속성기반 암호기법을 활용한 블록체인 서비스 유형 연구1)

류혜원*, 김형종*
*서울여자대학교 정보보호학과
bella5065@swu.ac.kr

Access controlled Blockchain services based on Attribute-Based Encryption

Hyewon Ryu*, Hyung-Jong Kim*
*Dept of Information Security, Seoul Women's University

요 약

블록체인은 P2P 네트워크로 탈중앙화된 신뢰성 기반 데이터 공유 서비스를 제공한다. 다양한 블록체인 플랫폼 중에서도 이더리움은 가장 상용화된 플랫폼으로 비트코인의 한계를 극복하면서도 스마트 컨트랙트를 통한 신뢰성 있는 서비스를 제공한다. 본 논문에서는 블록체인 기반 분산 컴퓨팅 플랫폼인 이더리움에 속성기반 암호기법을 적용하여 네트워크 내의 블록체인에 대한 제한적 접근 서비스를 제안하고 이를 통해 블록체인 서비스 유형을 제시한다.

1. 서론

블록체인은 4차 산업혁명을 이끄는 핵심 기술 중 하나이며 대표적인 서비스로는 비트코인과 이더리움이 있다. 이더리움은 스마트 컨트랙트를 통해 거래가 이뤄지며 탈중앙화된 네트워크로 구성되어 참여자 노드 간의 합의 알고리즘을 통해 거래와 검증이 이루어진다. 이더리움은 코인을 송금하는 것이 주목적인 비트코인을 확장 시켜 블록체인 기술의 활용성을 높여주었다. 네트워크에 참여하는 노드는 모든 거래 내역을 볼 수 있으며, 거래에 직접 참여할 수도 있다. 본 논문에서는 속성기반 암호기법을 이더리움 네트워크에 적용하여 모든 참여자 노드의 거래에는 관여하지 않지만, 거래 정보 열람을 제한할 수 있는 이더리움 네트워크 플랫폼의 프로토콜을 제안한다. 이를 통해 제한적 접근 서비스 기반의 비즈니스 모델을 제시한다.

2. 배경 지식 및 관련 연구

2.1 블록체인[1][2]

블록체인은 2008년 '사토시 나카모토'라는 익명의 인물이 연구를 공개함에 따라 알려졌다. P2P 네트워크, 암호화, 분산 장부, 분산 합의와 같은 4가지 기반 기술로 구성되어 상호보완적인 관계를 통해 탈중앙화, 데이터의 무결성 유지 및 보장이라는 특징을 나타낸다. 참여자들이 데이터를 저장하고 검증하므로 임의의 조작이 어렵다.

2.2 이더리움[3][4][5]

이더리움은 2015년 개발된 스마트 컨트랙트 기능을 구현한 블록체인 기반 분산 컴퓨팅 플랫폼으로 이더(Ether)라는 암호 화폐 기능을 제공한다. 비트코인의 주목적이 가상화폐 송금이라면 이더리움은 더 나아가 스마트 컨트랙트를 이용해 자유롭게 개발할 수 있는 것이 특징이다. 스마트 컨트랙트는 디지털 방식으로 계약의 협상, 체결 그리고 검증하는 것으로, 정해진 계약 조건이 성립하면 네트워크 안에서 자동으로 실행된다. 거래와 관련된 모든 정보는 블록체인에 저장되며 이를 통해 신뢰성 있는 서비스를 제공한다.

2.3 속성기반 암호기법[6]

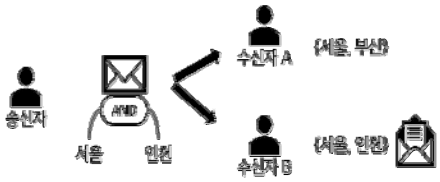
속성기반 암호기법은 ID 기반 암호방식에서 확장된 개념으로 속성집합과 접근구조를 바탕으로 암복호화를 실시한다. 속성기반 암호기법은 사용자의 ID뿐만 아니라 소속, 직무, 나이 등과 같은 속성집합을 사용하여 접근구조를 지정하고 이것을 암복호화 시 사용한다. 그래서 속성기반 암호기술을 사용한 경우 속성에 대한 중복의 권한을 부여할 수 있다.

