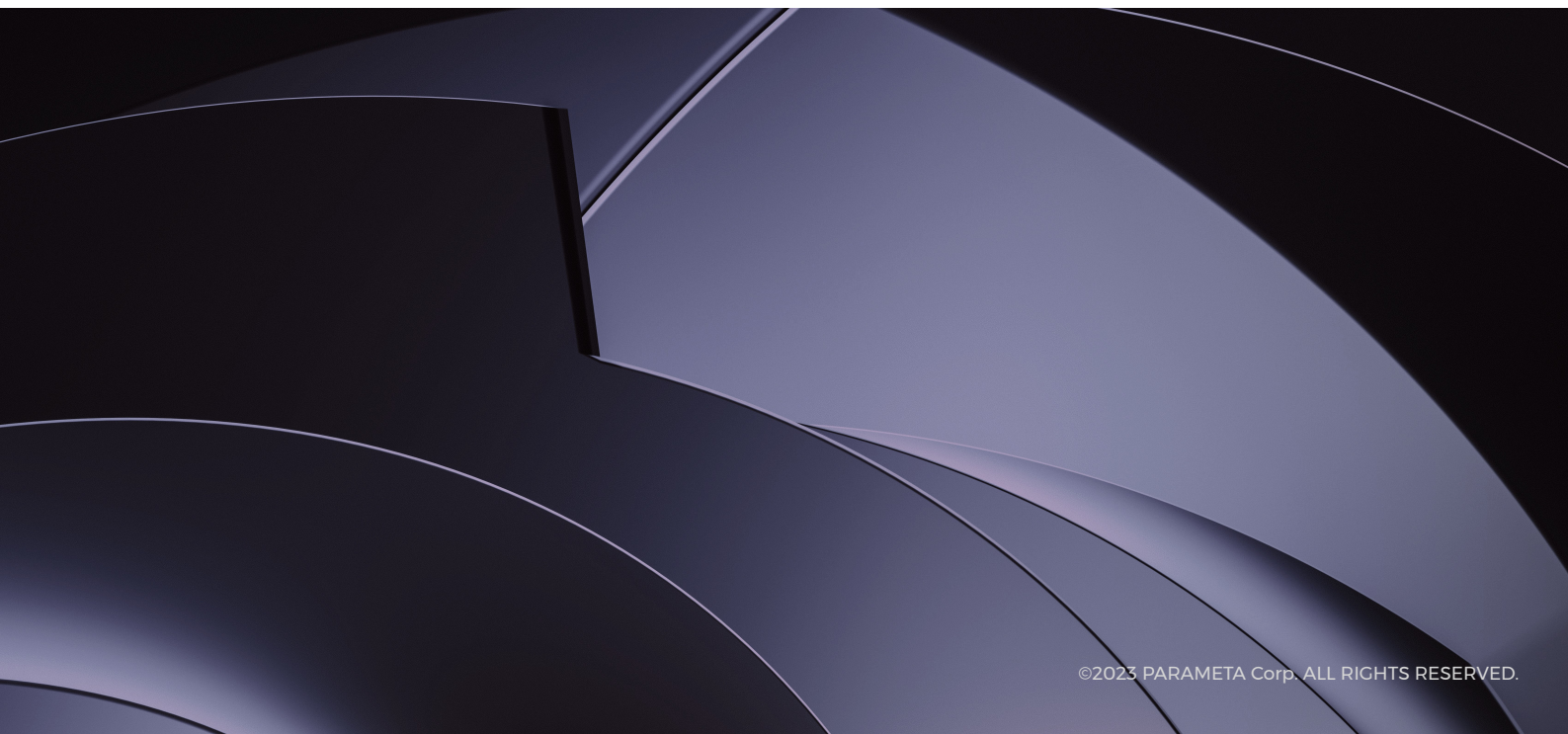
Technical Report

loopchain measure and improve performance



Abstract

이 문서에서는 블록체인의 성능 향상에 필요한 기술을 간략하게 살펴보고, 해당 기술들이 loopchain에 어떻게 적용되어 어느 정도의 성능을 발휘하는지 시험한 결과를 제공한다.

loopchain 2.0에서는 트랜잭션 병렬 실행 기능을 적용하여 최대 20K TPS의 성능을 보여주고 있으며, 앞으로 개발될 loopchain 3.0에서는 BlockSTM, Willow Merkle Tree, Spearmint 합의 등을 적용하여 획기적으로 성능을 개선할 예정이다.

loopchain 3.0에 BlockSTM을 적용한 프로토타입에서는 최대 84K TPS의 성능이 측정되었다.

