Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 2 pp. 452-458, 2021

https://doi.org/10.5762/KAIS.2021.22.2.452
ISSN 1975-4701 / eISSN 2288-4688

블록체인 기반 새로운 신원확인 체계

정용훈
주식회사 바스랩

Blockchain-based new identification system

Yong-Hoon Jung
BaaS LAB

요 약 인터넷 환경과 컴퓨팅 환경이 활용되는 분야 증가로 개인정보의 활용가치와 중요성이 높아지고 있으며, 사용자 인증 기술 또한 변화하고 있다. 현재까지 금융권 위주로 사용되고 있는 공인인증서는 폐지 문제로 생체인증 기술로 교체되고 있다. 하지만 생체정보는 한번 유출되면 수정할 수 없다는 문제점을 내포하고 있다. 최근 블록체인 기술의 등장으로 사용자 인증 방식에 대한 연구가 활발하게 진행되고 있다.
본 논문에서는 공인인증서와 블록체인 기반 사용자 인증 방법 모두를 시스템 변경 없이 사용할 수 있도록 설계하였으며, 주민등록번호를 대체할 수 있는 새로운 분산 ID(DID) 발급 및 재발급, 검증, 위임 방법을 제안한다. 제안하는 시스템에서는 블록체인에 제한 없이 사용이 가능하다. 단 현재 사용되고 있는 분산 ID는 검증을 위해 상호연동지원센터에 응용프로그램 설치가 필요하다. 분산 ID는 별도의 회원가입 없이 인증할 수 있으므로 무분별한 정보 수집을 방지할 수 있다. 기존 시스템과 보안성, 편의성, 확정성을 비교하였으며, 다양한 공격방법과 휴대성, 대리 사용 등을 통해 우수함을 입증하였다.

Abstract The value and importance of personal information are increasing due to the increasing number of fields where the Internet environment and computing environment are used, and user authentication technology is also changing. Until now, accredited certificates, which are mainly used in the financial sector, are being replaced with biometric authentication technology due to the problem of revocation. However, another problem is that biometric information cannot be modified once it is leaked. Recently, with the advent of blockchain technology, research on user authentication methods has actively progressed. In this paper, both public certificate and blockchain-based user authentication can be used without system change, and a new DID issuance and reissuance method that can replace the resident registration number is presented. The proposed system can be used without restrictions in a blockchain. However, the currently used DID requires installation of an application at the Interworking Support Center for verification. Since a DID can be authenticated without registering as a member, indiscriminate information collection can be prevented. Security, convenience, and determinism are compared with the existing system, and excellence is proven based on various attack methods, its portability, and proxy use.

Keywords : Authentication, Identification, One-time Random number, DID, Blockchain

*Corresponding Author : Yong-Hoon Jung(BaaS LAB)
email: jung7773@naver.com
Received November 9, 2020 Revised December 8, 2020
Accepted February 5, 2021 Published February 28, 2021

1. 서론

최근 블록체인 기술의 등장으로 중앙화된 시스템에서 탈중앙화 시스템으로 변화하고 하고 있다. 블록체인 기술은 합의원장과 스마트 컨트렉트를 이용하여 문서, 증명, 인증, 검증, 저장 등이 필요한 다양한 분야에서 보안성과 신뢰성을 향상시키기 위해 지속적인 연구가 진행되고 있다.

사용자 인증은 온라인 서비스에 주로 사용되고 있으며 ID/PW, 공인인증서, SMS, PIN 등이 사용되고 있다. 하지만 분실 및 도용, 위임 등으로 사고가 빈번하게 발생하고 있다[1].

최근 블록체인 기술을 이용한 사용자 인증 방법으로 사용자의 개인정보 또는 민감정보를 서비스 제공기관이 수집하지 않고 사용자의 휴대폰, 개인 클라우드, 블록체인 등에 안전하게 저장하는 방법에 대한 연구가 활발하게 진행되고 있다.

제안하는 블록체인 기반 통합 신원확인 체계는 기존 사용자 인증 방법과 제안하는 방법을 시스템 변경 없이 모두 사용할 수 있는 통합 신원확인 체계를 제안한다. 제안하는 통합 신원확인 체계는 향후 민간기업과 공공기관이 생성하는 모든 분산ID(DID)를 수용할 수 있으며, 공인인증서, SMS, PIN 등 모두 사용할 수 있는 방법을 제공한다.

