Cyber Insurance Design for Validator Rotation in Sharded Blockchain Networks: A Hierarchical Game-Based Approach

Jing Li, Dusit Niyato, *Fellow, IEEE*, Choong Seon Hong, *Senior Member, IEEE*, Kyung-Joon Park, *Senior Member, IEEE*, Li Wang, *Senior Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—Sharding is a promising solution to achieving scalability within the blockchain network. A sharded blockchain network consists of a beacon chain and several committees powered by the participants (i.e., validators) through the Proof-of-Stake (PoS) consensus protocol. Efficient and scalable as it can be, the sharded blockchain based on PoS is vulnerable to discouragement attack. A discouragement attack occurs when malicious validators censor messages to discourage validators from participating in the network. Furthermore, no rate-limiting validator rotation (enter/exit quickly) makes it more challenging to detect such an attack. In this paper, considering the undetermined rotation and the discouragement attack, we render the beacon chain an intermediary, allowing the beacon chain to interact with validators and the cyber-insurer, aiming to encourage the validators' stable rotation through insurance compensation. Specifically, we utilize a two-stage hierarchical game-based model to formulate the complicated interactions under the cyber insurance framework. In the first stage, the beacon chain develops compensatory strategies according to the insurer's profile. In the second stage, the beacon chain designs a series of contracts for validators, including insurance items, compensatory strategies, and rotation requirements. Consequently, the proposed scheme incentivizes validators to remain online by transferring risk to the cyber insurer and enables the sharded blockchain network to weaken the attack's impact through validators' stable rotation. This paper presents closed-form solutions for the proposed model, in which the beacon chain and the cyber insurer can gain maximized profits. The simulations demonstrate the feasibility and superiority of the proposed model.**

***Index Terms*—Blockchain, sharding, cyber insurance, discouragement attack, Stackelberg game, contract theory.**

Manuscript received October 9, 2020; revised March 10, 2021; accepted May 3, 2021. Date of publication May 6, 2021; date of current version September 9, 2021. This work is partially supported by NSF EARS-1839818, CNS1717454, CNS-1731424, and CNS-1702850. This work is also partially supported in part by the National Natural Science Foundation of China under Grant No. U2066201 and Grant 61871416, and in part by the Beijing Municipal Natural Science Foundation under Grant L192030. The associate editor coordinating the review of this article and approving it for publication was A. Veneris. *(Corresponding author: Jing Li.)*

Jing Li is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA (e-mail: jli84@uh.edu).

Dusit Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798 (e-mail: dniyato@ntu.edu.sg).

Choong Seon Hong is with the Department of Computer Science and Engineering, Kyung Hee University, Yongin-si 446-701, South Korea (e-mail: cshong@khu.ac.kr).

Kyung-Joon Park is with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu 42988, South Korea (e-mail: kjp@dgist.ac.kr).

Li Wang is with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100088, China (e-mail: liwang@bupt.edu.cn).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/TNSM.2021.3078142

I. Introduction

BLOCKCHAIN is an ingenious invention of Nakamoto and is described in the remarkable project [1]. It is a permissionless platform with the characteristics of decentralization, tamper-resistance and transparency [2]. With the advent of Bitcoin (BTC) [3], blockchain technology has acquired significant attention. Ethereum is another world's leading programmable project [4] based on the blockchain technology framework [5]. Unlike Bitcoin, mostly focusing on financial issues, Ethereum aims to be a "World Computer," which allows everyone to be a developer to write its own code and create new kinds of applications [5]. A blockchain is constructed by a series of undeniable blocks, where each block is generated and confirmed by the different parties. These blocks are connected before and after within one chain. The core technology of coordinating all the participants across the distributed network is called consensus protocol. The first practicable consensus protocol in the blockchain framework is known as the Proof of Work (PoW) [1], in which miners can only win the opportunity of mining block by competing in hash rate against others. In the early development stage of the blockchain, PoW indeed provides the benefits, such as Denial-of-Service (DoS) attack defense and Sybil attack defense. The success of Bitcoin [4] has proved this point.

Considering the aggravation of hash rate competition causes a massive waste of resources, numerous researchers seek new alternatives that serve the same function. Proof of Stake (PoS) is first proposed in the Bitcoin Forum [6], i.e., the leader selection relies on the number of stakes rather than the computational resources. That means the leader selection of PoS follows a relative deterministic way compared with that of PoW, such as by turns. Moreover, there is no need to issue more rewards to compensate for energy consumption. As described above, the significant advantages of PoS can

be summarized in three aspects: comparable decentralization, economic saving, and security [7].

With the extensive research on consensus protocols, more potential attacks are being studied. Cyber-attacks can take more implicit forms. Vitalik explores a new type of attack that may disrupt the whole blockchain network, which is called *Discouragement Attack* [8]. A discouragement attack means the attackers would act maliciously inside a consensus mechanism to gradually reduce other validators' revenue, even at a certain cost to themselves. The final purpose is to encourage the validators to drop out of the mechanism. It is worth noting that a discouragement attack is the cheapest way to corrupt the incentive scheme of a PoS based blockchain. In the best case, attackers can do this without losing a cent only by censoring the honest nodes and driving their reward to zero. Consequently, they will encourage rational validators to drop out of the system [9].

Recently, Vitalik published a new idea about the validator sharding set update [10], which prevented the validators from withdrawing. In the previous design, every validator is able to exit/enter the sharding committees at the end of each round [11]. That means the malicious validators can perform a large-scale attack without being detected because the system cannot perform the detection in a short time. A better way is to set a withdrawal delay, which means the validators must wait in a queue for withdrawing before being free to exit the committee. In a nutshell, this idea is to make time for the system to detect the attack and malicious nodes, allowing the system to prevent the discouragement attack. However, there are still some open questions, i.e., determining the withdrawal delay for all the validators and selecting the validators in a queue. Considering the risk introduced by the discouragement attack, the blockchain network requires an appropriate incentive scheme to encourage the validators to stay online and neutralize the whole network's risk.

A. Related Work

As the core of blockchain technology, the consensus protocol has been the research priority for blockchain experts. With the advantage of energy-efficient, PoS is increasingly the focus of research attention. Here are some PoS schemes but are not completely different from the framework of PoW, e.g., Proof of Activity [12], Proof of Burn [13] and Proof of Luck [14].

The joint efforts from both industry and academia areas make great strides in moving blockchain technology forward, which brings opportunities and benefits for a wide range of areas, including finance, business, industry. IBM developed a blockchain platform based on Hyperledger Fabric [15], providing solutions and services for multiple institutions [16], including financial services, supply chain, manufacturing, media, and entertainment, retail. The applications of blockchain technology to some hot industrial areas, e.g., the Internet of Things, also attracted extensive attention, e.g., Atonomi [17], Chain of Things [18] and IoTeX [19].

With the decentralized, tamper-resistance nature, the blockchain-mediated application presents a vast potential. Choo *et al.* [20] discuss the ongoing challenges when applying blockchain in industry, governments, and academia. Guan *et al.* [21] adopt the blockchain technology to securely aggregate and store the near-real-time data and preserve the users' privacy. Pal *et al.* [22] design a decentralized and asynchronous delegation model by using the blockchain technology and demonstrate the feasibility by using Ethereum private blockchain platform. Liang *et al.* [23] utilize the blockchain technology to establish a decentralized storage system, which realizes the dynamic storage and update and fast repair. Yang *et al.* [24] introduce the blockchain technology to help protect the topology privacy in Mobile Edge Computing (MEC). Keshk *et al.* [25] apply the blockchain to build up a privacy-preserving framework in the smart power networks.

Although blockchain technology presents various advantages, there still exist scalability and efficiency issues inside. Ethereum 2.0 [26] combines sharding technology and PoS, focusing on further improving network efficiency in a scalable way. A creative structure proposed by Ethereum Foundation is the beacon chain, introducing PoS into Ethereum, where there was only PoW before. All the data structures inside the beacon chain are akin to the public chain powered by Proof of Work. However, the different aspect is that the beacon chain is operated by a committee composed of many validators using Proof-of-Stake consensus. Such a committee is pseudo-randomly assigned to verify a shard of the current block. As the intermediary between the public chain and the numerous committees, the beacon chain is responsible for managing administrative transactions throughout the whole blockchain network with shardings, which include a registry of validator addresses, the state of each validator, attestations, and links to shards. The beacon chain can coordinate with the whole network and ensure a smooth transition between a pure PoW blockchain system to a pure PoS one.

However, the blockchain network deployed with PoS is vulnerable to discouragement attack, a critical threat to most of the PoS-based blockchains but is less studied. Saito [9] proposed a solution that can ensure the cost of producing a block fluctuates depending on the degree of support a node receives from the rest of the network. They adopted a new workload measurement that is a derivative of the volume of transaction fees gathered from other nodes. Apart from developing a new consensus protocol, applying cryptography is an alternative. But it is virtually impossible to discriminate between attackers and honest validators inside a PoS mechanism, especially the attacker sacrificing short-term profit just looks like a victim. Moreover, relying on consensus development and cryptography application to deal with a specific cyber risk is exceptionally costly to an existing blockchain network.

One of the most effective ways to transfer cyber risk is cyber insurance. The market for cyber insurance has vitality spurred in recent years, which is expected to reach $5 billion by 2018 and exceed $7.5 billion by 2020 [27]. The market with colossal potential motivates more and more researchers to investigate it in various network scenarios. Khalili *et al.* [28] have explored the interdependent nature of cybersecurity and the latest Internet measurement for evaluating the security posture. They focus on the theoretical details more, the other

promising works regarding cyber insurance, see, e.g., [29], [30], and [31]. Their "interdependent nature" idea does an excellent job explaining the relation between the entities and the networks, which can also apply to the participants and the blockchain networks. Feng *et al.* [32], adopt the cyber insurance tool to neutralize the cyber risk caused by double-spending in the blockchain network and model the problem as a two-stage Stackelberg game. Lu *et al.* [33] introduce cyber insurance to heterogeneous wireless networks (HWNs) and reviews the cyber risks of the enabling technologies for HWNs. As we discussed above, none of the works consider the discouragement attack.

B. Motivation and Contribution

Inspired by the above work, we explore the discouragement attack within the PoS mechanism in the blockchain networks with shards. We adopt cyber insurance as a risk-management to mitigate the risk and motivate the validators' online time (i.e., withdraw delay [10]). Owing to the anonymity nature and the weak leadership of the beacon chain, the problems of *hidden information* and *hidden action* coexist. Hidden information and hidden action are two terms specific to economics. In this paper, the validators' type information is the hidden information and their efforts after singing the contracts are the hidden action. Besides, considering the cyber insurer, the interactions of the three parties, i.e., cyber insurer, blockchain infrastructure provider, and validators, are complex and difficult to analyze. There is not an existing model that can be applied directly to formulate the problem. One practical model to set up a cyber insurance framework is the contract theory [34], which has been extensively studied, e.g., [35], [36], [37], and [38]. Specifically, we designed a cyber-insurance framework, modeling the interactions between the beacon chain and its underlying validators in [38] but without the role and effect of cyber-insurer. We did not take the interactions between cyber-insurer and blockchain into account and just assumed that cyber-insurer could gain nothing from the insurance, which is less applicable in reality. Therefore, we establish a two-stage hierarchical game model by combining the Stackelberg game and contract theory, formulating the complicated interactions among cyber-insurer, blockchain, and validators, and allowing the cyber-insurer and blockchain to obtain the maximized profits. First of all, we analyze the discouragement attack model and the expected loss for all kinds of validators (i.e., malicious, censored, and uncensored). Then, the cyber-insurer will take the lead in the upper sub-game of Stage I (more details regarding this model are given in Section III), determining the premium and claim factor. Consider that the blockchain infrastructure provider follows the leader's rules and determines a discount factor for premium.In Stage II, the blockchain infrastructure provider designs a series of contracts for participants, determining the contract components based on the attack model and cyber-insurer's premium and claim factor. By such a design, the information asymmetry can be overcome by contract theory [34]. As a result, the validator needs to pay only a discounted premium but is entitled to cyber insurance compensation. The cyber insurer needs to pay only a discounted claim but will obtain a full premium. It is the blockchain to compensate for the premium and claim for the cyber insurer and validators, respectively.

