Technical Report

Measure and improve loopchain performance

Abstract

In this report, we will introduce the parallel execution of transactions technology, measure its performance in loopchain, and explain what technologies will be applied to improve the performance of loopchain in the future.

In loopchain 2.0, we have shown performance of up to 20K TPS by applying the parallel execution of transactions technology, and in the upcoming loopchain 3.0, we will dramatically improve performance by applying BlockSTM, Willow Merkle Tree, and Spearmint consensus.

In the prototype that applied BlockSTM to loopchain 3.0, performance of up to 84K TPS was measured.

Introduction

The scalability of blockchain has been an issue since its inception, but there has been no visible growth. As a result, blockchain services have been delayed when mass minting NFTs, and financial transactions have not been able to provide complete blockchain services, such as conducting major transactions off-chain and only recording the results on the blockchain. Because of this, some people have doubted the effectiveness of blockchain.

At a time when meaningful services utilizing blockchain are emerging, such as the minting and trading of NFTs and the integration of fragmentary investments or token securities into the system, the performance of blockchain is gaining attention again. In order for blockchains to support real-world transactions, they must be capable of handling at least tens of thousands of TPS. However, Ethereum-based blockchain platforms have shown performance of up to 4,000 TPS. Theoretically, and judging by the numbers we're seeing in practice, this seems to be the limit. To go beyond this and achieve tens of thousands of TPS, the underlying structure of the platform would need to change.

Blockchain platforms such as Solana, Aptos, and SUI have been designed from the ground up to enable blockchains to perform at high performance. The technologies they use are slightly different, but they all have in common that they improve performance by executing transactions in parallel. loopchain also uses the parallel execution of transactions technology to achieve high performance, and this feature is constantly being improved.

loopchain is a blockchain core developed by PARAMETA, which is characterized by PBFT-based consensus algorithm, Java and Python-based smart contracts, trustless interchain based on BTP (Blockchain Transmission Protocol), and high transaction processing performance. loopchain has been applied and actively used in public blockchain networks ICON and HAVAH, and in the enterprise field, it is utilized in various sites such as financial, public, and authentication fields.

The following technologies have been applied to loopchain 2.0 for high-performance transaction processing.

- **Multi-channel**

  Multi-channel is a feature that enables transaction requests, consensus, and smart contracts to be executed by channel by organizing a virtual network of channels for each task within one independent blockchain network. In other words, nodes are divided into related groups and each group is assigned a separate channel to enable block generation and validation by channel. This allows you to form various channels for each business by connecting only the parties to that business to one node, and increases processing performance by generating blocks in parallel for each channel.

- **Parallel execution of transactions**

  If transactions are independent of each other, they don't have to be executed sequentially and can be reordered. This is a way to increase performance by allowing each processor to process independent transactions independently, alleviating the bottleneck caused by sequential transaction execution. In general, parallel execution or parallel computing technologies have been developed in various fields to increase the performance of software programs.

In this report, we will introduce the parallel execution of transactions technology, measure its performance in loopchain, and explain what technologies will be applied to improve the performance of loopchain in the future.

Related technologies

In a blockchain, the order of execution of transactions is very important, and they must be executed in an agreed upon order. This sequential execution creates bottlenecks and makes it difficult to improve performance. By default, transactions cannot be executed in parallel within a single chain, so many systems have tried to improve performance by utilizing parallel chains such as sharding or L2, as in Ethereum. However, separate chains are not effective because there is no trust in inter-chain communication, and separate proofs need to be generated to provide trust, resulting in high overhead.

Another approach to improving blockchain performance is technology that enables parallel execution of transactions, and some blockchains are seeing dramatic performance improvements. Aptos and Solana are two of them.

- **BlockSTM by Aptos**

Aptos has reported that it can achieve 160K TPS performance with a technology called BlockSTM.

Reference
- https://arxiv.org/pdf/2203.06871.pdf
- Block-STM: How We Execute Over 160k Transactions Per Second on the Aptos Blockchain

