

코스모스에서 블록체인 간 메시지 전달 시간 측정 및 분석

김 정 연*, 주 흥 택°

Inter-Blockchain Communication Message Relay Time Measurement and Analysis in Cosmos

Jungyeon Kim*, Hongtaek Ju°

요 약

블록체인은 다양한 분야별로 플랫폼이 증가하면서 블록체인 간의 연동을 위한 블록체인 상호운용성에 대한 필요성이 제기되고 있다. 코스모스는 블록체인 간 통신 프로토콜(IBC)로 가상 자산 교환과 상호 기능을 활용할 수 있다. 체인 간 통신은 체인 내 통신 대비 긴 처리 과정으로 인해 체인 간 트랜잭션 증가에 따라 전체 네트워크의 초당 트랜잭션 처리 속도(TPS)를 저하할 수 있다. 따라서 블록체인 상호운용성을 활용하는 경우에는 확장성과 호환성 사이의 균형을 고려하여 설계할 수 있도록 블록체인 간 통신 성능을 평가해야 한다. 본 논문은 코스모스에서 블록체인 간 메시지 전달 시간 측정 방법과 수행한 결과를 제시하였다. 또한 블록체인 간 메시지 전달 시간 분포를 추정하고 메시지 전달 구간별 상관 관계에 대해 분석하였다.

키워드 : 코스모스, 상호운용성, 블록체인 간 통신, 블록체인 간 메시지 전달 시간

Key Words : Cosmos, Interoperability, Inter-Blockchain Communication, Inter-Blockchain Message Relay Time

ABSTRACT

The blockchain platform increase in various fields, and the need for blockchain interoperability for interworking between heterogeneous blockchains is being raised. Cosmos can utilize virtual asset exchange and mutual functions with Inter-Blockchain Communication protocols (IBC). Inter-chain communication can reduce the transaction processing speed (TPS) per second of the entire network as the number of inter-chain transactions increases, due to the longer processing process than intra-chain communication. Therefore, when using blockchain interoperability, it should be evaluate the communication performance between blockchains so that they can be designed with a balance between scalability and compatibility. In this paper, we propose a method for measuring message relay time between blockchains in Cosmos and present the results of the measuring. We also estimated the message relay time distribution between blockchains and analyzed the correlation for each message relay period.

* 본 연구는 한국연구재단 기초연구사업(NRF-2018R1D1A1B07050380) 지원으로 수행되었습니다.

• First Author : Keimyung University Department of Computer Engineering, jungyeonkim@stu.kmu.ac.kr, 학생회원

° Corresponding Author : Keimyung University Department of Computer Engineering, juht@kmu.ac.kr, 종신회원

논문번호 : 202207-152-B-RU, Received July 27, 2022; Revised August 16, 2022; Accepted August 17, 2022

I. 서 론

블록체인은 가상화폐에 최초로 적용되어 탄생한 기술이나 탈중앙화(Desentralization)와 보안(Security)에 장점을 가지고 있어 금융, 물류 등 다양한 분야로 확대되고 있다. 응용 분야가 확대되면서 블록체인의 수와 디지털 자산은 빠른 속도로 증가하고 있지만, 대부분의 블록체인은 고립된 상태로 유지되어 각각의 정보들은 본래 속한 블록체인 생태계 내에서만 독립적으로 작용한다¹¹. 또한 근본적으로 단일 블록체인의 P2P(Peer to Peer) 네트워크 성능 한계, 합의 과정의 비효율성으로 하나의 블록체인에서 충분한 서비스 요구 성능을 제공하지 못하는 문제가 있다. 이에 다양한 프로젝트가 블록체인 생태계를 활성화하기 위해서 각각의 블록체인을 하나로 묶는 이종 블록체인 간 상호운용성(Heterogeneous Blockchain Interoperability)의 정의, 기술 그리고 전망 등에 관한 연구는 활발하게 진행되고 있는 반면에, 블록체인 상호운용성 성능에 관한 전체적인 실증연구는 미흡한 실정이다¹²⁻¹⁴. 이는 블록체인 상호운용성 기술의 초기에 해당하기 때문이라 유추할 수 있다. 따라서 블록체인 상호운용성의 성능을 선제적으로 파악하여 블록체인 상호운용성 기술이 활성화될 수 있는 실증 연구가 필요하다.

코스모스(Cosmos)는 서로 다른 독립 블록체인들이 통신할 수 있도록 연결하는 플랫폼이다¹⁵. 기존 블록체인은 에너지 비효율, 제한적인 거버넌스 메커니즘과 확장성(Scalability) 문제를 가지고 있다^{6, 7}. 이를 해결하기 위해 코스모스는 블록체인 간 통신 프로토콜(IBC; Inter-Blockchain Communication)로 여러 병렬 블록체인을 연결하여 수평적으로 확장(Horizontal Scaling)한다¹⁸. 2022년 8월 16일 기준으로 코스모스는 41개의 블록체인을 연결한다. 코스모스에 첫 번째로 연결된 블록체인이자 경제 중심지 역할을 수행하는 코스모스 허브(Cosmos Hub)의 시가총액은 약 4조 3,658억이다. 코스모스 네트워크에 참여하는 블록체인들은 블록체인 간 통신 메시지를 통해서 서로 다른 블록체인과 통신할 수 있다⁹. 블록체인 간 상호 연동을 통해서 블록체인 응용 프로그램은 여러 블록체인을 활용할 수 있고 트랜잭션 처리가 병렬로 진행되므로 높은 초당 거래 속도(TPS; Transactions Per Second)를 제공받을 수 있다. 하지만 블록체인 간 상호 연동 비율이 증가함에 따라 전체 네트워크의 TPS를 감소시킬 수 있다. 이 문제를 해결하기 위해 블록체인 간 통신 프로토콜에 대한 성능 개선과 확장성과 호환성 사이의 균형을 고려하는 설계가 필수적이다.

