ethereum, the address during the transaction has nothing to do with the user's identity, and criminals will use such functions for illegal transactions. However, CBP2P is applied to real money, and registration through the user's identity prevents such problems.

- Wallet data: In Bitcoin and Ethereum, wallet software will help users generate public and private keys, and users will retain data. If lost, users will not be able to access the wallet. In CBP2P, the bank saves the user's wallet data to prevent risk loss.

Table 2. Feature comparison between CBP2P and Bitcoin and Ethereum

Comparison Item	Bitcoin	Ethereum	CBP2P
Trading Time (Avg.)	10 min	8 sec	4 sec
Data size of user sync	71.8GB	132.5GB	0
Storage Location of data	Every node	Every node	Trusted bank
Mining pool distribution	ghash.io (48%)	f2pool (27.4%)	Average
Identity	Anonymous	Anonymous	Real name
Wallet data	User custody	User custody	Bank custody

6.2 Current Payment

We compared and analyzed the current payment model, as shown in Table 3. In current Taiwanese regulations, the paid-in capital required for electronic payments is 500 million, third parties are not restricted, and banks are 10 billion. Therefore, in terms of capital scale, it is secure to use banks as payment units than companies, and in terms of functions, third-party payments do not support stored value and transfer. Moreover, users' money stored in electronic payment software cannot be circulated with other companies, bringing many inconveniences and risks. Not only can users' assets not be transferred between companies, but they also face the risk of mismanagement by the company.

Table 3. Feature comparison between CBP2P and current payment

Comparison Item	Electronic Payment	Third-Party Payment	CBP2P
Established paid-in capital limit	500 million TWD.	Unlimited	10 billion TWD. (Bank standard)
Prepaid	V	X	V
Transfer	V	X	V
Circulation	X	X	V
User asset storage	Company	Not stored	Every bank

In the current banking and payment system, the company's architecture is centralized. A single unit can save the user's data and assets, facing the risk of malicious collapse or data corruption. However, the distributed blockchain technology in this paper solves this problem. The user's prepaid assets are stored in the blockchain, and various banks disperse the blockchain data. The user's assets are not stored in a specific unit like the previous centralized architecture. Still, the user's assets are stored in each bank, which is advantageous for using blockchain technology.

7 Conclusion

In the age of progressive information, people may not need paper money or bankbooks in the future. The purpose of this article is to apply bitcoin technology to an electronic bank payment system that digitizes data. As a result, users can conduct transactions directly through third parties, which saves the extra cost of the electronic platform and ensures the data storage of trusted bank consortia.

At the same time, we solved the problem of insufficient, instant huge data synchronization and anonymity in Bitcoin and too much centralization, internal attacks, and guessing attacks in the exchange.

Users only need to register an e-wallet to quickly experience the benefits of fast transactions and security brought by the blockchain. The transaction process is not necessary through a third party or platform. Users do not need to provide storage space and synchronize historical data, so the trust bank will cooperatively maintain the reliability and integrity of the data. For the bank, the common blockchain can reduce the related back-end costs and achieve data preservation. At the same time, the banks in the same industry will not concern the privacy issues such as customer information.

We will integrate the banking systems and operate and implement email services in the future. In addition to electronic payment functions, users will also receive various consumer services. For example, we can combine intelligent contracts to enable more banks to participate and obtain accurate information in terms of bank loans. Furthermore, since POW would consume many computation resources, it's also a future work using proof of stake or other consensus mechanisms.

Acknowledgments

The Ministry of Science and Technology, Taiwan (ROC), partially supported this research under contract no.: MOST 109-2221-E-468-011-MY3 & MOST 111-2622-8-468-001-TM1. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Cryptography Mailing list at https://metzdowd.com, 2009. https://bitcoin.org/bitcoin.pdf

[2] R. Dennis, G. Owenson, B. Aziz, A Temporal Blockchain: A Formal Analysis, *IEEE International Conference on Collaboration Technologies and Systems (CTS'16)*, Orlando, FL, USA, 2016, pp. 430-437.

[3] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1nd ed, O'Reilly Media, 2014.

[4] Wikipedia, *Double-spending* [Online]. Available: https://en.wikipedia.org/wiki/Double-spending

[5] N. Christin, Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace, *22nd International World Wide Web Conference Committee (IW3C2'13)*, Rio de Janeiro, Brazil, 2013, pp. 213-224.

[6] I. C. Lin, T. C. Liao, A Survey of Blockchain Security Issues and Challenges, *International Journal of Network Security*, Vol. 19, No. 5, pp. 653-659, September, 2017.

[7] W. T. Tsai, R. Blower, Y. Zhu, L. Yu, A System View of Financial Blockchains, *IEEE Symposium on Service-Oriented System Engineering (SOSE'16)*, Oxford, UK, 2016, pp. 450-457.

