이더리움 블록체인 성능 향상을 위한 기술 동향*

홍상원 ○, 신재철, 이상준

숭실대학교 컴퓨터학부

qpakzk@gmail.com, jcgod413@gmail.com, sangjun@ssu.ac.kr

Technology Trends for Enhancing Ethereum Blockchain Performance

Sangwon Hong ○, Jaecheol Shin, Sangjun Lee

School of Computer Science and Engineering, Soongsil University

요 약

이더리움은 블록체인 상에서 프로그래밍 가능한 스마트 컨트랙트를 실행시킬 수 있는 환경을 제공해주는 탈중앙화된 컴퓨팅 플랫폼이다. 플랫폼이라는 특성 때문에 이더리움 기반 서비스들이 대거 등장하고 있지만 이더리움은 이를 감당하지 못하고 있다. 대표적으로 이더리움 기반 서비스인 Cryptokitties는 출시된 이후, 이전보다 pending 트랜잭션이 6배까지 증가하여 이더리움 네트워크가 마비되는 사태가 발생하였다. 본 논문에서는 낮은 TPS를 이더리움 성능 문제의 대표적인 원인으로 보았고 낮은 TPS 문제를 완화하기 위한 기술들로 라이덴 네트워크, 플라즈마 그리고 샤딩의 기술 동향을 살펴보았다.

1. 서론

블록체인(blockchain)은 신뢰할 수 있는 제 3의 기관이 없이도 P2P(peer-to-peer) 네트워크에 참여하고 있는 노드(node)들이 합의 알고리즘(consensus algorithm)에 의해 안전하게 데이터를 통신하고 위•변조 없이 영구적으로 데이터를 기록할 수 있는 탈중앙화(decentralized)된 컴퓨팅 시스템이다[1].

이더리움(Ethereum)은 Turing complete한 가상 머신인 EVM(Ethereum Virtual Machine)을 내장한 블록체인으로서 프로그래밍 가능한 스마트 컨트랙트(smart contract)를 실행시킬 수 있는 환경을 제공해주는 탈중앙화된 컴퓨팅 플랫폼이다[2].

이더리움 기반 서비스들이 대거 등장하고 있지만[3][4] 이더리움은 이를 감당하지 못하는 성능 문제에 직면해있다. 이더리움 성능이란 이더리움의 트랜잭션(transaction) 처리 속도를 의미한다. 이더리움의 성능 문제를 보여준 대표적인 사례로는 Cryptokitties[5]가 있다. 2017년 11월 28일 Cryptokitties가 출시된 이후로 트랜잭션이 급증하여 이더리움 네트워크가 마비되었다. ETH Gas Station[6]에 따르면 2017년 12월에 Cryptokitties가 이더리움 블록체인 네트워크 트래픽의 10% 이상을 차지했고 Etherscan[7]에 따르면 Cryptokitties 출시 이전보다 pending 트랜잭션이 6배 증가한 결과를 나타냈다[8].

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (2018-0-00209-001)

본 논문에서는 이더리움 성능 문제의 원인을 파악하기 위해 TPS(transactions per second)를 기준으로 이더리움 성능과 기존 전자 결제 시스템 성능을 비교해 보았다. 그리고 이더리움 성능 문제를 해결하기 위해 제안되고 있는 기술들을 살펴보았다.

2. 이더리움 성능 문제의 원인

TPS는 초당 처리하는 트랜잭션 수를 말한다. 기존 전자 결제 시스템인 VISA는 24,000 TPS, Paypal은 193 TPS인 반면 이더리움은 20 TPS에 불과하다[9]. VISA, Paypal의 TPS와 이더리움의 TPS를 비교한 결과 이더리움 성능 문제의 원인은 낮은 TPS 때문이다. 이처럼 이더리움은 TPS가 현저히 낮기 때문에 상용 시스템에 적용하기 어려운 수준이다. 이더리움의 낮은 TPS 문제를 개선하기 위한 기술들로는 라이덴 네트워크[10][11], 플라즈마[12], 샤딩[13]이 제안되었다.

3. 이더리움 성능 향상을 위한 기술 동향

3.1. 라이덴 네트워크(Raiden Newtork)[10][11]

결제 채널(Payment Channel)은 채널이 열려있는 동안 채널의 당사자들이 미리 위탁한 예치금(deposit) 내에서 중간 트랜잭션을 off-chain에서 처리하고 시작 트랜잭션과 최종 트랜잭션만 블록체인에 기록하는 방법이다. 그림 1과 같이 라이덴 네트워크는 결제 채널들을 연결하여 하나의 채널과 같은 효과를 낼 수 있는 기술이다.

라이덴 네트워크를 활용하면 중간 트랜잭션들을 블록체인에 커밋(commit)하지 않기 때문에 이더리움 네트워크에 전파되는 트랜잭션 수가 감소하여 이더리움의 낮은 TPS로 인해

발생하는 문제를 완화할 수 있다.

