Blockchain-based Secure Platform for Coalition Loyalty Programs Management

Cong T. Nguyen[1,2,3], Dinh Thai Hoang[1], Diep N. Nguyen[1], Hoang-Anh Pham[2,3],
Nguyen Huynh Tuong[2,3] and Eryk Dutkiewicz[1]
[1] School of Electrical and Data Engineering, University of Technology Sydney, Australia
[2] Ho Chi Minh City University of Technology, Vietnam
[3] Vietnam National University Ho Chi Minh City, Vietnam

***Abstract*—In this paper, we propose a novel blockchain-based platform for the coalition loyalty program management. The platform allows the customers to freely exchange loyalty points (in forms of blockchain tokens) from different existing blockchain-based loyalty programs by utilizing sidechain technology. Moreover, by adopting Proof-of-Stake consensus mechanism, we can further increase customer engagement by allowing the customers to participate in the consensus process to earn additional tokens. However, this might lead to situations where the customers centralize all tokens to a single chain/loyalty program if the chain offers more rewards for consensus participation. Through security and performance analyses, we show that such centralization of stakes poses a threat to the security and performance of the platform. Therefore, we develop a non-cooperative game model to analyze the rational behavior of the users. We find that the consensus participation rewards govern the user behavior and the decentralization of the system. Numerical experiments confirm our analytical results and show that the ratios between the consensus rewards have a significant impact on the system's security and performance.**

Keywords- Blockchain, Proof-of-Stake, loyalty programs, and non-cooperative game.

I. Introduction

Despite the omnipresence of loyalty programs in various industries such as travel, retail, and financial services, they are still facing huge challenges. According to [1], companies have spent more than $1.2 billion each year on loyalty programs in the U.S. alone. Nevertheless, the performance of these programs rarely met the expectations, which leads to the termination of many programs [1]. The main reason is the wide diversity of programs coupled with their complex processes, which leads to many difficulties for the customers to exchange or use their loyalty points [2]. To overcome these shortcomings, companies have created coalition loyalty programs where the loyalty points can be collectively accumulated and spent on different options offered by different companies [3]. Nevertheless, these coalition programs require highly secure and effective platforms for loyalty points exchanging and redemption.

Recently, blockchain technology has emerged to be a secure and effective solution for loyalty program management thanks to its advantages of transparency, decentralization, and immutability. Organizations including Singapore Airlines [4] and American Express [5] have recently introduced their blockchain-based solutions for coalition loyalty program management. Moreover, several companies have been forming blockchain-based coalition loyalty programs such as Loyalwallet (https://loyalwallet.io/) Dragonchain (https://dragonchain.com/), and Krispay [4]. However, these programs were developed on individual blockchains, which requires merging different blockchains into a single blockchain network. Such single-blockchain platforms have several limitations. Firstly, once the blockchains are merged, the companies will lose control over their individual programs. Moreover, merging two different blockchain networks may suffer many technical issues due to different policies, requirements, and technologies used in the companies. Furthermore, when using a shared blockchain network, it is very difficult if a company wants to implement new policies for its services and customers as these policies need to obtain the agreements from other companies in the network. Consequently, these limitations may prevent the companies from joining single-blockchain coalition programs. Recently, sidechain technology [6] has been developed to enable the transfers of network tokens (e.g., loyalty points) between different blockchain networks. This enables multi-blockchains coalition programs, which is a promising solution to the aforementioned problems because the companies are no longer required to merge their blockchains, and they can also retain their controls over their own loyalty programs.

To further attract customer engagement to the loyalty programs, the customers can be incentivized to participate in the consensus mechanisms in the individual blockchains to earn additional loyalty points. Among the blockchain consensus mechanisms, the Proof-of-Work (PoW) [7] has several limitations including huge energy consumption and significant delay, e.g., one hour on average [9], which makes it unsuitable for loyalty programs. To overcome these problems, a new consensus mechanism has been developed recently, namely Proof-of-Stake (PoS) [8], [9], [12], which has many advantages, including negligible energy consumption and especially very low consensus delay [9]. Furthermore, users who participate in the PoS have a chance to obtain rewards in the forms of tokens. However, this might have an effect on the system as a whole, since the users may be attracted to the blockchain with the highest reward. Such centralization to a single blockchain might have negative impacts on the security and performance of the other blockchains in the same coalition loyalty program. Therefore, the impact of user consensus participation needs to be analyzed.

