Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain

Hyunjae Lee, MyungJae Shin, Kyeong Seon Kim, Yeongeun Kang, and Joongheon Kim
School of Software, Chung-Ang University, Seoul, Republic of Korea
joongheon@cau.ac.kr

***Abstract*—This paper presents a new approach for avoiding double-spending attacks via the concept of recipient-oriented concepts in private blockchain networks. Together with the concepts of stealth address and masternode at recipient sides, transactional privacy is assured and transaction recipients become active which receive transaction propagation unilaterally. Based on this approach, it can be shown that recipient-oriented method is suggested for preventing the double-spending attacks in this paper. In addition, the proposed method is possible to prevent double spending attacks using the verification time of the recipient and blocking time of the transaction.**

I. Introduction

Bitcoin was first emerged as a cryptocurrency that allows untrusted participants to make secure transactions without relaying on trusted central third party. It is possible through the blockchain technique that demonstrates a logical way to ensure transactions are kept secure in distributed network environment [1]. Even so, there is a weakness in transaction procedure where token is exchanged between participants. In the conventional cryptocurrency such as Bitcoin, digital signature is used to prove the owner of the token and to demonstrate the sender of the transaction. However, there is no operation for the recipient to intervene for verifying legitimacy of token. Due to this asymmetry, the digital signature can not handle appropriately double spending problems alone.

For example, if the sender owns 1 token and sends transactions to several recipients with signature of sender at the same time using a token that used once, the recipients can only confirm that the sender has sent transaction. The recipient does not know whether this is a double spending transaction or not. The problem is only transactions that are deemed to be valid will be recorded in distributed ledger. In addition, there is no criterion for what kind of transaction should be accepted when such double payment occurs. Thus the recipient is forced to judge that the transaction between itself and sender is correct. Moreover, there is a possibility that the transaction can be invalidated after an attack using a structure in which a longer blockchain is recognized as a main validated chain even if the receiver confirmed that the transaction is recorded in ledger.

These problems are likely to occur in private Blockchain, which is a permitted ledger that can only be accessed by authorized users in the process of reading, writing, and consensus. In a private blockchain, not only the transaction of the token, but also the transactions of the assets between corporations occur. A number of researches have already done to prevent attacks on private blockchain, but they do not take into account the asymmetric of the recipient and sender. In this paper, we propose recipient oriented transaction method which avoid double spending attack by controlling the time of validation and broadcast.

Our proposed *recipient-oriented transaction* allows the receiver of a transaction to directly check and broadcast the validity of the transaction before it is written to the block. It consists of two major concepts: stealth address and masternode. First, stealth address ensures the privacy of recipients, which is a disposable public key that is a combination of public key of recipient and random data. In this algorithm, it is used to indicate the transaction address to which recipient will connect. Once the sender has created a transaction, it automatically creates a unique disposable public key for the transaction, which, if delivered to the recipient, allows the recipient to access the transaction via this public key. After that, the transaction can be approved and broadcast with private key of the recipient. Second, masternode provides special operations unlike other normal nodes. It receive a fee and provide differentiated operation such as InstantSend. In our method, the recipient performs this role for own transaction. The recipient performs verification of transactions personally. If recipient approves that there is no problem with the transaction, the transaction is locked and approved. Thereby, locked resources will be filtered during verification by other recipients. At this point, it is a major part of our method to make it impossible for the sender to predict when to lock and approved.

II. Recipient-Oriented Transaction

A. Backgrounds

1) Stealth address: This concept uses unique disposable public key which is combined with public view key and public spend key of the recipient and random data. All transactions make automatically its own stealth address that has critical information such as *who can spend this amount of credits on this transaction*. Then, the recipient can detect the information using private key of the recipient.

2) Masternode: Masternode is treated as a mediator as well as a guarantor for InstantSend and PrivatrSend. The PrivateSend operation is to mix incoming transaction up in order to make them untraceable. Masternode immediately confirms the transaction by using InstantSend operation. However, since the masternode does not create blocks, transaction must also be included in the block later. Instead, it is named with special