[8] A. Nayak, K. Dutta, Blockchain: The Perfect Data Protection Tool, *IEEE International Conference on Intelligent Computing and Control (I2C2'17)*, Coimbatore, India, 2017, pp. 1-3.

[9] B. Gipp, N. Meuschke, A. Gernandt, *Decentralized Trusted Timestamping Using the Crypto Currency Bitcoin*, February, 2015. https://arxiv.org/abs/1502.04015.

[10] M. Conoscenti, A. Vetrò, J. C. De Martin, Blockchain for the Internet of Things: A Systematic Literature Review, *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA'16)*, Agadir, Morocco, 2016, pp. 1-6.

[11] G. Zyskind, O. Nathan, A. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, *IEEE Security and Privacy Workshops (SPW'15)*, San Jose, CA, USA, 2015, pp. 180-184.

[12] Y. Liu, M. He, F. Pu, Anonymous Transaction of Digital Currency Based on Blockchain, *International Journal of Network Security*, Vol. 22, No. 3, pp. 444-450, May 2020.

[13] N. Hajdarbegovic, *Bitcoin Miners Ditch Ghash.Io Pool over Fears of 51% Attack* [Online]. Available: https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack, 2014.

[14] Z.-C. Li, J.-H. Huang, D.-Q. Gao, Y.-H. Jiang, L. Fan, ISCP: An Improved Blockchain Consensus Protocol, *International Journal of Network Security*, Vol. 21, No. 3, pp. 359-367, May, 2019.

[15] G. I. Navaroj, E. G. Julie, Y. H. Robinson, Adaptive practical Byzantine fault tolerance consensus algorithm in permission blockchain network, *International Journal of Web and Grid Services*, Vol. 18, No. 1, pp. 62-82, 2021.

[16] X.-J. Wen, Y.-Z. Chen, X.-C. Fan, W. Zhang, Z.-Z. Yi, J.-B. Fang, Blockchain consensus mechanism based on quantum zero-knowledge proof, *Optics & Laser Technology*, Vol. 147, Article No. 107693, March, 2022.

[17] P. K. Kaushal, A. Bagga, R. Sobti, Evolution of Bitcoin and Security Risk in Bitcoin Wallets, *IEEE International Conference on Computer, Communications and Electronics (Comptelix'17)*, Jaipur, India, 2017, pp. 172-177.

[18] Bank for International Settlements, *Committee on Payments and Market Infrastructure: Digital currencies*, November, 2015.

[19] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using Blockchain for Medical Data Access and Permission Management, *IEEE 2nd International Conference on Open and Big Data (OBD'16)*, Vienna, Austria, 2016, pp. 25-30.

[20] D. Ackerman, H. Mehrpouyan, Modeling Human Behavior to Anticipate Insider Attacks via System Dynamics, *Symposium on Theory of Modeling and Simulation (TMS-DEVS'16)*, Pasadena, CA, USA, 2016, pp. 1-6.

[21] H. Mayer, *ECDSA Security in Bitcoin and Ethereum: A Research Survey*, pp. 1-10, 2016. https://blog.coinfabrik.com/wp-content/uploads/2016/06/ECDSA-Security-in-Bitcoin-and-Ethereum-a-Research-Survey.pdf

[22] V. Yousefipoor, M. H. Ameri, J. Mohajeri, T. Eghlidos, A Secure Attribute-Based Keyword Search Scheme Against Keyword Guessing Attack, *IEEE 8th International Symposium on Telecommunications (IST'16)*, Tehran, Iran, 2016, pp. 124-128.

[23] S. Solat, M. Potop-Butucaru, *ZeroBlock: Preventing Selfish Mining in Bitcoin*, pp. 1-17, 2016. https://hal.archives-ouvertes.fr/hal-01310088v1/document

[24] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A Survey on the Security of Blockchain Systems, *Future Generation Computer Systems*, Vol. 107, pp. 841-853, June, 2020.

[25] H. Song, Y. Chen, Digital Financial Transaction Security Based on Blockchain Technology, *Journal of Physics: Conference Series*, Vol. 1744, Article No. 032029, 2021.

Biographies

Zhao-Ping Peng received the M.S. degree in Management Information Systems of Science from National Chung Hsing University. His currently working as a software engineer at TSMC, responsible for equipment automation and R&D system development.

Mao-Lun Chiang received the M.S. degree in Information Management from Chaoyang University of Technology and the Ph.D. degree in Department of Computer Science from National Chung-Hsing University, Taiwan. He is an associate professor in the Bachelor Degree Program of Artificial Intelligence at the National Taichung University of Science and Technology, Taiwan. His current research interests include Ad Hoc, mobile computing, distributed data processing, fault tolerant computing, artificial Intelligence, and cloud computing.

Iuon-Chang Lin received the Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor and chair of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, blockchain security, and cloud computing.

Chou-Chen Yang, He got his Phd. degree in computer science, University of North Texas, 1994. He was a professor in the dept. of management information system, NCHU. His researches include network security, AI, and data mining.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a distinguished professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.