2021년도
학사학위논문

블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션 제안

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

2021년 11월 30일

순천향대학교 공과대학
정보보호학과

박현성

2021년도
학사학위논문

블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션 제안

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

2021년 11월 30일

순천향대학교 공과대학
정보보호학과

박현성

블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션 제안

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

지도교수 유 일 선

이 논문을 공학사학위 논문으로 제출함

2021년 11월 30일

순천향대학교 공과대학
정보보호학과

박현성

박 현 성 의 공학사학위논문을 인준함

2021년 11월 30일

심 사 위 원 유 일 선 인
심 사 위 원 염 흥 열 인
심 사 위 원 임 강 빈 인
심 사 위 원 이 선 영 인
심 사 위 원 김 태 근 인

순천향대학교 공과대학

정보보호학과

차 례

표 차 례

그 림 차 례

초 록

최근 탈중앙화 기술인 블록체인의 산업 적용이 활발하게 이루어지고 있다. 블록체인 기술은 하나의 네트워크에서 각 노드 또는 참여자 간 공유하는 디지털 원장(합의 데이터)을 의미한다. 블록체인 네트워크에서 트렌젝션이 발생할 때, 구성원들의 합의과정을 통해 해당 거래를 인증하고, 블록체인에 기반을 둔 거래 정보는 임의로 변경할 수 없으므로 거래의 신뢰성이 높고 정보 추적에 쉽다는 장점들이 있다. 또한, 이를 바탕으로 4차 산업혁명의 핵심기반 기술로 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.

주요어 : 인증, 공인인증, 공인인증서, 탈중앙화, 블록 인증서, 블록인증, 블록체인, 인증 체인

제 1 장 서 론

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 인증시스템을 통합하는 과정을 통해 신뢰성을 더욱 높일 수 있다. 본 논문에서는 공인인증서의 새로운 시대를 위해 블록체인의 유효성 검사 기법을 이용한 블록인증시스템 보안 솔루션을 제안한다.

제 2 장 공인인증서와 블록체인

제 1 절 공인인증서

(1) 개요

국내 인터넷 금전거래를 이용할 때 인증을 위해 필요한 전자서명으로, X.509 v3 공개키 기반구조 인증서를 생성한다. 최상위인증기관인 RA와 공인인증기관인 CA가 존재하며 가입자 인증서 검증을 수행한다.

(2) 저장 위치와 저장방법

공인인증서의 주요 저장 매체로는 보안토큰, 스마트카드나 저장 매체, 휴대전화 등이 있으며, 공인인증서 전용 소프트웨어를 통해 공인인증서를 발급하거나 이용할 때 공인인증서를 저장할 수 있도록 지원된다. 공인인증서를 저장할 때 사용하는 PC 자체의 디스크나 이동식 디스크(USB, SD카드)를 많이 사용하고 있으나, 이는 국가에서 권고하고 있는 저장 매체가 아닐뿐더러, 악성코드에 의한 공인인증서 유출 등의 문제로 인해 보안이 적용된 저장 메체에 공인인증서 저장을 권고한다.

(3) 인증

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

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

(4) 문제점

1. 공인인증서 저장 문제

공인인증서를 PC 또는 저장 매체에 저장할 때 기본적으로 NPKI 폴더에 저장되고 있으므로 다음과 같은 문제점이 도출된다.

• 이용자들은 Active X나 별도 프로그램을 공인인증서를 사용하기 위해 설치해야 함에 따른 위험
• 단순히 복사 및 붙여넣기를 통해 이용자의 인증서 개인키가 쉽게 복제, 유출됨
• 세계 시장에서 권고하는 보안 수준을 따라가지 못하거나, 제한적인 인터넷 환경 발생

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 애플리케이션 등 다른 프로그램들을 누구나 쉽게 설치할 수 있다는 것이 문제가 되고 있다. KISA에서는 다음 문제를 인식하여 보안토큰 이용 권고를 하고 있지만, 보안토큰을 이용하는 국내 사용자는 드물다.

2. 국제 공인인증 문제

국내 최상위 공인인증기관 KISA는 국내 한정 인증기술로 국외적으로 신뢰받지 못하고 있다. 따라서 다음과 같은 상황이 발생하였다.

