https://doi.org/10.5392/JKCA.2018.18.07.620

커미트먼트 스킴을 응용한 사설 블록체인 기반 스마트 컨트랙트의 보안 모델

Security Model of Smart Contract Based Private BlockChain Using Commitment Scheme

김영수, 박영수, 이병엽
배재대학교 사이버보안학과

Young Soo Kim(experkim@gmail.com), Young-Soo Park(1484011@pcu.ac.kr),
Byoung Yup Lee(bylee@pcu.ac.kr)

요약

블록체인의 활용이 기업의 비즈니스 분야로 확대되면서 중요 정보의 기밀성 보호에 대한 중요성이 부각되고 있다. 블록체인은 트랜잭션의 공유와 공개에 따른 트랜잭션의 무결성 위협에 대한 보안문제를 해결하고 있으나 기밀성 보호는 취약하다. 따라서 기업에서 블록체인을 비즈니스 처리에 활용하기 위해서는 기업의 중요정보와 개인정보에 대해서 기밀성을 제공할 수 있는 보안 메커니즘이 필요하다. 이의 해결을 위해서 이더리움의 스마트 컨트랙트와 커미트먼트 스킴을 이용한 사설 블록체인 기반 암호화 프로토콜의 응용 모델을 제안하고 구현한다. 이는 사설 블록체인에 기밀성과 무결성이 강화된 스마트 컨트랙트를 통해서 비신뢰 참여자간 비즈니스를 수행할 수 있게 해줌으로써 블록체인 서비스의 활성화에 기여한다.

■ 중심어 : | 커미트먼트모델 | 사설블록체인 | 스마트컨트랙트 | 보안모델 | 암호화프로토콜 |

Abstract

With the widespread adoption of blockchain in the field of business, the importance of confidentiality of critical information has been emerging. Although blockchain models solve the security problem regarding integrity threat by sharing transactions and making them public, it is vulnerable in terms of confidentiality. Therefore, a security mechanism to provide confidentiality of critical information and private information of a firm is necessary to utilize block chain in the process of work. In order to solve the problem, we suggest Private blockchain based cryptographic protocol application model using Smart contract commitment scheme of the Ethereum. It can contribute to activation of blockchain services by enabling non-trusted participants to perform businesses through application of smart contract enhanced in terms of confidentiality and integrity to private blockchain.

■ keyword : | Commitment Scheme | Private Blockchain | Smart Contract | Security Model | Cryptography Protocol |

* 이 논문은 2018학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임.
접수일자 : 2018년 06월 27일
수정일자 : 2018년 07월 16일
심사완료일 : 2018년 07월 16일
교신저자 : 이병엽, e-mail : bylee@pcu.ac.kr

Ⅰ. 서 론

최근 급부상하고 있는 블록체인은 분산 원장, 공유 원장 기술 등 여러 이름으로 불리우며, 향후 글로벌 사회·문화·경제 체계를 변화시킬 혁신 미래 기술로 부각되고 있다. 블록체인은 신생기술로서 수많은 접근법과 이에 파생된 기술이 혼재되어 있고 공통 표준이 없이 발전하고 있는 상태이다. 최근 이러한 블록체인 파생 기술을 지원하고 상호운영성과 안전에 대한 표준화에 대한 요구도 높아지고 있다. 기존의 비트코인이 금융 트랜잭션에 초점을 두고 있는 반면 이더리움은 모든 산업 분야에서 프라이빗 블록체인을 구성하는데 사용된다. 이더리움은 비트코인이 갖는 블록체인의 한계점인 금융에 국한된 스크립트 기능을 확장한 스마트 콘트랙트를 통하여 서로 신뢰할 수 없는 두 당사자간에 신뢰를 제공하는 시스템이다. 상대방을 신뢰하지 않더라도 시스템상으로 거래의 안전성을 보장해 준다. 이더리움 블록체인 기반 스마트 컨트랙트는 기존 트랜잭션의 무결성만 보장하던 블록체인 시스템의 한계를 넘어 조건과 상황에 따라 자동으로 계약 내용을 이행하는 스마트 컨트랙트 시스템으로 진화하였다. 이러한 블록체인 기반 스마트 컨트랙트는 블록체인의 가장 핵심적인 특징으로 여겨지며 이더리움 이후의 대부분의 새로운 블록체인은 스마트 컨트랙트의 기능을 기본적으로 탑재한다. 이러한 스마트 컨트랙트는 공개 블록체인뿐 아니라 사설 블록체인쪽에서도 활발하게 연구되고 있다. 사설 블록체인은 비트코인, 이더리움과 같이 누구나 참여할 수 있는 블록체인이 아닌 제한된 참여자만 참가할 수 있는 블록체인이다. 블록체인에 참여하는 누구나 본인이 직접 참여하지 않은 트랜잭션의 정보를 포함하여 모든 트랜잭션 이력을 조사할 수 있는 공개 블록체인의 경우에 기밀성 제공에 한계를 보이는 반면 프라이빗 블록체인을 구성하는 경우에는 일반적으로 트랜잭션정보의 기밀성을 보장하는 보안 메커니즘을 개발하여 구축하고 있으나 허가된 접근 데이터의 참여자 권한 관리 미흡 등으로 침해 사고가 발생한다[1-3]. 또한 블록체인기술 적용시 화폐로서는 이용될 수 없는 화폐 증표로서의 태생적인 한계를 가지고 있고 화폐증표에 법적인 지위를 줄려고 해도 화폐 자체를 사용하는데 수수료 등이 발생하고

