Blockchain and Stackelberg Game Model for Roaming Fraud Prevention and Profit Maximization

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

***Abstract*—Roaming fraud is one of the most significant financial losses for mobile service providers. The inefficiency of current exchanging data management methods among mobile service providers is the main obstacle for roaming fraud prevention. In this paper, we introduce a novel blockchain-based data exchange management system to address roaming fraud problems in mobile networks. This system provides a secure and automatic data exchange service among mobile service providers and mobile subscribers. In addition, we introduce an emerging Proof-of-Stake (PoS) consensus mechanism for the proposed blockchain-based roaming fraud prevention system, which can significantly reduce the delay in exchanging information as well as implementation costs for mobile service providers. To further enhance benefits and security efficiency for the proposed blockchain system, we develop an economic model based on Stackelberg game. This game model is very effective in maximizing profits for both the stakeholders and stake pool and useful in designing a robust blockchain-based mobile roaming management system. Through performance analysis and numerical results, we show that our proposed framework not only provides an effective solution to prevent mobile roaming fraud but also opens many business opportunities for future mobile networks.**

Keywords- Blockchain, Proof-of-Stake, mobile roaming fraud, and Stackelberg game.

I. Introduction

Despite the continuous revenue growth, mobile service providers (MSPs) have been facing several obstacles, especially fraud attacks which cause over $32.7 billion annual loss[1]. Among many types of fraud attacks, roaming fraud is the most harmful type which can cause significant losses up to €40,000 per hour in some incidents[2]. Roaming fraudsters often exploit the current inefficient data exchange management method between two MSPs for free-riding roaming service usage. In particular, when a subscriber gains access to the services of the Home Public Mobile Network (HPMN) via the Visited Public Mobile Network (VPMN), the HPMN may not be able to charge the subscriber properly due to the long delay in exchanging data between the two networks. However, the HPMN still has to pay the VPMN for using the VPMN's roaming facilities [1].

Currently, the roaming fraud protection system employs several countermeasures, such as frequently validating subscriber's information and limiting service usage, which cause several negative impacts on the quality of service and customer satisfaction [1]. Besides these preventive measures, the roaming fraud protection system also collects and examines roaming data, e.g., call records, to detect and respond if fraud attacks occur. In the current fraud protection system, data collection is the weakest step due to the significant delay in data exchange between MSPs [1]. Generally, methods such as Fraud Information Gathering System [2] and Near Real Time Roaming Data Exchange (NRTRDE) [3] can be employed to speed up the data exchanging process. However, the first method can only support data exchange in a near real-time manner for a limited number of subscribers, meanwhile the data exchange delay of NRTRDE is high, i.e., more than 4 hours [3]. In practice, it is reported that a fraudulent SIM can use up to 18 hours of service on average before being detected[2]. Consequently, the significant delay in data exchange remains a big challenge to the current roaming fraud protection system.

Recently, blockchain technology has emerged to be a secured and effective solution for data management in many decentralized networks thanks to its advantages of transparency, decentralization, and immutability. Organizations including Deutsche Telekom and SK Telecom[3], IBM[4], and Enterprise Ethereum Alliance[5] have announced their blockchain-based solutions for roaming, focusing on identity management, automating billing processes, and fraud prevention. However, these solutions are still under development and facing some challenges. Specifically, most current blockchain-based data management systems are employing the Proof-of-Work (PoW) mechanism [4] which relies on a computational power competition between the participants to reach the consensus. Consequently, the PoW mechanism requires a huge energy consumption, e.g., the Bitcoin network consumes more energy than that of some countries[6], and has a significant delay, i.e., one hour on average [5]. To overcome these limitations, a new consensus mechanism, namely Proof-of-Stake (PoS) [5], [6], [7], has been developed recently, in which the consensus can be achieved only by proving stake ownership. As a result, the PoS mechanism has many advantages, including negligible energy

[1] https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/9436-report-us-32-7-billion-lost-in-telecom-fraud-annually

[2] https://www.prnewswire.com/news-releases/starhome-mach-operators-roaming-fraud-losses-can-reach-40000-per-hour-598836021.html

[3] https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-and-sk-telecom-pave-the-way-for-the-future-564180

[4] https://www.ibm.com/thought-leadership/institute-business-value/report/blockchaintelco

[5] https://cointelegraph.com/news/enterprise-ethereum-alliance-publishes-on-blockchain-uses-in-telecoms

[6] https://digiconomist.net/bitcoin-energy-consumption

978-1-7281-3106-1/20/$31.00 ©2020 IEEE

consumption and especially very low consensus delay, over the PoW mechanism [5]. With these advantages, PoS-based blockchain is expected to be a very effective solution to deal with roaming fraud for future mobile networks.

