A Contract-Theoretic Cyber Insurance for Withdraw Delay in the Blockchain Networks with Shards

1st Jing Li
Department of Electrical and Computer Engineering
University of Houston
Houston, USA
jli84@uh.edu

2nd Dusit Niyato
School of Computer Engineering
Nanyang Technological University
639798, Singapore
dniyato@ntu.edu.sg

3rd Choong Seon Hong
Department of Computer Science and Engineering
Kyung Hee University
Yongin-si, Gyeonggi-do, Korea
cshong@khu.ac.kr

4th Kyung-Joon Park
Department of Information and Communication Engineering
Daegu Gyeongbuk Institute of Science and Technology
Daegu 42988, Korea
kjp@dgist.ac.kr

5th Li Wang
School of Electronic Engineering
Beijing University of Posts and Telecommunications
Beijing, China
liwang@bupt.edu.cn

6th Zhu Han
Department of Electrical and Computer Engineering
University of Houston
Houston, USA
hanzhu22@gmail.com

***Abstract*—As the basis of the most existing blockchain networks, Proof of Work (PoW) consensus protocol highly relies on the computational resources, and thus causing a huge waste of energy. Proof of Stake (PoS) is the alternative to relieve the PoW dilemma. However, it is also under threat, i.e., discouragement attack, which is a way to bring down the blockchain networks without any effective defense against it. To prevent the discouragement attack, the founders of Ethereum argue that the system should set a withdraw delay instead of allowing the validators entry/exit quickly. But how to determine the delay is still an open question. In this paper, we adopt the cyber insurance idea and propose the insurance contract to help determine the withdraw delay, as well as the insurance claim to relieve the loss of victims. Specifically, instead of requiring the insurance premium from the validators, the cyber insurer first signs the contract with the blockchain representative (e.g., beacon chain). Then the blockchain representative would sign a series of contracts with the validators. By such design, the validators can obtain the insurance claim without paying the premium, while the blockchain networks can keep the validators staying online to resist the discouragement attack. Finally, through the simulations, we demonstrate that the proposed model is capable of providing adaptive insurance contracts for the different validators and keeping the profits of the blockchain network and the cyber insurer.**

***Index Terms*—Blockchain, Proof of Stake, discouragement attack, cyber insurance, contract theory.**

I. Introduction

As the decentralized computing paradigm, the tamper-proof ledger and the trustless platform, blockchain technology is capable of various of the commercial and industrial applications. Blockchain was first proposed by Nakamoto in the remarkable project [1], and designed to perform as a platform with the characteristics of permissionless, decentralization, tamper-resistance, transparency for the trustless parties [2]. With the advent of Bitcoin (BTC) [3], the 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 the financial issues, Ethereum aims at being a "World Computer", which allows everyone to be a developer to write his own code in order to create new kinds of applications [5].

The basic idea of the blockchain is that a series of undeniable blocks that are verified by the different parties without a central party. These blocks are connected with each other 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], which requires all the participants can win the opportunity of mining block only by competing their hash rate with each other. 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. Also, the Ethereum Foundation deployed PoW in their 1.0 version, wherein many distributed applications has been developed based on it, e.g., DAI [6], DeFi [7], Wyre [8] and so on.

As a result, the aggravation of the hash rate competition causes a huge waste of resources. Numerous researchers are seeking for new alternatives that serve as the same function. Proof of Stake (PoS) is firstly proposed in the Bitcoin Forum [9], i.e., the leader selection relies on the number of stake rather than the computational resources. Ethereum Foundation initiated the Ethereum 2.0 [10] to realize this mechanism. As one of the most popular blockchain projects, it also introduces the sharding technology to further improve the performance.

978-1-7281-5089-5/20/$31.00 ©2020 IEEE

Every validator is able to exit/entry the sharding committees at the end of each round. However, the blockchain network that is deployed with PoS is also vulnerable to a series of the new forms of attacks. Vitalik explored a new type of attack that may bring down the whole blockchain network, which is called *Discouragement Attack* [11].

Recently, Vitalik publishes a new idea about the validator sharding set update [12], which prevents the validators from all withdrawing as soon as they perform a large scale attack before they can be detected. A better way is to set a withdrawal delay, and thus, the validators can exit their sets by waiting in a queue for withdrawing. This idea is obviously resistant to the discouragement attack, but there still exits some open questions, i.e., how to determine the withdrawal delay for all the validators and how to select the validators in a queue. With the consideration of the risk introduced by the discouragement attack, it is necessary to design an appropriate incentive scheme for the blockchain networks, which encourage the validators to stay online as well as neutralize the risk for the whole networks.