채굴을 위해서 비용이 발생할 뿐만 아니라 막대한 자원들을 무의미하게 낭비하는 문제점이 있다. 프라이빗 블록체인 구성이 가능한 Hyperledger fabric는 트랜잭션 기밀성을 보장 가능하도록 각각 Channel 기능을 제공한다. 기밀성을 제공하는 커미트먼트 스킴을 이용한 보안 프로토콜은 여러 암호 함수를 이용하여 개발되고 있으며, 그 중에서 영지식을 이용한 응용 프로토콜로 멘탈 포카 프로토콜과 검증비밀분산공유(VSS, Verifiable Secret Sharing) 프로토콜, zcash프로토콜 등 다수의 보안 프로토콜이 존재한다. 사설 블록체인기반 스마트 컨트랙트를 이용하여 허가된 기밀정보에 접근할 수 있는 그룹 참여자의 제어와 암호화를 통해서 기밀성을 제공하는 보안 모델을 제안한다. 이를 위해서 본 논문은 다음과 같이 구성된다. 2장에서는 블록체인 기반 스마트 컨트랙트 모델을 분석하고 3장에서는 블록체인의 트랜잭션 보안 위협 모델을 분석하였다. 4장에서는 커미트먼트 스킴을 응용한 스마트 컨트랙트의 보안 모델을 제안한다. 5장에서는 결론과 시사점을 기술한다.

Ⅱ. 블록체인 기반 스마트 컨트랙트 모델

2.1 블록체인 계층 구조

블록체인의 서비스 계층 구조를 이루는 기술은 [그림 1]과 같이 다양하게 개발되고 전개되고 있다. 블록체인을 활용한 서비스 시스템 환경 전체를 담당하는 구조화된 표준화 모듈의 결합체인 블록체인 플랫폼은 블록체인(Blockchain)과 비순환 방향 그래프(Directed Acyclic Graph,DAG) 기반의 블록체인 플랫폼으로 제 1세대 블록체인인 비트코인과 이의 불완전성을 극복하기 위해서 등장한 플랫폼이 이더리움이었고, 이더리움의 한계를 극복하기 위해서 비순환 방향 그래프(Directed Acyclic Graph, DAG) 기반의 3세대와 4세대로서 해시그래프(Hashgraph)와 오픈그래프(Opengraph)가 등장하고 있다[4]. 비트코인은 전자 화폐 시스템으로 탄생했기 때문에 데이터 구조나 프로토골은 화폐 시스템에 특화돼 있

다. 시스템 자체는 범용적이지만 그곳에 흐르는 데이터와 처리를 다른 방법으로 사용하는 데는 한계가 있다. 따라서 2세대 블록체인인 이더리움은 통화에 특성화되어 있던 블록체인을 스마트 계약(Smart Contract)을 통해서 여타 다른 용도로 사용할 수 있는 가능성을 열었다. 소위 블록체인 기반의 어플리케이션(Decentralized Application, Dapp)을 구현할 수 있게 된 것이다. 그러나 블록체인이라는 분산 원장기반의 비트코인과 이더리움은 트랜잭션의 우선순위를 보장하지 않는다. 이러한 한계를 극복하기 위한 플랫폼 기술로 제3세대인 해쉬그래프와 제4대인 오픈그래프가 개발되었다.