• 서버인증에 사용될 수 없음
• 국내 공인인증 기술을 국외 서비스에 적용하거나 국외 진출이 불가능함

미국 국립표준기술 연구소(NIST)에서 공개한 전자인증 지침(Electronic

Authentication Guideline)에 의하면, 전자파일 형태로 배포된 인증서(Soft crypto token), 즉 공인인증서와 같은 파일 형태의 인증서가 가지는 보안 강도는 매우 위험하다고 평가하였다.

Table 2. Token Types Allowed at Each Assurance Level

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

[그림 1]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 공격으로 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. 웹브라우저나 일반적인 통신 기능을 위해서 별도의 보안 프로그램을 설치하게끔 한다. 이는 사용자의 불편함만을 호소하게 하며, 또한 보안 프로그램을 설치하면서 관리자 권한을 위임하여 보안 문제를 일으키는 모순이다.

(5) 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.

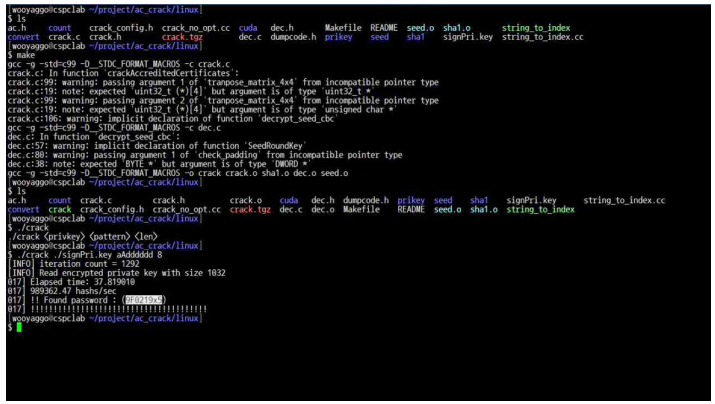
구분	'10년	'11년	'12년	'13년	'14년	'15년	'16년	합계
유출건수	0	0	8	8,710	41,733	22,796	6,850	80,097

[그림 2] 공인인증서 유출 현황(KISA)

더욱이 공인인증서가 유출되면 디지털 서명 정보의 위·변조가 불가피하며, 유출된 공인인증서는 악의적인 목적을 가지고 사용될 수 있다.

2. 공인인증서 비밀번호 탈취

공인인증서의 유출은 비밀번호를 탈취하고 악의적인 이용으로 이어진다. 공인인증서는 두 개의 파일로 구성되어있다. 하나는 공개키 파일이며 나머지 하나는 암호키 파일이다. 일반적으로 국내 공인인증서의 암호는 8자리 이상의 대소문자 영문, 기호, 숫자 등으로 구성되어있다. 최근 특수문자를 필수적으로 포함하여 암호를 설정한다. 하지만 기존의 쉬운 패턴의 암호는 보안전문가에 의해 불과 몇 분 만에 탈취할 수 있었다. 현재 공인인증서에 사용되는 이러한 방식은 보안에 있어서 큰 취약점을 가지고 있다.



[그림 3] 공인인증서 비밀번호 탈취 화면

제 2 절 블록체인 네트워크(Blockchain Network)

블록체인은 최근 등장한 데이터 분산 처리 기술로써, 네트워크에 참여하는 모든 사용자가 상호 간 발생하는 거래 명세 등의 데이터를 분산하고 저장하는 기술을 의미한다. 블록들을 체인 형태로 묶은 형태로, 블록체인에서 '블록'에 해당하는 부분은 개인과 개인의 거래(P2P)가 이루어진 데이터가 기록되는 장부가 된다. 형성된 블록들은 시간순으로 차례대로 연결된 '체인'의 구조를 가지게 된다. 모든 노드가 거래 내역을 보유하고 있으므로 거래 내역을 확인할 때 모든 사용자가 보유한 장부를 비교하고 확인해야 한다. 이런 특징으로 블록체인은 '공공 거래장부' 또는 '분산 거래장부'로도 불리기도 한다.

[그림 4] 블록체인 거래 과정 개념도

블록체인은 무한히 확장 가능한 분산 공개 장부이며, 해당 데이터 안에 포함된 개별 거래는 모두 디지털 서명이 이루어져 있으므로 시중 은행이나 제3자의 개입이 없어도 진본임을 보증할 수 있다. 수천, 수만 개의 노드에 분산된 공개 체인 데이터들은 갑작스러운 장애나 공격이 발생하더라도 블록체인이라는 네트워크 전체는 영향을 받지 않는다.

