Cyber Risk Management with Risk Aware Cyber-insurance in Blockchain Networks

Shaohan Feng*, Zehui Xiong*, Dusit Niyato*, Ping Wang*, Shaun Shuxun Wang†, and Yang Zhang‡
*School of Computer Engineering, Nanyang Technological University (NTU), Singapore
†Nanyang Business School, Nanyang Technological University (NTU), Singapore
‡School of Computer Science and Technology, Wuhan University of Technology, China

***Abstract*—Benefit from the capabilities of providing decentralized tamper-proof ledgers and platforms for data-driven autonomous organization, open-access blockchains based on proof-of-work protocols have gained tremendous popularity. Yet, the proof-of-work based consensus protocols under threats, e.g., double-spending. In this paper, by adopting the cyber-insurance as an economic tool to neutralize cyber risks, we propose a novel approach of cyber risk management for blockchain-based service. The blockchain service market under our consideration is composed of four entities, i.e., the infrastructure provider, blockchain provider, cyber-insurer, and users. The blockchain provider purchases the computing resources, e.g., a cloud, from the infrastructure provider to maintain the blockchain consensus and then offers blockchain services to the users. The blockchain provider optimize its profit by strategizing its investment in the infrastructure in order to improve the security of the blockchain and the service price charged to the users. In the meantime, to prevent the potential damage incurred by the attacks and then fully secure the cyber-space, the blockchain provider purchases a cyber-insurance from the cyber-insurer. In return, the cyber-insurer adjusts the insurance premium according to the perceived risk level of the blockchain service and will pay the claim to the blockchain provider once attacks happen. Based on the rationality of the market entities, we model the interaction among the blockchain provider, users, and cyber-insurer as a two-stage Stackelberg game. Specifically, the blockchain provider and cyber-insurer lead to set their pricing/investment strategies in the upper level subgame, and then the users follow to determine their demand of the blockchain service in the lower level subgame. Specifically, we consider the scenario of double-spending attacks and provide a series of analytical results about the Stackelberg equilibrium in the market game.**

***Index Terms*—Blockchain service, double-spending attack, cyber-insurance, game theory.**

I. Introduction

In the recent years, thanks to the capability of being able to distributively provide the irreversible, tamper-evident database of tokenized asset transactions, blockchain technologies have attracted tremendous attention from both industry and academia [1]. Relying on the condition of honest majority to guarantee the data integrity and service security, especially when the Nakamoto consensus protocol based on proof-of-work (PoW) is adopted [1], open-access/permissionless blockchains include the advantages such as open access, disintermediation, and pure self-organization. However, permissionless blockchain networks can be vulnerable to a series of insider attacks by malicious consensus nodes due to the fact that they admit no identity control [2]. As the most fundamental one of different types of attacks targeting permissionless blockchain networks [3], double spending can be executed through various attacks, e.g., goldfinger attacks [2]. Briefly, a double-spending attacker attempts to simultaneously spend the same set of blockchain tokens in two different transactions. This can be executed sequentially by two steps: 1) persuading part of the network and the transaction receiver to confirm one transaction, and 2) persuading the majority of the network to override that transaction with a conflicting transaction spending the same set of tokens. Worsely, due to the factors such as randomness in solving the PoW puzzles [1] and information propagation delay, the malicious nodes, i.e., attackers, only need to hold a certain level of PoW computing power to succeed with a high probability in the double-spending attacks. Note here that the double-spending attack is applicable to other blockchain-based resource trading services and systems, e.g., energy trading, even though it is initially devised for Bitcoin [4].

Due to the inherent characteristics of openness, the approach in [5] can not completely secure the PoW-based permissionless blockchain networks, which critically hinders the broader adoption of permissionless blockchains, especially in business services requiring high-level service security. Although the studies on the improvement of blockchain protocols have never stopped, perfectly secured blockchain networks are still impossible, and finding an alternative mean of cyber-risk management is therefore necessary. Recently, cyber-insurance has been recognized as a promising approach to efficiently manage the cyber risks by transferring them to insurers [6]. Similar to the traditional insurance, the customer of a cyber-insurance product, i.e., a policyholder, is insured once it settles the contract with the insurer by paying a premium. If attacks happen and the damage is within the coverage of the insurance policy, the insurer will pay the claim to the customer accordingly.

In this paper, we introduce a novel approach of jointly providing the risk management and security enhancement to the blockchain users and providers against attacks through the means of the cyber-insurance. As shown in Fig. 1, We consider

This work was supported in part by WASP/NTU M4082187 (4080), Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, NRF2015-NRF-ISF001-2277, EMA Energy Resilience under Grant NRF2017EWT-EP003-041, and National Natural Science Foundation of China (No. 61601336).

978-1-5386-4727-1/18/$31.00 ©2018 IEEE

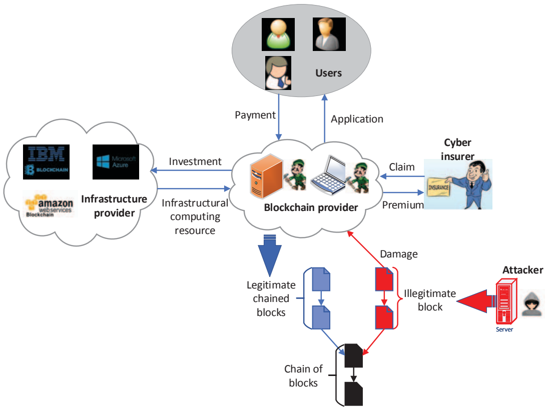

Figure 1: An overview of the blockchain service market.

a PoW-based blockchain service market composed of three entities, i.e., the users, blockchain provider, and cyber-insurer, under the threat of double-spending attacks. The blockchain provider purchases the computing resource from cloud-based infrastructure providers for maintaining the network consensus and then offers the service, e.g., P2P energy trading for smart grids, implemented on top of the blockchain for the users' consideration. The blockchain provider makes profit by charging the users with the transaction processing fees and block mining fees [1]. To neutralize the economic/financial loss incurred by double-spending attacks, the blockchain provider purchases the insurance from the cyber-insurer, which adopts an adjustable premium pricing strategy according to its perceived risk level of the blockchain. We propose a two-stage Stackelberg game model to analyze the dynamics of the considered market. On the upper stage of the game, the blockchain provider and the cyber-insurer lead to adopt their best-response strategies for profit maximization. On the lower stage, the users adjust their service demands according to the cost and the security level of the blockchain.

