Cutting-Edge Consensus Algorithms in Scalable and Interoperable Blockchain

Abstract

The development of consensus algorithms is crucial for enhancing the scalability and interoperability of blockchain technology, which is key to its wider adoption. However, existing consensus algorithms, including Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), face challenges such as high consensus delay, low throughput, and limited transaction scalability, primarily due to their high computational and communication complexity. Moreover, these algorithms rely on third parties to communicate across diverse blockchain platforms, making blockchain vulnerable, which emphasizes the necessity for interoperable solutions. In addition, ensuring information privacy within blockchain systems remains a significant challenge.

Therefore, in this thesis, we develop novel consensus algorithms while focusing on improving consensus delay and throughput. The proposed modified Practical Byzantine Fault Tolerance (mPBFT) and Lightweight Consensus Algorithm (LCA) consensus algorithms are the improvement over the PBFT consensus protocol, which reduces the computation and communication complexity. The GridChain (a reputation based consensus algorithm) and Weighted Node Selection Byzantine Fault Tolerance (WNS-BFT) are the reputation and trust-based consensus algorithms that establish trust among the nodes while keeping the performance high. Additionally, to improve the performance further, we have developed a technique called BlockTree (a nonlinear structured, scalable, and distributed ledger) and UnoShard (Harmonizing Scalability and Security) schemes that address the issue of limited scalability by enabling the parallel processing of transactions. Furthermore, to address the interoperability issues between the diverse blockchain platforms, we developed a technique called CrossLedger (a pioneer cross-chain asset transfer protocol) that eliminates the presence of third parties for communication. This thesis has also addressed the issue of information privacy in the proposed technique called zk-SGB, a privacy-preserved blockchain framework for energy trading in a smart grid using zero-knowledge-proof (ZKP) without compromising system integrity.

Next, this thesis discusses the various applications based on blockchain technology, such as the Internet of Things (IoT), Intelligent Transportation Systems (ITS), and Energy Trading in the Smart Grid. We have developed three schemes for IoT using smart contracts. The first scheme is a BLISS (Blockchain-based Integrated Security System for Internet of Things (IoT) Applications), and the second scheme is SCAB-IoTA (Secure Communication and Authentication for IoT Applications using Blockchain. We have implemented these schemes on the Ethereum blockchain testnet. Additionally, we have developed a testbed using Raspberry Pi devices to show the efficiency of the proposed scheme. Furthermore, we have developed two schemes for ITS. The first scheme is a LBSV (Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV), and the second scheme is SmartCoin (A Novel Incentive Mechanism for Vehicles in Intelligent Transportation System Based on Consortium Blockchain). The LBSV and SmartCoin work on mPBFT and LCA consensus algorithms, respectively. Furthermore, we have also developed three schemes for the smart grid application. The first scheme is a SmartGrid-NG (Blockchain Protocol for Secure Transaction Processing in the Next Generation Smart

Grid), the second scheme is an ETradeChain (Blockchain-Based Energy Trading in the Local Energy Market (LEM) Using a Modified Double Auction Protocol), and the third scheme is zk-SGB (Privacy-Preserved Blockchain Framework for Energy Trading in Smart Grid Using Zero Knowledge Proof). The first two schemes are focused on trading and transaction processing and work on GridChain and two-level consensus algorithms, respectively. The zk-SGB is designed to achieve privacy in smart grid transaction processing and works on the WNS-BFT consensus algorithm. A Raspberry Pi 4 Model B devices based testbed has been developed for the implementation of ITS and smart grid schemes.