3장에서는 통합 신원확인 체계를 구축하기 위한 각각의 역할, 기능, 분산ID(DID) 발급 방법 등을 기술한다. 4장에서는 제안하는 통합 신원확인 체계에 대한 안전성과 편의성, 확장성을 기준으로 기존 시스템과 비교 분석을 통해 우수성을 입증하였다.

2. 관련연구

2.1 블록체인

블록체인은 공공 거래 장부로 불리는 데이터 분산 처리기술을 의미한다. 블록체인 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술을 말한다. 블록체인에서 블록은 개인과 개인의 거래(P2P) 데이터가 기록되는 장부를 말한다. 이런 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 체인 구조를 가지게 된다[2].

모든 사용자가 거래 내역을 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인해야 한다. 기존 거래 방식에서는 중앙 서버를 공격하는 방식으로 데이터 위변조가 가능하다. 블록체인 기술은 데이터를 여러 명이 나누어 저장하기 때문에 위변조가 어렵다는 특징을 가진다. 블록체인 네트워크를 위변조하기 위해서는 참여자의 거래 데이터를 모두 공격해야하기 때문에 사실상 해킹은 불가능하다.

또한 블록체인은 다수가 데이터를 저장, 증명하기 때문에 중앙 관리자가 존재하지 않는다.

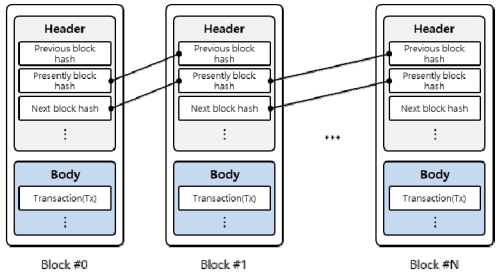

Fig. 1. Blockchain Structure

최근 블록체인 환경에서 사용자 인증, 사용자 식별 등에 관한 연구가 활발하게 진행되고 있다. 여러 민간 기업들은 DID 얼라이언스를 출범하고 분산ID(DID) 제품을 출시하고 있으며, 대학 및 연구소에서는 논문을 통해 발표되고 있다[1-5]. 또한 정부 기관에서도 블록체인 기술을 이용한 신분증 사업을 추진하고 있다.

2.2 사용자 인증

사용자 인증 방법은 ID/PW, 공인인증서, 생체인증, PIN 등 다양한 방법을 사용하고 있으며, 최근 생체정보, 블록체인 등을 이용한 인증 기술이 활발하게 연구되고 있다[4].

2.2.1 PKI(Public Key Infrastructure)

인터넷이나 인트라넷 상의 사용자들에게 보안 서비스를 제공하는 체계로 국가 공개키 기반구조(NPKI, National Public Key Infrastructure)를 따르고 있다.

최상위 인증기관은 한국인터넷진흥원(KISA)에서 역할을 하고 있으며, 하위에는 5개의 인증기관(CA, Certificate Authority)이 있다. 인증기관은 한국인터넷진흥원을 대행하여 인증서 발급 및 재발급 서비스를 제공한다. 인증기관 하위에는 공인인증서의 접수 및 등록 등의 일을 대행하는 은행, 증권사와 같은 등록대행기관(RA)이 존재한다[6].

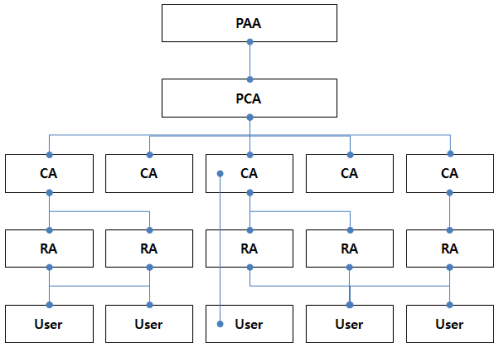

Fig. 2. Public Key Infrastructure

사용자들은 인증기관 또는 은행, 증권사에서 인증서를 발급 및 재발급 받을 수 있다.

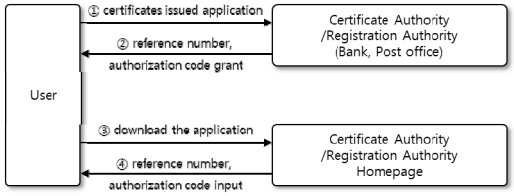

Fig. 3. Issuing Certificates

인증서는 인터넷상에서 전자거래 등을 안심하게 사용할 수 있도록 해주는 사이버 증명서로 인감증명서와 비유할 수 있다. 인증서로 전자서명을 하면 상대방이 서명한 사람이 누구인지를 확인할 수 있으며, 전자문서의 위조나 변조 예방 및 거래 사실을 증명할 수 있다[5].