In this paper, we develop a novel PoS-based blockchain framework for mobile roaming service management. Among the PoS consensus mechanisms introduced recently, we adopt the Ouroboros consensus mechanism [6] which has several significant advantages, including low delay (2 minutes on average[7]) and the ability to mitigate various types of attacks [5]. In a PoS-based blockchain network, user participation is crucial to maintain the network's operations and security. Therefore, we propose an economic model based on Stackelberg game to incentivize user participation by jointly maximizing the users' profits. Through performance analysis and numerical results, we then show that our proposed blockchain-based roaming framework can not only prevent mobile roaming fraud but also open new business opportunities for future mobile networks.

II. Blockchain-based Roaming System

A. Current Roaming System

The current roaming management system is illustrated in Fig. 1(a) [1]. In particular, firstly, a roaming pact is established between two MSPs. Then, when a subscriber wants to use the service of the HPMN while being in the VPMN, the subscriber sends a request to the VPMN. The VPMN then queries the HPMN about the subscriber's information and subscribed services. After receiving confirmation from the HPMN about the subscription, the VPMN grants the subscriber access to the corresponding services through roaming facilities. The Call Detail Records (CDRs), consisting of the call duration, source and destination of the services, are then sent to a Data Clearing House (DCH). This DCH operates as a middleman to validate and transmit the CDRs to the HPMN. Once the HPMN receives the CDRs, it will pay the VPMN in accordance with the roaming pact [1].

B. Proposed Roaming System

Our proposed roaming system provides a platform for roaming management which not only supports and automates complex interactions among the MSPs and subscribers, but it also provides a universal currency, i.e., blockchain network tokens, for payments. As illustrated in Fig. 1(b), the main procedure of the roaming management platform consists of seven steps as follows:

- *Step 1:* Two MSPs negotiate a roaming pact containing tariff plans for roaming services and payment agreements between the two MSPs. The roaming pact is then stored in the blockchain as a smart contract, i.e., a user-defined program which is automatically enforced when the conditions stated in the smart contract are met [8].
- *Step 2:* When a subscriber wants to use the services at a VPMN, the subscriber queries the VPMN to receive the information about available services and tariff plans.
- *Step 3:* If the subscriber decides to use the service, the subscriber sends a transaction containing a sufficient amount of digital tokens as defined by the tariff plans to the smart contract's address.
- *Step 4:* The VPMN will grant the subscriber access to roaming facilities once the transaction in step 3 is successfully sent to the smart contract.
- *Step 5:* When the subscriber finishes using roaming services, the VPMN sends a transaction containing CDR data of the services provided to the smart contract's address.
- *Step 6:* The smart contract then automatically calculates and sends the subscriber's invoice to the HPMN. A transaction from the HPMN to the VPMN is also triggered by the smart contract for the payment of roaming services.
- *Step 7:* The smart contract sends the remaining tokens to the subscriber.

C. Security Analysis of the Proposed Roaming System

By adopting the Ouroboros consensus mechanism, our proposed roaming management system can achieve a very small delay in exchanging data compared to that of the current roaming systems. In particular, it takes approximately 20 seconds to add a block to the chain and 3 minutes to confirm a transaction[8]. As a result, fraud attacks can be detected approximately 4 hours earlier compared to that of the traditional roaming fraud protection system. Moreover, the Ouroboros consensus mechanism is proven to be secured against several types of attacks such as double-spending and grinding attacks [6].