Cyber insurance is a useful economic tool for transferring the cyber risk, which motivates more and more researchers to investigate it in various network scenarios. Khalili *et al.* [13] investigate 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 the cyber insurance, see e.g., [14] and [15]. Their "interdependent nature" idea does a good job of explaining the relation between the entities and the networks, which can also apply to the participants and the blockchain networks. Feng *et al.* [16], 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. Other cyber insurance researches in the networks, see e.g., [17], [18] and [19].

Inspired by the above work, we explore the discouragement attack within the PoS mechanism in the blockchain networks with shards, adopt the cyber-insurance as an incentive for motivating the validators' online duration. Owing to the anonymity of the validators and the weak leadership of the beacon chain, there exists the *information asymmetry* problem between them. Therefore, we formulate the problem under the contract theory [20] framework. First of all, we analyze the discouragement attack model and the expected loss for all kinds of validators (i.e., malicious, censored, uncensored), and propose the contract design with the attack model. Second, we can determine the the different validators' delay (the time when they are permitted to leave) and specify their insurance claim by the contracts. The beacon chain with a weak leadership design the contracts for all the validators and pay all the premium for the risk incurred by the discouragement attack, and the cyber insurer will pay the claim for the victims. The validators would prefer such 'free' contracts for their benefit. Last but not the least, by determining the delay and the claim at the same time, the blockchain networks, cyber insurer and the validators can benefit from the contracts. We prove the feasibility of the contracts and present the optimal results in the simulation.

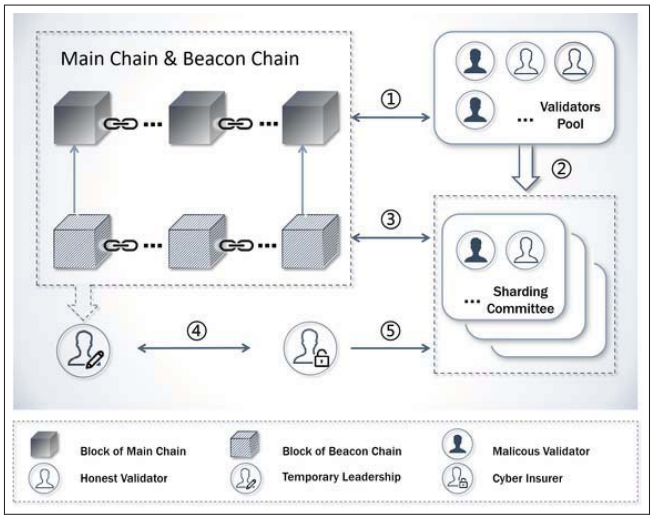


Fig. 1. An overview of the blockchain networks with shards.

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

II. System Model

In this section, we first introduce the discouragement attack model, the reward distribution function, the expected loss, then present the utility models for the validators, beacon chain and the cyber insurer.

A brief overview of the system model can be referred to Fig. 1. We propose the contract theoretic incentive scheme, and use the cyber insurance as the incentive for validators' participation. We will explain the details of the work process in order. (1) The main chain that is deployed with the PoW consensus protocol is the first layer of Ethereum 2.0, which is responsible for recording all the finalized transaction, as well as recruiting the validators. (2) The malicious validators are controlled by the attacker, and blend in with other honest validators in the validator pool. All of the validators will be randomly selected by RANDAO+VDF [10] to form the different sharding committees. (3) The beacon chain that is deployed with PoS consensus protocol is the second layer of Ethereum 2.0, which is responsible for recording the administrative transactions of all the sharding committees. Thus, the beacon chain is able to design the contracts with a weak leadership. (4) A block manager with a temporary leadership signs the insurance contract with the cyber insurer, and pays the premium for the validators. (5) The cyber insurer will

pay the claim for the victims if there exists a discouragement attack.

From the incentive perspective, the beacon chain tries to maximize the participation (i.e., delay and online deposits) to hold its market value and minimize the premium for the insurer. For the validators, 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 the contracts with a longer online time, which means a higher claim for the potential risk, but an inappropriate contract would lead to a lower profit.