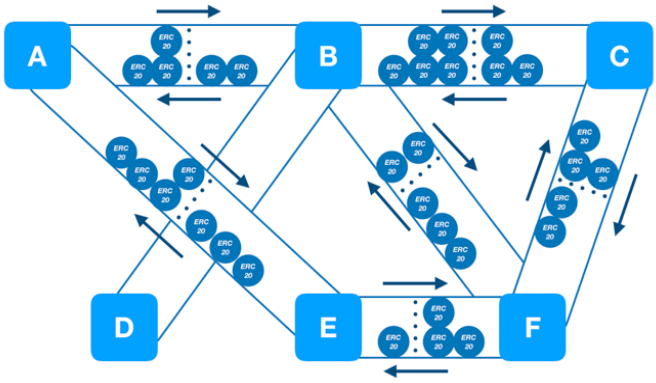

그림 1. 결제 채널들을 연결한 라이덴 네트워크

3.2. 플라즈마(Plasma)[12]

플라즈마는 그림 2와 같이 루트 체인(root chain)인 이더리움 메인 체인 상에 사이드 체인인 플라즈마 체인들이 트리 구조로 연결되어 있는 방식이다. 부모 체인은 자식 체인의 블록 헤더 해시값을 가지고 있기 때문에 루트 체인은 모든 플라즈마 블록체인의 블록 헤더 해시값을 가지고 있는 효과를 얻는다.

플라즈마는 플라즈마 블록체인으로 트랜잭션을 분산시켜 이더리움 블록체인에서 처리해야할 트랜잭션 수를 줄일 수 있기 때문에 이더리움의 낮은 TPS로 인해 발생하는 문제를 완화할 수가 있다.

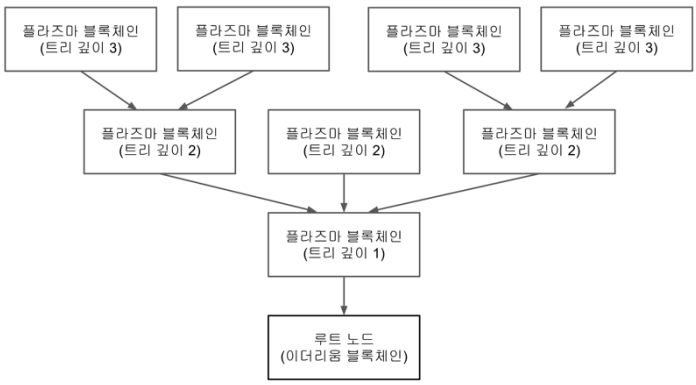

그림 2. 플라즈마 블록체인 트리 구조

3.3. 샤딩(Sharding)[13]

샤딩은 이더리움 네트워크를 샤드(shard) 단위로 나누어서 블록체인의 데이터를 분산 저장하여 한 노드가 검증해야 하는 데이터를 분할하는 방식이다. 그림 3의 (a)와 같이 기존 이더리움에서는 모든 노드가 과거의 모든 블록 데이터를 저장하고 모든 트랜잭션을 처리해야 하기 때문에 성능이 떨어지게 된다. 반면 그림 3의 (b)와 같이 이더리움에 샤딩을 적용한다면 샤드 별로 블록체인 데이터를 분산 저장하고 트랜잭션을 처리하기 때문에 한 노드가 검증해야 하는 데이터 수가 줄어들어 이더리움의 TPS를 향상시킬 수 있다.

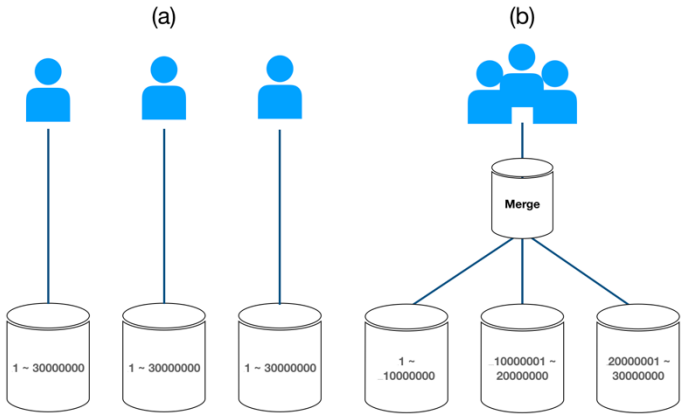

그림 3. 샤딩 이전(a)과 이후(b)의 이더리움 블록체인

4. 결론 및 향후 연구

본 논문에서는 이더리움의 낮은 TPS 문제를 이더리움 성능 문제의 원인으로 파악하였다. 그리고 이 문제를 해결하기 위한 기술로 라이덴 네트워크, 플라즈마, 샤딩을 소개하였다.

각각의 기술들은 이더리움 성능을 향상시킬 수 있는 해결책이지만 세 기술이 함께 적용되었을 때 어떠한 경우에 기술들 간의 충돌 없이 이더리움 성능 향상에 시너지를 높일 수 있을지에 대한 추가적인 연구가 필요하다.

참고 문헌

[1]Michael Crosby, et.al., “BlockChain Technology: Beyond Bitcoin”, Applied Innovation Review, Sutardja Center for Entrepreneurship & Technology, UC Berkeley, 2016.

[2]Vitalik Buterin, “A Next Generation Smart Contract & Decentralized Application Platform,” Ethereum Foundation, 2014.

[3]CoinMarketCap, https://coinmarketcap.com/tokens/

[4]State of the DApps, https://www.stateofthedapps.com/

[5]Cryptokitties, https://www.cryptokitties.co/

[6]ETH Gas Station, https://ethgasstation.info/

[7]Etherscan, https://etherscan.io/chart/pendingtx

[8]http://www.bbc.com/news/technology-42237162

[9]https://www.valuewalk.com/2018/01/transactions-speeds-cryptocurrencies-stack-visa-paypal/

[10]Raiden Network, https://raiden.network/

[11]Joseph Poon, Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”, Paper DRAFT Version 0.5.9.1, https://lightning.network/, 2016.

[12]Joseph Poon, Vitalik Buterin, “Plasma: Scalable Autonomous Smart Contracts”, Ethereum Foudation, 2017.

[13]https://github.com/ethereum/sharding/blob/develop/docs/doc.md