Nevertheless, there is one type of attack, namely 51% attack [6], that can break most of blockchain networks, including both the PoW-based and PoS-based blockchain networks. Specifically, if an adversary can control more than 51% of total computational power in a PoW-based network or 51% of total stakes in a PoS-based network, the adversary can control all transactions in the network, such as block new transactions from taking place or being confirmed. Therefore, it is crucial to attract more participants to the PoS-based blockchain system in order to increase the network's total stakes and protect the system from an adversary in controlling the majority of network stakes. In the next section, we will introduce an effective economic model which can jointly maximize profits for the participants, thereby encouraging them to participate in the network and thus improving network security.

D. Stake Pools and Stakeholders

In the proposed system, the MSPs and subscribers also can take part in the consensus mechanism and earn additional profits for their participation. Specifically, in the PoS-based blockchain network, a user is selected in advance to create a block, and a reward, e.g., a number of digital tokens, is paid to that user for the participation. The probability P_i that user (stakeholder) i with stake S_i is selected to create a block and obtain the reward in a network of N users is:

$$P_i = \frac{S_i}{\sum_{n=1}^{N} S_n}. \tag{1}$$

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

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

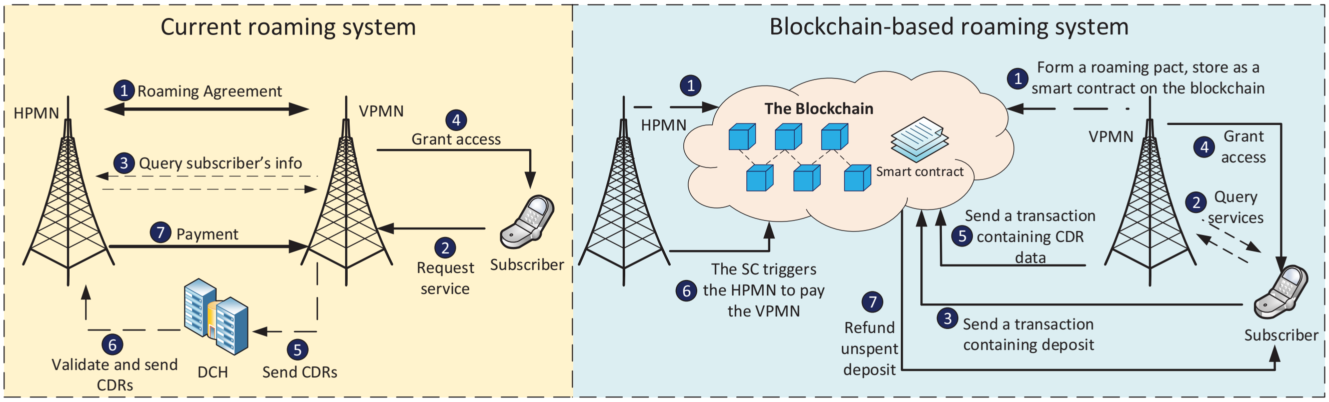

Current roaming system
1 Roaming Agreement
HPMN
VPMN
4 Grant access
3 Query subscriber's info
7 Payment
2 Request service
Subscriber
6 Validate and send CDRs
DCH
5 Send CDRs
Blockchain-based roaming system
1
HPMN
The Blockchain
Smart contract
1 Form a roaming pact, store as a smart contract on the blockchain
VPMN
4 Grant access
2 Query services
Send a transaction 5 containing CDR data
The SC triggers 6 the HPMN to pay the VPMN
7 Refund unspent deposit
3 Send a transaction containing deposit
Subscriber

Fig. 1: Illustrations of (a) current roaming system and (b) proposed blockchain-based roaming system.

In (1), a stakeholder with a small S_i is less likely to be selected. Moreover, consensus participation requires a constant connection to the network, which incurs an operational cost, e.g., \$40 to \$300 per month[9]. Consequently, stakeholders often pool their stakes together to increase their opportunities to be selected and share operational costs, which results in the formation of stake pool [5]. This stake pool formation can be utilized to attract more users to the network as it can provide additional profits for the stakeholders, e.g., the subscribers, and the stake pool (formed by MSPs).