A. Discouragement Attack Model

Discouragement attack means that the malicious validators controlled by the attacker acting illegally inside the PoS consensus mechanism in order to reduce other validators' revenue. Specifically, the malicious ones censor some of the honest validators' signing results, and control the result by holding a certain amount of stake. Thus, the censored validators would gain nothing because their signatures are not included in the finalized results. As a result, the honest validators would refuse to sign or vote any more and be offline gradually. And the malicious ones control more and more stakes and rewards. Finally, the attacker behind them can initiate the double-spending attack, censorship attack or any other kind of attack on the chain by manipulating the finalized blocks.

Suppose $\mathcal{N}$ is the total number of the validators in the validator pool, M is the malicious validators, $\hat{n}$ is the threshold of validators for confirming the results, and N is the total validator number.

For a certain committee $\mathcal{I}$, we model the attack as a binomial distribution variable. Thus, the attack probability $\mathcal{A}$ can be expressed as follows:

$$\mathcal{A} = 1 - \sum_{k=0}^{\hat{n}-1} \binom{N}{k} (M/\mathcal{N})^k (1 - M/\mathcal{N})^{(N-k)}. \quad (1)$$

B. Reward Distribution Function and Expected Loss

To better analyze the attack model, the paper [11] introduces a useful concept called *griefing factor* and a reward distribution function with the bounded griefing factor. If there exists a majority attack, the validators can be identified as three types: the malicious validators, the censored validators and the uncensored validators. We present the reward distribution and the loss of the above three groups validator under the majority attack. Suppose there are N validators in committee $\mathcal{I}$, $\hat{n}$ malicious validators, $\hat{k}$ censored validators and the total reward for each round is R. It is obvious that each every validator contributing to a PoS blockchain's work earns R/N if no one is malicious. But if there exist the malicious validators, according to Vitalik's idea [21], 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:

$$l_1 = \frac{R}{N}. \quad (2)$$

$$l_2 = \frac{R}{N} - \frac{R(N-\hat{k})}{N^2} = \frac{R\hat{k}}{N^2}. \quad (3)$$

C. Validator Utility Model

According to the Ethereum 2.0 design, the validators will be randomly selected from the validator pool into the different sharding committees. Thus, there exists a variety of validators with different stakes or savings. We first classify the users into different types: type-1, type-2, ..., type-$\mathbb{N}$. The classification criterion is based on their savings in blockchain. Let θ_i represent the type, and the type θ_i follows the inequation:

$$\theta_1 < \theta_2 < ... < \theta_{\mathbb{N}}. \quad (4)$$

In order to determine the appropriate delay for the different types of validators and maximize the profits of the blockchain infrastructure provider and the cyber insurer, we first set the contracts between the blockchain infrastructure provider and the validators as: (d_i, c_i), where d_i is the delay for the validators when they can apply to exit or switch, and c_i is the claim that they can get from the insurance. That means, the validators have to keep their online time and online activities to obtain the sufficient insurance claim. Otherwise, they would be punished or at a high risk of reward loss.

For type-i validators, the utility that can be obtained from the insurance contract (d_i, c_i) i s as follows:

$$u_{v(i)} = \mathcal{A}\beta_1\theta_i c_i - \frac{d_i}{T}\mathbb{E}(loss) + (1-\mathcal{A})\beta_2\frac{d_i}{T}\frac{R}{N} - \omega d_i, \quad (5)$$

where β_1 and β_2 are the evaluation factors for c_i and R, T is the time slot of one round, $\mathbb{E}(loss)$ is the expected loss of a validator when the discouragement attack occurs, and ω is the expected unit cost of the validators keeping online. Thus, the first term of (5) is the evaluation function of insurance claim, the second term denotes the expected loss of the delay d_i and the third term is the expected reward obtained from the blockchain networks. Note that every validator has the probability of being censored in each round. Suppose the malicious validators initiate the censorship attack on the validators randomly, and the expected number censored validators is $\hat{k}$ considering the cost and benefit. Thus, we have the expected loss function for the validators:

$$\begin{aligned} \mathbb{E}(loss) &= \mathcal{A}\frac{\hat{k}}{(N-\hat{n})}l_1 + \mathcal{A}\frac{(N-\hat{k}-\hat{n})}{(N-\hat{n})}l_2, \\ &= \mathcal{A}\frac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\frac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}, \end{aligned} \quad (6)$$

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.