Introduction

블록체인의 확장성 문제는 초창기부터 이슈화되어 왔지만, 눈에 보일 만한 성장이 이루어지지는 않았다. 그로 인해 NFT 대량 민팅 시 블록체인 서비스가 지연된다거나, 금융 거래 시 주요 거래를 오프체인에서 진행한 뒤 그 결과만 블록체인에 기록한다거나 하는 등 완전한 블록체인 서비스를 제공하지는 못해 왔다. 이 때문에 블록체인의 효용성을 의심하는 사람들도 있어 온 것이 사실이다.

NFT 민팅과 거래가 활성화되고 조각투자 또는 토큰증권의 제도권 편입이 추진되는 등 블록체인을 활용한 의미 있는 서비스가 나타나는 현시점에서, 블록체인의 성능은 다시 주목받고 있다. 블록체인으로 실생활의 거래를 지원할 수 있으려면 적어도 수만 TPS를 처리할 수 있는 성능이 되어야 한다. 하지만 이더리움 기반의 블록체인 플랫폼들은 최고 4000 TPS 정도의 성능을 보여주고 있다. 이론적으로, 그리고 실제 확인되는 수치로 판단해 보건대 이 정도가 한계인 것으로 추측된다. 이를 뛰어넘어 수만 TPS의 성능을 발휘하려면 플랫폼의 기본 구조 자체가 바뀌어야 할 것으로 예상된다.

Solana, Aptos, SUI 등의 블록체인이 고성능을 발휘할 수 있도록 기반 구조부터 새로 설계된 블록체인 플랫폼들이다. 이들의 사용 기술은 조금씩 다르나, 트랜잭션을 병렬로 실행시켜 성능을 향상하는 기술이라는 점은 공통적이다. loopchain도 트랜잭션을 병렬로 실행시키는 기술 적용으로 고성능을 발휘하고 있으며, 해당 기능은 지속적으로 개선되고 있다.

loopchain은 파라메타가 자체 개발한 블록체인 코어로서, PBFT 기반 합의 알고리즘, Java와 Python 기반 스마트 컨트랙트, BTP(Blockchain Transmission Protocol) 기반의 Trustless 인터체인, 그리고 높은 트랜잭션 처리 성능을 보여주는 것이 그 특징이다. loopchain은 퍼블릭 블록체인 네트워크인 ICON과 HAVAH에 적용, 활발히 사용되고 있으며 엔터프라이즈 영역에서는 금융, 공공, 인증 분야 등 다양한 사이트에 활용되고 있다.

---

loopchain 2.0에는 고성능 트랜잭션 처리를 위하여 다음 기술이 적용되었다.

- **멀티채널**

  멀티채널은 하나의 독립적인 블록체인 네트워크 내에서 업무별로 채널이라는 가상의 네트워크를 구성하여 채널별로 거래 요청, 합의 및 스마트 컨트랙트를 수행할 수 있도록 하는 기능이다. 즉, 노드를 관련된 그룹으로 나누고 각 그룹마다 별도의 채널을 할당하여 채널별로 블록 생성 및 검증이 가능하도록 한다. 이로써 하나의 노드에 해당 업무 당사자들만 연결되어 업무별로 채널을 다양하게 형성할 수 있으며, 채널별로 블록을 병렬 생성하기 때문에 처리 성능을 높일 수 있다.

- **트랜잭션 병렬실행**

  트랜잭션들이 서로 독립적일 경우, 굳이 순차적으로 실행할 필요가 없으며 순서가 바뀌어도 상관없다. 서로 독립적인 트랜잭션들을 각각의 프로세서들이 독립적으로 처리하도록 하여 순차적 트랜잭션 실행에서 오는 병목 현상을 완화, 성능을 높이는 방법이다. 일반적으로 소프트웨어 프로그램의 성능을 높이기 위해 다양한 분야에서 병렬 실행 또는 병렬 컴퓨팅 기술이 발전해 왔다.