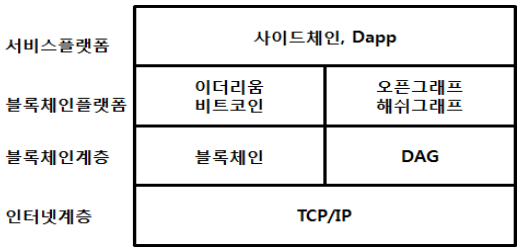

그림 1. 블록체인의 서비스 계층 구조

블록체인 플랫폼은 네트워크 상의 모든 참여자들이 공인된 중개자 없이도 투명하게 트랜잭션 기록을 검증할 수 있게 함으로써 공유로 인해 야기되는 개인정보의 노출과 위변조를 방지하기 위하여 익명성과 무결성을 보장하는 암호기술을 적용하고 있으나 트랜잭션의 기밀성을 지원하는 보안 기술은 취약하다. 따라서 암호기술을 블록체인에 접목하여 기밀성을 보장하고 강화 할 필요가 있다.

2.2 스마트 컨트랙트 모델

오늘날 스마트 컨트랙트의 가장 일반적인 개념은 블록체인에 저장된 프로그램을 말한다. 블록체인은 본질적으로 트랜잭션의 위변조로부터 보호하는 분산되고 공유된 분산 장부(distributed shared ledger)로서 공유를 목적으로 무결성의 보호에 초점을 맞추고 있다. 공개 블록체인에 탑재되는 스마트 컨트랙트는 토큰 관리에 가장 많이 사용되는 반면 사설 블록체인의 스마트 컨트랙트는 트랜잭션의 기밀성 보호를 위해서 인증 및 암호화 등의 보안 기능를 내재해서 사용한다. 스마트 컨트랙트의 동작 모델은 [그림 2]와 같다.

사용자가 송금이나 업무용 트랜잭션을 만들어 블록체인에 전송하면 블록체인의 노드들은 해당 트랜잭션을 공유한다. 블록체인 내부의 합의 알고리즘에 의해서 선택된 블록체인의 노드가 해당 트랜잭션을 포함해 블록을 생성하고 블록을 브로드캐스팅한다. 블록을 전달받은 각 노드는 블록을 자신의 블록체인에 추가하고 해당 블록에 저장되어 있는 트랜잭션을 실행시켜 자신의 스마트 컨트랙트 데이터베이스를 갱신시킨다[5-7]. 이러한 과정을 통해 모든 블록체인의 노드들이 같은 스마트 컨트랙트의 상태 데이터베이스를 공유하게 된다. SQL 질의 구문이 데이터베이스 서버에 전송되어 실행되는 것과 같이 스마트 컨트랙트의 메서드 호출구문이 트랜잭션의 형태로 블록체인 노드에 전송이 되면 모든 노드에서 이를 실행하여 블록체인에 저장한다. 따라서 블록체인 기반 스마트 컨트랙트는 모든 트랜잭션 데이터를 공유하기 때문에 특정한 사람이 스마트 컨트랙트의 실행 결과를 조작하려해도 조작할 수 없으며 블록체인이 모든 트랜잭션의 무결성을 보장해 주는 방식으로 스마트 컨트랙트의 무결성도 보장할 수 있다.

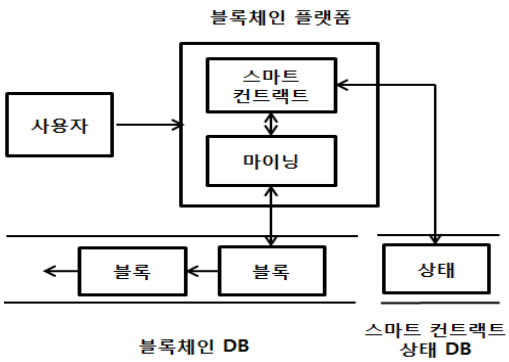

그림 2. 스마트 컨트랙트 모델

이를 통해 사설 블록체인에 기밀성과 무결성이 강화된 스마트 컨트랙트를 탑재함으로써 비신뢰 사용자 및 기관간 공동 업무를 수행할 수 있게 해준다.

