블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션 제안

- A proposal of a Block Certification System Security Solution using the Blockchain Validation Techniques -

박 현성*

* 순천향대학교 정보보호학과

요 약

최근 탈중앙화 기술인 블록체인의 산업 적용이 활발하게 이루어지고 있다. 블록체인 기술은 네트워크 구성원 간 공유되는 디지털 원장(ledger)을 의미한다. 새로운 거래가 발생할 때마다 구성원들의 동의를 통해 해당 거래를 인증하고, 블록체인에 기반한 거래 정보는 임의로 변경할 수 없기 때문에 거래의 신뢰성이 높고 정보 추적에 쉽다는 장점들을 가지고 있다. 또한, 이를 바탕으로 4차 산업혁명의 핵심기반기술로 주목받고 있다. 이와 동시에 기존 공인인증 시스템과 Active X의 폐지 방침이 발표되었고, 그에 따른 대안이 요구되고 있다. 하지만 기존 공인인증 시스템은 현재의 보안 수준을 따라오기 어려울 정도의 낙후된 기술이기 때문에, 근본적인 변화를 통해 변화되어야 한다. 경쟁을 통한 보안 기술의 발전과 혁신이 필요하고 기존의 목적을 잃지 않는 기술이 필요하다. 따라서 본 논문에서는 기존 공인인증서의 문제점을 파악하고 이를 해결할 수 있는 블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션을 제안한다.

키워드

인증, 공인인증, 공인인증서, 탈중앙화, 블록인증서, 블록인증, 블록체인, 인증체인

목 차

Ⅰ. 서론

1999년부터 도입된 공인인증서 제도가 최근 정부의 '전자서명법' 개정안을 마련하고 제도 폐지 방침을 발표함에 따라 변화의 길을 걷게 되었다. 이는 현행 공인인증서 제도는 보안 측면적, 실용적 문제가 있음을 의미한다. 사회 전반적으로 현재의 공인인증시스템은 시장독점을 초래하고 있으며, 앞으로의 전자서명 기술·서비스 발전과 올바른 시장 경쟁을 방해하고 있다는 문제점을 가지고 있다. 하지만 기존의 공인인증방식을 보완시키기에는 기술적으로 문제가 많으며, 개정될 인증제도 또한 같은 문제를 포함하고 있다.

이를 근본적으로 해결하기 위해서 인증서 관리체계를 관리하는 인증기관의 탈중앙화가 이루어져야 하며 깨끗하고 투명한 인증체계를 가져야 한다. 이는 블록체인이라고 불리는 보안 기술을 통해 기존의 인증기관이 안전한 인증서 관리체계를 구성하고 유지하기 위해 구성했던 시스템과 주요 기능들을 안전하고 효과적으로 수행할 수 있다. 더불어 수많은 인증기관을 통합하여 인증 시스템을 통합하는 과정을 통해 신뢰성을 더욱 높일 수 있다. 본 논문에서는 공인인증서의 새로운 시대를 위해 블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션을 제안한다.

Ⅱ. 공인인증서와 블록체인

1. 공인인증서

(1) 개요

국내 인터넷 금전거래를 이용할 때 인증을 위해 필요한 전자서명으로, X.509 v3 기반으로 인증서가 생성된다. 최상위인증기관인 RA와 공인인증기관인 CA가 존재하며 가입자 인증서 검증을 수행한다.

(2) 저장위치와 저장 방법

공인인증서 저장매체로는 보안토큰, 저장토큰(스마트카드), 휴대전화 등이 있으며, 공인인증서 S/W를 통해 공인인증서의 발급 및 이용 시 공인인증서를 저장할 수 있도록 지원된다. 공인인증서 저장을 위해 데스크톱 PC의 하드디스크 및 USB 메모리(이동식 디스크)를 많이 사용하고 있으나, 악성코드에 의한 공인인증서 유출 등의 문제로 인해 가급적 안전한 공인인증서 저장매체 이용을 권고하고 있으나 사용자의 저장장치, 즉 일반 폴더인 NPKI 폴더에 저장한다(웹브라우저에도 저장이 가능).

