On Cyber Risk Management of Blockchain Networks: A Game Theoretic Approach

Shaohan Feng, *Student Member, IEEE*, Wenbo Wang, *Member, IEEE*, Zehui Xiong, *Student Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Ping Wang, *Senior Member, IEEE*, and Shaun Shuxun Wang

Abstract—Open-access blockchains based on proof-of-work protocols have gained tremendous popularity for their capabilities of providing decentralized tamper-proof ledgers and platforms for data-driven autonomous organization. Nevertheless, the proof-of-work based consensus protocols are vulnerable to cyber-attacks such as double-spending. In this paper, we propose a novel approach of cyber risk management for blockchain-based service. In particular, we adopt the cyber-insurance as an economic tool for neutralizing cyber risks due to attacks in blockchain networks. We consider a blockchain service market, which is composed of the infrastructure provider, the blockchain provider, the cyber-insurer, and the users. The blockchain provider purchases from the infrastructure provider, e.g., a cloud, the computing resources to maintain the blockchain consensus, and then offers blockchain services to the users. The blockchain provider strategizes its investment in the infrastructure and the service price charged to the users, in order to improve the security of the blockchain and thus optimize its profit. Meanwhile, the blockchain provider also purchases a cyber-insurance from the cyber-insurer to protect itself from the potential damage due to the attacks. In return, the cyber-insurer adjusts the insurance premium according to the perceived risk level of the blockchain service. Based on the assumption of rationality for the market entities, we model the interaction among the blockchain provider, the users, and the cyber-insurer as a two-level Stackelberg game. Namely, the blockchain provider and the cyber-insurer lead to set their pricing/investment strategies, and then the users follow to determine their demand of the blockchain service. 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, mining, attack, double-spending, cyber-insurance, game theory

1 Introduction

In the past few years, blockchain technologies have attracted tremendous attention from both industry and academia for distributively providing the irreversible, tamper-evident database of tokenized asset transactions [1]. Furthermore, with the smart contracts [2] enabled on top of the decentralized consensus [1], blockchains are envisaged to be the "game changer" in various areas ranging from Peer-to-Peer (P2P) resource allocation/trading, e.g., distributed cloud storage [3], to financial services, e.g., digital identity management [4] and online markets for crowdsourcing services [5]. Although with the advantages such as open access, disintermediation, and pure self-organization, open-access/permissionless blockchains rely 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]. Since permissionless blockchain networks admit no identity control, they can be vulnerable to a series of insider attacks by malicious consensus nodes [6]. Among different types of attacks, double spending [7] is the most fundamental one and can be executed through various attacks such as goldfinger attacks, netsplit attacks and brute-force attacks [6]. In brief, a double-spending attacker attempts to simultaneously spend the same set of blockchain tokens in two different transactions. This can be performed by first persuading part of the network and the transaction receiver to confirm one transaction, and then persuading the majority of the network to override that transaction with a conflicting transaction spending the same set of tokens. In other words, double-spending attacks are executed through intentional blockchain forking. 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 although the double-spending attack is initially devised for Bitcoin, the attack is also applicable to other blockchain-based resource trading services and systems, for example, energy trading [8], plug-in hybrid electric vehicle (PHEV) charging credit management [9], wireless spectrum trading [10], bandwidth exchange in community networks [11] and cache storage trading [12].

Although a few approaches, e.g., [13], have been introduced in blockchains to deter and prevent attacks, due to the inherent characteristics of openness, the PoW-based

- *S. Feng, W. Wang, Z. Xiong, D. Niyato, and P. Wang are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. E-mail: {feng0089, ZXIONG002}@e.ntu.edu.sg, {wbwang, dniyato, wangping}@ntu.edu.sg.*
- *S.S. Wang is with Nanyang Business School, Nanyang Technological University, Singapore. E-mail: shaun.wang@ntu.edu.sg.*

Manuscript received 2 May 2018; revised 24 Aug. 2018; accepted 6 Oct. 2018. Date of publication 18 Oct. 2018; date of current version 8 Oct. 2021.
(Corresponding author: Shaohan Feng).
Digital Object Identifier no. 10.1109/TSC.2018.2876846

1939-1374 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

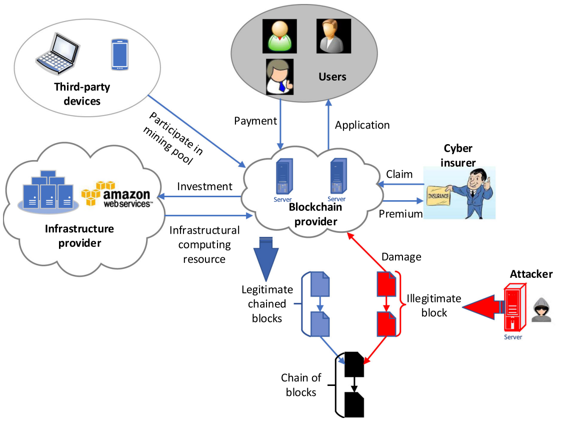


Fig. 1. An overview of the blockchain service market.

permissionless blockchain networks may not be completely secure. This critically hinders the broader adoption of permissionless blockchains, especially in business services that require high-level service security. Along with the studies on the improvement of blockchain protocols, blockchain service providers are also looking for an alternative means of cyber-risk management. Recently, cyber-insurance has been recognized as a promising approach to efficiently manage the cyber risks by transferring them to insurers [14]. 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. To date, a number of cyber-insurance products have been made available in the market [15]. According to the types of target systems, these products can be categorized into specific groups designed for service providers such as ISPs and clouds, single mobile/work stations, networks of devices and dedicated cyber-physical/industrial systems.

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 in other insurable cyber-systems, the market design of cyber-insurance for blockchain networks also has to address a few important issues. First, from the cyber-insurer's perspective, the scope and policy of the cyber-insurance have to be clearly defined in regard to what kind of attacks to be covered and how to quantify the risk, the possible damage and thus the insurance premium. Second, alongside the reactive risk transfer with the cyber-insurance, rational blockchain providers also have to consider the proactive strategy in security improvement and thus balance the investment in the infrastructure and in the cyber-insurance.

To answer these questions, we consider a PoW-based blockchain service market under the threat of double-spending attacks (see Fig. 1). The market is composed of three entities, namely, the users, the blockchain provider, and the cyber-insurer. The users subscribe to a service, e.g., P2P energy trading for smart grids, which is implemented on top of the blockchain provided by the blockchain provider. We consider that the blockchain provider is composed of a group of individual honest machines which are responsible for maintaining the data consensus in the framework of PoW-based permissionless blockchains. The blockchain provider purchases the computing resource from cloud-based infrastructure providers[1] or deploys more computing power internally for maintaining the network consensus. Meanwhile, in order to lower the cost on infrastructure, third-party devices are encouraged to join the decentralized consensus process by dedicating their individual computing resources into the network. Working as a single blockchain provider, the group of consensus machines make 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. More specifically, the major contributions of this paper are summarized as follows:

(1) We formulate the mechanisms of blockchain service pricing, blockchain infrastructure investment and cyber-insurance premium adjustment as a joint market equilibrium problem. We model the interactions among the three parties in the market as a two-level Stackelberg game. We provide and prove a few important theoretical discoveries regarding the properties of the equilibrium in the market game.