III. Stackelberg Game Formulation

We consider a PoS-based blockchain network with one stake pool and a set $\mathcal{N}$ of N stakeholders. The stakeholders have stake budgets $\mathbf{B} = (B_1, \dots, B_N)$ and individual operational costs $\mathbf{C} = (C_1, \dots, C_N)$. The stake pool has its own stake σ (i.e., the stakes that the pool's owner invest to the pool) and a fee α which is the profit margin of the pool's owner, e.g., Stakecube, a real-world stake pool, charges 3% of each stakeholder's reward[10]. A stakeholder i can use its budgets to invest p_i stakes to the pool and m_i stakes to individually participate in the consensus process, such that $p_i + m_i \leq B_i$. The probability P^w that the pool is selected to be the leader and obtain a block reward R is

$$P^w = \frac{\sigma + \sum_{n\in\mathcal{N}_p} p_n}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j}, \tag{2}$$

where $\mathcal{N}_p$ is the set of stakeholders who invest stakes to the pool. After receiving the reward R, the pool calculates each stakeholder's reward r_i^p based on the proportion P_i^p of stakeholder i's stakes in the total stakes of the pool, which is

$$P_i^p = \frac{p_i}{\sigma + \sum_{n\in\mathcal{N}_p} p_n}. \tag{3}$$

The pool then charges a fee of α percentage from each stakeholder's reward before the reward is finally delivered to each stakeholder. Thus, when a stakeholder i invests p_i stakes to the pool, the stakeholder's expected reward r_i^p is given by:

$$\begin{aligned} r_i^p &= P^w P_i^p (1-\alpha)R, \\ &= \frac{p_i}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j}(1-\alpha)R. \end{aligned} \tag{4}$$

When the stakeholder uses m_i stakes for individual participation (i.e., self-mining), its expected reward is

$$r_i^m = \frac{m_i}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j} R - C_i, \tag{5}$$

where $\dfrac{m_i}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j}$ represents the proportion of stakeholder i's stakes in the total stakes of the blockchain network. The total profit of the pool consists of the profit from its own stakes, which is

$$M_p = \frac{\sigma}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j} R, \tag{6}$$

and the fees it charges the stakeholders, which is

$$U_p = \sum_{i\in\mathcal{N}_p} \left(\frac{p_i \alpha}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^{N} m_j} R \right). \tag{7}$$

In practice, a stake pool usually announces its fee first, e.g., the Stakecube pool's fee is always declared on its website[10]. Based on that information, the stakeholders will decide how much to invest to the pool. Therefore, the interaction between the stake pool and the stakeholders can be formulated as a single-leader multi-followers Stackelberg game [9], which consists of one leader (the pool) who declares its fee, i.e., $s_p = \alpha$ first, and then the stakeholders, i.e., followers, will decide how much to invest to the pool and/or for self-mining, i.e., $s_i(p_i, m_i)$. Let $\mathcal{S}_i$ denote the set of all possible strategies of follower i, the best response s_i^* of follower i is the strategy set which gives the follower the best payoff given a fixed strategy s_p of the leader, i.e.,

$$U_i(s_i^*, s_p) \geq U_i(s_i', s_p), \forall s_i' \in \mathcal{S}_i. \tag{8}$$

[9] https://forum.cardano.org/t/how-many-stake-pools/16132/12
[10] https://cryptoshib.com/stakecube/

Based on the follower's best response, the Stackelberg strategy for the leader is a strategy s_p^* such that

$$s_p^* = \underset{s_p}{\operatorname{argmax}} U_p(s_p, s_i^*). \tag{9}$$

The Stackelberg solution then can be defined by a tuple (s_p^*, s_i^*), and its corresponding utility tuple (U_p^*, U_i^*) is the Stackelberg equilibrium of the game. The game can be divided into two stages. At the first stage, the leader announces its strategy. Then, at the second stage, the followers determine their strategies in response to the leader's strategy. Using backward-induction-based analysis, the Stackelberg equilibrium of this game is determined in the following.

A. Follower Strategy

In this game, a follower's possible strategies can be divided into four cases:

- *Case 1:* Only invest stakes to the pool.
- *Case 2:* Only invest stakes for self-mining.
- *Case 3:* Simultaneously invest stakes to the pool and for self-mining.
- *Case 4:* Do not invest stakes to the PoS-based blockchain network.

Although a stakeholder can use any amount within its budget to invest, we prove in the following theorem that a rational follower will always invest all its budget to the network.

