UMass Dartmouth
COLLEGE OF ENGINEERING

Computer and
Information Science
Department

MASTER'S PROJECT (FALL 2018)

TOPIC: ***A Blockchainless Approach for Trusted Public Construction Bidding***

PRESENTOR: Naoto Nicol

ADVISOR: Dr. Haiping Xu

DATE & TIME: Friday, December 14, 2018, 2:30PM

LOCATION: Dion 302G (Demo)

COMMITTEE MEMBERS: Dr. Iren Valova and Dr. Maoyuan Sun

ABSTRACT

Public construction bidding is conventionally a centralized process, where interested companies send their bids to a government agency before a deadline. This approach assumes that the government agency is trustworthy and fair. However, in reality, it happens that bidding information may be disclosed before the auction ends, resulting in an unfair auction. In order to enforce fairness in the bidding process, it is critical to establish a trusted process for public construction bidding. In this project, we aim to develop such a process using a blockchainless approach with cryptographic guarantees. Blockchain, as a type of distributed ledger technology, has increased in popularity recently due to its decentralized and immutable nature. Our project adopts a different but related blockchainless approach based on a directed acyclic graph (DAG). The DAG-based approach offers the same distributed and immutable properties over a peer-to-peer network like a blockchain, but is faster and requires much less computational overhead. Instead of mining blocks of transactions as in a blockchain, a DAG links a transaction, containing a list of its parents, documents and transaction signatures, to other transactions via a less complex validation process. If a parent transaction is not found in a local data storage, it may be retrieved from its peers in the network. However, if any of the parents cannot be verified, a transaction is considered invalid and will not be added into the DAG. Furthermore, to create a trusted public construction bidding process, a bid submitted for a project must be encrypted using a secret phrase, preventing disclosure of bidding information before a winner is announced. Once the auction is over, the secret phrase is released over the network, and at this point, every company's bid become public and visible. The project provides a well-designed interface to users to review the life cycle of a project and to independently check if there was any tampering of data.