The rest of the paper is organized as follows. Section II describes the preliminaries about blockchains and cyber-insurance, the system model, and the formulation of Stackelberg game. Section III investigates the existence and uniqueness of the equilibrium in the proposed Stackelberg game. Section IV presents the numerical performance evaluation. Section V concludes the paper.

II. System Description and Game Formulation

In this section, we first introduce the model of successful attack probability for double spending and the concept of risk-adjusted premium. After formulating the utilities of the blockchain provider, users, and cyber-insurer, we investigate the problem of users' service demand, service pricing and infrastructure, i.e., computing power, investment by the blockchain provider and premium pricing by the cyber-insurer jointly as a hierarchical market game.

A. Preliminaries

1) Successful Attack Probability: We consider that the blockchain provider is responsible for maintaining a permissionless, PoW-based blockchain for service provision. Extending the analysis in [7] and [8], we assume that during a time period of T, the total computing resource of the blockchain network measured by the hash rate is fixed as H. Following the Nakamoto consensus protocol, every consensus node runs an independent Poisson process for puzzle-solving. The average time for a new block to be mined in the blockchain network is T_0 [1]. Then, in the time period of T, the expected number of blocks being successfully mined in the network is $\frac{T}{T_0}$. Let h denote the investment in computing resources by the blockchain provider, i.e., the honest nodes, and a denote the investment in computing resources by the attackers. Then, if the computing efficiency for hash queries are roughly the same, the blockchain provider and the attackers divide the total computing resource H as $\bar{h}H$ and $\bar{a}H$, respectively, where $\bar{h}=\frac{h}{a+h}$ and $\bar{a}=\frac{a}{a+h}$ are the investment ratios. According to the probabilistic model for winning the PoW-based puzzle solving race [7], the number of blocks that are mined by the blockchain provider and waiting for confirmation during T is $\frac{T}{T_0}\frac{\bar{h}H}{H}=\frac{T}{T_0}\bar{h}$. On the other hand, instead of following the Poisson distribution based model, the number of blocks successfully mined by attackers during T can be accurately modeled as a negative binomial variable [7]. Therefore, with the investment ratio $\bar{h}$, the probability for attackers to succeed in double spending during T can be expressed as follows (see Theorem 1 in [8]):

$$\mathrm{P}\left(\bar{h}\right)=I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h},\frac{1}{2}\right),\bar{h}\geq\frac{1}{2}, \tag{1}$$

where $I_w\left(u,v\right)$ is the regularized incomplete Beta function:

$$I_w\left(u,v\right)=\frac{\Gamma\left(u+v\right)}{\Gamma\left(u\right)\Gamma\left(v\right)}\int_0^w t^{u-1}(1-t)^{v-1}\mathrm{d}t \tag{2}$$

with $\Gamma\left(\cdot\right)$ being the gamma function. The model of exponential decay in (1) is discovered in [9] and proved in [8].

We consider that the blockchain provider receives payments from the users in the form of transaction fees in a confirmed block. Under double-spending attacks, the blockchain provider has to compensate the loss of the users with a fixed rate for each transaction in the block that is finally overridden. Assume that the number of transactions included in each block is the same, and hence the transaction fee and compensation rate are fixed for each transaction. Let N_{T} denote the number of transactions in a block, r denote the block mining reward for each block and q denote the total compensation rate for each block. Then, with the investment ratio $\bar{h}$, the blockchain provider's potential loss is $\frac{T}{T_0}\bar{h}N_{\mathrm{T}}q$ under the double-spending attack, and the probability of successful attack is:

$$\mathrm{P}\left(\bar{h}\right)=\begin{cases}I_{4(1-\bar{h})\bar{h}}\left(\frac{T}{T_0}\bar{h},\frac{1}{2}\right), & \bar{h}\geq\frac{1}{2},\\ 1, & \bar{h}<\frac{1}{2},\end{cases} \tag{3}$$

where $\int_0^{1/2} \mathrm{P}\left(\bar{h}\right) \mathrm{d}\bar{h} = \int_0^{1/2} 1\mathrm{d}\bar{h} = \frac{1}{2}$ and $\int_{1/2}^{1} \mathrm{P}\left(\bar{h}\right) \mathrm{d}\bar{h} = 1 - \int_0^{1/2} \mathrm{P}\left(\bar{h}\right) \mathrm{d}\bar{h} = \frac{1}{2}$. Here, we only focus on the case where the investment ratio of the blockchain provider is no less than $1/2$. The reason is that when $\bar{h} < 1/2$, the probability of successful double spending is always equal to 1 as shown in (3), which is trivial and thus not our focus.