THEOREM 1. *Let s_i' denote a strategy where follower i uses less than its total budget, i.e., $m_i' + p_i' < B_i$, with corresponding utility U_i', and s_i is a strategy where follower i uses all its budget, i.e., $m_i + p_i = B_i$, with corresponding utility U_i. For every $s_i', s_i \in \mathcal{S}_i$, we always have $U_i' < U_i$.*

Proof: We consider the Cases 1, 2, 3, and 4 as follows.

- *Case 1:* When follower i invests p_i' to the pool, $U_i'^1$ is equal to r_i^p in (4). Now, if the follower invests all the budget to the pool, its payoff is given by

$$U_i^1 = \frac{B_i}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}(1-\alpha)R. \tag{10}$$

Then, the difference in payoff between the two strategies is

$$U_i^1 - U_i'^1 = \frac{B_i - p_i'}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}(1-\alpha)R. \tag{11}$$

Since $p_i' < B_i$, $U_i^1 - U_i'^1 > 0, \forall i \in \mathcal{N}$.

- *Case 2:* When follower i uses m_i' for self-mining, $U_i'^2$ is equal to r_i^m in (5). If the follower self-mines with all its budget, its expected payoff is given by

$$U_i^2 = \frac{B_i R}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j} - C_i. \tag{12}$$

The difference in payoff between the two strategies is

$$U_i^2 - U_i'^2 = \frac{B_i - m_i'}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}R. \tag{13}$$

Since $m_i' < B_i$, $U_i^2 - U_i'^2 > 0, \forall i \in \mathcal{N}$.

- *Case 3:* When follower i simultaneously invests stakes to the pool and self-mines using less than its total budget, the expected payoff is

$$U_i'^3 = \frac{m_i' + p_i'(1-\alpha)}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}R - C_i. \tag{14}$$

If the follower uses all the budget invest to the pool and for self-mining, its expected payoff is

$$U_i^3 = \frac{m_i + p_i(1-\alpha)}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}R - C_i. \tag{15}$$

The difference in payoff is

$$U_i^3 - U_i'^3 = \frac{(p_i + m_i) - (p_i' + m_i') + (p_i' - p_i)\alpha}{\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j}R. \tag{16}$$

In (16), $(p_i + m_i) - (p_i' + m_i') = B_i - (p_i' + m_i')$ is always positive. Thus, if $p_i' < p_i$, $U_i^3 - U_i'^3$ is always positive.

- *Case 4:* In this case, follower i gets a payoff of $U_i^4 = 0$, which is less than the payoff of Cases 1, 2, and 3. Moreover, if the follower does not invest any stake to the blockchain network, the follower does not have any impact on the game.

To sum up, in all cases, the follower always gets a greater payoff by investing all its budget, regardless of the leader's strategy and other followers' strategies. ■

From Theorem 1, since a follower will always invests all its budget, the total network stakes becomes a constant, i.e.,

$$\sigma + \sum_{n\in\mathcal{N}_p} p_n + \sum_{j=1}^N m_j = \sigma + \sum_{i=1}^N B_i. \tag{17}$$

Then, we can determine the best response of each follower as proven in Theorem 2.

THEOREM 2. *A follower's best response is to use all its budget either to invest stakes to the pool or for self-mining.*

Proof: The expected payoffs of follower i in Cases 1, 2, and 3 are given by (10), (12), (15), respectively. The difference in payoff between Case 2 and Case 3 can be calculated by

$$U_i^2 - U_i^3 = \frac{p_i \alpha R}{\sigma + \sum_{n=1}^N B_n}, \tag{18}$$

which is always positive. Therefore, Case 3 can be removed from $\mathcal{S}_i$. Then, to maximize the profit, the follower can choose Case 1 or Case 2. The difference in payoff is

$$U_i^2 - U_i^1 = \frac{B_i \alpha R}{\sigma + \sum_{n=1}^N B_n} - C_i. \tag{19}$$

As observed from (19), if $C_i < \frac{B_i \alpha R}{\sigma + \sum_{n=1}^N B_n}$, the difference is positive, which means that Case 2 yields more profits than Case 1, and vice versa. Therefore, follower i's best response is to consider its investment threshold T_i which is given by

$$T_i = \frac{C_i(\sigma + \sum_{n=1}^N B_n)}{B_i R}. \tag{20}$$

In other words, if $\alpha \leq T_i$, follower i will invest all stakes to the pool, otherwise it spends all stakes for self-mining. ■

