先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	大規模システム管理 (笠原　正治　(教授))		
学籍番号	1911240	提出日	令和 3年 1月 14日
学生氏名	藤田　健太郎		
論文題目	Mining Pool Selection Problem under Block WithHolding Attack Block WithHolding 攻撃が存在する場合のマイニングプール選択問題		

要旨

In current Proof-of-Work (PoW) blockchain systems, miners usually form mining pools to compete with other pools/miners in the mining competition. Forming pools can give miners steady revenues but will introduce two critical issues. One is mining pool selection, where miners select the pools to join in order to maximize their revenues. The other is Block WithHolding (BWH) attack, where pools can inject part of their hash/mining power into other pools to obtain additional revenues without contributing to the mining process of the attacked pools. Reasoning that the BWH attack will have significant impacts on the pool selection, we therefore investigate the mining pool selection issue in the presence of BWH attack in this thesis.

We first focus on the scenario with observable BWH attack and apply the evolutionary game theory to model the mining pool selection of miners. Evolutionarily Stable States (ESSs) of the game are obtained to characterize the stable population states of the pools. Previous studies investigated this problem from the perspective of pool managers and neglected the revenues from attacked pools (attacking revenues), leading to less accurate and insightful findings. This thesis, however, focuses on the payoffs of miners and carefully takes the attacking revenues into consideration.

Arguing that attackers are not willing to expose them in practice, we then consider the scenario with unobservable BWH attack and employ Reinforcement Learning (RL) techniques to analyze the intelligent pool selection of miners. We adopt three typical RL models, i.e., Q-Learning (QL), Deep Q Network (DQN) and Advanced Actor-Critic (A2C), to dynamically learn the optimal pool selection policies of an intelligent miner and use a discrete-event simulator to measure the reward of the miner.

To demonstrate how the problems are solved in the above two scenarios, we focus on the representative case with two mining pools. We also provide extensive simulation and numerical results to show the impact of BWH attack on the mining pool selection of miners (observable attack) and also the learning performances of the proposed RL-based mining pool selection methods (unobservable attack).