(3) 인증

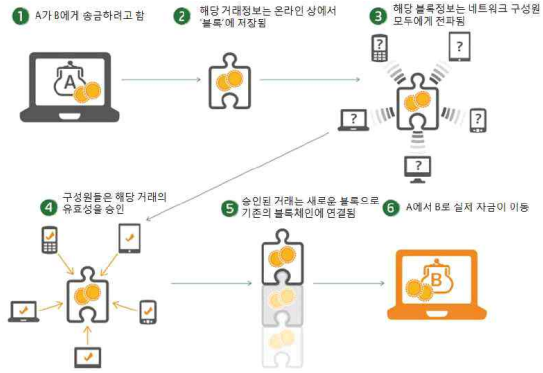
최상위인증기관으로부터 발급된 공인인증서는 특정 SW를 사용할 때만 다음과 같은 인증과정을 거친다.

① 전자거래업체로부터 거래정보 전자서명 요청
② 가입자 전자서명 제출
③ 공인인증기관이 가입자 인증서 검증
④ 최상위인증기관으로부터 공인인증기관 인증서 검증

2. 블록체인

(1) 블록체인 기술

블록체인은 데이터 분산 처리 기술이다. 즉, 네트워크에 참여하는 모든 사용자가 모든 거래 명세 등의 데이터를 분산, 저장하는 기술을 지칭한다. 블록들을 체인 형태로 묶은 형태로, 블록체인에서 '블록'은 개인과 개인의 거래(P2P) 데이터가 기록되는 장부가 된다. 형성된 블록들은 시간순으로 순차적으로 연결된 '사슬(체인)'의 구조를 가지게 된다. 모든 사용자가 거래내역을 보유하고 있어 거래 내역을 확인할 때 모든 사용자가 보유한 장부를 비교하고 확인해야 한다. 블록체인은 '공공 거래장부' 또는 '분산 거래장부'로도 불리기도 한다.



<그림 1> 블록체인 기반 거래과정 개념도

블록체인은 거대한 분산 공개 장부이며, 그 장부 안에 포함된 개별 거래는 모두 디지털 서명이 붙어 있어 은행이나 다른 제3자의 개입이 없어도 진본임을 보증할 수 있다. 수천, 수만 개의 노드에 분산된 공개 장부들은 어느 한 지점에 장애나 공격이 발생하더라도 블록체인이라는 네트워크 전체는 문제없이 계속 돌아갈 수 있다. 작업 증명이라는 수학적 계산 작업과 경제 관점에서의 논리를 통해 위/변조가

사실상 불가능한 구조를 갖게 되어, 그 안에 기록된 거래들은 은행과 같은 중앙의 보증 기관 없이도 신뢰할 수 있는 거래로서 확정될 수 있다.

(2) 블록체인 기술의 장점

1) 보안성 향상

분산원장 기술은 암호화된 데이터와 암호화된 키값으로만 거래가 이루어지므로 보안성을 높일 수 있다. 새로운 블록은 기존의 블록과 연결되므로 전체 블록안의 데이터 변조와 탈취가 불가능하다. 이는 각각의 참여 노드의 분산화로 해킹이 불가능하다.

2) 거래 속도 향상

거래의 인증 및 증명과정에서 제3자를 제외한 실시간 거래가 이루어지므로 거래 기록의 신뢰성 확보와 거래의 효율성, 속도가 향상된다. 또한 분산원장 기술로 오류를 최소화할 수 있어 거래의 정정과 수정을 위한 시간이 감소한다.

3) 비용 감소

거래 정보와 인증을 위한 중앙 서버와 집중화된 시스템이 필요 없기 때문에 거래 비용 감소로 이어진다. 거래 정보가 분산되어 있어 해킹의 위험으로부터 보호한다.

4) 가시성 극대화

네트워크 참여자들의 실시간 거래 모니터링이 가능하다. 따라서 투명성과 부인방지의 기능을 할 수 있다.

Ⅲ. 공인인증서 취약점

1. 공인인증서의 문제점

(1) 공인인증서 저장 문제

비표준적 위치(NPKI 폴더)에 저장되고 있으므로 다음과 같은 문제점이 도출된다.