Since from Theorem 1 we have $p_i^* = B_i - m_i^*$, we can represent the best response of follower i by p_i^*. From Theorem 2, the best response p_i^* can be expressed as follows:

$$p_i^*(\alpha) = \begin{cases} 0 & \text{if } \alpha > T_i, \\ B_i & \text{if } \alpha \leq T_i. \end{cases} \tag{21}$$

B. Leader Strategy

Based on the best responses of the followers, the Stackelberg strategy s_p^* of the leader can be determined by Theorem 3.

Theorem 3. *The optimal fee α^* is equal to one of the investment thresholds of the followers, i.e., $\alpha^* = T_k, k \in \mathcal{N}$.*

Proof: The pool's optimal fee α^* is the fee that maximizes its utility, i.e.,

$$\alpha^* = \underset{\alpha}{\operatorname{argmax}}(M_p + U_p). \tag{22}$$

As the total network stakes is a constant, M_p becomes constant, and thus it does not need to be optimized. Thus, we only need to consider the following utility function of the leader

$$U_p = \sum_{i \in \mathcal{N}_p} \left(\frac{B_i \alpha}{\sigma + \sum_{n=1}^{N} B_n} R \right), \tag{23}$$

which depends on the participants in $\mathcal{N}_p$. Without loss of generality, we arrange the followers in the following order $\frac{C_i}{B_i} \leq \frac{C_{i+1}}{B_{i+1}}, \forall i \in \mathcal{N}$. As $\mathcal{N}_p$ depends on α, i.e., the followers choose to invest all stakes to the pool or for self-mining based on α as shown in (21), U_p can be represented as follows:

$$U_p = \begin{cases} \sum_{i=1}^{N} \left(\frac{B_i \alpha}{\sigma + \sum_{n=1}^{N} B_n} R \right) & \text{if } \alpha \leq T_N, \\ \sum_{i=1}^{N-1} \left(\frac{B_i \alpha}{\sigma + \sum_{n=1}^{N} B_n} R \right) & \text{if } T_N < \alpha \leq T_{N-1}, \\ \dots, & \\ \frac{B_1 \alpha}{\sigma + \sum_{n=1}^{N} B_n} R & \text{if } T_2 < \alpha \leq T_1, \\ 0 & \text{if } \alpha > T_1. \end{cases} \tag{24}$$

In (24), U_p is a piecewise function where each sub-function is defined over an interval of α bounded by T_i (an example of U_p is shown in Fig. 2(c)). Moreover, since each sub-function is a strictly increasing function of α, the unique maximum of each sub-function is attained at the upper-boundary of the interval, i.e., at $\alpha = T_i$. Thus, the α^* is equal to the upper-boundary of a certain sub-function of U_p, i.e., $\alpha^* = T_k, k \in \mathcal{N}$ such that

$$\sum_{i=1}^{k} \left(\frac{B_i T_k R}{\sigma + \sum_{n=1}^{N} B_n} \right) \geq \sum_{i=1}^{l} \left(\frac{B_i T_l R}{\sigma + \sum_{n=1}^{N} B_n} \right), \forall l \in \mathcal{N}. \tag{25}$$

■

Since (25) only contains constants, the leader's Stackelberg strategy can be straightforwardly determined. Assume that $\alpha^* = T_k$ is a Stackelberg strategy of the leader, the Stackelberg utility of the leader can be determined as follows

$$U_p^* = \sum_{i=1}^{k} \left(\frac{B_i T_k}{\sigma + \sum_{n=1}^{N} B_n} R \right). \tag{26}$$

