Efficient Peer-to-Peer E-Payment Based on Asynchronous Dual Blockchain

Wei-Chih Hong[1], Ying-Chin Chen[1], Ren-Kai Yang[1], Bo Li[2], Jung-San Lee[1]

[1] Department of Information Engineering and Computer Science, Feng-Chia University, Taiwan
[2] Department of Computer Science, University of Illinois at Urbana-Champaign, USA
weizhihong@gmail.com ycchen.blythe@gmail.com, a9017100@gmail.com, lxbosky@gmail.com, leejs@fcu.edu.tw

Abstract

The number of people surfing over the e-commerce has reached to 1.6 billion, while the transaction scale has approached to 2,304 billion dollars at the end of 2017. No doubt that the security and efficiency of an e-payment system have attracted lots of attention in the field of e-commerce. That is the reason why the blockchain technique has been widely spread to most of the e-commerce mechanisms. A blockchain employment can be used to guarantee the properties of decentralization and non-tampering, which provide users a more stable and reliable trading process and prevent malicious behaviors, including double-spending and sybil attack. Nevertheless, the overhead of each transaction process is too heavy to realize immediate transaction. In this study, we aim to speed up the performance of transaction through an asynchronous dual blockchain. Moreover, we have exploited the reputation mechanism to reduce resource consumption. The new method has inherited the security from a blockchain technique. Specifically, the experimental results have demonstrated that the asynchronous dual block-chain is fairly safe and efficient.

Keywords: Peer-to-peer e-payment, dual blockchain, asynchronous storage, sybil attack

1 Introduction

This explosive development of networks has brought in a brand-new marketing model. People get used to shell out for a transaction through an electronic payment (e-payment) instead of physical currency. According to the report of Statista E-commerce worldwide [1], the number of people surfing over the e-commerce has reached to 1.6 billion, while the transaction scale has approached to 2,304 billion dollars at the end of 2017. Figure 1 displays the global retail electronic commerce (e-commerce) sales from 2014 to 2021. The growth trend is quite positive and astonishing. Such a large transaction amount has resulted in the urgent requirement of an e-payment technique.

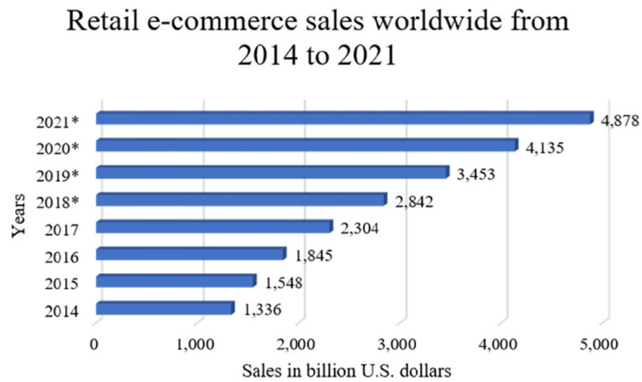


Figure 1. Global retail E-commerce sales

The nowadays physical money is often issued through the government bank or a trusted third party. It is not difficult to confirm the validity of physical money by the adoption of specific anti-forgery technologies. By contrast, it is always a crucial challenge in designing an e-payment mechanism since it is not easy to check the legality of virtual currency received from networks or resist the malicious usage of double spending. As people usually surf and purchase over the Internet with misgivings, an e-payment technique needs to import a trusted third party to verify network user identity and virtual currency validity. Notwithstanding this importation could solve the trust issue to guarantee system security and preserve stable transaction, a trusted third party has to charge an extra fee for users. It is just like to pay commission while transferring money via conventional bank systems, which is regarded as an unnecessary overhead for most users.

In 2008, Nakamoto has proposed a peer-to-peer (P2P) electronic cash system without the deployment of a centralized party [2]. This cryptocurrency is the so called Bitcoin. The adoption of a trusted third party has been replaced by the technique of blockchain. The verification mechanism has been established in a distributed structure instead of a centralized mode. All the transaction information and currency validity could be authenticated by multiple users on the Internet. That

*Corresponding Author: Jung-San Lee; E-mail: leejs@fcu.edu.tw
DOI: 10.3966/160792642020092105013

is, the maintenance costs of system security have been spread out to network nodes, and there is no more a central party to monopolize the agency fee. Each single user who tries to join the transaction verification is able to compete with others for the reward. It could also achieve the benefit of sharing economy in an e-commerce environment.

A blockchain of Bitcoin is a type of payment rail that transfers money from a peer to another one. As displayed in Figure 2, it could be learned as a distributed and public digital ledger that is used to record transactions across many network users. Participants possess all transaction information and know the details of other accounts. For instance, node *b* can check whether node *a* possesses enough money to complete the deal according to the ledger. Once the verification is finished, the corresponding transaction record will be updated to other ledgers. Specifically, all involved records cannot be altered retroactively based on the employment of cryptography technique. To guarantee the consistency of all transaction ledgers, the PoW (Proof of work) algorithm has been applied to being a consensus mechanism in the blockchain. Users need to pay a considerable amount of computation power to fulfill the condition of PoW. The first completing user then adds the transaction record to the ledger and broadcasts it to the network. Once other users have confirmed the transaction, they will upgrade the content of their corresponding ledgers.

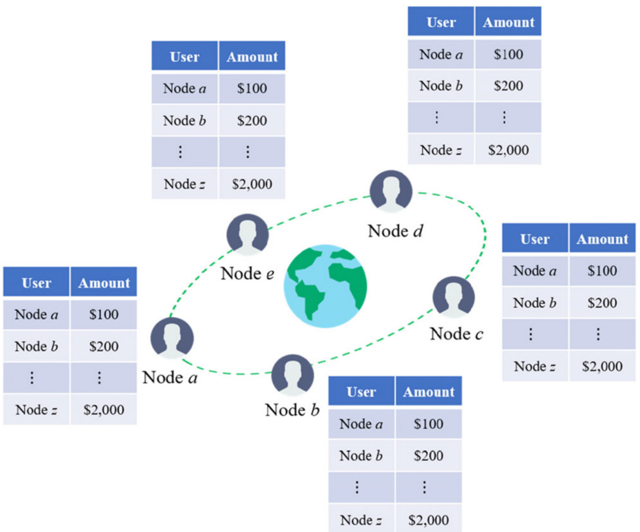


Figure 2. Distributed digital ledgers in a blockchain

In such decentralized e-payment system, the examination of transaction validity depends on the decision of a group of users, and the reliability of ledger counts on the adoption of consensus mechanism. It is computational infeasible for a single user to disturb the whole marketing. A user who tries to tamper previous transaction record or mount the behavior of double spending must fail due to the challenge of most users. Namely, the content of ledger is determined based on the majority decision. Only under the condition that a malicious user is able to dominate half of the network nodes in the blockchain, the tampering could be achieved. Although the consistence of transaction ledgers can be preserved in the blockchain, the spent computing power and time overhead have limited the adaptability to real-time services [3].

