효율적인 Private Blockchain을 위한 KSI기반의 인증관리에 관한 연구+

라경진, 이임영
순천향대학교 컴퓨터학과
e-mail:[rababi, imylee]@sch.ac.kr

A Study on KSI-based Authentication Management for Efficient Private Block Chain

Gyeong-Jin Ra, Im-Yeong Lee
Dept of Computer Science Engineering, Soonchunhyang University

요 약

블록체인은 DLT 기술로서, P2P 네트워크의 영역별로 유지 관리되는 트랜잭션의 추가 전용 공유 레코드 기술이다. 그 중 Private Blockchain은 허가된 사용자 멤버만으로 구성된 블록체인 환경으로, 소수의 신뢰노드만이 블록 생성 합의에 참여하여 빠른 블록체인을 형성하고 이를 하나의 원장으로 공유한다. 따라서 본 논문에서는 Private Blockchain의 허가된 사용자의 신원확인을 위한 인증구조인 PKI(Public Key Infrastructure)와 AKI(Accountable Key Infrastructure)를 비교 분석하고 KSI(Keyless Signature Infrastructure)기반의 인증관리를 제안한다.

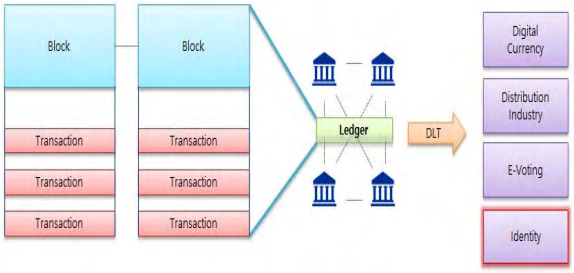
1. 서론

최근 4차산업혁명의 도래와 함께 탈중앙화방식의 블록체인 기술이 주목받고 있다. 블록체인은 DLT 기술 중의 하나로, 참여 노드가 모두 동일한 원장을 기록 및 소지하는 자료구조 기술이다[1]. 특히 프라이빗 블록체인은 신원이 허가된 노드만이 참여 주체가 된다. 또한 특정 몇몇 노드만이 블록 검증 및 생성을 하거나 블록을 전파하여 모든 노드가 같은 원장을 갖는 것이 목표이므로 블록생성 속도가 빠르다. 따라서 프라이빗 블록체인은 별도의 허가된 노드를 구성하고 신원확인 절차가 필요하다. ID 기반의 사용자 인증시스템은 사용자의 법적 신원에 근거하여 공개키를 생성하고 이를 TTP(Trusted Third Party)에 의해 공개키 인증서와 사용자ID를 바인딩하게 되는데, 이는 블록체인의 탈중앙성과 상충하며 다시 단일지점오류에 의한 MIMT(Man In-the- Middle Attack)의 위협을 가지게 된다(그림 2). 따라서 본 논문에서는 기존 인증관리를 비교분석하고, 프라이빗 블록체인에서의 KSI 기반의 멤버 인증 관리를 제안한다.

2. 관련 연구

2.1 PKI

PKI는 공개키 기반 구조로 PKI는 공개키와 소유주체를 묶어주는 인증서(Certificate)를 생성, 배포, 사용, 저장, 철회하는 구조를 갖는다. 하지만 PKI는 신뢰 된 발급 기관으로부터 발급받는 TTP(Trusted Third Party)라는 중앙집중형 시스템으로 장애 시 전체 또는 일부 서비스의 중단을 가져오는 단일장애지점(SPOF, Signle of Failure)를 가진다[2].

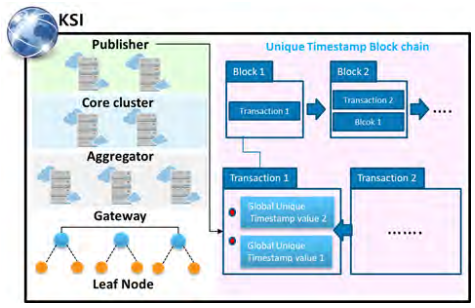


(그림 1) 블록체인과 활용 어플리케이션 및 DID

2.2 AKI

AKI는 자가인증프로토콜인AIP(Accountable Internet Protocol)의 공개키 검증 환경으로 기존 인증 시스템인 PKI의 “Single point of failure”을 보완하였다. 기존의 인증체계의CA(Certificate Authority)이외의 ILS(Integrity Log Server) 와 Validator로 구성되며 ILS는 인증서를 해시트리 기반으로 저장하여 인증서를 효과적으로 관리하고 데이터 변조에 대해서 빠르게 대처한다[3]. 하지만 추가 ILS와 Validator 구축이 필요하며 TLS 및 추가 시스템은 하이브리드 구조로 근본적인 탈중앙이 이루어지지 않는다.