2.3.1 CP-ABE(Ciphertext-Policy)[6]

CP-ABE는 송신자가 데이터를 암호화할 때 접근구조를 지정한다. 지정된 접근구조에 부합하는 속성집합이

1) 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2019-2018-0-01799)

있는 수신자만 데이터를 복호화할 수 있다.



(그림 1) CP-ABE

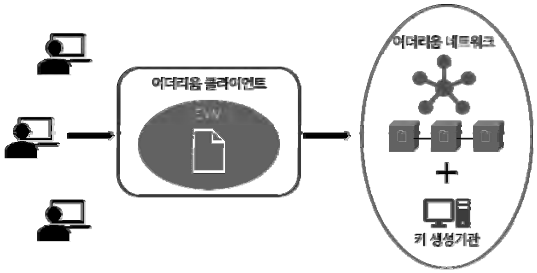
2.3.2 속성기반 암호기법 관련 연구

M2M 통신 환경에서 속성기반 암호기술을 활용한 연구에서는 M2M Device의 식별, 인증 프로토콜을 설계하여 안전한 데이터를 송수신하는 방안을 제안하였다[7]. 속성기반 암호방식을 이용한 안전한 메신저 시스템에서는 이기종 디바이스 간의 안전한 암호화 키 동기화와 기기 분실과 변경에 따라 메시지 동기화를 가능하게 하는 것을 제안하였다[8]. 접근제어가 가능한 다중기관 속성기반 암호전송 알고리즘 연구에서는 속성기반 암호기술과 암호전송 알고리즘의 결합을 통해 군의 통신, 군사위성에 적용하는 것에 대해 제시하였다[9].

3. 연구내용

3.1 이더리움 시스템 가정

이더리움 플랫폼에서 사용자가 노드에 접속하여 스마트 컨트랙트를 작성하면, 배포되고 컴파일 후 EVM이 실행할 수 있는 바이트 코드가 출력된다. 이 과정을 거쳐 바이트 코드가 포함된 트랜잭션이 발생하면 블록에 포함되고 마이너 노드에 의해 채굴되어 블록체인에 연결되고 스마트 컨트랙트가 실행된다[10].



(그림 2) 이더리움 네트워크 가정

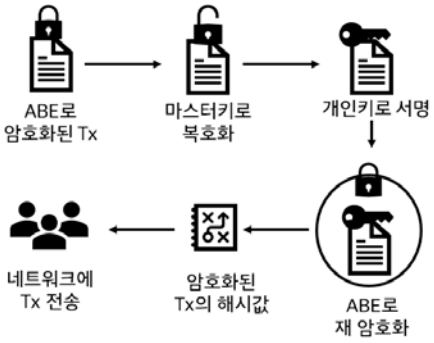
본 논문에서는 속성기반 암호기법 중에서 CP-ABE 방식을 사용하여 이더리움에 적용한다. 이를 실현하기 위해서 (그림 2)와 같이 속성집합과 접근구조를 자동으로 설정해주고 키 관리를 담당할 별도의 키 생성기관이 필요하다.

3.2 트랜잭션 암복호화

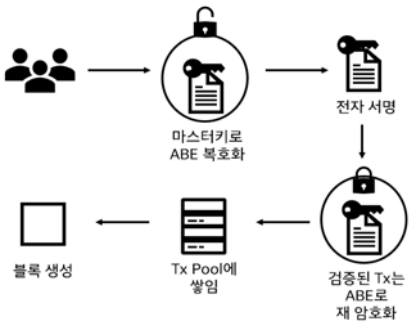
트랜잭션이 발생하면 시스템은 속성기반 암호기법을 바탕으로 암호화된 트랜잭션을 생성한다. 트랜잭션은 블록 헤더에 배열 형태의 해시값으로 저장된다. 거래 내역을 확인하기 위해 해당 트랜잭션이 있는 블록을 찾은 후 헤더에 저장된 트랜잭션의 해시값과 실제 트랜잭션이 저장된 트리 노드의 루트 노드 해시값을 알아야 한다. 이러한 정보를 통해 알게 된 트랜잭션에는 거래 수수료와 송신자, 수신자의 계정과 같은 정보가 있으며 디지털 서명에 사용되는 중요한 정보도 저장되어 있다. 그러므로 트랜잭션을 암호화한다면 트랜잭션 검증과정을 위해 마스터키로 복호화해야 한다.