Actually, the cryptocurrency bitcoin is just one of the blockchain applications. Lots of industries have tried to import this technique to overcome their corresponding problems. Public-key cryptography and one-way hash function have been employed in the blockchain to realize the anti-forgery in a decentralized management and preserve the properties of anonymity, non-repudiation, integrity, and reliability [4]. Unfortunately, the efficiency and expansion of blockchain have limited the applicability of nowadays marketing. To ensure the security of record, a user has to pay lots of computing power to complete the transaction. Researchers thus try to refine the kernel algorithm of blockchain to speed up the updating performance of block information and to reduce the power consumption on verification [5]-[8]. Although they have passable progress in two issues, the problem of storage overhead in each node remains. Otte et al. [9] proposed a decentralized management without the adoption of consensus mechanism, said as Trustchain. A transaction record is kept by the buyer and the seller, respectively. Other network nodes do not need to spend time for data consistency. As illustrated in Figure 3, each block is a transaction record, while the hash value in a block contains the information of previous transaction; thus, leading to a blockchain. Since the transaction record has been recorded in both PeerA and PeerB, they are capable of modifying the content of a transaction *tx*. To launch a double spending, they can conceal or tamper block data and re-compute the whole block to cheat a verifier. These attempts could be found after examining the information of two blocks. That is, what we can do is to find a dishonest user but not to stop a malicious double spending. The loss of user has occurred even the technique of Trustchain can outperform traditional blockchain in terms of real-time service. This has demonstrated that it is not suitable for an e-payment application.

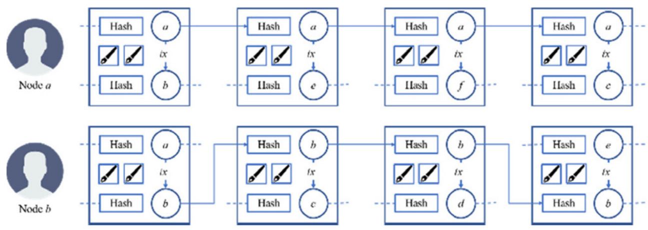


Figure 3. Diagram of Trustchain

In this article, we aim to introduce a brand-new decentralized e-payment platform, defined as asynchronous dual blockchain. The adoption of asynchronous data storage and reputation mechanism can be used to diminish the resource consumption. In an asynchronous data storage mode, a node needs not to wait for verification from each node but to keep its relevant transactions. Thus, the computing power consumption and storage hardware requirement could be lowered down effectively. Aside from the seller and buyer, involved verifiers have to store the transaction data to avoid double spending or dishonest behaviors. A reputation value is applied to being the condition of transaction launch and the motivation of verification. An originator has to pay a specific reputation value as reward to attract verification help from other nodes, while a user needs to authenticate transactions of others to earn reputation value to start a transaction. In the asynchronous dual blockchain, the reputation value can be used to help recognize malicious nodes to resist Sybil attack, in which an attacker may create multiple clones in a legal way and gain illegal profits through these clones [10].

The new method has inherited the security from a blockchain technique. The followings are the essential properties of the asynchronous dual blockchain e-payment.

(1) Fairness: An e-payment mechanism shall be able to avoid illegal transactions and behaviors to guarantee users profits.

(2) Efficiency: Each single node only needs to maintain its ledger containing its involved transactions to approach a real-time deal and reduce hardware overhead. Note that the content synchronization of ledgers takes lots of time and equipment requirement.

(3) Prevention of double spending: Besides the seller and buyer, each verifier has to maintain a ledger with involved verification records to ensure the reliability of transaction.

The rest of this is organized as follows. In section 2, we give the preliminary explanation. The proposed e-payment mechanism is described in section 3, followed by the security analysis and experimental results in sections 4 and 5. Finally, we make conclusions in section 6.

2 Component Definitions

In this section, we describe the components of the dual blockchain network. This includes the necessary information of user for transaction process.

Definition 1. Wallet: The wallet includes the public/private key and address, such as identification and account of traditional bank system. The public/private key is constructed according to [4], while the address is generated by the public key through SHA256.

Definition 2. Reputation (rep_i) : The rep_i is the condition value that enables node i to perform transactions and verifications. If a node launches a transaction, it has to pay rep_i value. On the other hand, a node can earn the rep_i value after offering verification services. Each node joins the dual blockchain with an initial rep_i = 0.5, which is a median value, so that a new node still has the ability to launch transactions. Here rep_i is ranged within [0, 1], which could be used to avoid the unlimited growth of reputation. A node has offered the higher contribution, its reputation is closed to 1; otherwise, it approaches to 0. Additionally, competitiveness $match_i$ is the index that node i strives for earning opportunities of verification, which is shown in (1).

$$match_i = rep_i \times (1 - e^{-\lambda/(\mu-\lambda+1)}) \quad \textbf{(1)}$$

where λ and (μ-λ) are the numbers of transaction and verification, respectively.