여기에서는 트랜잭션 병렬 실행 기술에 대해서 알아보는 동시에 loopchain에서의 성능을 측정해 보고, 향후 어떠한 기술을 적용해 loopchain의 성능을 개선할 것인지 설명하고자 한다.

Related technologies

블록체인에서는 트랜잭션들의 실행 순서가 매우 중요하며, 합의된 순서대로 실행되어야만 한다. 순차적 실행을 이유로 병목 현상이 생기며, 이 때문에 성능 향상이 어려운 구조를 지니고 있다. 기본적으로 하나의 체인 내에서는 트랜잭션을 병렬로 실행시키지 못하므로, 이더리움 등에서와 같이 샤딩이나 L2와 같은 병렬 체인을 활용하여 성능을 개선하고자 해 왔다. 하지만 별도의 체인은 체인 간 통신에 있어서의 신뢰가 없으며, 신뢰를 주기 위해서는 별도의 proof를 생성해야 하는 등 오버헤드가 커서 효과적이지 못한 면이 있다.

블록체인 성능 향상을 위한 또 다른 접근 방법이 트랜잭션의 병렬 실행을 가능하게 하는 기술이며, 이를 통하여 획기적인 성능 향상을 보이고 있는 블록체인들이 있다. 여기서는 Aptos와 Solana를 소개한다.

- **BlockSTM by Aptos**

Aptos는 BlockSTM이라는 기술을 적용하여 160K TPS의 성능을 발휘할 수 있을 것이라고 리포팅했다.

참고자료

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

- **Sealevel by Solana**

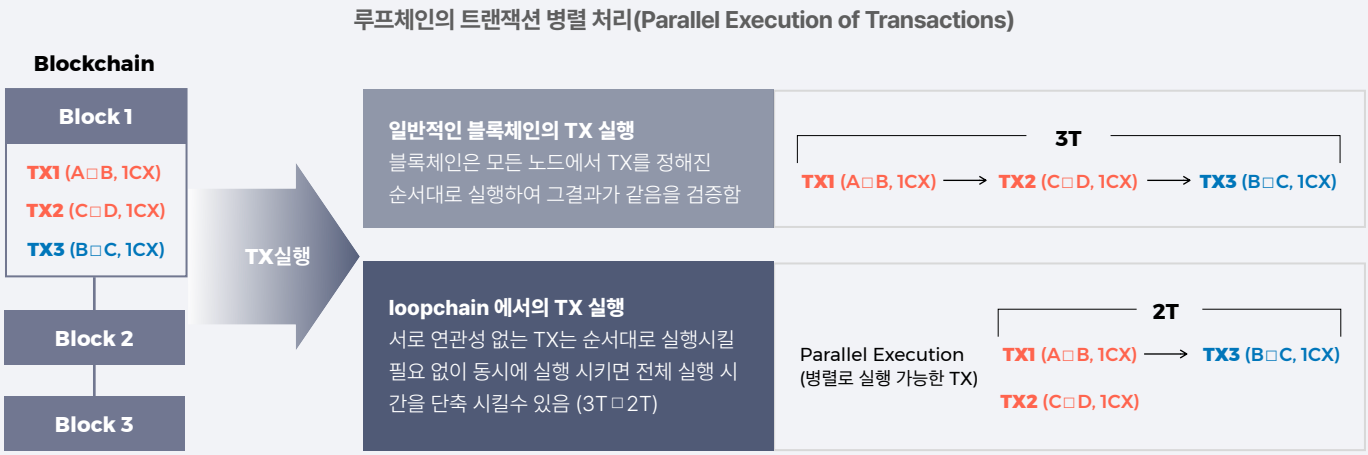
Solana는 트랜잭션 병렬 기술을 적용하여 약 4000 TPS의 성능을 보이고 있다.

