정 보 보 호 학 회 지
제 34 권 제1호, 2024. 2

퍼블릭 블록체인을 활용한 DID 어플리케이션 개발

구 재 욱*, 김 도 훈**

요 약

본 연구에서는 퍼블릭 블록체인 기술을 적용하여 탈중앙화된 식별 정보(DID) 어플리케이션을 개발하였다. 기존의 컨소시엄 블록체인을 사용한 DID는 일부 참가자들 간의 신뢰를 기반으로 동작하여 특정 그룹의 중앙화된 통제 가능성으로 인해 보안 문제가 발생하는데, 이를 극복하기 위해 퍼블릭 블록체인을 도입하여 안전하고 투명한 디지털 식별 체계를 제시한다. 또한, 본 연구에서는 웹앱 형태의 DID 어플리케이션을 사용자 친화적이고 직관적인 디자인으로 구현하여 사용자들이 쉽게 식별 정보를 관리하고 교환할 수 있도록 하였다. 더불어 안전한 키 관리 및 전자 서명 기술을 적용하여 사용자들은 자신의 식별 정보를 완전히 통제할 수 있으며, 이를 통해 탈중앙화된 신뢰 모델을 체험할 수 있다.

Ⅰ. 서 론

현대 디지털 환경에서 신원 확인은 점점 더 중요한 과제로 부상하고 있으며, 이에 따른 탈중앙화된 식별 체계의 필요성이 대두되고 있다. 그러나 기존의 컨소시엄 블록체인을 활용한 DID는 일부 참가자들 간의 신뢰를 기반으로 동작하며, 특정 그룹의 중앙화된 통제 가능성으로 인해 보안 문제가 제기되고 있다. 이러한 문제점을 개선하고자, 본 연구에서는 퍼블릭 블록체인[1] 기술을 적용하여 안전하고 투명한 디지털 신원 관리 시스템을 구현하고자 한다. 퍼블릭 블록체인은 분산된 데이터 저장 및 불변성의 특성으로 알려져, 사용자의 개인정보를 안전하게 보호하면서도 탈중앙화된 환경을 제공할 수 있는 이상적인 기술적 기반으로 간주된다.

이러한 배경 아래, 본 연구에서는 웹앱 형태의 디지털 신원 확인 어플리케이션을 개발하였다. 이 어플리케이션은 분산 네트워크에서 동작하며, 사용자가 자체적으로 신원 정보를 안전하게 관리하고 교환할 수 있는 기능을 제공한다. 블록체인의 특성을 통해 개인정보의 불변성과 안전성을 보장하며, 사용자 친화적인 웹앱 디자인을 통해 식별 체계에 대한 사용자 경험을 향상하고자 한다.

또한 퍼블릭 블록체인을 활용한 DID[2]의 설계 및 구현 과정, 그리고 결과에 대해 다루고 있다. 이를 통해 컨소시엄 블록체인의 취약점을 극복하며 분산화와 안전성을 강화하는 방향으로 연구를 진행하였다. 따라서 퍼블릭 블록체인이 어떻게 탈중앙화된 디지털 신원 관리 시스템의 핵심 요소로 작용할 수 있는지에 대한 통찰을 제공하고자 한다.

Ⅱ. 관련연구

본 장에서는 컨소시엄 블록체인 형태의 DID에 대해서 분석한다.

2.1. Proof-of-Transaction

"트랜잭션의 증명 (PoT)[2]"은 Infra Blockchain에서 블록체인 기반 서비스 제공자들에 대한 인센티브 시스템으로 작용한다. 각 블록체인 계정이 블록체인 코어 노드를 실행할 때마다 트랜잭션 투표가 계속해서 누적되며, 이는 해당 계정이 의미 있는 블록체인 트랜잭션을 생성하고 블록체인 생태계에 경제적 활동을 기여한 증거로 작용한다. 이러한 누적 투표 양은 Infra Blockchain에서 블록 생산자 선출의 주요 기준으로 활용된다.

Proof-of-Work (PoW) 및 Proof-of-Stake (PoS)[3]와 달리 PoT는 계산 능력이나 블록체인의 고유 암호화폐 소유를 보상하는 대신, 실제 경제 활동을 블록체

* 경기대학교 컴퓨터공학과 (학부생, paeter3@kyonggi.ac.kr)
** 경기대학교 AI컴퓨터공학부 (조교수, karmy01@kyonggi.ac.kr)

인으로 가져오는 서비스 제공자를 장려한다. PoW 및 PoS와는 달리 PoT는 실제 트랜잭션을 생성하고 기존의 계산 능력이나 재무 자산만을 활용하는 것이 아니라, 블록체인 경제에 직접 기여하는 이들에게 보상한다.

2.2. Transaction-as-a-Vote

"Transaction-as-a-Vote"(TaaV)는 Proof-of-Transaction (PoT) 블록체인 합의 알고리즘의 핵심 개념으로, 이 접근 방식에서는 블록체인 트랜잭션에 블록 생산 후보에 대한 선택적 투표가 포함될 수 있다. 사용자가 트랜잭션을 시작할 때 트랜잭션 수수료가 발생하면 "트랜잭션 투표" 필드에서 블록 생산자로 지정할 수 있는 블록체인 계정을 지정할 수 있다. 트랜잭션 메시지는 해당 블록체인 계정의 개인 키로 암호화되어 체인 상에 암호화 증명이 제공된다.

가장 많은 투표를 받은 블록 생산자는 새로운 블록을 생성하고 트랜잭션 수수료를 수집하는 그룹으로 선출된다. 투표는 트랜잭션 수수료 금액을 기준으로 가중치가 부여되어, 높은 트랜잭션 수수료는 더 큰 투표 영향을 준다. 이 시스템은 블록 생산자에게 이익을 가져오는 경제 활동에 기여하는 트랜잭션에만 수수료가 부과되도록 보장한다.

