Declaration

I hereby declare that the work presented in this thesis titled *Cutting-Edge Consensus Algorithms in Scalable and Interoperable Blockchain* submitted to the Indian Institute of Technology Jodhpur in partial fulfillment of the requirements for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work carried out under the supervision of Dr. Debasis Das. The contents of this thesis, in full or in parts, have not been submitted to, and will not be submitted by me to, any other Institute or University in India or abroad for the award of any degree or diploma.

Lokendra Vishwakarma
P19CSE012
Computer Science and Engineering
Indian Institute of Technology Jodhpur

Certificate

This is to certify that the thesis titled *Cutting-Edge Consensus Algorithms in Scalable and Interoperable Blockchain*, submitted by Lokendra Vishwakarma (P19CSE012) to the Indian Institute of Technology Jodhpur for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work done by him under my supervision. To the best of our knowledge, the contents of this report, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. Debasis Das
Ph.D. Thesis Supervisor
Computer Science and Engineering
Indian Institute of Technology Jodhpur

To My Brave Son Hrishiv,
My Companion and Better Half Nootan, and My Loving Parents.

Acknowledgements

This journey has been a roller-coaster ride for me, filled with many ups and downs, both in my personal life and in my PhD journey. This ride would not have been completed without the many wonderful and amazing people who have supported me and believed in me along the way. With this acknowledgment, I try to express my deepest appreciation and gratitude.

First and foremost, I owe my deepest gratitude to a truly brilliant mind and a very kind soul, my supervisor, **Dr. Debasis Das**. Thank you, Dr. Das, for your untiring support, help, patience, and encouragement throughout my studies, which made this work possible. Your advice and guidance, even when you were away, have been priceless. I have been extremely lucky to have you as my supervisor and friend. Thank you from the bottom of my heart for being there for me whenever needed in my research and beyond. I would like to give special thanks to the Head of the Department, **Prof. Gaurav Harit**, for his valuable support in every aspect of my PhD journey. I am immensely grateful to my student research committee (SRC) professors, **Dr. Suman Kundu**, **Dr. Palash Das**, **Dr. Nilkamal Hazra**, and my former SRC member **Dr. Chiranjoy Chattopadhyay**, for their invaluable guidance, advice, support, and enthusiasm. They were always there to support me and consistently pushed me out of my comfort zone to empower me as a person and researcher.

I would like to express my deepest gratitude to **Prof. Sajal K. Das** (Missouri S&T, USA). His extensive knowledge and unwavering support played a crucial role in shaping my research and refining my thinking. Our conversations were consistently insightful and enjoyable, motivating me to pursue excellence. Prof. Das's wisdom and generosity had a profound influence on both my work and personal development. I would also like to thank to **Prof. Christian Becker** (University of Stuttgart) **Prof. Sukumar Nandi** (IIT Guwahati, India) and **Prof. Athanasios V. Vasilakos** (Lulea University of Technology, Sweden) for the collaborative work. Your feedback and guidance provide me with a great sense of knowledge and clarity. In the last leg of my PhD journey, I met with **Dr. Nitin Awathare**, who taught me to think about the research problem from different directions and different perspectives. I am also very thankful to him for his support and guidance, which broadened my thinking in blockchain research.

I believe that no journey is complete without friends. In this journey, my friends have been my pillars of strength, both emotionally and spiritually. To my dear friends **Himani, Ankur Nahar**, and **Aashish Bohra**, your unwavering support has been a beacon of light throughout this journey. Your friendship has been a true blessing, and I am deeply grateful for your presence in my life. This journey became even more special with the spiritual engagement due to my friend **Jayant Vyas**. From being a colleague in Indore to becoming a special friend at IIT Jodhpur, your friendship has been life-changing for me. **Amritesh Kumar**, you are truly a pure soul, and your support has been invaluable. You have always been there for me, offering support beyond just the PhD work. **Monu Nagar, Arju**, our camaraderie has been a source of resilience. Together, we have faced challenges, celebrated victories, and created memories that will last a lifetime. I also extend my heartfelt thanks to every member of the VANET lab; **Bhumika, Umang, Shristy, Samanyu**, and **Koustav** for their support and engaging discussions throughout this journey.

Without the support of family, none of this would have been possible. I am deeply thankful to my father **Mr. Ratan Lal Vishwakarma** and mother **Ms. Sunita Vishwakarma** for believing in me and my dreams. You encouraged me to pursue my goals and passions. There are not enough words to express my gratitude toward you. To my wife **Ms. Nootan**, you are truly my life companion. You were more worried during all

my failures, and you cheered for me and celebrated my tiniest achievements. We have shared many difficult times, and you stayed strong and motivated me to go beyond my limits.

Last but not least, to my brave son **Harshiv**, your arrival in my life brought a ray of hope to do better. Your smile and laughter suppressed all the stress of this journey. Harshiv, thank you for being my brightest star and ray of hope; this achievement is dedicated to you, my brave boy.