(2) We incorporate the social externality [17], [18] among blockchain users in our end-user utility model. Also, by modeling the impact of computing power on the blockchain security, we consider the blockchain provider's strategy to incorporate both dimensions of infrastructure investment and insurance spendings. Furthermore, by adopting the concept of "risk-adjusted premium", we mathematically capture the impact of attack probability on premium pricing from the cyber-insurer's perspective.

(3) We conduct extensive evaluation to assess the performance of the three parties with their equilibrium strategies at different levels of the attacker-controlled computing power.

The proposed market framework introduces a novel incentive-compatible business ecosystem, where the blockchain service users benefit from enjoying more resilient services, and both the blockchain provider and the cyber-insurer are able to gain more profits. In fact, the potential of cyber-insurance for blockchain, Bitcoin specifically, has been perceived in the market. For example, Petra Insurance Brokers (www.insurewithpetra.com) introduces the concept of insurance for Bitcoin transactions. Likewise, BitCoin Financial Group unveils "BitSecure", which is a Bitcoin theft insurance policy (www.bitcoinfinancialgroup.com). This product covers both external hacking and employee theft. Moreover, more

[1] For example, Amazon AWS provides the blockchain infrastructures through its partner ecosystem [16].

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

insurance products are emerging in which a few of them focus on general blockchain services. Therefore, our proposed concept and framework of cyber insurance for blockchain services has a clear and direct practical implication. Moreover, from the perspective of market design, the blockchain services are typically highly customized for a certain environment and application. Thus, we consider the mutual trading between single insurer and single provider. The model of a many-to-many market for multiple insurers and providers is likely to be intractable and needs further development, and hence it is beyond the scope of this paper. Finally, the model developed in this paper can be readily extended to blockchains with the emerging consensus protocols based on the generalized proof of concepts [1], where investment in other resources, e.g., stakes, is needed to prevent attacks.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 describes the preliminaries about blockchains and cyber-insurance, the system model, and the formulation of Stackelberg game. Section 4 investigates the existence and uniqueness of the equilibrium in the proposed Stackelberg game under practical assumptions. Section 5 presents the numerical performance evaluation. Section 6 concludes the paper.

2 Related Works

The permissionless blockchain network was originally conceptualized in the famous grassroot cryptocurrency project "Bitcoin" as a decentralized database for tamper-proof recording and trusted timestamping for the transactional data between P2P users. Permissionless blockchains have been widely recognized for the superb consensus scalability, the tamper-evidence data organization and the capability of supporting the distributed, general-purpose virtual machines [1], [19]. For this reason, in recent years there has seen a plethora of emerging application based on blockchains such as Internet finance and property digitization [20], self-organization for Internet of Things [21] and other nonfinancial applications, e.g., notary documents and anti-counterfeit solutions [22].

Permissionless blockchain networks creatively solve the problems of replicated consensus in open-access networks by introducing the financial incentive and cryptical zero-knowledge proof into the consensus process [1]. More specifically, any node in the blockchain network is allowed to issue digitally signed transactions to other nodes by "broadcasting" the transactions in a gossip manner over the P2P links between the nodes. The consensus nodes pack up an arbitrary subset of unapproved transactions into a cryptographically protected data structure, i.e., the "block", and rival with each other in a block publishing race (also known as block mining) to acquire the block mining reward [23]. Following the Nakamoto protocol for blockchain state maintenance [1], the consensus nodes only accept the longest chain among all the locally observable candidates of the blockchain state as their canonical view of the blockchain. To determine the winner of a block mining race, the consensus nodes have to perform an exhaustive search for the solutions of the crypto-puzzles built upon their proposed blocks. In other words, the nodes that acquire more computing power will have higher probability of winning the race and hence the more power of controlling the blockchain state [1]. Therefore, the honest consensus nodes have to secure a sufficiently large amount of computing power to guarantee the well-being of the blockchain services, e.g., data integrity [23]. Grabbing more computing power, on the other hand, is also from which the malicious nodes start to breach the blockchain networks.

Cyber-insurance, in the meanwhile, has been recognized as an innovative tool to manage the cyber risks and alleviate the damage of cyber-attacks for the insured customers [24]. Cyber-insurance provides the coverage on losses and liabilities from network/information security breaches. This greatly incentivizes the security investments by cyber-physical systems. However, compared with classical insurance, cyber-insurance introduces a number of unique issues. For example, due to the interdependence of security systems or lack of statistical data, it is difficult to assess the systems' vulnerability and hence hard to estimate the risk transferred to the cyber-insurer [15]. For the transaction-oriented cyber services built upon permissionless blokchains, the designer of cyber-insurance also faces the similar issues. Nevertheless, recent studies on the mechanisms of double-spending attacks [25], [26], [27] have shed light upon the possible approaches in analytically assessing the risks of this fundamental threat on the blockchain systems. For example, in [25], the authors proposed a new protocol which requires the consensus nodes, i.e., block miners, to confirm transactions only if the inputs of the transactions have not been spent, hence preventing users from double-spending their funds. Based on the characteristics of intentional forking in double-spending attacks, the authors in [26], [27] introduced the methods to estimate the probability of successful double-spending attacks by analyzing the investments in computing resource of both the blockchain maintainers and attackers. With these studies, it is now possible to estimate the probability of successful double spending and evaluate the potential risks transferred to the cyber-insurers.

Furthermore, under the condition that the probability distribution of risk can be estimated, the authors in [28] proposed a risk-adjusted premium for pricing risks based on the Proportional Hazard (PH) transform, namely, a power transform in the decumulative distribution function of the risks. Since the PH transform satisfies the elementary principles of assigning premiums, i.e., scale-invariance and translation-invariance, it has been adopted in a number of works concerning the premium determination. In addition, a class of premium functions which are comonotonicity additive and stochastic dominance preservative were studied in [29]. Therein, the premium determination method based on the PH transform was generalized with an axiomatic approach, and the principles such as the absolute deviation principle [30] were thoroughly studied and compared.

However, to the best of our knowledge, it still remains an open field of research to employ the cyber-insurance for alleviating the damage of double-spending attack for the blockchain providers. The aforementioned works inspire a vision of quantifying the risk of double-spending attacks based on the computing resources owned by the blockchain maintainers and attackers. Then, the corresponding insurance premium can be determined under the framework based on the PH transform. By transferring the risks caused by double spending to the cyber-insurers, the cyber-physical services residing on the blockchains can be much more robust. This is also the major objective of our studies.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

3 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, the users, and the 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.