블록체인의 장점으로 크게 4가지가 있다. 먼저 블록체인 기술은 데이터와 키를 암호화된 상태로 전송되므로 일반적인 보안성을 높일 수 있다. 새로운 블록은 기존의 블록은 머클트리라는 구조에 의해 상호관계를 형성하므로 전체 블록 안의 데이터 변조와 탈취를 할 수 없다. 이는 각각의 참여 노드의 분산화로 해킹이 불가능하다. 두 번째로 거래의 인증 및 증명과정에서 제3자를 제외하고 사용자 상호 간의 거래가 이루어지므로 거래 기록에 대한 신뢰성 확보와 거래의 효율성, 속도가 향상된다. 또한, 분산원장 기술로 오류를 최소화할 수 있어 거래의 정정과 수정을 위한 시간이 감소한다. 세 번째로 거래 데이터를 저장하거나 인증을 위한 중앙 서버와 집중화된 시스템이 필요하지 않으므로 거래 비용 감소로 이어진다. 거래 정보가 분산되어 있어 해킹의 위험으로부터 보호한다. 마지막으로 네트워크 참여자들의 실시간 거래 모니터링이 가능하다. 따라서 투명성과 부인 방지의 기능을 할 수 있다.

(1) 퍼블릭 블록체인(Public Blockchain)

퍼블릭 블록체인(Public Blockchain)은 누구나 접속할 수 있는 블록체인으로 인터넷에 연결된 기기라면 종류에 상관없이 몇 가지 컴퓨터 장비를 이용하여 블록체인 네트워크에 참여할 수 있다. 즉 개방형 네트워크 또는 퍼블릭 네트워크 그룹이라고도 한다. 네트워크의 참여 주체가 불분명하므로 일종의 보상제도인 코인(또는 토큰)을 발행하여 운영된다. 퍼블릭 블록체인 네트워크 참여자의 각각 '노드(node)'라고 부르는데, 각 노드들은 블록체인에 데이터를 공유하여 저장하고, 새로운 블록을 검증하고 합의할 수 있는 능력을 갖춘다. 각각의 노드들은 시간과 장소에 상관하지 않고 네트워크의 참여와 탈퇴 할 수 있으며, 블록체인 네트워크에 참여 또는 탈퇴하는 것은 다른 노드들의 승인이 필요 없고, 각각의 노드 참여자가 표현하는 의사에 따라 결정한다. 퍼블릭 블록체인의 경우 참여자들의 합의 과정에서 발생하는 전기료나 운영비용을 감당할 수 있도록, 암호화폐라는 가치를 발행하여 보상하며 수수료를 받는다.

퍼블릭 블록체인의 장점은 다수 익명의 참여로 인해 투명성이 강화된 모델

이며, 많은 노드에 의해 보안성이 증가하였다. 단점으로는 불특정 참여자에 의해 합의가 진행되고 네트워크상의 노드들의 동기화가 이루어져야 하므로 속도가 느리다. 또한, 참여가 자유로워서 인증 안된 참여자들도 악의적인 목적을 가진 해커도 퍼블릭 블록체인에 접근할 수 있다.

대표적으로 비트코인, 이더리움, 비트코인캐시, 모네로 등이 있으며 이들이 사용하는 대표적인 합의 알고리즘은 작업 증명, 지분증명, 위임지분증명 등이 있다.

(2) 프라이빗 블록체인(Private Blockchain)

프라이빗 블록체인(Private Blockchain)은 조직적이고 제한적으로 허가를 받은 사람들에 의하여 운영되는 블록체인이다. 블록체인의 운영과 참여와 같은 활동의 주체가 정해져 있으므로 퍼블릭 블록체인과 같은 보상은 받지 않는다. 블록체인의 데이터를 읽거나 작성, 합의 과정을 진행하는 노드가 미리 지정되어 있고 필요에 따라 노드의 수를 늘리거나 줄임으로써 공공기관이나 금융기관 같은 조직에서 사용하기 쉽다.

프라이빗 블록체인의 장점은 인가된 소수의 노드만이 참여하기 때문에 기밀성 측면에서 높은 보안성을 보여주며, 비교적 적은 노드들을 보유하므로 트랜잭션 속도가 빠르다. 하지만 이는 곧 단점으로 꼽히며 적은 수의 노드들에 의해 합의가 진행되기 때문에 데이터의 중앙집권화가 이루어질 수 있다..