To address the abovementioned problems, we develop a novel multi-blockchains platform for coalition loyalty program management. In particular, we first adopt sidechain technology

which does not require complex and costly solutions for merging different blockchain networks and also allows the companies to retain control over their individual loyalty programs. Among the available blockchain consensus mechanisms, we adopt the PoS-based Ouroboros consensus mechanism [8] which has a low delay (approximately 3 minutes on average[1]) and proven security properties [8]. These characteristics are advantageous in governing a secure and efficient platform for coalition loyalty program management. We then conduct security and performance analyses of the system, especially in the cases of adversarial attacks, to show that the security and performance of the system depend on the users' consensus participation. Thus, we model the rational user behavior using the non-cooperative game theory to examine how the users will act and to what extent such actions affect the system. Through numerical experiments, we then show the impacts of the user behavior and the rewards on the security and performance of the proposed system.

II. System Model and Analysis

A. Proposed System

1) System overview: Fig. 1 illustrates our proposed coalition loyalty management system which consists of the companies, the customers, and the decentralized token exchange platform. In the system, each company has its own loyalty program managed on its individual blockchain network. Each company's blockchain contains a ledger that stores the customer accounts and their loyalty points records. When a customer purchases a product from a company, the corresponding loyalty points are sent to the customer in forms of blockchain tokens (each company may have a different type of tokens). Such transfer of tokens is recorded on the blockchain as a transaction.

2) Token exchange platform: To form the coalition program, the companies negotiate the loyalty points exchange rates among them in advance. Then, each company creates and stores a smart contract (i.e., a user-defined program which is automatically enforced when the conditions stated in the smart contract are met [13]) on the blockchain. This smart contract specifies the exchange rate between the two tokens and triggers the exchange of loyalty points between the two companies. When a new company wants to join the coalition, it just needs to negotiate the exchange rates with the coalition and create corresponding smart contracts. This reduces the setup times and implementation costs for new companies who want to join the coalition, as well as let the companies maintain their independent controls over their individual programs.

When the customers want to redeem their loyalty points from one company at the vendors of another company, they can freely exchange the tokens to that company's tokens via the proposed decentralized token exchange scheme. Sidechain technology is the core technology of the proposed token exchange scheme. This technology refers to the methods that enable the transfers of assets (e.g., coins) between different blockchain networks (i.e., sidechains). Depends on the level of centralization, these

[1]https://cardanodocs.com/cardano/proof-of-stake/

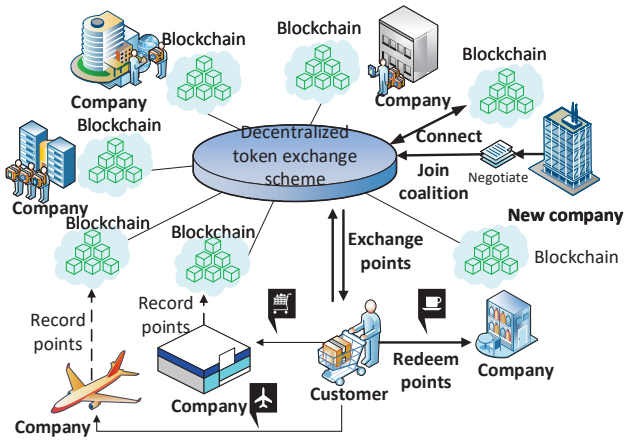


Fig. 1: An illustration of the proposed system.

methods can be further classified into centralized two-way pegs, federated two-way pegs, and Simplified Payment Verification (SPV). Although the first two schemes can achieve a high processing speed, they both require trust in a single or a group of entities, which is more vulnerable to corruption, single-point-of-failure, and security threats [6]. In contrast, the SPV scheme does not require a central authority to validate cross-chain transactions. Thus, for validation, a user can submit an SPV proof which shows that the transfer transaction belongs to a valid block of the originating chain. Although this process requires a longer time for confirmation, it eliminates the risk of centralization and single-point-of-failure [6]. Therefore, we propose to use the SPV scheme for our platform.

As illustrated in Fig. 2, the token exchange procedure consists of several steps. At the beginning, two companies negotiate a loyalty point-exchange agreement which specifies the exchange rate between the two tokens. This agreement is then stored in each chain as a smart contract. Then, when a customer wants to exchange some T_2^o tokens into T_1^o tokens, the customer sends a transaction $Tx1$, containing some T_2^o tokens, from its account on sidechain 2 to the smart contract SC_2. The customer then sends a transaction $Tx2$ and an SPV proof from its account on sidechain 1 to SC_1. $Tx2$ triggers SC_1 to validate the sent SPV proof. During the confirmation period, SC_1 checks (1) the validation of the SPV proof and (2) any conflicts of the submitted SPV proof. After the confirmation period, SC_1 sends a number of T_1^o tokens to the customer's address on sidechain 1 in accordance with the exchange rate.