Definition 3. Reward (*rwd*): Because of the fact that each transaction needs to be verified, the node must offer the *rwd* to attract others to verify the transaction, which is deducted from rep_i . The *rwd* is displayed in (2).

$$rwd = match_i \times e^{-\lambda/(\mu-\lambda+1)} \quad \textbf{(2)}$$

Definition 4. Condition of the verification: The conditions of the verification are illustrated in (3)(4)(5).

$$R_v = \sum_{i=1}^{n} match_i \quad \textbf{(3)}$$

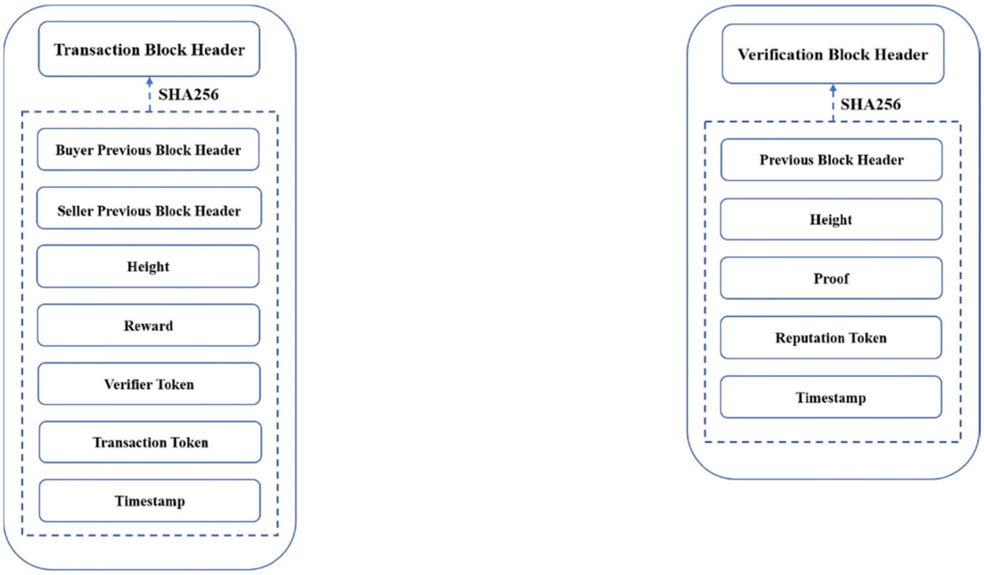
$$R_t = 2 - \sum_{i=1}^{2} rep_i \quad \textbf{(4)}$$

$$R_v - R_t > 0 \quad \textbf{(5)}$$

First, the R_v is the sum of $match_i$ of verifiers according to (3), where n is the total number of nodes. Next, the buyer and seller aggregate rep_i to obtain the R_t , as defined in (4). Lastly, if R_v is larger than R_t , then the verification begins, which is shown in (5).

Definition 5. Transaction block (Tblock): Each user has a transaction chain consisting of Tblocks to preserve the historical transactions, as illustrated in Figure 4(a). The content of the Tblock is defined in Table 1.

Definition 6. Verification block (Vblock): In dual blockchain network, a node has a verification chain consisting of the Vblocks to maintain other node transaction records, as displayed in Fig. 4(b). Moreover, the reputation of the node is stored in Vblocks. The content of the Vblock is defined in Table 2.



(a) Content of Tblock (b) Content of Vblock

Figure 4. Illustrating the block information of dual blockchain

Table 1. The information of the Tblock

Name	Definition
Transaction block header (TBH)	TBH is the hash value of current transaction content through SHA256. The information is used to protect the integrity of the Tblock and stored in Vblock of verifiers. If the owner tampers the block content, it will be changed dramatically. The other nodes can find and doubt this malicious behavior and reject the transaction.
Buyer previous block header (BPBH)	The TBH of buyer's previous transaction
Seller pervious block header (SBPBH)	The TBH of seller's previous transaction
Height (λ)	The number of the Tblock, which indicates the number of user's transaction.
Reward	The *rwd* of buyer's commitment.
Verifier token (VT)	The information includes the hash value of the verification block, $address_i$ and rep_i.
Transaction token (TT)	The information of transaction *Data*.
Timestamp	The time of Tblock establishment.

Table 2. The information of the Vbloc k

Name	Definition
Verifier token header (VBH)	VBH is the hash value of current verification service through SHA256. The information is used to project the integrity of the Vblock and stored in Tblock's VT.
Previous block header (PBH)	The Pervious VBH value.
Height (λ)	The number of the Vblock, which indicates the number of offered verification and performed transaction.
Proof	The content includes the information of TT and TBH.
Reputation token (RT)	The content includes rep_i of user and signed result $Sig_c(rep_i)$ from the contributor c.
Timestamp	The time of Vblock establishment.

3 Prposed Scheme

In this section, we describe the implementation of e-payment on asynchronous dual blockchain. The framework of transaction is shown in Figure 5. It is illustrated that transaction chain (Tchain) consists of Tblocks and verification chain (Vchain) is made up of Vblocks, in which they are used to maintain the transaction records and reputation values by user, respectively. Here, only the buyer means that the user wants to launch a transaction with others and broadcasts the transaction message to the dual blockchain networks. After that, other users verify the message by the public key of the buyer, and further decide whether or not to act as verifiers of this transaction. The proposed method contains initialization phase, transaction phase, verification phase, and information update phase, which are described in subsections 3.1, 3.2, 3.3, and 3.4. The used notations are shown in Table 3.

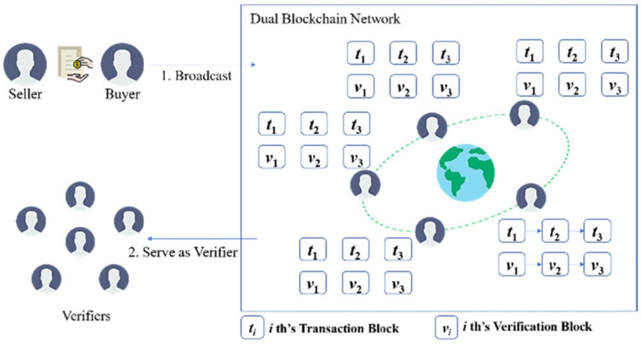


Figure 5. The framework of the transaction

Table 3. Notations

Sign	Definition	Sign	Definition
B	Buyer	SK_i	Private key of user i
S	Seller	tx	Amount formal tx = ($address_B$ to $address_S$)
V_j	The jth verifier	$Sig_i(.)$	Digital signature of user i
W	The V_j with the highest $mach_i$ in the verification is called winner	$H(.)$	One-way hash function
i	The user i plays a role of B, S, V_j, and W	$\|\|$	Concatenation symbol
$address_i$	Address of user i	T	The time of transaction establishment
PK_i	Public key of user i		

3.1 Initialization Phase

Before the user i initiates a transaction, it is necessary to build the wallet, in which the method of generation is identical to the bitcoin network [2]. After that, the transaction process is displayed in Figure 6. The details are described as follows.