코스모스에서 블록체인 간 통신 프로토콜 성능 개선과 설계는 블록체인 간 메시지 전달 성능 평가와 연결에 대한 기초 연구를 기반으로 도출되어야 한다.

본 논문은 코스모스에서 블록체인 간 통신 메시지 전달 시간 측정 방법을 제안한다. 본 논문에서는 코스모스 허브와 오스모시스(Osmosis) 메인넷(Mainnet)에서의 대체 가능 토큰 전송을 수행하고 이에 따라 발생한 블록체인 간 통신 메시지를 수집한다. 수집된 블록체인 간 통신 메시지로 블록체인 간 메시지 전달 시간을 측정하고 통계적 특성과 지연 구간을 분석한다. 본 논문의 결과는 블록체인 상호운용성 성능 개선 연구를 위한 기초 자료로 활용될 수 있다.

본 논문의 구성으로 2장은 코스모스 구조와 블록체인 간 통신 방법에 대해 논한다. 3장에서는 코스모스에서 블록체인 간 메시지 전달 시간 측정 방법과 분석 방법에 대해 설명한다. 4장에서는 수행된 결과와 분석 결과를 제시한다. 마지막으로 5장에서는 본 논문의 결론을 맺는다.

II. 관련 연구

2.1 블록체인 간 메시지 전달 시간 측정 연구

Kan, Luo 등¹⁰은 라우터(Router) 역할을 하는 노드를 배치하여 블록체인 네트워크를 생성하고 체인 간 트랜잭션을 전달하는 대화형 다중 블록체인 아키텍처를 제안했다. 제안한 아키텍처의 체인 내 트랜잭션은 평균 1520.56TPS인 반면에 체인 간 트랜잭션은 최대 899.81TPS로 보다 낮은 성능을 보였다. TPS 감소는 주로 라우터 블록체인 간에 통합 트랜잭션을 확인하는 단계에서 발생하고 있다는 결과를 확인했다.

Wu, Ou 등¹¹은 블록체인 간 네트워크의 성능을 모델링하기 위해 대기열 이론(Queueing Theory)에 기반한 이론적 솔루션을 제안했다. 제안된 모델은 BitXHub¹² 네트워크의 실제 트랜잭션 처리량 및 평균 응답 시간과 실험 결과의 비교를 통해서 효율성을 검증하였다.

이처럼 블록체인 상호운용성의 성능을 분석한 연구는 많지 않다. 블록체인 상호운용성 기술의 성능을 모델링하고 테스트넷에서 TPS를 측정한다. 이에 비해 실제 사용을 고려하여 메인넷에서 블록체인 간 통신 성능을 세부적으로 측정할 연구는 수행되지 않았다. 블록체인 상호운용성의 성능 최적화를 위해서는 블록체인 간 통신 시간에 대한 측정 및 분석 연구가 필요하다.

2.2 코스모스 블록체인 간 통신 과정

코스모스의 블록체인 간 통신 프로토콜(IBC; Inter-Blockchain Communication)은 독립 블록체인에 있는 모듈 간의 신뢰할 수 있고 인증된 통신을 위한 엔드 투 엔드(End-to-End) 연결 지향 프로토콜이다¹³⁾. 블록체인 간 통신 프로토콜은 알려지지 않은 동적 토폴로지에 배치된 이기종 블록체인 간의 상호 운용을 위해 설계되었으며 다양한 합의 알고리즘과 상태 머신으로 작동한다. 블록체인 간 통신 프로토콜은 코스모스 허브(Cosmos Hub), 오스모시스(Osmosis), 에모스(Evmos), 주노(Juno) 등과 같이 텐더민트(Tendermint) 기반인 블록체인과 상호 작용 시에 사용할 수 있다¹⁴⁾.

그림 1은 블록체인 간 통신 프로토콜을 사용하여 코스모스 허브에서 이기종 블록체인인 오스모시스로 대체 가능 토큰 전송(Fungible Token Transfer) 과정을 보여준다. 코스모스 허브에서 오스모시스로 대체 가능 토큰을 전송하고 싶은 사용자가 코스모스 허브 노드로 대체 가능 토큰 전송을 요청한다. 요청을 수신한 코스모스 노드는 송신 지갑 주소, 수신 지갑 주소, 토큰의 양, 토큰 단위, 송신 포트, 송신 채널을 입력받고 시간 초과 블록 높이, 타임스탬프(Timestamp)와 시퀀스(Sequence)를 추가하여 IBC Transfer 트랜잭션을 발행한다. 시퀀스는 제네시스 블록(Genesis Block)부터 생성된 특정 채널(Channel)을 통해 생성된 거래 총 수이며, 특정 거래를 가리킨다. 한 건의 거래에 대한 모든 블록체인 간 통신 트랜잭션은 동일한 시퀀스 값을 가지고 있다¹⁴⁾. IBC Transfer 트랜잭션은 코스모스 허브에서 전파되고 검증자(Validator)들의 합의