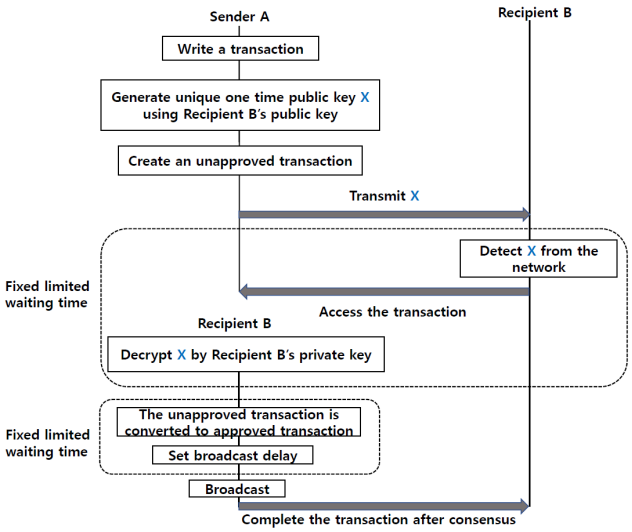

Fig. 1: Recipient-Driven Transaction Workflow

mark when recorded in a block. To prevent double payment before the transaction is recorded in block, masternode change the status of the transaction and lock it so that resources are not paid multiple times in the blockchain network. We have used this concept to devise a recipient-driven method that allows recipients to perform verification on transactions.

B. Method

In our method, each transaction is completed only if the recipient determines the transaction is valid within a fixed waiting time. The procedure is illustrated in Fig. 1.

1. As similar to the conventional transaction process, the sender put necessary information in the transaction history.
2. The sender generates a unique one-time public key for the transaction using the recipient's public address; and makes the transaction unapproved (default).
3. The sender forwards the unique disposable public key to the recipient.
4. Recipients use the unique disposable public key received to detect transactions coming to the recipient.
5. Perform validation on the transaction and change the state of transaction using private key of the recipient.
6. The recipient sets the propagation time after the change.
7. The process after broadcasting transaction follows the conventional process.

This algorithm is similar to conventional blockchain, however the recipient intervenes during the verification and propagation of transactions. To prevent delays of malicious recipients, fixed waiting time is set so that transactions can be initialized; and the transaction is automatically refunded to the sender.

1) Adapting Stealth Address and Masternode: In this algorithm, every transaction must be initially in "Unapproved" thus senders keep wait for recipients. The state of transaction and the propagation can only be done using the private key of recipient and unique disposable public key. There are 5 steps to get unique one-time address T that let the recipient detect and control the transaction.

1. Recipient's public key: $A = \alpha.G$
2. Sender's public key: $B = \beta.G$
3. Using Diffie-Hellman, shared key S exists: $S = \beta.A = \alpha.B$
4. Stealth Address SA and private key γ: $SA = H(S).G$ and $\gamma = H(S) \bmod Q$
5. The recipients get a transfer address T to detect the transaction: $T = H'(H(b.A).G)$

When a recipient tries to access to the transaction using the unique one-time address T, the transaction checks if the recipients private key can generate the public key in the transaction by calculating the recipients private key using elliptic curve cryptography. If the generated public key is exactly same with the public key in the transaction, the recipient is proved. In other words, through the generated T, only the recipient of transaction are authorized to handle the procedure of propagation of the transaction process.

2) Approve and Delay: The recipient of the transaction determines whether the resource used in the transaction is valid such as token and approves the transaction. Through this, propagation of transaction is not initiated from the sender but from the recipient. This algorithm prevents the sender from spreading multiple double-payment transactions over network. In addition, transaction verification time is hidden thus it is difficult for cooperative malicious node to send double-payment transactions as soon as normal node approves transaction. Even if the approval verification is correct, double spending prevention is performed by a sequence that allows the recipient to set the propagation time after the approval.

III. Concluding Remarks and Future Work

This paper proposes *recipient oriented transaction* to prevent double spending problem through intervention during the transaction propagation. By using the concept of stealth address and masternode, transactional privacy is assured and transaction recipients become active agents different from conventional blockchain that receive transaction propagation unilaterally. The recipient accesses and verifies the transaction. After that depending on the result, recipient switches the state of transaction to the approved and locked. Then the sender knows the status of the transaction but can not recognize the broadcast time which actually propagates the transaction to the network. As a result, it is possible to prevent double spending attacks using the verification time of the recipient and blocking time of the transaction. As future research, the performance evaluation via real-world software prototype is scheduled.

Acknowledgment

This work was supported by the National Research Foundation of Korea (2017R1A4A1015675). J. Kim is a corresponding author of this paper.

References

[1] C. Cai, X. Yuan, and C. Wang, "Hardening Distributed and Encrypted Keyword Search via Blockchain," in *Proc. IEEE Symposium on Privacy-Aware Computing (PAC)*, August 2017.