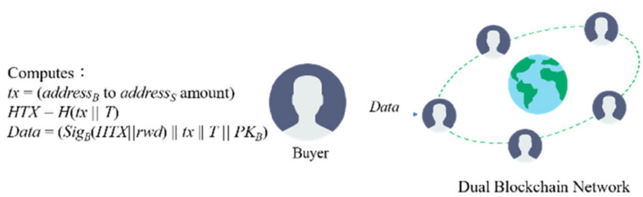


Figure 6. Initialization phase

Step 1. User i calculates the key pair SK_i and PK_i based on [4].

Step 2. User i generates $address_i$ of the PK_i via SHA256.

Step 3. The B calculates tx which is the result of coordination with S.

Step 4. The B generates $Sig_B(HTX \,\|\, rwd)$ through the digital signature algorithm [4], where $HTX = H(tx \,\|\, T)$ and rwd is computed from (2).

Step 5. The B calculates transaction information $Data = (Sig_B(HTX \,\|\, rwd) \,\|\, tx \,\|\, T \,\|\, PK_B)$ and broadcasts the outcome to the dual blockchain network, which would be verified by the other users.

3.2 Transaction Phase

When the other users receive $Data$ from Step 5 of subsection 3.1, it will be verified by $Sig_B(HTX \,\|\, rwd)$ using the PK_B. Then, the user i decides whether to become the V_i according to the reward. If the user i wants to join the competition of reward, it is necessary that the user i confirms the integrity of the Tchain from the B and S, as shown in Figure 7. The details of procedure are displayed as follows.

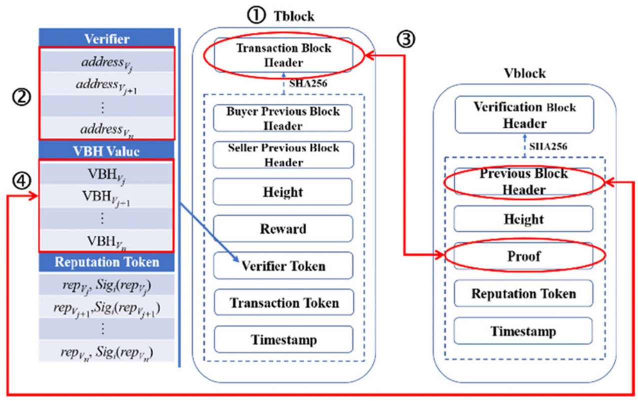


Figure 7. Transaction phase

Step 1. The V_i requests the latest Tblocks from B and S.

Step 2. The V_i finds the $address_i$ from the Tblock's VT for linking the corresponding Vblock and requests TBH from Vblocks' Proofs of the past transaction verifiers.

Step 3. The V_i confirms the integrity of transaction records from B and S via the Proof in Vblock.

Step 4. The V_i compares PBH with VBH, where the PBH is identical to the VBH of the previous Vblock. The reason is that the V_i competed with others through the previous Vblock. It is used to examine the integrity of the Vblock.

3.3 Verification Phase

After all the V_i have completed the integrity of the historical transactions, it can initiate the competition of rwd according to (5), as shown in Figure 8.

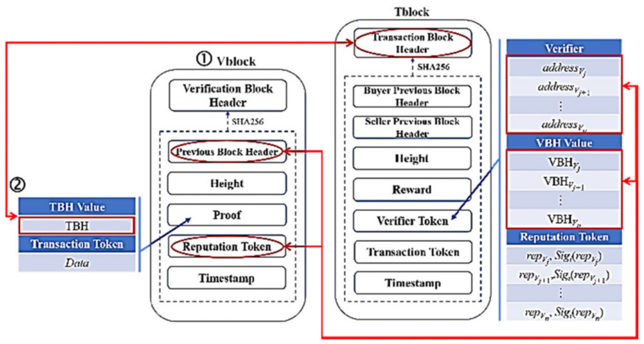


Figure 8. Verification phase

Step 1. Involved B, S, and V_i request the latest Vblock from each other.
Step 2. The B, S, and V_i check the TBH in Proof and request Tblock from the owner via the *Data*.
Step 3. The B, S, and V_i examine the PBH and RT by the VT. If the PBH is equal to VBH in VT, the completeness of Vblock is confirmed.

3.4 Information Update Phase

In this phase, we describe the process how users update the Tblock and Vblock, as shown in Figure 9.

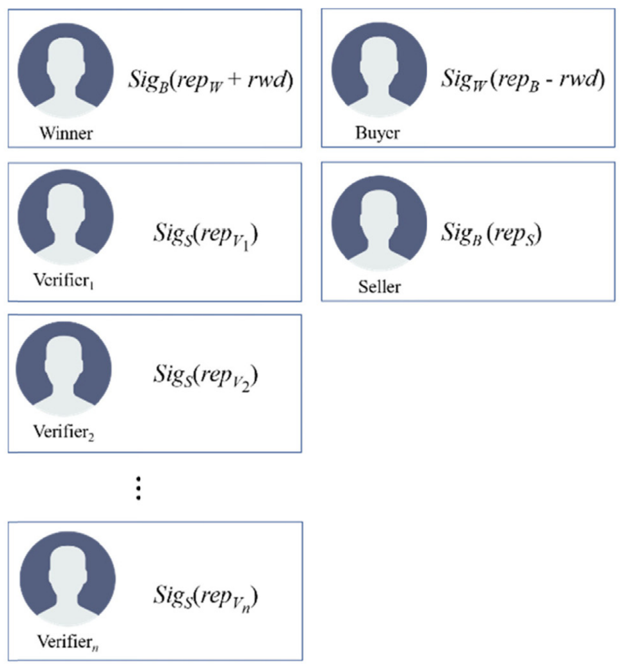


Figure 9. Information update phase

Step 1. The W can obtain the latest $rep_W^{new} = Sig_B(rep_w + rwd)$ from B. Later, the latest $rep_B^{new} = Sig_W(rep_w + rwd)$ of the B is received by the W.
Step 2. The other V_i and S have the latest $rep_{V_i}^{new} = Sig_B(rep_{V_i})$ and $rep_W^{new} = Sig_B(rep_s)$, respectively.
Step 3. The W computes the TBH of the new Tblock containing SPBH, BPBH, Height, Reward, VT, TT, and Timestamp through SHA256. Afterward, the result will be updated in Tchain by B and S.
Step 4. Involved B, S, and V_i calculate the new Vblock including PBH, Height, Proof, RT, and Timestamp via SHA256. Finally, the transaction process is completed.