C. Existence and Uniqueness of the Stackelberg Equilibrium

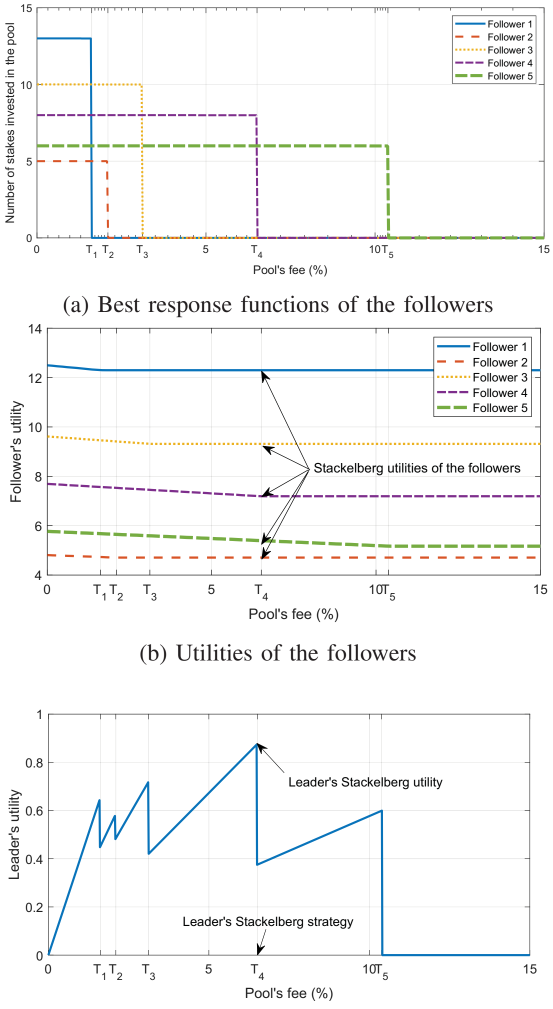
Since there is a unique maximum of each sub-function of U_p, there exists at least one global maximum of U_p. As a result, there exists at least one Stackelberg utility of the leader. Moreover, as can be seen from (8), there is a uniquely defined response of each follower i for every fixed value of α. Therefore, there exists at least one Stackelberg equilibrium of this game. Although the existence of a Stackelberg equilibrium is proven, its uniqueness cannot be guaranteed, because there may exist two or more sub-functions of U_p with equal the highest local maximum. Suppose that there is a Stackelberg equilibrium at $\alpha^* = T_k$, if there exists one $j \in \mathcal{N}$ such that

$$\sum_{i=1}^{k} \left(\frac{B_i T_k}{\sigma + \sum_{n=1}^{N} B_n} R \right) = \sum_{i=1}^{j} \left(\frac{B_i T_j}{\sigma + \sum_{n=1}^{N} B_n} R \right), \tag{27}$$

then $\alpha = T_j$ constitutes another Stackelberg strategy of the leader. If there is no such j, the game admits a unique Stackelberg equilibrium. In case j exists, although both $\alpha = T_k$ and $\alpha = T_j$ yield the same utility, they result in different numbers of followers who invest stakes to the pool. In this case, we propose to choose the equilibrium with the lowest α to attract more stakeholders to the pool. Thus, this solution can guarantee the uniqueness of the Stackelberg equilibrium.

IV. Numerical Results

To evaluate our proposed economic model, we first consider a small game, i.e., $\mathcal{G}_1$, consisting of one leader and five followers with parameters $\mathbf{C} = (0.3, 0.2, 0.1, 0.5, 0.6)$, $\mathbf{B} = (13, 5, 10, 8, 6)$, $R = 50$, and $\sigma = 10$. As can be seen from Fig. 2(a), if α is lower than the investment threshold T_i of follower i, the follower's best response is to invest all its budget to the pool, i.e, $p_i^* = B_i$. When α increases beyond T_i, the follower stops investing stakes to the pool and switches to self-mining. As illustrated in Fig. 2(b), the utility of follower i decreases as α increases, and it becomes constant when $\alpha > T_i$. Fig. 2(c) shows the pool's profit U_p in $\mathcal{G}_1$. As α increases, U_p increases linearly. However, when α becomes greater than T_1, the U_p drops. The reason is that at this point, follower 1 stops investing stakes to the pool, and thus the pool cannot earn any profit from follower 1. Nevertheless, as α continues to increase, U_p increases again since the fees the pool charges the remaining followers increase with α. Similarly, as α continues to increase beyond the investment thresholds T_2 and T_3, followers 2 and 3 stop investing stakes to the pool, and U_p changes accordingly. At $\alpha^* = T_4$, the leader obtains its global maximum U_p^*, i.e., there is a unique Stackelberg equilibrium with the leader's utility $U_p^* = 0.87$ and the leader's strategy $\alpha^* = T_4 = 6.51\%$ in this game. When α is higher than T_4, U_p first drops and then increases, but it is always lower than U_p^*. Finally, when $\alpha > T_5$, all