The cyber-insurance for blockchain-based service under our consideration works as follows. The blockchain provider firsts pay the premium determined by the cyber-insurer. If the double-spending attack happens, which is detected by the provider or users, the provider files the claims to the cyber-insurer. The cyber-insurer verifies the claim and makes the payment to the provider to compensate for the damage of the double spending. The methods to detect and verify the double spending attack are available and can be adopted, e.g., by deploying an observer as in [31], and hence they are not the focus of this paper.

3.1 Preliminaries

3.1.1 *Successful Attack Probability*

We consider that the honest consensus nodes work jointly as a single blockchain provider and are responsible for maintaining a permissionless, PoW-based blockchain for service provision. Extending the analysis in [26] and [27], 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 [26], 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 [26]. 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 [27]):

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

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

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

with $\Gamma(\cdot)$ being the gamma function. The model of exponential decay in (1) is discovered in [32] and proved in [27].

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:

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

where $\int_0^{1/2}\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}=\int_0^{1/2}1\mathrm{d}\bar{h}=\frac{1}{2}$ and $\int_{1/2}^{1}\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}=1-\int_0^{1/2}\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}=\frac{1}{2}$. 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.

3.1.2 *Premium Determination*

The cyber-insurer offers a cyber-insurance service to the blockchain provider and covers its total loss when the attack happens. In other words, after the blockchain provider buys the cyber-insurance, the risk of double-spending attack will be transferred to the cyber-insurer. By adopting the concept of risk-adjusted premium in [29], 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 $\mathrm{P}\big(\bar{h}\big)$ given by (3). Then, the expected loss for the cyber-insurer can be formulated as follows:

$$\begin{aligned}\mathrm{E}_{loss}&=\int_{1/2}^{1}\frac{T}{T_0}\bar{h}N_{\mathrm{T}}q\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}=\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\bar{h}\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}\\ &=\frac{T}{T_0}N_{\mathrm{T}}q\left[\bar{h}F\big(\bar{h}\big)\Big|_{\bar{h}=1/2}^{\bar{h}=1}-\int_{1/2}^{1}\mathrm{F}\big(\bar{h}\big)\mathrm{d}\bar{h}\right]\\ &=\frac{T}{T_0}N_{\mathrm{T}}q\left[\frac{3}{4}-\int_{1/2}^{1}\mathrm{F}\big(\bar{h}\big)\mathrm{d}\bar{h}\right]\\ &=\frac{T}{T_0}N_{\mathrm{T}}q\left[\int_{1/2}^{1}\frac{3}{2}\mathrm{d}\bar{h}-\int_{1/2}^{1}\mathrm{F}\big(\bar{h}\big)\mathrm{d}\bar{h}\right]\\ &=\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\frac{3}{2}-\mathrm{F}\big(\bar{h}\big)\mathrm{d}\bar{h}\\ &=\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{\bar{h}}\mathrm{P}(\theta)\mathrm{d}\theta\right]\mathrm{d}\bar{h},\end{aligned} \tag{4}$$

where $\mathrm{F}\big(\bar{h}\big)$ is the cumulative distribution function for $\mathrm{P}\big(\bar{h}\big)$, i.e., $\mathrm{F}\big(\bar{h}\big)=\int_0^{1/2}\mathrm{P}\big(\bar{h}\big)\mathrm{d}\bar{h}+\int_{1/2}^{\bar{h}}\mathrm{P}(\theta)\mathrm{d}\theta=\int_0^{1/2}1\mathrm{d}\bar{h}+\int_{1/2}^{\bar{h}}\mathrm{P}(\theta)\mathrm{d}\theta=\frac{1}{2}+\int_{1/2}^{\bar{h}}\mathrm{P}(\theta)\mathrm{d}\theta$. Based on the formulated distribution of

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

the insurance risk and the concept of risk-adjusted premium, the cyber-insurer can determine the premium as follows:

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

where $\omega(x, \gamma)$ is an increasing concave function of x and belongs to the families of elementary transforms given in Section 5 of [29]. Without loss of generality, we adopt the PH transform in our study, i.e., $\omega(x, \gamma) = x^{\frac{1}{\gamma}}$, $\gamma \geq 1$ in Section 5.1 of [29]. Then, the corresponding premium can be expressed as follows:

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

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

3.2 System Model

3.2.1 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 $\mathrm{F_U}$ 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 $\mathrm{Pr}\,[\mathrm{j\ buys\ the\ service}]$ denote the probability that user j subscribes to the service, then, the utility of user i can be expressed as follows [33]:

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

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, is the price of the service for user i.[2] The forth term of (7), i.e., $\alpha \sum_{j \in \mathcal{N}} g_{ij} \mathrm{Pr}[\mathrm{j\ buys\ the\ service}]$, represents the positive social externality among the users. g_{ij} is the element of the externality matrix $\mathbf{G}$ [17], [18] 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 $g_{ii} = 0$, $\forall i \in \mathcal{N}$.[3] Finally, α is a constant controlling the level of social externality for the entire network.

3.2.2 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:

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

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). Thesecond 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., $\frac{T}{T_0} N_{\mathrm{T}} q \int_{1/2}^{1} [1 - \int_{1/2}^{t} \mathrm{P}(\theta)\mathrm{d}\theta]^{1/\gamma}\mathrm{d}t$, 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:

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

where the first term is the premium paid by the blockchain provider. The second term, i.e., $\mathrm{P}\big(\bar{h}\big)\bar{h}\frac{T}{T_0}N_{\mathrm{T}}q$, is obtained as 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 [34]. Here, we define $\sigma\big(\bar{h}, \gamma\big) = \sigma_1\big(\bar{h}\big)\sigma_2(\gamma)$, where $\sigma_1\big(\bar{h}\big)$ is an increasing convex function of $\bar{h}$ with the following properties:

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

[2] Note here 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.

[3] Note here that our model can also be used to analyze the scenario that the users may act independently. For example, if $g_{ij} = g_{ji} = 0$, user j has zero level of the social externality (influence) on user i and vice versa. Hence, users i and j act independently.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

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, $\sigma_2(\gamma)$ is an increasing convex function of γ and $\sigma_2(\gamma)|_{\gamma=1} = 0$. 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:

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

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.