4 Security Analysis

In this section, we are going to analyze how the proposed method could resist potential threats, including Sybil attack, double spending, and replay attack.

4.1 Sybil Attack

The reputation mechanism is used to avoid malicious users in current e-commerce platform, such as e-Bay and Amazon. Nevertheless, the calculating and maintenance of a reputation value is a crucial challenge in a decentralized management environment [11-16]. As to a malicious node in the asynchronous dual blockchain, it might try to create multiple copies to fulfill the verification constraint on a transaction, as shown in (5). Even it could help its clones to increase corresponding reputation values, the malicious node must fail in this attempt of illegal earning of reputation. The initial reputation value of a new joining node is set to 0.5, and the reputation value of a verifier shall be calculated via (1). This has implied that it is an essential condition of performing at least one transaction to be a verifier. Namely, the malicious node must finish a deal with each single clone before launching a Sybil attack, where it requires multiple copies to join the verification to comply with the condition of (5). Due to these confirmation requirements, a malicious node has to pay much more time and higher reward cost to earn reputation without offering true verification services. In case that a malicious node refuses to follow the verification conditions, the involved user must reject the transaction. Thus, the new method can effectively prevent the Sybil attack through the punishment of cost increase.

4.2 Double Spending

The forbiddance of double spending is an important security requirement in an e-payment platform, in which a user cannot reuse a digital coin in any form to bring the loss for a seller. In the asynchronous dual blockchain, a user who intends to launch this illegal behavior has to conceal or tamper a completed transaction and offer an incorrect Tblock to a payee and verifiers; thus, fooling involved nodes to achieve the double spending. As depicted in Figure 10, a node with this attempt may modify the transaction or camouflage the second block. Nevertheless, the TBH must be different from that kept in the Proof of a verifier. Therefore, it is easy to figure out this tampering to deny the transaction. Regarding to conceal the third block and provide the second one to seller and verifiers, involved participants can detect the existence of the third block recorded in the Vblock of verifiers. Accordingly, the seller can learn the truth and reject this misbehavior to avoid transaction loss.

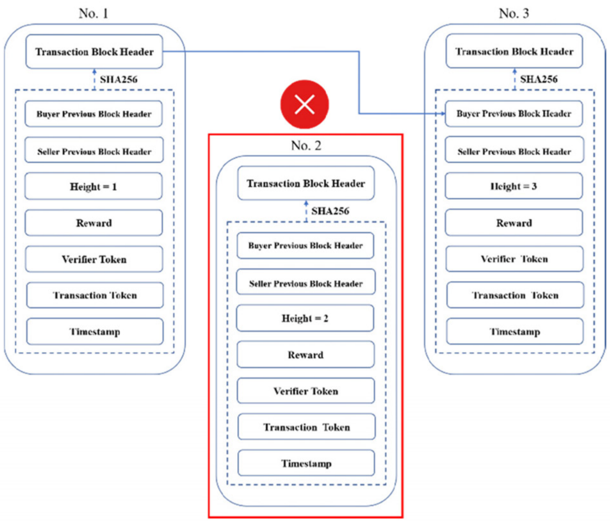


Figure 10. Diagram of double spending

4.3 Replay Attack

No doubt that all the transferred data over the Internet could be intercepted nowadays. Furthermore, malicious attackers might be able to access protected resources via replaying the intercepted request including personal information and verifier token to pass the authentication. In the proposed e-payment platform, the numbers of transactions and verification services have dominated the offered reward "*rwd*" of a payer and earned reputation "$match_i$" of being a verifier. Once a node tries to replay a used token to enlarge the length of blockchain without launching a real transaction or verifying data for others, it must fail due to the evidence of Proof and VT. As displayed in Figure 11, a node may replay the second Tblock to be the third one in a Tchain. This attempt, however, must be compromised in the transaction phase. A verifier is able to detect this misbehavior by comparing the TBH of replayed Tblock with the one recorded in its Proof. By the same play, applying the second Vblock to being the new one, as illustrated in Figure 12, must be known to verifiers. According to the VBH confirmation, VBH of Vblock must be different from that of Tblock. Thus, a replayed block cannot succeed in enlarging the lengths of Tchain and Vchain to disturbing the transaction fairness.

5 Performance Analysis

Here we give the performance examination on the dual blockchain via individual transaction marketing and participant behavior.