We summarize the main contributions of this paper in the following.

- We utilize cyber insurance as risk-management (i.e., it works as an economic mechanism) that motivates the validators to be online and reduces their losses from the discouragement attack. The proposed scheme allows the blockchain to keep more validators with high online active participation for a required time, which contributes to the market value and makes time for the developers to detect discouragement attacks and malicious nodes.
- We propose a hierarchical game model by combing the Stackelberg game and contract theory together, analyzing the interactions among the cyber-insurer, blockchain infrastructure provider, and validators, and then formulating the problems in two stages.
- In the hierarchical game model, the cyber-insurer is the leader in upper Stage I, determining the premium and claim factor for the validators. Based on the cyber-insurer's strategy in Stage I, the blockchain infrastructure provider, as the follower in lower Stage II, determines the contract items, including discount and compensation factors. The validators would be given a set of insurance contracts in Stage II. Thus, we can maximize the cyber insurer and blockchain infrastructure provider's profit and determine the online duration for the validators.
- Detailed illustrations are given to show the solving process. Accordingly, we present the closed-form of the optimal premium, claim, and compensation parameters obtained through backward induction. With the extensive simulations, we compare the impacts of different key parameters on the optimal results and show the profit differences between the proposed model and the benchmark model, demonstrating the feasibility and efficacy of the proposed model.

The rest of the proposed paper is organized as follows. In Section II, we present the system model, including the discouragement attack model, reward distribution, expected loss, griefing factor, utility models of the beacon chain, cyber insurer, and validators. In Section III, we provide the specific design of the contract, including the problem formulation and optimal solutions. In Section IV, we give the problem formulation and optimal solution of the Stackelberg game. In Section V, we illustrate the simulation results and the analysis. In Section VI, we give the conclusion for the proposed scheme.

II. System Model

This section will introduce the discouragement attack model, the reward distribution function, the expected loss, and then present the utility models for the validators, blockchain, and the cyber insurer. The overview of the sharded blockchain with cyber insurance model can be referred to Fig. 1. We consider the market with one cyber insurer and one blockchain network. From the incentive perspective, the beacon chain tries to maximize the participation (i.e., delay and online deposits)

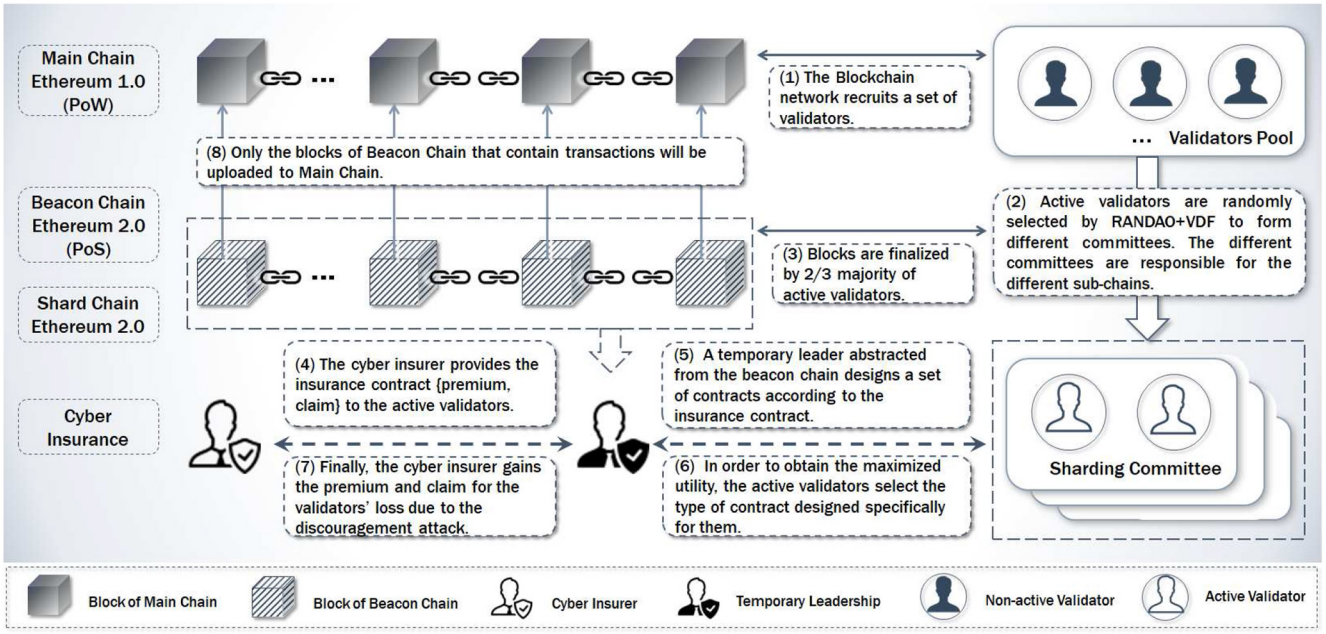


Fig. 1. An overview of the sharded blockchain network with cyber insurance.

of validators to hold its market value. The malicious ones would like to choose the contract with a small "delay," but they cannot escape from the security review when waiting in the queue. The honest ones prefer contracts with a longer online time, which means a higher claim for the potential risk.

The core idea of discouragement attack is long-term censorship on honest participants, which the attackers conduct through the power of their collusion [8]. As long as some messages are published for audit, verification, or packaging, the attackers act illegally inside the PoS consensus mechanism to reduce other validators' revenue [39]. Fig. 2 depicts a comparison regarding the discouragement attack effects with/without cyber-insurance. According to the rewarding function in [8], the malicious users initiate censorship on these honest users to decrease the rewards in phase (1). Then in phase (2), the honest users realize that the rewards are slashed round after round, even though they vote honestly. Without enough incentives, these honest users will intend to drop out of the system in phase (3). Finally, the honest users' withdrawal enables the malicious users to launch much more severe attacks, such as the double-spending attack. However, cyber insurance can guarantee honest users' rewards by compensating for their loss in phases (a) and (b). With an unaffected reward, the honest users will tend to stay in the system for a longer time in phase (c), which forces the malicious one to drop out of the system due to the increasing cost.

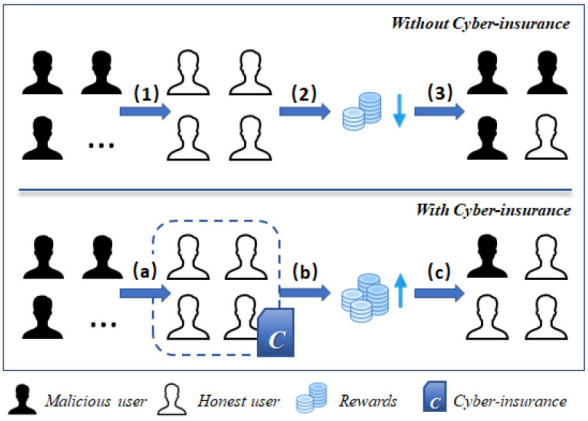


Fig. 2. How does the cyber-insurance work when discouragement attack occurs.

A. Discouragement Attack Model

Discouragement attack means that the malicious validators are controlled by the attacker acting illegally inside the consensus mechanism in order to reduce other validators' revenue. Although it is virtually impossible to censor any transaction on a blockchain network, censorship can occur when signing the signatures [39]. Take the sharded blockchain as an example. In [8], there are N validators in a single committee, sharing a maximum total reward of R in each round. If the total number of whom signing the messages is M ($M \leq N$), then they can earn a reward of $\frac{R}{N} \cdot \frac{M}{N}$ because of signing a message. When the attackers collude to stop including messages from some other validators (not all validators), the censored validators will gain nothing because their signatures are not included in the finalized results [40]. Following that M is virtually reduced, both the reward of attackers and non-censored validators decreases. Even though the attackers are forced to inflict economic damage to themselves due to censorship, they still have the incentive to expect long-term profit in the future. Consequently, the victims realize that their incentive is decreasing and then exit the blockchain network. A possible, as well as the worst case, is that most honest validators drop out of the network with all attackers remaining, allowing the attackers to easily launch the double-spending attack or any other severe attacks on the chain manipulating the finalized blocks.

To better analyze the attack model, the paper [8] introduces a useful concept called *griefing factor* and a reward distribution function with the bounded griefing factor. The discouragement attack can be classified into two types: majority attack and minority attack. A majority attack means the attacker has a greater power to control a majority of the validators, while the minority attack is the opposite case. In a majority attack, the validators can be identified as three types: the malicious validators, the censored validators, and the uncensored validators. In a minority attack, there are only two types of validators: the malicious validators and the remaining validators. We will explain the reward distribution and loss function under the majority attack in the following. Suppose there are *N* validators in committee $\mathcal{I}$, $\hat{n}$ malicious validators, $\hat{k}$ censored validators, $N-\hat{k}-\hat{n}$ uncensored validators, and the total reward for each round is *R*. Each validator contributing to a PoS blockchain's work earns *R*/*N* if no one is malicious. But if there exist malicious validators, according to Vitalik's idea [41], we have the reward distribution function: $\frac{R(N-\hat{k})}{N^2}$. Thus, we have the loss function l_1 for each censored validator and the loss function l_2 for each uncensored validator:

$$l_1 = \frac{R}{N}, \tag{1}$$

$$l_2 = \frac{R}{N} - \frac{R(N-\hat{k})}{N^2} = \frac{R\hat{k}}{N^2}. \tag{2}$$

Thus, we have the expected loss function as follows:

$$\mathcal{L} = \left\{ \frac{\hat{k}}{(N-\hat{n})} l_1 + \frac{(N-\hat{k}-\hat{n})}{(N-\hat{n})} l_2 \right\} \tag{3}$$

where $\hat{k}/(N-\hat{n})$ denotes the probability of being censored, and $(N-\hat{k}-\hat{n})/(N-\hat{n})$ denotes the probability of not being censored.

B. Cyber Insurer Utility Model

This paper will first classify all the validators into the different types according to their activeness. For the validators of type-*i*, the cyber insurer determines the premium p_i and coverage factor β_i. For the cyber insurer, it can get profit from the gap between the premium and the claim. The premium p_i is given by the type-*i* validators, as well as the blockchain infrastructure provider. The claim is determined by the loss $\mathcal{L}$ and the coverage factor β_i. Thus, the cyber insurer's utility obtained from a validator can be expressed by

$$U_{c,i}(p_i, \beta_i) = p_i - \beta_i \mathcal{L}. \tag{4}$$

C. Blockchain Utility Model

The blockchain network is decentralized, which means no central trusted party is dealing with the administrative transaction. However, it is not the same case in a blockchain network with shards. According to [5], the beacon chain consists of the dedicated blocks for recording the administrative transactions. The block managers can be considered to be temporary leaders. Moreover, the contract items and the related details on execution can be encoded into a smart contract.

The blockchain infrastructure provider acts as a medium between the cyber insurer and the validators. It follows the cyber insurer's strategies and determines a series of compensation strategies (*discount factor*,*compensation factor*) for all types validators to further incentivize their online time d_i. By such design, the whole blockchain network's value can be increased by motivating the validators with higher activeness to stay online for a longer time. The utility function is expressed as follows:

$$U_{b,i} = \Pi(\theta_i, d_i) - \alpha_i p_i - \Theta(u\beta_i \mathcal{L}), \tag{5}$$

where $\Pi(\cdot)$ is an increasing function that is used for calculating the revenue from validators' delay d_i and activeness θ_i, the second term is the compensatory premium for the cyber insurer with the discount factor α_i, and the last term is the compensatory claim for the validators with the compensation factor *u*.