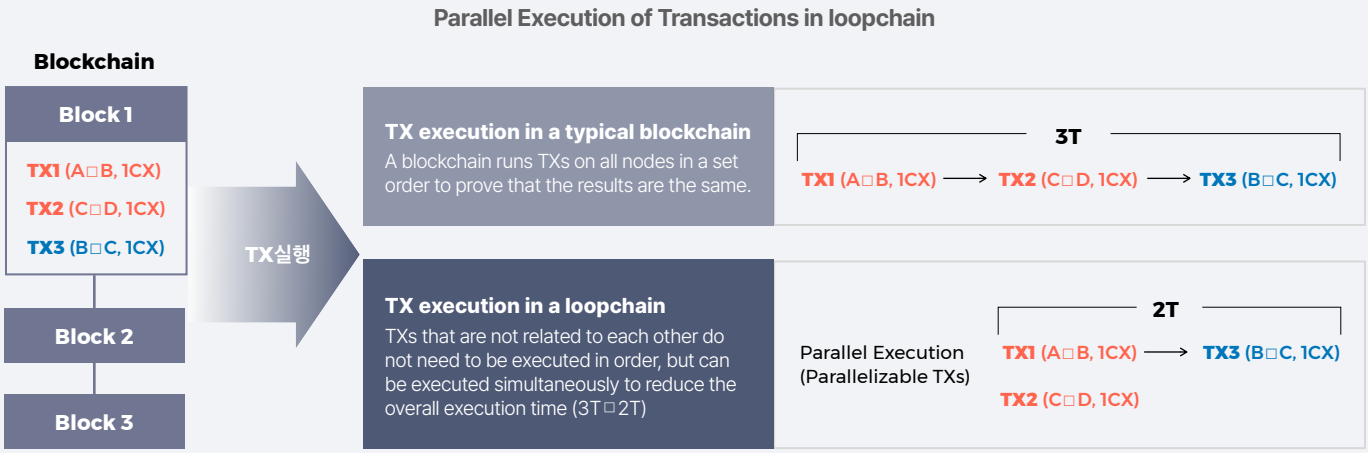
- **Sealevel by Solana**

Solana is using its parallel processing of transactions technology to achieve performance of around 4000 TPS.

Reference
- Sealevel — Parallel Processing Thousands of Smart Contracts | by Anatoly Yakovenko | Solana | Medium

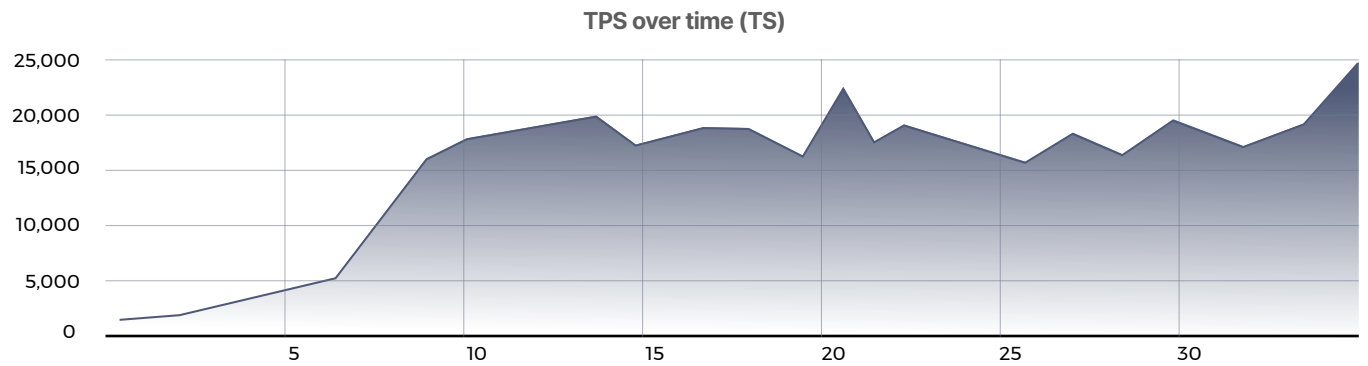
Parallel processing of transactions in loopchain 2.0

By applying a processing technology that allows transactions to be executed in parallel when the accounts involved are independent of each other, loopchain has realized parallel execution of transactions, dramatically reducing the time required to execute transactions in a block. The more TXs that can be executed in parallel, the shorter the overall execution time of the block. Not only asset transfers, but also smart contract execution can be executed in parallel as long as the smart contract functions called by the TXs are independently executable. (loopchain uses the 'isolated' directive to specify that they can be executed independently.)



To check the maximum performance when applying the parallel execution of transactions technology in loopchain, we set up the following environment, excluding network and consensus delays.