Ⅲ. 블록체인의 트랜잭션 보안 위협 모델

3.1 블록체인의 보안 모델

블록체인의 기본 특성은 공유로 P2P 기술에 추가된 증명 알고리즘이 무결성을 제공하고 신뢰를 인증할 제3의 기관이 필요 없기 때문에 제3의 기관에 신뢰를 보장하기 위해 투입해야 할 비용과 시간이 절약된다. 이외에도 블록체인은 실시간으로 정보를 공유하기 때문에 직렬로 처리할 업무를 병렬로 처리해 효율성을 높인다. 다시 말해 블록체인의 기본 특성인 공유성은 투명성과 무결성을 보장하고, 이는 기존 서비스의 신뢰성과 효율성을 향상시키는 가치를 제공한다. 블록체인의 무결성은 암호학적 해쉬함수의 결과 값을 체인을 위한 토큰 값으로 사용하여 실현된다. 이는 해쉬함수의 입력 데이터가 1비트라도 다르면 완전히 상이한 결과값을 출력하고 해쉬함수의 결과값을 가지고 입력값을 알아내기 어려운 두 가지 성질에 기초를 두고 있다. [그림 3]과 같이 블록체인은 블록과 블록이 해쉬라는 토큰값을 사용하여 체인처럼 연결되어 있고 블록내부에 포함된 트랜잭션에 대한 해쉬값이 머클루트의 값으로 포함되어 있다. 따라서 트랜잭션이 바뀌게 되면 머클루트의 해시값이 바뀌게 되고 이로 인해서 또 다시 블록의 해시값이 변경되기 때문에 트랜잭션을 위변조하기 위해서는 분산되어 공유되고 있는 모든 블록의 트랜잭션을 변경해야 하는데 이는 거의 불가능하므로 블록체인은 트랜잭션의 무결성을 제공한다.

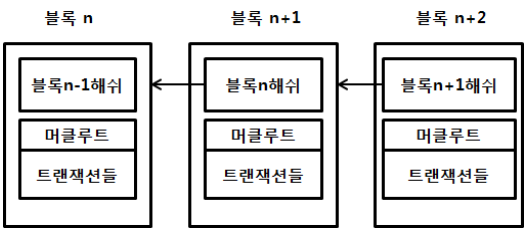

그림 3. 무결성 제공 메커니즘

공개 블록체인은 중앙에서 별도로 개인정보를 관리하는 기관이 없고 송금 및 비즈니스 트랜잭션의 처리를 위한 인증을 요구하지 않는 익명성 보호를 위한 보안 메커니즘을 내재하고 있다[8-11]. [그림 4]와 같이 암호학적 해쉬 함수를 사용해서 공개키로부터 어카운트 어드레스를 생성하고 인증정보를 관리하지 않으므로 어카운트 어드레스를 통한 사용자의 신원에 대한 인증 정보를 활용하여 침해사고를 사전적으로 차단할 수 없고 침해사고가 발생된 이후에 식별된 어카운트 어드레스와 관련된 트랜잭션을 추적하여 자금 내역을 파악할 수는 있다. 반면 사설 블록체인은 특정 기관이 구성한 블록체인으로 인증과 접근제어를 통해서 노드 참여 여부를 포함한 블록체인 자체를 관리할 수 있는 권한을 가지고 형성한 블록체인이다. 따라서 사설 블록체인의 관리자가 악의적 개입을 통해서 익명성과 기밀성을 침해할 가능성이 크다. 블록체인의 익명성은 블록체인 참여자의 인증정보에 대한 기밀성을 의미하므로 사설 블록체인의 경우 중앙기관의 블록체인 관리자가 몰래 엿볼 가능성이 충분하므로 익명성이 낮다.

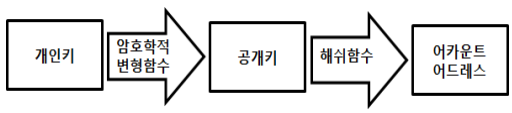

그림 4. 어카운드 어드레스 생성 메커니즘

사용자는 [그림 5]와 같이 송금 및 비즈니스 트랜잭션을 위해서 수신자의 공개키로 코인을 lock 해서 보내고 수신자는 코인을 사용하기 위해서 자신의 개인키를 사용해서 unlock한다. 블록체인에 저장되는 모든 트랜잭션은 수수료를 지급해야 하므로 모든 트랜잭션은 어카운트 어드레스와 논리적으로 연결된다. 특정 어카운트 어드레스와 관련된 송금 내역을 추적할 수는 있지만 사용자의 인증 정보는 알 수 없는 익명성 보안 메커니즘이 내재되어 있다.