Lokendra Vishwakarma
P19CSE012
Computer Science and Engineering
Indian Institute of Technology Jodhpur

List of Figures

1.1 Typical graphical representation of blockchain . . . 2
1.2 Working mechanism of PoW . . . 4
1.3 Working mechanism of PoS . . . 5
1.4 Working mechanism of PBFT . . . 6
1.5 Fork in blockchain . . . 12

3.1 An example of a sharded blockchain with three shards. Each shard has its own local ledger L_1, L_2, L_3, and one global ledger. . . . 28
3.2 Struture of BlockTree . . . 31
3.3 Types of blocks and their arrangement . . . 34
3.4 Intra-shard consensus process of UnoShard based on PBFT . . . 40
3.5 This figure illustrates the generation of local blocks (LB_i) and VoteChain of VoteBlocks (VB_j). A Shard Coordinator (SC) is elected in each shard, as depicted here. . . . 44
3.6 Comparative analysis of BlockTree with state-of-the-art schemes based on the (a) consensus delay and (b) throughput . . . 47
3.7 Comparative analysis of BlockTree with state-of-the-art schemes based on (a) fairness and (b) block congestion control . . . 49

4.1 *CrossLedger*'s asset transfer mechanism between two blockchains, source blockchain A and destination blockchain B . . . 56
4.2 Essential parameter exchange between AF_A and AF_B . . . 62
4.3 Sequence for asset transfer communication from blockchain A to blockchain B . . . 65

5.1 System model for IoT application . . . 74
5.2 Device authentication process in BLISS . . . 76
5.3 Candidate-to-candidate secure communication in BLISS . . . 79
5.4 Cluster creation and device authentication . . . 83
5.5 Secret-key share and M2M communication . . . 84
5.6 Testbed for one cluster of 5 Raspberry Pi model B devices . . . 86
5.7 Metamask interface to connect with Ethereum testnet . . . 87
5.8 Output of the JoinCluster contract. The function call isAvailableDeviceID shows the device is found, mentioned under the decoded output . . . 88
5.9 A basic network model of proposed ITS solution . . . 97
5.10 Representation of TPD with computation of different parameters. . . . 98
5.11 (a) Initialization phase of LBSV, (b) Registration phase of LBSV . . . 101
5.12 Communication phase of LBSV . . . 104
5.13 Communication between Vehicle, RSU, and Controller Node . . . 108
5.14 (a) Storage and communication cost of SmartCoin (SC) and LBSV with state-of-the-art scheme (b) Consensus delay of SmartCoin (SC) and LBSV with state-of-the-art scheme . . . 111

5.15 Computational efficiency of SDN . . . 112
5.16 Fault tolerance in SmartCoin . . . 115
5.17 SmartGrid-NG system architecture . . . 121
5.18 ETradeChain system model . . . 129
5.19 Testbed setup for SmartGrid-NG using one computer system and eight Raspberry Pi boards . 138
5.20 Implementation environment for ETradeChain testbed . . . 139
5.21 ETradeChain working process on the RP4 devices. These are the command line interface of RP4 doing all the required processing . . . 140
5.22 Comparative analysis of GridChain based on (a) consensus delay and (b) throughput (number of transactions executed per second) with state-of-the-art schemes . . . 141
5.23 Comparative analysis of ETradeChain based on (a) consensus delay and (b) throughput with state-of-the-art schemes . . . 143
5.24 Sequence diagram for communication between the consumer (smart meter) and prosumer (consensus node) in *zk-SGB* . . . 152
5.25 Comparative analysis of *zk-SGB* based on (a) consensus delay and (b) throughput with state-of-the-art schemes . . . 158

List of Tables

1.1 Comparative analysis between Public, Private, and Consortium blockchains 9

2.1 Comparison of consensus algorithm enhancements 19
2.2 Comparison of state-of-the-art schemes for scalable blockchain 22
2.3 Comparison of state-of-the-art schemes for interoperable blockchain 24

5.1 Symbol table for BLISS and SCAB-IoTA 74
5.2 Individual computation time of different cryptographic functions for IoT testbed 88
5.3 Computation cost (CC) and energy consumption (EC) of BLISS, SCAB-IoTA, compared with state-of-the-art schemes on Desktop and Raspberry Pi (RP) 89
5.4 Comparative storage and communication cost of BLISS, SCAB-IoTA with state-of-the-art schemes 89
5.5 Comparative security analysis of BLISS and SCAB-IoTA with state-of-the-art schemes . . . 90
5.6 Symbol table for LBSV and SmartCoin 98
5.7 Types of messages and the corresponding SmartCoins 106
5.8 Individual computation time of different cryptographic functions in the testbed environment 110
5.9 Computation cost (CC) and energy consumption (EC) of LBSV and SmartCoin compared with state-of-the-art schemes on Desktop and Raspberry Pi (RP) 110
5.10 Comparative storage and communication cost of LBSV and SmartCoin with state-of-the-art schemes 111
5.11 Comparative security analysis of LBSV and SmartCoin with state-of-the-art schemes based on different attacks 117
5.12 Mathematical symbol table for SmartGrid-NG and ETradeChain 121
5.13 Individual computation time of different cryptographic functions for smart grid testbed . . . 141
5.14 Performance analysis of SmartGrid-NG based on the comparison of computation cost (CC) in milliseconds and energy consumption (EC) in Joule on Desktop and Raspberry Pi 4 2GB (RP) with state-of-the-art schemes 142
5.15 Performance analysis of ETradeChain based on the comparison of computation cost (CC) in milliseconds and energy consumption (EC) in Joule of ETradeChain on Raspberry Pi 4 (RP) 2GB and 4GB with state-of-the-art schemes 143
5.16 Comparison of storage and communication cost of ETradeChain with state-of-the-art schemes 144
5.17 Security comparisons of SmartGrid-NG and ETradeChain with state-of-the-art schemes . . 144
5.18 Comparison of computation cost (CC) in milliseconds and energy consumption (EC) in Joule of *zk-SGB* on Raspberry Pi 4 (RP) 2GB and 4GB with state-of-the-art schemes 159