The Game among Bribers in a Smart Contract System

Abstract. Blockchain has been used to build various applications, and the introduction of smart contracts further extends its impacts. Most of existing works consider the positive usage of smart contracts but ignore the other side of it: smart contracts can be used in a destructive way, particularly, they can be utilized to carry out bribery. The hardness of tracing a briber in a blockchain system may even motivate bribers. Furthermore, an adversary can utilize bribery smart contracts to influence the execution results of other smart contracts in the same system. To better understand this threat, we propose a formal framework to analyze bribery in the smart contract system using game theory. We give a full characterization on how the bribery budget of a briber may influence the execution of a smart contract if the briber tries to manipulate its execution result by bribing users in the system.