2.1.2 FIDO

FIDO(Fast Identity Online)는 온라인 환경에서 바이오 인식 기술을 활용한 인증방식에 대한 글로벌 인증 표준 기술이다.

FIDO 인증 프로토콜은 UAF(Universal Authentication Framework)와 U2F(Universal Second Factor) 기술로 분류된다.

UAF는 패스워드를 입력하지 않는 형태의 인증으로 Authenticator가 기기에 포함된 형태이다.

U2F는 기존 패스워드 기반의 인증 후 2Factor 형태로 Authenticator를 통한 FIDO 인증을 수행한다. Authenticator가 기기에 포함되지 않는 형태이다[7].

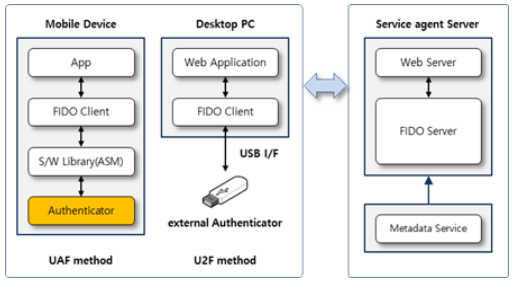

Fig. 4. FIDO system

2.3 DID(Decentralized Identifier)

W3C Working group 에서는 분산 신원확인 기술에 대해 표준화를 추진하고 있다. W3C 분산 신원확인 기술(DID)은 검증 가능하고 탈중앙화된 디지털 신원을 증명하기 위한 새로운 형식의 식별자를 말한다. 이러한 새로운 식별자는 DID 컨트롤러가 DID의 제어권을 증명하고, 중앙화된 레지스트리, 신원 제공자, 인증기관 등으로부터 독립적으로 구현할 수 있도록 설계하고 있다.

DID는 DID 주체와 관련된 URL로써, DID문서라는 방식을 통해 해당 주체와 신뢰할 수 있는 상호작용을 가능케 하는 도구이다. DID문서는 특정 DID를 어떻게 사용하는지에 대한 간단한 설명 문서이다. 각 DID 문서는 암호학적 요소, 검증 메소드 서비스 엔드포인트 등으로 표현될 수 있다. 해당 요소들은 DID 컨트롤러가 DID의 통제권에 대한 증명을 가능하게 하는 메커니즘 집합을 제공한다. 서비스 엔드포인트는 DID주체와 신뢰할 수 있는 상호작용을 가능하게 한다[8-10].

3. 본론

본 논문에서는 기존 인증서와 새로운 블록체인 기반 신원확인 체계 모두 사용 가능한 통합 신원확인 체계이다. 제안하는 통합 신원확인 체계에서 사용자 인증을 위해 분산ID(Decentralization Identity) 발급, 재발급, 검증 등을 제안한다.

제안하는 통합 신원확인 체계는 블록체인, 상호연동지원센터,(Verification Center : VC), 검증기관(Verification Authority : VA), 등록대행기관(Registration Authority : RA), 사용자로 구성된다.

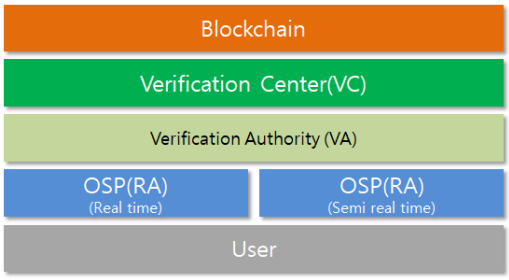

Fig. 5. System architecture

블록체인은 용도에 따라 컨소시엄(Consortium), 프라이빗(Private), 퍼블릭(Public) 블록체인으로 선택이 가능하다. 컨소시엄 블록체인은 컨소시엄 구성원에 의해 승인 받은 참여자만이 블록 생성에 참여할 수 있으며, 프라이빗 블록체인과 유사하다. 컨소시엄 블록체인은 은행, 증권과 같이 제한된 기관에서 사용한다.

프라이빗 블록체인은 상호연동지원센터(최상위 기관)에서 분산ID 발급 및 등록, 재발급을 위해 사용되며, 최상위 기간 이외 접근이 불가능하다.