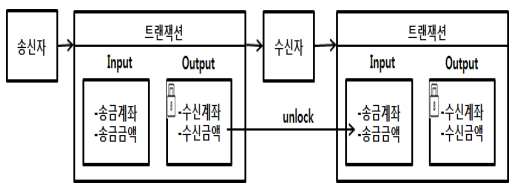

그림 5. 익명성 제공 메커니즘

3.2 스마트 컨트랙트의 보안 위협 모델

블록체인은 사용자에게 트랜잭션을 공개해서 공유하므로 기밀성을 지킬 수 없는 구조이다. 따라서 모든 사용자가 트랜잭션의 모든 기록을 볼 수 있으므로 개인정보 또는 중요한 비즈니스 비밀을 포함하고 있는 트랜잭션을 블록체인에 저장하는 것은 바람직하지 않다. 블록체인의 기밀성에 대한 가장 큰 보안 위협은 [그림 6]과 같이 인가되지 않은 트랜잭션 정보의 유출을 위한 중간자 공격과 신분도용 행위가 있다. 또한 스마트 컨트랙트를 이용해서 중요한 비즈니스 정보나 개인정보를 조회, 추가, 삭제 할 수 있기 때문에 스마트 컨트랙트에 의한 기밀성을 침해하는 위협이 존재한다. 따라서 블록체인에 저장되는 트랜잭션의 암호화와 스마트 컨트랙트를 실행하는 참여자의 인증 등 트랜잭션 정보의 유출을 최소화할 수 있는 방안을 고려해야 한다[12-14].

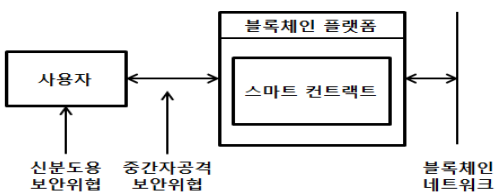

그림 6. 스마트 컨트랙트의 보안 위협 모델

Ⅳ. 커미트먼트 스킴을 응용한 스마트 컨트랙트의 보안 모델

4.1 커미트먼트 스킴

암호화 메커니즘은 불가분의 관계이지만 암호화 메커니즘은 블록체인의 존재 여부와 무관하게 발전 진화하고 있다. 따라서 블록체인과 암호화 기술의 융합을 통해서 정보보호를 강화할 필요가 있다. 특히 다양한 암호화 기술과의 융합을 통해서 블록체인은 더 좋은 보안성을 제공할 수 있다. 블록체인에 커미트먼트 스킴을 이용한 암호학적 응용 프로토콜이 접목되어 개발되고 있다[15-17]. 커미트먼트 스킴은 [그림 7]과 같이 다른 사용자가 알 수 없도록 트랜잭션 정보를 숨기는 커미트(Commit) 과정과 숨겨져 있는 데이터를 드러내는 공개(Reveal) 과정으로 구성된 보안 모델이다. 암호화 전자봉투 C에 포함한 트랜잭션의 정보 X와 검증값 V를 전송하는 커미트 단계에서 송신자 S는 전송한 트랜잭션의 내용을 변경할 수 없다. 송신자로부터 비밀키 P를 수신해서 암호화 전자봉투의 트랜잭션의 정보 x를 개봉하고 검증 알고리즘을 수행하는 공개(Reveal)단계에서 수신자는 암호화 전자 봉투를 개봉하기 전까지는 기밀정보를 알 수 없다. 커미트먼트 스킴의 목적은 송신자가 드러낼 시점에 비밀키를 넘겨줌으로써 미래의 어떤 시간까지 트랜잭션에 대한 기밀성을 유지하는 대신 송신자 자신도 변경할 수 없는 트랜잭션을 정의하는 것이다.

