Journal of Korea Multimedia Society Vol. 24, No. 6, June 2021(pp. 760-767)
https://doi.org/10.9717/kmms.2021.24.6.760

프라이빗 블록체인을 사용한 DID 활용 연구

박종규[†], 권성근[††], 권기룡[†††], 이석환[††††]

A Research on the Use of DID Using a Private Blockchain

Jong-Gyu Park[†], Seong-Geun Kwon[††], Ki-Ryong Kwon[†††], Suk-Hwan Lee[††††]

ABSTRACT

The identity verification is one of the most important technologies in online services. Many services in society are provided online, and the service is provided after confirming the user's identity. Users can do a lot of things online, but they also have side effects. Online digital information is easily manipulated and it is difficult to verify its authenticity, causing social confusion. Accordingly, there has been a movement for individuals to directly manage their identity information using DID. In this paper, we propose a system that can authenticate identity by directly adding own personal information and issuing an identifier using DID technology based on a private blockchain. Then, to verify the proposed system, the scenario is executed and verified.

Key words: ID Authentication, Decentralized Identifier, Private Blockchain, Online Services, Fraud Detection

1. 서 론

최근 사회의 많은 서비스들이 오프라인 영역에서 온라인으로 이루어지면서 생활의 아주 밀접한 영역까지 온라인 서비스의 혜택을 받고 있다. 이제 사람들은 금융, 쇼핑, 문화 등 민간 부문의 서비스 뿐만 아니라 교육, 건강, 민원 등 정부의 행정 서비스까지 온라인으로 사용하고 있다. 이렇게 온라인으로 서비스를 받기 위해서 필수적인 기술 중 하나는 신원 증명 기술이다. 가장 기본적인 신원 증명으로는 아이디와 패스워드를 이용한 고전적인 방법부터 신뢰할 수 있는 기관으로부터 발급받아 사용하는 인증서나 최근엔 스마트폰 등을 활용한 지문인식, 얼굴인식 등 바이오 인증 기술도 있다. 그러나 일반적인 신원 증명 기술은 사용자가 서비스를 받을 수 있는 최소한의 자격을 갖추었는지만 확인하는 것으로써 서비스나 서비스를 통해 생성되는 정보에 대한 식별자를 구분하지는 않는다. 그리고 디지털 정보는 조작이 쉽고 원본의 진위를 확인하기가 어려워 페이크 뉴스와 같이 잘못된 정보가 온라인에 유포되면 이를 검증하기가 쉽지 않다.

일반적으로 온라인에서 정보의 출처를 표시하기

※ Corresponding Author : Suk-hwan Lee, Address: (49315) 37, Nakdong-daero 550beon-gil, Saha-gu, Busan, Korea, TEL : +82-51-200-7782, FAX : +82-51-200-7783, E-mail : skylee@dau.ac.kr
Receipt date : May 25, 2021, Approval date : May 28, 2021
[†] Dept. of Computer Engineering, Dong-A University (E-mail : pjk5401@gmail.com)
[††] Dept. of Electronics Engineering, KyungIl University (E-mail : sgkwon@kiu.ac.kr)
[†††] Dept. of IT Convergence and Application Engineering, Pukyong National University (E-mail : krkwon@pknu.ac.kr)
[††††] Dept. of Computer Engineering, Dong-A University
※ This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1F1A1069124, 2020R1I1A306659411) and also supported by supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP- 2021-2020-0-01797) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

위해 디지털 워터마크 기술이나 디지털 권리 관리(Digital Rights Management, DRM) 기술을 활용하고, 정보의 위변조 여부 확인을 위해 해시함수를 이용한 무결성 검사를 한다[1]. 그러나 워터마크는 주로 이미지나 영상 등의 미디어에서 사용되어 그 활용범위가 상대적으로 좁고, DRM 등은 별도의 DRM 솔루션을 활용해야 하는 점이 단점이다. 해시함수를 이용한 무결성 검사는 기술적으로 매우 많은 곳에서 활용중이지만 일반 사용자가 직접 해시함수를 사용하여 어떠한 서비스에 적용하기에는 어려운 점이 많다.