퍼블릭 블록체인은 은행, 증권 등을 제외한 모든 기관에서 사용이 가능하며, 실시간 검증이 아닌 준 실시간 검증을 필요로 하는 곳에서 사용된다. 예를 들어 학교, 회사 등이다.

3.1 블록체인

블록체인은 인증서와 분산ID, 문서(증명서) 등을 저장하는 용도로 사용된다. 프라이빗 블록체인은 최상위 기관만 접근이 가능하며, 발급된 분산ID 등록 및 재발급 용도이다. 분산ID 폐기는 별도의 체인을 구성하여 관리한다.

퍼블릭 블록체인은 실시간 서비스가 필요하지 않은 문서(각종 증명서) 등을 저장하는 용도로 주로 사용되며, 모든 참여자가 블록 생성에 참여할 수 있다.

컨소시엄 블록체인은 실시간 서비스가 필요한 금융권과 같은 기업에서 사용하기 적합한 형태이다. 블록 생성은 승인 받은 참여자만 블록 생성에 참여할 수 있다. 예를 들어 은행에서는 본점과 지점만 블록 생성에 참여할 수 있도록 제한할 수 있다.

합의 알고리즘은 처리 속도가 빠른 DPoS 방식을 사용하였다. 합의 알고리즘에 대한 제한은 없다.

상호연동지원센터는 기존 인증서 사용자를 위한 별도의 블록체인을 구성할 수 있다. 이 경우 유효한 인증서 검증을 위한 블록체인과 폐지된 인증서를 검증할 수 있는 블록체인이 별도로 필요하다.

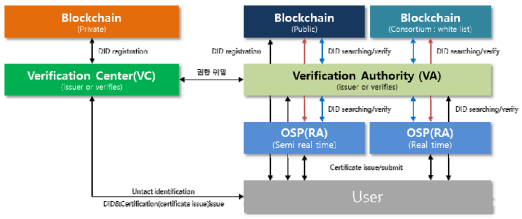

Fig. 6. Proposed system

3.2 상호연동지원센터(VC, Verification Center)

상호연동지원센터는 인증서 사용자와 블록체인 사용자 모두가 사용할 수 있도록 호환성을 제공한다. 상호연동지원센터의 역할로는 분산ID 발급, 등록, 재발급, 검증, 폐기 등과 검증기관 권한 위임 및 관리 등을 한다.

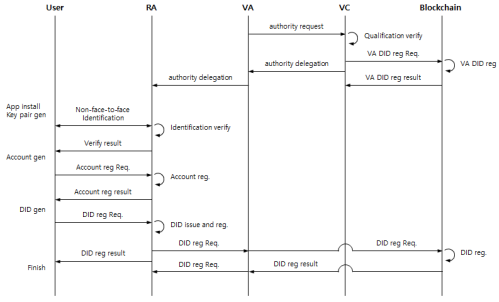

Fig. 7. Proposed System flow

상호연동지원센터에서는 블록체인 코드를 이용하여 블록체인을 구분한다. 만약 기존 공인인증서인 경우 구분코드를 “00” 으로 구분하여 기존 인증서 시스템을 이용하거나 새로운 인증서 확인체계를 이용하게 된다.

사용자 DID는 사용자의 휴대폰에 저장되며 복구를 위해 프라이빗 블록체인에 저장하여 상호연동지원세터가 관리한다.

3.3 검증기관(VA, Verification Authority)

검증기관은 상호연동지원센터로부터 권한을 위임 받아 분산ID 발급, 검증, 증명서 발급, 검증, 폐기, 수정 등의 역할을 한다. 검증기관은 상호연동지원센터로부터 허가를 받아야 하며, 허가를 받기 위한 시설 및 장비 등을 규격에 맞게 구비해야 한다. 검증기관은 상호연동지원센터가 관리하는 프라이빗 블록체인에는 접근이 불가능하다.

검증기관은 등록 대행기관을 지정할 수 있다.

3.4 등록 대행기관(RA, Registration Authority)

등록 대행기관은 검증기관으로부터 허가 받은 기관 또는 기업만 가능하다. 등록 대행기관의 역할은 분산ID 신청 접수 대행, 인증서 접수, 차체 발급한 증명서 검증 등 검증기관 보조 역할을 한다.