3.3 Stackelberg Game Formulation

Considering the payoff functions of the market entities given in (7), (8), (9), it is natural to model the interactions in the blockchain service market as a two-stage game. In the first upper stage, the blockchain provider determines the price of the blockchain service, namely, the levels of acceptable transaction fees for each user p_i, and its ratio of investment in computing resources $\bar{h}$. Meanwhile, the cyber-insurer decides on the premium coefficient γ by considering the insurance risk transferred from the blockchain provider. In the second lower stage, each user determines whether it will buy the blockchain service or not based on the prices and the investment ratio set by the blockchain provider. Accordingly, the interactions among the blockchain provider, the cyber-insurer and the users are formulated as a two-leader-multi-follower Stackelberg game. Specifically, the mutual interaction between the blockchain provider and cyber-insurer forms a noncooperative two-player leader-level subgame for achieving the equilibrium of the service price, the investment ratio, and the cyber-insurance policy. Then, the interaction among a number of users forms the follower-level noncooperative subgame for determining the service demand from the blockchain provider.[4] The Stackelberg game can be formally defined as follows.

(1) *User-level noncooperative subgame*: Given the fixed investment ratio $\bar{h}$ as well as the price vectors $\mathbf{p} = \left[p_1, p_2, \ldots, p_{|\mathcal{N}|}\right]^{\top}$, the user-level (follower) noncooperative subgame is defined by a four-tuple $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$, where

- $\mathcal{N}$ is the set of active users;
- $\mathcal{X} = \left\{\left[x_1,\ x_2,\ \ldots x_{|\mathcal{N}|}\right]^{\top}\middle| x_i \in [0,1], i \in \mathcal{N}\right\} \subset \mathbb{R}^{|\mathcal{N}|}$ defines the domain of $\mathbf{x}$ as an M-polyhedron;
- $\mathbf{x} = \left[x_1, x_2, \ldots x_{|\mathcal{N}|}\right]^{\top}$ is the vector of the users' decision variables, where x_i is the service demand of user i and $\mathbf{x} \in \mathcal{X}$;
- $\mathbf{u} = \left[u_1,\ u_2, \ldots,\ u_{|\mathcal{N}|}\right]^{\top}$ is the vector of the users' utilities with the given strategy $\mathbf{x}$, where $\forall i \in \mathcal{N}$, and u_i is given in (7).

(2) *Leader-level noncooperative subgame*: Assume that the users' demand $\mathbf{x}$ has been found to be a parametric equilibrium as a function, i.e., mapping, of the leaders' strategies. Then, the blockchain provider and the cyber-insurer form a noncooperative game as a five-tuple $\mathcal{G}_{\mathrm{L}} = \{\left[\mathbf{p}^{\top}, \bar{h}\right]^{\top}, \mathcal{D}_{\mathrm{P}}, \gamma, \mathcal{D}_{\mathrm{I}}, \Pi\}$, where

- $\left[\mathbf{p}^{\top}, \bar{h}\right]^{\top} = [p_1, p_2, \ldots, p_{|\mathcal{N}|, \bar{h}]}^{\top}$ is the strategy vector of the service prices and the investment ratio set by the blockchain provider with $p_i > 0, \forall i \in \mathcal{N}$ and $\bar{h} \in \left[\frac{1}{2}, 1\right)$;
- $\mathcal{D}_{\mathrm{P}} = \left\{\left[\mathbf{p}^{\top}, \bar{h}\right]^{\top}\middle| p^{\mathrm{u}} \geq p_i > 0, \forall i \in \mathcal{N},\ \ \bar{h} \in \left[\frac{1}{2}, 1\right)\right\}$ is the domain of the prices and investment ratio of the blockchain provider, where p^{u} is the upper bound of the price p_i imposed by the government or market regulators;
- γ is the cyber-insurer's premium coefficient for premium determination;
- $\mathcal{D}_{\mathrm{I}} = \{\gamma | \gamma^{\mathrm{u}} \geq \gamma > 1\}$ defines the domain of γ, where γ^{u} is the upper bound of γ imposed by the government or regulators;
- $\Pi = \left[\Pi_{\mathrm{p}}, \Pi_{\mathrm{I}}\right]^{\top}$ is the profit vector for the blockchain provider and the cyber-insurer.

4 Game Equilibrium Analysis

Based on the formulation of the Stackelberg game in Section 3.3, we are ready to analyze the market equilibrium using backward induction. We first obtain the Nash Equilibrium (NE) of the user-level noncooperative 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 noncooperative subgame $\mathcal{G}_{\mathrm{u}}$ by solving the bounded linear complementarity problem of the subgame [33]. Then, we substitute the parametric NE of $\mathcal{G}_{\mathrm{u}}$ into the leader-level noncooperative 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 noncooperative subgame is negative definite. Hence, we prove that the Stackelberg Equilibrium (SE) of the market game exists and is unique.

4.1 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

[4] The reason that the users are in the same level, i.e., lower-level, is that they have the same set of information and make decisions simultaneously. This is different from the blockchain provider that usually invests in the infrastructure and buys the cyber-insurance first to improve the security level of its blockchain-based service and then provides the service to the users. The cyber-insurer sells the cyber-insurance to the blockchain provider and forms a noncooperative relationship with the blockchain provider. As such, the cyber-insurer and blockchain provider make their decisions simultaneously and hence before the users. As a result, the blockchain provider and cyber-insurer are considered to be the leaders and their problems are defined in the upper-level.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

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 $u_i = 0$:

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

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

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

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

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

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

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

Furthermore, (15) can be rewritten into the following matrix form:

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

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 are ready to investigate the properties of the NE in the user-level noncooperative 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.

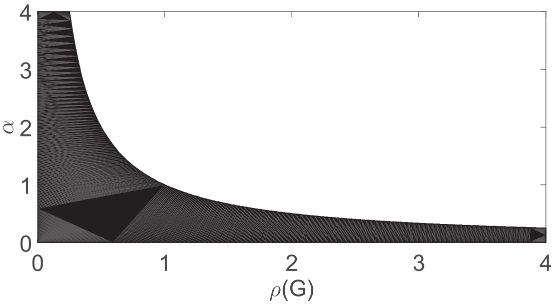


Fig. 2. An illustration of Assumption 1.

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 [33]. It is a linear instance of the general mixed complementarity problems discussed in [35]. As discussed in [35], 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.[5]

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.[6]

Based on Theorem 6.2.3 in [36], "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 $\mathcal{G}_\mathrm{u}$. Thereby, 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:

- $\mathcal{S}_0 = \Big\{i\Big|\big\{\big(1+\bar{h}\big)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\big\}_i < 0, \forall i \in \mathcal{N}\Big\}$ is the set of users which will not buy the blockchain service,
- $\mathcal{S}_1 = \Big\{i\Big|\big\{\big(1+\bar{h}\big)\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\big\}_i > 0, \forall i \in \mathcal{N}\Big\}$ is the set of users which surely will buy the blockchain service,
- $\mathcal{S} = \mathcal{N}\backslash(S_0 \cup S_1) = \{i|\{(1+\bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i = 0, \forall i \in \mathcal{N}\}$ is the set of users which buy the blockchain service with a probability over $[0, 1]$.