3) Blockchain individual consensus mechanism: Due to the advantages of low computational requirements, low delay, and the ability to attract customers to participate in the blockchain consensus, the PoS mechanism is chosen for our system. Among several variants of the PoS mechanism, we choose to adopt the Ouroboros consensus mechanism because of its proven security properties [8]. In Ouroboros, time is divided into epochs, and each epoch is divided into time slots. At the first time slot of epoch e_k, a committee of stakeholders executes an election protocol to elect the leaders for the epoch e_k, such that for each time slot there is one designated leader who creates one

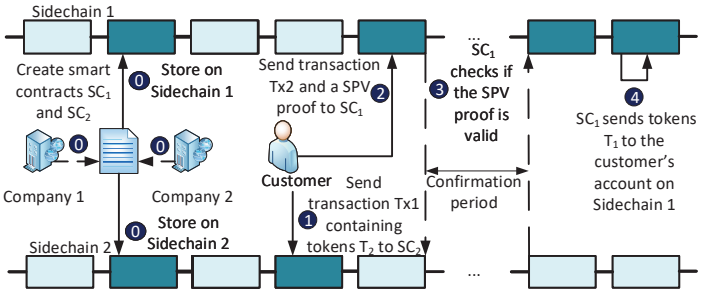


Fig. 2: An illustration of the token exchange procedure.

new block to add to the chain. The committee also elects the committee members for the epoch e_{k+1}.

To elect the leaders and committee, the current epoch's committee members create the seeds for the FTS algorithm (which is a hash function that takes any string as input and outputs a token index [9]). The current owner of the index is then chosen as a leader of this epoch or a committee member of the next epoch. The selected leaders will then be able to create new blocks to add to the chain and obtain a block reward, e.g., a number of tokens. The expected payoff U_n of stakeholder n who has s_n stakes (tokens) in a blockchain network of N users is:

$$U_n = \frac{s_n}{\sum_{n=1}^{N} s_n} R, \tag{1}$$

where R is the block reward (tokens per block). On the one hand, this creates an opportunity for the company to further increase customer engagement by incentivizing the customers to participate in the company blockchain via the block rewards. On the other hand, this poses a threat to the multi-chains system's security. As can be seen from (1), a stakeholder's reward is directly proportional to the chain's block reward. Consequently, a chain with a high block reward may attract more stakes from stakeholders, causing the centralization of stakes and leaving the other chains more vulnerable to attacks. In the following, we will analyze how the stakes level affects a blockchain's security and performance.

B. Security and Performance Analysis

1) Adversary model: To analyze the security and performance of the considered system, we first define the adversary model. The adversary with a stake budget B_A attempts to attack the consensus process of the blockchain networks, aiming to revert a transaction by creating conflicting blocks. Let B_n and γ denote the stake budget of stakeholder n and the honest stake ratio, respectively. Then, the ratio of adversarial stakes is $1-\gamma = \frac{B_A}{\sum_{n=1}^{N} B_n + B_A}$. We assume that the adversary can move its stakes to any chain to perform attacks such as double-spending, grinding, nothing-at-stakes, and 51% attacks [9]. In a double-spending attack, the adversary firstly sends a transaction to spend some tokens, e.g., to redeem some loyalty points. After that transaction is confirmed, i.e., the loyalty points are redeemed, the adversary can create a fork (a different version of the blockchain) to erase the transaction from the blockchain. If that fork is accepted by the honest users, the adversary can gain back the tokens it already spent. For grinding and nothing-at-stakes attacks, when the adversary is elected to be the leader, it can create multiple blocks to influence the leader election process or create forks for a double-spending attack. In the 51% attack, the adversary who controls more than 50% of the blockchain's stakes will try to revert transactions or attack the leader election process (the leader election process no longer guarantees unbiased randomness if the adversary control more than 50% stakes [8]).

2) Security Analysis: To maintain the blockchain's operations and security, a consensus mechanism must satisfy the common prefix property (CP) with parameter $\kappa \in \mathbb{N}$ [11]. The property is satisfied if for any pair of honest users, their versions of the chain $\mathcal{C}_1, \mathcal{C}_2$ must share a common prefix. Specifically, assuming that $\mathcal{C}_2$ is longer than $\mathcal{C}_1$, removing κ last blocks of $\mathcal{C}_1$ results in the prefix of $\mathcal{C}_2$. We will prove that the adopted consensus mechanism can satisfy the common prefix property with overwhelming probability in the following Theorem.