2) Premium Determination: The cyber-insurer offers a cyber-insurance service to the blockchain provider, and the blockchain provider transfers the risk of double-spending attack to the cyber-insurer by buying the cyber-insurance. By adopting the concept of risk-adjusted premium in [10], the cyber-insurer dynamically determines the price, i.e., premium, of its cyber-insurance product according to the insurance risk distribution. According to our previous discussion, the cyber-insurer has an insurance risk, i.e., paying the claim of $\frac{T}{T_0}\bar{h}N_{\mathrm{T}}q$ with the probability of $\mathrm{P}\left(\bar{h}\right)$ given by (3). Then, the expected loss for the cyber-insurer can be formulated as follows:

$$\begin{aligned} \mathrm{E}_{loss} &= \int_{1/2}^{1} \frac{T}{T_0}\bar{h}N_{\mathrm{T}}q\mathrm{P}\left(\bar{h}\right)\mathrm{d}\bar{h} = \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\bar{h}\mathrm{P}\left(\bar{h}\right)\mathrm{d}\bar{h} \\ &= \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]\mathrm{d}\bar{h}, \end{aligned} \tag{4}$$

where $\mathrm{F}\left(\bar{h}\right)$ is the cumulative distribution function for $\mathrm{P}\left(\bar{h}\right)$, i.e., $\mathrm{F}\left(\bar{h}\right) = \int_0^{1/2}\mathrm{P}\left(\bar{h}\right)\mathrm{d}\bar{h} + \int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta = \int_0^{1/2} 1\mathrm{d}\bar{h} + \int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta = \frac{1}{2} + \int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta$. Based on the formulated distribution of the insurance risk and the concept of risk-adjusted premium, the cyber-insurer can determine the premium as follows:

$$\Lambda\left(\gamma\right) = \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\omega\left(1-\int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta,\gamma\right)\mathrm{d}\bar{h}, \tag{5}$$

where $\omega\left(x,\gamma\right)$ is an increasing concave function of x and belongs to the families of elementary transforms given in Section 5 of [10]. Without loss of generality, we adopt the PH transform in our study, i.e., $\omega\left(x,\gamma\right) = x^{\frac{1}{\gamma}}$, $\gamma \geq 1$ in Subsection 5.1 of [10]. Then, the corresponding premium can be expressed as follows:

$$\Lambda\left(\gamma\right) = \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}\bar{h}, \tag{6}$$

where γ is the premium coefficient deciding on the insurance policy. Thus, the cyber-insurer adjusts the premium by controlling γ according to the insurance risk. It is worth noting that the term $\left[1-\int_{1/2}^{\bar{h}}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]$ in (6) is smaller than 1. Therefore, the larger γ is, the higher the premium $\Lambda\left(\gamma\right)$ will be.

B. System Model

1) The User's Utility: We suppose that each user in the blockchain service market has a service demand, which is determined by an intrinsic value θ_i from the uniform distribution F_{U} over the interval $[0,1]$. Here, θ_i can be interpreted as the probability for user i to buy the blockchain service. We further assume that the intrinsic values of the users are independently distributed. The users also experience social externalities in which the decision of one user can influence the decisions of the other users. Let $\Pr\left[\text{j buys the service}\right]$ denote the probability that user j subscribes to the service, then, the utility of user i can be expressed as follows [11]:

$$u_i = \bar{h} + \theta_i - p_i + \alpha\sum_{j\in\mathcal{N}} g_{ij}\Pr\left[\text{j buys the service}\right]. \tag{7}$$

In (7), the first term, i.e., $\bar{h}$, is the investment ratio of the blockchain provider. $\bar{h}$ represents the positive effect owning to the effort of the blockchain provider in preventing the security breach due to double-spending attacks. According to (1), the larger $\bar{h}$ is, the lower the successful probability of double-spending attacks is, and consequently the less the users will be affected. The third term, i.e., $p_i \in [0, p^{\mathrm{u}}]$, is the price of the service for user i[1]. The forth term of (7), i.e., $\alpha\sum\limits_{j\in\mathcal{N}} g_{ij}\Pr\left[\text{j buys the service}\right]$, represents the positive social externality among the users. g_{ij} is the element of the externality matrix $\mathbf{G}$ [12] and represents the level of the social externality (influence) that user j has on user i. We assume that $g_{ij} \neq 0$, $\forall i \neq j$ and $g_{ii} = 0$, $\forall i \in \mathcal{N}$. Finally, α is a constant controlling the level of social externality for the entire network.

2) Profits of the Blockchain Provider and the Cyber-insurer: The goals of the blockchain provider and the cyber-insurer are to maximize their individual profits. Based on our previous discussion, the payoff functions of the blockchain provider can be expressed as follows:

$$\begin{aligned} \Pi_{\mathrm{P}}\left(\bar{h},\mathbf{p}\right) = &\sum_{i\in\mathcal{N}} p_i x_i - \frac{a\bar{h}}{1-\bar{h}} + \bar{h}\frac{T}{T_0}N_{\mathrm{T}}r \\ &- \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}t, \end{aligned} \tag{8}$$

where the first term $\sum_{i\in\mathcal{N}} p_i x_i$ is the revenue obtained from the users' payment for the blockchain service and x_i is the probability that user i buys the service defined in (13). The second term, i.e., $h = \frac{a\bar{h}}{1-\bar{h}}$, is the blockchain provider's investment in the infrastructure, and we have $h = \frac{a\bar{h}}{1-\bar{h}} \Leftrightarrow \bar{h} = \frac{h}{a+h}$. The third term, i.e., $\bar{h}\frac{T}{T_0}N_{\mathrm{T}}r$, is the block mining reward received by the blockchain provider for maintaining the service. The last term, i.e., $\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}t$, is the premium paid by the blockchain provider to the cyber-insurer, and q is the compensation price for one transaction.

