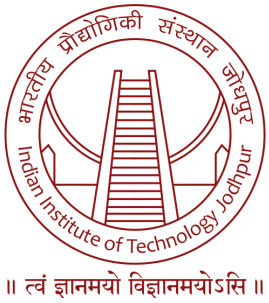
Cutting-Edge Consensus Algorithms in Scalable and Interoperable Blockchain

A Thesis Submitted By
Lokendra Vishwakarma

in partial fulfillment of the requirements for the award of the degree of
Doctor of Philosophy



Indian Institute of Technology Jodhpur
Computer Science And Engineering
April 2024

6

Conclusion and Future Work

CONCLUSION

This thesis provides a comprehensive investigation into the expansive capabilities of blockchain technology, extending its applications well beyond the confines of cryptocurrency. Chapter 1 introduces the foundational concepts of blockchain, setting the stage for the in-depth exploration that follows. Chapter 2 thoroughly reviews existing literature, highlighting key challenges and gaps in current blockchain research. This contextual foundation leads to the subsequent contributions, where novel solutions are proposed to address critical issues such as scalability, interoperability, and domain-specific applications of blockchain. Chapter 3 focuses on the critical issue of scalability in public blockchains by introducing two novel sharding-based blockchain protocols, namely BlockTree and UnoShard. BlockTree implements a hierarchical structure that divides the network based on the number of miners in each group, significantly enhancing transaction handling and scalability. This structure allows for efficient block validation and propagation, mitigating common bottlenecks that typically hinder scalability. On the other hand, UnoShard leverages DPoS to divide the network into shards, distributing the workload across these shards to enable effective scaling without compromising security. It also ensures fair shard allocation, load distribution, and efficient intra-shard and cross-shard consensus to provide a robust solution to the scalability challenges. Our comparative analysis reveals that both BlockTree and UnoShard outperform state-of-the-art scalability solutions, offering promising directions for the future of scalable public blockchains. Chapter 4 then transitions the focus from scalability to interoperability, introducing the CrossLedger protocol. CrossLedger is designed to enable secure and efficient cross-chain asset transfers, addressing the complexities of interoperability in multi-blockchain environments. By ensuring essential features such as non-repudiation, unlinkability, confidentiality, atomicity, and interoperability, CrossLedger paves the way for a more interconnected and versatile blockchain ecosystem.

Chapter 5 explores blockchain applications within the context of smart cities, focusing on IoT, ITS, and Smart Grid. Each section of this chapter presents independent solutions tailored to the specific challenges of these domains. For IoT, BLISS and SCAB-IoTA enhance communication security and data integrity. In ITS, LBSV and SmartCoin provide blockchain-based solutions for secure vehicular communication and incentivized data sharing. The mPBFT consensus algorithm in LBSV and LCA in SmartCoin both demonstrate superior performance compared to existing state-of-the-art solutions. In the Smart Grid domain, SmartGrid-NG, ETradeChain, and zk-SGB offer innovative approaches to energy management and decentralized energy trading. Each of these systems introduces novel consensus algorithms, such as GridChain

in SmartGrid-NG, a two-level consensus mechanism in ETradeChain, and the WNS-BFT in zk-SGB, all of which enhance the fairness, efficiency, and security of their respective applications.

Overall, this thesis emphasizes the vast potential of blockchain technology across various domains. By addressing critical challenges in scalability, interoperability, and application-specific implementations, this work contributes to the advancement of blockchain technology and its integration into the digital infrastructure. The findings of this thesis highlight the transformative impact blockchain can have on diverse fields, providing a strong foundation for future research and innovation in this rapidly evolving area.

FUTURE DIRECTION

Future research in blockchain technology could significantly benefit from focusing on enhancing interoperability across diverse blockchain platforms, building on the foundation established by CrossLedger. While CrossLedger has enabled cross-chain communication, there is still considerable potential for creating more adaptable and universal protocols that facilitate seamless interactions across a broader range of blockchain networks. Additionally, the scalability improvements achieved through BlockTree and UnoShard demonstrate the promise of sharding techniques. In these approaches, the focus has been on the efficient division of the network to enhance throughput and security; however, future efforts should also explore the efficient placement of transactions within different shards to further improve throughput and reduce latency. Moreover, integrating blockchain with emerging technologies such as redactable blockchain and quantum computing presents an exciting frontier. By combining these technologies, future research could unlock new possibilities for creating even more powerful, scalable, and versatile blockchain applications that address a wide range of real-world challenges.