D. Validator Utility Model

The validators are randomly selected from the validator pool. Thus, there exists a variety of validators with different activeness. We first classify the validators into different types: type-1, type-2, ..., type-*i*, ..., type-$\mathbb{N}$. The classification criterion is based on their history activeness in the blockchain. In order to analyze the activeness of the different validators without loss of generality, we model the activeness of all the validators as the Normal Distribution $\hat{\mathcal{A}}$ with mean μ and variance σ^2. For a certain range of activeness $[a_i, a_{i+1})$, we model it as a truncated normal distribution $\mathcal{A}_i$, which is expressed as:

$$\mathcal{A}_i(x; \mu, \sigma, a_i, a_{i+1}) = \frac{\frac{1}{\sigma}\phi(\frac{x-\mu}{\sigma})}{\Phi(\frac{a_{i+1}-\mu}{\sigma}) - \Phi(\frac{a_i-\mu}{\sigma})}, \tag{6}$$

where the validators whose activeness lies in interval $[a_i, a_{i+1})$ belong to type *i*. The activeness $\hat{a}_i$ observed and analyzed by the blockchain infrastructure provider contains a random noise:

$$\pi(\hat{a}_i, \mathcal{N}) = \hat{a}_i - \mathcal{N}, \tag{7}$$

where $\mathcal{N}$ is the network delay, a zero mean Gaussian noise with variance σ'.

All validators have options of not buying a contract, directly buying an insurance contract from the cyber-insurer, or buying a mixed contract from the blockchain. Intuitively, an honest and rational validator tends to buy a contract (either from the cyber-insurer or blockchain) to prevent monetary loss caused by discouragement attacks. The single contract from the cyber-insurer allows the buyers free to enter and exit the blockchain network. By contrast, a mixed contract provided by blockchain can additionally offer a discount factor and a compensation factor in exchange within a fixed length for the validator being online. For incentive reasons, validators buying mixed contracts from blockchain is profitable. Even having to stay online for a fixed duration, the validators' benefits will be protected by the mixed contract with a lower cost and a higher claim. We will present and explain the validator's utility of choosing contracts of different categories in the following.

1) No Contract: If the validator does not sign any contract, it will bear the total cost of its effort as well as the potential loss caused by the discouragement attack. Therefore, the type-*i* validator's utility per unit time is

$$u_i^- = -c[\pi(\hat{a}_i)]^2 - \mathcal{L}. \tag{8}$$

Thus, the expected utility without contract is as follows:

$$\begin{aligned} U_i^- &= E(-c[\pi(\hat{a}_i)]^2 - \mathcal{L}), \\ &= -c\hat{a}_i^2 + c\sigma'^2 - \mathcal{L}. \end{aligned} \tag{9}$$

Obviously, due to the potential loss, the validator would choose to do nothing to lower the total cost. Note that "doing nothing" means the validator will not do any other activities that the consensus protocol does not require.

2) With Single Contract: If the validator signs the contract with the cyber insurer directly, it can only obtain the insurance contract (p_i, β_i), where p_i is the premium and β_i is the claim factor with $0 \leq \beta \leq 1$. Without the compensation factors, the validator receives the profit as follows:

$$\mathbb{P}_i^- = -p_i - \mathcal{L} + \beta_i \mathcal{L}. \tag{10}$$

3) With Mixed Contract: This paper considers the blockchain infrastructure provider to be an intermediary to interact with the cyber insurer and the validator, further motivating the validators by providing the mixed contract with a discount factor and a compensation factor. Thus, the type-*i* validators will be provided a series of mixed contracts $\{[p_i, \beta_i], [\alpha_i, u\beta_i, d_i]\}$, where α_i is the discount factor with $0 \leq \alpha \leq 1$, *u* is the compensation factor with $0 \leq u \leq 1$ and d_i denotes the delay (i.e., the validator's online time), it means the validator will receive a discount of the insurance contract through keeping active online. For a base premium *p* and a loss $\mathcal{L}$, the validator receives the profit from the mixed contract $(p_i, \alpha_i, \beta_i, d_i)$ is defined as follows:

$$\mathbb{P}_i^+ = -p_i + \alpha_i p_i - \mathcal{L} + \beta_i \mathcal{L} + u\beta_i \mathcal{L}. \tag{11}$$

Thus, we have the profit given by the mixed contract is defined as follows:

$$\begin{aligned} f(p_i, \alpha_i, \beta_i) &= \mathbb{P}_i^+ - \mathbb{P}_i^-, \\ &= \alpha_i p_i + u\beta_i \mathcal{L}, \end{aligned} \tag{12}$$

which means the type-*i* validator needs to pay a premium $p_i - \alpha_i p_i$ instead of p_i, and obtains $(1+u)\beta_i \mathcal{L}$ as the claim for the loss.

Intuitively, the validator with a high activeness is desired by the blockchain infrastructure provider, since a high activeness contributes to a more value of the network. To motivate the validators, a high discount factor should come with a high coverage factor, which both are offered by the contract. Based on the cyber insure strategy (p_i, β_i), the blockchain infrastructure provider determines its own policy. We set $\alpha_i = g(\beta_i)$ for the ease of analysis, with $g'(\beta_i) > 0$ and $g''(\beta_i) \leq 0$. Then $f(p_i, \alpha_i, \beta_i)$ can be rewritten as $G(p_i, \alpha_i) := f(p_i, \beta_i, \alpha_i)$. With the pre-defined compensation factor *u*, let $(p_i, \beta_i, \alpha_i, d_i)$ denote the mixed contract $\{[p_i, \beta_i], [\alpha_i, u\beta_i, d_i]\}$. Therefore

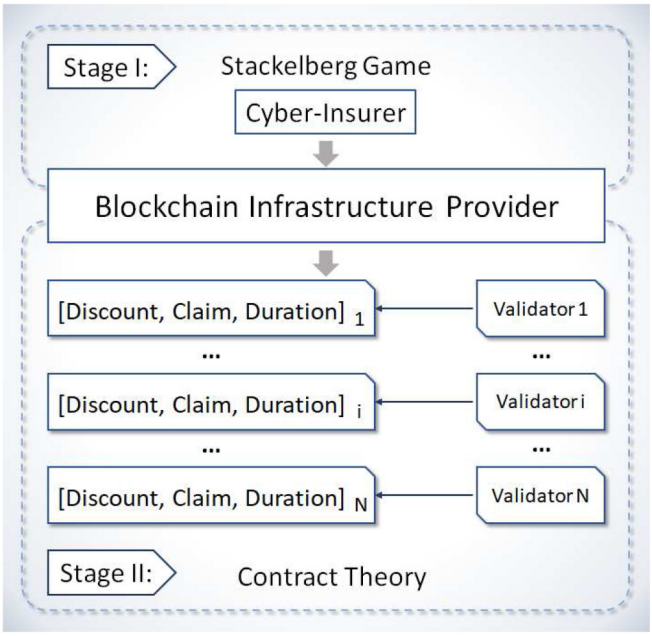


Fig. 3. A two-stage hierarchical game model.

we first have the utility function per round for the validators:

$$u_i^+ = \mathcal{A}_i G(p_i, \alpha_i) + \gamma \mathcal{A}_i \pi(\hat{a}_i) - c[\pi(\hat{a}_i)]^2 - h(d_i), \tag{13}$$

where γ is the pre-defined coefficient and the second term $\gamma \mathcal{A}_i \pi(\hat{a}_i)$ denotes the benefit from the observed activeness that is evaluated by the contract, and $h(d_i)$ represents capital lockup cost with the delay d_i per round, which means the validator would suffer a loss because its deposit is locked up in the blockchain network and cannot be redeemed for the period d_i the, i.e.,

$$h(d_i) = \mathrm{d}\{e_0 \mathcal{D} \exp\{\epsilon_0 d_i\}\}, \tag{14}$$

where ϵ_0 is the annual interest rate with $0 < \epsilon_0 < 1$, e_0 is the pre-defined coefficient and $\mathcal{D}$ is the lockup deposit. Thus, we have $h(\cdot)$ is an increasing function of d_i. The time for each round is so tiny compared with the online time d_i, we use the differentiation to present the discounted value approximately.

III. Problem Formulation of the Hierarchical Game

This section will model the interactions of the cyber insurer, blockchain infrastructure provider, and validators as a hierarchical game, where the interaction between the cyber insurer and blockchain infrastructure provider is a Stackelberg and the interaction between the blockchain infrastructure provider and validators is a contract game. As shown in Fig. 3, Stage I denotes the Stackelberg game, while Stage II represents the contract game.

A. Stage I: Stackelberg Game Formulation

The Stackelberg game includes two sub-games of strategies made by the participants in the model. Cyber-insurer will determine the premium and claim strategies in the upper game after considering blockchain's action. The blockchain

infrastructure provider follows the cyber insurer's rules and determines the contracts for validators accordingly in the lower game. The anonymity of the blockchain network makes it more difficult for the cyber insurer to have accurate knowledge of the validators. The cyber insurer can only obtain the probability distribution of the validators based on their activeness history. Let λ_i denote the probability of the type-*i* validators with $\sum_{i=1}^{\mathbb{N}} \lambda_i = 1$. According to Section II, the revenue of cyber insurer obtained from all the types of validators is $U_c = \sum_{i=1}^{\mathbb{N}} \{u_c(p_i, \beta_i)\}$. Thus, the utility function of the cyber insurer in the leader's sub-game is expressed as follows:

$$U_c = \sum_{i=1}^{\mathbb{N}} \lambda_i \{p_i - \beta_i \mathcal{L}\}. \tag{15}$$

Once acquiring the knowledge of the insurance contract from the cyber insurer, the blockchain infrastructure provider determines an incentive policy for each type of the validators in order to gain more market value and resist the discouragement attack through validators' rotation. Based on the premium and claim factor, the blockchain infrastructure provider determines a discount factor for the validators' premium and a compensation factor for the validators' claim. Thus, we have the utility function for the blockchain infrastructure provider as follows:

$$U_b = \sum_{i \in \mathbb{N}} \lambda_i \{\Pi(\theta_i, d_i) - p_i \alpha_i - \Theta(u \beta_i \mathcal{L})\}, \tag{16}$$

where $\Pi(\cdot)$ is the evaluation function of the validators' delay, the second term $p_i \alpha_i$ is the discount premium for the validators and $\Theta(\cdot)$ is the cost of compensation claim.

B. Stage II: Contract Model Design

In Stage II, we elaborate the contract theory framework to model the interactions between the blockchain infrastructure provider and the validators. The blockchain infrastructure provider acts as a medium between the cyber insurer and the validators. Given an insurance contract with the premium and claim factor determined by the cyber insurer, the validators obtain a series of contracts from the blockchain. To incentivize the validators and determine the validators' delay, the blockchain infrastructure provider designs a set of contracts, including the discount factor, compensation factor, and online requirement. Recall the utility function of validators in Section II-D3, and we will have the expectation function as follows:

$$\begin{aligned} U_i^+ &= E(\mathcal{A}_i G(p_i, \alpha_i) + \gamma \mathcal{A}_i \pi(\hat{a}_i) - c[\pi(\hat{a}_i)]^2 - h(d_i)), \\ &= \theta_i G(p_i, \alpha_i) + \gamma \theta_i \hat{a}_i - c\hat{a}_i^2 + c\sigma'^2 - h(d_i), \end{aligned} \tag{17}$$

in which θ_i represents the expected value of the truncated normal distribution $\mathcal{A}_i$, i.e., $\theta_i = E(\mathcal{A}_i)$.