- single node Prepare 500,000 TXs for 1000 users to randomly send coins to each other
- Start block generation using the generated
- TXs concurrency 4 (utilizing 4 processors)
- Hardware running the node : Intel(R) Xeon(R) Gold 6128 CPU @ 3.40GHz / 64GB RAM / NVMe



Up to 20K TPS performance can be achieved with the parallel execution of transactions technology in loopchain. The code and materials for all tests are available in the "Repository" below.
https://forms.gle/yeeewUwGLTB7yzs16

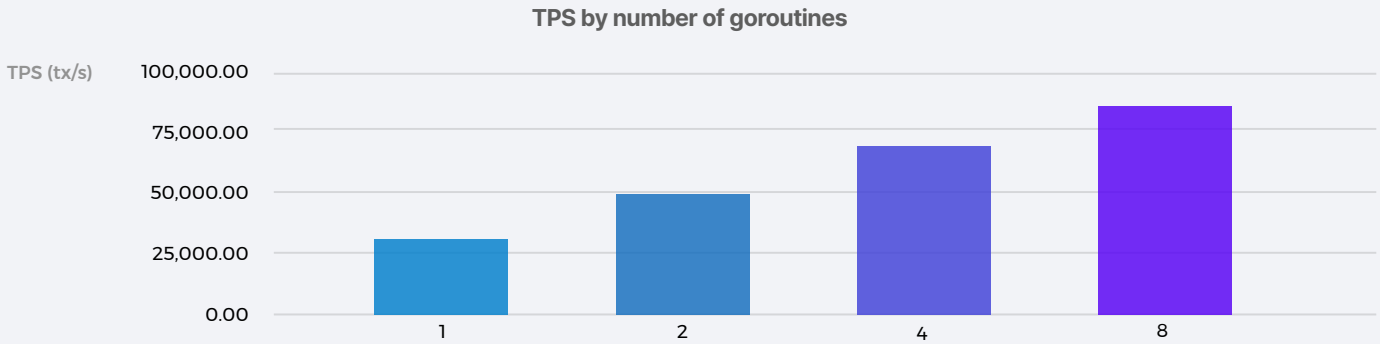
loopchain 3.0 performance

loopchain 3.0 is being developed to support BTP-based interchanges, Solidity smart contracts, and a high-performance blockchain core with tens of thousands of TPS. It aims to realize up to 100K TPS by applying the following technologies.

BlockSTM

BlockSTM is a method of executing transactions within a block in parallel, and is a technology adopted by Aptos. It is characterized by not requiring transaction write sets or dependency information between transactions.

We developed a loopchain 3.0 prototype with BlockSTM and measured its performance as follows. When 100,000 users (wallets) randomly exchange coins with each other, the performance is up to 84K TPS.



*goroutines : Shows concurrency. So if it's 8, then 8 processes will run concurrently.

WMT (Willow Merkle Tree)

WMT is a Sparse Merkle Tree that is a variant of JMT (Jellyfish Merkle Tree) with optimized space efficiency and computational efficiency for LSM (Log-Structured Merge) Tree-based Key-Value Database. JMT assumes that the key is a hash and is designed to work efficiently in this case, while WMT is designed to work efficiently even when the key is not a hash.

Spearmint Consensus

Spearmint is a PBFT Consensus Algorithm based on Tendermint. It is designed to maximize TPS by pipelining the three stages of block propagation, execution, and voting. It reduces the message complexity compared to Tendermint by ensuring that the message complexity is O(n) when there is no network failure. However, like Tendermint, it does not generate a fork before finalization, so there is no fork management burden.

P2P Network Enhancement

It improves the performance of P2P networks for efficient sharing of transaction and block data.

Conclusion

We have confirmed the maximum TPS performance of loopchain 2.0 and estimated the target performance through prototypes of performance enhancement technologies to be applied to loopchain 3.0.

Improving the performance of the blockchain so that there are no delays in NFT minting, ST transactions, and payments on the blockchain is a key technology element for blockchain revitalization. PARAMETA's loopchain is a blockchain that can seamlessly support these blockchain-based services.

loopchain 3.0 will be developed as a high-performance blockchain that applies technologies such as BlockSTM, Willow Merkle Tree, and Spearmint. In addition, it will support Solidity for the convenience of dApp service development and provide BTP for trustless interchain.

References

- Block-STM: Scaling Blockchain Execution by Turning Ordering Curse to a Performance Blessing
- Block-STM: How We Execute Over 160k Transactions Per Second on the Aptos Blockchain
- Sealevel — Parallel Processing Thousands of Smart Contracts | by Anatoly Yakovenko | Solana | Medium
- Jellyfish Merkle Tree
- Tendermint White Paper
- loopchain Test Code Application Page
- Parallel Execution of Transactions in loopchain to Improve Blockchain Performance
- PARAMETA's Blockchain Core Underlying Technology, loopchain
- What is BTP? | ICON Community

Technical Report

PARAMETA