On the other hand, the premium paid by the blockchain provider is the revenue of the cyber-insurer. Due to the uncertainty of double-spending attacks, we adopt the expected claim as the cyber-insurer's cost. Then, the cyber-insurer's payoff function can be expressed as:

$$\begin{aligned} \Pi_{\mathrm{I}}\left(\gamma\right) = &\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}t \\ &- \mathrm{P}\left(\bar{h}\right)\bar{h}\frac{T}{T_0}N_{\mathrm{T}}q - \sigma(\bar{h},\gamma), \end{aligned} \tag{9}$$

where the first term is the premium paid by the blockchain provider. The second term, i.e., $\mathrm{P}\left(\bar{h}\right)\bar{h}\frac{T}{T_0}N_{\mathrm{T}}q$, is obtained as

[1] Note that the uniform pricing in which all users are charged with the same price is a special case of the discriminative pricing adopted in this paper.

the product of the successful attack probability and the total claim paid to the blockchain provider for covering its loss. Finally, since the premium increases as the cyber-insurer's decision variable γ increases, a rational cyber-insurer will keep γ as high as possible to maximum its revenue. However, when the blockchain provider increases its investment ratio, the successful attack probability will decrease. As a result, the blockchain provider will have less incentive to pay an extremely high premium. Therefore, we introduce the last term in (9) to model the possibly negative impact on the expected payoff of the cyber-insurer as both the values of $\bar{h}$ and γ increase, which is similar to the concept of the punishment on insurer adopted in [13]. Here, we define $\sigma\left(\bar{h},\gamma\right) = \sigma_1\left(\bar{h}\right)\sigma_2\left(\gamma\right)$, where $\sigma_1\left(\bar{h}\right)$ is an increasing convex function of $\bar{h}$ with the following properties:

$$\sigma_1\left(\bar{h}\right)\begin{cases} >0, & \bar{h} > \dfrac{1}{2}, \\ =0, & \bar{h} = \dfrac{1}{2}, \\ <0, & \bar{h} < \dfrac{1}{2}. \end{cases} \tag{10}$$

The conditions in (10) indicates that with $\bar{h} > \frac{1}{2}$, the blockchain provider's effort in investing the computing resource effectively reduces the successful attack probability. Consequently, the probability of the cyber-insurer paying the claim to the blockchain provider is also reduced. Then, keeping the highest premium has a negative effect on the cyber-insurer's payoff, e.g., by hurting its reputation or curbing the incentive for the blockchain provider to buy the insurance. Under the other two conditions in (10), the lack of enough investment in infrastructure of the blockchain provider will induce higher probability of being successfully attacked, hence leading to a positive effect on the cyber-insurer's payoff due to the higher demand of financial protection. Additionally, $\sigma_2\left(\gamma\right)$ is an increasing convex function of γ and $\sigma_2\left(\gamma\right)|_{\gamma=1} = 0$. As such, when $\gamma = 1$, the expected loss in (4) is equal to the premium in (6), and there is no negative effect on the cyber-insurer's reputation. For tractable analysis, we adopt the following model:

$$\sigma\left(\bar{h},\gamma\right) = \sigma_1\left(\bar{h}\right)\sigma_2\left(\gamma\right) = \underbrace{\left(\bar{h}-\frac{1}{2}\right)^3}_{\sigma_1\left(\bar{h}\right)}\underbrace{\left(\gamma-1\right)\gamma^{\beta}}_{\sigma_2\left(\gamma\right)}, \quad \beta > 1. \tag{11}$$

It is worth noting that the cyber-insurer's payoff function in (9) may also adopt other models for $\sigma\left(\bar{h},\gamma\right)$. The selected model in (11) has no effect on our subsequent analysis.

III. Game Equilibrium Analysis

Using backward induction, we first obtain the Nash Equilibrium (NE) of the user-level subgame $\mathcal{G}_{\mathrm{u}}$ by characterizing a system of interdependent demands. We provide the sufficient conditions for the existence and uniqueness of the NE in the user-level subgame $\mathcal{G}_{\mathrm{u}}$ by solving the bounded linear complementarity problem of the subgame [11]. Then, we substitute the parametric NE of $\mathcal{G}_{\mathrm{u}}$ into the leader-level subgame $\mathcal{G}_{\mathrm{L}}$. Under a reasonable assumption, we show that the Jacobian matrix constructed from the payoff functions of each player in the leader-level subgame is negative definite. Hence, we prove that the Stackelberg Equilibrium (SE) of the market game exists and is unique.

A. Equilibrium Analysis for User-Level Noncooperative Subgame

Intuitively, user i only buys the service when it has a positive payoff, namely $u_i > 0$. This indicates that there exists a threshold $\tilde{\theta}_i$ for the intrinsic value θ_i in (7), such that user i will buy the service only when $\theta_i > \tilde{\theta}_i$. $\tilde{\theta}_i$ can be obtained by setting $u_i = 0$:

$$\begin{aligned} 0 &= \bar{h} + \tilde{\theta}_i - p_i + \alpha\sum_{j\in\mathcal{N}} g_{ij}\mathrm{Pr}\left[\text{j buys the service}\right] \\ &= \bar{h} + \tilde{\theta}_i - p_i + \alpha\sum_{j\in\mathcal{N}} g_{ij}\mathrm{Pr}\left[\theta_j > \tilde{\theta}_j\right] \\ &= \bar{h} + \tilde{\theta}_i - p_i + \alpha\sum_{j\in\mathcal{N}} g_{ij}\left[1-\mathrm{F_U}\left(\tilde{\theta}_j\right)\right] \\ \Leftrightarrow \tilde{\theta}_i &= p_i - \bar{h} - \alpha\sum_{j\in\mathcal{N}} g_{ij}\left[1-\mathrm{F_U}\left(\tilde{\theta}_j\right)\right], \end{aligned} \tag{12}$$

where $1-\mathrm{F_U}\left(\tilde{\theta}_j\right)$ denotes the probability that user j draws a valuation above the threshold $\tilde{\theta}_j$. For ease of exposition, let $x_i = 1-\mathrm{F_U}\left(\tilde{\theta}_i\right)$ denote the probability that user i buys the service, and x_i can be further expressed as follows:

$$\begin{aligned} x_i &= 1-\mathrm{F_U}\left(\tilde{\theta}_i\right) = 1-\mathrm{F_U}\left(p_i - \bar{h} - \alpha\sum_{j\in\mathcal{N}} g_{ij}\left[1-\mathrm{F_U}\left(\tilde{\theta}_j\right)\right]\right) \\ &= 1 - p_i + \bar{h} + \alpha\sum_{j\in\mathcal{N}} g_{ij}x_j. \end{aligned} \tag{13}$$