THEOREM 1. *The common prefix violation probability is less than or equal to* $(1-\gamma)^{\kappa}$.

Proof: Any fork created by the adversary must include all the blocks created by the honest leaders. This is because if an honest leader does not change its block, then the adversary can either adopt the block in the fork or replace it with another block. However, as the list of leaders is known, the adversary must include the honest block in the fork. Otherwise, it will create an invalid fork that will be rejected. Moreover, any change in a block's content results in a different block's hash, and the block's hash is linked to its previous block. Thus, the chain from the first block to the latest honest block is confirmed by every honest user. As a result, the adversary can only create forks with κ last blocks different from the honest fork if it is elected to be the leader for κ consecutive blocks. Since $(1-\gamma)$ is the ratio of adversarial stakes in the total network stakes, the probability that the adversary is elected to be the leader for κ consecutive blocks is

$$\mathrm{P}^{\mathrm{r}}_{\mathrm{CP}} = (1-\gamma)^{\kappa}, \tag{2}$$

which is also the probability that the common prefix property is violated. ■

In our system, the adversary can create multiple blocks for grinding and nothing-at-stakes attack. However, grinding attacks are mitigated because the leader election process cannot be affected by creating multiple blocks. Moreover, transactions cannot be reverted without violating the common prefix probability [8]. Therefore, nothing-at-stakes and double-spending attacks are mitigated if the common prefix property holds. As can be seen from (2), the common prefix violation probability is proportional to the adversarial stakes ratio. Moreover, the adversary who controls more than 51% of the network's stakes (51% attack) can successfully influence the leader election process [8]. Thus, the centralization of stakes into one chain poses a serious threat to the other chains' security.

3) Performance Analysis: Besides security, the adversarial ratio also negatively impacts the performance of a blockchain. As can be seen from (2), the common prefix violation probability decreases as κ increases. This means that to confirm a transaction, the stakeholders have to wait until κ_c more blocks are added to the chain, such that $(1-\gamma)^{\kappa_c}$ is extremely small (e.g., 0.1%). Formally, the transaction confirmation time t_c is $t_c = \kappa_c T_b$, where T_b is the time it takes to add one block to the chain (e.g., $T_b = 20s$ in Ouroboros [8]), and κ_c is defined by

$$\kappa_c = \min\{\kappa | (1-\gamma)^{\kappa} < 0.1\%\} \tag{3}$$

As observed from (2) and (3), the more stakes the adversary can control in a blockchain network, the more impacts it can have on the network's security and performance. Therefore, the stake distribution, i.e., how the total stakes of the system distribute to each chain, has a significant impact on the system's security and performance. Since the stakeholders are rational (i.e., they aim to maximize their profits), the major factor that decides the final stake distribution is the investment strategy of each stakeholder, i.e., the number of stakes a stakeholder invests in each chain. Therefore, we will examine the stakeholder strategy using game theory in the next Section to see how such rational behaviors affect the proposed system.

III. Problem Formulation

A. Stakeholders and Sidechains

The proposed system consists of a set $\mathcal{M}$ of M interconnected blockchain networks (chains) and a set $\mathcal{N}$ of N players (stakeholders). The chains have block rewards $\mathbf{R} = (R_1, \dots, R_M)$. Each stakeholder has a budget of stakes, denoted as $\mathbf{B} = (B_1, \dots, B_N)$. In the proposed system, the stakeholders can use their stakes to take part in the consensus process of every chain to earn additional profits. In particular, when stakeholder n invests s_n^m to chain m, its expected payoff U_n^m is:

$$U_n^m = \frac{s_n^m}{s_n^m + \sum_{i \in \mathcal{N}_{-n}} s_i^m} R_m, \tag{4}$$

where $\mathcal{N}_{-n}$ is the set of all stakeholders except stakeholder n. Since the stakeholders can exchange their tokens, they can freely invest stakes within their budgets to any chain, i.e., $\sum_{m=1}^{M} s_n^m \leq B_n$. Thus, the total payoff of stakeholder n is

$$U_n = \sum_{m=1}^{M} U_n^m = \sum_{m=1}^{M} \left(\frac{s_n^m}{s_n^m + T_m} R_m \right), \tag{5}$$

where $T_m = \sum_{i \in \mathcal{N}_{-n}} s_i^m$ expresses the total stakes invested in chain m by all the other stakeholders.

