A Partitioned Parallelized and Programmable Blockchain System

Mingrui Cao, Haoyang Li, Qinquan Hu, and Bin Cao

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Background and Aim

Consortium blockchain, in which nodes are permissioned and verified, is designed to promote organizational collaboration and address industry-specific problems, such as decentralized identification, mutual trust and zero knowledge proof. As the application fields of consortium blockchains broaden and the integration of related industries keeps accelerating, consortium blockchains face the challenge of scalability. In this work, we propose the Partitioned, Parallelized, and Programmable blockchain system (P3-Chain), constructing a multi-shard two-tier architecture. Its key design insight is to extend scalability on the perspective of nodes count, architecture and scheduling simultaneously.

Design Principles

To achieve the objectives, P3-Chain introduces an asynchronous chaining methodology, guided by the following three principles.

- **By obeying Partitioning on Transaction**: Nodes are partitioned into shards based on different functions and each function is executed by specific types of transaction.
- **By obeying Parallelizing on Block**: Each shard proposes blocks in a parallelizing manner, and blocks asynchronously undergo inter-shard transactions ordering and execution.
- **By obeying Programming on Consensus**: The intra-shard consensus algorithm can be programmed for different shards to modify their functionalities. To achieve a specific function of a shard, the shard can customize its intra-shard transactions ordering and execution, and set restrictions for the results.

Model Architecture

Programmable Consensus

Intra-shard consensus algorithm consists of multiple Match-Tidy-Wrap (MTW) schemes in P3-Chain. Every MTW scheme provides three programmable function interfaces: $TxMatch$, $TxTidy$, and $BlockWrap$. $TxMatch$ defines the transaction filtering strategy, $TxTidy$ outlines the strategy for transaction selection and ordering, and $BlockWrap$ determines the method for transaction executing and block generating. By customizing these three interfaces, various MTW schemes can be crafted to handle transactions that invoke distinct smart contracts.

Performance Comparison

P3-Chain performs better than popular blockchain systems, including FISCO BCOS, partitioned Fisco, Hyperledger Fabric, partitioned Fabric and Ethereum. Moreover, the performance decrease is insignificant as system scales.

Application

Let’s sink the blockchain function to 5G with OpenAirInterface (OAI).

- **Initiate**: The unique decentralized identity (DID) initiated in the communication network based on 5G user identity information is the key for users to participate in 6G services, Web3 and etc.
- **Authenticate**: DID could be authenticated through the blockchain platform, which helps the third party to make user identity reliable.
- **Bind**: The data, authorities and values derived from the unique identity of the whole network are closely bound to the DID itself.