Towards a Dynamic Reputation Management Scheme for Cross-chain Transactions

Lin-Fa Lee and Kuo-Hui Yeh

July 20, 2022

Towards a Dynamic Reputation Management Scheme for Cross-chain Transactions

Lin-Fa Lee[1], Kuo-Hui Yeh[1]

[1]Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan R.O.C.

***Abstract*—Recently, research communities have dedicated their efforts to the development of versatile and innovative Blockchain-based application systems. These systems are usually independent and thus difficult to be integrated and cooperated with each other during cross-chain transactions in terms of the interoperability perspective. In addition, there may be potential risks once external malicious attackers desire to control or manipulate nodes in cross-chain systems. It is necessary to have a solution preventing users' misbehaviors during the process of information and value exchange among different blockchains. In this paper, we propose a dynamic reputation management scheme which can effectively detect misbehaviors and identify potential security risks during cross-chain transactions. Our scheme conducts a mechanism evaluating reputation and trustworthiness of nodes and chains, respectively, through their current state and transactions history. This characteristic can help any cross-chains system well-react and be resistant against ongoing-endangered behaviors within a reasonable computation time.**

***Index Terms*—blockchain, cross-chains, reputation management, interoperability**

I. Introduction

Blockchain technology has become one of the most subversive innovative technologies after the bitcoin [1] system was proposed in 2008. Since then, Blockchain has been adopted and utilized in different applications, such as financial, medical and cryptocurrency, with its de-centralized property and immutability. However, the heterogeneity of current Blcokchain platform technologies leaves it in a dilemma where it is difficult to integrate the value and information exchange processes of multiple blockchain platforms with versatile consensus protocol. The study [2] has proposed several critical issues for cross-chain transaction circumstances. For example, when one blockchain system tries to access the data from another blockchain system for cross-chain transactions, it is necessary to have a consensus on data access, processing and storage and, after that, to walk toward to a mechanism ensuring trustworthy and consistency on data/transactions exchanged among communicating entities from different blockchains. Nevertheless, once two application systems belong to separate organizations and each of them has its own blockchain system, the different architecture and consensus mechanism will lead to security issues when data exchange and data access across chain systems, i.e. denial of services (DoS) attacks [3], double-spending [4] and selfish-mining attack [5]. For this reason, it is necessary to design a secure method that can guarantee the trustworthiness of cross-chain interoperability process. Furthermore, the method must be universally suitable to heterogeneous blockchain systems in numerous application scenarios.

Hence, in this study we are devoted to develop a reputation management scheme to effectively detect and identify potential malicious attackers during cross-chain transactions. Our scheme focuses on evaluating the system trustworthiness in terms of nodes and chains. Moreover, to ensure the security of cross-chain interoperability, we adopt seven indicators resistant against existing known attacks as show in Table 1. These indicators will be considered as major evaluation criteria on rating the reputation of the nodes involved within cross-chains transactions.

TABLE I
REPUTATION INDICATORS AND THREATS WITH CONDITION JUDGEMENT THAT USED IN OUR PROPOSED SCHEME

Reputation Indicator	Initial Value	Condition Judgement	Pre-define weight	Corresponding Attack & Threat
(Node) ***Node connect status***	None	$\begin{cases} if\ \text{Async},\ -1 \\ if\ \text{sync},\ 0 \end{cases}$	1	None
(Node) ***Hardware usage***	Average GPU compute power of a period of time.	$\begin{cases} Increase\ or\ Decrease\ rapidly\ ,-1 \\ Slow\ or\ Constant\ ,\ 0 \end{cases}$	0.6	Selfish mining, Block withholding, Majority attack
(Node) ***Average spending time of transaction***	Current time + Expect time of block generation.	$\begin{cases} Overtime\ ,\ -1 \\ On\ time\ ,\ 0 \\ Less\ time\ consumption,\ -1 \end{cases}$	0.4	Double-spending, Consensus delay
(Node) ***Transaction consequence***	None	$\begin{cases} Success\ ,1 \\ Failure,\ -1 \end{cases}$	1	DDoS, Double-spending, Time-jacking attacks
(Chain) ***Average network hashrate***	Average network hashing power of a period of time	$\begin{cases} Increase\ or\ Decrease\ rapidly\ ,-1 \\ Slow\ or\ Constant\ ,\ 0 \end{cases}$	0.6	Stale orphaned blocks, Selfish mining, Majority attack
(Chain) ***The delay time in block propagation***	None	$\begin{cases} Delay\ \frac{E(T)}{2}\ time,-1 \\ On\ time,\ 0 \end{cases}$	1	Consensus delay, Selfish mining, Block withholding, Stale & Orphaned blocks, Time-jacking attacks
(Chain) ***Average spending time of each transaction***	Expect time $E(T) = \frac{Difficulty\_value}{Hash\_rate}$	$\begin{cases} Overtime\ ,\ -1 \\ On\ time\ ,\ 0 \\ Less\ time\ consumption,\ -1 \end{cases}$	0.4	Double-spending, Consensus delay

II. The Proposed Scheme

In this section, we introduce our proposed dynamic reputation management scheme in which three independently heterogeneous blockchain systems including one relay chain are involved with. The rely chain are responsible for the agreement of transaction and the corresponding consensus which will be uploaded and accepted by these three heterogeneous blockchain systems. As shown in Fig. 1, we have a major relay-chain and two sub-chains in our system scenario. Each blockchain system and each node will have a specific reputation value as the degree of trust in the next interactions (and transactions). As the proposed system is used to prevent the misbehavior in heterogeneous blockchains, the analysis of the node and the chain's past normal transaction records is adopted to detect potential misbehaviors. In addition, the proposed system allows to dynamically modify indicator weights by nodes in the relay-chain according to the frequency of current misbehaviors.

