이더리움2.0 세레니티에 대한 고찰

장경배* 최승주* 서화정*†

*한성대학교 IT융합공학과

A Study on Ethereum 2.0 : Serenity

Kyoung-Bae Jang* Seung-Ju Choi* Hwa-Jeong Seo*†

*Division of IT Convergence Engineering, Hansung University.

요 약

2009년 블록체인 기술을 활용한 최초의 암호화폐 비트코인이 등장하고 그 분산화된 시스템 구조의 장점이 부각되면서 블록체인은 4차 산업혁명의 주요 핵심기술로 자리잡았다. 초기에 블록체인은 비트코인과 같이 단순한 금융거래 역할만 수행하였지만, 2015년 2세대 블록체인이라고 불리는 이더리움(Ethereum)이 등장하였다. 이더리움의 핵심은 스마트 컨트랙트(Smart Contract)를 사용한 블록체인 시스템이다. 하지만 스마트 컨트랙트 사용 시 발생하는 느린 트랜잭션 처리속도는 이더리움의 한계로 꼽힌다. 이에 이더리움 개발자인 비탈릭 부테린(Vitalik Buterin)은 한계를 극복하고 세레니티라고 불리는 이더리움2.0을 개발중이라고 밝혔다[1]. 본 논문에서는 이더리움2.0의 주요기술과 기존 이더리움과의 차이점을 비교하고 이더리움의 한계 극복과 진화에 대해 살펴보고자 한다.

I. 서론

블록체인은 데이터를 블록에 담아 체인으로 연결한 형태의 분산형 데이터 베이스이다. 블록체인에서 발생하는 모든 거래는 중앙화된 서버가 아닌 공공장부에 보관되기 때문에 모든 참가자는 거래 기록을 공유하고 비교해볼 수 있다. 공공장부의 거래는 네트워크 참가자 과반수의 합의에 의해 확인되고 일단 입력되면 데이터를 지울 수 없기 때문에 위변조가 불가능하다. 신뢰할 수 없던 온라인 세계에서 분산된 합의 시스템을 구축하고 공공장부에 절대적인 기록을 작성하여 거래가 발생했다는 사실을 명확히 보장할 수 있는 블록체인 기술은 암호화폐에서 완벽하게 사용되며 비트코인은 1세대 블록체인으로 자리 잡았다. 그리고 단순 금융거래로 사용되고 있는 이 블록체인 기술을 다양한 분야에서 사용하기 위해 또 다른 블록체인 이더리움이 등장하였다. 이더리움은 스마트 컨트랙트를 사용한 블록체인 네트워크에서 거래의 일정 조건이 만족되면 자동으로 거래가 성사되는 시스템이다. 거래내용은 코드로 구성되어 있고 이 코드는 블록체인의 한 블록에 존재하게 된다. 그리고 사용자들은 스마트 컨트랙트의 주소에 접근하여 해당 코드를 실행할 수 있다. 거래내용이 담긴 이 코드는 블록체인을 구성하는 블록에 올려지기 때문에 조작이 불가능하다. 따라서 코딩된 내용에 따라 프로그램이 그대로 실행된다. 신뢰의 핵심은 “우리는 코드만 믿는다” 이다. 스마트 컨트랙트를 내세운 이더리움의 등장으로 개발자들은 다양한 서비스를 제공하는 분산화된 어플리케이션(Decentralized Application)을 이더리움 플랫폼 상에서 개발하여 사용할 수 있다. 이렇게 이더리움은 2세대 블록체인으로 자리잡았다. 하지만 많은 유저들이 생겨남에 따라 처리해야 하는 거래 또한 많아지고 하나의 거래를 처리하는데 많은 노드들이 참여해야 하기 때문에 트랜잭션 처리속도는 현저히 느려졌다. 그 결과, 트랜잭션의 처리속

도는 초당 15건 밖에 되지 않고 속도의 한계에 부딪혔다. 온라인 환경에서 블록체인 기술을 도입시킴으로써 신뢰의 문제를 극복하였지만 처리속도는 현저히 떨어졌다. 이는 이더리움만이 아닌 블록체인 공통이 극복해야할 문제이다. 그래서 현재, 속도를 개선하기 위해 블록체인에 다양한 기술들이 도입되고 있다. 이더리움도 기존 이더리움의 구조를 개선하고 몇 가지 새로운 기술을 적용시킴으로써 전송속도는 높이고 비용은 낮춘 세레니티라고 부르는 이더리움2.0 개발을 진행 중이다.