본 논문에서는 온라인 상에서 제공되는 서비스와 사용자가 서비스를 사용하는 것, 그로 인해 어떠한 정보가 생성되는 것을 '행위'로 규정하였다. 그리고 이 행위에 식별자를 두어 온라인에서의 행위 그 자체를 검증하고자 한다. 예를 들어 기자가 기사를 작성하면 그 행위에 식별자를 발행하고, 이후 기사를 읽는 사람들은 기사와 함께 배포된 식별자를 확인하여 실제로 발행된 기사인지 확인할 수 있다. 각 행위에 발급하는 식별자는 기존의 단일 기관에서 배포하는 식별자가 아닌 탈중앙화 식별자(Decentralized IDentity, DID)를 사용한다[2,3]. 탈중앙화 식별자는 식별자를 생성하는 주체가 스스로 정보의 관리를 하는 것이 특징이다. 특히 탈중앙화 식별자를 이용한 신원확인을 할 때 개인이 직접 저장한 정보 중 꼭 필요한 것만 신원확인에 활용할 수 있다. 예를 들면 자신이 성인임을 증명하고자 주민등록증을 제출할 때 현재 주소지도 나오게 되는데 이는 불필요한 개인정보이며 성인임을 증명하고자 한다면 출생연도만 보여주면 된다.

본 논문에서는 상기한 행위에 대한 식별자를 만들고 검증하기 위해 기존의 탈중앙화 신원확인(Decentalized IDentifiers, DIDs)에서 제안하는 방식[3,4] 중에서 검증에 필요없는 부분들은 제외하였다. 또한 DID는 탈중앙화의 성격으로 인해 주로 블록체인 기술을 사용하는데, 이는 대부분 퍼블릭 블록체인이다. 그러나 본 논문에서는 프라이빗 블록체인으로 네트워크를 구성하여 신원인증기관(정부와 같은 행정기관)을 네트워크에 참여시켜 DID 생성 및 활용의 전 주기를 구성하고 행위 증명 시나리오를 검증해보았다[5].

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 기술적 배경이 되는 블록체인과 탈중앙화 신원확인에 대해서 알아보고, 3장에서 제안하는 프라이빗 블록체인 기반 DID 시스템에 대해 설명한다. 그리고 본 시스템을 활용하여 검증할 수 있는 행위에 대한 시나리오를 제안한다. 4장에서는 3장에서 제안한 시나리오를 테스트하여 검증하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 프라이빗 블록체인

블록체인은 2008년 S. Nakamoto[6]는 가명의 인물이 발표한 비트코인 문서에서 소개되어 비트코인과 더불어 암호화폐가 전 세계적으로 주목받게 되면서 함께 관심을 받게 되었다[5]. 주로 암호화폐를 구성하는 기술로 인지되고 있지만 실제로는 분산화된 데이터 저장 기술의 일종으로 데이터를 블록이라 부르는 모델에 해시함수를 이용하여 체인 형태로 이어나가는 것이 특징이다. 또한 다수의 노드들로 구성된 네트워크에서 중앙집중형 시스템을 갖지 않고 네트워크에 참여하는 노드들이 합의 알고리즘을 통해 블록 생성(데이터 저장)을 결정한다. 이러한 특성으로 인해 블록에 저장한 데이터는 수정하거나 지울 수 없어 신뢰성이 필요한 데이터의 저장 및 관리에 활용되고 있다. 특히 블록체인 안에 프로그램의 형태로 삽입되는 스마트 컨트랙트는 디지털로 실행되는 계약서로써 블록체인의 합의 알고리즘을 바탕으로 서로 신뢰할 수 없는 온라인 사용자들 간의 거래를 가능하게 한다[7].