According to the probability density function of the truncated normal distribution in Section II-D, we have

$$\theta_i = \int_{a_i}^{a_{i+1}} \frac{x \frac{1}{\sigma} \phi(\frac{x-\mu}{\sigma})}{\Phi(\frac{a_{i+1}-\mu}{\sigma}) - \Phi(\frac{a_i - \mu}{\sigma})} \, \mathrm{d}\, x. \tag{18}$$

In the utility function in (17), the optimal activeness for a validator of type-*i* within the contract can be obtained by $a_i^* := \arg\max_{\hat{a}_i \geq 0} \{\theta_i G(p_i, \alpha_i) + \gamma \theta_i \hat{a}_i - c\hat{a}_i^2 + c\sigma'^2 - h(d_i)\}$. Then we solve this problem by setting its first derivative condition as zero, which is expressed as $\frac{\partial U_i^+}{\partial \hat{a}_i} = 0$. Given $\hat{a}_i^* = \frac{\gamma \theta_i}{2c}$, it is easy to enable optimal activeness to approach the expected value or a higher one through setting γ. Thus, we rewrite the utility function in (17) by substituting $\hat{a}_i^* = \frac{\gamma \theta_i}{2c}$, which is expressed as

$$U_i^+ = \theta_i G(p_i, \alpha_i) + \frac{\gamma^2 \theta_i^2}{4c} + c\sigma'^2 - h(d_i). \tag{19}$$

We will prove the feasibility of the contract by introducing the constraints of Individual Rationality (**IR**) and Incentive Compatibility (**IC**). Individual Rationality (**IR**) and Incentive Compatibility (**IC**) are two significant constraints of the contract theory [34], which enable the rational validators to select the specific contract that is designed for their own types rather than others.

Definition 1: Individual Rationality (IR). IR means that a rational type-*i* ($\forall i \in \{1, \ldots, \mathbb{N}\}$) validator will accept a contract only when the utility provided by the contract is not less than that of no-contract case, i.e.,

$$\begin{aligned} U_i^+(p_i, \beta_i, \alpha_i, d_i) &= \theta_i G(p_i, \alpha_i) + \frac{\gamma^2 \theta_i^2}{4c} + c\sigma'^2 - h(d_i) \\ &\geq U_i^-(0, 0, 0, 0), \end{aligned} \tag{20}$$

where $U_i^-(0, 0, 0, 0)$ denotes the utility function without the contract.

Definition 2: Incentive Compatibility (IC). IC means that a type-*i* validator can only obtain the maximum profit by choosing the contract $(p_i, \beta_i, \alpha_i, d_i)$ rather than all the other contracts $(p_j, \beta_j, \alpha_j, d_j)$ $(\forall i, j, i \neq j)$, i.e.,

$$U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_j, \beta_j, \alpha_j, d_j). \tag{21}$$

A contract is considered to be feasible only when these two constraints are satisfied. The contract designer can only maximize its profit with IR and IC constraints. Therefore, the problem of the contract model can be expressed as:

$$\max_{(p_i, \beta_i, \alpha_i, d_i)} \quad U_b = \sum_{i \in \mathbb{N}} \lambda_i \{\Pi(\theta_i, d_i) - p_i \alpha_i - \Theta(u \beta_i \mathcal{L})\}, \tag{22}$$

s.t.

$$\begin{aligned} &(22a) \quad U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^-(0, 0, 0, 0), \\ &(22b) \quad U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_j, \beta_j, \alpha_j, d_j), \\ &(22c) \quad \theta_1 < \theta_2 < \cdots < \theta_{\mathbb{N}}, \end{aligned}$$

wherein (22a) and (22b) are the IR and IC constraints, respectively, and (22c) is the monotonicity condition. Obviously, the problem (22) is not a convex problem and cannot be solved directly. Thus, we transform this problem by reducing the constraints in the following.

IV. Optimal Solution for the Hierarchical Game

In this section, we apply backward induction to solve the problems. That means we will first solve Stage II's problem by assuming that the solution of Stage I is given. Then we finally

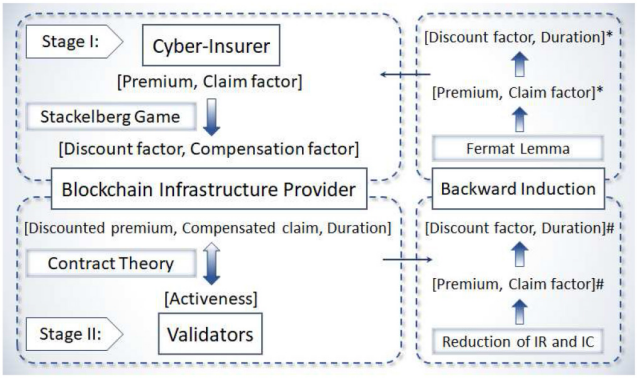


Fig. 4. An overview of problem formulation and solution.

obtain all the solutions by substituting them to the problems in Stage I. As shown in Fig. 4, in Stage II, given the premium$^{\#}$ and claim factor$^{\#}$ ('#' means that the parameters are assumed to be known in Stage II), we can obtain the optimal discount factor and online time by reducing the IR and IC constraints under the contract framework. Then in Stage I, after substituting the parameters obtained in Stage II into the objective function, we finally are able to get the optimal premium* and claim factor* ('*' means that the parameters are the final optimal solutions). The algorithms for solving the problems are presented in Algorithm 1 and Algorithm 2.

A. Stage II: Contract Theory Model

In this sub-section, we reduce the numbers of IC and IR constraints according to the contract theory framework [34] and then obtain a new optimal problem with the reduced constraints.

Lemma 1 (Reduction of IR): For all the types, $\forall i \in \{1, \ldots, \mathbb{N}\}$, if we have $\theta_1 < \theta_2 < \cdots < \theta_{\mathbb{N}}$, then the IR constraint of type-*i* holds only when the constraint of the lowest type validator is satisfied.

Proof: Please refer to Appendix Lemma 1 for details. ■

Lemma 2 (Monotonicity): For any contract $(p_i, \beta_i, \alpha_i, d_i)$, $p_i \geq p_j$, $\beta_i \geq \beta_j$, $\alpha_i \geq \alpha_j$ and $d_i \geq d_j$ if and only if $\theta_i \geq \theta_j$.

Proof: Please refer to Appendix Lemma 2 for details. ■

Lemma 3 (Reduction of IC): There are four definitions regarding the IC constraints between type-*i* and type-*j* ($\forall i \neq j$):

(a) If $\forall j \in \{1, 2, \ldots, i-1\}$, the constraints are called Downward Incentive Constraints (**DIC**s).
(b) If $j = i-1$, the constraint is called Local Downward Incentive Constraint (**LDIC**).
(c) If $\forall j \in \{i+1, \ldots, N\}$, the constraints are called Upward Incentive Constraints (**UIC**s).
(d) If $j = i+1$, the constraint is called Local Upward Incentive Constraint (**LUIC**).

With the monotonicity conditions $\theta_1 < \theta_2 < \cdots < \theta_{\mathbb{N}}$, the DICs can be reduced as LDICs, i.e., $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1})$ and the UICs can be reduced as the LUICs, i.e., $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_{i+1}, \beta_{i+1}, \alpha_{i+1}, d_{i+1})$.

Proof: Please refer to Appendix Lemma 3 for details. ■

From Lemma 3, we can conclude that Nash Equilibrium always exists. If an optimal contract portfolio $\Omega_i = \{p_i,\ \alpha_i, \beta_i, d_i\}$ forms an Nash Equilibrium, for type-*i* validator and the other alternative contract portfolios Ω_{-i}, we must have

$$U_i^+(\Omega_i) \geq U_i^+(\Omega_{-i}), \tag{23}$$

which can be derived from Lemma 3. We will also demonstrate this conclusion through the simulation in Section V.

To solve the new optimization problem defined in (22), we first reduce the IC constraints for all the types of contracts ($\forall i, \in \{2, \ldots, \mathbb{N}\}$) by setting $U_i^+(p_i, \beta_i, \alpha_i, d_i) = U_i^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1})$ and have the following equations:

$$\begin{aligned}\theta_i G(p_i, \alpha_i) + \frac{\gamma^2 \theta_i^2}{4c} + c\sigma'^2 - h(d_i) \\ = \theta_i G(p_{i-1}, \alpha_{i-1}) + \frac{\gamma^2 \theta_{i-1}^2}{4c} + c\sigma'^2 - h(d_{i-1}).\end{aligned} \tag{24}$$

For the type-1 utility function, we reduce the IR constraint by setting $U_i^+(p_i, \beta_i, \alpha_i, d_i) = U_i^-(0, 0, 0, 0)$ and have

$$\theta_1 G(p_1, \alpha_1) + \frac{\gamma^2 \theta_1^2}{4c} + c\sigma'^2 - h(d_1) = -c\hat{a}_1^2 + c\sigma'^2 - \mathcal{L}. \tag{25}$$

Then we add all the IC constraints and obtain

$$\theta_i G_i = (\theta_i - \theta_{i-1}) G_{i-1} + \cdots + \theta_2 G_1 + c\sigma'^2 - h(d_1). \tag{26}$$

where G_i denotes $G(p_i, \alpha_i)$. Then, we add the reduced IR constraint of type-1 in (25) to (26) and have

$$\theta_i G(p_i, \alpha_i) - h(d_i) = \sum_{j=1}^{i-1} \Delta_j - \frac{\gamma^2 \theta_1^2}{4c} - \mathcal{L}, \tag{27}$$

where $\Delta_j = (\theta_{j+1} - \theta_j) G(p_j, \alpha_j)$. Without loss of generality, we set $\alpha_i = g(\beta_i) = e_1 \beta_i^{(1-\eta)}$, $\Pi(\theta_i, d_i) = e_2 h(d_i) + e_2 \theta_i^{\epsilon_2}$ and $\Theta(u\beta_i \mathcal{L}) = e_3 \theta_i^{\epsilon_3} u\beta_i \mathcal{L}$, where e_1, e_2 and e_3 are the evaluation factors, and $\epsilon_1 > 0, \epsilon_2 > 0, \epsilon_3 > 0$ and $0 < \eta < 1$ are the pre-defined coefficients. Therefore, we rewrite the objective function of the blockchain as follows:

$$\max_{(p_i, \beta_i, \alpha_i, d_i)} \ U_b = \sum_{i \in \mathbb{N}} \lambda_i \big\{ e_2 h(d_i) + e_2 \theta_i^{\epsilon_2} - p_i \alpha_i - e_3 \theta_i^{\epsilon_3} u \beta_i \mathcal{L}) \big\}. \tag{28}$$

Based on (27), we have

$$h(d_i) = \theta_i G(p_i, \alpha_i) - \sum_{j=1}^{i-1} \Delta_j + \frac{\gamma^2 \theta_1^2}{4c} + \mathcal{L}. \tag{29}$$

We rewrite the objective function (28) by substituting (29), i.e.,

$$\begin{aligned}\max_{(p_i, \beta_i, \alpha_i, d_i)} \ U_b = \sum_{i \in \mathbb{N}} \lambda_i \Bigg\{ e_2 \Bigg[\theta_i G(p_i, \alpha_i) - \sum_{j=1}^{i-1} \Delta_j + \frac{\gamma^2 \theta_1^2}{4c} + \mathcal{L} \Bigg] \\ + e_2 \theta_i^{\epsilon_2} - p_i \alpha_i - \frac{e_3}{e_1^{\frac{1}{(1-\eta)}}} \theta_i^{\epsilon_3} u \alpha_i^{\frac{1}{(1-\eta)}} \mathcal{L} \Bigg) \Bigg\}.\end{aligned} \tag{30}$$