From (13), we can characterize a system of the users' interdependent demands as follows:

$$x_i = \begin{cases} 0, & \text{if } 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j < 0, \\ 1, & \text{if } 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j > 1, \\ 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j, & \text{otherwise.} \end{cases} \tag{14}$$

After subtracting each condition in (14) by the value of its corresponding x_i, we convert (14) into the following form:

$$x_i = \begin{cases} 0, & \text{if } 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j - x_i < 0 - \underbrace{x_i}_{=0} = 0, \\ 1, & \text{if } 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j - x_i > 1 - \underbrace{x_i}_{=1} = 0, \\ 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j, & \text{if } 1 - p_i + \bar{h} + \alpha\sum\limits_{j\in\mathcal{N}} g_{ij}x_j - x_i = 0. \end{cases} \tag{15}$$

Furthermore, we rewrite (15) into the following matrix form:

$$x_i = \begin{cases} 0, & \text{if } \left\{\left(1+\bar{h}\right)\mathbf{1} - \mathbf{p} - \left(\mathbf{I}-\alpha\mathbf{G}\right)\mathbf{x}\right\}_i < 0, \\ 1, & \text{if } \left\{\left(1+\bar{h}\right)\mathbf{1} - \mathbf{p} - \left(\mathbf{I}-\alpha\mathbf{G}\right)\mathbf{x}\right\}_i > 0, \\ \left\{\left(1+\bar{h}\right)\mathbf{1} - \mathbf{p} + \alpha\mathbf{G}\mathbf{x}\right\}_i, & \text{if } \left\{\left(1+\bar{h}\right)\mathbf{1} - \mathbf{p} - \left(\mathbf{I}-\alpha\mathbf{G}\right)\mathbf{x}\right\}_i = 0, \end{cases} \tag{16}$$

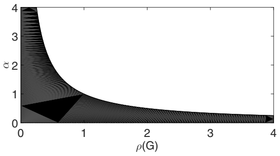

Figure 2: An illustration of Assumption 1.

where $\mathbf{I}$ is the identity matrix, $\mathbf{1} = [1, 1, \ldots, 1]^\top \in \mathbb{R}^{|\mathcal{N}| \times 1}$ and $\{\cdot\}_i$ represents the i-th entry of a vector. With (16), we can investigate the properties of the NE in the user-level subgame.

Assumption 1. *$\alpha \rho (\mathbf{G}) < 1$, where $\rho(\cdot)$ is the spectral norm of a matrix.*

The physical meaning of Assumption 1 is illustrated in Fig. 2, where the black area is the feasible area of $\alpha\rho(\mathbf{G})$. If $\alpha\rho(\mathbf{G})$ exceeds the feasible area, the social externality will be too strong such that every user will buy the service, which is impossible in reality.

THEOREM 1. *The user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$ admits a unique NE under Assumption 1.*

Proof. (16) is defined as a bounded linear complementarity problem in [11]. It is a linear instance of the general mixed complementarity problems discussed in [14]. As discussed in [14], the linear instance of a complementarity problem admits a unique solution, i.e., the NE, to the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$, if $(\mathbf{I} - \alpha\mathbf{G})$ is a P-matrix[2].

Since $\alpha\rho(\mathbf{G}) < 1$ under Assumption 1, all the eigenvalues of the matrix $\alpha\mathbf{G}$ belong to $(0, 1)$ and hence all the eigenvalues of the matrix $(\mathbf{I} - \alpha\mathbf{G})$ belong to $(0, 1)$. Therefore, $(\mathbf{I} - \alpha\mathbf{G})$ is a non-singular M-matrix[3]. Based on Theorem 6.2.3 in [15], "any non-singular M-matrix is a P-matrix", $(\mathbf{I} - \alpha\mathbf{G})$ is a P-matrix and then there exists a unique NE in the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$. The proof is completed. □

According to the system of interdependent demands (16), the set of users $\mathcal{N}$ can be partitioned into three subsets, i.e., $\mathcal{S}_0$, $\mathcal{S}_1$, and $\mathcal{S}$ as follows:

- $\mathcal{S}_0 = \left\{ i \middle| \left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x} \right\}_i < 0, \forall i \in \mathcal{N} \right\}$,
- $\mathcal{S}_1 = \left\{ i \middle| \left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x} \right\}_i > 0, \forall i \in \mathcal{N} \right\}$,
- $\mathcal{S} = \{ i | \{(1 + \bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i = 0, \forall i \in \mathcal{N}\}$.

Then, we obtain the following theorem:

THEOREM 2. *The users in the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$ only belong to $\mathcal{S}$, i.e., $\mathcal{S} = \mathcal{N}$, $\mathcal{S}_0 = \emptyset$, and $\mathcal{S}_1 = \emptyset$. Given the service price vector $\mathbf{p}$, the optimal solution to the system of interdependent demands (16) is*

$$\mathbf{x}^* = (\mathbf{I} - \alpha\mathbf{G})^{-1} \left[\left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} \right]. \tag{17}$$

Proof. We denote the optimal price by $\mathbf{p}^*$ and the optimal demand by $\mathbf{x}^*$. Then, we show that $\mathcal{S}_0 = \emptyset$ and $\mathcal{S}_1 = \emptyset$.

