Table of Contents

Declaration I

Certificate III

Abstract V

Acknowledgments IX

Table of Contents XI

List of Figures XV

List of Table XVII

1 Introduction 1
- 1.1 Underline Blockchain Terminology . . . 1
- 1.2 Consensus Algorithms . . . 3
  - 1.2.1 Proof Based Consensus Algorithms . . . 3
  - 1.2.2 Vote Based Consensus Algorithm . . . 5
- 1.3 Smart Contracts . . . 7
- 1.4 Type of Blockchain . . . 8
  - 1.4.1 Public Blockchain . . . 8
  - 1.4.2 Private Blockchain . . . 8
  - 1.4.3 Consortium Blockchain . . . 9
- 1.5 Challenges in Blockchain . . . 9
  - 1.5.1 Scalability . . . 10
  - 1.5.2 Interoperability . . . 10
  - 1.5.3 Privacy . . . 11
  - 1.5.4 Vulnerabilities in Blockchain . . . 11
- 1.6 Blockchain Applications . . . 13
  - 1.6.1 Internet of Things (IoT) . . . 13
  - 1.6.2 Intelligent Transportation Systems (ITS) . . . 14
  - 1.6.3 Smart Grid . . . 14
- 1.7 Motivation and Contributions . . . 14
- 1.8 Thesis Structure . . . 16

2 Related Work 17
- 2.1 Consensus Algorithm Enhancements . . . 17
- 2.2 State-of-the-art Schemes for Scalable Blockchain . . . 18

2.3 State-of-the-art Schemes for Interoperable Blockchain . . . 21
2.4 State-of-the-art Schemes for Blockchain Application . . . 23

3 Scalable Blockchain **27**
3.1 Challenges in Achieving Scalability . . . 27
3.2 Blockchain Sharding . . . 28
3.3 Contributions . . . 29
3.4 BlockTree: A Nonlinear Structured, Scalable Distributed Ledger . . . 30
3.4.1 Sharding in BlockTree . . . 31
3.4.2 Transaction Sharding . . . 31
3.4.3 Leader Selection, Leader Block, and Data Block . . . 32
3.4.4 Remuneration Model . . . 36
3.5 UnoShard: Harmonizing Scalability and Security . . . 36
3.5.1 Shard Allocation . . . 37
3.5.2 Intra-Shard Consensus . . . 38
3.5.3 Cross-Shard Consensus . . . 40
3.6 Performance Analysis . . . 45
3.6.1 Simulation Environment . . . 46
3.6.2 Consensus Delay . . . 46
3.6.3 Throughput . . . 47
3.6.4 Fairness . . . 47
3.6.5 Block Congestion Control . . . 48
3.7 Security Analysis . . . 49
3.7.1 Prevention of Double Spending . . . 51
3.7.2 Illegitimate Fork Prevention . . . 51
3.7.3 Scalability Enhancement . . . 52

4 Interoperability **53**
4.1 Challenges in Interoperable Blockchains . . . 53
4.2 *CrossLedger*: A Pioneer Cross-Chain Asset Transfer Protocol . . . 54
4.2.1 System Model . . . 55
4.2.2 Background . . . 56
4.2.3 Methodology . . . 61
4.2.4 Essential Characteristics of Interoperable Blockchahin . . . 65
4.3 Security Analysis . . . 67

5 Blockchain Applications **71**
5.1 Solution for IoT Application . . . 72
5.1.1 Motivation and Contribution . . . 72
5.1.2 System Model . . . 73
5.1.3 Adversary Model . . . 74
5.1.4 BLISS: Blockchain-based Integrated Security System for Internet of Things (IoT) Applications . . . 75
5.1.5 SCAB-IoTA: Secure Communication and Authentication for IoT Applications Using Blockchain . . . 81
5.1.6 Implementation Detail and Performance Analysis . . . 85
5.1.7 Security Analysis . . . 89

5.2 Solution for ITS Applications . . . 94
5.2.1 Motivation and Contribution . . . 95
5.2.2 Network Model . . . 96
5.2.3 Assumptions . . . 98
5.2.4 Adversary Model . . . 99
5.2.5 LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-enabled IoV . . . 100
5.2.6 SmartCoin: A Novel Incentive Mechanism for Vehicles in Intelligent Transportation System Based on Consortium Blockchain . . . 105
5.2.7 Implementation Environment and Performance Analysis . . . 108
5.2.8 Security Analysis . . . 112
5.3 Blockchain-based Secured Smart Grid System . . . 117
5.3.1 Motivation and Contribution . . . 118
5.3.2 Basic Terminologies in Smart Grid . . . 119
5.3.3 SmartGrid-NG: Blockchain Protocol for Secure Transaction Processing in Next Generation Smart Grid . . . 120
5.3.4 ETradeChain: Blockchain-Based Energy Trading in Local Energy Market (LEM) using Modified Double Auction Protocol . . . 128
5.3.5 Implementation Detail and Performance Analysis . . . 137
5.3.6 Security Analysis for SmartGrid-NG and ETradeChain . . . 144
5.4 Privacy-Preserving Energy Trading in Smart Grid . . . 148
5.4.1 Techniques Used to Provide Privacy in Blockchain . . . 149
5.4.2 *zk-SNARK* Background . . . 149
5.4.3 Public Traceability . . . 150
5.4.4 *zk-SGB*: Privacy-Preserved Blockchain Framework for Energy Trading in Smart Grid Using Zero Knowledge Proof . . . 150
5.4.5 Consumer and Prosumer Communication Based on zk-SNARK . . . 151
5.4.6 WNS-BFT: Consensus Algorithm . . . 152
5.4.7 Performance Analysis . . . 156
5.4.8 Security Analysis of zk-SGB . . . 158

6 Conclusion and Future Work **163**

Publications **164**

References **169**