- 이용자들이 별도 프로그램을 자신의 컴퓨터에 설치해야 하는 번거로움과 보안상 위험이 따름
- 단순히 복사 및 붙여넣기를 통해 이용자의 인증서 개인키가 쉽게 복제, 유출됨
- 글로벌 표준과 동떨어진, 고립된 인터넷 환경을 조성하고 있음

NPIK 폴더 내의 파일이 유출되면, 공격자는 Brute Forcing을 통해 암호를 쉽게 알아낼 수 있다. 공인인증서는 5회 이상 비밀번호 오류 시 자동 폐기가 되는 것이 정상이나, 공인인증서 시스템 자체에서 구현된 것이 아니기 때문에 별도의 접근을 통해 비밀번호를 알아낼 수 있다. 특히 국내 스마트폰 사용자와 사용량의 증가와 함께 공인인증서 해킹 사례가 더욱 증가했다. 개인 핸드폰이 PC보다 보안이 취약하다는 부분과 외부 프로그램을 쉽게 설치할 수 있다는 점이 문제가 되고 있다. KISA에서는 다음 문제를 인식하여 보안토큰 이용 권고를 하고 있지만, 보안토큰을 이용하는 국내 사용자는 드물다.

(2) 국제 공인 인증 문제

국내 최상위 공인인증기관 KISA는 국제적으로 인정받거나 신뢰받지 못하고 있다. 따라서 다음과 같은 상황이 발생하였다.

- 서버인증에 사용될 수 없음
- 국내 공인인증업체의 외국 진출이나 세계 인증 시장 진출이 불가능함

미국 국립표준기술 연구소(NIST)가 발간한 전자인증 가이드라인(Electronic Authentication Guideline)에 의하면, 전자파일 형태로 배포된 인증서(Soft crypto token)의 보안 강도는 높게 평가되지 못하고 있다.

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

<그림 2> NIST Electronic Authentication Guideline, p.39

(3) 가용성 문제

공인인증서의 검증시스템은 국내 소수의 RA와 CA가 인증하는데, 안전성에 문제가 발생하게 된다. RA나 CA가 인증서 검증을 수행하지 못하거나 악의적인 공격에 의하여 정상적인 기능을 하지 못하게 될 때, 기존의 공인인증시스템은 모두 마비가 될 수 있다.

(4) 별도의 플러그인, Active X, 프로그램 설치

공인인증서를 사용하려면 사용자는 해당 기관에서 권장하는 프로그램들을 설치해야 한다. 웹 브라우저나 일반적인 통신 기능을 위해서 별도의 보안 프로그램을 설치하게끔 한다. 이는 사용자의 불편함만을 호소하게 만들며, 또한 보안 프로그램을 설치하면서 관리자 권한을 위임하여 보안 문제를 야기하는 모순이다.

2. 공인인증서 해킹 사례

(1) 공인인증서 유출

최근 5년 동안 유출된 공인인증서가 8만 건이 넘는다. 2012년부터 2016년까지 최근 5년간 공인인증서 유출 건수는 8만 97건으로 확인되었다. 확인되지 않거나 드러나지 않은 공인인증서의 유출 규모는 알 수 없으며, 피싱 사이트, 불법 소프트웨어, 불법 APK 등 다양한 매체와 수법을 통하여 유출이 이루어지고 있다.

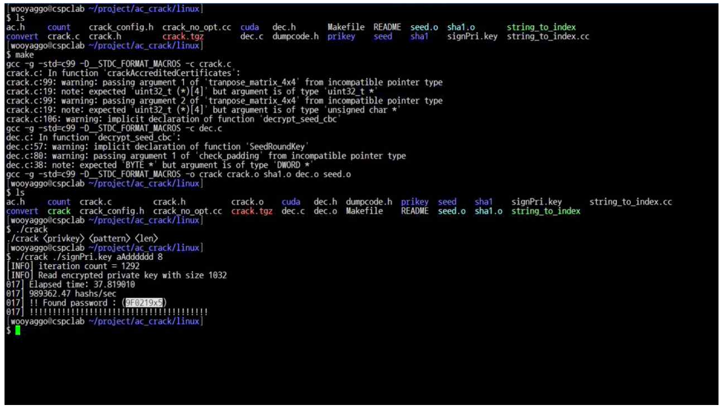
구분	'10년	'11년	'12년	'13년	'14년	'15년	'16년	합계
유출건수	0	0	8	8,710	41,733	22,796	6,850	80,097

<그림 3> 공인인증서 유출 현황(KISA)

더욱이 공인인증서가 유출되면 디지털서명정보의 위・변조가 불가피하며, 유출된 공인인증서는 악의적인 목적을 가지고 사용되어질 수 있다.