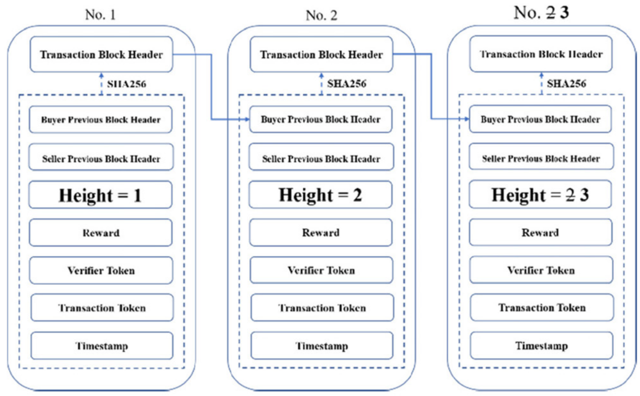


Figure 11. Diagram of replay attack in tchain

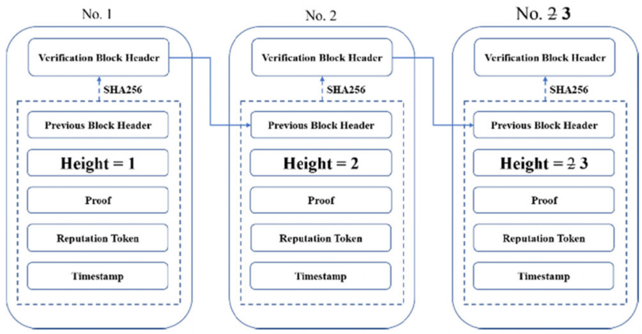


Figure 12. Diagram of replay attack in vchain

5.1 Performance of Transaction

A personal computer installed with Windows 10 64-bit is applied to simulate the dual blockchain system, equipped with an Intel Core i5-7500 3.40GHz and 8G RAM. Algorithms were implemented in Python. Note that an effective transaction shall be confirmed and recorded via verifiers. According to the definition of (5), the confirming and recording tasks could be triggered only when the number of verifier has fulfilled the condition. That is, the number of participant in the marketing has significantly influenced the transaction performance. In Figure 13, offers the evaluation results on different numbers of participant involved in the marketing. To dig out the performance, we gathered the time costs to complete 25,000 transactions under 300, 600, and 900 users, respectively. In the scenario of 300 users, it takes 509.91 seconds to finish all tasks, while the average performance is 49.9 transaction/s. As to the situation of 600 users, it requires 252.17 seconds to accomplish all jobs, and the average outcome is 99.13 transaction/s. Respecting the case of 900 users, it only spends 167.03 seconds to carry all transactions out, and the average is 149.67 transaction/s. According to these simulation results, we have the finding that the more number of participants, the higher transaction performance. The main reason is that it requires multiple verifiers to help complete the transaction check. Once lots of nodes stay in the market, it is easy to fulfill the condition of (5). In particular, it is unnecessary to spend time for waiting the answer from consensus algorithm in the asynchronous storage structure. Thus, the waiting time of being verified could be lowered down effectively. As to the current Bitcoin network, it requires 3,571.42 seconds to complete 25,000 transactions [17, 19, 20]. This has demonstrated the higher efficiency in comparison with traditional blockchain. Note that the time costs of initiation and information phases are not included in the performance. The initiation phase is considered as a pre-process in the dual blockchain network so that it shall not be calculated in the transaction procedure, including the computations of key and wallet address. As to the information update phase, the burden of message transferring depends on Internet speed and hardware of each participant. Consequently, we focus on performance evaluation of transaction and validation phases.

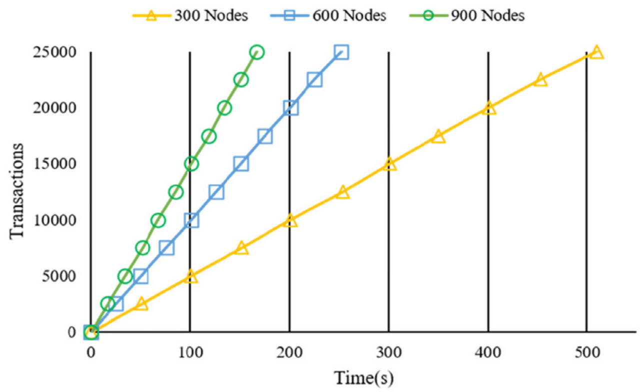


Figure 13. Performance on different numbers of participant

Obviously, the technique of conventional blockchain could not be truly deployed to trading marketing [3]. Regarding to VISA (Visa International Service Association) [18], the average number of transactions within one second is 2,000. By contrast, about seven transactions could be accomplished in a second under the 1 MB block size in Bitcoin [17]. In case to approach the trading performance of VISA, each involved node in Bitcoin has to raise hardware cost to keep more transaction records. This is the reason why we tried to adopt the asynchronous storage structure, in which each node only needs to maintain its involved transactions in the ledger. Therefore, the overhead to preserve the ledger can be reduced effectively, and the transaction performance can be enhanced significantly.

Previous figure has shown the evidence that the more number of nodes in the market can enhance the transaction performance. In Figure 14, we give the performance of asynchronous dual blockchain in an accumulative market, in which we added 1,000 nodes into the market once 2,000 transactions have been completed. With this accumulation, it requires only 12,000 nodes in the scenario to reach the average number of transaction within one second, which is the real VISA transaction performance [18].

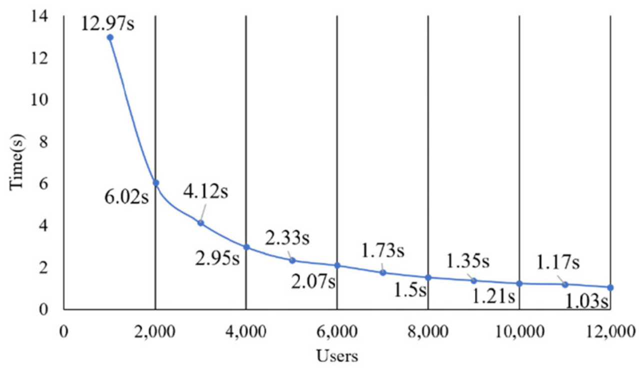


Figure 14. Performance in an accumulative market

5.2 Discussions on The Balance and Imbalance Scenarios

To demonstrate the practicability of asynchronous dual blockchain, we further simulated balance and imbalance scenarios of Tblock and Vblock, which display the real cases in the word. A balance scenario means that the number of transaction is similar to that of verification, while an imbalance one represents either the number of transaction is larger or smaller than that of verification. According to **Definition 2** and **Definition 3**, we have learned that the reputation and reward have directly dominated a transaction accomplishment, including the launching condition and required verification. Thus, the design of (5) has pointed out that the ratio of transaction to verification must influence the performance of trading marketing. Under the situation of 300 nodes and 25,000 transactions, Figure 15 depicts the performance of three cases: balance, underproduce, and oversupply. In a balance case, each node offered a verification service after taking a transaction initiation. The underproduce case is of the setting that each node launched four transactions and offered one verification service, while the oversupply instance is with the inverse scene.