1) $\mathcal{S}_0 = \emptyset$: We first assume that $\mathcal{S}_0 \neq \emptyset$. This means that $\exists i \in \mathcal{N}$, such that $x_i{}^* = 0$ and $\{(1+\bar{h})\mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}^*\}_i < 0$. Because $\left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x} \right\}_i = 1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j - x_i - p_i$ is continuous on p_i and $1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j{}^* > 0$, there exists a $p_i{}'$ where $p_i{}' < p_i{}^*$ such that $1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j{}^* - p_i{}' > 0$ and correspondingly $x_i{}' > 0$. This indicates that when the service price charged to user i decreases from $p_i{}^*$ to $p_i{}'$, user i has an incentive to increase its demand from $x_i{}^* = 0$ to $x_i{}' > 0$. Consequently, the revenue of the blockchain provider will increase since $p_i{}^* x_i{}^* = 0$ while $p_i{}' x_i{}' > 0$. Therefore, $x_i{}^*$ and $p_i{}^*$ cannot be the optimal demand and price for user i, respectively. Hence, $i \notin \mathcal{S}_0$, $\forall i \in \mathcal{N}$ and $\mathcal{S}_0 = \emptyset$.

2) $\mathcal{S}_1 = \emptyset$: Similarly, we assume that $\mathcal{S}_1 \neq \emptyset$. This means that $\exists l \in \mathcal{N}$, $x_l{}^* = 1$ and $\left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x}^* \right\}_l > 0$. Since $\left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x} \right\}_l = 1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j - x_l - p_l$ is continuous on p_l, there exists an ϵ where $\epsilon > 0$ such that $1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j{}^* - (p_l{}^* + \epsilon) > 0$ and $x_l{}^* = 1$. Let $\epsilon = \bar{h} + \alpha \sum_{j\in N} g_{ij} x_j{}^* - p_l{}^*$, we have $1 + \bar{h} + \alpha \sum_{j\in\mathcal{N}} g_{ij} x_j{}^* - (p_l{}^* + \epsilon) = 0$, and here $x_l{}^* = 1 - (p_l{}^* + \epsilon) + \bar{h} + \sum_{j\in\mathcal{N}} g_{lj} x_j{}^* = 1$. This means that even if the service price of user l increases from $p_l{}^*$ to $(p_l{}^* + \epsilon)$, the demand of user l is still equal to 1 while the profit of the blockchain provider has been increased from $p_l{}^* x_l{}^* = p_l{}^*$ to $(p_l{}^* + \epsilon)\, x_l{}^* = p_l{}^* + \epsilon$. Moreover, since

$$\begin{aligned} &\left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x}^* \right\}_l - \epsilon \\ =& 1 + \bar{h} - (p_l{}^* + \epsilon) - \underbrace{x_l{}^*}_{1} + \alpha \sum_{j\in\mathcal{N}} g_{lj} x_j{}^* = 0, \end{aligned} \tag{18}$$

user l belongs to $\mathcal{S}$ instead of $\mathcal{S}_1$. Therefore, $p_l{}^*$ and $x_l{}^*$ are not the optimal price and demand for user l, respectively. Hence, $l \notin \mathcal{S}_1$, $\forall l \in \mathcal{N}$ and $\mathcal{S}_1 = \emptyset$.

To conclude, given any price vector $\mathbf{p}$ of the blockchain service, the condition

$$\left\{ \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x}^* \right\}_i = 0 \tag{19}$$

will be satisfied for all user $i \in \mathcal{N}$. Therefore,

$$\left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x}^* = \mathbf{0} \leftrightarrow (\mathbf{I} - \alpha\mathbf{G})\,\mathbf{x}^* = \left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p}. \tag{20}$$

Since we have already shown that the matrix $(\mathbf{I} - \alpha\mathbf{G})$ is a non-singular matrix in Theorem 1, the inverse of $(\mathbf{I} - \alpha\mathbf{G})$ exists. Multiply both sides of (20) by $(\mathbf{I} - \alpha\mathbf{G})^{-1}$, the optimal solution to the system of interdependent demands, or equivalently, the NE to the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$, is

$$\mathbf{x}^* = (\mathbf{I} - \alpha\mathbf{G})^{-1} \left[\left(1 + \bar{h}\right)\mathbf{1} - \mathbf{p} \right]. \tag{21}$$

The proof is completed. □

B. Equilibrium Analysis for Leader-Level Noncooperative Subgame

After deriving the equilibrium demand of the users, we investigate the leader-level noncooperative subgame $\mathcal{G}_{\mathrm{L}}$ for the blockchain provider and the cyber-insurer. At the NE, no player can increase its profit by choosing a different strategy

[2] A matrix A is a P-matrix if all its principal minors are positive.

[3] A matrix A is a non-singular M-matrix if $A = I - B$ for a positive matrix B with largest eigenvalue $\rho(B) < 1$.

provided that the other player' strategy is unchanged [16]. In what follows, we first prove that an NE exists in the leader-level subgame $\mathcal{G}_{\mathrm{L}}$. Then, we prove that this NE is unique.

Substituting the optimal demand of the users derived in (21) into the profit function of the blockchain provider, we can rewrite (8) into a matrix form as follows:

$$\begin{aligned}\Pi_{\mathrm{P}}\left(\bar{h}, \mathbf{p}\right) =& \mathbf{p}^{\top}\left(\mathbf{I}-\alpha \mathbf{G}\right)^{-1}\left[\left(1+\bar{h}\right)\mathbf{1}-\mathbf{p}\right]-\frac{a\bar{h}}{1-\bar{h}}+\bar{h}\frac{T}{T_0}N_{\mathrm{T}}r \\ &-\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}\left(\theta\right)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}t.\end{aligned} \tag{22}$$

Then, we can obtain the following theorem regarding the NE of the leader-level subgame.