Redactable Blockchain is one of the growing trends in the field of blockchain optimization. The traditional blockchains are immutable, which is its core principle. While this principle is a crucial pillar of blockchain security, it also presents challenges in situations where data must be altered or deleted, such as in the case of errors, obsolete information, or compliance with data protection regulations like the General Data Protection Regulation (GDPR) in Europe or IT ACT in Bharat. The redactable blockchain concept has the potential to address all these issues by allowing specific data in the blockchain ledger to be altered or deleted under strict conditions without compromising the overall integrity and security of the blockchain. Designing an efficient redactable blockchain scheme could open new avenues for blockchain applications such as IoT, ITS, and Smart Grid.

The rapid growth of quantum computing poses a serious challenge to traditional blockchain technology. Parallelly it also provides opportunities. It poses challenges because quantum computers, with their ability to solve complex mathematical problems, could potentially break the traditional cryptographic algorithms, such as SHA and ECC, that underpin the security of blockchain systems. Due to this vulnerability of cryptographic algorithms used in blockchain, the demand for quantum-resistant cryptographic techniques is much higher so that they can protect the blockchain against quantum attacks. Additionally, quantum computing could also be leveraged to create new types of blockchain systems—quantum blockchains—that exploit quantum entanglement and other quantum phenomena to achieve unprecedented levels of security, efficiency, and scalability. In future research, we will explore all the possibilities of quantum blockchain deployment in the real world scenarios.

Publications and Achievements

This appendix lists important publications that resulted from the methods and solutions I developed during my PhD research. These papers have undergone peer review and have been shared at reputed transactions, journals and conferences, confirming the new techniques and applications I created in my research on blockchain scalability, interoperability, and different applications. We have included the findings from these publications, particularly in the sections discussing methods and results. Along with the publications, we have also included the list of honours and achievements that we have made during the whole journey of the PhD program.

TRANSACTIONS

1. **Vishwakarma, Lokendra**, Ankur Nahar, and Debasis Das. "LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV." **IEEE Transactions on Vehicular Technology** 71, no. 6 (2022): 5983-5994, **Impact Factor: 6.8**

2. Kumar, Amritesh, **Lokendra Vishwakarma**, and Debasis Das. "LandChain: A MultiChain Based Novel Secure Land Record Transfer System." **IEEE Transactions on Reliability** (2024), **Impact Factor: 5.9**

3. Barbhaya, Umang Rajendra, **Lokendra Vishwakarma**, and Debasis Das. "ETradeChain: Blockchain-Based Energy Trading in Local Energy Market (LEM) Using Modified Double Auction Protocol." **IEEE Transactions on Green Communications and Networking** (2023), **Impact Factor: 4.8**

JOURNALS

1. **Vishwakarma, Lokendra**, and Debasis Das. "SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain." **Journal of Parallel and Distributed Computing** 154 (2021): 94-105, **Impact Factor: 3.8**

2. **Vishwakarma, Lokendra**, and Debasis Das. "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain." **Vehicular Communications** 33 (2022): 100429, **Impact Factor: 6.7**

3. **Vishwakarma, Lokendra**, and Debasis Das. "BlockTree: a nonlinear structured, scalable and distributed ledger scheme for processing digital transactions." **Cluster Computing** 24, no. 4 (2021): 3751-3765, **Impact Factor: 4.4**

4. **Vishwakarma, Lokendra**, and Debasis Das. "BLISS: Blockchain-based Integrated Security System for Internet of Things (IoT) Applications." **International Journal of Information Security** (2024): 1-17, **Impact Factor: 3.2**

5. Gupta Shristy, Amritesh Kumar, **Lokendra Vishwakarma**, Debasis Das, "Enhancing Blockchain Scalability and Security: The Early Fraud Detection (EFD) Framework for Optimistic Rollups", **Cluster Computing**, 2024, **Impact Factor: 4.4**

6. Kumar, Amritesh, **Lokendra Vishwakarma**, and Debasis Das. "R-PBFT: A secure and intelligent consensus algorithm for Internet of vehicles." **Vehicular Communications** 41 (2023): 100609, **Impact Factor: 6.7**

CONFERENCES PROCEEDINGS

1. **Vishwakarma, Lokendra**, Amritesh Kumar, Jeevan Madugunda, Debasis Das. "FinBlock: Secure and Fast Transaction Confirmation with High Throughput for FinTech Application" In **IEEE Wireless Communications and Networking Conference 21–24 April 2024, Core Ranking: B**

2. **Vishwakarma, Lokendra**, Debasis Das, Sajal K. Das, and Christian Becker. "SmartGrid-NG: Blockchain Protocol for Secure Transaction Processing in Next Generation Smart Grid." In Proceedings of the 25th **International Conference on Distributed Computing and Networking**, pp. 174-185. 2024, **Core Ranking: B**.

