Verifiable Sealed-Bid Auction on the Ethereum Blockchain

Hisham S. Galal and Amr M. Youssef

Concordia Institute for Information Systems Engineering,
Concordia University, Montréal, Quebéc, Canada

Abstract. The success of the Ethereum blockchain as a decentralized application platform with a distributed consensus protocol has made many organizations start to invest into running their business on top of it. Technically, the most impressive feature behind Ethereum's success is its support for a Turing complete language. On the other hand, the inherent transparency and, consequently, the lack of privacy poses a great challenge for many financial applications. In this paper, we tackle this challenge and present a smart contract for a verifiable sealed-bid auction on the Ethereum blockchain. In a nutshell, initially, the bidders submit homomorphic commitments to their sealed-bids on the contract. Subsequently, they reveal their commitments secretly to the auctioneer via a public key encryption scheme. Then, according to the auction rules, the auctioneer determines and claims the winner of the auction. Finally, we utilize interactive zero-knowledge proof protocols between the smart contract and the auctioneer to verify the correctness of such a claim. The underlying protocol of the proposed smart contract is partially privacy-preserving. To be precise, no information about the losing bids is leaked to the bidders. We provide an analysis of the proposed protocol and the smart contract design, in addition to the estimated gas costs associated with the different transactions.

Keywords: Ethereum, Smart Contract, Sealed-Bid Auction.