B. Game Theoretical Analysis

Non-cooperative game theory [14] models the situations of conflicting interests among the players. Specifically, in a non-cooperative game, each player acts independently to maximize its profit which is affected by the actions of all other players. As shown in (4), the payoff of stakeholder n on chain m increases when s_n^m increases. However, its payoff decreases as the other stakeholders increase their investments in the same chain, i.e., T_m increases, which implies the conflict of interests among the stakeholders. Therefore, this competition among the stakeholders can be analyzed by applying the non-cooperative game theory. Formally, the game is denoted by $\mathcal{G}(\mathcal{N}, (\mathcal{S}_n)_{n \in \mathcal{N}}, (U_n)_{n \in \mathcal{N}})$, which consists of three components: the set of players $\mathcal{N} = (1, \dots, N)$, the strategy set $\mathcal{S}_n$ consists of all possible strategies for each player n, and the payoff function of each player U_n. Specifically, in this game, $\mathcal{N}$ is the set of stakeholders, U_n is given by (4), and $\mathcal{S}_n$ is defined as

$$\mathcal{S}_n = \{\mathbf{s}_n = [s_n^1, \dots, s_n^M] | \sum_{m=1}^{M} s_n^m \leq B_n\}. \tag{6}$$

A desirable outcome of a non-cooperative game is the pure-strategy Nash equilibrium [14]. At the Nash equilibrium, every player cannot get a better payoff by unilaterally changing to any other strategies. As a result, if the system reaches the Nash equilibrium, it becomes stable because no player has the incentive to deviate from the equilibrium. We first prove the existence of the Nash equilibrium in the following Theorem.

Theorem 2. *There is at least one Nash equilibrium in this game.*

Proof: According to [14], if S_n is compact and convex and U_n is quasi-concave $\forall n \in \mathcal{N}$, there exists at least one Nash equilibrium. Taking the second-order partial derivative of U_n, we have

$$\frac{\partial^2 U_n^m}{\partial (s_n^m)^2} = \frac{-2 R_m T_m}{(s_n^m + T_m)^3} \leq 0. \tag{7}$$

Thus, U_n^m is concave over $\mathcal{S}_n$. Then, $U_n = \sum_{m=1}^{M} U_n^m$ is also concave over $\mathcal{S}_n$. Moreover, from (6), it is straightforward to derive that S_n is compact and convex $\forall n \in \mathcal{N}$. ■

Then, we prove in the following Theorem that a rational player will always invest all its budget.

Theorem 3. *Every player n will invest all its budget, i.e., $\sum_{m=1}^{M} s_n^m = B_n$, regardless of other players' strategies.*

Proof: Assume that player n is employing strategy $\mathbf{s}_n$ which invests less than the available budget, i.e., $\sum_{m=1}^{M} s_n^m < B_n$. The utility function in this case is given in (5). Without loss of generality, if the player chooses a strategy $\mathbf{s}'_n$ which invests the remaining budget Δs_n^j into a chain j, its utility function becomes:

$$U'_n = \sum_{m \in \mathcal{M}_{-j}} \left(\frac{s_n^m}{s_n^m + T_m} R_m \right) + \frac{s_n^j + \Delta s_n^j}{s_n^j + \Delta s_n^j + T_j} R_j, \tag{8}$$

where $\mathcal{M}_{-j}$ is the set of all chains except chain j. Then, the difference in the utilities between the two strategies is:

$$U'_n - U_n = \frac{\Delta s_n^j \sum_{k \in \mathcal{N}_{-n}} s_k^j}{(s_n^j + \Delta s_n^j + T_j)(s_n^j + T_j)}, \tag{9}$$

which is always positive. This means that $\mathbf{s}_n$ always gives a lower payoff than $\mathbf{s}'_n$ regardless of the other players' strategies. ■

An important result from Theorem 3 is that the strategies which invest less than the total budget can be removed from $\mathcal{S}_n, \forall n \in \mathcal{N}$. Thus, we can reformulate the utility function to reflect the budget constraint as follow:

$$U_n = \sum_{m=1}^{M-1} \left(\frac{s_n^m}{s_n^m + T_m} R_m \right) + \frac{B_n - \sum_{m=1}^{M-1} s_n^m}{B_n - \sum_{m=1}^{M-1} s_n^m + T_M} R_M. \tag{10}$$

As a result, we can prove the uniqueness of the Nash equilibrium in the following Theorem.