(2) 공인인증서 비밀번호 탈취

공인인증서의 유출은 비밀번호를 탈취하고 악의적인 이용으로 이어진다. 공인인증서는 두 개의 파일로 구성되어 있다. 하나는 공개키 파일이며 나머지 하나는 암호키 파일이다. 보통 인증서의 암호는 8자리 이상의 영문, 숫자 조합으로 구성되어 있다. 최근 특수문자를 포함하여 암호를 설정한다. 하지만 쉬운 패턴의 암호는 보안 전문가에 의해 불과 몇 분 만에 탈취할 수 있었다. 현재 공인인증서에 사용되는 이러한 방식은 보안에 있어서 큰 취약점을 가지고 있다.



<그림 4> 공인인증서 비밀번호 탈취 화면

Ⅳ. 블록인증시스템 보안 솔루션 제안

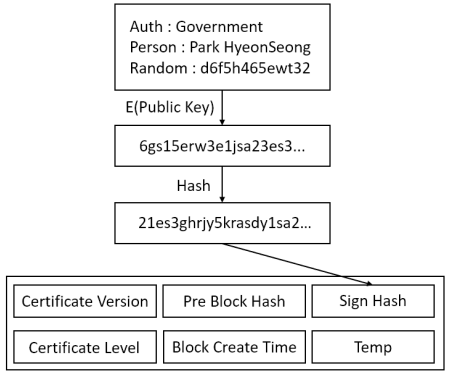
블록체인과 공인인증서를 융합한 개념을 가진 인증서를 블록인증서라고 칭하도록 한다, 기존의 암호화 방식을 유지하고 무결성과 기밀성, 가용성 측면의 보안서비스를 제공한다.

1. 구조

(1) 인증체인

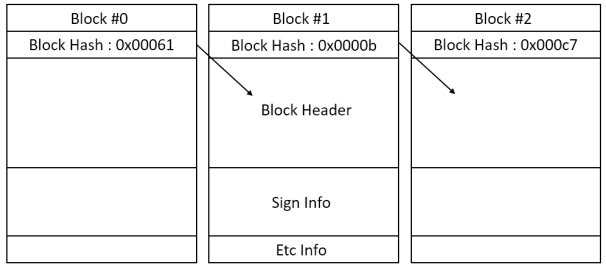
인증 체인의 구조는 다음과 같다.

• Auth : 인증 발급 기관
• Person : 발급 받는 사람
• Random : 사용자 고유 랜덤 번호
• Certificate Version : 인증서 버전
• Certification Level : 인증 레벨
• Previous Block Hash : 이전 블록 해시값
• Sign Hash : 개인키로 암호화한 디지털 서명 내용의 해시값
• Block Create Time : 블록 생성 시간
• Nonce : 임의의 넌스값



<그림 4> 인증체인 - 블록

• Block Hash : 블록헤더와 거래 정보의 해시값
• Block Header : 블록구조와 동일
• Sign Info : 디지털 서명 정보
• Etc Info : 블록 내에 있는 정보 중에서 블록 헤더와 서명 정보에 해당하지 않는 정보를 말하며, 블록 해시 계산에 사용되지 않음



<그림 5> 인증체인 - 체인

(2) 블록인증서

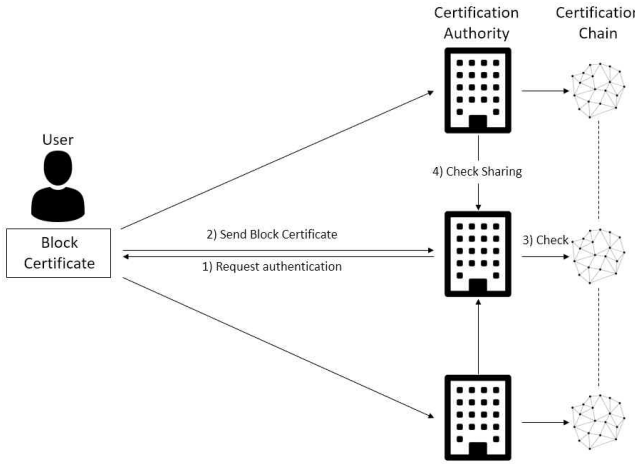
사용자가 가지고 있는 블록인증서(디지털 서명)의 정보는 다음과 같다. 인증체인의 Sign Info부분을 모두 가지고 있다. 블록을 이루는 Sign Hash값과 공개키, 체인 번호, 블록 번호 등을 가지고 있으며 사용자의 개인키로 암호화되어 사용자만이 가지게 된다.