Algorithm 1 Optimal Solution to the Problem in Stage II

Input: The premium from Stage I: $\hat{p}$, the claim factor from the Stage I: $\hat{\beta}$, the historical statistical distribution of the validators' activeness: $\mathcal{A}$, the number of types: $\mathbb{N}$, the probability of the different type validator: λ, and the loss: $\mathcal{L}$;

Output: The discount factor $\hat{\alpha}$ and the online time $\hat{d}$ for all the validators;

1: //Reduction of IC constraints;
2: **for** $i = \mathbb{N}$; $i \geq 2$; $i--$ **do**
3: Set $U_i^+(\hat{p}_i, \hat{\beta}_i, \alpha_i, d_i) = U_i^+(\hat{p}_{i-1}, \hat{\beta}_{i-1}, \alpha_{i-1}, d_{i-1})$;
4: Set $\psi_i = U_i^+(\hat{p}_i, \hat{\beta}_i, \alpha_i, d_i) - U_i^+(\hat{p}_{i-1}, \hat{\beta}_{i-1}, \alpha_{i-1}, d_{i-1})$;
5: **end for**
6: //Reduction of IR constraints;
7: Set $U_1^+(\hat{p}_1, \hat{\beta}_1, \alpha_1, d_1) = U_1^-(0,0,0,0)$;
8: Set $\psi_1 = U_1^+(\hat{p}_1, \hat{\beta}_1, \alpha_1, d_1) - U_1^-(0,0,0,0)$;
9: //Add all reduced IC constraints and IR constraint together;
10: **for** $i = \mathbb{N}$; $i \geq 1$; $i--$ **do**
11: Set $\Psi_i = \psi_i$;
12: **for** $j = i-1; j \geq 1; j--$ **do**
13: $\Psi_i = \Psi_i + \psi_j$;
14: **end for**
15: **end for**
16: **for** $i = \mathbb{N}$; $i \geq 1$; $i--$ **do**
17: Obtain d_i from $\Psi_i = 0$;
18: Substitute d_i into the problem: $\max_{(\hat{p}_i, \hat{\beta}_i, \alpha_i, d_i)} U_{b,i} = \Pi(\theta_i, d_i) - p_i\alpha_i - \Theta(\mu\beta_i\mathcal{L})$;
19: Compute $\hat{\alpha}_i = \arg\max U_{b,i}(\alpha_i) = e_1\left\{\frac{\hat{p}_i[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}{\mathcal{L}(e_3\theta_i^{\epsilon_3}\mu - e_2\theta_i)}\right\}^{\frac{1-\eta}{\eta}}$;
20: Compute $\hat{d}_i = \frac{1}{\epsilon_0}\log\left\{\frac{\theta_i G(\hat{\alpha}_i) - \sum_{j=1}^{i-1}\Delta_j + \frac{\gamma^2\theta_1^2}{4c} + \mathcal{L}}{e_0\epsilon_0\mathcal{D}}\right\}$;
21: **end for**

Algorithm 2 Optimal Solution to the Problem in Stage I

Input: The discount factor $\hat{\alpha}$, online time $\hat{d}$ that are obtained from Stage II, the historical statistical distribution of the validators' activeness: $\mathcal{A}$, the number of types: $\mathbb{N}$, the probability of the different type validator: λ, and the loss: $\mathcal{L}$;

Output: The Optimal premium: p^*, claim factor: β^*, discount factor: α^*, and online time: d^* for all the validators;

1: **for** $i = \mathbb{N}$; $i \geq 1$; $i--$ **do**
2: Transfer β_i from $\hat{\alpha_i}$: $\beta_i = \left\{\frac{p_i[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}{\mathcal{L}(e_3\theta_i^{\epsilon_3}u - e_2\theta_i)}\right\}^{\frac{1}{\eta}}$;
3: Substitute β_i into the problem: $U_{c,i} = p_i - \beta_i\mathcal{L}$;
4: Compute $p_i^* = \arg\max U_{c,i}(p_i)$;
5: Compute $\beta_i^* = \left\{\frac{p_i^*[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}{\mathcal{L}(e_3\theta_i^{\epsilon_3}u - e_2\theta_i)}\right\}^{\frac{1}{\eta}}$;
6: Compute $\alpha_i^* = e_1\beta_i^{*(1-\eta)}$;
7: Compute $d_i^* = \frac{1}{\epsilon_0}\log\left\{\frac{\theta_i G(\alpha_i^*) - \sum_{j=1}^{i-1}\Delta_j + \frac{\gamma^2\theta_1^2}{4c} + \mathcal{L}}{e_0\epsilon_0\mathcal{D}}\right\}$;
8: **end for**

Therefore, we have the first derivative of α_i as follows:

$$\frac{\partial U_b(i)}{\partial\alpha_i} = \frac{e_2\theta_i u\mathcal{L}}{(1-\eta)e_i^{\frac{1}{1-\eta}}}\alpha_i^{\frac{\eta}{1-\eta}} + p_i e_2\theta_i - p_i - \frac{e_3\theta_i^{\epsilon_3}u\mathcal{L}}{(1-\eta)e_1^{\frac{1}{1-\eta}}}\alpha_i^{\frac{\eta}{1-\eta}}. \quad (31)$$

Next, by differentiating $\frac{\partial U_b(i)}{\partial\alpha_i}$ with respect to α_i, we have

$$\frac{\partial^2 U_b(i)}{\partial\alpha_i^2} = -\frac{\eta u\mathcal{L}(e_3\theta^{\epsilon_3} - e_2\theta_i)}{(1-\eta)^2 e_1^{(\frac{1}{1-\eta})}}\alpha_i^{\frac{2\eta-1}{1-\eta}}. \quad (32)$$

Obviously, we have $\frac{\partial^2 U_b(i)}{\partial\beta_i^2} < 0$ by setting $e_3\theta_i^{\epsilon_3} > e_2\theta_i$ and come to the conclusion that (28) is a concave function. Finally, given the premium p_i determined by Stage I, we derive the optimal solution α_i^* of the contract model by setting $\frac{\partial U_b(i)}{\partial\alpha_i} = 0$. We have

$$\hat{\alpha_i} \coloneqq e_1\left\{\frac{p_i[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}{u\mathcal{L}(e_3\theta_i^{\epsilon_3} - e_2\theta_i)}\right\}^{\frac{1-\eta}{\eta}}. \quad (33)$$

According to equation (14) and (27), then we obtain the optimal online time as follows:

$$\hat{d}_i \coloneqq \frac{1}{\epsilon_0}\log\left\{\frac{\theta_i G(p_i,\beta_i) - \sum_{j=1}^{i-1}\Delta_j + \frac{\gamma^2\theta_1^2}{4c} + \mathcal{L}}{e_0\epsilon_0\mathcal{D}}\right\}. \quad (34)$$

B. Stage I: Stackelberg Game Model

Recall $\alpha_i = g(\beta_i)$, then we obtain the optimal claim factor as follows:

$$\hat{\beta}_i \coloneqq \left\{\frac{p_i[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}{u\mathcal{L}(e_3\theta_i^{\epsilon_3} - e_2\theta_i)}\right\}^{\frac{1}{\eta}}. \quad (35)$$

Then transforming (35) to obtain p_i, we have

$$p_i = \frac{u\mathcal{L}(e_3\theta_i^{\epsilon_3} - e_2\theta_i)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}\beta_i^{\eta}. \quad (36)$$

Substituting (36) into (15), we obtain a new utility function of the cyber insurer as follows:

$$U_c = \sum_{i\in\mathbb{N}}\lambda_i\left\{\frac{\mathcal{L}(e_3\theta_i^{\epsilon_3}u - e_2\theta_i)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}\beta_i^{\eta} - (1-u)\beta_i\mathcal{L}\right\}. \quad (37)$$

Therefore, we take the first derivative of β_i as follows:

$$\frac{\partial U_c(i)}{\partial\beta_i} = \frac{\mathcal{L}\eta(e_3\theta_i^{\epsilon_3}u - e_2\theta_i)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}\beta_i^{\eta-1} - (1-u)\mathcal{L} \quad (38)$$

By differentiating $\frac{\partial U_c(i)}{\partial\beta_i}$ with respect to β_i, we have

$$\frac{\partial^2 U_c(i)}{\partial\beta_i^2} = \frac{\mathcal{L}\eta(\eta-1)(e_3\theta_i^{\epsilon_3}u - e_2\theta_i)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}\beta_i^{\eta-2}. \quad (39)$$

Obviously, we have $\frac{\partial^2 U_c(i)}{\partial\beta_i^2} <$ with $0 < \eta < 1$. Thus, we can obtain the optimal price of the claim factor by setting $\frac{\partial U_c(i)}{\partial\beta_i} = 0$, i.e.,

$$\beta_i^* = \left\{\frac{\eta(e_3\theta_i^{\epsilon_3}u - e_2\theta_i u)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}\right\}^{\frac{1}{1-\eta}}. \quad (40)$$

Finally, we have the optimal price of premium as follows:

$$p_i^* = \mathcal{L}\mathcal{F}^{\frac{1}{1-\eta}}(\eta)^{\frac{\eta}{1-\eta}}, \quad (41)$$

where $\mathcal{F} = \frac{(e_3\theta_i^{\epsilon_3}u - e_2\theta_i u)}{[e_2 e_1\theta_i(1-\eta) - e_1(1-\eta)]}$.

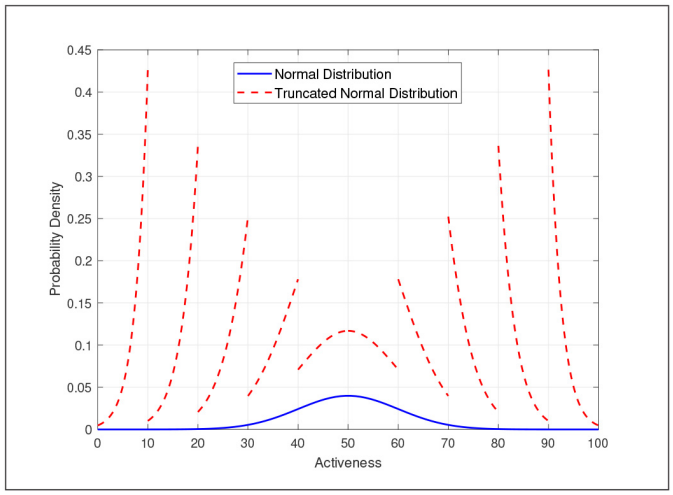


Fig. 5. Probability density of the truncated normal distribution and the normal distribution.

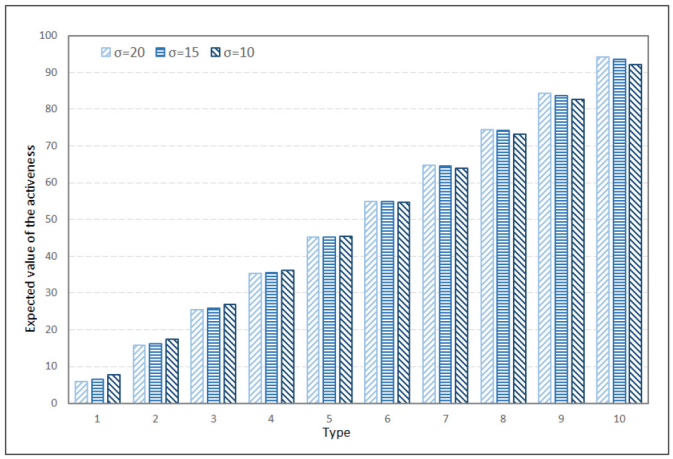


Fig. 6. The expected activeness for each type validators.