Theorem 3. *There exists at least one NE in the leader-level noncooperative subgame $\mathcal{G}_{\mathrm{L}}$ if and only if $a > \frac{1}{8}\mathbf{1}^{\top}(\mathbf{I}-\alpha\mathbf{G})^{-1}\mathbf{1}$. Then, the Stackbelberg equilibrium of the market game exists.*

Proof. We use congruent matrix to prove the concavity for the Hessian matrix of Π_{P} with respect to $\left[\mathbf{p}^{\top}, \bar{h}\right]^{\top}$ and Π_{I} with respect to γ. The proof is omitted due to the space limit. □

Theorem 4. *The NE in the leader-level noncooperative subgame $\mathcal{G}_{\mathrm{L}}$ is unique if and only if $a > \frac{9(\beta+1)^2(\gamma^u)^{\beta+1}}{128\beta}$ and hence the Stackbelberg equilibrium is unique.*

Proof. We prove that the Jacobian matrix is negative definite by using its congruent matrix. The proof is omitted due to the space limit. □

IV. Performance Evaluation

In this section, we conduct extensive numerical simulations to evaluate the performance of the market entities at the equilibrium in each stage. We consider a group of $|\mathcal{N}|$ users in the blockchain service market. The off-diagonal elements of social externality matrix $\mathbf{G}$, i.e., g_{ij}, $\forall i \neq j$, is generated following the uniform distribution over the interval of $[0, 10]$. The domain of definition for α is set as $\left[5\times10^{-4}, 8\times10^{-4}\right]$ according to the parameter setting in [11]. The other default coefficients are given as follows: $\beta = 10$, $p^{\mathrm{u}} = 1$, $\gamma^{\mathrm{u}} = 2$, $T = 100$, $T_0 = 10$, $N_{\mathrm{T}} = 100$, $r = 10$, $q = 10$ and $a = 100$. Note that the price that we present in the figures of simulation results is the mean value of the discriminatory prices. The triple integral in the premium-related term in the profit functions of the blockchain provider and the cyber-insurer, i.e., (8) and (9), is calculated using the method of rectangular integral with 100 as the number of intervals.

A. Numerical Results

1) The impact of the number of users: We first evaluate the impacts by the number of users on the payoff of the market entities in Fig. 3, where the number of users increases from 50 to 120. Then, we evaluate the performance under three levels of social externality, e.g., 6.5×10^{-4}, 7×10^{-4}, and 7.5×10^{-4} which represent weak, medium, and strong levels of social externality, respectively. As expected, the profit of the blockchain provider increases significantly when the social externality becomes stronger. As the number of users increases, the profit of the blockchain provider also increases under the given social externality settings. Moreover, the increase of the profit of the blockchain provider becomes larger when the social externality is stronger. Intuitively, the reason is that the social externality stimulates the demand of each user. In return, the blockchain provider can raise the price of service accordingly and hence improves its profit. Meanwhile, as the social externality becomes stronger, the blockchain provider also achieves greater profit. This indicates that the attack may incur more loss to the blockchain provider. Therefore, the blockchain provider has a higher incentive to invest in the infrastructure to prevent double-spending attack. This explains the result that the investment by the blockchain provider increases at a higher rate with $\alpha = 7.5\times10^{-4}$ than with $\alpha = 6.5\times10^{-4}$. As a result, the stronger social externality reduces the successful attack probability at a higher rate. Correspondingly, as shown in Fig. 3(f), the premium coefficient γ decreases at a higher rate with the stronger social externality. This result indicates that the premium also decreases at a higher rate with stronger social externality. Thus, the cyber-insurer's profit decreases at a higher rate when the social externality becomes stronger as shown in Fig. 3(b).

2) The impact of attacker's computing resource: Finally, we evaluate in Fig. 4 the impact of the attackers' computing resource on the performance of the users, the blockchain

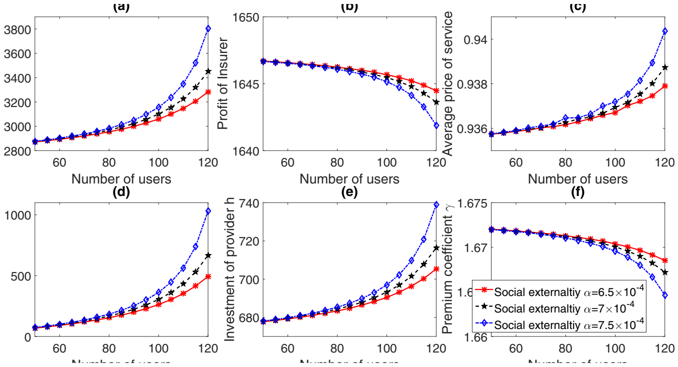

Figure 3: The results with increasing number of users.

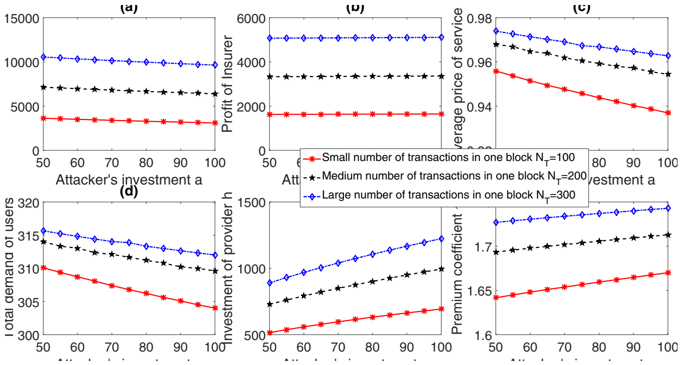

Figure 4: The result with increasing attacker's computing resource.