프라이빗 블록체인은 블록체인 네트워크에 참여하는 노드를 제한하는 것으로 특정 권한을 가진 노드가 네트워크에 참여할 노드를 선택할 수 있다[8,9]. 이로 인해 발생하는 기존 블록체인과의 가장 큰 차이점은 중앙화 여부이다. 따라서 프라이빗 블록체인은 블록체인의 데이터 신뢰성을 보장하려는 기업에서 주로 사용한다. 프라이빗 블록체인은 네트워크에 참여할 노드를 선택할 수 있으므로 네트워크에 대한 신뢰를 가정한다. 따라서 프라이빗 블록체인에서 합의 알고리즘은, 신뢰할 수 없는 노드들 사이에 신뢰

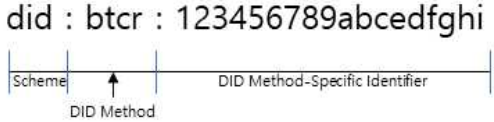

Fig. 1. A simple example of a decentralized identifier (DID).

Table 1. DID Methods.

Method Name	DLT or Network	Authors
did:example:	DID Specification	W3C Credentials Community Group
did:btcr:	Bitcoin	Christopher Allen, Ryan Grant, Kim Hamilton Duffy
did:ethr:	Ethereum	uPort
did:corda:	Corda	Nitesh Solanki, Moriz Platt, Pranav Kirtani
did:github:	Github	Transmute
did:icon:	ICON	ICONLOOP

를 만들어주는 것이 목표가 아니라 네트워크나 시스템의 장애 허용을 수행하는 것이 주를 이룬다.

2.2 탈중앙화 신원확인

탈중앙화 신원확인(Decentralized IDentifiers)은 탈중앙화 식별자(Decentalized IDentity)를 사용하는 신원증명 기술로 식별자를 생성하고 관리하는데 단일 기관이나 중앙의 시스템이 처리하는 것이 아니라 개인이 직접 ID를 발급하고 관리한다. 중앙 시스템이 없기에 분산 네트워크에서 이를 처리하는데 블록체인의 분산원장 및 증명 시스템이 DID의 요구사항과 잘 부합하기에 현재 대부분의 DID는 퍼블릭 블록체인을 기반으로 구현되고 있다. DID의 요구사항은 아래와 같다[1].

- 탈중앙화(decentralized) : 중앙 발행 기관이 없어야 한다.
- 지속성(persistent) : 식별자는 지속적이어야 하지만 기관의 지속적인 운영을 요구하지는 않아야 한다.
- 암호로 검증(cryptographically verifiable) : 식별자에 대한 제어를 암호로 증명해야 한다.
- 분해성(resolvable) : 식별자로 메타데이터를 검색할 수 있어야 한다.

DID는 크게 세 부분으로 나누어진 텍스트 문자열로 각각 1) Scheme, 2) DID Method, 3) DID Method에 따른 상세 식별자로 나뉜다[2].

Scheme은 URI에서 이 ID가 DID임을 정의한다. DID Method는 이 DID를 저장하는 방법이며 저장소로 사용할 분산원장이나 네트워크로 생각하면 된다. 마지막으로 DID Method-Specific Identifier는 해당 분산원장에서 DID가 저장된 실제 주소이다. 위의 DID를 해석하면 비트코인(btcr)에 저장된 DID Documents에 접근할 수 있다. DID Documents에는 DID의 소유자만이 알 수 있는 정보 등이 들어있으며 그 정보를 검증하여 DID로 신원을 증명한다.

3. 프라이빗 블록체인 기반 DID

3.1 프라이빗 블록체인 기반 DID 시스템 개요

본 논문에서는 상기의 DID의 구조를 프라이빗 블록체인인 하이퍼레저 패브릭(Hyperledger Fabric)

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:btcr:123456789abcdefghi",
  "authentication": [{
    "id": "did:btcr:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:btcr:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Code 1. A simple example of DID document.