대표적인 블록체인으로는 Hyper ledger fabric, R3, CRODA 등이 있으며 이들이 사용하는 대표적인 합의 알고리즘은 PBFT(Practical Byzantine Fault Tolerance) 등이 있다.

(3) NFT(Non-fungible Token)

NFT(Non-fungible Token)는 대체 불가능 토큰이라고 불리며, 기존 블록체인 기술을 응용하여 만들어진 가상자산이다. 기존 블록체인은 디지털상에서 화폐의 가치를 가진 암호화폐의 거래 기록에 불과하다면, NFT는 하나의 데이터로 고유한 데이터 값을 가지고, 그것을 포함한 유일한 데이터다. NFT를

발행하면 해당 데이터의 소유권, 생성일시, 거래 이력이 생성된다. 일종의 '디지털 데이터의 정품 인증서'라고 할 수 있다. NFT를 활용한 서비스들이 급격하게 증가하면서 앨범 사진과 동영상, SNS의 글을 모티브로한 서비스가 등장하였다. 최근에는 국내 게임사에서 NFT를 활용한 모바일 게임을 출시하거나 캐릭터를 생성하여 활용하고 있다. 이는 본 논문에서 제안한 블록인증시스템의 결점을 보완할 수 있다.

위조가 어려움	복제가 어려우므로 데이터나 작품의 희소성을 보호하며, 위조품이 발생하여 문제가 발생하지 않기 위해 거래 추적이 가능함
추적하기 쉬움	블록체인 데이터는 블록체인 네트워크의 종류에 따라 투명하므로 데이터 출처, 발행 시간, 소유자, 거래내용과 같은 기타 정보를 볼 수 있음
부분에 대한 소유권 인정	NFT의 공동 소유권을 인정하기 때문에, 여러 명의 구매자가 동등한 소유권한을 가짐
순환 증가	NFT는 한번 거래가 끝난 이후에도 계속해서 거래할 수 있음 이를 이용하여 게임 아이템 등과 같은 경매 시스템에도 도입됨

[표 1] NFT 장점

제 3 장 블록인증시스템 보안 솔루션 제안

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

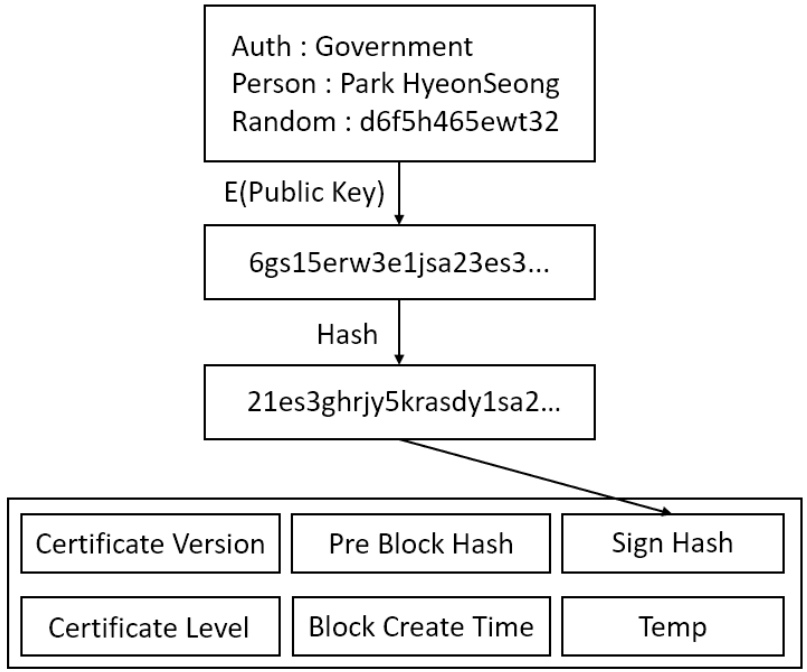
제 1 절 구조

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

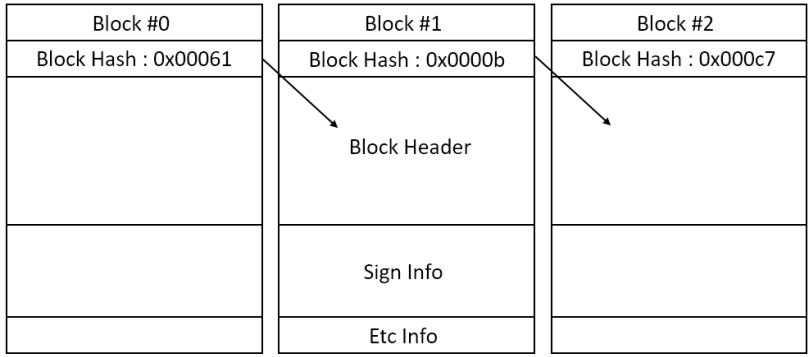
(1) 인증 체인

인증 체인의 구조는 다음과 같다.