TABLE I
PARAMETER SETTING

Parameters	Values
Mean of validators distribution	$\mu = 50$
Variance of validators distribution	$\sigma = 10$
Number of types	$n = 10$
Number of committee members	$N = 1000$
Number of malicious validators	$\hat{n} = 100$
Total reward for each round	$R = 1000$
Evaluation parameter (1)	$e_0 = 100$
Evaluation parameter (2)	$e_1 = 0.5$
Evaluation parameter (3)	$e_2 = 1$
Evaluation parameter (4)	$e_3 = 10$
Annual interest rate	$\epsilon_0 = 0.135$
Pre-defined coefficients	$\eta = 0.1, 0.2, 0.3$
Number of censored validators	$k = 100, 300, 500, 700$
Compensation factor	$u = 0.1, 0.2, 0.3$
Deposit	$\mathcal{D} = 8500$

V. SIMULATION RESULTS AND NUMERICAL ANALYSIS

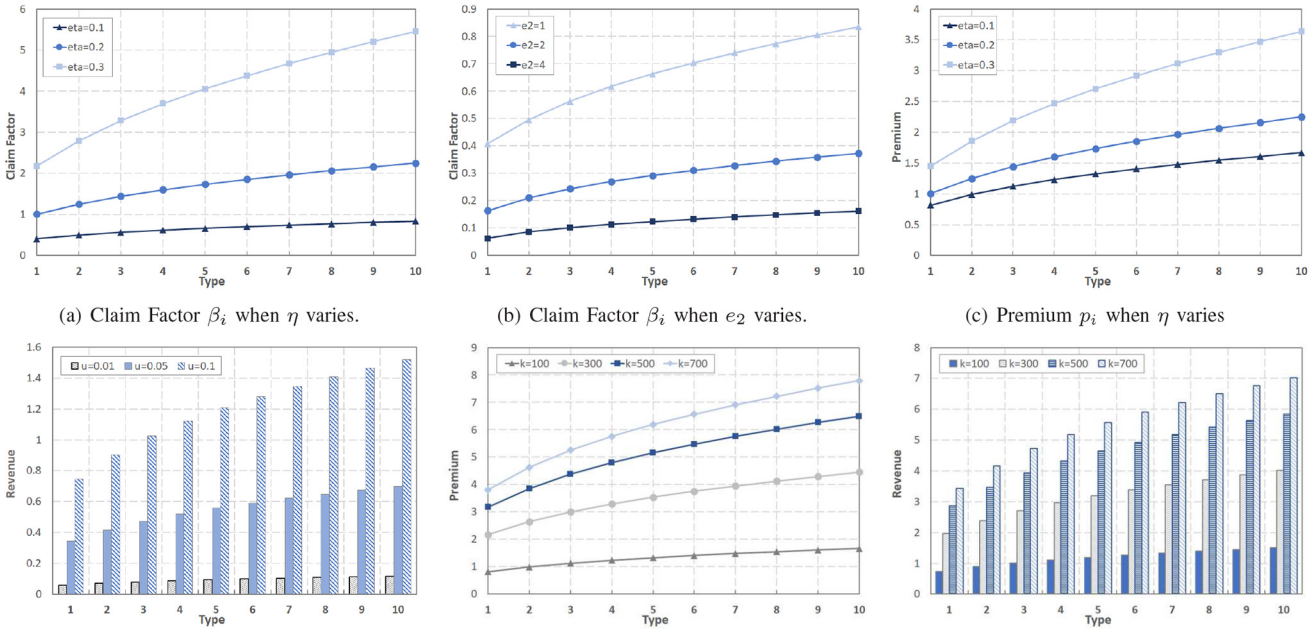
In this section, we first illustrate the distribution of activeness, present the expected value for each type of validator, and then evaluate the impact of the blockchain infrastructure provider decision on the premium and claim factor. Finally, we show the utilities of the validators, the profit of the blockchain infrastructure provider, and the cyber insurer's revenue.

In the initial phase, we consider the activeness of the whole validators to be a *Normal Distribution* with $\mu = 50$ and $\sigma = 10$. In our design, the metric of activeness is uniformly classified into ten intervals, i.e., each interval denotes a single type of validators. When considering the types separately, the probability density function for each type of activeness is modeled as the *Truncated Normal Distribution* with the same parameters $\mu = 50, \sigma = 10$. As shown in Fig. 5, we plot the probability density function (pdf) of truncated normal distribution (i.e., red dot line) according to the pdf of normal distribution (i.e., solid blue line). When only considering a certain type i and its corresponding activeness scope $(a_i, a_{i+1}]$, our plotting result shows that the probability density has been shifted to a higher value. The reason is that the definite integral on the interval $(a_i, a_{i+1}]$ is one while the other elements outside this interval are set to be zero. The probability density change also increases the expected value to a value higher than that of the original normal distribution.

For type i that fits the truncated normal distribution $\mathcal{A}_i(\mu, \sigma, a_i, a_{i+1})$, we present the expected value θ_i with different σ in Fig. 6. We can see that the expected value increases along with the σ decreases in the first five types, but in the last five types, the case is completely opposite. For further analysis, we set $\mu = 50$, $\sigma = 10$, $e_1 = 0.5$, $e_3 = 10$ and $\epsilon_3 = 1.3$. For the discouragement attack assumption, we set $N = 1000$, $\hat{n} = 100$, $k = 100$ and $R = 1000$ for the analysis of the parameters. We list the main parameters in Table I.

According to the Stackelberg game principle, the cyber insurer's optimal claim and premium strategies depend on the decisions made by the lower sub-game. We next study the impact of blockchain infrastructure provider's decisions. According to the utility function in (30), the blockchain infrastructure provider identifies the weight for each item by using the evaluation parameters, i.e., e_1, e_2, e_3, η and u. According to the closed-form of the optimal solution in (40), it is easy to conclude that the optimal solution β_i^* increases along with e_3 and u increase but decreases as e_2 and e_1 grow.

From Fig. 7(a) and Fig. 7(c), we can observe that the claim factor increases when η grows but decreases along with the e_2 grows, where η is applied to define the discount factor α_i. However, the claim factor is a parameter that denotes the claim ratio, which should be less than one. Similar to the previous two sub-figures, the revenue of cyber-insurer also increases as the η grows. Fig. 7(a) only illustrates the growing trend of β_i, wherein $\beta_i \geq 1$ cannot be adopted in a real scenario. Thus, we set $\eta = 0.1$ in the following simulations. From Fig. 7(d), we observe that the compensation factor that the blockchain infrastructure provider determines can also impact the cyber



(a) Claim Factor β_i when η varies.

(b) Claim Factor β_i when e_2 varies.

(c) Premium p_i when η varies

(d) The revenue of cyber insurer when compensation factor varies.

(e) The premium of cyber insurance when the loss varies.

(f) The revenue of cyber insurer when the loss varies.

Fig. 7. The impacts of different parameters on the cyber insurer's decision and revenue.

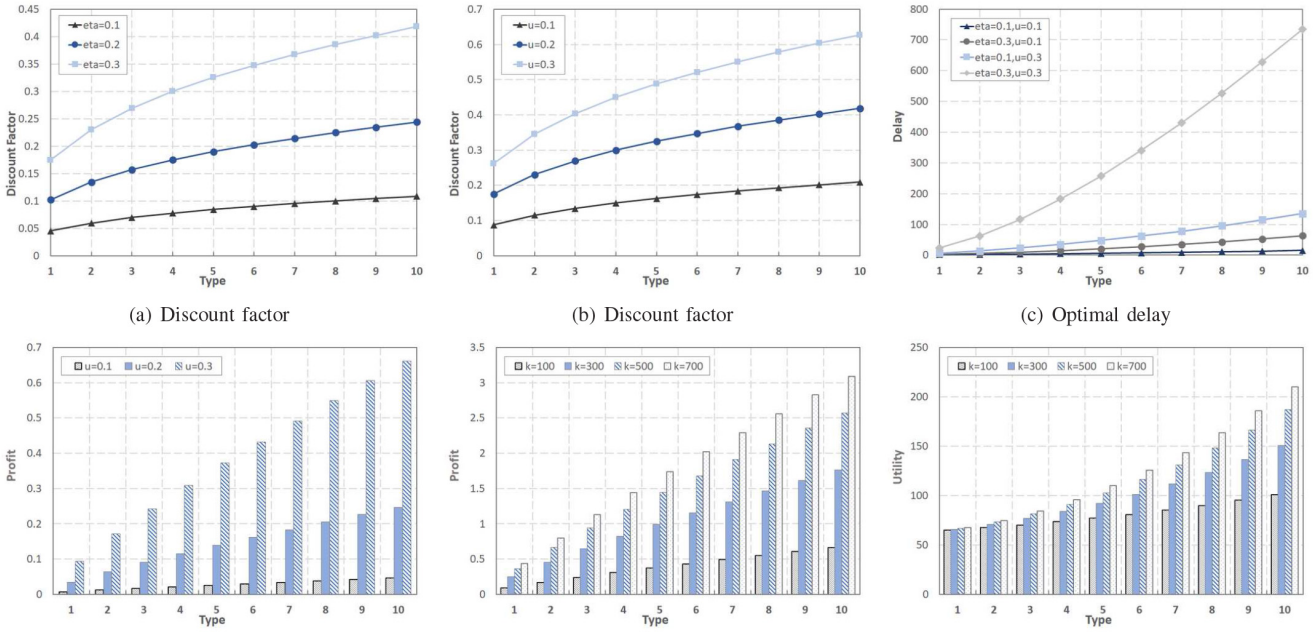
insurer's revenue. The claim should also be given consideration since $\beta_i \geq 1$ when u>0.1, which is not valid. We examine the impact by limiting $u \leq 0.1$. Fig. 7(d) illustrates that a higher compensation factor u would lead to a higher cyber insurer's revenue.

The discouragement attack can be classified into two types: majority attack and minority attack. A majority attack means the attacker has a greater power to control a majority of the validators, while the minority attack is the opposite case. Thus, we set $N = 1000$ validators in total and $\hat{n} = 100$ malicious validators, and let $k = 100$, $k = 300$ denote the minority attack and $k = 500$, $k = 700$ denote the majority attack. Recall the expected loss function in (3), and we can conclude that the expected loss for each validator will be increased when the censored validators grow in number, which finally approaches its reward per round *R*/*N*. Given $e_2 = 1$ and $\eta = 0.1$, we have the growing premium and revenue when increasing the loss, as shown in Fig. 7(e). Besides, Fig. 7(f) also shows that a higher loss brings a higher revenue for the cyber insurer. A positive correlation of the loss, premium, and revenue satisfy the cyber insurer's benefit requirement.

Based on the optimal solutions of cyber insurer, we next investigate the impact of different parameters and loss on the contract (α_i, d_i) individually. In Fig. 8(a) and Fig. 8(b), we set $e_3 = 1.5$ and figure out that, the discount factors α_i of all the contracts increase in terms of η and the compensation factor u. If the metric unit of delay is 'one day', then we set $T = 365$. According to [26], the deposit is 32 ETH (i.e., around 8,500$). Thus, we set $e_0\epsilon_0 = 13.5$ and $\mathcal{D} = 8,500$ to observe the optimal delay. From Fig. 8(c), we can conclude that η and u have the same impact on the optimal delay, i.e., a higher η and a higher u result in a higher optimal delay. Vitalik suggests "1-3 months to rotate the entire validator set" in [10], and the setting in Fig. 8(c) exactly satisfies the statement.

We can also examine the impact of compensation factor u on the profit $G(p_i, \alpha_i)$. Due to the higher discount factor and the claim factor, validators can obtain a higher profit from the contract (α_i, β_i), as shown in Fig. 8(d). Moreover, a higher compensation factor will bring more benefits for the cyber insurer as well as the validators. Still, it does not mean that the blockchain infrastructure provider compensates them by sacrificing its own profit. Fig. 8(c) shows that a validator must stay online for a longer time in order to obtain a larger compensation factor, wherein a longer delay contributes to a higher profit for the blockchain network. Similarly, when the attacker censors more validators, we observe that the validators gain the increasing profit from their own contracts, as shown in Fig. 8(e), which is consistent with our previous assumption in Section II. In Fig. 8(f), it shows that the blockchain network's utility increases in terms of loss growth.