3.5 사용자

사용자는 스마트폰에 Wallet을 설치해야 하고, 설치된 Wallet에 분산ID, 증명서, 인증서 등을 보관한다. Wallet에 보관된 분산ID, 각종 증명서 등은 본인이 원하는 곳에 직접 전달하거나 권한을 부여하여 정보에 대한 접근 범위를 지정할 수 있다.

3.6 분산ID 발급

분산ID 발급은 대면과 비대면 모두 가능하며, 본인 확인 절차는 필수 사항이다. 본인 확인 방법에는 휴대폰, 신분증 진위확인, 기존 계좌 활용, I-PIN 등 사용이 가능하다.

분산ID 발급에 필요한 정보로는 사용자 Account, Device ID, Salt값이 필요하다. Account는 사용자가 직접 생성 또는 자동 생성이 가능하며 발급기관에 제출한다. 제출된 Account 정보는 발급기관에서 블록체인에 등록한다. Account 생성은 다음과 같은 식(1)을 통해 생성된다.

$$Account = BIP39(12digit\,user\,string) \quad (1)$$

How to create an account

생성된 Account 정보와 Device ID, Salt값을 이용하여 분산ID를 생성한다. 생성된 Account 정보와 DID 사용자 정보는 발급기관에 전송되며, 발급기관에서는 이를 검증 후 분산ID 발급 및 블록체인에 등록한다. DID 사용자 정보는 다음과 같은 식(2)를 통해 생성된다.

$$DID_{Userinfo} = 01 \| Account \| User_{DS}(Account) \| RA_{DS} \quad (2)$$

DID generation based on user information

생성된 분산ID는 발급기관을 통해 블록체인에 저장된다. 블록체인에 저장되는 분산ID 정보는 다음과 같다.

$$DID = 01 \| DID_{Userinfo} \| RA_{DS}(DID_{Userinfo} \| DID_{RA}) \| CI \| KR \| M \| Y \quad (3)$$

Completed DID

"01"은 블록체인을 식별하기 위한 코드값으로 서로 다른 블록체인을 구분한다. $RA_{DS}(DID_{User_info}||DID_{RA})$는 사용자의 디바이스에서 생성된 DID와 발급기관 DID를 전자서명한 값이다. "KR"은 국가 분류 코드이며, "M"은 성별, "Y or N"은 성인 여부를 의미한다.

CI는 본인확인 용으로 본인확인 기관으로부터 발급한 CI와 사설(VC or VA) CI 두 가지가 있다 첫 번째는 본인확인 기관으로부터 발급된 CI 생성은 식(4)와 같다.

$$CI = HMAC_{SK}((RN \| Padding) \oplus S_A) \quad (4)$$

How to create CI of identity verification agency

두 번째 사설 CI로 생성 방식은 본인확인 기관에서 발급하는 CI와 유사하다. 생성 방법은 식(5)와 같다.

$$CI = HMAC_{SK}((Account(\text{or } DID) \| Padding) \oplus S_A) \quad (5)$$

How to create private CI

Account는 본인확인 완료 후 발급된 Account만 허용되며 12자리 문자(12Byte)이다. Padding은 입력 값을 512비트(bit)로 만들기 위해 Account 96비트(bit)를 제외한 416비트(bit)를 "0x00 ~ 000"으로 채워 넣는다. SK와 SA는 VC와 VA가 공유하는 비밀정보로 64바이트(byte)로 이루어진다.

3.7 분산ID 검증 및 재발급

분산ID 검증은 상호연동지원센터, 검증기관을 통해서만 검증된다. 상호연동지원센터와 검증기관은 분산ID와 인증서 모두를 검증할 수 있다.

분산ID 검증은 블록체인에 등록된 사용자 분산ID와 공개키를 이용하여 발급기관 전자서명 검증으로 완료된다. 분산ID 재발급은 상호연동지원센터에서만 가능하며, 본인확인 후 재발급 된다. 재발급은 기존 기기를 사용하는 경우와 새로운 기기를 사용하는 경우 달라진다. 기존 기기를 사용하는 경우 본인확인 후 블록체인에 등록된 분산ID를 사용자에게 전달한다. 새로운 기기인 경우 기존 Device ID가 변경되었으므로 삭제 후 새롭게 생성한다. 삭제한 분산ID와 Device ID는 별로 관리하여 재사용할 수 없도록 한다.