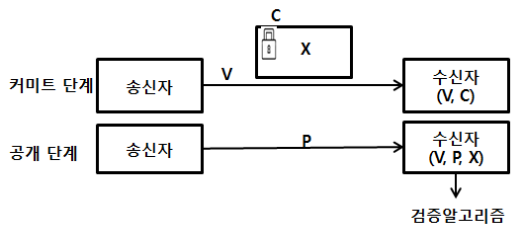

그림 7. 암호학적 커미트먼트 스킴

블록체인기반 전자투표시스템에서 공개키 기반 커미트먼트 결과 값과 해시값을 함께 전송해서 검증 과정을 수행하는 해쉬기반 커미트먼트 모델을 사용한 응용 프로토콜을 개발하여 투표결과 집계를 구현할 수 있다. 커미트 단계에서 투표자는 자신의 개인키를 사용하여 암호화한 투표내용과 해쉬값을 전자투표관리서버에 전송한다. 공개단계에서 공개관리서버는 투표자의 공개키를 수신하여 복호화한 후에 투표내용을 식별하고 이로부터 계산한 해쉬값과 수신한 해쉬값의 비교를 통한 검증 수행 후 투표결과를 집계한다.

4.2 스마트 컨트랙트의 응용 모델

블록체인 스마트 컨트랙트는 블록체인과 결합해 엄청난 부가가치를 창출할 낼 수 있는 잠재력 있는 기술인 반면 보안을 내재화하지 않으면 보안 위협 요인이 되기 때문에 이로 인해 침해사고가 발생한다. 스마트 컨트랙트의 기반 기술인 블록체인은 암호학적 해싱 함수를 사용하여 트랜잭션의 무결성 위협에 대한 보안문

제를 해결하고 있으나 스마트 컨트랙트의 트랜잭션에 대한 기밀성을 보장해 주지 않는다. 이의 해결을 위해서 스마트 컨트랙트의 트랜잭션 정보를 모든 사용자에게 일률적으로 공개하는 대신 트랜잭션정보 공개 범위를 제한할 수 있는 암호화 기법이나 인증기술을 접목한 사설 블록체인의 개발이 필요하다. 스마트 컨트랙트 기반 사설 블록체인은 기밀성 보호가 요청되는 비즈니스 트랜잭션의 처리를 위해서 소규모 단위의 그룹으로 사용자를 제한하고 인가된 정보의 접근제어를 수행하는 보안 기능을 내재화하여 구축되어야 한다.

이를 위해서 [그림 8]과 같은 스마트 컨트랙트에 영지식 증명 기반 커미트먼트 스킴을 제안한다. 이는 허가된 트랜잭션의 기밀정보에 접근할 수 있는 응용 모델로 그룹 참여자의 제어를 통해서 기밀성을 제공한다. 영지식증명은 내가 알고 있는 어떤 중요한 정보에 대하여 그것을 보여주지 않으면서 그것을 알고 있다는 것을 상대방에게 증명해 보이는 커미트먼트 스킴으로서 익명성과 기밀성을 제공하는 방법이다. 사용자(송신자)는 랜덤 값 r과 공개되어 있는 큰 두 소수의 곱 N(p*q)을 사용해서 계산된 x와 ID를 전송하면 스마트 컨트랙트(수신자)는 0 또는 1중 랜덤하게 선택한 e값을 사용자에게 보낸다. 사용자는 각 경우에 대해 1<=S<=N-1인 비밀키 S를 선택해서 계산된 V(S2 mod N)를 공개하고 S와 N을 사용해서 계산된 y와 해시값 h1(패스워드, x, y)를 스마트 컨트랙트에게 보낸다. 스마트 컨트랙트는 DB에서 ID에 대응되는 패스워드를 획득해서 계산된 해쉬값 h2(h(패스워드,x,y))와 수신한 h1을 비교하고 수신한 x, y와 공개값 v로부터 y2와 x*ve mod N가 같은지를 계산해서 검증을 하게 된다. 사용자는 S를 노출하지 않고 x라는 것을 입증함으로써 인증을 통과한다.

