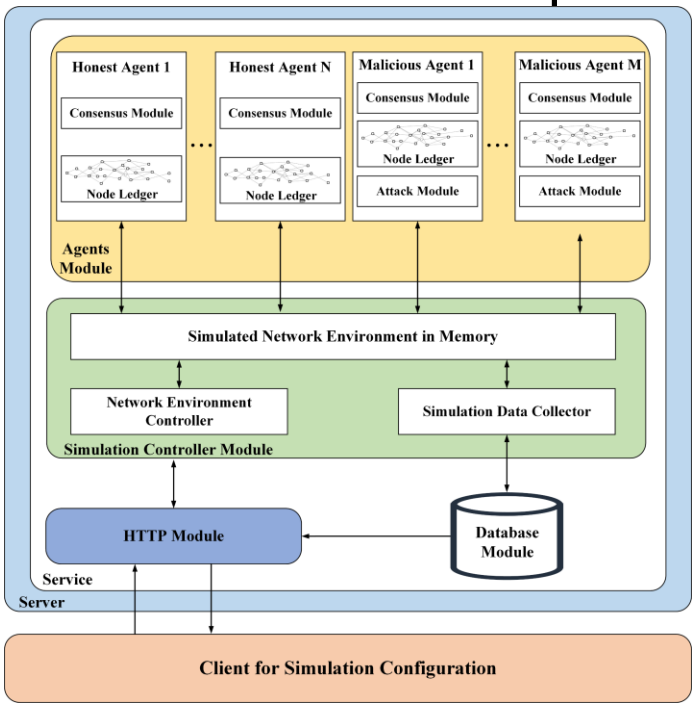
Simulation study on the security of consensus algorithms in DAG-based distributed ledger

Shuzhe LI, Hongwei XU, Qiong LI, Qi HAN

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2497-y

Problems & Ideas

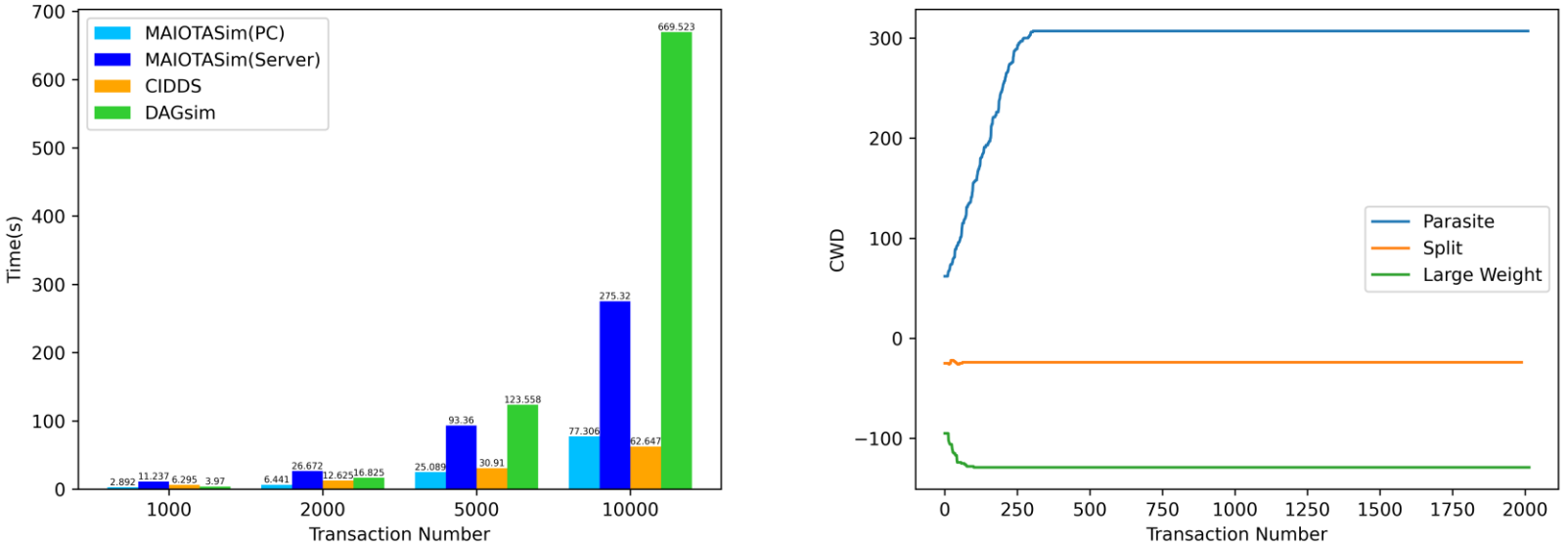
- Problems of the security of consensus algorithms in DAG-based distributed ledger:
  - The security of the TSAs after removing the coordinator has not been studied thoroughly
  - Current simulation only very little attention has been paid to the security of IOTA consensus algorithms.
- Ideas: Use MAS and some optimization methods to design and realize a simulation platform



The system architecture of MAIOTASim, which includes client, server and service, HTTP module, simulation controller module, agents module and database module.

Main Contributions

- Contributions:
  - An IOTA-oriented simulation platform, i.e. MAIOTASim, is designed and implemented using Multi-Agent technology, which can support the simulation of 10,000-level transactions at a scale of 100-level nodes.
  - A new security indicator, so called Cumulative Weight Difference(CWD), is proposed to evaluate consensus algorithms.
  - The securities of different consensus algorithms of IOTA are evaluated via MAIOTASim.



Left: simulation speed using MCMC for different platforms; Right: CWD when use MCMC with α=0.05, the CWD between different transactions can also compare the confidence of different transactions.