으로 구현하고자 한다. 우선 프라이빗 블록체인을 사용하므로 실질적 의미로써의 탈중앙화의 개념은 흐려질 수 있으나 발급한 DID의 신원을 보장해 줄 수 있는 기관이 블록체인 네트워크에 들어옴으로써 블록체인의 고질적 문제인 오라클 문제를 해소해 줄 수 있을 것으로 보았다. 예를 들어 DID는 개인이 직접 만들어서 관리하는 식별자이므로 미성년자가 자신이 성인이라는 정보를 거짓으로 기입하여 DID를 만들었다고 하면, 해당 DID에 대한 소유자임을 증명할 수 있으므로 미성년자가 성인이라는 의미가 된다. 그러므로 실제 성인임을 신뢰기관에서 인증 받은 후 신뢰기관이 발급한 정보를 추가하여 DID를 만들면 이는 믿을 수 있는 정보가 된다. 이러한 이유로 신뢰기관에 해당하는 노드와 서비스 기관들의 노드가 블록체인 네트워크에 참여하게 된다. Fig. 2에서 gov, com0, com1은 블록체인 네트워크에 참여하는 3개의 조직이다. peer0은 각 조직마다 1개의 노드만 있는 것을 의미한다. gov는 DID의 신원을 보장하는 신뢰기관이며 com0과 com1은 서비스를 제공하는 일반 기업의 조직이다. 사용자는 Client를 이용하여 DID 발급 및 검증 api를 사용한다. 3개의 조직은 Channel 1을 사용하며 이를 통해 Ledger나 ChainCode(하이퍼레저에서 사용되는 스마트컨트랙트)를 공유한다. Odering Service는 프라이빗 블록체인인 하이퍼레저에서 사용하는 서비스이며 Oderer로 불리는 노드가 각 조직의 peer들이 발생시키는 트랜잭션을 수집하여 정리한 후 블록을 만든다. 이때 채널의 트랜잭션이 Oderer로 집중되므로 트랜잭션들을 효율적으로 정리하기 위해 메시지 큐 방식을 사용하여 장애허용 시스템을 구현한다.

사용자는 Client를 통해 각 조직에서 제공하는 서

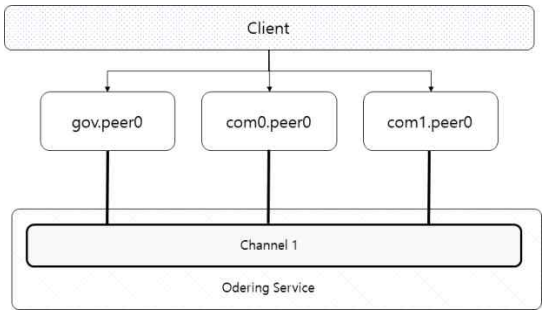

Fig. 2. Private blockchain DID system network architecture.

비스를 이용하며 이러한 서비스를 본 논문에서는 '행위'라고 규정한다. 그리고 이 행위를 검증함으로써 온라인으로 제공되는 서비스에 대한 신뢰를 높이고자 한다. 본 논문에서는 DID로 신원증명을 하는 행위에 대한 시나리오를 제안한다.

3.2 신원증명 DID 시나리오

신원증명 DID 시나리오에는 3개의 참여주체가 있으며 각각 gov, com0, user라고 한다. 이 중 gov와 com0은 프라이빗 블록체인 기반 DID 시스템에 참여하고 있다. user는 자신의 이름과 나이, 주소가 포함되어 있는 DID를 만들고자 한다. com0은 15세 이상에게만 서비스를 제공하는데, user는 여기에 자신이 만든 DID를 제출하여 com0의 서비스를 받고자 한다. 이때 DID에 있는 나이만 제출하고 이름과 주소는 제출하지 않는다. 그러나 자신이 만든 DID로는 15세 이상임을 증명할 수 없어 신뢰기관인 gov의 인증을 받아 자신의 DID에 기록하고자 한다. com0은 user가 제출한 DID를 받아 gov의 인증을 확인하고 user에게 서비스를 제공할 수 있다. 또한 user의 DID에 기록된 gov의 인증을 받은 이름, 나이, 주소 정보는 user의 동의 없이는 볼 수 없다.