Therefore, the objective of type-i validators is to maximize the utility obtained from the insurance contract (d_i, c_i), described by

$$\max_{(d_i,s_i)} \quad u_{v(i)} = \mathcal{A}\beta_1\theta_i c_i - \frac{d_i}{T}\Bigg\{\mathcal{A}\frac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\frac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}\Bigg\} + (1-\mathcal{A})\beta_2\frac{d_i}{T}\frac{R}{N} - \omega d_i \geq 0. \tag{7}$$

D. Blockchain Utility Model

In a blockchain network with shards (e.g., Ethereum 2.0 [5]), the beacon chain records all the administrative information within the network. Thus, we consider the block managers of the beacon chain can be considered as the temporary leaders, who are responsible for designing the contracts for all types of the validators. The profit obtained from a type-i validator is defined as

$$U_{B(i)} = \pi(\theta_i, d_i) + u(\theta_i) - \sigma(d_i, \gamma) - v(d_i, R) - P_i, \tag{8}$$

where $\pi(\cdot)$ is a monotonically increasing function for evaluating the online deposit of the type-i validators with $\pi' > 0$ and $\pi'' \leq 0$, $u(\cdot)$ is the function for evaluating the market value contributed by the online deposits, with $u' > 0$ and $u'' \geq 0$, $\sigma(\cdot)$ is the function for evaluating the loss of market value that is caused by the type-i validators based on its delay d_i and the risk factor γ, with $\sigma' > 0$ and $\sigma'' \geq 0$, $v(\cdot)$ is the total reward that is assigned to the validators, with $v' > 0$ and $v'' \geq 0$, and the last term is the premium that is submitted to the cyber insurer. Intuitively, the longer delay and the higher type offer the more profit for the blockchain network.

Therefore, the objective of the blockchain is to maximize the utility obtained from the validators of all types with the pre-estimated probability distribution λ_i is

$$\max_{(d_i,c_i)} \quad U_B = \sum_{i\in\mathbb{N}} \lambda_i \Big\{\pi(\theta_i, d_i) + u(\theta_i) - \sigma(d_i, \gamma) - v(d_i, R)\Big\} - P. \tag{9}$$

E. Cyber Insurer Utility Model

According to the previous analysis, the cyber insurer provides the claim $\mathcal{C}$ for the validators to relieve the loss caused by the discouragement attacks, where $\mathcal{C} = \sum_{i=1}^{\mathbb{N}} \lambda_i c_i$. But it would receive the premium submitted by the blockchain service provider instead of the validators. It is clear that insurer's revenue is the difference of the premium and the claim. The utility function of the cyber insurer is as follows:

$$U_C = P - \mathcal{A}\mathcal{C}, \tag{10}$$

III. Contract Design

In this section, we first formulate the problem among the validators, the beacon chain and the cyber insurer. With the consideration of all parties' profits, we present the proof of individual rationality and incentive compatibility constraints. And then, we obtain a new problem by reducing the constraints. Finally, the optimal result can be obtained through the mathematical tools.

A. Problem Formulation

Before formulating the problem, we first introduce two necessary principles under the contract theory framework [20]: Individual Rationality (**IR**) and Incentive Compatibility (**IC**). IR means that a rational validator will accept a contract only when the utility provided by the contract is larger than zero, i.e.,

$$u_{v(i)} = \mathcal{A}\beta_1\theta_i c_i - \frac{d_i}{T}\Bigg\{\mathcal{A}\frac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\frac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}\Bigg\} + (1-\mathcal{A})\beta_2\frac{d_i}{T}\frac{R}{N} - \omega d_i \geq 0. \tag{11}$$

For the cyber insurer, he would design a contract to maximize his own profit. In this paper, we consider that the insurer's profit not only includes the difference between the premium and claim, but also includes the investment of the insurance premium [22]. Thus, the IR rules for the cyber insurer can be described as accepting the contract only when his utility is larger than zero, i.e.,

$$P - \mathcal{A}\mathcal{C} \geq 0. \tag{12}$$

IC means that a type-i validator can only obtain the maximum profit by choosing the contract (d_i, c_i) rather than all the other contracts (d_j, c_j) $(\forall i, j, i \neq j)$, i.e.,

$$u_{v(i)}(d_i, c_i) \geq u_{v(i)}(d_j, c_j). \tag{13}$$

Therefore, we can formulate the optimal problem as follows:

$$\max_{(d_i,c_i)} \quad U_B = \sum_{i\in\mathbb{N}} \lambda_i \Big\{\pi(\theta_i, d_i) + u(\theta_i) - \sigma(d_i, \gamma) - v(d_i, R)\Big\} - P, \tag{14}$$

s.t.