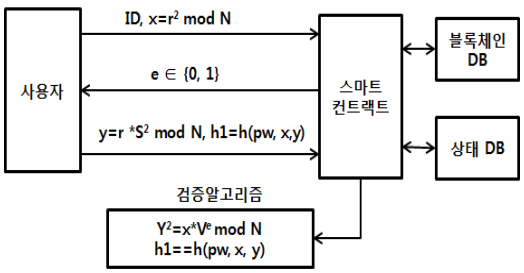

그림 8. 스마트 컨트랙트의 사용자 인증 모델

스마트 컨트랙트는 그룹제어를 통한 트랜잭션의 기밀성 보호를 위해서 인증에 성공한 사용자에게 commit한 결과값을 전송하고 이를 사용자가 reveal해서 볼 수 있도록 그룹키를 보내주게 된다. 스마트 컨트랙트의 그룹 제어를 위한 응용 프로코콜에서 사용되는 그룹키 생성 모델은 [그림 9]와 같다. 스마트 컨트랙트는 사용자의 그룹키를 유도하기 위해서 사용자 인증시에 획득한 사용자의 그룹 ID와 자신의 마스터키를 이용해서 계산된 해시값을 그룹키로 생성하여 사용자에게 전송한다. 그룹키 유도함수를 통한 계층적 키 관리 기법은 스마트 컨트랙가 사용자의 그룹키를 저장할 필요가 없고 자신이 알고 있는 사용자 그룹 정보로 부터 하위계층의 그룹키를 유도함으로 그룹키의 관리를 단순화시킨다.

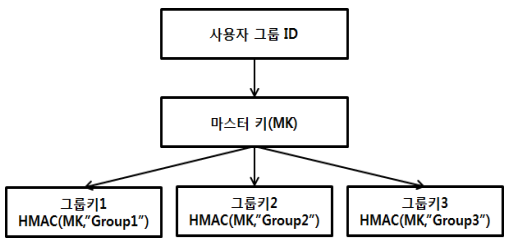

그림 9. 그룹제어를 위한 그룹키 유도함수 모델

기밀성 보호를 위한 커미트먼트 모델을 응용한 보안 프로토콜에 해시와 공개키 기반 커미트먼트 모델이 많이 연구 활용되고 있다. 제안 모델은 영지식을 응용한 커미트먼트 모델로서 계산량 및 통신량의 문제점을 갖고 있다. 따라서 향후 이러한 문제점을 해결하고 효율성을 개선한 응용 프로토콜을 연구할 필요가 있다. 또한 제안 모델은 암호화 기법을 사용하는 커미트먼트 모델로서 암호화는 사용자 편의성과 트레이드업 관계를 가지고 있다. 따라서 암복호화 처리속도에 따른 반응속도를 측정함으로써 실용성을 확인할 수 있다. 이를 위해서 향후 모델의 성능과 효율성 검증을 위한 시뮬레이터에 대한 추가 연구가 필요하다.

V. 결 론

공개 블록체인의 경우 공유를 목적으로 무결성 보호

에 특화되어 있기 때문에 신원을 요구하지 않고 트랜잭션에 대한 기밀성을 보장하지 않지만, 사설 블록체인의 경우 소규모 단위의 사용자 그룹으로 구축되어 사용되므로 내부의 기밀성이 중요해진다. 따라서 기업에서 블록체인기반 응용시스템을 구축하는 경우에 기밀 정보가 노출 되지 않도록 필수적으로 암호기술을 접목해서 사용해야 한다. 기업의 비즈니스 분야로 블록체인의 활용이 확대되면서 트랜잭션 정보의 기밀성 보안 위협은 해결해야 할 중요과제이다. 이와 같이 트랜잭션정보의 기밀성을 보장하는 보안 메커니즘을 접목한 사설 블록체인의 구축이 활성화 되고 있으나 허가된 접근 데이터의 참여자 권한 관리 미흡 등으로 침해 사고의 발생 가능성이 확대되고 있다. 이의 해결을 위해서 본 논문에서도 사용자 그룹의 트랜잭션 보호를 위해서 스마트 컨트랙트에 commitment 모델을 적용해서 사설 블록체인의 보안성을 강화하는 보안 모델을 제안하였다. 제안 모델은 스마트 컨트랙트의 사용자의 인증을 위해서 영지식증명모델을 스마트 컨트랙트에 접목하여 비밀키를 노출시키지 않고 자신을 입증함으로써 비밀키를 반복적으로 사용할 수 있도록 하였고 그룹 트랜잭션의 기밀성 보호를 위해서 사용하는 그룹키를 계층적으로 생성하고 관리함으로써 그룹키의 효율적 관리를 제공한다. 또한 스마트 컨트랙트의 취약점이 되고 있는 트랜잭션 정보의 침해 위협을 감소시키고 비신뢰 참여자간 비즈니스 활성화에 기여한다. 제안 모델은 이더리움 블록체인 플랫폼에 탑재되어 스마트 컨트랙트의 트랜잭션에 대한 익명성과 기밀성을 제공하는 알고리즘으로 활용될 수 있다. 그러나 본 논문의 제안 모델은 영지식을 이용한 커미트먼트 스킴 응용 프로토콜로서 계산량 및 통신량의 문제점을 고려하고 있지 않다. 따라서 향후 이러한 문제점을 해결하고 효율성을 개선한 응용 프로토콜을 연구할 필요가 있다.