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*

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

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

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

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

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 $\{(1+\bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_i = 1 + \bar{h} + \alpha\sum_{j\in\mathcal{N}} g_{ij}x_j - x_i - p_i$ 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 $\{(1+\bar{h})\mathbf{1} - \mathbf{p}^* - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}^*\}_l > 0$. Since $\{(1+\bar{h})\mathbf{1} - \mathbf{p} - (\mathbf{I} - \alpha\mathbf{G})\mathbf{x}\}_l = 1 + \bar{h} + \alpha\sum_{j\in\mathcal{N}} g_{ij}x_j - x_l - p_l$ 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

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

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

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

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

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

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

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 (21) by $(\mathbf{I} - \alpha\mathbf{G})^{-1}$, then, the optimal solution to the system of interdependent demands, or equivalently, the NE to the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$, is

$$\mathbf{x}^* = (\mathbf{I} - \alpha\mathbf{G})^{-1}[(1+\bar{h})\mathbf{1} - \mathbf{p}]. \tag{22}$$

The proof is completed. □

4.2 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 provided that the other player′ strategy is unchanged [37]. In what follows, we first prove that an NE exists in the leader-level noncooperative subgame $\mathcal{G}_{\mathrm{L}}$. Then, we prove that this NE is unique.

Substituting the optimal demand of the users derived in (22) into the profit function of the blockchain provider, we can rewrite (8) into a matrix form as follows:

$$\begin{aligned}\Pi_{\mathrm{p}}(\bar{h}, \mathbf{p}) = \mathbf{p}^\top(\mathbf{I} - \alpha\mathbf{G})^{-1}[(1+\bar{h})\mathbf{1} - \mathbf{p}] - \frac{a\bar{h}}{1-\bar{h}} + \bar{h}\frac{T}{T_0}N_{\mathrm{T}}r\\ - \frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1 - \int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]^{1/\gamma}\mathrm{d}t.\end{aligned} \tag{23}$$

The first-order partial derivative of the profit of blockchain provider as well as that of the cyber-insurer are shown in (24), and the second-order partial derivatives of the blockchain provider and cyber-insurer are shown in (25). Then, we can obtain the following theorem regarding the NE of the leader-level noncooperative 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. Please refer to Appendix A,, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TSC.2018.2876846 in [38] for the proof. □

Next, we show the uniqueness of the NE in the leader-level noncooperative subgame in Theorem 4, and hence the Stackbelberg equilibrium is unique.

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. Please refer to Appendix B, available in the online supplemental material in [38] for the proof. □

4.3 Equilibrium Searching for Leader-Level Noncooperative Subgame

Since in our previous discussion we have provided the closed-form NE to the user-level noncooperative subgame $\mathcal{G}_{\mathrm{u}}$ in (22), we only have to focus on the derivation of the NE in the leader-level noncooperative subgame $\mathcal{G}_{\mathrm{L}}$. Given (22), the search for the SE is reduced to the search of the NE of a two-player noncooperative game. By Theorem 3, we know that $\mathcal{G}_{\mathrm{L}}$ is a concave game with the convex and compact strategy space (see also the proof to Theorem 3). By Theorem 4, we know that $\mathcal{G}_{\mathrm{L}}$ admits a unique NE when the condition given therein is satisfied. This suggests the use of the iterative best response to solve for the NE in $\mathcal{G}_{\mathrm{L}}$. The iterative best-response algorithm is described in Algorithm 1, and its convergence property is guaranteed by Theorem 5.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

$$\begin{cases} \frac{\partial \Pi_{\mathrm{P}}}{\partial \bar{h}} = \mathbf{p}^{\top}(\mathbf{I}-\alpha\mathbf{G})^{-1}\mathbf{1} - \frac{a}{\left(1-\bar{h}\right)^{2}} + \frac{1}{\gamma}\frac{T}{T_0}N_{\mathrm{T}}r, \\ \frac{\partial \Pi_{\mathrm{P}}}{\partial \mathbf{p}} = (\mathbf{I}-\alpha\mathbf{G})^{-1}\left[\left(1+\bar{h}\right)\mathbf{1}-\mathbf{p}\right], \\ \frac{\partial \Pi_{\mathrm{I}}}{\partial \gamma} = -\frac{1}{\gamma^2}\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]^{1/\gamma}\ln\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]\mathrm{d}t - \left(\bar{h}-\frac{1}{2}\right)^{3}[(\beta+1)\gamma^{\beta}-\beta\gamma^{\beta-1}], \end{cases} \tag{24}$$

$$\begin{cases} \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \mathbf{p}^2} = -(\mathbf{I}-\alpha\mathbf{G})^{-1}, \\ \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \mathbf{p}\partial \bar{h}} = (\mathbf{I}-\alpha\mathbf{G})^{-1}\mathbf{1}, \\ \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \mathbf{p}\partial \gamma} = \left(\frac{\partial^2 \Pi_{\mathrm{I}}}{\partial \gamma\partial \mathbf{p}}\right)^{\top} = \mathbf{0}, \\ \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \bar{h}\partial \mathbf{p}} = \mathbf{1}^{\top}(\mathbf{I}-\alpha\mathbf{G})^{-1}, \\ \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \bar{h}^2} = -\frac{2a}{\left(1-\bar{h}\right)^{3}}, \\ \frac{\partial^2 \Pi_{\mathrm{P}}}{\partial \bar{h}\partial \gamma} = 0, \end{cases} \quad \begin{cases} \frac{\partial^2 \Pi_{\mathrm{I}}}{\partial \gamma\partial \bar{h}} = -3\left(\bar{h}-\frac{1}{2}\right)^{2}[(\beta+1)\gamma^{\beta}-\beta\gamma^{\beta-1}], \\ \frac{\partial^2 \Pi_{\mathrm{I}}}{\partial \gamma^2} = \frac{2}{\gamma^3}\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]^{1/\gamma}\ln\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]\mathrm{d}t \\ \qquad +\frac{1}{\gamma^4}\frac{T}{T_0}N_{\mathrm{T}}q\int_{1/2}^{1}\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]^{1/\gamma}\ln^2\left[1-\int_{1/2}^{t}\mathrm{P}(\theta)\mathrm{d}\theta\right]\mathrm{d}t \\ \qquad -\left(\bar{h}-\frac{1}{2}\right)^{3}[\beta(\beta+1)\gamma^{\beta-1}-\beta(\beta-1)\gamma^{\beta-2}]. \end{cases} \tag{25}$$