아래 Fig. 3은 신원증명 DID 시나리오의 구성과 단계를 보여준다. gov의 DID는 T이고 신뢰기관이므로 스스로 신원을 증명할 수 있다고 가정한다. 또한 DID T는 블록체인에 저장되어 있다. user는 gov의 인증을 받아 DID U를 발급하고자 한다. Eu는 user의 public key로 암호화한 것이며 Et는 gov의 public key로 암호화한 것이라고 한다.

step 1 : user는 신뢰기관 gov에게 자신의 개인정보 name:user, age:20, addr:korea를 제출한다. 이때, gov는 user에게 실제 나이를 증명하기 위해 모바일 인증 등을 요청할 수 있다.

step 2 : gov는 user가 제출한 각 정보를 자신의 private key로 암호화하여 user에게 반환한다.

step 3 : user는 gov에게 받은 암호화된 정보를 다시 각각 자신의 public key로 암호화 한다. 개별적으로 암호화 하는 이유는 이후 자신이 필요한 정보만 제출하기 위해서이다. 그리고 gov 에게 인증을 받았다는 의미로 authentication에 T를 입력하고, 각각 암호화한 개인 정보, 그리고 자신의 public key를 포

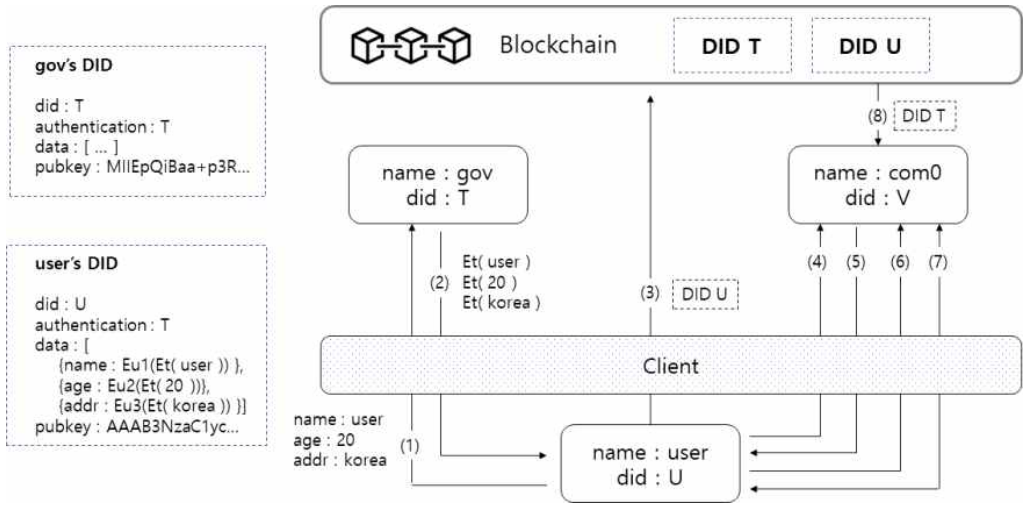

Fig. 3. DID Identity authentication scenario.

함하여 DID U를 만들어 블록체인에 저장한다.

step 4 : user는 com0에게 자신의 DID U를 알려준다.

step 5 : com0은 임의의 값을 DID U의 pubkey로 암호화하여 user에게 DID U의 소유자가 맞는지 확인한다.

step 6 : user는 com0의 질문에 응답하여 DID U의 소유자임을 증명한다.

step 7 : com0이 user에게 자신의 public key를 보내준다. user는 Eu2로 암호화된 자신의 나이 정보를 개인키로 풀어 Et(20)을 얻은 후 다시 com0이 보낸 public key로 암호화하여 com0에게 돌려준다.

step 8 : com0은 DID U에서 인증자가 T인 것을 확인하고, 블록체인에서 DID T를 가져온다. 그리고 DID T에 있는 공개키와 자신의 개인키를 사용해 user가 보내온 나이 정보를 얻는다.

step 1~3까지는 user가 gov의 인증을 받아 DID U를 블록체인에 저장하는 과정이다. 추가로 필요한 개인 정보가 있다면 기존의 DID에 추가하여 새로 받은 인증으로 추가하여 이어 나가면 된다. step 4~8까지는 user가 com0에게 자신의 DID로 신원인증을 하는 과정이다. 여기서 gov의 개입은 필요없으며 user와 com0이 기존에 발급된 DID 정보와 몇 번의 핸드세이크를 거쳐 user의 개인정보를 com0이 취득한다.

