Investigating Byzantine Agreement Consensus Algorithm of Algorand

Yu Liu

Supervisor: Dr. Ling Chen
Dr. Wei Bian

School of Computer Science
University of Technology Sydney

This dissertation is submitted for the degree of
Master of Analytics

March 2020

I would like to dedicate this thesis to my loving parents ...

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Yu Liu
March 2020

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, Yu Liu declare that this thesis, is submitted in fulfilment of the requirements for the award of Master of Analytics, in the school of Computer Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution. This research is supported by the Australian Government Research Training Program.

Signature:

Production Note:
Signature removed prior to publication.

Date:

06/03/2020

Acknowledgements

I would like to express my sincerest gratitude to my principal supervisor, Dr Ling Chen, who gave me the opportunity to embark on this research degree and for being extremely patient and supportive in guiding me over the course of this journey. I would also like to thank my co-supervisor, Dr Wei Bian, who encouraged me to explore blockchain technology and encouraged me to put the pieces together to form a complete work. I could not have finished this research without their valuable help.

Thanks to all my research colleagues and friends in the school of Computer Science for their kind help to overcome my struggles. I would like to express my appreciation to Mr Wei Wu, Miss Jiamiao Wang, Mr Shaosheng Wang, Mr Yunqiu Xu, Miss Congai Li, and all my other lovely friends in this school.

Last but not least, I thank my parents for their support. They have always encouraged, guided, and supported me, no matter when I succeeded or failed.

Abstract

After its rapid development and broad adoption in its early stage, blockchain technologies are experiencing a bottleneck in terms of their scalability in processing transactions. There have been various proposals to overcome this difficulty, but very few are able to avoid the curse of the blockchain trilemma in relation to balancing scalability, decentralization, and security. However, Algorand demonstrates its superior capability to process transactions and maintain safety when the number of users increase. In particular, its consensus diminishes the probability of chain forks, which generates the feasibility of double-spend attacks in blockchains. In order to determine if Algorand could be the answer to the trilemma, this thesis presents an investigation of its consensus algorithms and a thorough analysis of its performance and some potential downsides of the proposal.

Table of contents

List of figures

List of tables