Algorithm 1. Iterative Best-Response for Searching Leader Noncooperative Subgame NE

```
Initialization: Select any feasible initial strategies as $\mathbf{s}_{\mathrm{I}}(0) = \gamma(0)$, $\mathbf{s}_{\mathrm{P}}(0) = [\mathbf{p}(0), \bar{h}(0)]^{\top}$ and set $t = 0$.
while $\mathbf{p}(0), \bar{h}(0), \gamma(0)$ do not satisfy the termination condition do
    for all $k = \{\mathrm{P}, \mathrm{I}\}$ do
        Set the adversary joint strategies as
            $\mathbf{s}_k(t+1) = \arg\max_{\mathbf{s}_k} \Pi_k(\mathbf{s}_k, \mathbf{s}_{-k}(t))$ s.t. $\mathbf{s}_k \in \mathcal{D}_k$,    (26)
        where $\mathbf{s}_{-k}$ represents the adversary's strategy.
    end for
    Set $t \leftarrow t+1$.
end while
```

Theorem 5. *If the condition in Theorem 4 is satisfied, Algorithm 1 converges to the unique SE from anywhere of the strategy domains of the blockchain provider and cyber-insurer.*

Proof. With the concavity of the payoff functions Π_{P} and Π_{I} proved in Appendix A,, available in the online supplemental material in [38] and the negative definite Jacobian matrix $\mathbf{J}$ proved in Appendix B, available in the online supplemental material in [38], Theorem 5 immediately follows Theorem 10 in [39]. □

5 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 $\left[5 \times 10^{-4}, 8 \times 10^{-4}\right]$ according to the parameter setting in [33]. 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. Note that our proposed concept of cyber-insurer and blockchain service is the first in the literature. There is no similar work with which we can compare on a reasonably fair basis. For example, the authors in [40] formulated a bilevel game to investigate the interactions among the attackers, users, and cyber-insurer in computer networks. However, since we incorporate the specific and unique feature of the blockchain technology, i.e., successful attack probability in (1), reasonable comparison is therefore not applicable.

5.1 Numerical Results

5.1.1 Demonstration of Best Response and NE

Fig. 3 demonstrates the NE obtained from interative best responses with the given simulation parameters. In Fig. 3a, the profit of the cyber-insurer changes with the different premium charged to the blockchain provider. According to our previous discussion, the profit of the cyber-insurer is controlled by the value of γ. For a given weak level of the social externality, e.g., $\alpha = 6.5 \times 10^{-4}$, there is a corresponding strategy where the cyber-insurer's profit is maximized.

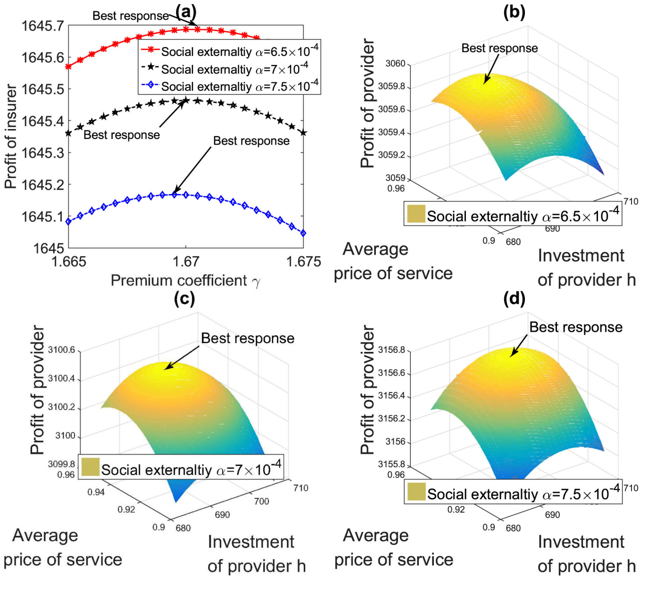


Fig. 3. Best response.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

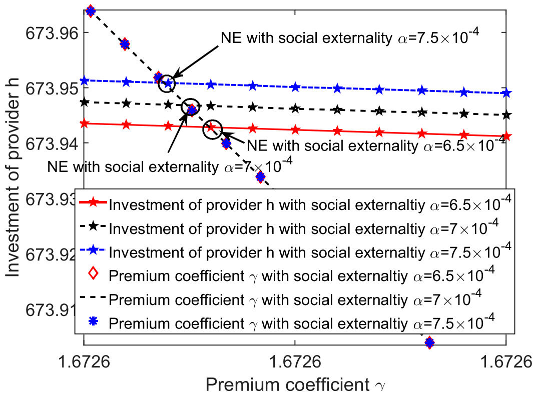


Fig. 4. Nash equilibrium.

The strategy is marked by the arrowhead of "Best response" and constitutes the NE strategy of the cyber-insurer under the given social externality setting. We observe from Fig. 3a that as a function of the premium coefficient γ, the profit is unimodal, and thus the optimal solution can be obtained analytically. Similarly, there exists the optimal point in each of Fig. 3b, 3c, and 3d for the blockchain provider. The optimal points are marked by the arrowhead of "Best response" and constitute the NE strategy of the blockchain provider under different levels of social externality. Note that all the results shown in the figures are obtained given that the users play the NE in the user-level game.

Fig. 4 illustrates the equilibrium strategies for the investment of the blockchain provider and the premium coefficient γ for the cyber-insurer under different levels of social externality. The NE is the point at which the best responses for the blockchain provider and cyber-insurer intersect. Again, this is given that the users play the NE in the user-level game. Under different levels of social externality, different NE are observed. As the level of social externality grows higher, i.e., a decision of one user has stronger effect to the decisions of other users, the other users are more likely to buy the same service if one user buys the service. As expected, when the level of social externality grows higher, the users are more likely to also buy the service, the blockchain provider has more money and more incentives to invest in the infrastructure and accordingly the premium coefficient γ decreases (see Fig. 4). The reason for this result is explained in the subsequent discussions.

5.1.2 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. 5, 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 $\alpha = 7.5 \times 10^{-4}$ than with $\alpha = 6.5 \times 10^{-4}$. As a result, the stronger social externality reduces the successful attack probability at a higher rate. Correspondingly, as shown in Fig. 5f, 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. 5b.

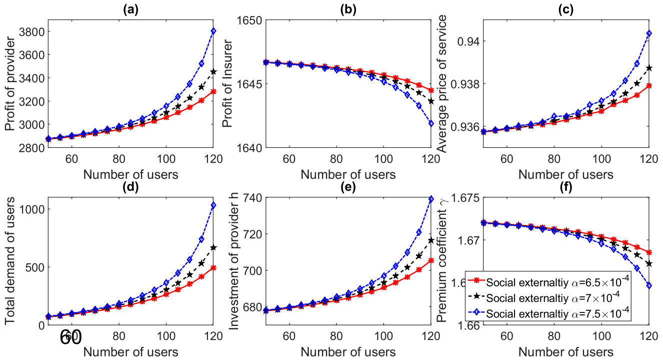


Fig. 5. The results with increasing number of users.