<그림 6> 블록 인증서

2. 알고리즘

(1) 인증체인

1) 사용자 개인키 생성



<그림 7> 블록인증 시스템 전체 구조도

사용자는 자신의 비밀키와 공개키를 생성해야 한다. 비밀키는 오로지 사용자 자신만이 알 수 있으며, 공개키는 인증체인의 Sign Info를 암호화할 때 사용되고, 인가된 기관만이 인증정보를 가질 수 있도록 블록인증서에 기록된다.

2) 블록 헤더

Certificate Version은 인증서 버전을 의미한다. 기본 필드이며 하드포크를 통한 펌웨어 업그레이드 시 필드값이 변한다. Certification Level은 인증 레벨을 의미한다. 인증체인에 등록된 Sign Info의 수준을 얘기하며, 높을수록 범용에 가깝다. Sign Hash는 디지털 서명의 주요 내용을 사용자의 공개키로 암호화한 값을 해시를 통하여 얻은 해시값이다. 다음 블록에 영향을 주며, 해시값의 비교에 쓰인다. Previous Block Hash는 이전 블록의 기타 정보를 제외한 해시 값을 받아온다. Block Create Time은 해당 서명을 블록화하는 시점의 시간을 기록한다. 인증서의 유효기간을 확인할 때 주로 쓰인다. Nonce는 임의의 넌스값이다. 체인의 위·변조를 막기 위해서 추가한 필드값이다.

3) 블록 생성

하나의 블록 헤더가 만들어지면 블록을 생성한다. 하나의 블록은 Block Index, Block Hash, Block Header, Sign Info, Etc Info로 구성된다. Block Index는 블록의 번

호를 의미하며, 블록인증서로 올바른 사용자의 블록을 찾아가기 위해 사용된다. Block Hash는 Etc Info를 제외한 모든 데이터의 해시값이다. 무결성을 검증하고 다음 블록 생성에 관여하기 때문에 위·변조를 방지하는 역할을 한다. Sign Info는 블록 헤더를 만들 때 사용된 모든 디지털 서명 정보와 동일하다.

4) 체인 생성

생성된 블록들은 시간의 흐름에 따라 순차적으로 이어지며 작업증명을 통해 유효성 검사를 통과한 블록들은 정해진 주기마다 하나의 체인으로 결합하여 완성된다. 2번의 컨펌을 통하여 인증체인을 완성한다. 완성된 체인은 신뢰기관 및 인증기관들이 모두 가지고 있을 수 있다.

(2) 사용자 인증

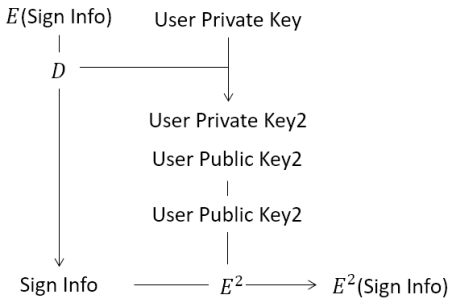
사용자의 인증이 요구될 때 블록인증서의 소유자는 자신의 블록인증서를 아래 <그림 8>과 같이 사용자의 개인키로부터 파생된 개인키로 블록인증서를 암호화하여 파생된 공개키와 함께 전송한다. 인증을 요구하는 기관뿐만 아니라 다른 신뢰기관으로의 유효성을 입증받기 위해 블록인증서를 공유하게 되므로 파생된 공개키가 사용된다.

인증을 요구한 기관은 암호화된 디지털 서명을 복호화하여 디지털 서명 정보를 알아낸다. 디지털 서명에 기록된 체인 번호와 블록 번호를 추적하여 블록 정보에 접근한다. 디지털 서명에 적힌 공개키로 디지털 서명의 일부 정보를 암호화하고 인증 체인에서 사용한 해시값을 만든다. 그리고 인증 체인 블록 헤더부분의 해시값과

비교하여 무결성을 입증한다. 이 과정을 통과하면 인증체인에 기록된 보안 레벨에 따라 사용자의 접근권한이 달라지며 인증의 유효성을 가진다. 인증기관 및 신뢰기관과의 인증 성공률이 51%이상일 때, 사용자의 인증이 성공한다.

(3) 인증서 폐기

인증서 폐기는 인증체인이 아닌 인증폐기체인에서 이루어진다. 인증폐기체인에 폐기된 블록인증서 정보를 추가한다. 인증체인에서 생성된 Sigh Hash값이 인증폐기체인의 주요 정보이며, 해시값의 비교를 통해서 빠르게 폐기된 블록인증서임을 찾



<그림 8> Sign Info 재가공

아낼 수 있다.