1.1 세레니티 : 이더리움2.0

부테린은 이더리움을 활용하는 유저들이 증가함에 따른 트랜잭션 처리속도의 한계를 이미 예상하였다. 이에 부테린은 느린 속도로 인한 확장성의 문제를 해결하기위해 자신들이 2015년에 제시했던 이더리움 생태계 구축을 위한 4단계 로드맵 중 마지막 4단계인 '세레니티'의 시대가 온다고 밝혔다. 세레니티는 평온이라는 뜻으로 모든 변화 후 평온을 찾는다는 의미를 가진다. 즉 많은 유저들이 이더리움을 사용함에 있어 불편함 없는 완벽한 이더리움 생태계를 구축하는 것이다. 그리하여 2018년 10월 부테린은 이더리움2.0을 세레니티라고 부르자 제안하였다. 이더리움2.0의 핵심인 합의 알고리즘을 PoW(Proof of Work) 방식에서 PoS(Proof of Stake)로의 전환, 샤딩(Sharding) 그리고 새로운 가상머신 ewasm(Ethereum flavored WebAssembly), 이 3가지 주요기술에 대해서 살펴보고자 한다.

1.1.1 합의 알고리즘의 전환

현재 이더리움에서는 생성된 블록의 유효성을 검토하고 블록체인에 반영 여부를 결정하는 합의 알고리즘으로 PoW를 사용하고 있다. PoW 방식은 강한 컴퓨팅 능력을 가진 유저일수록 블록체인에 데이터를 올리는데 있어 많은 기여를 할 수 있다. 기존에는 컴퓨팅 능력이 강한 유저들이 네트워크에 많은 기여를 할 수 있기 때문에 블록체인의 취지에 맞지 않은 중앙화 사례도 몇몇 발생하였다. 하지만 그림 1과 같이 PoS 방식에서는 컴퓨팅 능력에 기반 한 작업이 아닌 유저가 가지고 있는 지분으로 대체한다. 지분을 가지고 있는 각 노드들은 합의하는 블록에 자신들의 지분을 증명함으로써 블록을 네트워크에 올리게 된다.

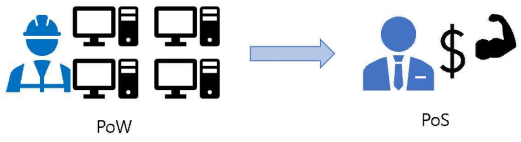


그림 1
Pow에서 Pos로의 전환

PoS에서는 컴퓨팅 파워가 아닌 지분에 따른 정당한 합의과정이 이루어지므로 중앙화를 방지할 수 있다. 51퍼센트의 컴퓨팅 파워를 보유하는 것 보다 51퍼센트의 지분을 보유하는 것이 훨씬 비용이 많이 들기 때문이다. 또한 많은 컴퓨팅 파워를 요구하지 않기 때문에 블록체인을 구성하는데 사용되는 에너지도 최소화 할 수 있다. PoS 방식은 탈중앙화와 에너지 절약의 장점이 부각되지만 한계 또한 존재한다. 바로 합의과정에 있어 별다른 패널티가 존재하지 않는 것이다. 그 결과, 보상을 받기위해 하나의 거래에서 서로 다른 내용이 발생하였을 때 각 블록에 모두 자신의 지분을 증명하는 상황이 발생하는 것이다. 어떤 내용이 진짜인지 거짓인지 상관없이 자신이 합의과정에 참여했다는 이유로 이득을 볼 수 있기 때문이다. 이것이 Nothing at Stake 현상이다. 어느 쪽이든 나는 상관없다는 것이다. 이더리움은 이러한 현상을 보증금 제도를 통해 해결하고자 하였다. 자신이 증명하는 블록에 보증금을 건다. 그런데 만약 블록이 거짓임이 드러나게 되면 보증금을 빼앗는 방식이다. 그 결과, 효율적인 합의 알고리즘인 PoS방식을 사용하는 동시에 유저가 아무데나 자신의 지분을 증명하는 상황 또한 방지할 수 있다. PoS를 성공적으로 도입시키기 위해 부테린과 저스틴 드레이크(Justin Drake)는 비콘체인(Beacon Chain)을 제시하였다[2]. 기존 PoW체인과 상호작용하는 PoS방식을 사용하는 새로운 체인이다. 또한 이더리움은 기존 생태계

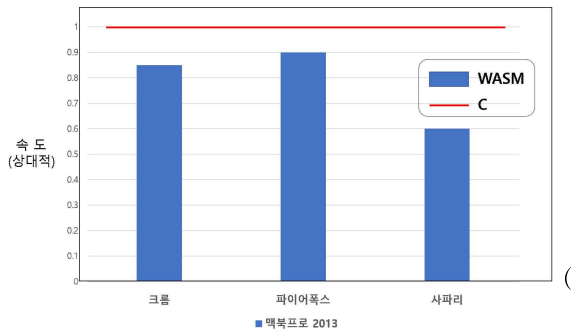
를 파괴하지 않기 위해 PoW에서 PoS로 한 번에 전환하지 않고 조금씩 그 비중을 늘리며 최종적으로는 PoS로 완벽히 전환하는 안정적인 방법[3]을 선택했다.

