https://doi.org/10.7840/kics.2022.47.10.1598

블록체인 기반 영지식을 활용한 개인정보 인증 구현

이 광 규◆

Implementation of Personal Information Authentication Using Blockchain-Based Zero Knowledge Proofs

Kwang-Kyu Lee◆

요 약

인증 프로세스는 사용자가 합법적인지 확인하는 데 사용되어야 하는 주요 단계이며, 사용자가 합법적인 사용자인지 확인하고 해당 사용자에게만 액세스 권한을 부여하는 데 사용되어야 한다. 최근에는 로그인 프로세스에 보안 계층을 추가하여 인증에 하나의 요소만 사용하는 취약점을 해결하기 위해 대부분의 애플리케이션에서는 이중인증과 OTP 체계를 사용하고 있지만, 이 방법도 허가 없이 사용자 계정에 액세스할 수 있는 방법이 알려져 보안에 취약하다. 본 논문에서는 최소한의 개인정보만을 노출 조건으로 사용자를 인증하는 블록체인의 Smart Contract 기반으로 영지식(ZKP:Zero Knowledge Proofs)개인정보 인증 기법을 구현한다. 이는 블록체인 기술을 기반으로 인증 프로세스에 많은 보안 기술을 제공하고, 개인정보 인증을 기존의 인증방식보다 빠르고 안전하게 수행할 수 있다.

Key Words : Blockchain, OTP(One Time Password), Two-Factor Authentication, Multi-Factor Authentication, ZKP(Zero Knowledge Proofs)

ABSTRACT

The authentication process is a key step that should be used to verify that a user is legitimate, and it should be used to verify that a user is a legitimate user and grant access only to that user. Recently, most applications use two-factor authentication and OTP schemes to address the vulnerability of using only one factor for authentication by adding a security layer to the login process, but this method also allows access to user accounts without permission. This is a known security vulnerability. In this paper, we implement the Zero Knowledge Proofs (ZKP) personal information authentication technique based on the smart contract of the block chain that authenticates the user with only minimal personal information exposure condition. It provides many security technologies to the authentication process based on blockchain technology, and can perform personal information authentication faster and more safely than existing authentication methods.

Ⅰ. 서 론

블록체인은 탈중앙화, 지속성, 익명성 및 감시 가능성을 기반으로 암호화폐, 금융 서비스, 위험 관리, 사물인터넷(IoT) 등공공 및 사회 서비스에 이르는 광범위한 분야에 응용되고 있다[1]. 하지만 블록체인 네트워크의 다양한 변형과 새로운 기술의 급속한 발전에도 불구하고 보안이 완벽하게 담보되고 있는지에 대해서는 논란의 여지가 있다. 블록체인 기술을 이용한 분야로는 비트코인, Smart Contract 인증, 보안 및

※ 본 논문은 2022년도 신한대학교 교내연구비에 의해 연구되었음
◆ First Author : Shinhan University Department of IT Convergence, kklee@shinhan.ac.kr, 정회원
논문번호 : 202205-104-C-RN, Received May 19, 2022; Revised August 8, 2022; Accepted August 12, 2022

P2P(Peer-to -Peer)분산 데이터 저장 기술로 발전하고 있다[2]. 하지만 위와 같은 기술은 보안상 문제가 대두되고, 대체인증으로 생체인증, SMS 인증, 온도 이미지 인식 등이 나왔으나, 이들 인증방식도 기술적 프로토콜 자체의 보안 취약성, 난수표 복제의 용이, H/W 기기의 분실에 대한 위험성, 생체정보의 훼손으로 인한 인식불능 등이 문제점으로 드러났다[3]. 따라서 여러 인터넷 서비스에서 더욱 효과적이고 신뢰할 수 있는 인증 시스템을 구현하는 인증이 필요하다. 패스워드 인증이 지금까지 많이 사용되었으나 패스워드기반의 사용자 인증은 보안상 취약점이 많아, 인증 보안 취약성을 개선하기 위해 SMS인증, OTP인증, 이중인증(Two-Factor Authentication), 다중인증(multi-factor authentication), 생체인증 등 대체 인증시스템으로 발전하였다. 하지만 이런 인증 기술도 더 안전한 인증, 생산성 향상, 신뢰증진을 위해 여러 범위에 걸쳐 설치하기에는 문제가 있었다. 그럼 기존의 인증 시스템이 어떤 문제점과 한계가 존재하는지 살펴보기로 하자.

첫 번째는 패스워드/아이디 인증이다. 패스워드는 사용자와 관리자로 분류되며, 우선 사용자 입장에서 너무 많은 패스워드, 점점 복잡해지는 패스워드, 주기적 변경이 필요한 패스워드 등의 문제점들을 가지고 있으며, 관리자 입장에서는 패스워드 관리와 보호를 위한 비용, 패스워드통제 불가능 등을 들 수 있다. 두 번째는 SMS 인증이다[4]. SMS 인증은 휴대폰으로 SMS 인증번호를 발송하고 수신된 인증번호를 입력하여 본인 여부를 확인하는 기술이나, 사용자가 반드시 휴대폰 가입자여 한다는 전제 조건과 휴대폰 가입절차의 취약, 발신자 신원확인 불가, 수신사 신원확인 불가, SMS 열람 가능, 대기시간 보안이 취약하다는 것과 유효시간 내 SMS 인증코드에 대한 불법인증이 가능하고 보안성이 낮은 것이 단점이다. 세 번째는 OTP 인증이다[5]. OTP는 OTP 토큰과 OTP 인증 서버 간에 비동기 방식 또는 동기 방식으로 OTP값을 생성하며, 보안의식 고취에 따른 보안카드나 공인인증서 이외의 다중요소인증의 일회용 패스워드로 사용된다. 하지만 OTP는 일부 알고리즘의 일회용 패스워드 추측이 가능하고, 인증 대기시간 문제, 암호화 구조 유출 위험, 별도의 OTP 단말기 구매비용 요구, 별도 기기 휴대폰을 갖고 다니는 등 불편함이 있다. 네 번째는 이중인증이다[6]. 이중인증은 두 가지 인증 방법을 조합하여 적용하는 안전성을 향상시키는 인증 방식이다. 주로 아이디/패스워드 인증 외에 SMS기반 OTP나 보안토큰(HSM), 바이오 생체인증 등 2차 인증을 통합 사용한다. 지식 기반의 경우 분실 여부를 인지하기 어렵고, 약한 암호를 사용하거나 서로 다른 계정에서 동일한 암호를 사용하는 사용자의 경우 해커의 공격에 취약하다. 다섯 번째는 다중인증이다[7]. 다중인증은 완벽한 인증은 없다는 생각으로부터 출발했으며, 대부분 우리는 일반적으로 패스워드를 사용한다. 하지만 패스워드는 사용자의 활동, 습관, 심지어는 이름을 가지고도 쉽게 유추되기 때문에 보안에 취약하다. 여섯 번째는 생체인증이다. 생체인증은 목소리, 지문, 안면 인식, 손금, 홍채 인식, 지문 스캐닝, 지리적 위치 등 신체 정보를 이용하여 신원을 확인하는 정보보안 기술이다. 하지만 생체정보를 노리는 범죄의 악용, 생체정보를 얻기 위한 신체적인 위협, 신체정보가 훼손되면 그 생체정보를 이용할 수 없다는 단점이 있다. 본 논문에서는 블록체인 기반으로 신분증 상에 기록된 최소한의 개인정보를 제공하는 블록체인의 Smart Contract에 기반한 zk-SNARK(zero-knowledge Succinct Non-interactive ARgument of Knowledge)의 영지식 기법과 블록체인을 활용하여 사생활 보호형 개인정보 인증 기법을 제안한다. 영지식을 이용한 개인정보 인증 기법을 제안한다. 영지식 증명은 증명에 필요한 참, 거짓 이외에는 어떠한 정보도 드러내지 않고 문장에 대한 정합성을 증명하는 기술이다. 특히, 영지식 증명은 증명자가 자신이 알고 있는 지식과 정보를 공개하지 않으면서, 그 지식을 알고 있다는 사실을 검증자에게 증명하는 시스템으로, 개인은 사용자 신원증명정보를 본인이 직접 발급하는 것이 가능하다. 즉, 영지식 증명을 통해 개인은 탈중앙성, 불변성, 투명성, 가용성을 갖는 개인정보를 제3의 신뢰기관에 신뢰성 있게 인증할 수 있다. 본 논문 구성은 다음과 같다. 2장에서는 블록체인과 패스워드기반의 인증시스템 관련 연구를 살펴보고, 3장에서는 블록체인 기반의 영지식을 이용한 인증기법을 제안하고, 제안기법을 구현 및 평가한다. 끝으로 4장에서는 결론을 기술한다.

Ⅱ. 관련 연구

블록체인은 2008년 암호화폐인 비트코인에서 처음 적용된 기술로, 발생하는 거래를 저장하는 분산원장이다. 블록체인은 마치 네트워크 참여자들이 하나의 데이터베이스를 참조하는 듯 한 논리적 관점을 제공한다. 각 참여자는 제안된 데이터가 유효할 경우에만 이에 동의하고 본인의 원장을 업데이트한다. 동의한 참여자가 많을수록 원장을 위변조하기 어려워지므로 더 많은 신뢰가 부여된 것이다. 이와 같이 신뢰와 거래인증을 통해 보상을 받는 거래내역으로 블록체인에 데

이터가 저장된다. 따라서 블록체인은 P2P 방식을 기반으로 하여 소규모 데이터들이 체인 형태로 무수히 연결되어 형성된 분산 데이터 저장 환경에 관리 대상 데이터를 저장함으로서 트랙잭션을 추가하게 된다. 각 블록은 유일하게 해싱 알고리즘으로 연결된 블록의 형태로 원장을 조직화 하며, SHA-256 알고리즘을 갖고 고정길이 256비트 해시 또는 메시지 다이제스트를 생성한다. 한편, 사용자는 인터넷 인증 서비스를 이용하기 위해 아이디/패스워드로 접근한다[8-9]. 패스워드 인증 기법은 스마트폰이나 PC를 통해 사용자 아이디/패스워드를 입력하면 패스워드의 해시 값이 서버에 전달되어 데이터베이스에 저장된 사용자 패스워드의 비교 검증으로 인증하는 방식이다. 패스워드는 유출되면 피해가 크며, 패스워드를 통한 인증은 서버에 패스워드를 저장하여 관리한다는 취약점이 존재해 사용자 인증을 SHA-256이나 SHA-512 등 안전한 해시함수를 사용하고 있다. 하지만 패스워드를 안전한 해시 값으로 교체해서 저장해도 사용자의 입력 한때 공격이 여전히 가능하다. 따라서 이와 같은 패스워드의 인증 대체 방법으로 사용자의 스마트 폰을 이용한 SMS 인증이나 OTP 인증을 요구하거나 SNS, 포털 등 과 같은 대체 인증을 사용하고 있지만, 위 방법도 인증의 하드웨어 방식과 인증서버의 네트워크 환경에 영향을 받아 시스템의 보안 안전성을 장담할 수 없다.

최근에는 기본 정보 외 다양한 추가 인증 수단을 제공함으로 써 기업 전산환경을 보호하고 사용자 신원을 보호하는 다중인증 기술이 부각되고 있다. 다중인증이란 세 가지 인증 요소, 즉, 인증자와 검증자만 아는 지식을 비교하는 지식 기반 인증, 소지한 별도 매체의 고유정보를 제시해 인증하는 소지 기반 인증, 인증자의 신체적인 특성을 이용해 인증하는 생체인식 등으로 인증기술 발전을 가져올 것으로 기대되지만, 이 방법도 불필요한 개인정보의 과다 노출과 생체정보의 훼손으로 인한 인증 불가 등이 약점으로 드러났다. 또한, 인터넷 공간에서 공유되는 개인정보는 본인 인증이나 인터넷 공간에서의 활동 내역 등이 해당되는데, 영지식은 이와 같은 개인 정보의 수집을 최소화하여 공용 블록이나 공유 및 기타 네트워크에서 사용자의 개인 정보 보호가 강화된다는 장점이 있다[10]. 하지만 영지식의 특징은 확률을 기반으로 한다는 것이다. 이에 따라 영지식은 세 가지 조건을 만족해야 한다. 첫 번째는 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 하는 완전성(Completeness)이다. 두 번째는 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 하는 건전성(Soundness)이다. 끝으로 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 하는 영지식이다(Knowledge Proof). 영지식은 블록체인을 통해 공용 블록/공유 및 기타 네트워크에서 사용자의 개인 정보 보호와 비효율적인 인증 및 검증 방법을 대체하여 정보 보안 강화하고 블록체인 처리량 및 확장성을 향상시켜 개인정보의 무결성을 보장하는 장점이 있다. 블록체인에서 사용되는 영지식 증명은 한 번의 증명으로 검증자에게 증명 사실을 확인시키는데, 이 때 구성하는 프로그램을 작성하여 회로(Circuit)로 변환하는데는, 암호에 대한 지식이 없으면 회로를 사용할 수 없다는 특징이 있다. 따라서. 영지식을 사용하는 도구는 암호학적 지식과는 무관하게 사용가능하며, Smart Contract를 이용하는 회로 검증은 안전한 데이터의 무결성이 보장되어 블록체인 내에 영지식을 이용할 때 많은 도움이 될 것으로 기대된다.

Ⅲ. 제안기법

3.1 영지식을 이용한 인증 기법

본 장에서는 사용자 인증을 위해 2장에서 언급한 기존의 인증 방식이 아닌 그림 1과 같은 블록체인의 Smart Contract 환경의 영지식을 이용한 새로운 인증 모델을 제시한다.

이 방법은 위변조를 방지할 수 있고, 비용 절감, 계약과정이 간단하며, 빠르게 계약이 가능하다. 또한, 중개자가 필요 없으며, 프로그래밍 코드를 사용한 계약으로 내용의 모호한 부분지 적은 기술이다. 영지식은 계정 정보와 블록체인에만 국한되지 않고, 개인 정보 보호와 서비스 인증뿐만 아니라, 서비스 효율성을 높인다. 따라서 인증에 필요한 최소 데이터만이 오고감

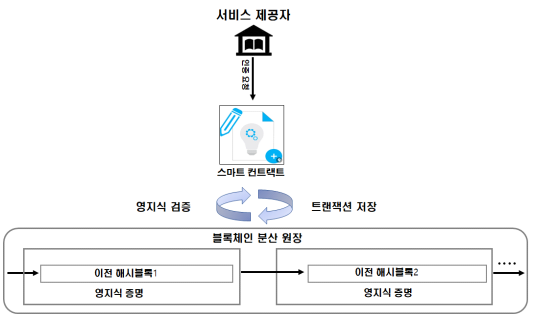

그림 1. 제안 시스템 모델
Fig. 1. Proposal system model

으로서 과도한 정보 노출 문제를 방지하는 기술이다. 이더리움(Eethereum) 블록체인은 데이터 위변조를 방지하고 신뢰성과 무결성을 보장하는 기술로 블록체인을 기반으로 하는 암호화폐 시스템의 Smart Contract 사용 환경을 구축하고 있다. Smart Contract는 계약 당사자가 사전에 협의한 내용을 미리 프로그래밍하여 전자 계약서 문서 안에 넣어두고, 이 계약 조건이 모두 충족되면 자동으로 계약 내용이 실행되도록 하는 시스템으로 데이터 신뢰도가 증가된다. 그림 2는 이더리움 환경의 블록체인에 익명의 사용자 정보를 영지식을 이용하여 인증하는 시나리오이며, 다음과 같이 진행된다.

① 서비스 제공자가 사용자의 신원인증 정보를 요청 한다.
② 사용자는 인증기관에 신원정보 발행을 요청한다.
③ 인증기관은 블록체인 기반 Smart Contract에 사용자의 신원정보를 영지식과 해시값으로 등록한다.
④ 인증기관은 Smart Contract 실행으로 사용자 신원정보가 기록된 영지식을 사용자에게 제공한다.
⑤ 사용자는 서비스 제공자에게 신원정보 인증에 필 요한 최소한의 영지식 정보를 서비스 제공자에게 전달한다.
⑥ 서비스 제공자는 이더리움 기반의 블록체인에 저 장된 영지식 정보를 검증하여 신원확인을 완료한다.

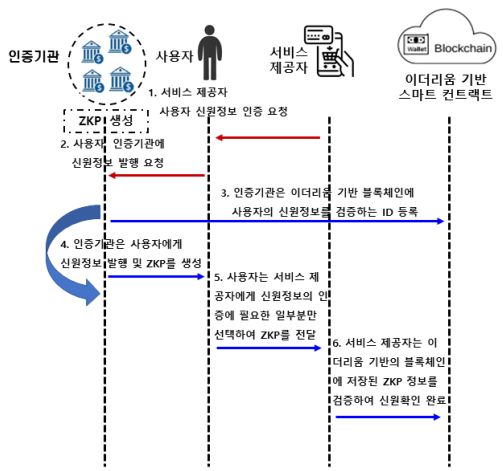

그림 2. 영지식을 이용한 인증 기법
Fig. 2. Authentication method using zero knowledge proofs

영지식 증명은 중앙기관에 의존하지 않는 신용인증 방법으로 개인정보를 보호할 뿐 아니라 한 번 계산한 결과를 재계산하지 않는 특징과 적은 비용으로 최소 정보를 제공한다는 장점이 있다. 또한, 영지식과 블록체인의 Smart Contract를 결합하면 프라이버시 보장 데이터 증명을 활용하여 다른 서비스도 중앙기관의 개입 없이 제공할 수 있다.

3.2 제안기법의 구현

본 논문에서 제안한 영지식 기법은 윈도우 환경의 객체지향 언어로 가장 많이 쓰이는 자바를 이용하여 구현하였다. 블록체인 기반 영지식을 활용한 개인정보 인증을 구현하기 위해 Smart Contract를 작성 배포하여 그림 3과 같은 SHA-256 알고리즘으로 256비트 해시 블록을 채굴하였다.

블록과 트랜잭션은 블록체인을 구성하는 필수 요소이다. 블록은 체인에 있는 각 블록이 이전 블록의 해시 값을 포함하여 연결되며, 블록 안에 있는 해시 값은 암호화 해시로 각각의 블록을 유일하게 식별해주는 값이다. 식별자는 SHA-256 암호화 알고리즘을 이용해 블록헤더를 해시 적용해 생성한다. 이전 블록에 대한 참조를 포함하려면 해당 블록의 암호화 해시를 알아야 하며, 이전 블록 다음에 그 다름의 블록이 있어야 한다. 채굴하는 트랜잭션 데이터는 임의로 3개(Master, First, Second)를 채굴하여 블록에 저장하고, 최초의 시작 블록인 Master를 생성하고 계좌나 블록 정보들이 저장될 다음 블록의 First, Second 순으로 블록을 연결 접속한다. 그 결과 그림4와 같은 채굴을 확인할 수 있다.

채굴은 블록체인이라고 불리는 비트코인의 공공 원장에 거래 기록을 추가하는 과정을 말하며. 채굴의 존

```
package zeroKnowledgeBlockChain;

import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Base64;
import java.util.logging.Level;
import java.util.logging.Logger;

public class Generator {
    public static String generateHash(String text) {
        try {
            MessageDigest digest = MessageDigest.getInstance("SHA-256");
            byte[] hash = digest.digest(text.getBytes(StandardCharsets.UTF_8));
            String encoded = Base64.getEncoder().encodeToString(hash);
            return encoded;
        } catch (NoSuchAlgorithmException ex) {
            Logger.getLogger(Generator.class.getName()).log(Level.SEVERE, null, ex);
        }
        return null;
    }
}
```

그림 3. SHA-256 비트로 채굴하는 암호화 코드
Fig. 3. Crypto blocks mined with SHA-256 bits

그림 4. SHA-256 비트로 채굴한 암호화 코드
Fig. 4. Encryption code mined with SHA-256 bits

재 이유는 모든 거래의 정확성을 확인하고 네트워크 상에 있는 모든 참여자들이 이 원장을 열람할 수 있도록 하려는 것이다. 이는 또한 합당한 비트코인 거래와 다른 곳에서 쓴 돈을 다시 지출하는 것을 구분하는 데도 사용된다. 자바를 이용한 구현은 SHA-256을 영지식의 블록체인에 혼합해 넣는 방식으로 개인정보 인증을 확인하는 작업이다. SHA-256은 SHA 알고리즘의 한 종류로서 256비트로 구성되며 64자리 문자열을 반환한다. SHA-256은 미국의 국립표준기술연구소(NIST; National Institute of Standards and Technology)에 의해 공표된 표준 해시 알고리즘인 SHA-2 계열 중 하나이며 블록체인에서 가장 많이 채택하여 사용하고 있다. SHA-256 해시 함수는 어떤 길이의 값을 입력하더라도 256비트의 고정된 결과 값을 출력한다. 일반적으로 입력 값이 조금만 변동하여도 출력 값이 완전히 달라지기 때문에 출력 값을 토대로 입력 값을 유추하는 것은 거의 불가능하다. 아주 작은 확률로 입력 값이 다름에도 불구하고 출력 값이 같은 경우가 발생하는데 이것을 충돌이라고 한다. 이러한 충돌의 발생 확률이 낮을수록 좋은 함수라고 평가된다. SHA-256과 Smart Contract를 구현하기 위한 환경으로는 이더리움을 꼽으며, 이더리움은 블록체인 네트워크에서 Smart Contract을 생성하여 화폐의 전송이 아닌 프로그래밍 코드 형태의 데이터를 전송하여 해당코드를 실행하는 오픈 플랫폼이다. 이더리움은 블록체인을 기반으로 튜링 완전 프로그래밍 언어가 내장된 플랫폼으로 누구나 스마트 계약서 및 분산 응용 프로그램을 작성할 수 있다. 각 노드들은 이더리움 클라이언트를 설치하고 다음 명령을 호출하여 블록 연결에 참여하도록 네트워크를 구성하고 접속한다. 그림 5는 영지식으로 생성되는 Master, First, Second 블록들이며, 블록체인에 동기화를 위해 실행되고 각각의 해시 값으로 블록체인에 연결된다. k-SNARK의 영지식 기법과 블록체인을 활용하는 사생활 보호형 개인정보 관리기법은 zk-SNARK와 Smart Contract를 통해 합의된 내용의 개인정보를 제공할 때 사생활을 보장하면서도 정보의 과다 노출을 방지할 수 있다. 또한 블록체인의 영지식을 통해 정보의 무결성을 보장하면

그림 5. 영지식으로 생성된 Master,First,Second 코드
Fig. 5. Master, First, and Second blocks created with zero knowledge proofs

서도 개인정보 중심으로 정보를 관리할 수 있으며, 개인정보 공유를 기존의 인증방식보다 안전하고 용이하게 수행할 수 있다. 채굴된 Master, First, Second는 블록체인에 동기화를 위해 실행되며, 각각의 해시 값으로 그림 6과 같이 블록들이 생성되었으며 거래가 승인된다.

블록체인은 거래정보가 담긴 각각의 블록을 해시함수를 사용하여 연결하고, 위.변조 방지 및 추적 가능한 특성을 고려하여 블록체인에 저장된 정보는 트랜잭션의 분산 합의를 통해 실행된다. 해시 함수로 계산된 영지식 값은 Smart Contract 정보의 요구 사항, 특정 형식 및 조건을 미리 명확히 하고, 제3자의 참여 없이 영지식 증명의 유효성을 자동으로 판단하며, 서면으로 이루어지던 계약을 코드로 구현한다. 또한, 제3자의 개입 없이 영지식과 인증기관의 요청내용을 비교하여 참 또는 거짓을 출력한다. 인증기관이 개인정보를 검증하면 Smart Contract PBFT 합의 알고리즘으로 거래내역을 블록체인에 기록하므로 서 정보 인증이 마무리되며, 그림6과 같은 영지식성이 보장되도록 채굴과 세 개의 Master, First, Second 블록들이 생성됨을 확인할 수 있다.

3.3 평가 및 성능 분석

본 절에서는 제안 기법과 기존 합의 알고리즘의 성능을 테스트하기 위해 표 1과 같이 임의의 블록갯수

그림 6. 채굴과 Master, First, Second 블록들이 생 성되어 최종적으로 연결된 블록체인
Fig. 6. A block chain in which mining and Master,First, and Second blocks are created and finally connected

를 15개로 하여 각각의 블록 연결 수에 따른 처리시간을 측정하였다. 표 1에서 보는 바와 같이 15개 이상에서는 비교 값의 편차가 많이 나서 그 이상을 비교한다는 것은 무의미하며, 이는 제안기법이 Smart Contract 기반에서 영지식의 특성인 완전성, 건전성, 영지식성을 만족하여, 블록갯수가 증가하더라도 기존 합의 알고리즘에 비해 현저하게 처리속도가 감소됨을 알 수 있다. 이는 작업증명의 합의 알고리즘이 영지식 증명을 사용하지 않기에, 기존의 모든 노드의 승인을 받아야 하므로 속도가 느리다는 한계가 있기 때문이다. 현대 암호학에서는 영지식 증명을 다자간의 비대면 통신 프로토콜에서 정보보호 기능을 제공하기 위해 적용하는 암호 프로토콜 중 매우 중요하고 구현하기 까다로운 고급 암호 프로토콜의 한 종류로 취급하고 있다. 따라서 영지식 증명을 활용한 제안기법은 블록체인 기반에서 개인정보 인증을 보장하는 사실이 블록체인에 저장된 기존 사실들과 모순되지 않음을 아래와 같은 3가지 조건인 완전성, 건전성, 영지식성을 보임으로써 만족시켰다. 또한, 이를 토대로 기존 합의 알고리즘과의 실행속도는 전체 블록의 개수에 비례하므로 검증을 위한 시뮬레이션으로 그림 7과 같은 선형적인 결과를 얻을 수 있었다.

표 1. 제안기법과 합의 알고리즘의 처리시간 비교
Table 1. Comparison of processing time between the proposed method and the consensus algorithm

블록갯수	제안기법	합의 알고리즘	비율
1	1	1	1.000000
2	2	4	0.500000
3	3	9	0.333333
4	4	16	0.250000
5	5	25	0.200000
6	6	36	0.166667
7	7	49	0.142857
8	8	64	0.125000
9	9	81	0.111111
10	10	100	0.100000
11	11	121	0.090909
12	12	144	0.083333
13	13	169	0.076923
14	14	196	0.071429
15	15	225	0.066667

① 완전성(Completeness): 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 한다. 즉,블록체인에 기록된 사용자 증명 함수 내의 입력 값은 해시 함수로 결정되며, 항상 동일한 입력 값을 얻는다.

② 건전성(Soundness): 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 한다. 즉, 영지식은 계산적으로 확실한 것으로 간주된다. 따라서 증명자의 컴퓨팅 능력이 제한적이라고 가정했을 때, 정직하지 않은 증명자는 시스템

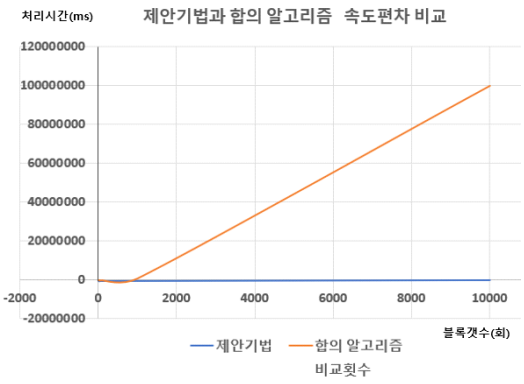

그림 7. 제안기법과 합의 알고리즘과 속도편차 비교
Fig. 7. Comparison of proposed technique, consensus algorithm, and speed deviation

을 속일 확률이 매우 낮아야 된다.

③ 영지식성(Zero-knowledge): 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 한다. 즉, 영지식 증명은 완벽한 영지식성을 가지며 인증 기법도 완벽한 하이딩 속성을 가진다.

제안기법은 패스워드기반이 아닌 블록체인 기반으로 사용자를 구현하였으며, Smart Contract와 영지식을 결합한 새로운 인증 모델로 기존의 인증보다 안정성이 보장됨을 보장할 수 있다. 또한, 블록체인에 개인정보를 저장하여 블록에 담겨 있는 분산 저장된 새로운 인증 패러다임이며, 소유주 확인이 어려워 개인정보를 보호할 수 있으며, 불필요한 개인정보 노출을 최소화하여 새로 요구되는 최소한의 인증 정보만 제공하고, 인증관련 정보가 없기 때문에 공격자의 공격을 피할 수 있다.