과정을 거친다. IBC Transfer 트랜잭션이 블록에 포함되고 결재의 완결성을 가지게 되면 코스모스 허브 블록체인에서 IBC Transfer 트랜잭션의 토큰은 잠금(Token Lock) 처리된다. 블록체인 간 통신 아키텍처에서 블록체인은 네트워크 인프라를 통해 서로 메시지를 직접 보내는 것이 아니라 보낼 메시지를 생성한 다음 릴레이어(Relayer)를 통해 송신 블록체인에서 수신 블록체인으로 물리적 중계를 받는다. 릴레이어는 블록체인 간 통신 프로토콜이 구현된 블록체인의 상태를 지속적으로 스캔하고 블록체인 간 통신 트랜잭션이 있을 때 중계해야 한다. 그림 1에서 릴레이어는 코스모스 허브와 오스모시스 네트워크에 모두 참여하고 있다. 릴레이어 운영은 누구나 할 수 있으며, 중계하는 블록체인에 따라 거래 수수료로 보상받을 수 있다¹⁵⁾. 릴레이어는 전달할 블록체인 간 통신 트랜잭션을 추가 및 종합(Bundling)하여 수신 블록체인으로 보내는 IBC RecvPacket을 포함한 블록체인 간 통신 트랜잭션을 발행 및 중계한다. 오스모시스에서 IBC RecvPacket 트랜잭션이 완결성을 가지면 수신 지갑 주소로 바우처가 발행(Voucher Minting)된다. 또한, 릴레이어는 수신 블록체인에서 토큰 전송 완료를 알리는 IBC Acknowledgement 트랜잭션을 구성하여 중계한다. 코스모스 허브는 IBC Acknowledgement 트랜잭션을 블록에 포함시켜 토큰 전송이 정상적으로 완료되었음을 증명한다. 블록체인 간 통신 프로토콜은 분산 네트워크를 통해 작동하고 잠재적으로 결함이 있는 릴레이어에 의존하여 메시지를 중계하므로 트랜잭션이 시간 내에 또는 목적지로 전송되지 않는 경우를 처리한다. 비정상적으로 IBC RecvPacket이 블록에 포함되지 못한 경우, 릴레이어는 IBC Timeout 트랜잭션을 생성 및 전달한다. 이를 수신한 송신 블록체인이 IBC Transfer 트랜잭션의 토큰 해제(Token Unlock) 프로세스를 실행한다¹⁴⁾. 위 과정에서 사용된 블록체인 간 통신 메시지는 4가지이며 표 1과 같다.

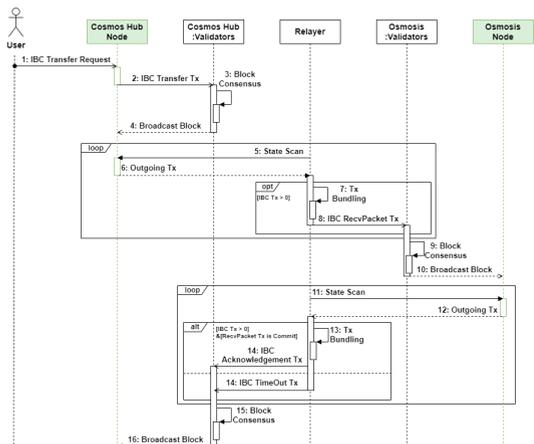


그림 1. 블록체인 간 통신 프로토콜 시퀀스 다이어그램
Fig. 1. Inter-Blockchain Communication protocol sequence diagram

표 1. 블록체인 간 통신 메시지
Table 1. Inter-Blockchain Communication message

Message Type	Description
IBC Transfer	송신 체인에서 토큰 잠금 처리
IBC RecvPacket	송신 체인의 토큰 잠금 완료 증명 및 수신 체인으로 토큰 전송
IBC Acknowledgement	수신 체인의 토큰 수신 완료 증명 및 송신 체인으로 토큰 전송 완료 응답
IBC Timeout	송신 체인으로 토큰 전송 실패 응답

III. IBC 메시지 전달 시간 측정 및 분석 방법

3.1 IBC 메시지 전달 시간 측정 방법

본 장에서는 코스모스 허브 블록체인과 오스모시스 블록체인 간의 메시지 전달 시간 수집 과정을 설명한다. 그리고 단편적으로 수집된 트랜잭션에서 블록체인 간 메시지 유효성 확인 및 추적 과정과 대체 가능 토큰 전송별 블록체인 간 메시지 전달 시간 계산 방법을 설명한다. 블록체인 간 메시지 전달 시간 측정 프레임워크는 그림 2와 같다.

본 논문에서 사용된 코스모스 허브와 오스모시스 클라이언트는 각 블록체인 메인넷 네트워크에 연결되어 참여하고 동기화 절차를 거쳐 최신 원장 상태를 유지한다. 이 클라이언트들은 네트워크에 참여하는 다른 일반 노드들과 동일하게 동작한다. 이 클라이언트들이 그림 2의 상단에 있는 측정 노드(Measurement Node)이다. 측정 노드의 코스모스 허브 클라이언트는 블록체인 간 통신 프로토콜을 기반으로 대체 가능 토큰 전

송을 주기적으로 실시하여 IBC Tx Generation 데이터를 발생시킨다. IBC Tx Generation의 데이터는 측정 노드의 코스모스 허브 클라이언트가 오스모시스 지갑 주소로 대체 가능 토큰 전송을 요청한 트랜잭션과 해당 트랜잭션을 전파한 시각이다.

전처리(PreProcess) 과정에서 앞서 발생시킨 대체 가능 토큰 전송의 성공 유무 및 전달 구간 시간 데이터를 수집하기 위해 측정 노드의 클라이언트들에게 블록에 포함된 트랜잭션 정보를 요청한다. 전처리 과정을 통해 IBC Tx Generation Controller가 생성한 후 커밋된 IBC Transfer Tx, IBC Recv Tx 그리고 IBC Ack Tx 데이터를 저장한다.