1.1.2 샤딩

현재 모든 노드들은 블록체인의 모든 트랜잭션을 저장하고 처리한다. 그로인해 네트워크의 규모가 거대해 질수록 거래 수수료와 처리시간이 증가하는 한계가 존재한다. 물론 이 기능은 높은 수준의 보안을 제공하지만 확장성은 현저히 떨어트리고 이더리움 또한 극복해야할 문제이다. 하지만 이 많은 정보들을 나눠서 처리하면 어떨까? 각 트랜잭션을 검증하는 노드들이 충분하다고 가정하면 여전히 안전할 수 있다. 그리하여 적절한 보안성은 유지하되 확장성은 늘리는 솔루션이 바로 샤딩이다. 이미 데이터베이스에서 적용되던 기술이고 이더리움은 확장성 문제를 해결하기 위해 적용시키고 있다. 샤딩이란 우선 블록들로 연결된 체인들을 샤드라는 단위로 분할한다. 그리고 트랜잭션을 나눠진 영역별로 처리한다. 기존 하나의 블록체인이 모든 트랜잭션을 처리하였다면 이제는 나눠진 샤드에서 병렬적으로 처리한다. 그 결과 트랜잭션 처리속도가 나눠진 샤드의 배수만큼 늘어나게 된다. 샤딩은 PoS가 이더리움에 구현된 이후에 도입될 예정이다. 두 기술이 병합된다면 트랜잭션을 처리할 때 지분을 가지고 있는 소수의 검증자 들을 무작위로 선정하여 샤드에 배정하여 검증한다. 그 결과, 빠른 트랜잭션 처리를 여러 곳에서 동시에 진행할 수 있기 때문에 처리량이 매우 증가한다. 하지만 샤딩을 블록체인에 구현 시에는 까다로운 부분이 존재한다. 분할된 샤드에서 트랜잭션을 처리하는 동시에 네트워크의 상태를 업데이트 할 수 있어야 되는 점이다. 이러한 어려움이 있더라도 이더리움2.0에 샤딩이 성공적으로 적용된다면 기존 이더리움에 비해 확연히 달라진 성능을 보여 줄 것이다.

1.1.3 ewasm

기존 이더리움에서는 유저들이 솔리디티(Solidity)언어로 스마트 컨트랙트의 코드를 작성하면 컴파일 되어 바이트 코드가 만들어지고, 이 바이트코드가 EVM(Ehtereum Virtual Machine)이라는 가상 머신에서 실행된다. 현재의 EVM은 초기 사양에서 발전해 왔으며 성능과 유연성 면에서 한계가 존재한다. 또한 여러 하드웨어 플랫폼에서도 속도에 최적화 되어있지 않다. 하지만 이더리움이 세레니티 단계로 진입하기 위해 이더리움2.0 에서는 웹 어셈블리(Web Assembly)를 기반으로 한 새로운 가상머신인 ewasm을 개발 중에 있다. 웹 어셈블리는 C++, Rust등 다양한 언어로 작성된 코드를 가상 머신에 최적화된 저수준 바이트 코드로 컴파일 하여 자바스크립트와 연동되게 만드는 접착 코드(glue code)를 붙여서 대부분 플랫폼 상에서 그림 2를 보면 네이티브에 가까운 속도[4]로 구동 가능하게 한다.



(

그림 2
wasm 속도 비교

앞서 언급한 장점에 기반하여 EVM을 대체할 새로운 가상머신이 바로 ewasm이다. 스마트 컨트랙트 작성시 웹 어셈블리로 컴파일되는 다양한 언어들을 사용할 수 있게 되며 웹 어셈블리에 기반한 빠른 실행속도를 제공한다. 그리고 ewasm에서 사용되는 웹 어셈블리는 기존에 안정적인 커뮤니티가 형성되어 있기 때문에 활용 가능성 또한 높다. 그러나 주의사항이 존재한다. 거래의 신뢰성을 위해 각 노드는 스마트 컨트랙트의 특정 조건에 대하여 언제나 똑같은 결과를 내놓아야 한다. 그러므로 이에 반하는 비 결정적인 웹 어셈블리의 기능은 ewasm 구현 시 모두 제외해야 한다. ewasm은 현재 진행중이며, 성공적으로 구현된다면 세레니티의 종

착에 한걸음 나아가게 될 것이다.