+ “본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음” (IITP-2015-R0992-15-1006)



(그림 2) KSI 구조

2.3 KSI

KSI는 2013년 A buldas et.al.이 제안한 방식으로 기존의 PKI기반 공개키 구조 방식과 달리 사용자 인증과 메시지의 무결성을 따로 계산한다(그림 2). 즉 인증은 해시체인의 불가역성을 이용한 공개키 구조를 하고, 메시지의 무결성은 글로벌 해시 트리를 생성하여 유일한 타임스탬프 값으로 제공한다[4]. 이는 블록체인으로 연결되어 인터넷과 같은 네트워크 서비스 내에서 강력한 투명성과 접근성을 제공한다.

3. 보안 요구사항

본 장에서는 KSI기반의 DID를 위해 다음과 같은 보안 요소가 요구된다.

• 사용자 인증(Authentication): 정당한 사용자는 사용자의 공개키-개인키를 통해 네트워크의 올바른 사용자임을 보장하여야 한다.

• 신뢰성(Reliability) : 네트워크 참여자는 네트워크의 무결성과 가용성을 보장받아 전체 네트워크를 신뢰할 수 있어야한다.

• 효율성(Efficiency) : KSI기반 인증관리 시스템은 안전하면서 전체 처리량의 오버헤드를 최소화하여 효율적으로 계산 및 가용이 되어야 한다.

4. 제안방식

본 논문은 제안하는 방식은 사용자, 인증 서버 네트워크 구성되며 KSI 시스템 방식을 따른다.

4.1 키 생성 과정

사용자는 인증 서버 네트워크와의 통신을 위해 공개키-개인키 쌍을 생성한다. 이는 해시체인의 비가역성 성질을 이용하여 해시이전의 값은 사용자만이 알고 있으므로 이를 통해 인증을 수행한다. 공개키 생성은 RadomeNumber로부터 단방향 해시 체인으로 거듭 생성한 마지막 값과 해시트리로 만든 최종 Root값 쌍으로 한다. 그리고 해시체인의 역방향을 하나씩 개인키로 사용한다.

4.2 인증 서버 등록 과정

사용자는 공개키와 자신의 ID 및 인증정보 해시한 값을 인증서버에 전송한다. 인증 서버는 글로벌 해시 트리를 통해 생성한 Root값과 세계협정시간을 Lingking하여 글로벌 타임 스탬프를 생성한다. 이후 인증 서버 간 블록체인을 통해 글로벌 타임 스탬프를 최종 Commit한다. 이후 글로벌 타임스탬프를 포함한 인증서를 사용자에게 반환한다.

4.3 사용자 인증 과정

사용자는 해시체인과 해시트리로 생성한 개인키와 함께 글로벌 타임 스탬프가 포함된 인증서를 인증 서버에 보낸다. 인증 서버는 글로벌 해시 트리 및 블록체인을 통해 사용자의 인증서 유효성을 검증한다.

5. 보안 요구사항 분석

• 사용자 인증(Authentication): 정당한 사용자는 해시체인 및 해시트리로 생성한 공개키-개인키 쌍과 글로벌 타임스탬프가 포함 된 공개키 인증서를 통해 올바른 사용자임을 보장한다.

• 신뢰성(Reliability) : 네트워크 참여자는 Private Blockchain을 통해 위·변조로부터 안전하고 Fault Tolerance를 가진 신뢰 네트워크를 형성한다.

• 효율성(Efficiency) : 사용자 및 인증 네트워크는 해시 연산만을 사용하여 계산량과 연산횟수를 줄여 효율성을 가진다.

6. 결론

본 논문에서는 KSI 기반의 프라이빗 블록체인을 위한 인증관리 제안하였다. 제안방식분석에 따라 보안요구사항을 만족하면서 기존 PKI와 AKI의 TTP 기반 인증서 및 주요 시스템 구축필요성을 탈피하였고, 안전성과 효율을 개선시켰다. 향후 구체화 된 환경에 적용하여 필요한 기반 프로토콜을 구현 및 실제 구현까지 확대 적용이 필요할 것으로 생각된다.

참고문헌

[1] Nakamoto, S., “Bitcoin: A peer-to-peer electronic cash system”, 2008

[2] M. Schukat, & P. Cortijo, “Public key infrastructures and digital certificates for the Internet of things”, In Signals and Systems Conference (ISSC), pp. 1-5, 2015.

[3] B.W. Jin, J.O. Park & M.S. Jeon, “A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment”, Journal of IIBC, Vol.16, No.6, pp.25-31, 2016.

[4] C. Jämthagen, & M. Hell, “Blockchain-based publishing layer for the Keyless Signing Infrastructure”, In 13th IEEE International Conference on Advanced and Trusted Computing, IEEE--Institute of Electrical and Electronics Engineers Inc, 2016.