3.8 권한 위임

검증기관은 상호연동지원센터로부터 권한을 위임 받아야만 한다. 검증기관은 상호연동지원센터가 정한 절차와 설비를 갖춰야만 권한을 위임 받을 수 있다. 권한을 위임 받기 위한 절차는 다음과 같다.

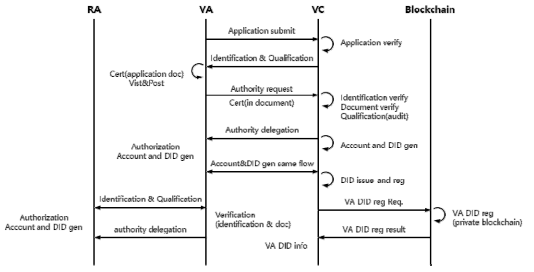

Fig. 8. Authority Delegation Procedure

4. 성능분석

성능 분석은 보안성을 중심으로 하였으며, 편의성과 확장성을 추가로 고려하였다. 보안성은 다양한 공격방식과 보안 침해 요소를 위주로 하였으며, 편의성 및 확장성은 등록 방법 및 본인확인, 시스템 확장성 등으로 한다.

4.1 보안성

기존 인증 시스템은 사용자의 인증 정보를 중앙에 저장함으로써 악의적인 사용자로부터 공격 포인트가 되고 있다. 공격 방식으로는 스파이웨어(spyware), 재전송 공격(Replay Attack), 추측 공격, Sniffing 등이 있다.

블록체인 기술은 정보를 중앙 서버에 저장하지 않고 블록체인에 분산 저장함으로서 시스템 공격 포인트가 늘어나기 때문에 공격에 대한 효율성이 떨어진다. 만약 정보를 획득한 경우 조합을 위한 알고리즘과 복호화키를 모를 경우 의미 없는 정보라 할 수 있다.

Table 1. Comparison of authentication techniques

	safety	convenience
PIN	lowness	height
PW	normal	normal
OTP	height	lowness
Certificate	height	lowness
Proposal	height	height

또한 모든 정보는 App내에서 암호화 및 복호화가 수행되며, App에 접근하기 위해서는 등록된 생체인증을 통해서만 접근이 가능하다.

Table 2. Safety comparison

	Certification	Proposal
Management entity	User	User
Copy	○	X
Steal	○	X
Man in the middle attack	○	X

발급된 분산ID는 사용자의 전용 App에서 1회 또는 일정 시간 동안 1회만 사용 가능하도록 하기 때문에 재전송 공격 및 추측 공격, 중간자 공격으로부터 안전하다.

중간자 공격은 암호화 통신을 기본으로 수행하며, 1회성 값을 추가하여 안전하다. 또한 생체정보와 디바이스 등록을 통해 복사와 도용으로부터 안전하다.

4.2 편의성 및 확장성

제안하는 신원확인 체계는 새로운 사용자 식별 정보로 주민등록번호를 대체할 수 있는 수단이다. 새로운 신원확인 체계는 특정 매체를 소유하지 않고 휴대폰만 있으면 사용할 수 있다. 사용자는 자신의 정보에 접근하려는 사용자(서비스제공기관)에게 접근 권한을 부여하고 정보를 이용할 수 있도록 함으로써 최소한의 정보를 공개할 수 있다.

기존 소유기반 인증 방식은 안전성을 높이기 위해 지식 기반 인증과 함께 사용되는 경우가 대부분이다. 또한 서비스 제공기관에 따라 회원가입 및 서비스가 제한적이다. 제안하는 신원확인 체계는 발급 받은 분산ID를 통해 회원가입 없이 사용이 가능하며, 서비스에 제한적이지 않다.

제안하는 신원확인 체계는 모든 블록체인 환경에서 사용이 가능하며, 확장성을 고려하여 별도의 블록체인 분류 코드를 사용하였다. 또한 사용자 휴대폰에 설치된 App 이외에 별도 설치 프로그램 또는 장치 없이 사용이 가능하다.

5. 결론

최근 인터넷과 정보통신 기기의 발달로 다양한 방법을 통해 개인을 식별하고 있다. 이로 인해 사용자의 개인정

보는 무분별하게 수집되어 마케팅 목적으로 활용되거나 거래되고 있다. 정부에서는 회원가입 시 개인정보를 최소로 수집하도록 하고 있으며, 불필요한 기존 개인정보를 삭제하도록 권고하고 있다.

제안하는 신원확인 체계는 기존 주민등록번호를 대체할 수 있으며, 기존 시스템과 호환이 가능한 새롭고 안전한 신원확인 체계를 제안하였다.

제안하는 신원확인 체계는 블록체인 기술과 전용 App(Wallet)을 기본으로 한다. 사용자의 신원인증을 위한 분산 ID(DID)는 사용자 휴대폰에서 직접 발급되며, 상호연동지원센터 및 검증기관에서 이를 검증하고 등록한다. 또한 전용 App에 접근하기 위해서는 생체인증 기술을 사용하여 본인이 아닌 타인이 사용 불가능하게 하였다. 또한 하나의 디바이스에서만 사용할 수 있도록 기기 등록을 통해 안전성을 확보하였다. 블록체인에 분산 저장된 정보를 사용하기 위해서는 사용자의 권한을 획득하기 전에는 접근이 불가능하다.

향후 사용자의 다양한 데이터를 안전하게 저장할 수 있도록 마이데이터(MyData) 서비스를 설계하고, 분산 ID와 연계하여 사용자 데이터를 관리할 것이다. 또한 권한 부여 방법을 좀 더 세밀하게 구분하여 개인 데이터가 불법적으로 사용되는 것을 방지할 것이다. 마이데이터 서비스는 발급받은 증명서를 별도 보관하지 않고 블록체인에 분산 저장한다. 분산된 정보에 접근한 내역은 사용자가 쉽게 확인할 수 있도록 분산 ID를 통해 접근한 사용자, 서비스 제공기관 등을 파악할 수 있도록 연구할 것이다.

References

[1] Kim Jai-Yong, Jung Yong-hoon, Jun Moon-Suk, Lee Sang-Beon, "User Integrated Authentication System using EID in Blockchain Environment", Journal of the Korea Academia-Industrial cooperation Society, Vol.21, No.3, pp.24-31, Mar. 2020.
DOI : http://dx.doi.org/10.5762/KAIS.2020.21.3.24

[2] S. G. Moon, M. S. Kim, H. J. Kim, "Design of an Integrated University Information Service Model Based on Block Chain", Journal of the Korea Academia-Industrial cooperation Society Vol. 20, No.2 pp. 43-50, 2019.
DOI : https://doi.org/10.5762/KAIS.2019.20.2.43

[3] S. D. Yoo, "A Study on Consensus Algorithm based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication , Vol.19, No.3, pp.25-32, 2019.
DOI : https://doi.org/10.7236/JIIBC.2019.19.3.25

[4] S. J. Han, S. T. Kim, S. Y. park, "A GDPR based Approach to Enhancing Blockchain Privacy", The Journal of The Institute of Internet, Broadcasting and Communication , Vol.19, No.5, pp.33-38, 2019.
DOI : https://doi.org/10.7236/JIIBC.2019.19.5.33

[5] Sang-Il Choi, "Implementation of Service Model for Data-Driven Integrated Urban Management Service Operation Using Blockchain Technology", The Journal of The Korea Academia Industrial, Vol.20, No.10, pp.503-514, 2019.
DOI : https://doi.org/10.5762/KAIS.2019.20.10.503

[6] Korea Certification Authority Centrol, KISA(Korea Internet Security Agency), http://rootca.or.kr/kor/main.jsp

[7] FIDO Alliance, https://fidoalliance.org/specifications/?lang=ko

[8] W3C Working Draft "Decentralized Identifiers (DIDs) v1.0", 14 July 2020, https://www.w3.org/TR/did-core/

[9] Security Technology Research Team, "Overseas Research Trends Related to Blockchain Interworking" FINANCIAL SECURITY INSTITUTE, Korea

[10] FINANCIAL SECURITY INSTITUTE, "Electronic Finance and Financial Security No. 22", Periodicals, FINANCIAL SECURITY INSTITUTE, Korea, pp97~110

정 용 훈(Yong-Hoon Jung) [종신회원]

- 2006년 8월 : 숭실대학교 일반대학원 컴퓨터학과(공학석사)
- 2010년 2월 : 숭실대학교 일반대학원 컴퓨터학과(공학박사)
- 2011년 3월 ~ 2014년 2월 : 서일대학교 조교수
- 2018년 8월 ~ 현재 : 바스랩 연구소장
- 2019년 11월 ~ 현재 : 유니허브랩 기술이사 겸직
- 현) 한국산학기술학회 상임이사

〈관심분야〉
블록체인, 사용자 인증, 네트워크 보안, 융합 보안