4. 실험 결과

본 실험에서는 3장에서 제안한 신원증명 DID 시나리오를 구현하여 실행하였다. 각 스텝별로 기능은 정상적으로 동작하며 암호키를 미리 생성해놓은 전제하에 전체 시나리오 실행에는 약 2초 정도이다. 공개키 암호 알고리즘은 golang의 crypto 라이브러리에서 제공하는 RSA를 사용하였다. 제안 방법의 com0은 user의 나이 이외의 정보는 얻을 수 없었다. 그러나 나이의 경우에는 20세 이상의 성인인지 여부만 확인할 필요도 있다. 이때에는 나이를 제공하기 보다 질문에 대한 참/거짓만 반환하면 되는데 이를 위해서 DID에 맞는 검증용 Chaincode를 만드는 방법이 필요해 보인다. 이 Chaincode는 필요한 정보가 있을 때 검증만을 위한 것으로 정보에 대한 포맷이 정해져 있지 않으므로 어떻게 유연성을 가져갈 것인가가 관건으로 보인다. 예를 들면 누군가는 DID를 생성하며 나이 필드를 age로 만들었지만 또 다른 누군가는 years로 만들 수도 있다.

4.1 DID 신원 증명

DID 기반의 신원 증명은 신원을 공증해주는 Gov가 네트워크에 함께 참여하고 있으며 Gov는 그 신원을 보장한다고 가정하였다. User는 자신이 직접 만든 DID를 Gov에게 공증 받은 후 Comp에 제출하여 신원을 인증받는다.

코드 2는 사용자가 자신이 정의한 필드로 DID를 만들어 제대로 생성되었는지 확인하는 테스트이다. 생성시 DID와 사용자 PrivateKey, PublicKey는 자

```
1  func TestCreateUser(t *testing.T) {
2      u := did.NewUser("Alice", 15, "kor")
3      // Test u's field
4      assert.Equal(t, u.Name, "Alice")
5      assert.Equal(t, u.Age, 15)
6      assert.Equal(t, u.Address, "kor")
7  }
```

Code 2. User DID Generation and Verification.

동으로 생성된다. DID Controller는 현재 자신이 DID를 생성한 Controller만 등록되어있다. 생성한 DID는 하이퍼레저 패브릭 블록체인에 저장된다.

코드 3은 사용자가 자신이 만든 DID를 Gov에게 제출하는 과정이다. Gov는 사용자가 보낸 DID u를 받아서 각 필드를 자신의 PrivateKey로 암호화한 후 새로운 DID u2를 리턴한다. 이 필드들은 Gov의 공증을 받았다는 의미이며 Gov의 PublicKey로 각 필드를 복호화하면 정상값으로 나오게 된다. Gov의 PublicKey로 암호화하면 이 값을 얻을 수 없기 때문에 서명과 비슷한 의미로 볼 수 있다.