5.1.3 The Impact of Social Externality

Fig. 6 illustrates the impact of social externality on the payoffs of the three market entities with 100 users. As expected, the users' total service demand increases as the social externality becomes stronger (see Fig. 6d). From Fig. 6a and 6b, we observe that the profit of the blockchain provider increases while the profit of the cyber-insurer decreases. The reason is that the users with stronger social externality are more sensitive to the security level of the blockchain service, and the security level depends on the investment ratio of the blockchain provider. Therefore, the blockchain provider will raise its investment as the social externality increases, which decreases the probability of successful double-spending attacks. Accordingly, the cyber-insurer reduces its premium as shown in Fig. 6f, and this will lead to the decrease of the cyber-insurer's profit. Moreover, since the investment by the blockchain provider increases, the security level of the blockchain service is improved, and thus the service demand of users increases. This situation results in the increase of the blockchain provider's profit.

Additionally, recall that the investment ratio of the blockchain provider depends on not only the investment from the blockchain provider, but also the computing resource owned by the attackers. For this reason, in our performance evaluation, we also vary the attacker's investment in computing resource by considering three cases with $a = 50$, $a = 100$ and $a = 150$, respectively. From Fig. 6f, we observe that the decreasing rate of the curves becomes higher as the attacker's investment increases, which means that decreasing rate of the premium becomes higher as the attacker's investment

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

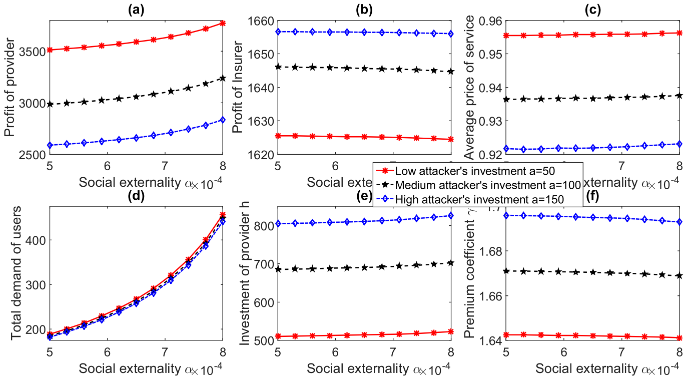


Fig. 6. The results with increasing social externality.

increases. The reason is that the increasing rate of the investment by the blockchain provider becomes faster as the attacker's investment increases, and this also results in a higher decreasing rate of the successful attack probability. Consequently, the decreasing rate of the probability of paying claim is the highest with $a = 150$ which is the largest attacker's investment.

5.1.4 *The Impact of Attacker's Computing Resource*

Finally, we evaluate in Fig. 7 the impact of the attackers' computing resource on the performance of the users, the blockchain 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 Fig. 7a and 7b 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. 7e). 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. 7e 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. 7f, 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 Fig. 7c and 7d). Consequently, this reduces the revenue and profit of the blockchain provider.

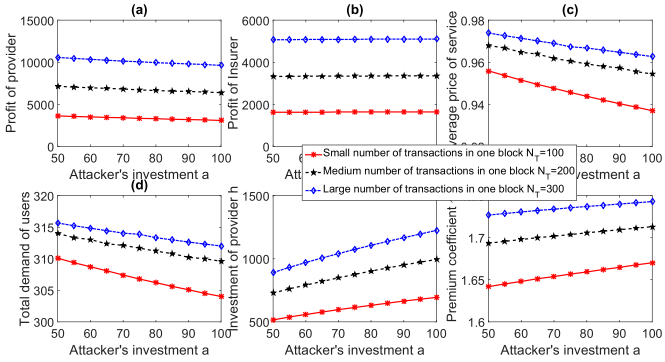


Fig. 7. The result with increasing attacker's computing resource.

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. 7e, 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. 7f). 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 Fig. 7c and 7d, where the decreasing rates of both the total user demand and the service price shrink as N_{T} increases.

6 Conclusion

In this paper, we have proposed a risk management framework of the blockchain service market by introducing the cyber-insurance as a mean for protecting financially the blockchain provider from double-spending attacks. We have modeled the interaction among the blockchain provider, the cyber-insurer and the users in the market 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

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.

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.

Acknowledgments

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, and EMA Energy Resilience under Grant NRF2017EWT-EP003-041.

References

[1] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, “Untangling blockchain: A data processing view of blockchain systems,” *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[2] M. Bartoletti and L. Pompianu, “An empirical analysis of smart contracts: platforms, applications, and design patterns,” *arXiv: 1703.06322*, 2017.

[3] H. Kopp, D. Mdinger, F. Hauck, F. Kargl, and C. Bsch, “Design of a privacy-preserving decentralized file storage with financial incentives,” in *Pro. IEEE Eur. Symp. Security Privacy Workshops*, Paris, France, Apr. 2017, pp. 14–22, doi: 10.1109/EuroSPW.2017.45.

[4] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, “A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain,” *IEEE Access*, vol. 5, pp. 17465–17477, Jun. 2017, doi: 10.1109/ACCESS.2017.2720760.

[5] J. Zou, b. ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, “A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services,” *IEEE Trans. Serv. Comput.*, p. 1, Apr. 2018, doi: 10.1109/TSC.2018.2823705.

[6] M. Conti, S. K. E., C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” *IEEE Commun. Surveys Tut.*, p. 1, May 2018, doi: 10.1109/COMST.2018.2842460.

[7] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in *Proc. ACM Conf. Comput. Commun. Security*, Oct. 2012, pp. 906–917.

[8] 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 Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, 2017.

[9] X. Huang, C. Xu, P. Wang, and H. Liu, “LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem,” *IEEE Access*, vol. PP, no. 99, p. 1, Mar. 2018, doi: 10.1109/ACCESS.2018.2812176.

[10] K. Kotobi and S. G. Biln, “Blockchain-enabled spectrum access in cognitive radio networks,” in *Proc. Wireless Telecommun. Symp.*, Apr. 2017, pp. 1–6.

[11] L. Ghiro, L. Maccari, and R. L. Cigno, “Proof of networking: Can blockchains boost the next generation of distributed networks?,” in *Proc. 14th Annu. Conf. Wireless On-Demand Netw. Syst. Serv.*, Feb. 2018, pp. 29–32.

[12] W. Wang, D. Niyato, P. Wang, and A. Leshem, “Decentralized caching for content delivery based on blockchain: A game theoretic perspective,” presented at the *IEEE ICC Next Generation Netw. Internet Symp.*, Kansas City, MO, USA, May 2018.

[13] S. Muhammad, M. Aziz, K. Charles, K. Kevin, and N. Laurent, “Countering double spending in next-generation blockchains,” presented at the *IEEE Int. Conf. Commun.*, Kansas City, MO, USA, May 2018.

[14] 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 *Proc. IFIP Netw. Conf.*, 2013, pp. 1–9.

[15] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, “Cyber-insurance survey,” *Comput. Sci. Rev.*, vol. 24, pp. 35–61, 2017.