1.2 이더리움2.0 : 세레니티 로드맵

이더리움은 자신들의 로드맵 마지막 단계인 세레니티에 진입하기 위해 이더리움 2.0 개발 0단계부터 6단계로 이루어진 로드맵을 발표하였다[5]. 샤딩없는 비콘체인을 도입함으로써 PoS로의 전환을 0단계로 지정하여 2019년 말까지 완료하겠다고 밝혔다. 1단계부터는 EVM을 활용하지 않는 기본 샤드 체인을 도입하고 2단계에는 ewasm을 기반으로한 가상머신을 도입할 예정이다. 2020년에는 1단계, 2021년에는 2단계를 수행할 것으로 예상하였다. 3단계 이후부터는 샤딩을 중심으로 PoS, ewsam의 완벽한 융합과 보완을 수행한다. 그리고 3단계 이후는 구체적인 시기를 현재 예상하기 어렵다고 밝혔다. 이더리움은 자신들의 최종목표인 세리니티에 종착하기 위해 이더리움2.0 개발에 전력을 다하고 있다. 부테린은 이더리움2.0은 기존 이더리움보다 최대 1,000배 빠른 처리속도를 보여줄 것이며 일상생활에서 스마트 컨트랙트를 아무 불편사항 없이 사용하는 것이 목표라고 말했다. 그 결과, 신용카드와 같은 실시간 서비스도 제공할 수 있게 된다. 이처럼 이더리움은 한계를 극복하는 동시에 진화하는 과정에 있다.

II. 결론

본 논문에서는 2세대 블록체인이라고 불리는 이더리움의 한계점에 대해 살펴보고 그 한계를 극복하고 진화하기위한 프로젝트 이더리움2.0 세레니티에 대한 핵심 기술 3가지를 분석해 보았다. 첫 번째, 합의알고리즘 PoW에서 PoS로 전환하였다. 이는 강한 컴퓨팅 능력을 가진 유저의 중앙화를 방지하며 보안성을 강화시켰다. 그리고 검증과정에서 많은 컴퓨팅 능력이 요구되지 않기 때문에 처리속도 또한 증가하였다. 두 번째, 샤딩 기술을 이더리움에 적용시킴으로써, 하나의 블록체인이 아닌 샤드 단위로 분할된 체인에서 발생되는 각 트랜잭션들을 병렬로 처리한다. 기존에 구성된 대규모 네트워크를 유지하며 분할시키는 어려움은 존재한다. 하지만 보안성을 지키는 선에서 샤딩과 이더리움이 성공적으로 융합된다면 나눠진 샤드의 배수만큼 성능이 증가하는 발전을 이룰 것이다. 마지막으로 웹 어셈블리의 다양한 언어를 사용할 수 있는 유연성과 빠른 실행속도를 이용하여 새로운 가상머신을 제공하고자 한다. 초창기 작품인 EVM은 다양한 기능을 제공하지만 성능적으로 뛰어나진 않다고 말했다. 그러나 이더리움2.0에 사용하기위한 ewasm은 많은 비용을 투자하고 전문 인력을 투입하고 있음을 밝혔다. 이렇게 이더리움 개발자들은 기존 구조를 개편하고 새로운 기술들을 적용시킴으로써 한계점을 극복하고 보안 또한 강화시키고자 한다. 세레니티 즉, 이더리움 생태계의 평온이라는 시기를 준비하고 있으며 우리는 블록체인의 발전으로 이어지는 이 이더리움2.0에 대하여 관심을 갖고 연구해야 된다고 생각하는 바이다.

[참고문헌]

[1] Ethereum Foundation, Latest on Ethereum by Vitalik Buterin (Devcon4) Dec, 2018 URL https://www.youtube.com/watch?v=kCVpDrlVesA&feature=youtu.be

[2] Ethereum Foundation, 4. Beacon Casper chain by Vitalik Buterin and Justin Drake (Ethereum Foundation) July, 2018 URL https://www.youtube.com/watch?v=GAywmwGToUI

[3] Vitalik Buterin, Virgil Griffith, Casper the Friendly Finality Gadget, Jan, 2019.

[4] David Herrera, Hanfeng Chen, Erick Lavoie and Laurie Hendren, WebAssembly and JavaScript Challenge: Numerical program performance using modern browser technologies and devices, March, 2018.

[5] James Ray, Sharding-roadmp, March, 2019. URL https://github.com/ethereum/wiki/wiki/Sharding-roadmap