PROJECT REPORT

SHA256 & SCRYPT ALGORITHM PROBABILITY ANALYSIS OF FINDING NEW BLOCK ON BLOCKCHAIN TECHNOLOGY

NOVAN AGENG MULYADI
14.K1.0074

Faculty of Computer Science
Soegijapranata Catholic University
2018

APPROVAL AND RATIFICATION PAGE

SHA256 & SCRYPT ALGORITHM PROBABILITY ANALYSIS OF FINDING NEW BLOCK ON BLOCKCHAIN TECHNOLOGY

by

NOVAN AGENG MULYADI – 14.K1.0074

This project report has been approved and ratified

by the Faculty of Computer Science on July, 20, 2018

With approval,

Supervisor,

YB. Dwi Setianto, ST., M.Cs
NPP : 058.7.2017.021

Examiners,

1.)

Suyanto Edward Antonius, Ir., M.Sc.
NPP : 058.1.1992.116

2.)

Shinta Estri Wahyuningrum, S.Si, M.Cs
NPP : 058.1.2007.272

3.)

YB. Dwi Setianto, ST., M.Cs
NPP : 058.7.2017.021

Dean of Faculty of Computer Science,

Endi Widyarto Nugroho, ST., MT
NPP: 058.1.2002.254

STATEMENT OF ORIGINALITY

I, the undersigned:

Name : NOVAN AGENG MULYADI

ID : 14.K1.0074

Certify that this project was made by myself and not copy or plagiarize from other people, except that in writing expressed to the other article. If it is proven that this project was plagiarizes or copy the other, I am ready to accept a sanction.

Semarang, July, 20, 2018

NOVAN AGENG MULYADI
14.K1.0074

ABSTRACT

In the language of cryptocurrency, a block is a record of new transactions that could mean the location of cryptocurrency, or medical data, or even voting records. Once each block is completed it's added to the chain, creating a chain of blocks: a blockchain. Because cryptocurrencies are encrypted, processing any transactions means solving complicated math problems using specified algorithm like SHA256 and Scrypt. People who solve these equations are rewarded with cryptocurrency in a process called mining. In this study the authors will find out the comparison of SHA256 and Scrypt to work on the blockchain.

To find out the comparison between SHA256 and Scrypt the author will do some test, test given to both algorithm on some Test System to observe which algorithm that has highest probability in finding new block.

the results of the tests done in this paper show that Scrypt is much slower to hash than SHA256 but the Scrypt algorithm has greater chance to found a new block.

Keywords: SHA256, Scrypt, Proof-of-Work, Blockchain, Comparison

PREFACE

This research compares the probability of finding new block between SHA256 Algorithm and Scrypt Algorithm consisting of six chapters. The first chapter is about backgrounds that compare SHA256 and Scrypt in general, the second chapter contains about research references like proceedings electronic publications and documentations, the third chapter will explain the Methodology in general such as the platform used, the experiments to be tested and the observed sections to collect the data, the fourth chapter will describe the test system and the program that will be used to observe, in the fifth chapter contains the results of experiments that have been done and the last sixth chapter contains the results of the conclusions of this research.

TABLE OF CONTENTS

INDEX OF TABLES AND ILLUSTRATION