- Auth : 인증 발급 기관
- Person : 발급받는 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
- Block Hash : 블록 헤더와 거래 정보의 해시값
- Block Header : 블록구조와 동일
- Sign Info : 디지털 서명 정보
- Etc Info : 헤더와 서명 정보에 해당하지 않는 나머지 기타 정보에 해당하며 이후 블록 생성에 관여하지 않음



[그림 5] 인증 체인 - 블록



[그림 6] 인증 체인 - 체인

(2) 블록인증서

사용자가 가지고 있는 블록 인증서(디지털 서명)의 정보는 다음과 같다. 인증 체인의 Sign Info 부분을 모두 가지고 있다. 블록을 이루는 Sign Hash 값과 공개키, 체인 번호, 블록 번호 등을 가지고 있으며 사용자의 개인키로 암호화되어 사용자만이 가지게 된다.

[그림 7] 블록인증서

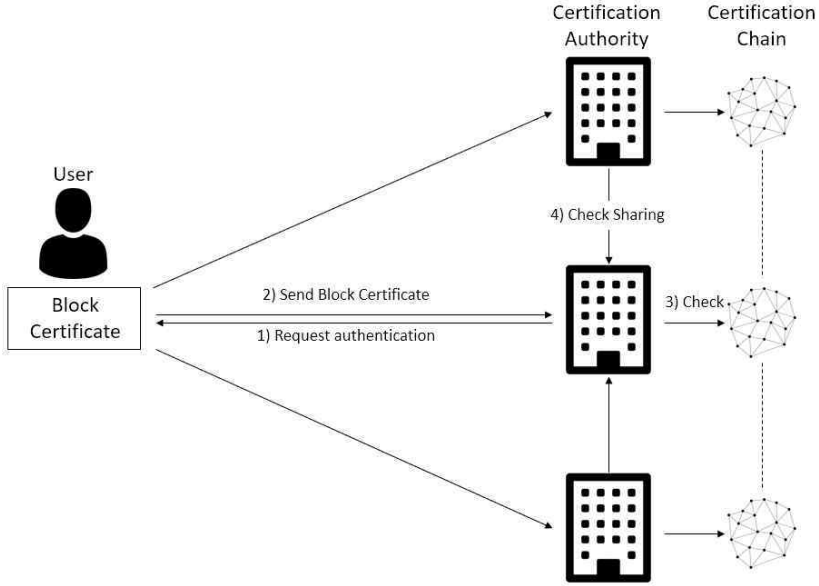
제 2 절 알고리즘

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

(1) 인증 체인

1. 사용자 개인키 생성

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



[그림 8] 블록인증 시스템 전체 구조도

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, 해시값

의 비교에 쓰인다. Previous Block Hash는 이전 블록의 기타 정보를 제외한 해시값을 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 필드 값이다.

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 번호를 의미하며, 블록 인증서로 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 같다.

4. 체인 생성

생성된 블록들은 시간의 흐름에 따라 차례대로 이어지며 작업 증명을 통해 유효성 검사를 통과한 블록들은 정해진 주기마다 하나의 체인으로 결합하여 완성된다. 2번의 컨펌 과정을 통하여 인증 체인을 완성한다. 완성된 체인은 신뢰기관이나 인증기관들이 모두 가지고 있을 수 있다.

