효율적인 이더리움 스마트 콘트랙트에 관한 연구

김대한*, 최광훈**, 김강석*, 김재훈*
*아주대학교 사이버보안학과
**아주대학교 컴퓨터공학과
e-mail:kimchdh@ajou.ac.kr

A Study on Efficient Ethereum Smart Contract

Kim Dae Han*, Choi KwangHoon**, Kim Kangseok*, Kim Jai-Hoon*
*Dept. of Cyber Security, Ajou University
**Graduate School of Computer Engineering, Ajou University

요 약

본 논문은 이더리움 네트워크에 트랜잭션 발행 시 발생하는 부하(비용)을 줄이기 위해 스마트 콘트랙트를 효율적으로 구성하는 방식에 대해 연구한다. 이더리움 네트워크에 부하를 줄이기 위해서는 발생되는 트랜잭션의 양도 중요하지만 발생하는 트랜잭션의 크기가 작은 효율적인 스마트 콘트랙트 배포와 간단한 구조를 가진 함수를 호출하는 것도 중요하다. 그렇기 때문에 이더리움 스마트 콘트랙트의 구조에 따른 성능 평가를 진행하여 최적의 성능을 보이는 스마트 컨트랙트 구성 방법에 대해 연구를 진행한다. 최적의 성능은 동일한 데이터를 넣을 수 있는 상황에 대해 평가하며 평가 방식은 데이터를 블록체인에 저장 할 때 발생하는 가스 비용 비교를 통해 결정한다. 스마트 콘트랙트의 성능 평가 항목으로는 콘트랙트 배포와 함수 호출시 데이터의 구조, 개수에 따른 가스 비용의 비교 분석을 통해 최저의 가스 비용으로 함수 호출 및 스마트 콘트랙트 생성 및 배포 시키는 구조에 대해 연구를 진행한다.

1. 서론

본 논문에서는 최적의 이더리움 기반의 스마트 콘트랙트를 구현하는 방법에 대하여 연구를 진행한다. 이더리움 기반의 스마트 콘트랙트는 블록체인 기술을 이용한다. 블록체인은 기존의 중앙 집권화 된 서버 방식의 시스템이 아니라 블록화 된 체인을 활용하여 탈중앙화 시스템을 의미한다. 탈중앙화 공간에 데이터를 저장하기 위해 발생하는 트랜잭션이 발생하며 과도한 트랜잭션 발생 시 TPS (Transaction per second)가 낮아져 네트워크의 속도가 느려지며 트랜잭션의 대기가 발생하게 된다. 대기가 발생한 트랜잭션은 영원히 성공되지 않을 수 있다. 이를 방지하기 위해서는 이더리움 블록체인에 배포하는 스마트 콘트랙트를 효율적으로 구성해야 한다. 또한 블록체인을 활용하여 탈중앙화 된 시스템을 구성할 때 고려해야할 부분 중 하나는 블록체인에 데이터를 넣는 비용이다. 이더리움에 스마트 콘트랙트를 배포하거나 데이터를 저장 시 가스라는 비용이 발생된다. 가스 비용은 저장하는 데이터에 자료형과 개수 및 계산 구조에 따라 다르며 이 가스 비용을 줄이는 것이 블록체인을 이용하는 사용자에게 중요하다. 그래서 본 논문에서는 블록체인 기반 DApp(Decentralized Application) 배포 시 스마트 콘트랙트를 구성하는 최적의 방식에 대해 연구한다. 최적의 스마트 콘트랙트는 가스 비용뿐만 아니라 트랜잭션의 부하를 적게 발생시켜 비용 적 측면뿐만 아니라 이더리움 네트워크가 정상적으로 작동하도록 도움을 줄 수 있다. 본 논문에서는 블록체인에 데이터 저장 시 동일한 데이터를 최저의 가스 비용으로 저장하는 방식에 대한 성능 평가를 진행한다. 성능 평가는 트랜잭션 발생 시 가스 비용 비교를 통해 이루어지며 가스 비용이 적은 트랜잭션이 우수한 성능을 나타낸다고 판단된다.

2. 관련 연구

스마트 콘트랙트란 1994년 닉 자보에 의해 처음 제안되었다. 2013년에 배포된 이더리움에서 솔리디티 언어를 사용하여 스마트 콘트랙트를 개발할 수 있다. 스마트 콘트랙트에서 개발자가 원하는 모든 종류의 거래를 처리 할 수 있으며 이 거래들은 이더리움 네트워크에서 무결성이 보장된다.

이더리움 Rinkeby는 합의 알고리즘으로 POA(Proof- of-Authority)를 사용한다. POA는 사전에 승인받은 권한을 이용하여 거래에 대한 유효성을 검사하는 합의 알고리즘이다. POA 합의 알고리즘은 다른 Test Net 과 Main Net 에서 사용하는 POW(Proof-of-Work), POS(Proof-of-Stake)에 비해 더 빠르게 합의를 이루어 낼 수 있어 트랜잭션 합의 시간을 줄일 수 있다[1].

이더리움의 처리 속도는 20TPS정도로 일반적인 데이터 양을 처리하기에는 어려움을 겪을 수 있는 처리 양이다. 이더리움에서 가장 대표적인 Dapp인 CryptoKitty가 배포되었을 때 CryptoKitty에서 발생하는 트랜잭션을 감당하지 못하고 이더리움 네트워크에 심각한 성능 저하를 일으켜 트랜잭션이 성공되지 못하고 대기되는 트랜잭션이 증가하였다. 이더리움은 낮은 TPS를 나타내기 때문에 이

더리움 네트워크를 나누어 성능을 향상 시키는 방식이 연구되고 있다[2].

이더리움의 트랜잭션의 TPS는 이더리움 네트워크가 혼잡해 질 때 더욱 성능이 저하된다. 네트워크가 배포되는 트랜잭션은 트랜잭션의 내용이 복잡해질수록 더욱 네트워크에 부하를 주었다. 간단하게 트랜잭션을 발생시킬 수 있다면 TPS가 급격하게 떨어지는 것을 줄일 수 있다[3].

또한 연산을 수행하는 과정같이 스마트 콘트랙트의 함수 호출에서 내부 함수가 복잡해지면 오버헤드가 증가한다. 오버헤드의 증가로 인해 이더리움 네트워크의 속도가 저하되어 이더리움 네트워크 사용이 불가능할 가능성이 있다. 암호화 같이 복잡한 계산은 블록체인 내부가 아닌 외부에서 진행 후 암호화 된 데이터를 넣는 것이 추천된다[3].

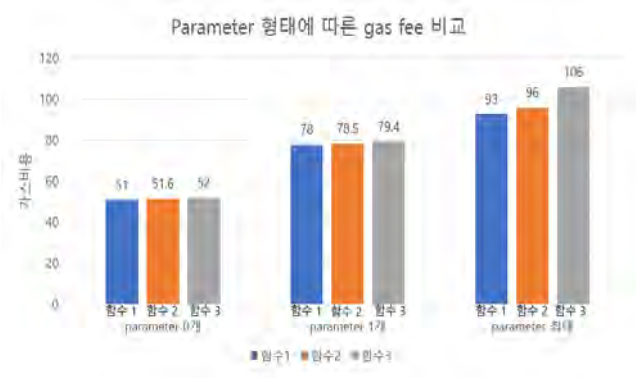
3. 본문

본 논문에서는 스마트 콘트랙트의 효율성을 비교하는 방식으로 2가지 방식을 취한다. 첫 번째로 스마트 콘트랙트의 함수 호출의 매개변수의 데이터 구조 및 개수에 따른 배포시의 가스 비용의의 최댓값과 추정 값을 이용하여 가장 적은 가스 비용을 나타내는 스마트 콘트랙트 개발 방법에 대해 테스트를 진행한다.

가스 비용 확인을 위한 테스트를 위한 환경은 Geth 1.8.15와 Mist 0.11.1을 사용하여 진행한다. 그리고 Main Net에서 테스트를 진행하면 더욱 더 정확한 결과가 나올 수 있지만 실제 돈을 사용하여 배포해야 한다는 점을 고려하여 테스트넷인 Rinkeby를 사용하여 테스트를 진행한다. Rinkeby는 합의 알고리즘으로 POA를 사용한다.

첫 번째로 함수 실행 시 함수 내부 및 매개변수에 따른 자료의 구조 및 개수에 따른 가스 비용을 측정한다. 이를 측정함으로써 똑같은 데이터를 저장할 수 있다면 어떤 방식으로 저장하는 것이 가장 효율적인 스마트 콘트랙트 구성이 되는지에 대한 방법을 연구한다.

트랜잭션 완료의 발생 시간은 현재 이더리움 네트워크의 상황에 따라서 달라질 수 있기 때문에 정확한 비교 분석이 가능한 가스 비용을 고려한다.



<표 1>

<표1>은 함수의 종류 3개에 따라서 가스 비용의 소모 정도의 테스트를 진행한다. 함수 1은 매개 변수로 address + string , 함수2 는 address + uint8 + string 그리고 함수 3은 address + uint128 +string을 인자로 받는다.

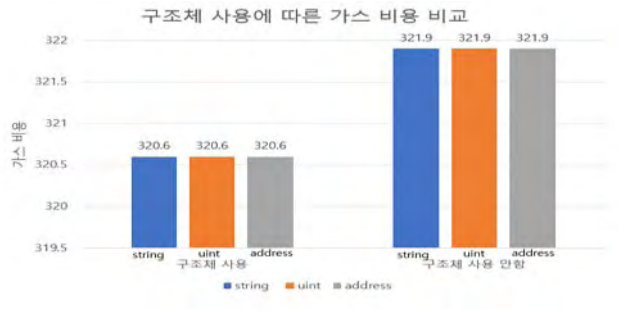
<표1>에서 확인해 보면 함수 1,2,3 모두 인자의 내용이 증가할수록 가스 수수료(gas fee)가 증가함을 확인할 수 있다. 함수를 배포할 때 미리 각 자료 형마다 256 비트의 공간을 확보해 놓았지만 여기에 확보된 공간에 데이터가 추가될 때 가스 비용이 다르게 증가하였다. 각 문자 1개별로 저장 공간은 숫자 8비트, 영어 16비트, 한글 40비트의 공간을 소모한다.