THEOREM 4. *There is a unique Nash equilibrium in this game.*

Proof: According to Rosen's theorem [15], a sufficient condition to guarantee the uniqueness of the Nash equilibrium is that the matrix $[\mathbf{G}(\mathbf{s}, \omega) + \mathbf{G}^T(\mathbf{s}, \omega)]$ is negative definite for a fixed $\omega > 0$. $\mathbf{G}(\mathbf{s}, \omega)$ can be calculated by:

$$\begin{bmatrix} \omega_1 \frac{\partial^2 U_1}{\partial s_1^1 \partial s_1^1} & \omega_1 \frac{\partial^2 U_1}{\partial s_1^2 \partial s_1^1} & \cdots & \omega_1 \frac{\partial^2 U_1}{\partial s_1^M \partial s_N^1} \\ \omega_1 \frac{\partial^2 U_1}{\partial s_1^1 \partial s_1^2} & \omega_1 \frac{\partial^2 U_1}{\partial s_1^2 \partial s_1^2} & \cdots & \omega_1 \frac{\partial^2 U_1}{\partial s_1^M \partial s_N^2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_N \frac{\partial^2 U_N}{\partial s_N^1 \partial s_1^M} & \omega_N \frac{\partial^2 U_N}{\partial s_N^2 \partial s_1^M} & \cdots & \omega_N \frac{\partial^2 U_N}{\partial s_N^M \partial s_N^M} \end{bmatrix} \tag{11}$$

Let $\omega_n = 1, \forall n \in \mathcal{N}$, the entries of $\mathbf{G}(\mathbf{s}, \omega)$ can be calculated as follows:

- $G_{i,i} = \frac{2R_i s_i^i}{(\sum_{n=1}^N s_n^i)^3} - \frac{2R_i}{(\sum_{n=1}^N s_n^i)^2}$.
- $G_{i,j} = G_{j,i} = \frac{2R_i s_i^i}{(\sum_{n=1}^N s_n^i)^3} - \frac{R_i}{(\sum_{n=1}^N s_n^i)^2}$, where $j \neq i$ and $j-1$ is divisible by M.
- All the other entries equal zero.

As a result, $\mathbf{G}(\mathbf{s}, \omega)$ can be expressed as a sum of 2 matrices $\mathbf{G} = \mathbf{D} + \mathbf{E}$, where $\mathbf{D}$ is a matrix with entries $D_{i,j} = D_{i,i} = G_{i,i}$, and $\mathbf{E}$ is a diagonal matrix with entries $E_{i,i} = -\frac{R_i}{(\sum_{p=1}^N s_n^i)^2}$. Since $\mathbf{D}$ has identical columns (columns i and $M+i$ are identical), it is negative semi-definite. As a result, $\mathbf{G}(\mathbf{s}, \omega)$ is the sum of a negative semi-definite matrix and a negative definite matrix ($\mathbf{E}$). Thus, $\mathbf{G}(\mathbf{s}, \omega)$ is negative definite. Therefore, $[\mathbf{G}(\mathbf{s}, \omega) + \mathbf{G}^T(\mathbf{s}, \omega)]$ is negative definite, and the proof is completed. ■

With the existence and uniqueness guaranteed, the only question remained is how to find the equilibrium point. Interestingly, for the considered game model, we can prove the exact formula of the Nash equilibrium in Theorem 5.

THEOREM 5. *The point where every player's strategy satisfies* $s_n^m = B_n \frac{R_m}{\sum_{i=1}^M R_i}, \forall m \in \mathcal{M}, \forall n \in \mathcal{N}$ *is the unique Nash equilibrium of this game.*

Proof: We prove that at the point where every player's strategy satisfies $s_n^m = B_n \frac{R_m}{\sum_{i=1}^M R_i}, \forall m \in \mathcal{M}, \forall n \in \mathcal{N}$, every player's strategy maximizes its utility (i.e., $\frac{\partial U_n}{\partial s_n^m} = 0$). Thus, this is the Nash equilibrium of this game. Substitute $s_n^m = B_n \frac{R_m}{\sum_{i=1}^M R_i}$ into $\frac{\partial U_n}{\partial s_n^m}$, we have