[16] AWS, “Aws blockchain partners.” [Online]. Available: https://aws.amazon.com/cn/partners/blockchain/, 2018.

[17] 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 J. Select. Areas Commun.*, vol. 35, no. 2, pp. 449–462, Feb. 2017.

[18] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Y. Zhang, “Economic analysis of network effects on sponsored content: A hierarchical game theoretic approach,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[19] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, Jul.-Sep. 2016.

[20] J. L. Zhao, S. Fan, and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue,” *Financial Innovation*, vol. 2, no. 1, 2016, Art. no. 28.

[21] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, vol. 4, pp. 2292–2303, May 2016.

[22] H. Wang, K. Chen, and D. Xu, “A maturity model for blockchain adoption,” *Financial Innovation*, vol. 2, no. 1, pp. 12, 2016.

[23] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in *Proc. 34th Annu. Int. Conf. Theory Appl. Cryptographic Tech. Part II*, Apr. 2015, pp. 281–310.

[24] S. Feng, Z. Xiong, N. Dusit, P. Wang, and S. Wang, “Joint pricing and security investment for cloud-insurance: A security interdependency perspective,” presented at the *IEEE Wireless Commun. Netw. Conf.*, Barcelona, Spain, Apr. 2018.

[25] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-ng: A scalable blockchain protocol.,” in *Proc. 13th Usenix Conf. Netw. Syst. Des. Implementation*, 2016, pp. 45–59.

[26] M. Rosenfeld, “Analysis of hashrate-based double spending,” *arXiv:1402.2009*. [Online]. Available: https://arxiv.org/abs/1402.2009, 2014.

[27] C. Grunspan and R. Pérez-Marco, “Double spend races,” *arXiv: 1702.02867*. [Online]. Available: https://arxiv.org/abs/1702.02867, 2017.

[28] S. Wang, “Insurance pricing and increased limits ratemaking by proportional hazards transforms,” *Insurance: Math. Econ.*, vol. 17, no. 1, pp. 43–54, 1995.

[29] S. Wang, “Premium calculation by transforming the layer premium density,” *ASTIN Bulletin: The J. IAA*, vol. 26, no. 1, pp. 71–92, 1996.

[30] D. Denneberg, “Premium calculation: Why standard deviation should be replaced by absolute deviation,” *ASTIN Bulletin: The J. IAA*, vol. 20, no. 2, pp. 181–190, 1990.

[31] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in *Proc. ACM Conf. Comput. Commun. Security*, 2012, pp. 906–917.

[32] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system. Bitcoin,” [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2009.

[33] F. Bloch and N. Quérou, “Pricing in social networks,” *Games Econ. Behavior*, vol. 80, pp. 243–261, 2013.

[34] F. Bloch, G. Genicot, and D. Ray, “Informal insurance in social networks,” *J. Econ. Theory*, vol. 143, no. 1, pp. 36–58, 2008.

[35] A. Simsek, A. Ozdaglar, and D. Acemoglu, “On the uniqueness of solutions for nonlinear and mixed complementarity problems,” Massachusetts Inst. Technol., [Online]. Available: https://economics.mit.edu/files/204, 2005.

[36] A. Berman and R. J. Plemmons, *Nonnegative Matrices in the Mathematical Sciences*. Philadelphia, PA, USA: SIAM, 1994.

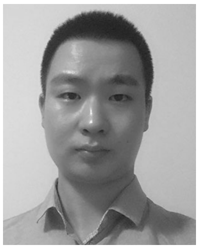
[37] M. J. Osborne, *An Introduction to Game Theory*, vol. 3. London, U.K. : Oxford Univ. press, 2004.

[38] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, “On cyber risk management of blockchain networks: A game theoretic approach,” *arXiv: 1804.10412*. [Online]. Available: https://arxiv.org/abs/1804.104122018, 2018.

[39] G. Scutari, F. Facchinei, J.-S. Pang, and D. P. Palomar, “Real and complex monotone communication games,” *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4197–4231, Jul. 2014.

[40] R. Zhang, Q. Zhu, and Y. Hayel, “A bi-level game approach to attack-aware cyber insurance of computer networks,” *IEEE J. Select. Areas Commun.*, vol. 35, no. 3, pp. 779–794, Mar. 2017.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.



Shaohan Feng received the BS degree from the School of Mathematics and Systems Science, Beihang Universiy, Beijing, China, in 2014 and the MS degree from the School of Mathematical Sciences, Zhejiang University, Hangzhou, China, in 2016. He is currently working toward the PhD degree in the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His current research interest includes resource management in cloud computing and communication networks. He is a student member of the IEEE.

Wenbo Wang (S'13-M'17)received the BS and MS degrees from the School of Automation, Beijing Institute of Technology, Beijing, China, and the PhD degree in computing and information sciences from Rochester Institute of Technology, Rochester, New York, in 2016. He is currently a research fellow with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include cross-layer optimization and mechanism design in multimedia wireless networks, cognitive radio networks, green wireless networks and Internet of Things (IoT). He is a member of the IEEE.

Zehui Xiong received the BEng degree with honors in telecommunication engineering from Huazhong University of Science and Technology, Wuhan, China, in 2016. He is currently working towards the PhD degree in the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include network economics, game theory for resource management, market models and pricing. He is a student member of the IEEE.

Dusit Niyato (M'09-SM'15-F'17) received the BEng from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand, in 1999 and the PhD degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include internet of things (IoT) and network resource pricing. He is a fellow of the IEEE.

Ping Wang (M'08-SM'15) received the PhD degree in electrical engineering from the University of Waterloo, Canada, in 2008. She is currently an associate professor with the Department of Electrical Engineering and Computer Science, York University, Canada. Before that, she was with Nanyang Technological University, Singapore. Her current research interests include resource allocation in multimedia wireless networks, cloud computing, and smart grid. She was a co-recipient of the Best Paper Awards from the IEEE International Conference on Communications in 2007, from the IEEE Wireless Communications and Networking Conference in 2012, and from IEEE Communications Society (ComSoc) Green Communications & Computing Technical Committee (TCGCC) in 2018. She has been serving as an associate editor for several journals including the *IEEE Transactions on Wireless Communications*, the *EURASIP Journal on Wireless Communications and Networking*, and the *International Journal of Ultra Wideband Communications and Systems*. He is a senior member of the IEEE.

Shaun Shuxun Wang received the BSc degree from Peking University, China, in 1986 and the PhD degree from the University of Waterloo, Canada, in 1993. He is a professor with the Nanyang Technological University, Singapore. He is the principal investigator of the National Research Foundation and Tel Aviv University (TAU) project (2017-2019) Quantification of Cyber Risk. His research interests include risk metrics for information security, big data and data integrity.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 08:05:38 UTC from IEEE Xplore. Restrictions apply.