A Blockchain-based Iterative Double Auction Protocol Using Multiparty State Channels

TRUC D. T. NGUYEN and MY T. THAI, University of Florida

Although the iterative double auction has been widely used in many different applications, one of the major problems in its current implementations is that they rely on a trusted third party to handle the auction process. This imposes the risk of single point of failures, monopoly, and bribery. In this article, we aim to tackle this problem by proposing a novel decentralized and trustless framework for iterative double auction based on blockchain. Our design adopts the smart contract and state channel technologies to enable a double auction process among parties that do not need to trust each other, while minimizing the blockchain transactions. In specific, we propose an extension to the original concept of state channels that can support multiparty computation. Then, we provide a formal development of the proposed framework and prove the security of our design against adversaries. Finally, we develop a proof-of-concept implementation of our framework using Elixir and Solidity, on which we conduct various experiments to demonstrate its feasibility and practicality.

CCS Concepts: • **Security and privacy → Software and application security**; **Distributed systems security**; • **Computer systems organization** → *Peer-to-peer architectures*;

Additional Key Words and Phrases: Iterative double auction, blockchain, state channel, trustless

ACM Reference format:
Truc D. T. Nguyen and My T. Thai. 2021. A Blockchain-based Iterative Double Auction Protocol Using Multiparty State Channels. *ACM Trans. Internet Technol.* 21, 2, Article 39 (March 2021), 22 pages.
https://doi.org/10.1145/3389249

1 INTRODUCTION

Blockchain, the technology that underpins the great success of Bitcoin [18] and various other cryptocurrencies, has incredibly emerged as a trending research topic in both academic institutes and industries associations in recent years. With great potential and benefits, the blockchain technology promises a new decentralized platform for the economy such that the possibility of censorship, monopoly, and single point of failures can be eliminated [26]. The technology, in its simplest form, can be seen as a decentralized database or digital ledger that contains append-only data blocks where each block comprises valid transactions, timestamp, and the cryptographic hash of the previous block. By design, a blockchain system is managed by nodes in a peer-to-peer network and operates efficiently in a decentralized fashion without the need of a central authority. Specifically, it enables a trustless network where participants of the system can settle transactions without having to trust each other. With the aid of the smart contracts technology, a blockchain system

Authors' addresses: T. D. T. Nguyen and M. T. Thai (corresponding author), University of Florida, Gainesville, Florida, 32611; emails: truc.nguyen@ufl.edu, mythai@cise.ufl.edu.

1533-5399/2021/03-ART39 $15.00
https://doi.org/10.1145/3389249