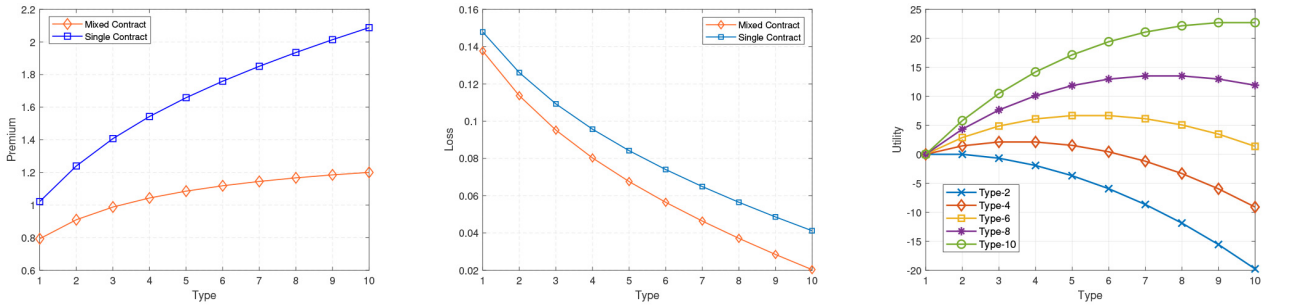
Finally, we compare the premium and the loss of the mixed contract case with the benchmark scheme 'single contract' case, as illustrated in Fig. 9. In Fig. 9(a), we observe that the premium in both cases increases with the validators' type. However, for type-*i* validators, the premium they need to pay in the 'mixed contract' case is less than that of the 'single contract' case. In Fig. 9(b), it shows that the loss in both cases decreases with the validators' type, which means the claim they get from the insurance increases with the validators' type. Apparently, the 'mixed contract' case can provide more insurance claim than a 'single contract' case. We also prove the feasibility of the proposed contract by illustrating the IR and IC constraints in Fig. 9(c). Due to the huge gap of the different utilities, we set a new utility function $U_{i,j} = U_i^+(p_j, \beta_j, \alpha_j, d_j) - U_i^+(p_1, \beta_1, \alpha_1, d_1)$ to denote the original utility without loss of generality. We



(a) Discount factor (b) Discount factor (c) Optimal delay

(d) Profit gained by validators when the compensation factor varies. (e) Profit gained by validators when the loss varies. (f) Blockchain's utility when the loss varies.

Fig. 8. The impacts of different parameters on blockchain's strategies and profits.



(a) The premium that the different-type validators need to pay (b) The loss of the different-type validators (c) Utilities of type-2, type-4, type-6, type-8 and type-10 validators when signing different contracts.

Fig. 9. The comparison with the single contract, and how the utility varies when signing different contracts.

plot the corresponding utilities of the selected type validators when signing the different contracts in Fig. 9(c), indicating that the type-i validator can only achieve maximum utility when selecting the contract that is exactly designed for his own type. This also confirms the inequality (23). For $\forall i \in \{1, \ldots, \mathbb{N}\}$, we have $U_{i,i} \geq 0$, which means $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_1, \beta_1, \alpha_1, d_1)$. Thus, IC and IR constraints are both satisfied.

VI. Conclusion

This paper first analyzes the discouragement attack model, the expected loss of the validators in the blockchain networks with shards, designing cyber insurance under a hierarchical model with the contract theory and Stackelberg game. The founders of Ethereum point out that the withdrawal delay mechanism can resist the discouragement attack. However, how to determine an appropriate delay is still an open question. Therefore, we propose an incentive scheme by integrating the cyber insurance idea to neutralize the cyber risks, determining the different validators' withdrawal delays, and providing the insurance claim for their loss. That means the blockchain system can keep more online deposits to resist the discouragement attack via the 'delay' determined in the contract. Simultaneously, the validators stay online to get insured for the loss caused by the discouragement attack. Moreover, the cyber insurer can also benefit from the insurance premium. With few research works on the discouragement attack, we analyze the attack model first and then explore the cyber insurance idea under the contract theory framework. Based on the simulation and analysis, we can conclude that the proposed contract scheme is able to keep the revenue of cyber-insurer and encourage the validators to be online by providing cyber insurance as an incentive.

Appendix
Proof of Lemma 1

Lemma 1 (Reduction of IR): For all the types, $\forall i \in \{1, \ldots, \mathbb{N}\}$, if we have $\theta_1 < \theta_2 < \cdots < \theta_{\mathbb{N}}$, then the IR constraint of type-i holds only when the constraint of the lowest type validator is satisfied.

Proof: According to the IR constraint $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^-(0,0,0,0)$, for type-1 validators, we have

$$U_1^+(p_1, \beta_1, \alpha_1, d_1) \geq U_1^-(0,0,0,0). \tag{42}$$

According to the IC constraint $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_j, \beta_j, \alpha_j, d_j)$ and $\theta_i > \theta_1$, we have

$$\begin{aligned} U_i^+(p_i, \beta_i, \alpha_i, d_i) &\geq U_i^+(p_1, \beta_1, \alpha_1, d_1), \\ U_i^+(p_1, \beta_1, \alpha_1, d_1) &\geq U_1^+(p_1, \beta_1, \alpha_1, d_1). \end{aligned} \tag{43}$$

Obviously, for given (42) and (43), we can come to the conclusion that

$$U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_1^-(0,0,0,0). \tag{44}$$

Thus, we complete this proof. ■

PROOF OF LEMMA 2

Lemma 2 (Monotonicity): For any contract $(p_i, \beta_i, \alpha_i, d_i)$, $p_i \geq p_j$, $\beta_i \geq \beta_j$, $\alpha_i \geq \alpha_j$ and $d_i \geq d_j$ if and only if $\theta_i \geq \theta_j$.

Proof: For ease of expression, we use $G(\beta_i)$ instead in the following proofs. According to the IC constraint $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_j, \beta_j, \alpha_j, d_j)$, we can obtain the following inequations:

$$\begin{aligned} \theta_i G(\beta_i) + \frac{\gamma^2\theta_i^2}{4c} + c\sigma'^2 - h(d_i) \geq \theta_i G(\beta_j) + \frac{\gamma^2\theta_i^2}{4c} \\ + c\sigma'^2 - h(d_j), \end{aligned} \tag{45}$$

$$\begin{aligned} \theta_j G(\beta_j) + \frac{\gamma^2\theta_j^2}{4c} + c\sigma'^2 - h(d_j) \geq \theta_j G(\beta_i) + \frac{\gamma^2\theta_j^2}{4c} \\ + c\sigma'^2 - h(d_i). \end{aligned} \tag{46}$$

Then, we can obtain a new inequation by adding (45) and (46) together:

$$(\theta_i - \theta_j)[G(\beta_i) - G(\beta_j)] \geq 0. \tag{47}$$

(a) Sufficiency: If $\theta_i > \theta_j$, we can get $G(\beta_i) - G(\beta_j) \geq 0$ by deriving from (47). As $G'(\beta_i) > 0$, we can conclude that $\beta_i > \beta_j$. So the sufficiency condition is proved.

(b) Necessity: The inequation in (47) can be transformed and rewritten as

$$\theta_i[G(\beta_i) - G(\beta_j)] \geq \theta_j[G(\beta_i) - G(\beta_j)], \tag{48}$$

where $G'(\beta_i) > 0$ and $\beta_i > \beta_j$. We have $G(\beta_i) - G(\beta_j) > 0$ and conclude that $\theta_i > \theta_j$ easily. ■

Proposition 1: For all the contracts $(p_i, \beta_i, \alpha_i, d_i)$ $(\forall i \in \{1, \ldots, \mathbb{N}\})$, we have $d_i \geq d_j$, if and only if $\beta_i \geq \beta_j$.

Proof: According to the IC constraint expressed in (46), we have

$$h(d_i) - h(d_j) \geq \theta_j[G(\beta_i) - G(\beta_j)]. \tag{49}$$

(a) Sufficiency: If $\beta_i \geq \beta_j$, we can conclude that $G(\beta_i) - G(\beta_j) > 0$ due to $G'(\beta_i) > 0$. Then, we $h(d_i) - h(d_j) > 0$ and $h(d_i) > h(d_j)$. Since $h'(d_i) > 0$, then $d_i > d_j$.

(b) Necessity: We have the following inequation according to the IC constraint expressed in (45):

$$\theta_i[G(\beta_i) - G(\beta_j)] \geq h(d_i) - h(d_j). \tag{50}$$

If $d_i \geq d_j$, we have $h(d_i) - h(d_j) > 0$ due to $h'(d_i) > 0$, which implies $\theta_i[G(\beta_i) - G(\beta_j)] > 0$. Since $G'(\beta_i) > 0$, then we easily have $\beta_i > \beta_j$. The proof is completed. ■

Lemma 2 indicates that in such a feasible contract, the validators who keep active online for a longer time will gain a higher discount factor and coverage factor.

PROOF OF LEMMA 3

Lemma 3 (Reduction of IC): There are four definitions regarding the IC constraints between type-*i* and type-*j* $(\forall i \neq j)$:

(a) If $\forall j \in \{1, 2, \ldots, i-1\}$, the constraints are called Downward Incentive Constraints (**DIC**s).
(b) If $j = i-1$, the constraint is called Local Downward Incentive Constraint (**LDIC**).
(c) If $\forall j \in \{i+1, \ldots, N\}$, the constraints are called Upward Incentive Constraints (**UIC**s).
(d) If $j = i+1$, the constraint is called Local Upward Incentive Constraint (**LUIC**).

With the monotonicity conditions $\theta_1 < \theta_2 < \cdots < \theta_{\mathbb{N}}$, the DICs can be reduced as LDICs, i.e., $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1})$ and the UICs can be reduced as the LUICs, i.e., $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_{i+1}, \beta_{i+1}, \alpha_{i+1}, d_{i+1})$.