provider and the cyber-insurer. We consider three different situations with different sizes of a block, i.e., the number of transactions included in that block, with $N_{\mathrm{T}} = 100$, $N_{\mathrm{T}} = 200$, and $N_{\mathrm{T}} = 300$. We observe from Figs. 4(a) and (b) that as the attacker's computing resource increases, the profit of the blockchain provider decreases and the profit of the cyber-insurer remains unchanged. The reason is that the blockchain provider needs to increase its infrastructure investment when the attacker's computing resource increases (see Fig. 4(e)). Otherwise, the successful attack probability will significantly increase, and it results in the increase in the cost of the blockchain provider. With an increasing computing resource controlled by the attackers, the investment ratio of the blockchain provider cannot remain as high as before. This result is illustrated in Fig. 4(e) with $\frac{h^*}{a+h^*}\Big|_{a=50} \approx \frac{18}{19} > \frac{h^*}{a+h^*}\Big|_{a=100} \approx \frac{12}{13}$ when $N_{\mathrm{T}} = 300$. Therefore, as the attackers' computing resource increases, the successful attack probability and consequently the probability of the cyber-insurer paying the claim increases accordingly. Then, as shown in Fig. 4(f), the cyber-insurer increases the premium to keep its profit unchanged. Ultimately, the cost of the blockchain provider also increases. Moreover, as the attackers' computing resource increases, even when the blockchain provider reduces the price of its service to attract more users, the total demand from the users still decreases (see Figs. 4(c) and (d)). Consequently, this reduces the revenue and profit of the blockchain provider.

Furthermore, we show that the impact of the attackers' computing resource on the other parties in the market is subject to the number of transactions in one block N_{T}. With the fixed transaction fee and compensation rate, the more transactions in a single block is, the more reward that the blockchain provider obtains from mining a block. Moreover, since the compensation price of one block increases as the number of transactions in one block increases, the more compensation it will pay to the users once the attacks happen. Then, the blockchain provider has more incentive to invest in the computing resource. This is consistent with Fig. 4(e), where the increasing rate of the investment by the blockchain provider is higher with $N_{\mathrm{T}} = 300$ than that with $N_{\mathrm{T}} = 100$. On the other hand, as the attacker's computing resource increases, the increasing rate of the successful attack probability is lower with $N_{\mathrm{T}} = 300$ than that with $N_{\mathrm{T}} = 100$. Consequently, the increasing rate of the premium is lower with $N_{\mathrm{T}} = 300$ than that with $N_{\mathrm{T}} = 100$ (see Fig. 4(f)). Moreover, as N_{T} increases, the increasing rate of the successful attack probability will decrease, and the users' demand will be less affected. This is consistent with Figs. 4(c) and (d), where the decreasing rates of both the total user demand and the service price shrink as N_{T} increases.

V. Conclusion

In this paper, to financially protect the blockchain provider from double-spending attacks, we have proposed a risk management framework of the blockchain service market by incorporating the cyber-insurance. The interaction among the blockchain provider, cyber-insurer, and users in the market has been modeled as a two-stage Stackelberg game. For the blockchain provider, we have considered the problem of balancing between the proactive protection strategy, i.e., investing in computing power, and the reactive protection strategy, i.e., purchasing the cyber-insurance. For the users, we have considered the impact of both the social externality and the service security on the users' valuation of the blockchain service. In particular, for the cyber-insurer, we have incorporated the risk-adjusted pricing mechanism for premium adaptation. We have studied the equilibrium strategies of the three parties in the market using backward induction. We have analytically examined the conditions for the Stackelberg game to exist and to be unique. Furthermore, we have conducted extensive simulations to evaluate the performance of the market entities at the equilibrium. For the future work, we will investigate the long-run competition between the blockchain provider and cyber-insurer.

References

[1] D. T. T. Anh, M. Zhang, B. C. Ooi and G. Chen, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. PP, no. 99, pp. 1–1, 2018.

[2] M. Conti, C. Lal, S. Ruj et al., "A survey on security and privacy issues of bitcoin," *arXiv preprint arXiv:1706.00916*, 2017.

[3] G. O. Karame, E. Androulaki and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, NC, USA, Oct. 2012, CCS '12, pp. 906–917, ACM.

[4] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2017.

[5] S. Muhammad, M. Aziz, K. Charles, K. Kevin and N. Laurent, "Countering double spending in next-generation blockchains," in *IEEE ICC 2018*, Kansas City, USA, May 2018.

[6] R. Pal, L. Golubchik, K. Psounis and P. Hui, "On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer," in *IFIP Networking Conference, 2013*. IEEE, 2013, pp. 1–9.

[7] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009*, 2014.

[8] C. Grunspan and R. Pérez-Marco, "Double spend races," *arXiv preprint arXiv:1702.02867*, 2017.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. bitcoin," 2009.

[10] S. Wang, "Premium calculation by transforming the layer premium density," *ASTIN Bulletin: The Journal of the IAA*, vol. 26, no. 1, pp. 71–92, 1996.

[11] F. Bloch and N. Quérou, "Pricing in social networks," *Games and economic behavior*, vol. 80, pp. 243–261, 2013.

[12] X. Gong, L. Duan, X. Chen and J. Zhang, "When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 449–462, 2017.

[13] F. Bloch, G. Genicot and D. Ray, "Informal insurance in social networks," *Journal of Economic Theory*, vol. 143, no. 1, pp. 36–58, 2008.

[14] A. Simsek, A. Ozdaglar and D. Acemoglu, "On the uniqueness of solutions for nonlinear and mixed complementarity problems," Tech. Rep., Massachusetts Institute of Technology, 2005.

[15] A. Berman and R. J. Plemmons, *Nonnegative matrices in the mathematical sciences*, SIAM, 1994.

[16] M. J. Osborne, *An introduction to game theory*, vol. 3, Oxford university press New York, 2004.