블록인증서는 생성시간을 기준으로 유효기간을 가지고 있기 때문에 오랜 시간이 지난 인증체인은 유효성검사에 영향을 주지 않는다. 따라서 블록인증시스템의 인증체인 중 일정 기간이 지난 인증체인의 부분은 머클트리값만 남기고 데이터를 파기할 수 있다.

3. 블록인증 시스템 공유 문제

(1) 법・제도

기존 공인인증시스템은 별도의 공인인증기관과 최상위공인인증기관을 통하여 인증과 발급을 수행하였다. 한정된 신뢰기관에서만 인증과 발급을 수행할 수 있게 정부에서 규정하였다. 블록인증 시스템아 적용되려면 한정된 신뢰기관이 아닌 인증이 필요한 기관을 신뢰해야한다. 일정 보안 수준을 갖춘 기관에 대해서 인증체인을 공유하고, 보안 레벨을 점검하여 타 기관과의 인증 요청 수준을 규정해야할 것이다.

(2) 노드 분산

블록인증시스템은 여러 노드의 검증을 필요로 한다. 인증을 필요로 하는 기관에서 다른 인증기관으로의 검증을 수행할 노드들을 찾고 선택하는 분산과정이 필요하다. 노드 선택 우선순위는 다음과 같다.

① 검색된 노드를 보안 수준에 따라 분류
② 보안 수준 별로 나뉜 노드들의 인증 수행 속도에 따라 인증 요청을 보냄
③ 모든 노드의 사용자 인증 성공률이 51% 이상일 때, 사용자 인증을 정상적

으로 마침
④ 만약 51%의 성공률을 넘지 못했을 때, 사용자 인증을 실패했음을 알림

4. 공인인증서와 블록인증서 비교

공인인증서와 블록인증서의 주요 사항 비교표는 다음과 같다.

	공인인증서	블록인증서
등록 기관	공인인증 등록기관(RA)	신뢰기관(보안 수준 별 상이)
인증 기관	공인인증 인증기관(CA)	모든 신뢰기관
서비스 기관	인증서 구분에 따른 서비스 제공	모든 신뢰기관
저장	PC, Mobile, Token, etc.	PC, Mobile, Token, etc.
유효기간	1년	2~3년
폐기	인증서 폐기 목록(CRL)	인증 폐기 체인(CRC)

<표 1> 공인인증서와 블록인증서 비교

(1) 등록 및 인증

공인인증서는 등록기관(RA)과 인증기관(CA)이 다르다. 공인인증서는 정부에서 지정한 등록기관(RA)에서만 사용자 등록 및 인증서 발급 요청을 할 수 있다. 사용자가 등록기관에 발급요청을 하면 등록기관은 인증기관에 인증서 발급요청을 보내어 인증서를 발급하는 과정을 거친다.

블록인증서는 등록기관과 인증기관이 동일하다. 블록인증서의 발급과 인증은 높은 보안 수준을 가진 신뢰기관에서 가능하다. 신뢰 기관은 디지털 서명들을 생성하여 블록으로 만든다. 생성된 블록은 다른 노드들과의 유효성 입증을 통해 인증체인으로 만들어진다.

공인인증서와 비교했을 때, 등록 및 인증 과정을 한 번에 진행하여 인증 시스템의 효율성을 높이고 여러 개의 신뢰노드들의 유효성을 통해 블록인증서가 완성되므로 정보의 무결성을 증명한다. 인증체인을 만들면서 모든 신뢰노드들이 같은 인증체인을 공유하기 때문에 어느 노드에서도 사용자가 서비

스를 이용할 수 있도록 인증할 수 있다.

(3) 서비스 기관

공인인증서는 개인, 은행, 범용 등 인증서의 역할별 구분이 나누어져있다. 따라서 특정 서비스를 이용하기 위해서는 해당 구분을 가진 공인인증서가 필요하거나 타 기관에서 발급된 공인인증서를 등록해야한다. 하지만 블록인증서는 모든 신뢰기관들이 동일한 인증체인을 가지고 있고, 신뢰 네트워크를 구성하고 있기 때문에 네트워크를 구성하고 있는 모드 노드들은 인증을 통해 서비스를 제공할 수 있다.