<표1>의 함수 2 와 함수 3은 uint의 크기만 다르다. 구조체의 경우를 제외하고 uint 뒤의 숫자가 다르더라도 할당하는 공간은 256 비트로 동일한 크기를 할당하지만 실제로 데이터 삽입이 이루어졌을 때는 각각 90과 106의 기스 수수료가 소모되었다. 이를 통해 미리 할당되어지는 공간은 동일하지만 자료형에 따라서 다르게 가스 비용이 소모 되는 것을 확인할 수 있다.

결국에는 모든 데이터를 string으로 넣어 저장하는 경우가 가장 적은 가스 수수료를 사용하였다. 데이터를 string으로 저장하면 사전에 string 데이터의 저장 순서 및 형태가 정의 되어있어야 하며 이를 파싱을 진행해야 원하는 데이터를 추출해야한다는 단점이 존재한다. 하지만 블록체인 네트워크에서 데이터를 읽는 과정은 가스 비용이 소모되지 않는다. string으로 모든 데이터를 저장하고 규칙대로 파싱을 진행할 수 있다면 가장 적은 가스 비용으로 동일한 데이터를 저장할 수 있다.

string으로 데이터를 저장한다면 바이트 단위로 string을 저장하면 저장 공간을 더 줄일 수 있을 것이라 생각하며 테스트를 진행해보았지만 바이트 단위로 string을 저장할 때 a, b, c, d, e, f 까지만 저장이 진행되고 그 이외의 영문자는 저장이 진행되지 않았다. 즉 address(계정 주소)와 같이 고정적인 형식을 필요로 하거나 스마트 콘트랙트 내에서 반환 값으로 데이터를 사용하는 경우가 아니라면 string형태로 저장을 진행한 후에 클라이언트에서 파싱을 진행하는 것이 효율적 스마트 콘트랙트 구성이다.

두 번째는 변수를 선언할 때 구조체를 사용할 경우와 구조체를 사용하지 않고 선언을 할 경우를 구분하여 가스 수수료 절약정도 테스트를 진행하였다.



<표 2>

<표2>는 스마트 콘트랙트를 배포 시 address, uint,

string을 각각 4개씩 선언하여 배포 시 소요되는 가스를 표로 나타내었다.

<표2>에서 보면 가스 차이가 1정도가 차이 났고 이 차이가 크지 않다. 하지만 이 차이는 4개의 변수만은 구조체로 선언 했을 때의 차이이므로 스마트 콘트랙트에 선언되는 모든 변수를 각 콘트랙트 별로 선언한다면 더 많은 더 많은 콘트랙트 배포 비용을 줄 일 수 있다.

자료 형에 따라서 동일한 가스 비용을 나타내는 이유는 자료의 구조에 따라서 다른 공간을 확보하는 것이 아니라 256 비트를 무조건 확보하며 256 비트 이상의 공간을 확보할 때는 256 비트 단위로 추가하는 방식으로 저장 공간을 확보한다.

4. 결론

본 논문에서는 스마트 콘트랙트의 데이터 자료 구조에 따른 가스 소모 비용을 비교 분석하여 최적의 스마트 콘트랙트를 구성하는 방법에 대해 연구를 진행하였다. 스마트 콘트랙트를 배포할 때는 각 콘트랙트 별로 원하는 자료 형을 구조체 내부에 선언하여 가스 비용을 줄일 수 있다. 또한 매개변수를 string으로 입력받아 데이터를 저장하고 읽어 올 때 반환 값을 parsing을 진행하면 가스 비용을 절약하여 블록체인을 이용할 수 있다.

가스 비용을 적게 사용하는 스마트 콘트랙트를 사용하는 것은 개인의 가스 비용을 절약할 수 있다. 또한 이더리움 네트워크 전체에 부하를 줄일 수 있어 전체 네트워크에 트랜잭션이 대기되는 비율을 줄일 수 있다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2018R1D1A1B07040573).

참 고 문 헌

[1] 임종철, 유현경, 곽지영, 김선미 “블록체인과 합의 알고리즘”, 2018 Electronics and Telecommunications Trends, 33권, 1호, pp.44-56

[2] 홍상원, 신재철, 이상준 “이더리움 블록체인 성능 향상을 위한 기술 동향”, 2018년 한국컴퓨터종합학술대회 논문집, pp.1943-1944.

[3] 송제호, 김상혁, 박성용 “이더리움 콘트랙트 성능 저하 현상 실험 및 분석”, 2018 정보과학회 컴퓨팅의 실제논문지, pp.381-384