$$\begin{aligned} \frac{\partial U_n}{\partial s_n^m} =& \frac{\sum_{j \in \mathcal{N}_{-n}} B_j \frac{R_m^2}{\sum_{i=1}^M R_i}}{\sum_{n=1}^N (B_n \frac{R_m}{\sum_{i=1}^M R_i})^2} - \frac{\sum_{j \in \mathcal{N}_{-n}} B_j \frac{R_M^2}{\sum_{i=1}^M R_i}}{\sum_{n=1}^N (B_n \frac{R_M}{\sum_{i=1}^M R_i})^2}, \\ =& \sum_{j \in \mathcal{N}_{-n}} B_j \left(\frac{\sum_{i=1}^M R_i}{\sum_{n=1}^N (B_n)^2} - \frac{\sum_{i=1}^M R_i}{\sum_{n=1}^N (B_n)^2} \right), \\ =& 0, \forall m \in \mathcal{M} \text{and } \forall n \in \mathcal{N}. \end{aligned} \tag{12}$$

The proof is now completed. ■

An important result from Theorem 5 is that at the equilibrium, the number of stakes a player invests in a chain only depends on its total budget and the ratios of block rewards between the chains, i.e., $\sum_{m=1}^M s_n^m = \sum_{n=1}^N B_n \frac{R_m}{\sum_{i=1}^M R_i}, \forall m \in \mathcal{M}$. This result can help the blockchain service providers to determine the stake distribution by setting their block rewards accordingly, which is vital to the system's security and performance.

IV. NUMERICAL RESULTS

In this Section, we simulate a system with 100 stakeholders (players) and 3 chains to evaluate stakeholder behaviors and their impacts on the system's security and performance. The block rewards $\mathbf{R} = [10, 30, 40]$ are adapted from several real-world PoS blockchain networks (Cardano, Algorand, and Tezos), whereas $\mathbf{B}$ are generated randomly with normal distribution in the ranges of $[10, 50]$. In particular, the simulation is divided into iterations. At each iteration, the strategy that maximizes player n's profit (while the strategies of all the other players are fixed) is computed. The obtained result is then fixed as the new strategy of player n, and the simulation continues to find the best strategy for player $n+1$ in the next iteration. The simulation is stopped when every player's strategy remains the same. During the simulation, we record the convergence of the player strategies to the Nash equilibrium and the final stake distribution. Then, based on the final stake distribution, we show the common prefix violation probability of each chain under different adversarial ratio. From the performance perspective, the common prefix violation probability can be expressed as the time required to confirm a block if the adversary decides to attack one of the three chains.

Fig. 3(a) illustrates the player strategies in this game. As observed from the figure, the player strategies converge and become stable after 100 iterations. At the stable state, the stake distribution is proportional to the block rewards ratio, i.e., the chain with a higher block reward has more stakes. Moreover, this shows that the simulation results match the analytical results we proved in Theorem 5.

Fig. 3(b) shows the common prefix violation probabilities with parameter $\kappa = 6$ when the adversary attacks with

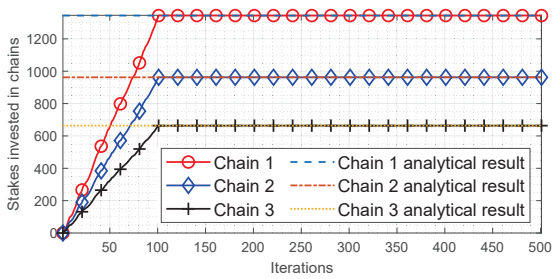
$B_A = [1, 500]$. At approximately $B_A = 320$ and $B_A = 470$, chain 3 and chain 2 can no longer satisfy the common prefix property with overwhelming probability (i.e., $\Pr_{\text{CP}} > 0.1\%$), respectively. This is because these two chains have fewer stakes than chain 1, and thus the adversarial ratios $(1 - \gamma)$ ratio are higher in these chains.

Fig. 3(c) illustrates the transaction confirmation time of 3 chains in case of adversarial attacks. To determine the transaction confirmation time, we calculate κ_c, and then we multiply κ_c with T_b to determine how long the stakeholders have to wait before a transaction is confirmed. The figure shows that the transaction confirmation time increases as the adversarial stake increases, and the chain with the highest number of stakes (chain 1) has the lowest transaction confirmation time.