3.3 트랜잭션 발생 시 동작 원리

노드 A로부터 노드 B에게 10이더(Ether)가 전송되는 스마트 컨트랙트가 생성되었다고 가정한다. (그림 3)과 같이 스마트 컨트랙트에 의해 생성된 트랜잭션은 시스템에 의해 자동으로 암호화되어있다. 이것을 블록에 포함하기 위해 네트워크 다른 노드에게 해당 트랜잭션에 대한 검증을 받아야 한다. 검증을 받기 위해 송신자인 노드 A는 키 생성기관으로부터 받은 마스터키로 트랜잭션을 복호화하고 자신의 개인 키로 서명한다. 그 후 시스템이 트랜잭션을 다시 암호화한다. 암호화된 트랜잭션이 이더리움 네트워크에 전송되고 이것을 검증하기 위해 다른 노드는 (그림 4)와 같이 키 생성기관이 제공한 마스터키로 해당 트랜잭션을 복호화한다. 복호화된 트랜잭션의 내용을 확인하여 송신자의 공개키를 얻고 트랜잭션을 검증한다. 최종적으로 검증된 트랜잭션은 시스템에 의해서 속성기반 암호기법으로 다시 암호화되고 트랜잭션 임시 풀에 쌓이게 된다. 마이너 노드에 의해 블록이 채굴되면 암호화된 트랜잭션의 해시값이 들어간 블록이 생성되어 블록체인에 연결된다.



(그림 3) 트랜잭션 프로토콜-송신자

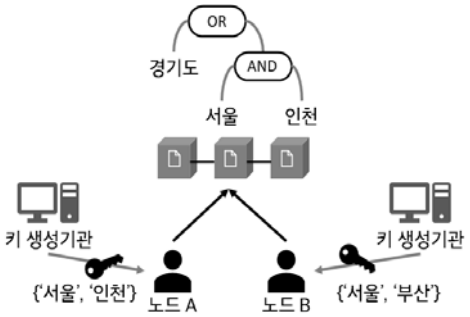


(그림 4) 트랜잭션 프로토콜-수신자

3.4 거래 내역에 대한 제한적 접근

거래 내역을 확인하고 싶은 노드는 트랜잭션을 복호화해야 한다. 트랜잭션을 복호화할 수 있는 개인 키는 별

도의 키 생성기관에 의해 생성되고 관리된다. 트랜잭션을 암호화할 때 접근구조에 부합하는 속성집합을 바탕으로 생성된 개인 키의 경우에만 복호화할 수 있다. 거래 내역을 보기 위해 대가를 지불한 노드에만 복호화가 가능한 개인 키를 전달하고, 그렇지 않은 노드에는 복호화 불가능한 속성집합으로부터 생성된 개인 키가 전달된다. 누구나 스마트 컨트랙트를 생성하거나 거래를 진행할 수 있지만, 내역을 보기 위해서는 키 생성기관으로부터 받은 개인 키로 복호화해야 한다. 그러므로 거래 내역에 대한 제한적 접근 서비스를 구현할 수 있게 된다.



(그림 5) 거래 내역에 대한 제한적 접근

(그림 5)의 경우, 노드 A는 {'서울', '인천'}이라는 속성집합으로부터 생성된 개인 키를 받았지만, 노드 B는 {'서울', '부산'}이라는 속성집합으로부터 생성된 개인 키를 키 생성기관으로부터 받았다. 트랜잭션 암호화 시 결정된 접근구조는 {경기도∨{서울∧인천}}이므로 노드 A는 트랜잭션을 복호화하여 거래 내역을 확인할 수 있게 된다. 반면, 노드 B는 확인할 수 없다.