(4) 저장

공인인증서는 특정 SW를 통해서 공인인증서를 관리한다. PC, Mobile, Token 등의 저장매체를 지원한다. 블록인증서는 특별한 SW없이 인증서를 관리할 수 있다. 공인인증서는 클라이언트단의 인증을 지원하지만 블록인증서는 서버단의 인증만을 지원한다. 기존 클라이언트단의 인증을 지원하게 되면, 악의적인 공격에 쉽게 노출되기 때문이다.

(5) 유효기간

공인인증서는 사용 구분에 관계없이 1년의 유효기간을 가지고 있다. 따라서 공인인증서는 1년마다 재발급, 갱신을 통해 새로운 인증서를 발급 받아야 한다. 이에 반해 블록인증서는 2~10년의 유효기간을 가지고 블록인증서를 발급받을 때 사용자가 유효기간을 선택할 수 있다. 블록인증서는 공인인증서보다 높은 보안수준의 신뢰 노드에서 이루어지기 때문에 긴 유효기간을 할당할 수 있다. 또한 인증서 재발급 불편을 없애기 위해서 기존 유효기간보다 선택의 폭을 넓혔다. 최대 10년의 유효기간이 끝난 인증체인의 부분은 사용하지 않기 때문에 머클트리의 루트해시값으로 압축하여 인증체인의 크기를 줄인다. 이는 인증체인 데이터가 무한정 커지는 것을 방지한다.

Ⅴ. 결론 및 향후 연구 방향

1. 결론

블록인증서는 블록체인을 통해 보안의 세 가지 요소를 모두 충족시키게 된다. 신뢰 기관과 인증을 요구하는 수많은 기관이 인증체인을 공유하고 비교하기 때문에 위·변조가 일어날 수 없다. 또한 공인인증서를 가동하기 위해 별도의 프로그램이 필요하지 않고, 단순히 디지털 서명을 검증하는 과정뿐만 아니라 인증체인을 가진 여러 신뢰기관의 인증을 받기 때문에 기밀성, 무결성, 가용성을 모두 충족하게 된다. 하지만 기존의 공인인증서와 동일하게 인증서가 유출되거나 유실되는 경우가 존재한다. 이를 해결하기 위해서는 보안토큰의 사용이 권장된다.

2. 향후 연구 방향

블록인증시스템을 본 논문을 통해 이론적으로 기술하였다. 실제 공인인증시스템을 대체할 시스템이 되기 위해서는 적용 과정이 필요하고, 이를 인증서 발급, 인증서 처리 속도 등 다양한 연구를 통해 증명할 것이다.

공인인증서의 강제 사용으로 이미 국내 보안 기술 시장은 이와 관련된 선의의 경쟁조차 없었으며, 독과점 상태로 인하여 위축된 보안 시장에 변화와 혁신이 필요하다는 것을 알려야 한다. 사용자의 인증이 보안의 중요 요소 중 하나인 것을 기억하며, 앞으로 더 발전된 기술이 시장에 등장하여 인증 시장이 활성화되기를 기대한다.

참고문헌

[1] 박정호, “블록체인 산업 현황 및 동향”, 정보통신산업진흥원, 제4차 산업혁명과 소프트파워 이슈리포트 2018-제17호

[2] 이제영, “블록체인(Blockchain) 기술동향과 시사점”, 과학기술정책연구원, 동향과 이슈, 2017.7.25. 제34호, ISSN 2383-6458

[3] 한겨레, 공인인증서 20년만에 폐지…기존 인증서는 계속 쓸 수 있어[Internet], Available: http://www.hani.co.kr/arti/economy/it/838222.html, 2018.03.29.

[4] 미국 국립표준기술 연구소(NIST), 전자인증 가이드라인(Electronic Authentication Guideline)(2006), 제39면

[5] 바젤위원회(BCBS), 전자금융 위험관리 원칙(Risk Management Principles for Electronic Banking) 중, 제4원칙

[5] 보안뉴스, [시큐리티 Q&A] 공인인증서와 ActiveX 보안문제 개선방향[Internet], Available:https://www.boannews.com/media/view.asp?idx=40931, 2014.05.12.

[6] 보안뉴스, 최근 5년간 유출된 공인인증서 8만 건 넘었다[Internet], Available: https://www.boannews.com/media/view.asp?idx=57632&kind=1&search=title&find=%B0%F8%C0%CE%C0%CE%C1%F5%BC%AD+%C0%AF%C3%E2, 2017.10.23.

[7] Vitalik Buterin, “차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼”