Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Large-Scale Systems (Shoji Kasahara (Professor))		
Student ID	2011312	Submission date	2022 / 1 / 21
Name	OSMANI SHAIRA		
Thesis title	Support Vector Machine based Detection of Block Withholding Attacks in a Bitcoin Mining Pool		

Abstract

In the Bitcoin system, transactions are recorded in a distributed ledger called blockchain, which is a sequence of blocks including issued transactions. Some special nodes called miners try to create a new valid block in order to acquire rewards (i.e., new Bitcoins) by solving cryptographic puzzles with certain difficulty (i.e., network difficulty). This process is called proof of work (PoW) and it requires a huge number of hash calculations.
To acquire the rewards while suppressing the electricity and investment costs, multiple miners tend to form a group called a pool to conduct PoW collaboratively. The manager of the pool, i.e., pool manager, divides the original PoW task into multiple sub-tasks and allocates them to the member miners.
It also sets the local difficulty of PoW (i.e., pool difficulty), which is easier than the network difficulty, to confirm the contribution of members.
Each member is requested to report their finding blocks and shares, which only satisfy the pool difficulty condition, to the pool manager. The pool manager distributes rewards to members according to their contributions.
It has been pointed out that some malicious miners can sabotage the mining process and gain more rewards by hiding found blocks. This attack is called block withholding (BWH) attack. Since the BWH attack reduces the pool rewards, it is important for the pool manager to detect it.
The pool manager can monitor the behavior of each miner in terms of the number of reported blocks and that of reported shares.
If a miner is honest, their ratio will reach the ratio of pool difficulty to network difficulty. Otherwise, it will be lower than the difficulty ratio. Focusing on this characteristic, we apply the support vector machine (SVM) to classify members into honest or malicious. Through simulation experiments using the modified version of the existing simulator PoolSim and the hashrate distribution of miners in the actual mining pool called ViaBTC, we demonstrate the relationship between the detection accuracy and the observation period.