참고자료

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

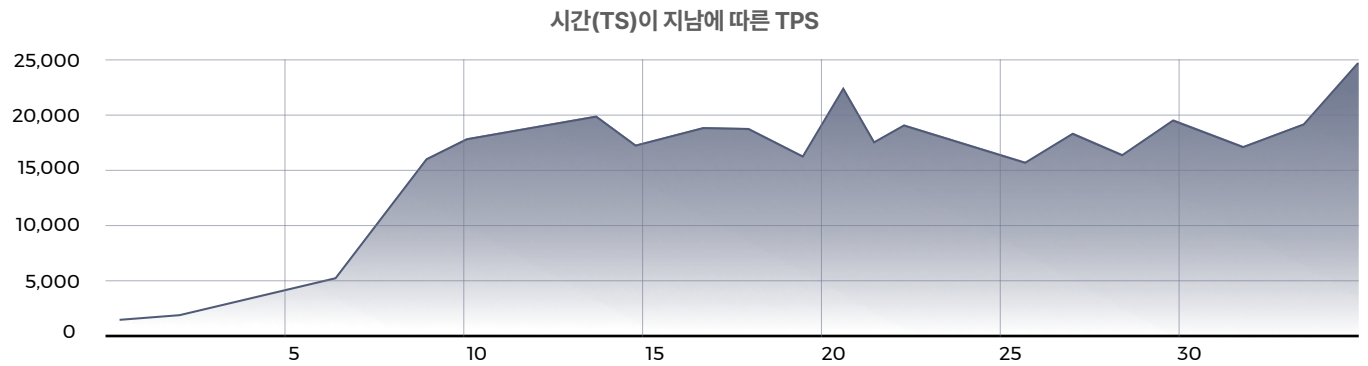
Parallel processing of transactions in loopchain 2.0

루프체인에서도 트랜잭션들이 관여하는 계정이 서로 독립적일 경우 이를 병렬로 실행할 수 있도록 하는 처리 기술을 적용, 트랜잭션들의 병렬 처리를 실현해 한 블록의 트랜잭션을 실행하는 데 소요되는 시간을 획기적으로 줄였다. 병렬로 실행할 수 있는 TX가 많으면 많을수록 해당 블록의 전체 실행 시간은 줄어들게 된다. 단순한 자산 이체뿐 아니라 스마트 컨트랙트 실행에 있어서도 TX가 호출하는 스마트 컨트랙트 함수가 독립적으로 실행 가능한 경우라면 병렬로 실행할 수 있다. (loopchain에서는 독립적으로 실행 가능함을 지정해 주는 'isolated' directive를 사용한다.)



loopchain의 트랜잭션 병렬 처리 기술 적용 시의 최대 성능 확인을 위해, 네트워크와 합의 지연을 배제하고 아래와 같은 환경을 세팅하여 시험했다.

- single node (합의 없음)
- 1000 user가 서로 코인을 랜덤하게 전송하는 TX를 500,000개 생성하여 준비
- 생성된 TX를 이용하여 블록 생성 시작
- concurrency 4 (processor 4개 활용)
- 노드를 실행한 하드웨어: Intel(R) Xeon(R) Gold 6128 CPU @ 3.40GHz / 64GB RAM / NVMe



loopchain의 트랜잭션 병렬 처리 기능을 통하여 최대 20K TPS 성능을 확인할 수 있다.
모든 시험에 필요한 코드 및 자료는 아래 Repository에서 얻을 수 있다.
https://forms.gle/yeeewUwGLTB7yzs16