$$\begin{aligned}
&(a) \quad \mathcal{A}\beta_1\theta_i c_i - \tfrac{d_i}{T}\Big\{\mathcal{A}\tfrac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\tfrac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}\Big\} + (1-\mathcal{A})\beta_2\tfrac{d_i}{T}\tfrac{R}{N} - \omega d_i \geq 0,\\
&(b) \quad P - \mathcal{A}\mathcal{C} \geq 0,\\
&(c) \quad u_{v(i)}(d_i, c_i) \geq u_{v(i)}(d_j, c_j),\\
&(d) \quad \theta_1 < \theta_2 < ... < \theta_{\mathbb{N}}.
\end{aligned}$$

wherein (a) and (b) are the IR constraints, (c) is the IC constraints, and (d) is the monotonicity condition. Although (14) is not the convex problem, we can obtain the optimal solution in the following steps.

B. Optimal Contract Solution

In this section, we first cut down the number of the constraints according to the **IC** and **IR** rules, and then obtain a new optimal problem with the reduced constraints. Finally, we can easily determine the optimal solutions by the mathematical tool.

Lemma 1: The IR constraint of type-i ($\forall i \in \{2, ..., \mathbb{N}\}$) validator holds only when the IR constraint of type-1 validators is satisfied.

Proof 1: According to the IR rules (11) in Section (III-A), for type-1 validators, we have

$$u_{v(1)}(d_1, c_1) = \mathcal{A}\beta_1\theta_1 c_1 - \frac{d_1}{T}\Bigg\{\mathcal{A}\frac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\frac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}\Bigg\} + (1-\mathcal{A})\beta_2\frac{d_1}{T}\frac{R}{N} - \omega d_1 \geq 0. \tag{15}$$

According to the IC rules (13) in Section (III), for type $\forall i \in \{2, ..., \mathbb{N}\}$, we have

$$u_{v(i)}(d_i, c_i) \geq u_{v(i)}(d_1, c_1). \tag{16}$$

Then based on the monotonic condition (4), i.e., $\theta_i > \theta_1$, we have

$$u_{v(i)}(c_1, c_1) \geq u_{v(1)}(d_1, c_1). \tag{17}$$

Obviously, for given (15), (16) and (17), we can come to the conclusion that

$$u_{v(i)}(d_i, n_i) \geq u_{v(1)}(d_1, n_1) \geq 0. \tag{18}$$

Thus, we complete this proof and demonstrate that only when the IR constraint of type-1 is kept, can the others be also satisfied.

■

Lemma 2: There are four definitions regarding the IC constraints between type-i and type-j ($\forall i \neq j$):

(a) If $\forall j \in \{1, ..., i-1\}$, 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 $\forall j \in \{i+1, ..., N\}$, 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, the DICs can be reduced as LDICs and the UICs can be reduced as the LUICs.

Proof 2: 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 $\forall i \in \{1, ..., N-1\}$. According to the IC constraints, then we have the following two inequations:

$$u_{v(i+1)}(d_{i+1}, c_{i+1}) \geq u_{v(i+1)}(d_i, c_i), \tag{19}$$

$$u_{v(i)}(d_i, c_i) \geq u_{v(i)}(d_{i-1}, c_{i-1}). \tag{20}$$

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

$$(\theta_{i+1} - \theta_i)\mathcal{A}\beta_1 c_i \geq (\theta_{i+1} - \theta_i)\mathcal{A}\beta_1 c_{i-1}. \tag{21}$$

To proceed the reduction of IC constraints, we add (21) to the inequation (20), and obtain a new inequation i.e.,

$$u_{v(i+1)}(d_i, c_i) \geq u_{v(i+1)}(d_{i-1}, c_{i-1}). \tag{22}$$

Combine the inequation (19) and (22), we can easily get:

$$u_{v(i+1)}(d_{i+1}, c_{i+1}) \geq u_{v(i+1)}(d_{i-1}, c_{i-1}). \tag{23}$$

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

$$\begin{aligned} u_{v(i+1)}(d_{i+1}, c_{i+1}) &\geq u_{v(i+1)}(d_{i-1}, c_{i-1}) \\ &\geq u_{v(i+1)}(d_{i-3}, c_{i-3}) \\ &\geq ... \\ &\geq u_{v(i+1)}(d_1, c_1) \\ &\geq u_{v(1)}(d_1, c_1). \end{aligned} \tag{24}$$

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

$$\begin{aligned} u_{v(i-1)}(d_{i-1}, c_{i-1}) &\geq u_{v(i-1)}(d_{i+1}, c_{i+1}) \\ &\geq ... \\ &\geq u_{v(i-1)}(d_{\mathbb{N}}, c_{\mathbb{N}}). \end{aligned} \tag{25}$$

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 (25).