코드 4는 사용자가 Comp에게 Gov에게 공증받은 u2 DID를 제출하는 과정이다. 이 인증 시나리오에서 Comp는 사용자에게 이름과 나이만 요구한다. 6번째 줄에서 사용자는 Gov에게 공증받은 u2의 Id를 제출하고, 그 다음 자신이 가진 DID 값들 중 이름과 나이만 제출한다. Comp는 사용자가 제출한 u2.Id와 일치하는 DID를 블록체인에서 찾아서 가져온다. 찾아온 DID의 필드에서 Controller를 순차적으로 확인하고 Controller의 공개키로 필드를 복호화 하여 사용자가 제출한 필드와 비교 검사를 한다. Comp는 미리 자신이 인정하는 Controller의 정보(여기서는 Gov)를 등록해둔다. Comp가 사용자에게 받은 DID값과 Gov의 공개키를 통해 복호화한 DID 값이 일치함을 확인하여 Comp는 사용자가 Gov의 인증을 받은 것으로 인정한다.

```
1  func TestAuthByGov(t *testing.T) {
2      gov := org.NewGov()
3      u := did.NewUser("Alice", 15, "kor")
4      u2 := gov.Auth(u)
5      // encrypts u's filed by Gov
6      dec_name = rsa.DecryptPKCS1v15SessionKey(rand.Reader, gov.PubKey, []byte(u2.Name))
7      dec_age = rsa.DecryptPKCS1v15SessionKey(rand.Reader, gov.PubKey, []byte(u2.Age))
8      dec_address = rsa.DecryptPKCS1v15SessionKey(rand.Reader, gov.PubKey, []byte(u2.Address))
9      assert.Equal(t, dec_name, "Alice")
10     assert.Equal(t, dec_age, 15)
11     assert.Equal(t, dec_address, "kor")
12 }
```

Code 3. Gov authentication and User DID encryption.

```
1          func TestAuthByComp(t *testing.T) {
2              gov := org.NewGov()
3              comp := org.NewComp()
4              u := did.NewUser("Alice", 15, "kor")
5              u2 := gov.Auth(u)
6              r := comp.Auth(u2.Id, u2.name, u2.age)
7              r2 := comp.GetDID(u2.Id)
8              f := comp.Compare(r, r2)
9            // Compare decrypted user's DID and Gov Authenticated DID
10             assert.Equal(t, f, true)
11         }
```

Code 4. Process of submitting an encrypted user DID.

```
1  func TestMakeBallots(t *testing.T) {
2      // init
3    comm := org.NewComm()
4    cand1 := did.NewCandidate()
5    cand2 := did.NewCandidate()
6    voter1 := did.NewVoter()
7    voter2 := did.NewVoter()
8    voter3 := did.NewVoter()
9    ballot1 := comm.MakeBallot(voter1)
10   ballot2 := comm.MakeBallot(voter2)
11   ballot3 := comm.MakeBallot(voter3)
12   assert.Equal(t, ballot1.CheckSign(comm), true)
13   assert.Equal(t, ballot1.CheckVoter(voter1), false)
14   assert.Equal(t, voter1.CheckVoter(ballot1), true)
15 }
```

Code 5. Issuing, signing, and ownership of ballots.

4.2 전자투표

전자투표는 선거관리위원회는 하나, 후보자는 두 명, 유권자는 세명으로 하며 각 후보자와 유권자는 전부 인증 받았다고 가정한다. 명칭은 각각 Comm, Cand1, Cand2, Voter1, Voter2, Voter3으로 한다. 코드 5에서 9~11번째 줄은 각 유권자에게 투표용지를 발급하는 과정이다. 투표용지에는 선거관리위원회의 서명이 들어가며 유권자의 공개키를 사용해 해당 유권자만 사용할 수 있도록 만든다. 12번째 줄은 발급된 투표용지 ballot1의 서명이 선거관리위원회의 서명이 맞는지 확인한다. 13번째 줄에서 ballot1이 voter1의 투표용지가 맞는지 검사하지만, ballot은 voter1의 PrivateKey를 알 수 없으므로 여기서는 검사가 실패한다. 14번째 줄에서 voter1이 투표용지 소유권 검사를 하면 자신의 개인키를 참조할 수 있으므로 참으로 나오게 된다.

선거위원회, 후보, 유권자 선언 및 투표용지 생성은 init으로 생략하였다. 유권자는 자신의 투표용지에 각각 후보를 투표한다. 여기서는 voter1과 voter2는 cand1에게 투표하였고, voter3은 cand2에게 투표하였다. Vote 함수 내부적으로는 각 유권자들은 자신의 개인키를 사용해 투표용지의 암호를 풀어 투표할 유권자의 ID로 업데이트한다.