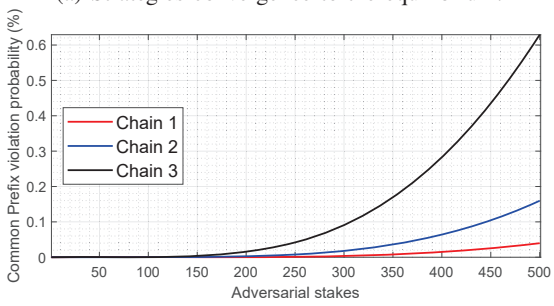
As observed from Fig. 3, the higher the block reward is, the more stakes a chain has, and the better the chain's security and performance can be. Thus, the block rewards have a significant impact on the system's operation and security. However, determining the block reward is not a simple task. On the one hand, the companies want to increase the block rewards to improve their chains' security and performance. On the other hand, the block reward is the cost that the companies have to pay, and thus it cannot be too high. Thus, the optimal setting of the block reward remains an open issue for future work.

V. Conclusion

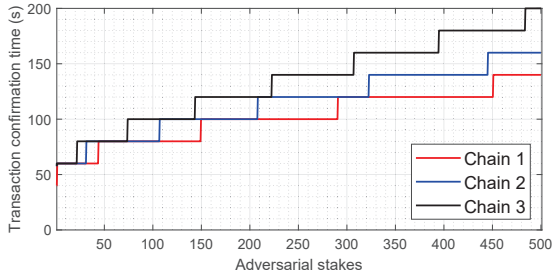
In this paper, we have proposed a novel blockchain-based system to effectively manage the coalition loyalty programs. The proposed blockchain system utilizes the advantages of Poof-of-Stake and sidechain technologies to allow the customers to freely exchange loyalty points from different existing loyalty programs. Moreover, new companies can join the coalition without the need for the complex and costly merging processes of different blockchain networks. We have also conducted security and performance analyses of the proposed system and showed that the user behaviors have a significant impact on the system security and performance. Through a non-cooperative game theory analysis, we have concluded that the user behaviors depend greatly on the block rewards. Finally, we have conducted numerical experiments to demonstrate that the block rewards dictate how the users behave and have a significant impact on system performance and security.



(a) Strategies convergence to the equilibrium.



(b) Common prefix violation probability.



(c) Transaction confirmation time.

Fig. 3: Simulation results.

References

[1] L. Steinhoff and R. W. Palmatier, "Understanding loyalty program effectiveness: managing target and bystander effects," *Journal of the Academy of Marketing Science*, vol. 44, no. 1, pp. 88–107, Aug. 2014.

[2] D. Kowalewski, J. McLaughlin, and A. J. Hill, "Blockchain Will Transform Customer Loyalty Programs," *Harvard Business Review*, Jul 27, 2017. [Online]. Available: https://hbr.org/2017/03/blockchain-will-transform-customer-loyalty-programs. [Accessed: 29-Mar-2020].

[3] E. Breugelmans et al., "Advancing research on loyalty programs: a future research agenda," *Marketing Letters*, vol. 26, no. 2, pp. 127-139, June 2015.

[4] Kayden, "Introducing Krispay: Mobile miles for everyday spend," *Got the Xtra Miles*. [Online]. Available: https://gothextramiles.com/2019/03/22/krispay-introducing-a-new-way-to-earn-miles/. [Accessed: 15-Apr-2020].

[5] N. Morris, "Amex is reinventing rewards using blockchain," *Ledger Insight*, 2019. [Online]. Available: https://www.ledgerinsights.com/amex-blockchain-rewards-american-express/. [Accessed: 15-Apr-2020].

[6] A. Back, (Oct. 2014). "Enabling blockchain innovations with pegged sidechains". [Online]. Available: http://kevinriggen.com/files/sidechains.pdf

[7] S. Nakamoto, (May 2008). "Bitcoin: A peer-to-peer electronic cash system". [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in *CRYPTO 2017*, Santa Barbara, USA, Aug. 20-24, 2017, pp. 357-388.

[9] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in *IEEE Access*, vol. 7, pp. 85727-85745, June 2019.

[10] M. Mitzenmacher and E. Upfal, *Probability and computing: Randomization and probabilistic techniques in algorithms and data analysis*. Cambridge: Cambridge university press, 2017.

[11] J. Garay, A. Kiayias and N. Leonardos "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Sofia, Bulgaria, April 26-30, 2015, pp. 281-310.

[12] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. of the 26th Symposium on Operating Systems Principles*, Oct. 2017, pp. 51-68.

[13] L. Luu, D. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. of the ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, Oct. 2016, pp. 254-269.

[14] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, UK: Cambridge University Press, 2012.

[15] J. B. Rosen, "Existence and Uniqueness of Equilibrium Points for Concave N-Person Games," *Econometrica*, vol. 33, no. 3, pp. 520-534, July 1965.