■

With the reduced constraints, the optimization problem (14) can be redefined as follows:

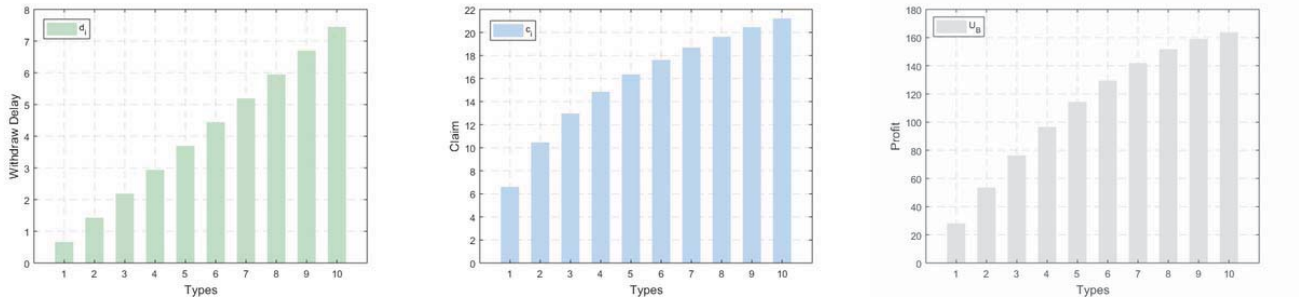
$$\max_{(d_i, c_i)} \quad U_B = \sum_{i \in \mathbb{N}} \lambda_i \Big\{\pi(\theta_i, d_i) + u(\theta_i) - \sigma(d_i, \gamma) - v(d_i, R)\Big\} - P, \tag{26}$$

s.t.

$$(a) \quad \mathcal{A}\beta_1\theta_1 c_1 - \frac{d_1}{T}\Bigg\{\mathcal{A}\frac{R\hat{k}}{N(N-\hat{n})} + \mathcal{A}\frac{R\hat{k}(N-\hat{k}-\hat{n})}{N^2(N-\hat{n})}\Bigg\} + (1-\mathcal{A})\beta_2\frac{d_1}{T}\frac{R}{N} - \omega d_1 = 0,$$

$$(b) \quad P - \mathcal{A}\mathcal{C} = 0,$$

$$(c) \quad u_{v(i)}(d_i, c_i) = u_{v(i)}(d_{i-1}, c_{i-1}).$$



(a) The optimal delay d_i for validators of the different types.

(b) The optimal insurance claim c_i for validators of the different types.

(c) The maximized profit that is contributed by validators of the different types.

Fig. 2. The optimal insurance contract (d_i, c_i).

TABLE I
PARAMETERS SETTING

Parameter	Value
Validators Setting	$\mathcal{N} = 1000, M = 500, N = 100$
	$\hat{n} = 50, \hat{k} = 25$
Weight Parameters	$\beta_1 = 1, \beta_2 = 0.1, \gamma = 1$
	$g_1 = 15, g_2 = 1.5, g_3 = 10, g_4 = 0.01$
Exponent Parameters	$\alpha_1 = 1, \alpha_2 = 2, \alpha_3 = 2$
Reward and Time Slot	$R = 100, T = 0.01$
Unit Cost	$\omega = 5$
Probability Parameter	$\lambda_i = 0.1$
Total Types	$\theta \in \{1, ..., 10\}$

To solve the problem (26), we set

$$\Delta_j = (\theta_{j+1} - \theta_j)\mathcal{A}\beta_1 c_j. \tag{27}$$

Then we add all the $\mathbb{N}$ IC constraints together and get

$$u_{v(i)}(d_i, c_i) = \begin{cases} \sum_{j=1}^{i-1} \Delta_j & \text{if } i \neq 1, \\ 0 & \text{if } i = 1. \end{cases} \tag{28}$$