Proof: All of the validators are classified into different types, and there exists the IC constraint between any two types. As a result, there are too many IC constraints in total, which will increase the difficulty of computation. Here we will prove that all of the IC constraints can be reduced as LDICs. Consider three adjacent types, i.e., type $i-1$, type i and type $i+1$, which follows $\forall i \in \{1, \ldots, N-1\}$. According to the IC constraints, we revise this inequation $U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_j, \beta_j, \alpha_j, d_j)$ and then have the following two inequations:

$$U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_{i+1}^+(p_i, \beta_i, \alpha_i, d_i), \tag{51}$$

$$U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_i^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1}). \tag{52}$$

According to the momotonicity condition $\theta_{i+1} > \theta_i$ and $\beta_i \geq \beta_{i-1}$, we have the inequation:

$$(\theta_{i+1} - \theta_i) G(\beta_i) \geq (\theta_{i+1} - \theta_i) G(\beta_{i-1}). \tag{53}$$

Then we transform the inequation (53) to the following one:

$$\begin{aligned} \theta_{i+1} G(\beta_i) + \frac{\gamma\theta_{i+1}^2}{4c} - \theta_i G(\beta_i) - \frac{\gamma\theta_i^2}{4c} \\ \geq \theta_{i+1} G(\beta_{i-1}) + \frac{\gamma\theta_{i+1}^2}{4c} - \theta_i G(\beta_{i-1}) - \frac{\gamma\theta_i^2}{4c}. \end{aligned} \tag{54}$$

To proceed the reduction of IC constraints, we add (53) to the inequation (54), and obtain a new inequation, i.e.,

$$U_{i+1}^+(p_i, \beta_i, \alpha_i, d_i) \geq U_{i+1}^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1}). \tag{55}$$

Combine the inequation (51) and (55), we can easily get:

$$U_i^+(p_i, \beta_i, \alpha_i, d_i) \geq U_{i+1}^+(p_i, \beta_i, \alpha_i, d_i), \tag{56}$$

$$U_{i+1}^+(p_i, \beta_i, \alpha_i, d_i) \geq U_{i+1}^+(p_{i-1}, \beta_{i-1}, \alpha_{i-1}, d_{i-1}). \tag{57}$$

Repeat the steps described above, we can obtain the following constraints:

$$\begin{aligned} U_{i+1}^{+}(p_{i+1},\beta_{i+1},\alpha_{i+1},d_{i+1}) &\geq U_{i+1}^{+}(\beta_{i-1},d_{i-1}) \\ &\geq U_{i+1}^{+}(p_{i-3},\beta_{i-3},\alpha_{i-3},d_{i-3}) \\ &\geq \cdots \\ &\geq U_{i+1}^{+}(p_1,\beta_1,\alpha_1,d_1) \\ &\geq U_1^{+}(p_1,\beta_1,\alpha_1,d_1). \end{aligned} \tag{58}$$

Similarly, for the type θ_{i-1} and all the contracts which follow $\forall i \in \{2,\ldots,\mathbb{N}\}$, we can easily obtain the following inequations by the same steps above:

$$\begin{aligned} &U_{i-1}^{+}(p_{i-1},\beta_{i-1},\alpha_{i-1},d_{i-1}) \\ &\geq U_{i-1}^{+}(p_{i+1},\beta_{i+1},\alpha_{i+1},d_{i+1}) \\ &\geq \cdots \\ &\geq U_{i-1}^{+}(p_{\mathbb{N}},\beta_{\mathbb{N}},\alpha_{\mathbb{N}},d_{\mathbb{N}}). \end{aligned} \tag{59}$$

Therefore, we present the proof that if the LDICs are satisfied, all the DICs also hold, as well as the LUICs and UICs proved in (59). ■

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] W. Wang *et al.*, "A survey on consensus mechanisms and mining management in blockchain networks," 2018. [Online]. Available: arXiv:1805.02707.

[3] S. Nakamoto. *Bitcoin*. Accessed: Jan, 2009. [Online]. Available: https://bitcoin.org/en/

[4] *Coinmarketcap*. Accessed: Oct. 22, 2020. [Online]. Available: https://coinmarketcap.com/

[5] *Ethereum Foundation*. Accessed: Oct. 12, 2020. [Online]. Available: https://www.ethereum.org/

[6] QuantumMechanic. *Proof of Stake Instead of Proof of Work*. Accessed: Jun. 11, 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=27787.0

[7] V. Buterin. *Proof of Stake Faq*. Accessed: Mar. 20, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-are-the-benefits-of-proof-of-stake-as-opposed-to-proof-of-work

[8] V. Buterin. *Discouragement Attacks*. Accessed: Dec. 16, 2018. [Online]. Available: https://github.com/ethereum/research/blob/master/papers/discouragement/discouragement.pdf

[9] D. Lancashire. *On Discouragement Attacks*. Accessed: Dec. 20, 2018. [Online]. Available: https://org.saito.tech/on-discouragement-attacks/

[10] V. Buterin. *Rate-Limiting Entry/Exits, Not Withdrawals*. Accessed: Feb. 3, 2019. [Online]. Available: https://ethresear.ch/t/rate-limiting-entry-exits-not-withdrawals/4942

[11] C. Beekhuizen. *Validated: Staking on ETH2 #0*. Accessed: Nov. 27, 2019. [Online]. Available: https://blog.ethereum.org/2019/11/27/Validated-Staking-on-eth2-0/

[12] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[13] P4Titan. *SlimCoin: A Peer-to-Peer Crypto-Currency With Proof-of-Burn*. Accessed: May 17, 2014. [Online]. Available: http://slimco.in

[14] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. ACM 1st Workshop Syst. Softw. Trusted Execution*, 2016, pp. 1–6.

[15] Hyperledger. *Hyperledger Fabric*. Accessed: Aug. 2020. [Online]. Available: https://www.hyperledger.org/projects/fabric

[16] IBM. *IBM Blockchain Services*. Accessed: Sep. 2020. [Online]. Available: https://www.ibm.com/blockchain/services

[17] Atonomi. *Atonomi: Bringing Trust and Security to IoT*. Accessed: Aug. 2020. [Online]. Available: https://atonomi.io/

[18] Chain of Things Telegram Group. *Chain of Things*. Accessed: Apr. 2020. [Online]. Available: https://www.chainofthings.com/

[19] IoTex. *Internet of Trusted Things*. Accessed: Apr. 2020. [Online]. Available: https://www.iotex.io/

[20] K.-K. R. Choo, Z. Yan, and W. Meng, "Blockchain in industrial iot applications: Security and privacy advances, challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4119–4121, Jun. 2020.

[21] Z. Guan *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[22] S. Pal, T. Rabehaja, M. Hitchens, V. Varadharajan, and A. Hill, "On the design of a flexible delegation model for the Internet of Things using blockchain," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3521–3530, May 2020.

[23] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6543–6552, Oct. 2020.

[24] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in and beyond," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7094–7104, Nov. 2020.

[25] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving framework based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020.

[26] E. Foundation. *Ethereum 2.0 (Serenity) Phases*. Accessed: Sep. 2020. [Online]. Available: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/

[27] PWC. (2020). *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*. [Online]. Available: https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html

[28] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: The role of pre-screening and security interdependence," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2226–2239, Sep. 2018.

[29] M. M. Khalili, P. Naghizadeh, and M. Liu, "Embracing risk dependency in designing cyber-insurance contracts," in *Proc. IEEE 55th Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, 2017, pp. 926–933.

[30] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security pre-screening," in *Proc. Int. Conf. Game Theory Netw.*, 2017, pp. 63–73.

[31] M. M. Khalili, M. Liu, and S. Romanosky, "Embracing and controlling risk dependency in cyber-insurance policy underwriting," *J. Cybersecurity*, vol. 5, no. 1, 2019, Art. no. tyz010.

[32] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, and Y. Zhang, "Cyber risk management with risk aware cyber-insurance in blockchain networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2018, pp. 1–7.

[33] X. Lu, D. Niyato, H. Jiang, P. Wang, and H. V. Poor, "Cyber insurance for heterogeneous wireless networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 21–27, Jun. 2018.

[34] P. Bolton and M. Dewatripont, *Contract Theory*. Cambridge, MA, USA: MIT Press, 2005.

[35] J. Li, T. Liu, D. Niyato, P. Wang, J. Li, and Z. Han, "Contract-based approach for security deposit in blockchain networks with shards," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2019, pp. 75–82.

[36] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[37] Z. Xiong, J. Zhao, D. Niyato, P. Wang, and Y. Zhang, "Design of contract-based sponsorship scheme in stackelberg game for sponsored content market," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

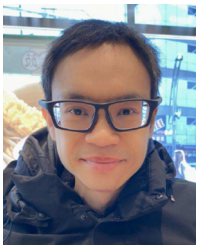
[38] J. Li *et al.*, "A contract-theoretic cyber insurance for withdraw delay in the blockchain networks with shards," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–7.

[39] V. Buterin. *The Censorship Problem*. Accessed: Jan. 28, 2015. [Online]. Available: https://blog.ethereum.org/2015/06/06/the-problem-of-censorship/ 28, 2015.

[40] hackingresear.ch. *Discouragement Attacks*. Accessed: Nov. 12, 2020. [Online]. Available: https://hackingresear.ch/discouragement-attacks/

[41] V. Buterin. *A Griefing Factor Analysis Model*. Accessed: Jun. 2018. [Online]. Available: https://ethresear.ch/t/a-griefing-factor-analysis-model/2338 2018.

Jing Li received the B.S. and M.S. degrees in computer science from North China Electric Power University, Beijing, China, in 2014 and 2018, respectively. She is currently pursuing the Ph.D. degree with Electrical and Computer Engineering Department, University of Houston, USA. Her research interests include the blockchain and game theory.



Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from the King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999, and the Ph.D. 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 are in the areas of Internet of Things, machine learning, and incentive mechanism design.

Choong Seon Hong (Senior Member, IEEE) received the B.S. and M.S. degrees in electronic engineering from Kyung Hee University, Seoul, South Korea, in 1983 and 1985, respectively, and the Ph.D. degree from Keio University, Tokyo, Japan, in 1997. He is working as a Professor with the Department of Computer Science and Engineering, Kyung Hee University. His research interests include future Internet, ad hoc networks, network management, and network security. He has served as the General Chair, the TPC Chair/Member, or an Organizing Committee Member for international conferences, such as NOMS, IM, APNOMS, E2EMON, CCNC, ADSN, ICPP, DIM, WISA, BcN, TINA, SAINT, and ICOIN. He was an Associate Editor of the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the *Journal of Communications and Networks*, and an Associate Technical Editor of *IEEE Communications Magazine*. He is currently an Associate Editor of the *International Journal of Network Management* and *Future Internet*. He is a member of ACM, IEICE, IPSJ, KIISE, KICS, KIPS, and OSIA.

Kyung-Joon Park (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering, and the Ph.D. degree in electrical engineering and computer science from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2005, respectively. From 2005 to 2006, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2006 to 2010, he was a Postdoctoral Research Associate with the Department of Computer Science, University of Illinois at Urbana–Champaign, Champaign, IL, USA. He is currently a Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His research interests include resilient cyber–physical systems and smart production systems.

Li Wang (Senior Member, IEEE) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2009. She is currently a Full Professor with the School of Computer Science (National Pilot Software Engineering School), BUPT, where she is also an Associate Dean and the Heads of the High Performance Computing and Networking Laboratory. She is also a Member of the Key Laboratory, Universal Wireless Communications, Ministry of Education, China. She also held Visiting Positions with the School of Electrical and Computer Engineering, Georgia Tech, Atlanta, GA, USA, from December 2013 to January 2015, and with the Department of Signals and Systems, Chalmers University of Technology, Gothenburg, Sweden, from August to November 2015 and July to August 2018. She has authored/coauthored almost 50 journal papers and two books. Her current research interests include wireless communications, distributed networking and storage, vehicular communications, social networks, and edge AI. She was a recipient of the 2013 Beijing Young Elite Faculty for Higher Education Award, the Best Paper Awards from several IEEE conferences, e.g., IEEE ICCC 2017, IEEE GLOBECOM 2018, IEEE WCSP 2019, and the Beijing Technology Rising Star Award in 2018. She was the Symposium Chair of IEEE ICC 2019 on Cognitive Radio and Networks Symposium and the Tutorial Chair of IEEE VTC 2019-fall. She also serves as the Vice Chair of Meetings and Conference Committee for IEEE Communication Society Asia–Pacific Board for the term of 2020–2021, and chairs the special interest group on Social Behavior Driven Cognitive Radio Networks for IEEE Technical Committee on Cognitive Networks. She has served on TPC of multiple IEEE conferences, including IEEE Infocom, Globecom, International Conference on Communications, IEEE Wireless Communications and Networking Conference, and IEEE Vehicular Technology Conference in recent years. She currently serves on the editorial boards for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, *Computer Networks*, IEEE ACCESS, and *China Communications*.

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Idaho. He is currently a John and Rebecca Moores Professor of Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, Houston, TX, USA, as well as in the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JSAC) in 2016, and the several best paper awards in IEEE conferences. He is also the winner of 2021 IEEE Kiyo Tomiyasu Award, for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks." He has been a 1% Highly Cited Researcher since 2017 according to Web of Science. He is currently an IEEE Communications Society Distinguished Lecturer from 2015 to 2018, AAAS Fellow since 2019 and ACM Distinguished Member since 2019.