전자투표에서 개인의 투표 이력을 남기지 않으면서 비밀투표가 되도록 유지하였다. 기존의 온라인 투표는 사용자가 후보에게 투표하며 직접 득표수 업데이트 함수를 호출하는 형태지만 여기서는 투표용지를 DID로 구현하여 실제 투표처럼 투표용지에 기표를 하고 이후 투표용지를 수거하여 개표하는 형식을 취했다. 투표용지는 사용자 개인키로만 사용할 수 있도록 전용으로 발급되어 중복 투표를 막는다.

5. 결 론

본 논문에서는 프라이빗 블록체인을 사용하여 DID 시스템을 일부 구현하였다. 본 논문에서의 DID 신원인증 시나리오는 DID로 할 수 있는 활용의 시작에 불과하며 신원인증 이후에 응용할 수 있는 시나리오들이 많이 있다. 특히 서비스를 통해 발생하는 모든 정보에 DID 식별자를 발급하여 검증할 수 있는 것이 장점이므로 본 시스템을 활용하여 다양한 시나리오를 개발하고 검증하고자 한다. 또한 각 시나리오에 맞는 일반화된 api 호출과 데이터 플로우를 정리하여 DID 아키텍처와 모델을 개선할 수 있다.

REFERENCE

[1] V. Torres, C. Serrao, M.S. Dias, and J. Delgado, “Open DRM and the Future of Media,” *IEEE Multimedia,* Vol. 15, Issue 2, pp. 28-36, 2008.

[2] Use Cases and Requirements for Decentralized Identifiers, https://www.w3.org/TR/did-use-cases/ (accessed May 21, 2021).

[3] Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/ (accessed May 21, 2021).

[4] B. Alzahrani, “An Information-Centric Networking based Registry for Decentralized Identifiers and Verifiable Credentials,” *IEEE Access,* Vol. 8, pp. 137198-137208, 2020.

[5] 박종규, *행위 인증을 위한 블록체인 DID 연구와 보안성 검사*, 동아대학교 석사학위논문, 2021년 6월.

[6] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Manubot*, 2019.

[7] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 49, Issue 11,

pp. 2266-2277, 2019.
[8] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, “A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future,” *IEEE Access*, Vol. 7, pp. 75845-75872, 2019.
[9] K.H. Kwak, J.T. Kong, S.I. Cho, H.T. Phuong, and G.Y Gim, “A Study on the Design of Efficient Private Blockchain,” *Computational Science/Intelligence & Applied Informatics*, pp. 93-121, 2019.

박 종 규

2014년 부산대학교 정보컴퓨터공학과 학사 졸업(공학사)
2018년 부산대학교 컴퓨터공학과 박사 수료
2020년~현재 동아대학교 컴퓨터공학과 석사 과정

관심분야 : 블록체인, 정보보안, 인공지능, 사물인터넷

권 기 룡

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)

2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2011년~2012년 Colorado State Univ., Visiting Scholar
2015년~2016년 한국멀티미디어학회 회장
2006년~현재 부경대학교 IT융합응용공학과 교수
2018년~현재 글로벌핀테크산업진흥센터 이사장
관심분야 : 멀티미디어 정보보호, 영상처리, 멀티미디어 통신 및 신호처리

권 성 근

1996년 경북대학교 전자공학과 학사
1998년 경북대학교 전자공학과 석사
2002년 경북대학교 전자공학과 박사

2002년~2011년 삼성전자 무선사업부 책임연구원
2011년~현재 경일대학교 전자공학과 교수
관심분야 : 멀티미디어 암호, 모바일 방송, 워터마킹

이 석 환

1999년 경북대학교 전자공학과 학사 졸업(공학사)
2001년 경북대학교 전자공학과 석사 졸업(공학석사)
2004년 경북대학교 전자공학과 박사 졸업(공학박사)

2005년~2020년 동명대학교 정보보호학과 교수
2021년~현재 동아대학교 컴퓨터공학과 교수
관심분야 : AI영상보안, 컴퓨터비전, 보안응용, 디지털트윈