

TABLE OF CONTENTS

ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	ix
INTISARI	x
ABSTRACT	xi
CHAPTER I INTRODUCTION	1
1.1 Background	1
1.2 Research Problem	7
1.3 Research Scope	8
1.4 Research Objectives	8
1.5 Research Benefit	9
1.6 Research Methodology	9
1.7 Thesis Organization	10
CHAPTER II LITERATURE REVIEW	11
CHAPTER III THEORETICAL BASIS	18
3.1 Blockchain	18
3.1.1 Distributed ledger	20
3.1.2 Consensus	23
3.1.3 Smart contract	26
3.2 Elliptic Curve Cryptography	27
3.2.1 Elliptic Curve Diffie-Hellman (ECDH)	30
3.2.2 Elliptic Curve Digital Signature Algorithm (ECDSA)	30
3.2.3 Elliptic Curve Integrated Encryption Scheme (ECIES)	32
3.3 Bayesian reputation system	33
CHAPTER IV ANALYSIS AND DESIGN	36
4.1 Assumptions	36
4.2 Proposed System Architecture	37
4.3 Protocol to Generate Invoice ID	43
4.4 Process Flow of Proposed System	47
CHAPTER V IMPLEMENTATION	53
5.1 System Environment	53
5.2 Smart Contract Implementation	56
5.2.1 Register invoice ID	56
5.2.2 Query invoice ID	57

5.2.3	Bidding process.....	57
5.2.4	Withdraw.....	58
5.2.5	End auction	59
5.2.6	Payback loan	60
5.3	Application Interface Implementation.....	61
CHAPTER VI EVALUATION AND DISCUSSION		72
6.1	Performance Evaluation	72
6.2	Security Evaluation	75
CHAPTER VII CONCLUSION		78
REFERENCES		79