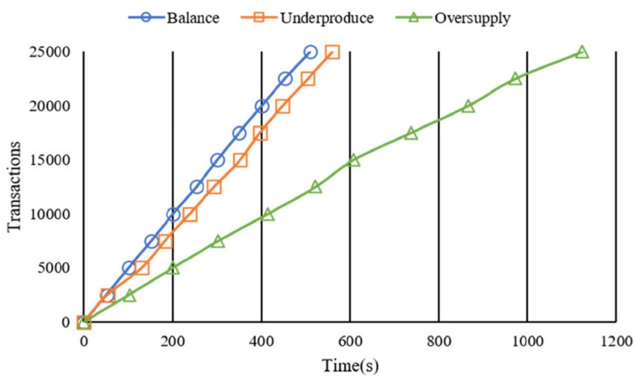


Figure 15. Performance of balance and imbalance cases

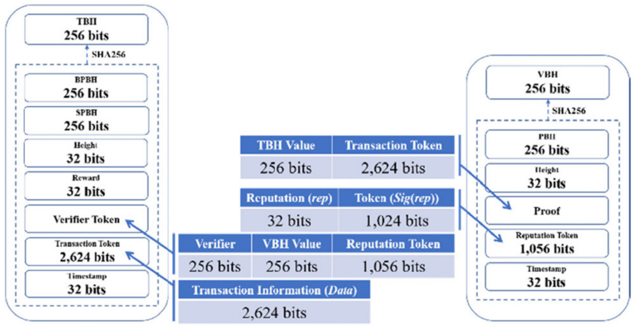
In the balance scene, it takes 509.91 seconds to complete 25,000 transactions, which could be considered as a baseline. Concerning the underproduce case, we have to spend 559.89 seconds for the same number of tasks. Obviously, the performance of the second case is not as well as that of the first one. It is due to the fact that each node must pay the reputation value to launch a transaction; thus, increasing the outcome of (4). This subsequently results in the requirement for higher number of verifiers in (5). As to the oversupply scenario, it takes 1,123.03 seconds to accomplish 25,000 transactions. Since the current weight of matchi must be lower than 0.1, it is hard to attract verifiers to compete for task reward. Based on the **Definition 2**, we can cleverly reduce the weighting of users who mainly focus on providing verification services to decrease the output of (3). Therefore, we need more number of verifiers to fulfill the condition of (5). Actually, the main reason for each single node in the environment of asynchronous dual blockchain to offer verification service is to gather reputation value for future transaction. It is meaningless for a node to spend too much time on offering verification services. This implies that the last case is rare in the real world, while the first two scenarios are the ones we have to evaluate the corresponding performance. As shown in Figure 14, no matter facing the balance or imbalance cases, the new method can yield a satisfactory trading efficiency.

5.3 Discussions on Storage Overhead

The cryptosystem used in the asynchronous dual blockchain is RSA-1024. As defined in Table 1, Table 2, and Table 3, the size of addressi is 256 bits and tx = 256+256+32 = 544 bits, while those of Height, Reward, and Timestamp are 32 bits. Furthermore, we have the following storage calculations, TT = 1,024 + 544 + 32 + 1,024 = 2,624 bits, Proof = 256+2,624 = 2,880 bits, and RT = 1,024+32=1,056 bits. Thus, we can summarize the storage overheads of Tblock and Vblock in Figure 16. Averagely, it takes six verifiers to complete one transaction in a balance trading scenario. Thus, we have the sizes of Tblock = 3,488+(256+ 256+1,056)×6 = 12,896 bits and Vblock = 4,512 bits. More precise, each transaction occupies 2.1 KB (12,896+4,512=17,408 bits) in the asynchronous dual blockchain. Compared with the block size of 1 MB in Bitcoin network, the new method can significantly outperform the conventional blockchain in terms of storage overhead. It relies on the fact that each node only needs to keep involved transactions instead of all records. That is, a partial of nodes have to share the responsibility of preserving the data integrity and non-tampering through the adoption of one-way hash function, digital signature, and distributed storage.

5.4 Comparisons with Related Works

Here we compared conventional blockchain and Trustchain with the asynchronous dual blockchain in terms of essential properties to highlight the contribution. The symbol "Y" means that the property can be confirmed, while "N" represents that it cannot be achieved. All the comparisons are listed in Table 4.



(a)Tblock storage overhead (b)Vblock storage overhea

Figure 16. Illustrating the overhead of the dual blockchain

First, these three techniques are realized in P2P network without a trust third party. Thus, they can confirm the property of decentralization. Second, they all import the cryptosystem and apply $(PK_B, address_i)$ to be the identity on the trade platform. No one can trace this pattern to learn the real personal information under the protection of cryptosystem. The anonymity then can be maintained in all methods. As to the encouragement, it is quite important to trigger verification services to finish a transaction in the distributed network. This is the kernel belief that all nodes have to replace a trust third party to take the responsibility of verification. Otherwise, the whole system may only become a practical one theoretically. It is clear that only the conventional blockchain and the new system can achieve this essential. Concerning the resistance to Sybil attack, it shall be guaranteed to prevent a node from the risk of unfair resource allotment. The discussion on how to confirm this property is explained in section 4.1. Referring to the problem of double spending which is a serious threat in an e-payment system, both the conventional blockchain and new method can avoid this malicious behavior, as discussed in section 4.2. Unfortunately, a malicious node might be able to launch this behavior successfully in Trustchain network. Even this attempt could be detected afterwards, the loss has happened. Regarding to the asynchronous storage, it has been employed in Trustchain and the new method. The verification of a transaction only depends on a partial group of nodes; thus, bringing in the efficiency improvement.

