디지털산업정보학회 논문지 제19권 제3호-2023년 9월
http://dx.doi.org/10.17662/ksdim.2023.19.3.037

스마트폰을 이용한 영지식증명 블록체인 개인정보 인증에 관한 연구*

이 광 규**

A Study on Zero Knowledge Proof Blockchain Personal Information Authentication Using Smartphone

Lee Kwangkyu

〈Abstract〉

In the future society, a means to verify the identity of the information owner is required at the beginning of most services that the information owner encounters, and the emergence and gradual spread of digital identification that proves the identity of the information owner is essential. In addition, as the utilization value of personal information increases, discussions on how to provide personal information are active. Therefore, there is a need for a personal information management method necessary for building a hyper-connected society that is safe from various hacking, forgery, alteration, and theft by allowing the owner to directly manage and provide personal information management. In this study, a decentralized identity information management model that overcomes the problems and limitations of the centralized identity management method of personal information and manages and selectively provides personal information by the information owner himself and implemented a smart personal information provision system(SPIPS: Smart Personal Information Provision System) using a smartphone.

Key Words : Blockchain, DID(Decentralized Identitifier), PBFT(Practical Byzantine Fault Tolerance), SPIPS(Smart Personal Information Provision System), ZKP(Zero Knowledge Proof)

Ⅰ. 서론

블록체인은 관리 대상 데이터를 블록이라고 하는 소규모 데이터들이 P2P(Peer-to-Peer) 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다[1]. 블록에는 해당 블록이 발견되기 이전에 사용자들에게 전파되었던 모든 거래 내역이 기록되어 있고, 이것은 P2P 방식으로 모든 사용자에게 똑같이 전송되므로 거래 내

*본 논문은 2023년도 신한대학교 교내연구비 지원에 의해 연구되었음
** 신한대학교 소프트웨어융합학과 교수(교신저자)

역을 임의로 수정하거나 누락시킬 수 없다. 블록은 발견된 날짜와 이전 블록에 대한 연결고리를 가지고 있으며 이러한 블록들의 집합을 블록체인이라 칭한다. 쉽게 말하자면 수많은 기록을 그냥 한 묶음으로 만들어 버리는 기술이다. 기존에 전자화폐로 거래할 때 중앙 서버에 거래 기록을 보관하는 것과는 달리, 블록체인은 모든 사용자에게 거래 기록을 보여주며 서로 비교해 위조를 막는다. 비트코인이 블록체인이라는 개념을 처음 실증하였고 이더리움(Ethereum)이 스마트 컨트랙트(Smart Contract)라는 개념을 처음 구현한 것에서 볼 수 있듯이, 블록체인과 암호화폐 사이에는 밀접한 관계가 있다[2]. 하지만 블록체인이 암호화폐에만 사용될 수 있는 기술은 아니다. 하지만 블록체인에 저장된 정보나 거래내역 기록은 절대 위·변조가 불가능하지만, 기록되기 전 데이터의 무결성에 대한 보장은 없으며, 분산원장을 통한 데이터 공동 관리는 거래 처리 속도와 저장 용량 문제가 있어 적용이 불가한 업무 영역도 존재한다. 블록체인 네트워크를 공격하는 것은 분산 데이터베이스에 대한 위변조를 하기 위해서이나, 일반적으로 데이터를 위변조하여 암호화폐를 탈취하거나 증식시키고, 블록체인을 이용한 인증 서비스에는 신원을 위장할 수도 있다. 공격은 언제나 공격자의 이득을 위해 수행되는 만큼 현재는 높은 가치가 있는 암호화폐가 주공격 대상이다. 따라서 이와 같은 블록체인의 프라이버시 문제를 해결할 수 있는 방법 중의 하나가 바로 영지식증명(Zero Knowledge Proof:ZKP)의 도입이다[3,4]. 블록체인을 이루는 핵심 기술은 두 가지가 있는데 하나는 합의 알고리즘, 또 다른 하나가 영지식증명이다. 합의 알고리즘은 블록체인 불변성을 제공하는 핵심 기술이고, 영지식증명은 프라이버시 문제를 해결하는 암호학적 방법으로 블록체인뿐만 아니라 프라이버시가 문제되는 곳에서 데이터를 활용할 수 있게 하는 방법이다[5]. 블록체인에 프라이버시를 제공한다는 것은 온체인 블록체인에 약정된 값이 올라가고 영지식을 사용해서 오프체인에서 데이터를 활용하는 방식으로 진행한다. 공개된 온체인 블록체인에서는 데이터가 감추어지기 때문에 프라이버시 문제를 해결할 수 있다. 뿐만 아니라 영지식 기법들은 빠른 검증을 제공하기 때문에 블록체인 성능향상, 크기 최소화 등에도 다양하게 활용되고 있다. 특히, P2P 거래정보에 개인정보 및 의료, 활동, 구난, 이력 정보를 저장하여 두고 필요한 상황에 맞는 정보만을 제공하는 스마트 개인정보 제공 시스템을 구축하여 개인정보의 사용 권한을 소유자에게 일임하여 프라이버시를 보호할 수 있다. 일반적인 블록체인 구조는 조건이 만족되는 블록이 많이 생길수록 데이터 신뢰도가 향상되나, 스마트 개인정보 제공 시스템은 거래정보에 개인정보가 저장되어 있어 블록 소유자의 승인 없이 데이터에 접근하는 권한은 부여할 수 없다. 영지식증명은 사전 정의된 연산에 대해 비밀 입력값은 공개하지 않으면서도 입출력 값의 관계에 해당하는 비밀 입력값을 알고 있음을 증명하는 암호 기술로, 프라이버시 보호가 필수적인 블록체인에서 영지식증명은 절대적이며, 영지식증명을 통해 환자는 제3의 인증기관이나 본인 인증을 거치지 않고, 필요한 개인정보를 스스로 선택하여 필요로 하는 기관에 신뢰성 있게 제공할 수 있다. 개인의 의료정보를 원격지 의사에게 전송하는 원격건강정보 모니터링 시스템에서 개인 건강정보의 보호에 관한 관심과 필요성의 증가가 일례가 되며, 본인 확인을 증명하는 방법으로 사용될 수 있다[6]. 본 제안에서는 zk-SNARK(Zero Knowledge Succinct Non-interactive Argument of Knowledge)를 블록체인의 헤더를 인증하는데 필요한 PBFT(Practical Byzantine Fault Tolerance)의 사전 협의가 이뤄진 알고리즘에 따라 분산 합의되는 영지식증명을 활용하여 개인정보를 보호하며, 거래정보에 해당하는 영역에 저장된 개별정보는 개인 인증정보와 결합하여 보호하고 소유자의 선택에 따른 정보를 안전하게 제공하는 개인정보 인증 구현을 보인다. 본 논문 구성은

다음과 같다. 2장에서는 블록체인과 영지식 기반의 인증 시스템 관련 연구를 살펴보고, 3장에서는 탈중앙화 정보관리 모델(DIDM)을 제시하고, 스마트폰을 이용한 스마트 개인정보 제공 시스템(SPIPS)을 구현 및 평가 한다. 끝으로 4장에서 결론을 기술한다.

II. 관련연구

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 데이터가 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. 기존의 중앙 집중식 디지털 ID 관리 시스템은 내부 공격 및 개인 정보 유출과 같은 위협에 노출되었으며[7], 이를 해결하고자 스마트 계약과 영지식증명 알고리즘을 활용하여 블록체인의 기존 사용자 신원 모델을 개선하고, 또한 사용자의 행동 프라이버시를 보호하기 위해 사용자가 속성 소유권을 서비스 제공자에게 선택적으로 공개할 수 있도록 하는 챌린지-응답 프로토콜을 포함하는 새로운 시스템 프로토타입을 제시하였다[8]. 일반적인 블록체인 구조는 조건이 만족 되는 블록이 많이 생길수록 데이터 신뢰도가 향상되나, SPIPS는 거래정보에 개인정보가 저장되어 있어 블록 소유자의 승인 없이 데이터에 접근하는 권한은 부여할 수 없다. 따라서 이러한 탈중앙화 신원증명이 우선 해결되어야 한다. 즉, 블록체인의 다른 참여자가 블록의 참을 인증하는 기능 이외의 거래 원장을 볼 수 있는 기능은 개인정보 보호의 취약점이 된다[9]. 개인정보의 활용 가치가 높아짐에 따라, 개인정보를 제공하는 방법에 대한 논의가 활발하나, 개인정보 활용을 위해 기관에서 필요로 하는 정보 이상의 정보가 노출되고, 병원 등의 기관에서 개인정보를 요구할 때마다 인증기관이 해당 정보에 대한 인증정보를 병원에 제공해야 하는 문제점을 극복하는 방안 마련을 했다[10]. 무선 통신의 바이오센서와 통합된 소형 모바일 장치는 의료 시스템의 혁명을 가져와 원격으로 환자를 모니터링하고 건강 서비스를 제공하지만, 스마트폰간의 무선 통신중 특히 블루투스를 사용하는 경우 앱에 의한 데이터 해킹, 도용 공격이나 불법 장치에 의해 가짜 데이터 주입이 허용 될 수 있다[11]. 또한, 온라인 의료 서비스를 위한 신원 인증 문제는 최근 몇 년 동안 의료 산업의 핵심 초점 중 하나였으며, 대부분의 의료 기관은 중앙 집중식 ID 관리 시스템을 사용하였다. 이는 의료 기관과 환자 간의 상호 데이터 교환의 불투명과 개인정보 과다 노출을 초래하였다[12]. 하지만 영지식증명을 통해 환자는 제3의 인증기관이나 본인 인증을 거치지 않고, 필요한 개인정보를 스스로 선택하여 필요로 하는 기관에 신뢰성 있게 제공할 수 있다[13]. 또한, 개인의 의료정보를 원격지 의사에게 전송하는 원격건강정보 모니터링 시스템에서 개인 건강정보의 보호에 관한 관심과 필요성의 증가는 일례가 될 수 있다. 스마트 개인정보 제공 시스템은 소유자가 블록체인에 접근하고, 정보를 선별하여 선택하면 예약된 실행을 진행하여 개인정보의 상태를 제공하거나 SPIPS를 활성화 할 수 있으며, SPIPS가 무결성만 보장하던 블록체인 시스템의 한계를 넘어, 조건과 상황에 따라 자동으로 실행되는 SPIPS로 진화된다. SPIPS가 발생 되면 개인 블록에는 개인정보의 이력을 기록, 개인정보 보안 유지나 개인정보 파기의 문제가 발생할 때 해결을 방법은

새로운 블록을 만들어 인증 받고, 인증 받은 블록으로 필요한 정보만 이동하는 방법으로 삭제할 수 있도록 하는 보완이 필요하다. 기관이나 병원에서 필요 이상의 개인정보를 요구하더라도 개인이 개인정보의 과도한 노출을 제한할 수 있고 기관에서 필요로 하는 정보만 산출하여 인증된 형태로 제공하며, 영지식증명은 데이터의 해시 한 약정 값을 블록체인에 올리며, 약정 값 계산은 일반적으로 임의 값을 더한 입력 값을 사용하여 계산하기 때문에, 약정 값으로부터 원래 입력 값을 구하는 것은 불가능하다. 따라서 블록체인에 올려져 있는 개인정보는 노출되지 않으며, 프라이버시 문제를 해결하는 암호학적 방법으로 개인정보를 제공하는 곳에서는 언제든 영지식증명 데이터를 활용할 수 있다. 개인정보 데이터가 갱신되면, 데이터의 갱신여부가 블록에 기록될 수밖에 없는데, 이는 개인정보가 자주 바뀌는 환자의 개인정보 보호를 침해할 가능성이 존재한다. 따라서 갱신여부를 드러내지 않고 개인정보를 제공할 방법이 필요하다. 개인정보가 철저히 보장되는 영지식증명의 응용 분야로, 영지식증명을 기반으로 한 블록체인 구현 방법은 정보의 무결성을 보장하면서도 개인정보 중심으로 정보를 관리 통제할 수 있으며, 개인정보 보호를 기존의 인증방식보다 안전하게 수행할 수 있다.

Ⅲ. 제안기법

3.1 영지식증명 블록체인을 이용한 인증

모든 노드가 동일 기록을 저장하는 블록체인은 수평적 분산원장의 네트워크의 한계점을 가지고 있다. 따라서 특정 합의 알고리즘에 기반하는 네트워크를 확장하고 블록체인에서 블록인 인증 범위를 헤더로 국한하고 개별 블록의 수정, 추가를 영지식증명 기법으로 확장하면 한계를 극복하기 위한 접근 방식 제한과 모두의 신뢰를 확보하는 투명성이 확실하게 확보하는 방법으로 판단한다. 영지식증명을 활용한 블록체인 기법은 개인정보 문제를 해결하는 암호학적 방법으로 블록체인뿐만 아니라, 개인정보를 다루는 곳에서 데이터를 활용할 수 있다. 공개된 온라인 블록체인에서는 데이터가 감추어져 있어서 개인정보 문제가 해결되고, 또한, 영지식증명 기법은 빠른 검증을 제공하여, 블록체인의 성능향상, 크기 최소화 등에도 유용하다. 개인정보 데이터가 갱신되면, 데이터의 갱신여부가 블록에 기록될 수밖에 없는데, 이는 개인정보가 자주 바뀌는 환자의 개인정보 보호를 침해할 가능성이 존재한다. 따라서 갱신여부를 드러내지 않고 개인정보를 제공할 방법이 필요하다. 퍼블릭 블록체인에서는 노드가 정보를 기록하고 관리하고 있어, 모든 노드가 정보 보호에 취약하며, 모든 노드가 동일 기록을 저장하는 블록체인은 수평적 분산원장의 네트워크의 한계점을 가지고 있다. 따라서 특정 합의 알고리즘에 기반하는 네트워크를 확장하고 블록체인에서 블록 인증 범위를 헤더로 국한한다. 개별 블록의 수정, 추가는 영지식증명 기법으로 확장하여 한계를 극복하며, 접근 방식 제한과 모두의 신뢰를 확보하는 투명성은 분명하게 확보될 필요성이 요구된다. 제안 기법은 <그림1>처럼 영지식증명 기반 블록체인 개인정보 신원 증명은 서비스 등록, 정보 생성 및 검증, 정보 공유 단계로 구성되며, 다음과 같이 진행된다.

① 정보 소유자는 SPIPS를 통해 자신의 개인정보를 블록체인에 기록

② 개인정보 요청기관은 의료기관 공개키를 정보 소유자에게 제공

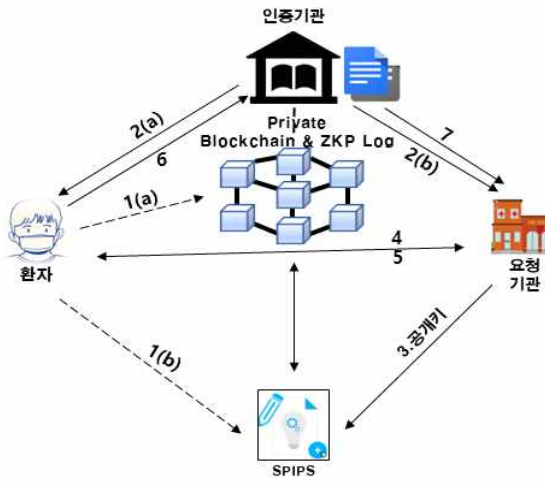
③ 정보 소유자는 개인정보 요청기관의 공개키를 SPIPS에 등록

④ 개인정보 요청기관의 필요 정보를 소유자에게 정보 제공 요청

⑤ SPIPS에 분류된 정보를 선별하여 기관의 공개키를 사용하여 암호화

⑥ 암호화된 정보를 개인의 공개키와 함께 정보 요청기관에 전송

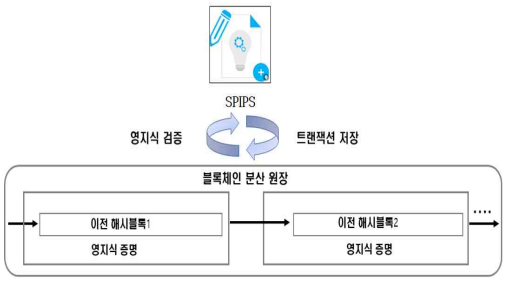
⑦ 정보 소유자와 개인정보 요청기관 간의 거래를 PBFT 알고리즘을 통한 분산 합의로 개인정보 이력에 제공



<그림 1> 제안 모델

3.2 구현 및 평가

본 논문에서 제안한 기법은 윈도우 환경의 안드로이드 스튜디오(Flamingo)자바 언어를 이용하여 스마트폰 상에서 구현하였다. 블록체인은 서로 다른 개인이나 법인이 통제하는 다수의 컴퓨터 시스템 상에서 같은 거래 원장 사본이 보관되는 디지털 분산원장의 한 형태이다. 즉, 거래정보를 기록한 장부인 원장이 블록이라는 단위에 디지털화되어 저장된다. 블록은 거래정보와 헤더로 나뉘는데, 본 연구에서 거래 내용은 개인정보 및 분류와 사용 이력을 저장하며, 헤더에는 블록의 사실(진위) 여부 등의 인증을 위한 암호코드 등이 저장된다. 탈중앙화 신원 증명에 영지식증명을 결합하여 개인정보 관리 주체를 소유권자인 개인에게 위임하는 것은 개인정보 보호를 보다 강화하는 효과를 얻을 수 있으며, 개인이 편리하게 정보를 관리할 수 있는 안전한 미래사회의 초석을 구축하는데 결과의 중요성이 있다. 영지식증명은 증명자와 검증자 간의 프라이버시 문제를 해결하는 암호학적 방법으로 블록체인뿐만 아니라 프라이버시 문제가 되는 곳에서 데이터를 활용할 수 있다. 블록체인에 프라이버시를 제공한다는 것은 온체인 블록체인에 약정된 값이 탑재되고, 영지식증명을 사용하여 오프체인에서 데이터를 활용하는 방식으로 진행한다. 본 절에서는 사용자 인증을 위해 기존의 인증 방식이 아닌 블록체인의 스마트 컨트랙트 환경의 스마트폰을 이용하여 새로운 영지식증명 블록체인 개인정보 제공 방법을 제시한다. 최종 완성된 SPIPS는 <그림2>와 같으며, 동작 방법은 SPIPS가 개인의 암호화된 정보를 영지식증명으로 요청기관에 제출하고 제출받은 기관에서는 추가 정보를 개인의 SPIPS에 전달하며, 전달받은 정보는 블록의 트랜잭션 영역에 분류되어 저장되고 보관하는 것으로 마무리된다.



<그림 2> 개인정보 소유자와 사용기관의 정보 교환

<그림3>은 스마트 컨트랙트 환경의 영지식증명 블록체인을 이용한 새로운 개인정보 제공 방법을 제시한다. 노드의 트랜잭션에 비트코인 재화 이동 명세 대신에 개인정보를 기록하고 관리하는 영지식증명 블록체인의 기본구조이다. 이 기본구조를 근거로 개

인정보를 사용하고자 하는 요청기관은 별도의 블록 연결 이력을 관리하여 레거시 관리체계의 연속성을 유지하면 된다.

```
public Block(Order order, String previousHash) {
    this.order = order;
    this.previousHash = previousHash;
    this.timeStamp = new Date().getTime();

    this.hash = Generator.generateHash(
            this.previousHash
            + this.timeStamp
            + this.order.toString());
}
```

<그림 3> 영지식증명 블록체인 기본구조

제안기법이 기존 레거시와 다른 점은 실명과 주민등록번호 대신에 블록체인이 그 위치를 대신하고, 블록체인의 고유 체인 아이디 값을 인식하고 관리해야 한다는 것이다. 개인정보를 제공하는 소유자 측면에서는 제공된 블록체인의 노드 연결을 해제하여 개인정보가 더 이상 요청기관에 남지 않는 것으로 정보를 보호할 수 있다. 따라서 <그림4>와 같은 초기 영지식증명 블록체인을 연결하는 아이디 생성이 필요하며, 블록 안에 담긴 거래 데이터를 검증하고, 블록을 성공적으로 생성하게 되면 코인을 주는데, <그림5>는 블록체인 상에서 거래 데이터를 검증 및 기록하고, 이에 대한 보상으로 트랜잭션을 연결하여 블록체인을 채굴한 화면이다. 또한, 개인정보 관리자인 소유자가 블록을 재연결하기 전까지는 모든 정보는 블라인드 되며, 블록체인 해시값만 남아 이를 관리하여 해시값의 소유자가 누구인지 추측 및 확인이 불가능하게 되는데, 최종적으로 <그림6>은 SPIPS가 개인의 암호화된 정보를 영지식증명으로 요청기관에 제출하고 제출받은 기관에서 추가 정보를 개인의 SPIPS에 전달하는 화면이다.

<그림7>은 스마트폰을 이용하여 두 개의 큐알 코드로 생성된 증명자와 검증자간의 원격 개인정보검증 초기 시뮬레이션 화면이며, 지금까지 기술한 영지

```
public static String generateHash(String text) {
    try {
        MessageDigest digest = MessageDigest.getInstance(algorithm:"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, msg:null, ex);
    }
    return null;
}
```

<그림 4> 영지식증명 블록체인 아이디 생성

```
public void mine(Block block) {
    this.blockChain.add(block);
    this.nodes.forEach((node) -> {
        try {
            node.add((Block) block.clone());
        } catch (CloneNotSupportedException ex) {
            Logger.getLogger(Node.class.getName()).log(Level.SEVERE, msg:null, ex);
        }
    });
}
```

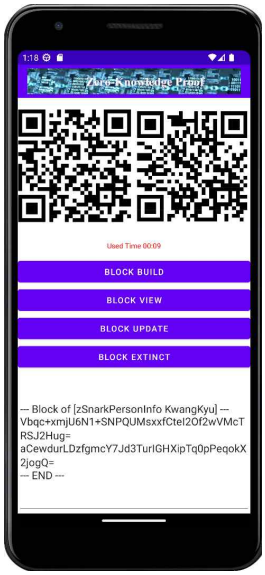
<그림 5> 영지식증명 블록체인 채굴

```
public String printBlockChain(String strBlock) {
    StringBuilder builder = new StringBuilder();

    builder.append("--- Block of [" + address + "] ---\n");
    for (Block block : this.blockChain.getBlocks()) {
        builder.append(block.hash).append(str:"\n");
    }
    builder.append(str:"--- END ---");

    strBlock = builder.toString();
    return strBlock;
}
```

<그림 6> 영지식증명 블록체인 생성 결과

식증명 블록체인 아이디 생성부터 채굴, 블록체인 결과를 스마트폰의 메뉴로 구성하였다. BLOCK BUILD는 온체인 상에서의 블록을 채굴 및 생성하며, 채굴된 블록체인은 <그림8>처럼 BLOCK VIEW로 확인할 수 있다. 또한, 새로운 블록이 연결되면 BLOCK UPDATE 메뉴로 추가하여 블록체인에 탑재되며, 블

<그림 7> 스마트폰을 이용한 영지식증명 블록체인 초기 화면



<그림 8> 스마트폰을 이용한 영지식증명 블록체인 생성 결과

록체인 연결에 실패할 경우는 BLOCK EXTINCT 메뉴로 초기화한다.

제안 기법은 스마트폰을 이용하여 블록체인의 신원증명기술을 활용할 뿐 아니라, 영지식증명을 적용하여 블록의 신뢰성 확보 및 증명 시간을 단축하고 탈중앙화가 가능함을 보임으로써, 이 분야 처음으로 스마트폰을 이용한 SPIPS를 성공적으로 구축하였다. 아울러 개인정보의 활용가치가 높아짐에 따라 개인정보를 제공하는 방법에 대한 논의가 활발하나, 개인정보를 요구하는 기관이나 인증기관은 필요 이상의 개인 정보가 노출되어, 여러 문제점의 한계를 극복하지 못하고 있다. 하지만, 본 제안의 PBFT 분산 합의 알고리즘의 영지식증명을 활용하여 저장된 개별정보는 개인 인증정보와 결합하여 보호되고, 소유자의 선택에 따른 정보를 안전하게 제공하는 개인정보 인증을 구현하므로 서, 무결성만 보장하던 블록체인 시스템의 한계를 넘어, 조건과 상황에 따라 자동으로 실행되는 SPIPS로 개인정보보호의 우수함을 보일 수 있었다.

IV. 결론

본 논문에서는 스마트폰의 탈중앙화 신원 증명에 영지식증명을 융합하여 개인정보 관리 주체를 소유권자인 개인에게 위임하는 스마트 개인정보 제공 시스템(SPIPS)을 구현하였다. 구현된 SPIPS는 zk-SNARK를 블록체인의 헤더를 인증하는데 필요한 PBFT의 알고리즘에 따라 영지식증명을 활용하였다. 제안 기법은 지금까지 스마트폰 환경에서는 처음으로 영지식증명 기반 개인정보 인증에 관한 기법으로 구현하였으며, 개인정보 인증 분야에서 사용 가능성이 높고 성능이 우수한 기법이다. 본 제안 기법의 구현으로 최종 완성된 SPIPS는 개인 정보를 소유자가 직접 안전하게 관리하고, 소유자의 선택에 따른 정보를 제공하여 개인 정보 보안성 향상에 기여할 수 있을 것이다. 향후에는 영지식증명 기반으로 비트코인과 같은 디지털 통화, 개인 정보를 공개하지 않고 발신자의 신원을 확인하는 보안 메시징과 같은 앱을 개발할 계획이다.

참고문헌

[1] Nakamoto Satoshi, “Bitcoin: A peer-to-peer electronic cash system”,Oct., 2008.[2]Ahmed Kosba, et al, “Hawk: The blockchain model of cryptography andprivacy-preserving Smart Contracts,” 2016 IEEE symposium on security and privacy(SP), pp. 839-858, San Jose, USA, May., 2016.

[3] S. Agrawal, C. Ganesh and P.Mohassel, “Non-interactive zero knowledge proofs for composite statements,” CRYPTO2018, pp. 643-673, Aug., 2018.

[4] Groth Jens, “On the size of pair ing-based non-interactive arguments,” Annual International Conference on the Theory andApplications of Cryptographic Techniques. Springer, Berlin, Heidelberg,2016.

[5] Rui Zhang, Rui Xue, and Ling Liu. “Security and Privacy on Blockchain” July., 2019.

[6] Wenyu Li, Chenglin Feng, Lei Zhang “A Scalable Multi-Layer PBFT Consensus forBlockchain”, May., 2021.

[7] B.G. Kim, Y.S. Cho, S.H. Kim, H. S. Kim “A Security Analysis of Blockchain-Based Did Services”, Jan., 2021.

[8] Xiaohui Yang, Wenjie Li, Azero-knowledge-proof -based digitalidentity management scheme in blockchain., 2020.

[9] C.H. Yoon, J.H. Hwang, M.J. Cho, “Study on DID Application Methods for Blockchain-Based Traffic Forensic.,Jan,. 2021.

[10] Duc Anh Luong; Jong Hwan Park “Privacy-Preserving Blockchain-Based Health care System for IoT Devices Using zk-SNARK,” May., 2022.

[11] A.E. Barros Tomaz, J.C. Do Nascimento ,A.S.Hafid, J.N. De Souza, “Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof andBlockchain,” IEEE. Nov., 2020.

[12] T. Bai, Y. Hu, J. He, H. Fan, Z, An, “A Healthcare Identity System Based on Fabric Block chain and Zero-Knowledge Proof,” mdpi.com, Oct., 2022.

[13] 이광규, “블록체인 기반 영지식을 활용한 개인정보 인증 구현,” 한국통신학회논문지, 47권10호, 2022년, pp.1598-1605.

■ 저자소개 ■

이 광 규
(Lee Kwangkyu)

1996년 3월~현재 신한대학교 소프트웨어융합학과 교수
2002년 8월 충북대학교 컴퓨터과학과(이학박사)
1991년 2월 동국대학교 수학과(이학석사)
1985년 2월 동국대학교 수학과(이학사)

관심분야 : 인공지능, 빅데이터, 블록체인, 정보보안
E-mail : kklee@shinhan.ac.kr

논문접수일 : 2023년 7월 06일
수정접수일 : 2023년 7월 20일(1차)
2023년 8월 04일(2차)
2023년 8월 21일(3차)
게재확정일 : 2023년 8월 25일