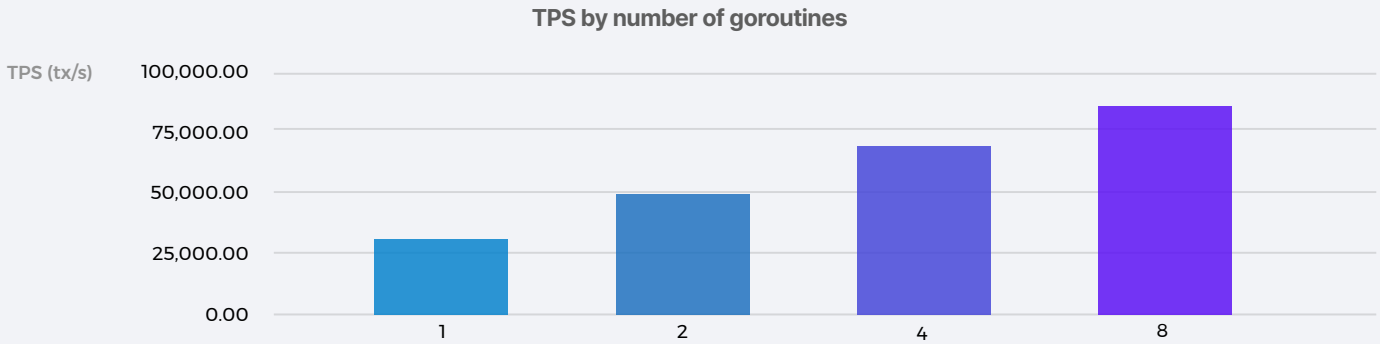
loopchain 3.0 performance

loopchain 3.0은 BTP 기반의 인터체인, Solidity 스마트 컨트랙트를 지원하고 수만 TPS의 고성능 블록체인 코어를 목표로 개발 진행 중이다. 다음과 같은 기술들을 적용하여 최대 100K TPS를 실현하는 것을 목표로 하고 있다.

BlockSTM

BlockSTM은 block 내의 transaction을 병렬로 실행하는 방법으로, 앞서 언급한 Aptos에서 채용한 기술이다. 특별히 transaction의 write set이나 transaction 간 의존성 정보 입력을 요구하지 않는 것이 특징이다.

BlockSTM을 적용한 loopchain 3.0 프로토타입을 개발하여 성능을 측정한 결과는 아래와 같다. 100,000명의 사용자(지갑)가 서로 랜덤하게 코인을 주고받았을 때, 최대 84K TPS의 성능을 발휘한다.



*goroutines : concurrency를 표시함.즉 8이면 8개의 process가 동시에 실행됨

WMT (Willow Merkle Tree)

WMT는 LSM(Log-Structured Merge) Tree 기반 Key-Value Database를 위해서 공간 효율성과 계산 효율성이 최적화된 JMT(Jellyfish Merkle Tree)를 변형한 Sparse Merkle Tree이다. JMT의 경우 Key가 Hash인 것을 가정하여 이 경우에 효율적으로 동작하도록 설계되어 있는 반면, WMT는 Key가 Hash가 아닐 때도 효율적 동작이 가능하도록 설계되었다.

Spearmint Consensus

Spearmint는 Tendermint 기반의 PBFT Consensus Algorithm이다. Block 전파, 실행, 표결의 세 Stage를 Pipelining 하여 TPS를 최대한 높이는 방향으로 설계되었다. 네트워크 장애가 없는 경우 Message 복잡도가 O(n)으로 동작하도록 하여, Tendermint 대비 Message 복잡도를 줄였다. 그러면서도 Tendermint와 마찬가지로 Finalization 이전 Fork를 발생시키지 않아 Fork 관리 부담이 없도록 한 것이 특징이다.

P2P Network Enhancement

트랜잭션과 블록 데이터의 효율적인 공유를 위해서 P2P 네트워크의 성능을 향상시킨다.

Conclusion

loopchain 2.0에서의 최대 TPS 성능을 확인했고, loopchain 3.0에 적용할 성능 향상 기술의 프로토타입을 통해 목표 성능을 예상해 봤다.

블록체인상에서 NFT 민팅, ST 거래, 결제 시 지연이 되지 않도록 블록체인의 성능을 향상하는 것은 블록체인 활성화를 위한 핵심적 기술 요소이다. 파라메타의 loopchain은 이러한 블록체인 기반 서비스를 원활하게 지원할 수 있는 블록체인이다.

loopchain 3.0은 BlockSTM, Willow Merkle Tree, Spearmint 등의 기술을 적용한 고성능 블록체인으로 개발될 예정이다. 그뿐만 아니라 dApp 서비스 개발의 편의를 위해 Solidity를 지원하고, Trustless Interchain을 위한 BTP를 제공할 예정이다.

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
- https://forms.gle/yeeewUwGLTB7yzs16
- 블록체인 성능 향상을 위한 루프체인의 트랜잭션 병렬 처리(Parallel Execution of Transactions)
- 파라메의 블록체인 코어 원천 기술, 루프체인(loopchain)
- What is BTP? | ICON Community

Technical Report