3.5 블록체인 서비스 유형 제시

제한적 접근 서비스의 1:1, 1:다, 다:다 모델을 제시할 수 있다. 1:1 모델의 경우, 희소성이 있는 재화나 기업과 기업 간의 이뤄지는 거래의 정확하고 신뢰성 있는 정보 제공을 위한 네트워크를 제시할 수 있다. 다이아몬드나 고가의 보석 제작, 유통, 거래 과정을 판매자가 블록체인에 저장하면 해당 보석을 구매하고자 하는 구매자는 조금의 대가만 지불하면 그 보석에 대한 믿을 수 있는 정보를 얻을 수 있기에 이를 통해 신뢰성 있는 거래를 할 수 있게 된다.

1:다 모델의 경우, 부동산 매물 정보, 중고차 유통과정 등과 같이 허위 매물 거래 문제를 방지하기 위해 판매자가 상품의 유통과정이나 정확한 정보를 블록체인에 저장하면 이를 확인하고 싶은 구매자들은 대가를 지불하고 해당 블록을 복호화하여 정보를 확인할 수 있게 된다. 이처럼, 정확한 매물 정보를 제공함으로써 신뢰성 있는 매매를 보장할 수 있다.

다:다 모델의 경우, 연구나 교육 자료를 이용해 누구나 지식을 제공할 수 있고 대가를 지불하는 이용자라면 누구나 지식을 얻을 수 있는 것과 같이 네트워크를 구성한다면 정보 열람 제한적 모델을 구축할 수 있다.

4. 결론

본 논문에서는 스마트 컨트랙트를 구현한 블록체인 기반 분산형 플랫폼인 이더리움 네트워크에 속성기반 암호기법을 적용하여 트랜잭션을 암복호화하는 프로토콜을 제안하였다. 이를 통해 접근구조에 일치하는 속성집합의 개인 키를 지닌 노드만 거래 내역에 접근할 수 있게 하였고, 그렇지 않은 개인 키를 지닌 노드는 블록에 접근하더라도 트랜잭션의 내용을 볼 수 없게 제한하였다.

연구내용을 바탕으로 이더리움 기반 블록에 대한 제한적 접근 서비스를 제공하는 서비스 유형 모델을 제시하였다. 또한, 속성기반 암호기술을 이더리움에 적용함에 따라 다른 암호기술도 이더리움에 적용할 수 있다는 가능성을 나타냈다.

참고문헌

[1] 이동영, 박지우, 이준하, 이상록, 박수용, "블록체인 핵심 기술과 국내외 동향". 정보과학회지, 35(6), 22-28, 2017.

[2] 서무경, 정이상, "4차 산업혁명시대의 블록체인 활용화에 관한 연구". 예술인문사회융합멀티미디어논문지, 287-296, 2018.

[3] 김휘경, 최용락, "블록체인 기반 이더리움 마이닝 관리 시스템". 한국IT서비스학회 학술대회 논문집, 230-233, 2016.

[4] 김은열, 김종원, 장현지, 신주범, "이더리움 스마트 계약을 활용한 블록체인 기반 설문조사 플랫폼 구현". 한국정보과학회 학술발표논문집, 2182-2184, 2018.

[5] 정한재, "이더리움을 이용한 에스크로 서비스 개선 모델". 한국컴퓨터정보학회 학술발표논문집, 26(1), 35-36, (2018).

[6] 박광용 송유진, "속성기반 암호기술", 정보보호학회지, 20(2), 85-92., April 2010.

[7] 이근왕, 진병욱, 김택중, "M2M 통신 환경에서 속성기반 암호기술을 활용한 통신 프로토콜 설계". 한국산학기술학회 학술대회논문집, , 313-315, 2014.

[8] 김연태, 김효승, 조효진, 이동훈, "속성기반암호화 기법을 이용한 안전한 메신저 시스템", Jounal of Security Engineering Vol. 12, No.5 pp469-486, 2015.

[9] 이문식, "접근제어가 가능한 다중기관 속성기반 암호 전송 알고리즘". 한국군사학논집, 74(3), 269-294, 2018.

[10] 명세인, 이종혁, "이더리움 노드 탐색 프로토콜 분석". 한국통신학회논문지, 43(12), 2081-2088, 2018.