참 고 문 헌

[1] 김영수, 문형진, 조혜선, 김병익, 이진해, 이진우, 이병엽, “계층적침해자원기반의 침해사고 구성 및 유형 분석,” 한국콘텐츠학회논문지, 제16권, 제11호, pp.139-153, 2016.

[2] 김영수, 김영수, 이병엽, “클라우드 환경에서 블록체인관리서버를 이용한 인증기반 내부망 분리 보안 모델,” 한국콘텐츠학회논문지, 제18권, 제6호, pp.434-442, 2018.

[3] V. Morabito, “Smart contracts and licensing,” in Business Innovation Through Blockchain, pp.101-124, Springer, 2017.

[4] Lemon Baird, The Swirlds Hashgraph Consensus Algorithm:Fair, Fast, Byzantine Fault Tolerance, Swirlds Tech Report Swirlds-TR-2016-01, May 31, 2016.

[5] W. Egbertsen, G. Hardeman, M. van den Hoven, G. van der Kolk, and A. van Rijsewijk, “Replacing paper contracts with ethereum smart contracts,” 2016.

[6] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, “Evaluation of logic-based smart contracts for blockchain systems,” in International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, pp.167-183, 2016.

[7] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, and N. Swamy, et al., “Formal verification of smart contracts:Short paper,” in Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp.91-96, ACM, 2016.

[8] M. Vukolić, “Rethinking permissioned blockchains,” in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, ACM, pp.3-7, 2017.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in 2016 IEEE Symposium on Security and Privacy (SP), IEEE, pp.839-858, 2016.

[10] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town crier: An authenticated data feed for smart contracts,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, ACM, pp.270-282, 2016.

[11] M. Al-Bassam, “Scpki: A smart contract based pki and identity system,” in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, ACM, pp.35-40, 2017.

[12] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on ethereum smart contracts (sok),” in International Conference on Principles of Security and Trust, Springer, pp.164-186, 2017.

[13] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab,” in International Conference on Financial Cryptography and Data Security, Springer, pp.79-94, 2016.

[14] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, “Blockchain contract: Securing a blockchain applied to smart contracts,” in 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, pp.467-468, 2016.

[15] Oleg Andreev, Hidden in Plain Sight: Transacting Privately on a Blockchain. blog.chain.com, 2017.

[16] Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp.263-280, 2012.

[17] Ivan Damgård, Commitment Schemes and Zero-Knowledge Protocols, In Proceeding, Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, pp.63-86, Jul. 1998.

저 자 소 개

김 영 수(Young Soo Kim) 정회원

- 2003년 8월 : 국민대학교정보관리학(정보관리학박사)
- 현재 : 충남 재활IT 융합 기술원 대표 컨설턴트
- 현재 : 배재대학교 사이버보안학과

<관심분야> : 빅데이터서비스보안, 정보 보안

박 영 수(Young Soo Park) 정회원

- 2017년 2월 : 배재대학교 사이버보안학(공학학사)
- 현재 : 배재대학교 사이버보안학(공학석사재학)

<관심분야> : 데이터통신, 데이터베이스, 정보보안

이 병 엽(Byoung Yup Lee) 종신회원

- 1991년 2월 : 한국과학기술원 전산학과(공학사)
- 1993년 2월 : 한국과학기술원 전산학과(공학석사)
- 1997년 2월 : 한국과학기술원 경영정보공학(공학박사)
- 1993년 1월 ~ 2003년 2월 : 대우정보시스템 차장
- 2003년 3월 ~ 2016년 2월 : 배재대학교 전자상거래학과 부교수
- 2016년 3월 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : XML, 지능정보시스템, 데이터베이스 시스템, 전자상거래학