Ⅳ. 결 론

영지식 증명은 암호학에서 누군가가 상대방에게 어떤 상태가 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제외한 어떤 것도 노출되지 않도록 하는 절차이다. 영지식 증명을 활용한 프로토콜의 가장 큰 특징은 정보를 공개하지 않고 정보의 유효성을 증명할 수 있는 방법이라는 것이다. 따라서 개인은 각 인증기관으로부터 스스로 신용정보를 수집하고 이를 이용하여 최소한의 정보로 서비스 제공자에 제공할 수 있다. 본 논문에서는 영지식과 블록체인의 Smart Contract를 이용함으로써 개인이 개인정보를 인증함에 있어 최소한의 요구사항에 맞도록 검증 가능한 영지식을 활용한 개인정보 인증 기법을 구현하였다. 영지식 증명을 통해 개인은 탈중앙화 되어 중앙기관이 아닌 개인들이 데이터의 주권을 갖고 서비스 제공자에게 신뢰성 있게 인증할 수 있다. 이는 블록체인을 통해 데이터의 신뢰성을 보장하면서도 보다 강화된 개인정보 데이터를 효율적으로 관리하며, 개인정보 인증을 기존의 인증방식보다 빠르고 안전하게 수행할 수 있다는 장점이 있다.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Busin. Rev.*, Oct. 2008. (https://doi.org/10.1007/978-3-030-17740-9_3)

[2] A. Kosba, et al., "Hawk: The blockchain model of cryptography and privacy-preserving Smart Contracts," *2016 IEEE Symp. SP*, pp. 839-858, San Jose, USA, May 2016. (https://doi.org/10.1109/sp.2016.55)

[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1-32, 2014. (https://doi.org/10.7717/peerjcs.815/table-7)

[4] M. Thomas and V. Panchami, "An encryption protocol for end-to-end secure transmission of SMS," *Int. Conf. Cir., Power and Comput. Technol.*, pp. 1-6, Nagercoil, India, Mar. 2015. (https://doi.org/10.1109/iccpct.2015.7159471)

[5] Y. S. Jeong, S. H. Han, and S. S. Shin, "A study on mobile OTP generation model," *J. Digital Convergence*, vol. 10, no. 2, pp. 183-191, Mar. 2012. (https://doi.org/10.14400/jdc.2015.1 3.1.283)

[6] C. T. Li, C. Y. Weng, and C. Fan, "Two-factor user authentication in multi-server networks," *Int. J. Secur. and Its Appl.*, vol. 6, no. 2, pp. 261-268, Jan. 2012. (https://doi.org/10.1002/sec.1109)

[7] S. Yevseiev, et al., "Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system," *East.-Eur. J. Enterprise Technol.*, vol. 6, no. 4, pp. 11-23, Dec. 2016. (https://doi.org/10.15587/1729-4061.2016.86175)

[8] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," *IEEE Trans. VLSI Syst.*, vol. 27, no. 12, pp. 2792-2801, Aug. 2019. (https://doi.org/10.1109/tvlsi.2019.2929420)

[9] M. Campanelli, D. Fiore, and A. Querol, "LegoSNARK: Modular design and composition of succinct zero knowledge proofs," in *Proc. 2019 ACM SIGSAC Conf. CCS '19*, pp. 2075-2092, London, United Kingdom, Nov. 2019. (https://doi.org/10.1145/3319535.3339820)

[10] S. Agrawal, C. Ganesh, and P. Mohassel, "Non-interactive zero knowledge proofs for

composite statements," *CRYPTO2018*, pp. 643-673, Aug. 2018. (https://doi.org/10.1007/978-3-319-96878-0_22)

이 광 규 (Kwang-Kyu Lee)

1985년 2월 : 동국대학교 수학과 학사
1991년 2월 : 동국대학교 수학과 이학석사
2002년 8월 : 충북대학교 전산과 이학박사
1996년~현재 : 신한대학교 IT융합공학부 교수
<관심분야>인공지능, 정보보안, 빅데이터, 블록체인