(2) 사용자인증

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

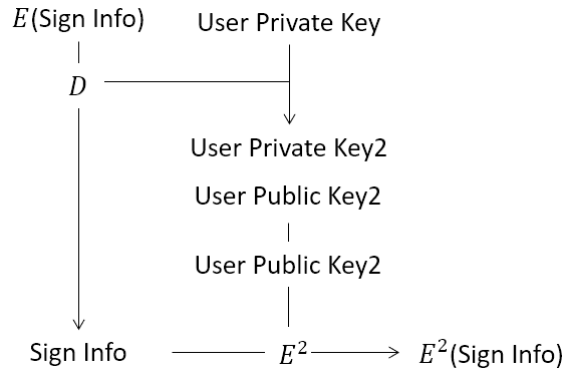
인증을 요구한 기관은 암호화된 디지털 서명을 복호화하여 디지털 서명 정보를 알아낸다. 디지털 서명에 기록된 체인 번호와 블록 번호를 추적하여 블

록 정보에 접근한다. 디지털 서명에 적힌 공개키로 디지털 서명의 일부 정보를 암호화하고 인증 체인에서 사용한 해시값을 만든다. 그리고 인증 체인 블록 헤더 부분의 해시값과 비교하여 무결성을 입증한다. 이 과정을 통과하면 인증 체인에 기록된 보안 레벨에 따라 사용자의 접근 권한이 달라지며 인증의 유효성을 가진다. 인증기관 및 신뢰기관과의 인증 성공률이 51% 이상일 때, 사용자의 인증이 성공한다.

(3) 인증폐기 체인

인증폐기는 인증 체인이 아닌 인증폐기 체인에서 이루어진다. 인증폐기 체인에 폐기된 블록 인증서 정보를 추가한다. 인증 체인에서 생성된 Sigh Hash 값이 인증폐기 체인의 주요 정보이며, 해시값의 비교를 통해서 빠르게 폐기된 블록 인증서임을 찾아낼 수 있다.

블록 인증서는 생성시간을 기준으로 유효기간을 가지고 있으므로 오랜 시간이 지난 인증 체인은 유효성 검사에는 영향을 주지 않는다. 따라서 블록인증시스템의 인증 체인 중 일정 기간이 지난 인증 체인의 부분은 머클트리값만 남기고 데이터를 파기할 수 있다.



[그림 9] Sign Info 재가공

제 3 절 블록인증 시스템 공유 문제

(1) 법과 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 신뢰해야 한다. 일정 보안 수준을 갖춘 기관에 대해서 인증 체인을 공유하고, 보안 레벨을 점검하여 타 기관과의 인증요청 수준을 규정해야 할 것이다.

(2) 노드 분산

블록인증시스템은 여러 노드의 검증이 필요하다. 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 수준별로 나뉜 노드들의 인증 수행 속도에 따라 인증요청을 보냄

③ 모든 노드의 사용자인증 성공률이 51% 이상일 때, 사용자인증을 정상적으로 마침

④ 만약 51%의 성공률을 넘지 못했을 때, 사용자인증에 실패했음을 알림

제 4 절 공인인증서와 블록 인증서 비교

공인인증서와 블록 인증서의 주요 사항 비교표는 다음과 같다.

	공인인증서	블록 인증서
등록기관	공인인증 등록기관(RA)	신뢰기관(보안수준별 상이)
인증기관	공인인증 인증기관(CA)	모든 신뢰기관
서비스 기관	인증서 구분에 따른 서비스 제공	모든 신뢰기관

저장	PC, Mobile, etc.	PC, Mobile, Token, etc.
유효기간	1년	2~3년
폐기	인증서 폐기 목록(CRL)	인증폐기 체인(CRC)

[표 2] 공인인증서와 블록 인증서 비교

(1) 등록 및 인증

공인인증서는 등록기관(RA)과 인증기관(CA)이 다르다. 공인인증서는 정부에서 지정한 등록기관(RA)에서만 사용자 등록 및 인증서 발급요청을 할 수 있다. 사용자가 등록기관에 발급요청을 하면 등록기관은 인증기관에 인증서 발급요청을 보내어 인증서를 발급하는 과정을 거친다. 블록 인증서는 등록기관과 인증기관이 같다. 블록 인증서의 발급과 인증은 높은 보안 수준을 가진 신뢰기관에서 가능하다. 신뢰기관은 디지털 서명들을 생성하여 블록으로 만든다. 생성된 블록은 다른 노드들과의 유효성 입증을 통해 인증 체인으로 만들어진다. 공인인증서와 비교했을 때, 등록 및 인증과정을 한 번에 진행하여 인증시스템의 효율성을 높이고 여러 개의 신뢰 노드들의 유효성을 통해 블록인증서가 완성되므로 정보의 무결성을 증명한다. 인증 체인을 만들면서 모든 신뢰 노드들이 같은 인증 체인을 공유하기 때문에 어느 노드에서도 사용자가 서비스를 이용할 수 있도록 인증할 수 있다.