유효한 트랜잭션 필터링(Valid Tx Filtering) 과정에서는 IBC Recv Tx와 IBC Ack Tx 데이터를 입력받아 각각 Valid IBC Recv Tx와 Valid IBC Ack Tx 데이터를 출력한다. 블록체인 간 트랜잭션은 다수의 릴레이어가 중계한다. 한 건의 블록체인 간 트랜잭션은 릴레이어의 중계 과정 중 상태 증명을 위한 IBC

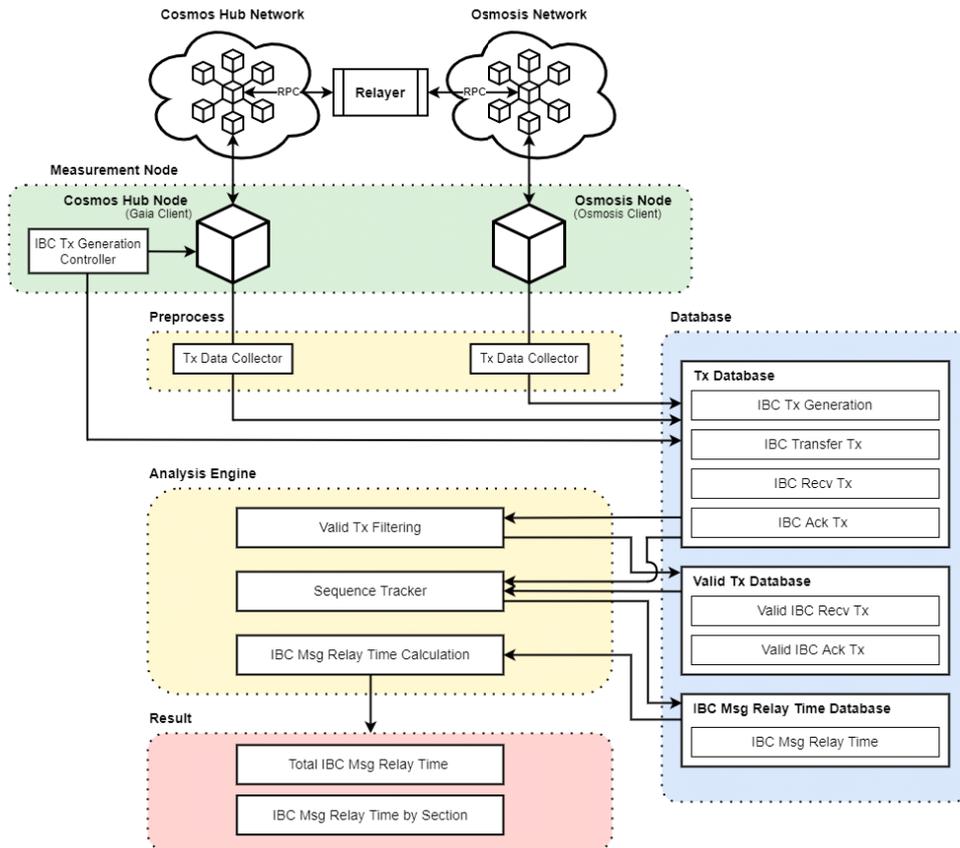


그림 2. IBC 메시지 전달 시간 측정 프레임워크
Fig. 2. IBC message relay time measurement framework

UpdateClient을 추가하면서 새로운 해쉬를 가진 트랜잭션으로 생성된다. 생성된 트랜잭션들은 수신 블록체인에 모두 포함된다. 블록에 포함된 트랜잭션 중 유효한 트랜잭션은 생성 및 전파한 릴레이어에게 트랜잭션 요금의 일부를 보상으로 제공한다¹¹⁶⁾. 유효한 트랜잭션 필터링은 IBC Recv Tx와 IBC Ack Tx 데이터에서 요금 필드가 양수값인 (Fee > 0) 트랜잭션을 필터링하여 Valid IBC Recv Tx와 Valid IBC Ack Tx 데이터로 저장한다.

시퀀스 추적(Sequence Tracker) 과정에서는 유효한 트랜잭션 필터링 과정을 마친 단편적인 트랜잭션들을 동일한 시퀀스를 기준으로 추적하여 블록체인 간 통신 트랜잭션별 타임스탬프 값을 집합한 IBC Msg Relay Time 데이터로 저장한다.

메시지 전달 시간 계산(IBC Msg Relay Time Calculation) 과정에서는 블록체인 간 통신 메시지 전달 시간과 구간별 시간을 계산한다. 또한, 측정 노드와 블록체인 네트워크의 시차를 조정한다. 블록체인 간 통신 메시지 전달 시간(IBC Msg Relay Time)은 IBC Transfer 트랜잭션을 전파하는 시각부터 IBC Acknowledgement 트랜잭션이 커밋되어 블록에 포함된 시각까지로 정의한다. 본 논문에서 정의하는 블록체인 간 메시지 전달 시간은 사용자가 대체 가능 토큰 전송을 전파하고 나서 거래 완료까지 걸리는 시간이다.

블록체인 간 통신 메시지 전달 시간은 3구간으로 나뉘며 그림 3과 같다. G to T time 구간은 IBC Transfer 트랜잭션 전파 시작 시각부터 커밋된 시각까지의 시간이다. T to R time 구간은 IBC Transfer 트랜잭션이 커밋된 시각부터 IBC RecvPacket 트랜잭션이 커밋된 시각까지의 시간이다. R to A time 구간은 IBC RecvPacket 트랜잭션이 커밋된 시각부터 IBC Acknowledgement 트랜잭션이 커밋된 시각까지의 시간이다.

블록체인 간 메시지 전달 과정의 시간은 순차적으로 증가하는 시간의 단조성을 가져야 한다. 하지만 그림 4와 같이 코스모스 허브의 Transfer_time에서 Generation_time까지의 G to T time 구간 데이터는

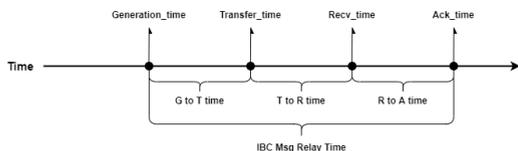


그림 3. IBC 메시지 전달 시간 구간 정의
Fig. 3. IBC message relay time interval definition

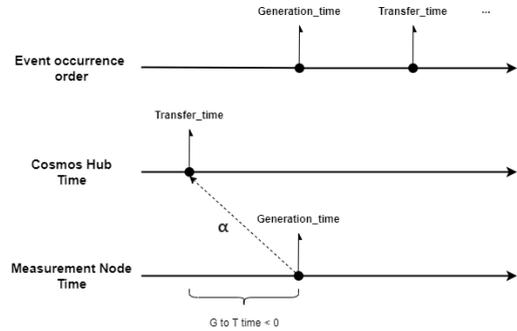


그림 4. 코스모스 허브와 측정 노드의 시차
Fig. 4. Time difference between Cosmos Hub and Measurement Node

음수로 측정되었다. 측정 노드의 시간이 코스모스 허브 시간보다 앞서 있음을 추정한다. 시차를 줄이기 위해 전체 G to T time 구간 데이터 중 최소값 α 를 Generation_time에 더한다.

코스모스 허브와 오스모시스는 텐더민트 합의 엔진을 사용한다^{17,18)}. 텐더민트의 블록 생성 시간은 검증자(Validator)가 블록 합의 과정 마지막 단계에서 제출하는 사전 커밋(Precommit)단계 메시지의 시간을 보팅 파워(Voting Power)에 비례하는 횡수로 나열한 시간 값들에서 중앙값이다¹⁹⁾. 코스모스 허브와 오스모시스 블록체인은 실험 기간에 전체 검증자의 수와 보팅 파워의 순위 변동이 없었기 때문에 일정한 시간을 유지할 것으로 간주한다.

3.2 IBC 메시지 전달 시간 분석 방법

본 논문에서는 블록체인 간 메시지 전달 시간 분포를 추정하고 메시지 전달 구간별 상관 관계에 대해 분석하기 위해 커널 밀도 추정, 상관 계수를 이용했다.

커널 밀도 추정(KDE; Kernel Density Estimation)은 분포에 대한 특정 함수를 가정하지 않고, 주어진 유한한 데이터 샘플을 기반으로 전체 모집단에 대한 추론을 하는 방법으로 수식 (1)과 같다. 본 논문에서 사용된 파이썬의 커널 밀도 추정값 플롯은 가우시안 커널 함수(Gaussian Kernel Function)를 사용하고 평활화 매개변수인 대역폭(h) 설정은 지원하지 않는다²⁰⁾.

$$\hat{f}_h(x) = \frac{1}{n} \sum_{i=1}^n K_h(x - x_i) = \frac{1}{nh} \sum_{i=1}^n K\left(\frac{x - x_i}{h}\right) \quad (1)$$

상관 계수(Correlation coefficient)는 상관관계 분석에서 두 변수 간에 선형 관계의 정도를 수량화하는 지표로 수식 (2)와 같다. 변수 2개에 관한 공식은 변수

평균으로부터 각 데이터 점의 거리를 비교하고 이 값을 사용하여 변수 간 관계가 데이터를 통해 그려진 가상선에 얼마나 밀접하게 적합할 수 있는지 알려준다. 상관 계수는 -1.00에서 +1.00사이의 값을 가진다. 변수와의 방향은 양의 상관관계(-)와 음의 상관관계(+)로 나타난다. 상관 계수의 절대값이 높을수록 두 변수 간의 관계가 높다고 할 수 있다. 일반적으로 $\pm 0.4 \sim 0.7$ 의 값을 가지면 상관관계가 있다고 할 수 있다.

$$r = \frac{\sum [(x_i - \bar{x})(y_i - \bar{y})]}{\sqrt{\sum (x_i - \bar{x})^2 * \sum (y_i - \bar{y})^2}} \quad (2)$$

IV. IBC 메시지 전달 시간 측정 및 분석 결과

4.1 실험 환경

본 논문에서 사용된 측정 노드가 설치된 서버는 Intel Xeon Silver 4114 CPU@2.20GHZ 2코어, 5TB HDD, 128GB의 RAM을 사용하며 운영체제는 Ubuntu 18.04 버전이며 하드웨어 최소 요구사항을 충족했다. 측정 노드는 코스모스 허브 클라이언트(Gaia Client) 7.0.2 버전과 오스모시스 클라이언트(Osmosis Client) 8.0.0 버전을 사용하고 Go-Language는 1.18.2 버전을 설치했다^{21,18)}. 측정 노드는 인터넷 접속 속도는 약 69.99Mbps이다.

본 논문은 코스모스 허브에서 오스모시스로 대체 가능 토큰 전송을 실시하고 각 클라이언트에서 수집한 블록체인 간 통신 트랜잭션 데이터를 수집해 블록체인 간 메시지 전달 시간을 측정하는 실험을 수행했다. 한국시간 2022년 6월 1일부터 2022년 6월 2일까지 24시간 동안 86.4초마다 대체 가능 토큰 전송을 발생시켜 총 1,000건의 블록체인 간 거래를 수행했다. 블록체인 간 메시지 전달 시간 데이터의 변수를 줄이기 위해 모든 대체 가능 토큰 전송은 코스모스 허브에서 오스모시스로 1,000uatm을 요금 260uatm을 지불하고 전송했다. ATOM은 코스모스 허브 블록체인의 암호화폐 단위이다. (1ATOM = 1,000,000uatm) 본 논문의 실험 기간에 코스모스 허브와 오스모시스 사이를 중계하는 릴레이어 수는 17개를 유지했다.

4.2 IBC 메시지 전달 시간 측정 결과

본 논문은 블록체인 간 메시지 전달 시간은 코스모스 메인넷에서 실험을 위해 발생시킨 블록체인 간 통신 트랜잭션을 수집하여 측정했다. 1,000건의 대체 가

능 토큰 전송을 발생시키고 이에 대한 블록체인 간 메시지 전송 결과를 수집했다. 대체 가능 토큰 전송 1,000건은 모두 시간 초과(Timeout)로 반환되는 경우 없이 거래를 완료했다.

그림 5는 블록체인 간 메시지 전달 시간을 오름차순으로 나열한 결과이다. 블록체인 간 메시지 전달 시간은 최소 28.176초, 최대 138.662초를 기록하고 평균적으로 55.448초가 걸린다. 중앙값은 52.153초로 평균과 거의 같은 위치에 있어 블록체인 간 메시지 전달 시간 데이터가 균형을 이루고 있음을 확인할 수 있다.

표 2는 블록체인 간 메시지 전달 구간별 시간을 계산한 결과이다. 측정 노드와 코스모스 허브의 시차를 맞추기 위해 Generation_time은 G to T time의 최소값 -13.081을 더했다. T to R time 구간의 분산과 표준편차가 낮은 사실을 고려하여 데이터가 평균을 중심으로 집중되어있다. 메시지 전달 구간별 시간 중 R to A time 구간이 다른 구간보다 약 1.3배인 결과를 보여준다. 이는 T to R time은 평균 13초에 전달될 가능성이 높고 R to A time이 다른 구간보다 낮은 성능

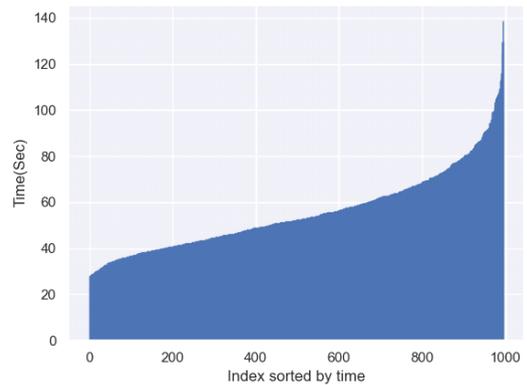


그림 5. 블록체인 간 메시지 전달 시간
Fig. 5. IBC message relay time

표 2. 블록체인 간 메시지 전달 구간별 시간
Table 2. Time for interval of IBC message relaying

Statistical Properties of interval(Sec)	IBC Msg Relay Time	G to T time	T to R time	R to A time
Min	28.17	0.00	3.00	5.00
Max	138.66	79.30	72.00	94.00
Mean	55.44	19.62	13.51	22.31
Median	52.15	16.73	13.00	18.00
Var	295.02	123.48	16.44	172.62
Std	17.17	11.11	4.05	13.13

을 가지고 있음을 의미한다. G to T time에서는 코스모스 허브에서 트랜잭션이 전파되고 블록에 포함되는 과정을 거친다. G to T time은 트랜잭션의 종류만 다른 상태로 블록체인 내 트랜잭션의 처리 과정과 동일하다. G to Time은 코스모스 허브에서의 체인 내 트랜잭션 처리 시간으로 추정한다.

4.3 IBC 메시지 전달 시간 분석 결과

그림 5에서 나타나듯이 실험값은 0 이하의 값을 가질 수 없고 약 800번째 값부터 기울기가 더 큰 쪽으로 증가하는 형태를 보이기 때문에 실험값은 로그 정규 분포를 따른다고 가정한다. 실험값에 자연로그를 취해 히스토그램으로 정렬하고 커널 밀도 추정을 사용하여 관찰 분포를 그림 6과 같이 파란색 실선으로 시각화했다. 검정색 실선은 로그 정규 분포를 나타낸다. 그림 6에서 로그를 취한 메시지 전달 시간과 로그 정규 분포는 시각적으로 유사한 형태를 보인다.

로그를 취한 실험값이 정규분포를 따르는지 증명하기 위하여 Kolmogorov-Smirnov 검정, Shapiro-Wilk 검정, Anderson-Darling 검정을 진행했다. Kolmogorov-Smirnov 검정은 특정 연속변수의 확률 분포가 이론적인 확률분포와 같은지를 알아보기 위한 비모수적 적합도 검정으로 경험적 누적 분포 함수(ECDF; Empirical Cumulative Distribution Function)를 기반으로 한다. Shapiro-Wilk 검정은 표본이 정규 분포를 따르는지 확인하며 일반적으로 작은 표본에 사용된다. Anderson-Darling 검정은 Kolmogorov-Smirnov 검정을 수정한 적합도 검정으로 특정분포의 꼬리(Tail)에 가중치를 두어 수행된다. 본 논문에서는

귀무가설을 해당 분포가 정규분포를 따른다고 설정하고 대립가설을 정규분포를 따르지 않는다고 설정했다.

표 3과 같이 Kolmogorov-Smirnov 검정 결과는 p-value가 0.839로 0.05 이상이므로 귀무가설을 기각할 수 없다. 마찬가지로 Shapiro-Wilk 검정에서도 p-value가 0.073로 0.05 이상이므로 귀무가설을 기각할 수 없다. Anderson-Darling 검정에서는 통계값이 0.362이고 임계값들이 [0.574, 0.653, 0.784, 0.914, 1.088]으로 모두 통계값보다 크므로 귀무가설을 기각할 수 없다. 따라서 실험 결과가 로그 정규 분포를 따른다고 할 수 있다.

블록체인 간 메시지 전달 시간 분포가 로그 정규 분포를 따르기 때문에 표준 정규 분포표를 이용하여 Z값이 1, 2, 3인 경우에 대해 각각 68.3%, 95.4%, 99.7%의 확률로 들어올 수 있는 값의 범위를 표 5에 나타내었다.

전체 블록체인 간 메시지 전달 시간과 구간별 시간의 상관관계 분석을 위한 상관 계수는 표 6과 같이 나타났다. 상관도가 가장 높은 구간은 IBC Acknowledgement 트랜잭션이 중계되는 R to A time 이다.

그림 7과 같이 IBC Msg Relay Time과 R to A time의 상관도를 산점도(Scatter plot)를 사용하여 나

표 3. Kolmogorov-Smirov, Shapiro-Wilk 검정 결과
Table 3. Kolmogorov-Smirov, Shapiro-Wilk test result

Test\Category	statistic	p-value
Kolmogorov-Smirov	0.0194284334	0.8391204478
Shapiro-Wilk	0.9971379041	0.0730665996

표 4. Anderson-Darling 검정 결과
Table 4. Anderson-Darling test result

Category\Test	Anderson-Darling
statistic	0.3620477324
critical_values	[0.574, 0.653, 0.784, 0.914, 1.088]
significance_level	[15. , 10. , 5. , 2.5 , 1.]

표 5. 확률별 예측 블록체인 간 메시지 전달 시간 범위
Table 5. Predicted IBC message relay time range by probability

probability(%)	IBC message relay time range(Sec)
68.3	(28.599, 62.768)
95.4	(19.304, 92.989)
99.7	(13.030, 137.761)

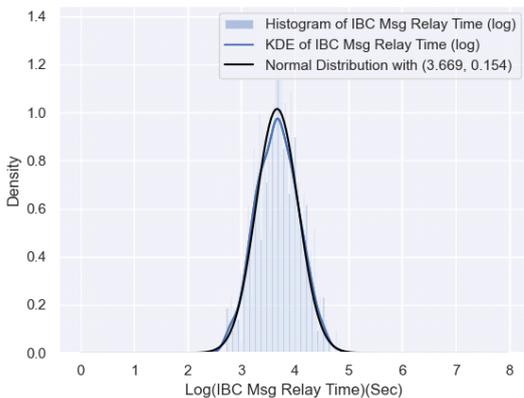


그림 6. Log를 취한 블록체인 간 메시지 전달 시간의 커널 밀도 추정
Fig. 6. Kernel density estimation of IBC message relay time taken logarithm

표 6. 블록체인 간 메시지 전달 시간과 구간 시간 간의 상관 계수
 Table 6. Correlation coefficient between IBC message relay time and interval time

Interval time	Corrlation coefficient
G to T time	0.602792
T to R time	0.214533
R to A time	0.731259

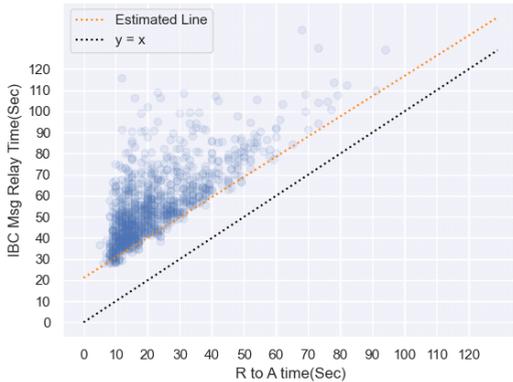


그림 7. 메시지 전달 시간과 R to A time 시간 산점도
 Fig. 7. IBC message relay time and R to A time scatter plot

타냈다. 산점도의 점은 투명도는 0.1로 설정했다. 기울기가 1인 그래프를 잘 따르는 경우 상관도가 높다고 볼 수 있다. 해당 그래프에서 추세선을 그렸을 때 추세선의 기울기는 0.957로 1에 가깝고 상관 계수 또한 0.73으로 0.7 이상이므로 블록체인 간 메시지 전달 시간과 R to A time의 상관도가 높다고 볼 수 있다. 반면 T to R time은 상관 계수가 0.215로 전체 성능에는 영향을 많이 끼치지 않는다.

V. 결론

본 논문에서는 코스모스에서 블록체인 간 메시지 전달 시간 측정 시스템을 제안하고 블록체인 간 메시지 전달 시간을 측정 및 분석하였다. 블록체인 간 메시지 전달 시간은 평균 55.448초이었다. 코스모스에서 블록체인 간 메시지 전달 시간은 코스모스 허브 블록체인 내 메시지 전달 시간보다 약 2.8배 오래 걸린다. 코스모스에서 블록체인 간 메시지 전달 시간은 로그 정규 분포를 따른다. 분포 추정 결과로 로그 정규 분포 양상 및 평균 범위는 성능을 예측하는데 사용할 수 있다. 또한, 전체 블록체인 간 메시지 전달 시간은 코스모스 허브에서 블록체인 간 대체 가능 토큰 거래

를 위한 토큰 잠금 처리와 거래 완료 확인 응답을 수신 과정에 영향을 받는다. 따라서 향후 연구로 코스모스에서 대체 가능 토큰 전송 시간을 단축시키는 방법으로 메시지 전달 시간 지연 원인 분석에 관한 연구, 기존 블록체인 간 프로토콜 향상에 관한 연구에 관한 연구를 수행할 예정이다.

References

- [1] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," *Int. Conf. Business Process Manag. Springer, Cham*, vol. 361, pp. 3-10, Sep. 2019. (https://doi.org/10.1007/978-3-030-30429-4_1)
- [2] S. H. Jeon, "International Standardization Trends and Considerations for Blockchain and Distributed Ledger Technology," *J. KICS*, vol. 46, no. 12, pp. 2333-2339, Dec. 2021. (<https://doi.org/10.7840/kics.2021.46.12.2333>)
- [3] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1-41, Nov. 2021. (<https://doi.org/10.1145/3471140>)
- [4] Monika and R. Bhatia, "Interoperability solutions for blockchain," in *Proc. IEEE ICSTCEE*, pp. 381-385, Bengaluru, India, Oct. 2020. (<https://doi.org/10.1109/ICSTCEE49637.2020.9277054>)
- [5] COSMOS, *What is Cosmos?*, Retrieved Mar., 14, 2022, from <https://v1.cosmos.network/intro>
- [6] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 16440-16455, Jan. 2020. (<https://doi.org/10.1109/ACCESS.2020.2967218>)
- [7] Ethereum, *Ethereum Proof-of-Stake Consensus Specifications*, Retrieved Mar., 14, 2022, from <https://github.com/ethereum/eth2.0-specs>
- [8] J. Kwon and E. Buchman, *Cosmos whitepaper* (2019), Retrieved Mar., 14, 2022, from <https://wikibitimg.fx994.com/attach/2020/12/16>

623142020/WBE16623142020_55300.pdf

[9] COSMOS, *Cosmos Market Capitalization*, Retrieved Mar., 14, 2022, from cosmos.network/ecosystem/tokens

[10] L. Kan, et al., "A multiple blockchains architecture on inter-blockchain communication," in *Proc. IEEE Int. Conf. Software Quality, Reliability and Security Companion (QRS-C)*, pp. 139-145, Lisbon, Portugal, Aug. 2018.
(<https://doi.org/10.1109/QRS-C.2018.00037>)

[11] O. Wu, et al., *Performance Modeling and Evaluation of the Inter-Blockchain Network: A Queuing Approach*(2021), Retrieved May, 10, 2022, from <https://ssrn.com/abstract=4043298>
(<https://dx.doi.org/10.2139/ssrn.4043298>)

[12] Hangzhou Hyperchain Technology Co., *BitXHab*, Retrieved May, 10, 2022, from <https://www.hyperchain.cn/en/products/bitxhub>

[13] C. Goes, "The interblockchain communication protocol: An overview," *arXiv preprint arXiv:2006.15918*, 2020.
(<https://doi.org/10.48550/arXiv.2006.15918>)

[14] COSMOS, *Overview*, Retrieved Mar., 14, 2022, from <https://ibc.cosmos.network/main/ibc/overview.html>

[15] COSMOS, *Relayer*, Retrieved Mar., 14, 2022, from <https://github.com/cosmos/relayer/tree/v1.0.0>

[16] COSMOS, *General Fee Payment*, Retrieved May, 10, 2022, from <https://github.com/cosmos/ibc/tree/master/spec/app/ics-029-fee-payment>

[17] COSMOS, *Validators Overview*, Retrieved May, 10, 2022, from <https://hub.cosmos.network/main/validators/overview.html>

[18] OSMOSIS, *Glossary*, Retrieved May, 10, 2022, from <https://docs.osmosis.zone/overview/terminology.html#consensus>

[19] COSMOS, *Data Structures*, Retrieved May, 10, 2022, from https://github.com/tendermint/tendermint/blob/master/spec/core/data_structure.s.md

[20] seaborn, *seaborn.kdeplot*, Retrieved Mar., 14, 2022, from <http://seaborn.pydata.org/generated/seaborn.kdeplot.html>

[21] COSMOS, *Join the Cosmos Hub Mainnet*, Retrieved Mar., 14, 2022, from <https://hub.cosmos.network/main/hub-tutorials/join-mainnet.html>

김 정 연 (Jungyeon Kim)



2020년 2월 : 계명대학교 경영학과, 컴퓨터공학과 졸업
2022년 8월 : 계명대학교 컴퓨터공학과 석사
<관심분야> 네트워크 관리 및 보안, 블록체인 모니터링 및 분석

[ORCID:0000-0002-5624-4579]

주 흥 택 (Hongtaek Ju)



1989년 8월 : 한국과학기술원 전자계산학과 졸업
1991년 8월 : 포항공과대학교 컴퓨터공학과 석사
2002년 2월 : 포항공과대학교 컴퓨터공학과 박사
2002년 9월~현재 : 계명대학교 컴퓨터공학부 교수
<관심분야> 네트워크 및 시스템 관리, IoT 관리, SDN 네트워크 관리, 블록체인 모니터링 및 분석

[ORCID:0000-0002-8434-485X]