3. **Vishwakarma, Lokendra**, Amritesh Kumar, and Debasis Das. "CrossLedger: A Pioneer Cross-chain Asset Transfer Protocol." In 2023 IEEE/ACM 23rd **International Symposium on Cluster, Cloud and Internet Computing (CCGrid)**, pp. 568-578. IEEE, 2023, **Core Ranking: A**

4. Kumar, Amritesh, Monu Nagar, **Lokendra Vishwakarma**, and Debasis Das. "HN-mPBFT: A Healthy Node based Modified Secure and Fast Consensus Mechanisms for Internet of Vehicles." In 2023 **International Wireless Communications and Mobile Computing (IWCMC)**, pp. 1638-1643. IEEE, 2023, **Core Ranking: B**

5. Nahar, Ankur, **Lokendra Vishwakarma**, and Debasis Das. "Metoids: Hybrid k-medoids-meta heuristic clustering-based routing optimization in vehicular ad-hoc networks." In 2022 IEEE 95th **Vehicular Technology Conference:(VTC2022-Spring)**, pp. 1-5. IEEE, 2022, **Core Ranking: B**

6. **Vishwakarma, Lokendra**, and Debasis Das. "BSS: Blockchain Enabled Security System for Internet of Things Applications." In 2020 IEEE 19th **International Symposium on Network Computing and Applications (NCA)**, pp. 1-4. IEEE, 2020, **Core Ranking: B**

COMMUNICATED

1. **Lokendra Vishwakarma**, Amritesh Kumar, Debasis Das. "UnoShard: Harmonizing Scalability and Security in Blockchain Sharding." In **IEEE Transactions on Information Forensics and Security (TIFS), 2024, Impact Factor: 6.8**

2. **Lokendra Vishwakarma**, Debasis Das. "zk-SGB: Privacy-Preserved Blockchain Framework for Energy Trading in Smart Grid Using Zero Knowledge Proof." In **IEEE Transactions on Consumer Electronics, Impact Factor: 4.3**.

3. **Lokendra Vishwakarma**, Umang Rajendra Barbhaya, Debasis Das, Sukumar Nandi. "GreenChain: Utilizing Consortium Blockchain for Peer-to-Peer Energy Trading in Smart Grid." In **ACM 31st**

Annual International Conference on Mobile Computing and Networking (MobiCom) Nov 2025, Hong Kong, China, Core Ranking: A*

4. Amritesh Kumar, **Lokendra Vishwakarma**, Debasis Das. "GB^2S: A Generalized Balanced Blockchain System." **IEEE Transactions on Reliability 2024, Impact Factor: 5**

5. Amritesh Kumar, Shristy Gupta, **Lokendra Vishwakarma**, Debasis Das. "CollyBus: A Novel Framework for Cross Border Transactions in Blockchain." In **22nd International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks. WiOpt 2024**

HONORS AND ACHIEVEMENTS

1. Received **SERB International Travel Support Grant** for participating in the IEEE Wireless Communications and Networking Conference (WCNC) 2024 at Dubai, United Arab Emirates, by the Science and Engineering Research Board, DST India.

2. Received **ACM India Research Facilitation Grant (RFG) 2024** for the overlength page charges for the publication in the **IEEE Transactions on Green Communications and Networking.**

3. Article Selected in the **ACM Academic Research and Careers for Students (ARCS) 2024** for the paper and poster presentation.

4. **Student Travel Award (STA)** for participating in the **ACM ICDCN 2024** in Jan 2024 and **ACM/IEEE CCGRID 2023** in May 2023 by CCGRID Student Grant Committee.

5. Published research article "Blockchain-based Security Protocol for Next-Generation Smart Grid Transactions." in **TechScape, 2020, Indian Institute of Technology Jodhpur**.

6. Awarded best **Teaching Assistantship (TA)** in the years 2022 and 2023.

7. Held the position of Chair at ACM Student Chapter IIT Jodhpur from July 2021 to July 2022.

8. Published Poster "pzLedger: Privacy Preservation for Energy Trading Transaction in Smart Grid" in **International Conference on Information Systems Security (ICISS 2022), National Conference**, IIT Tirupati, India.

9. Received **Student Travel Grant** from Science and Engineering Research Board (SERB), **Department of Science and Technology (DST), India**, for participating in Karyashala on Vehicular Communications for Next-Generation Intelligent Transportation Systems, held at Indian Institute of Technology Indore, July 2022.

10. Published Poster "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain" in **Network and Distributed System Security (NDSS) 2022 (Core Ranking: A*)**, San Diego, California, USA.

11. Received **Student Registration Grant** for participating in the **USENIX Security** August 2021 and **ACM SIGMETRICS**, June 2021.

12. Won the **first prize** in the Student's Pitch Competition in the category of Smart Infrastructure held as part of **Industry Day 2021**, organized at the **Indian Institute of Technology Jodhpur**, Rajasthan.