(2) 서비스 기관

공인인증서는 개인, 은행, 범용 등 인증서의 역할별 구분이 나누어져 있다. 따라서 특정 서비스를 이용하기 위해서는 해당 구분을 가진 공인인증서가 필요하거나 타 기관에서 발급된 공인인증서를 등록해야 한다. 하지만 블록 인증서는 모든 신뢰기관이 같은 인증 체인을 가지고 있고, 신뢰 네트워크를 구성하고 있어서 네트워크를 구성하고 있는 모든 노드는 인증을 통해 서비스를 제공할 수 있다.

(3) 저장

공인인증서는 특정 SW를 통해서 공인인증서를 관리한다. PC, Mobile, Token 등의 저장 매체를 지원한다. 블록 인증서는 특별한 SW 없이 인증서를 관리할 수 있다. 공인인증서는 클라이언트 단의 인증을 지원하지만, 블록 인증서는 서버 단의 인증만을 지원한다. 기존 클라이언트 단의 인증을 지원하게 되면, 악의적인 공격에 쉽게 노출되기 때문이다.

(4) 유효기간

공인인증서는 사용 구분과 관계없이 1년의 유효기간을 가지고 있다. 따라서 공인인증서는 1년마다 재발급, 갱신을 통해 새로운 인증서를 발급받아야 한다. 이에 반해 블록 인증서는 2~10년의 유효기간을 가지고 블록 인증서를 발급받을 때 사용자가 유효기간을 선택할 수 있다. 블록 인증서는 공인인증서보다 높은 보안 수준의 신뢰 노드에서 이루어지기 때문에 긴 유효기간을 할당할 수 있다. 또한, 인증서 재발급 불편을 없애기 위해서 기존 유효기간보다 선택의 폭을 넓혔다. 최대 10년의 유효기간이 끝난 인증 체인의 부분은 사용하지 않기 때문에 머클트리의 루트해시값으로 압축하여 인증 체인의 크기를 줄인다. 이는 인증 체인 데이터가 무한정 커지는 것을 방지한다.

제 4 장 결론 및 향후 연구 방향

제 1 절 결론

블록 인증서는 블록체인을 통해 보안의 세 가지 요소를 모두 충족시키게 된다. 신뢰기관과 인증을 요구하는 수많은 기관이 인증 체인을 공유하고 비교하기 때문에 위·변조가 일어날 수 없다. 또한, 공인인증서를 가동하기 위해 별도의 프로그램이 필요하지 않고, 단순히 디지털 서명을 검증하는 과정뿐만 아니라 인증 체인을 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.

최근 NFT의 이용이 급증하면서, 위조 불가 토큰의 개념이 진화하고 있다. 본 논문에서 제안한 블록 인증서의 모습은 NFT와 유사하며, 정해진 주체에 의해서만 발행되지만 발행하기 위해서 개인의 동의나 키를 발급받아 이용하여야 한다. 블록체인이나 NFT 모두 해당 네트워크의 결집도와 신뢰도에 의해 보안이 결정되기 때문에 오랫동안 유지되고 있고 퍼블릭으로 운영되는 블록체인 네트워크에서의 신뢰도가 가장 높다고 할 수 있으므로 초당 거래속도를 보장하는 네트워크에서 블록 인증서의 도입을 권장한다.

제 2 절 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.

참 고 문 헌

[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”

Abstract

Recently, the industrial application of blockchain, a decentralized technology, has been actively carried out. Blockchain technology refers to a digital ledger (consensus data) shared between each node or participant in a single network. When a transaction occurs in the blockchain network, the transaction is authenticated through the consensus process of the members, and transaction information based on the blockchain cannot be changed arbitrarily, so the reliability of the transaction is high and information tracking is easy. In addition, based on this, it is attracting attention as a core technology of the 4th industrial revolution. At the same time, the policy of abolition of the existing accredited authentication system and Active X has been announced, and alternatives are required accordingly. However, since the existing public authentication system is an outdated technology that is difficult to keep up with the current security level, it must be changed through a fundamental change. The development and innovation of security technology through competition is necessary, and technology that does not lose its original purpose is required. Therefore, in this paper, we propose a block authentication system security solution using the blockchain validation technique that can identify the problems of existing public certificates and solve them.