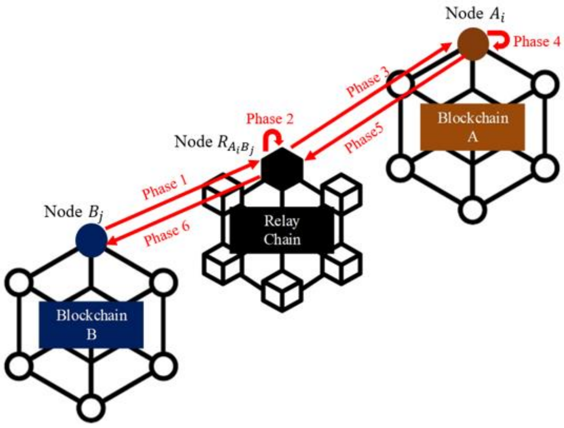

Figure 1: The interoperation process for cross-chains transactions.

A. *Cross-chain interoperation process (Figure 1)*

Suppose that node B_j in *Blockchain_B* wants to exchange information with node A_i in *Blockchain_A*. The details of the phases are presented as follows.

- Phase 1: Node B_j starts a request R_j to a bridge node $R_{A_iB_j}$, which is responsible for transaction exchanging between nodes A_i and B_j, in the relay chain. The bridge node $R_{A_iB_j}$ will establish a secure channel to *Blockchain_A* and launch a cross-chain interoperation.
- Phase 2: Node $R_{A_iB_j}$ will judge the trustworthiness of *Blockchain_B* in terms of the reputation value through the three chain-level indicators, i.e. *average network hashrate*, *the delay time in block propagation* and *average spending time of each transaction*, as shown in Table 1. Meanwhile, node $R_{A_iB_j}$ will evaluate if the reputation of node B_j is satisfied through the four node-level indicators, i.e. *node connect status*, *hardware usage*, *average spending time of transaction* and *transaction consequence*, presented in Table 1. If one of these seven indicators does not pass a pre-defined threshold, node R_{B_j} will be judged as a potentially misbehaved node. The incoming request R_j will be rejected and node $R_{A_iB_j}$ will send a message to node B_j as a termination commend. If all of these seven indicators are all passed, it will proceed to Phase 3.
- Phase 3: Node $R_{A_iB_j}$ then launches a request R_j' and sends R_j' to node A_i. At the same time, the trustworthiness of node A_i and *Blockchain_A* will be evaluated through the same steps in Phase 2. That is, the seven indicators presented in Table 1 will be adopted to examine whether node A_i and *Blockchain_A* is classified to misbehaved one or not.
- Phase 4: Similarly, based on the indicators, node A_i then evaluates if the reputation of node $R_{A_iB_j}$ is satisfied after obtaining the request R_j'. If it is not satisfied, node A_i will send a message to $\mathrm{R}_{\mathrm{A_iB_j}}$ to cancel the current transaction. Otherwise, node $\mathrm{A_i}$ will accept the request. Next, $\mathrm{A_i}$ will send a reply $\mathrm{P_i}$ to node $\mathrm{R}_{\mathrm{A_iB_j}}$.
- Phase 5: Node $R_{A_iB_j}$ will then check whether node A_i has successfully completed the request after receiving P_i. In case of a normal transaction (which is successfully completed), the reputation of node A_i will be adjusted and P_i will be sent back to node B_j through node $R_{A_iB_j}$. Otherwise, the reputation of node A_i will be adjusted and the transaction will be terminated.
- Phase 6: Node B_j confirms P_i and the cross-chain transaction will be considered as a finished one. In case of a failed transaction, the reputation of Node $R_{A_iB_j}$ will be adjusted by node B_j. Afterwards, the information related to the failed transaction will be reported by node B_j.

III. Conclusions

In this study, we propose a reputation management scheme for communicating entities during cross-chain transactions. We summarize a list of indicators for reputation evaluation in which these indicators are against various Bleckchain-relevant attacks. Then, the evaluated reputation will be utilized to detect and identify misbehaved node and chain. In brief, our proposed scheme can achieve the compatibility among multiple blockchains, and guarantee a certain success rate of cross-chains transactions as well.

References

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[2] Hai Jin, Xiaohai Dai, Jiang Xiao, "Towards A Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains," The IEEE Conference on 38th International Conference on Distributed Computing Systems (ICDCS 2018) , Vienna, Austria, 2-6 July 2018.

[3] Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal, Ari Juels, "BDoS: Blockchain denial-of-service," The 2020 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS'20), October 2020, pp. 601-619.

[4] Ghassan O. Karame, Elli Androulaki, Srdjan Capkun, "Double-spending fast payments in bitcoin," The 2012 ACM conference on Computer and communications security (ACM CCS'12), October 2012, pp.906-917.

[5] Ayelet Sapirshtein, Yonatan Sompolinsky, Aviv Zohar, "Optimal selfish mining strategies in bitcoin," International Conference on Financial Cryptography and Data Security (FC 2016), pp. 515-532, 17 May 2017.