Table 4. Comparisons of Essential Properties

Property \ Architecture	Blockchain	Trustchain	Ours
Decentralization	Y	Y	Y
Anonymity	Y	Y	Y
Encouragement	Y	N	Y
Sybil-Resistant	Y	Y	Y
Avoid Double Spending	Y	N	Y
Asynchronous	N	Y	Y
Supply and Demand Balance	N	N	Y

For the balance of supply and demand, it shall be ensured to avoid resource wastage and optimize the benefit. In conventional blockchain network, the reward comes from the block establishment. Network nodes are willing to spend lots of computing resources to fulfill the condition of consensus algorithm. Nevertheless, these resources are not well adjusted based on the market demand to mitigate unnecessary consumption. On the other hand, the selection of a verifier in Trustchain depends on the NetFlow accounting mechanism [9]. Without the help of verification reward, it may result in the underproduce problem. Once it takes more time to find a verifier, the performance of whole system must be lowered down. Concerning the dual blockchain, the reputation value is used to be the launch condition of a transaction, while the reward mechanism is applied to attracting verification services. According to the weight of reputation, the computing wastage on earning more rewards can be effectively mitigated. Namely, the new method can obtain a satisfactory balance between resource and reward.

6 Conclusions

Conventional blockchain technique is hard to be applied to a real-time e-payment platform due to the adoption of consensus algorithm and a large scale of data size. In this article, we have introduced asynchronous dual blockchain to design an e-payment mechanism. Inheriting the security from a blockchain technique, we have exploited the asynchronous storage and reputation strategy to reduce resource consumption. Experimental results have demonstrated that the asynchronous dual blockchain is fairly safe and efficient to reach a real-time application.

References

[1] Statista, E-commerce Worldwide, https://www.statista.com/study/10653/e-commerce-worldwide-statista-dossier, 2019.

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2009.

[3] Z. Zheng, S. Xie, H. N. Dai, X. P. Chen, H. M. Wang, Blockchain Challenges and Opportunities: A Survey, *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp. 352-375, October, 2018.

[4] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[5] C. W. Hsueh, C. T. Chin, EPoW: Solving Blockchain Problems Economically, *14th IEEE SmartWorld Advanced and Trusted Computing (ATC '17)*, San Francisco, CA, USA, 2017, pp. 1-8, Doi: 10.1109/UIC-ATC.2017.8397612.

[6] G. Wood, *Ethereum: A Secure Decentralized Generalized Transaction Ledger*, Technical Report EIP-150 Revision, April, 2017.

[7] C. Decker, R. Wattenhofer, A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels, *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, Edmonton, AB, Canada, 2015, pp. 3-18.

[8] F. Y. Gai, B. S. Wang, W. P. Deng, W. Peng, Proof of Reputation: A Reputation-based Consensus Protocol for Peer-to-Peer Network, *International Conference on Database Systems for Advanced Applications*, Gold Coast, Queensland, Australia, 2018, pp. 666-681.

[9] P. Otte, M. de Vos, J. Pouwelse, Trustchain: A Sybil-Resistant Scalable Blockchain, *Future Generation Computer Systems*, Vol. 107, pp. 770-780, June, 2020, Doi: 10.1016/j.future.2017.08.048.

[10] J. R. Douceur, The Sybil Attack, *First International Workshop on Peer-to-Peer Systems*, Cambridge, MA, USA, 2002, pp. 251-260.

[11] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina, The Eigentrust Algorithm for Reputation Management in P2P Networks, *12th International Conference on World Wide Web*, Budapest, Hungary, 2003, pp. 640-651.

[12] Y. C. Zhang, Y. G. Fang, A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, No. 8, pp. 1134-1145, August, 2007, Doi: 10.1109/TPDS.2007.1043.

[13] H. F. Yu, M. Kaminsky, P. B. Gibbons, A. D. Flaxman, SybilGuard: Defending Against Sybil Attacks via Social Networks, *IEEE/ACM Transactions on Networking*, Vol. 16, No. 3, pp. 576-589, June, 2008.

[14] Y. C. Zhang, S. S. Chen, G. Yang, SFTrust: A Double Trust Metric based Trust Model in Unstructured P2P System, *2009 IEEE International Symposium on Parallel & Distributed Processing*, Rome, Italy, 2009, pp. 1-7, Doi: 10.1109/IPDPS.2009.5161240.

[15] R. Dennis, G. Owen, Rep on the Block: A Next Generation Reputation System based on the Blockchain, *10th International Conference for Internet Technology and Secured Transactions (ICITST '15)*, London, UK, 2015, pp. 131-138.

[16] R. Dennis, G. Owenson, Rep on the Roll: A Peer to Peer Reputation System based on a Rolling Blockchain, *International Journal of Digital Society*, Vol. 7, No. 1, pp. 1123-1134, March, 2016.

[17] D. Hudson, 7 Transactions Per Second? Really?, http://hashingit.com/analysis/33-7-transactions-per-second, 2014.

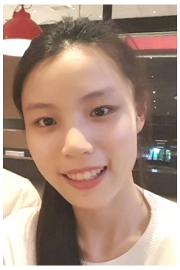
[18] Visa, Visa Incorporation at a Glance, https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf, 2015.

[19] J. S. Lee, Y. C. Chen, Y. H. Kang, R. K. Yang, Preserving Privacy and Fairness for an Innovative E-Commerce Model: Penny M-lottery, *Journal of Internet Technology*, Vol. 20, No. 5, pp. 1387-1400, September, 2019.

[20] J. S. Lee, K. S. Lin, An Innovative Electronic Group-buying System for Mobile Commerce, *Electronic Commerce Research and Applications*, Vol. 12, No. 1, pp. 1-13, January-February, 2013.

Biographies

Wei-Chih Hong received the B.S. and M.S. degrees in electrical engineering from NationalTaiwan University, Taipei, in 1996 and 1998, respectively. He received his Ph.D. degree at the Graduate Institute of Communication Engineering, National Taiwan University. During 1999-2003, he worked as an assistant researcher at the Telecommunication Laboratories of Chunghwa Telecom. Currently, he works as an assistant professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His research interests are in the areas of wireless networks, information security, cryptanalysis, and blockchain.



Ying-Chin Chen received her M.S. degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2018. Her current research interests include information security, visual secret sharing, and blockchain.

Ren-Kai Yang received his M.S. degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2019. His current research interests include network security and blockchain.

Bo Li has worked as an assistant professor at the Department of Computer Science of University of Illinois at Urbana-Champaign, USA from 2018. Her current research interests include image processing, machine learning, security, privacy, game theory, and blockchain.

Jung-San Lee received the BS degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 2002. He received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2017, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include network management, electronic commerce, and blockchain.