(a) Best response functions of the followers

(b) Utilities of the followers

(c) Leader's utility

Fig. 2: Results of $\mathcal{G}_1$.

followers choose to self-mine and $U_p = 0$. It is worth noting that at the equilibrium, only followers 4 and 5 invest stakes to the pool. If the pool tries to incentivize all followers to invest, it can only achieve a utility of $U_p = 0.57$ at $\alpha = T_1$.

We then consider a more practical scenario, namely $\mathcal{G}_2$, with 1000 followers under some parameters generated based on Cardano (https://stakingrewards.com/asset/ada), a real-world PoS-based blockchain network. In particular, we generate the game with $R = 1000$ and $\sigma = 10$, whereas $\mathbf{B}$ and $\mathbf{C}$ are generated randomly with normal distribution in the ranges of $[1, 1000]$ and $[0.1, 0.2]$, respectively. There is a unique Stackelberg equilibrium in $\mathcal{G}_2$, with $\alpha^* = 8.1\%$ and $U_p^* = 56.14$. Moreover, there are 859 followers investing approximately 69.5% of total network stakes to the pool at the equilibrium. We also analyze the pool's profit from each follower in Fig, 3. Generally, the pool's profit from a follower is proportional to that follower's budget and operational cost. However, if a follower's budget is very high, the follower will not invest stakes to the pool, e.g., followers with budgets greater than 600 do not invest stakes to the pool in $\mathcal{G}_2$. The reason is that, the threshold T_i is inversely proportional to the budget B_i.

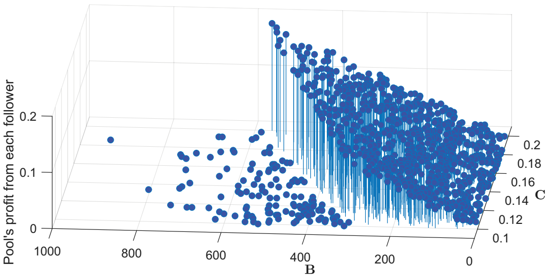


Fig. 3: The leader's profit from each follower.

Therefore, a follower with a high B_i has a low T_i, and thus the follower is more inclined to self-mine.

V. Conclusion

In this paper, we have proposed a blockchain-based system to address the roaming fraud problems for future mobile networks. We have also developed an economic model based on Stackelberg game to further enhance the benefits for the users, thereby encouraging more users to participate in the blockchain system. Then, we have analyzed and determined the best strategies for the stakeholders and the stake pool to jointly maximize their profits. In addition, we have proven the existence and discussed the uniqueness of the Stackelberg equilibrium in our model. Additionally, numerical experiments have been conducted to evaluate the system performance under different networking settings. The results show that our model can help to attract more investments and increase the profits of our proposed system.

Acknowledgement

This work was supported in part by the Joint Technology and Innovation Research Centre—a partnership between the University of Technology Sydney and the VNU Ho Chi Minh City University of Technology (VNU HCMUT).

References

[1] G. Macia-Fernandez, P. Garcia-Teodoro and J. Diaz-Verdejo, "Fraud in roaming scenarios: an overview," in *IEEE Wireless Communications*, vol. 16, no. 6, pp. 88-94, Dec. 2009.

[2] "3GPP TS 22.031 V15.0.0," *Technical Specification 22.031*, Jun. 2018.

[3] "GSMA Speeds Up The Transfer Of Roaming Call Records," *GSMA Newsroom*. [Online]. Available: https://www.gsma.com/newsroom/press-release/gsma-speeds-up-the-transfer-of-roaming-call-records/. [Last accessed: 25-Oct-2019].

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

[5] 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, Jun. 2019.

[6] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in *Annual International Cryptology Conference*, Santa Barbara, USA, Aug. 2017, pp. 357-388.

[7] 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.

[8] 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.

[9] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.