Thus, we can obtain the following equation according to (28):

$$c_i = \begin{cases} \frac{(e_2 - e_1 + \omega)d_i + \sum_{j=1}^{i-1} \Delta_j}{\mathcal{A}\beta_1\theta_i} & \text{if } i \neq 1, \\ \frac{(e_2 - e_1 + \omega)d_1}{\mathcal{A}\beta_1\theta_1} & \text{if } i = 1. \end{cases} \tag{29}$$

where $e_1 = (1 - \mathcal{A})\frac{\beta_2 R}{TN}$, $e_2 = \frac{\mathcal{A}R\hat{k}}{TN(N-\hat{n})} + \frac{\mathcal{A}R\hat{k}(N-\hat{k}-\hat{n})}{TN^2(N-\hat{n})}$. Without losing generality, we suppose the that $\hat{n} = \frac{1}{2}N$, without regard to the cumulative probability of other cases (i.e., $\hat{n} > \frac{1}{2}N$). Thus, we have $\mathcal{A} = \binom{N}{\hat{n}}(M/\mathcal{N})^{\hat{n}}(1 - M/\mathcal{N})^{(N-\hat{n})}$. Besides, we set $\pi(\theta_i, d_i) = g_1\theta_i d_i^{\alpha_1}$, $u(\theta_i) = g_2\theta_i^{\alpha_2}$, $\sigma(d_i, \gamma) = g_3\gamma d_i^{\alpha_3}$, and $v(d_i, R) = g_4 d_i R/TN$, where g_1, g_2, g_3, g_4, α_1, α_2 and α_3 are the pre-defined weight coefficients. Thus, the beacon chain can obtain the profit from type-i validators is as follows:

$$U_B(i) = g_1\theta_i d_i^{\alpha_1} + g_2\theta_i^{\alpha_2} - g_3\gamma d_i^{\alpha_3} - g_4\frac{d_i R}{TN} - \mathcal{A}c_i \tag{30}$$

After substituting (28) into (30), we have a new problem as follows:

$$U_B(i) = g_1\theta_i d_i^{\alpha_1} + g_2\theta_i^{\alpha_2} - g_3\gamma d_i^{\alpha_3} - g_4\frac{d_i R}{TN} - \frac{(e_2 - e_1 + \omega)d_i + \sum_{j=1}^{i-1} \Delta_j}{\beta_1\theta_i}. \tag{31}$$

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

$$\frac{\partial U_B(i)}{\partial d_i} = g_1\alpha_1\theta_i d_i^{(\alpha_1 - 1)} - g_3\gamma\alpha_3 d_i^{(\alpha_3 - 1)} - g_4\frac{R}{TN} - \frac{(e_2 - e_1 + \omega)}{\beta_1\theta_i}, \tag{32}$$

Next, by differentiating $\frac{\partial U_B(i)}{\partial d_i}$ with respect to d_i, we have

$$\frac{\partial^2 U_B(i)}{\partial d_i^2} = g_1\alpha_1(\alpha_1 - 1)\theta_i d_i^{(\alpha_1 - 2)} - g_3\gamma\alpha_3(\alpha_3 - 1)d_i^{(\alpha_3 - 2)}. \tag{33}$$

Set $\alpha_1 = 1$ and $\alpha_3 = 2$, then it is clear that $\frac{\partial^2 U_B(i)}{\partial d_i^2} = -g_3\gamma\alpha_3(\alpha_3 - 1) < 0$. Therefore, the optimal problem function is a concave function, we can obtain the optimal result by setting the first derivative as zero:

$$d_i = \frac{g_1\theta_i - \frac{g_4 R}{TN} - \frac{e_2 - e_1 + \omega}{\beta_1\theta_i}}{2g_3\gamma}. \tag{34}$$

IV. SIMULATION RESULTS AND NUMERICAL ANALYSIS

In this section, we first list the parameters setting in Table I, then obtain the optimal contracts (d_i, c_i) for all the types of validators, proving the feasibility of such contract-theoretic scheme by showing the profit of the beacon chain. Also we compare the utilities of the different-type validators.

As shown in Fig. 2(a), we can observe that the optimal withdraw delay increases along with the types, which conforms the closed-form solution (34). From Fig. 2(b), we can see that the optimal insurance claim grows along with the type increases. But apparently, the growth rate decreases along with the type. Both of the figures prove the monotonicity of the optimal contract (d_i, c_i).

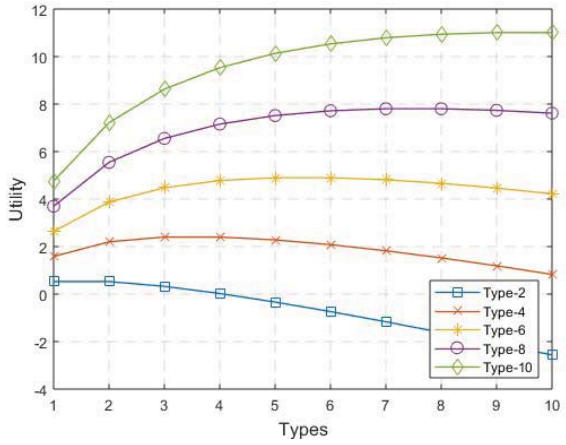


Fig. 3. Utilities of validators when sign different contracts.

Given the optimal contract (d_i, c_i), we obtain the total profit that is contributed by the different-type validators. From Fig. 2(c), it is clear that the beacon chain can acquire a more profit from the higher type, which complies with our contract design. Even given the lowest type, the profit is also larger than zero.

Finally, from the Fig. 3, we can see the validators of type-2, type-4, type-6, type-8 and type-10 signing the different contracts have various utilities. It shows apparently that the validators have the maximum utilities only when choosing the contract designed for their own, which prove the IC constraint. Besides, all these maximum incentives are positive, which explains the IR constraint.

V. Conclusion

In this paper, we first analyze the discouragement attack model and the expected loss of the validators in the blockchain networks with shards, and then design a cyber insurance under the contract theory framework based on the attack model. The founders of Ethereum point out that the withdraw 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 under the contract theory framework, by integrating the idea of the cyber insurance to neutralize the cyber risks, determine the different validators' withdraw delays and provide the insurance claim for their loss. That means, the blockchain system can keep more online deposit to resist the discouragement attack via the 'delay' determined in the contract, while the validators stay online to get insured for the loss caused by the discouragement attack. Besides, 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.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Self-published Paper*, 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. A survey on consensus mechanisms and mining management in blockchain networks. *arXiv preprint arXiv:1805.02707*, pages 1–33, 2018.

[3] Bitcoin. https://bitcoin.org/en/.

[4] Coinmarketcap. https://coinmarketcap.com/.

[5] Ethereum Foundation. Ethereum. https://www.ethereum.org/.

[6] Dai. https://makerdao.com/en/dai/.

[7] Defi. https://defi.network/.

[8] Wyre. https://www.sendwyre.com/.

[9] QuantumMechanic. Proof of stake instead of proof of work. https://bitcointalk.org/index.php?topic=27787.0. June 11, 2011.

[10] Ethereum Foundation. Ethereum 2.0 (serenity) phases. https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/.

[11] Vitalik Buterin. Discouragement attacks. https://github.com/ethereum/research/blob/master/papers/discouragement/discouragement.pdf. June 11, 2011.

[12] Vitalik Buterin. Rate-limiting entry/exits, not withdrawals. https://ethresear.ch/t/rate-limiting-entry-exits-not-withdrawals/4942. Feb 3, 2019.

[13] Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9):2226–2239, 2018.

[14] Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. Embracing risk dependency in designing cyber-insurance contracts. In *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 926–933. IEEE, 2017.

[15] Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. Designing cyber insurance policies: Mitigating moral hazard through security pre-screening. In *International Conference on Game Theory for Networks*, pages 63–73. Springer, 2017.

[16] Shaohan Feng, Zehui Xiong, Dusit Niyato, Ping Wang, Shaun Shuxun Wang, and Yang Zhang. Cyber risk management with risk aware cyber-insurance in blockchain networks. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2018.

[17] Ranjan Pal and Pan Hui. Cyberinsurance for cybersecurity a topological take on modulating insurance premiums. *ACM SIGMETRICS Performance Evaluation Review*, 40(3):86–88, 2012.

[18] M-Elisabeth Paté-Cornell, Marshall Kuypers, Matthew Smith, and Philip Keller. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, 38(2):226–241, 2018.

[19] Jonathan Chase, Dusit Niyato, Ping Wang, Sivadon Chaisiri, and Ryan Ko. A scalable approach to joint cyber insurance and security-as-a-service provisioning in cloud computing. *IEEE Transactions on Dependable and Secure Computing*, 2017.

[20] Patrick Bolton, Mathias Dewatripont, et al. *Contract theory*. MIT press, 2005.

[21] Vitalik Buterin. A griefing factor analysis model. https://ethresear.ch/t/a-griefing-factor-analysis-model/2338. June, 2018.

[22] Georges Dionne. *Contributions to insurance economics*, volume 13. Springer Science & Business Media, 2013.