다른 블록체인에서는 거버넌스 및 이익 공유를 위한 투표가 별도의 과정으로 이루어지지만, TaaV를 사용하는 Infra Blockchain에서는 블록체인 거래 처리에 투표 프로세스가 효과적으로 통합되어 사용자가 명시적인 투표 프로세스에 신경 쓸 필요가 없다.

2.3. Infra Digital Certificates

Infra Blockchain은 Transaction-as-a-Vote (TaaV) 및 Proof-of-Transaction (PoT)을 활용하여 디지털 인증서를 효과적으로 관리하고 안전하게 활용하는 서비스를 제공한다. 사용자는 블록체인 ID와 함께 TaaV를 이용하여 디지털 증명서를 발급받을 수 있다. 이러한 디지털 인증서는 PoT 메커니즘을 통해 블록체인에서 안전하게 검증되며, 영지식증명 기술을 활용하여 사용자가 개인정보를 최소한으로 노출하면서 안전한 방식으로 증명서를 제출할 수 있다.

각 발급 기관은 PoT를 통해 블록체인에서 투표를 받아 신뢰성 있는 디지털 인증서를 발급할 수 있으며 이를 통해 블록체인의 분산화와 PoT의 신뢰성을 결합하여 안전하고 효율적인 디지털 인증 서비스를 제공한다.

2.4. 컨소시엄 블록체인의 문제

컨소시엄 블록체인에서 도입된 "Transaction-as-a-Vote" (TaaV) 시스템은 블록 생성자 선출을 위해 트랜잭션 수수료에 대한 투표를 진행한다. 그러나 이러한 중앙화된 투표 프로세스는 블록체인의 거버넌스와 분산성에 취약성을 낳는다. 사용자들이 중앙화된 투표 시스템에 의존하면 블록체인의 합의 메커니즘이 중앙 집중화될 우려가 있다. 이에 더해, 컨소시엄 블록체인은 주로 특정 업체나 기관에 의존하므로 제한된 생태계를 형성하며, 이로 인해 해당 업체나 기관의 문제가 전체 블록체인 네트워크에 영향을 미칠 수 있어 단일 지점 고장으로부터 오는 위험을 키울 수 있다. 더불어, 특정 기관이나 업체에 의한 운영으로 인해 컨소시엄 블록체인은 퍼블릭 블록체인에 비해 분산성이 제한되어 특정 집단에 대한 신뢰 문제와 중앙화된 통제로 인한 보안 취약성을 야기할 수 있다.

Ⅲ. 퍼블릭 블록체인 기반의 DID

3.1. 퍼블릭 블록체인의 Verifiable Credential

Verifiable Credential은 개인이나 기관의 신원 정보를 디지털 형태로 표현하는 데이터 모델이다. 이 Credential은 소유자의 신원 정보, 발급자 정보, 그리고 Credential 자체에 대한 전자 서명 등을 포함한다. 이는 분산 식별자(DID)를 기반으로 하여 중앙 집중화된 신원 관리 체계를 극복하고, 사용자가 자신의 신원을 효과적으로 소유하고 제어할 수 있도록 한다.

Verifiable Credential 모델은 다음과 같은 필드로 구성되어 있다: ownerId(소유자의 ID), credentialTitle (Credential의 제목), 그리고 IssuedBy (Credential을 발급한 기관). 이 모델을 사용하여 Verifiable Credential을 생성하면, 각 Credential은 소유자의 ID, Credential 제목, 발급자 정보 등을 저장하게 된다.

이러한 Verifiable Credential은 퍼블릭 블록체인에 EVM의 스마트 컨트랙트를 통해 기록되어 정보를 저장한다. 컨소시엄 블록체인과 비교할 때, 퍼블릭 블록

체인은 전 세계적으로 분산된 네트워크로 구성되어 있어 중앙 집중화된 시스템과는 다른 차원의 신뢰성과 안전성을 제공한다. 이러한 특성들은 Verifiable Credential이 퍼블릭 블록체인에서의 사용을 더욱 강력하게 만들 수 있다.

3.2. Verifiable Credentail 생성 프로세스

Issuer는 Verifiable Credential을 생성하는데, 먼저 사용자의 유형이 "issuer"인지 확인한다. 인증된 issuer인 경우, 해당 issuer의 정보를 가져와서 Verifiable Credential 모델을 활용하여 새로운 Credential을 생성한다. 새로운 Credential은 소유자의 ID는 현재 issuer의 ID로, Credential 제목 및 발급자 정보는 사용자가 입력한 정보로 설정된다. 이후, 생성된 Verifiable Credential은 DB에 저장되며, 저장이 성공적으로 이루어지면 저장된 Credential과 성공 메시지를 응답으로 반환한다.

사용자가 "holder"로 로그인한 경우, 시스템은 현재 사용자인 Holder의 정보를 조회하고, 이에 따라 Issuer UserList와 Verifiable Credential 모델에서 관련 정보를 수집한다. 관련 정보는 다음과 같다. 사용자의 이름 또는 실명 정보, 사용자의 이메일 주소, 생년월일 정보, 발급받은 인증서의 유형, 발급받은 인증서의 이름, 인증서 발급일, 사용자의 국적, 사용자의 주소, 사용자가 성인인지 아닌지를 나타내는 값들이다.

이후, 시스템은 수집된 정보를 활용하여 Verifiable Credential을 생성한다. 이 Credential은 전자 서명 프로세스를 거친 후 Issuer의 비밀키로 암호화되어 퍼블릭 블록체인에 안전하게 저장된다. 또한, Holder의 DID Document가 업데이트되고, Verifiable Credential은 Holder VC List에 추가된다. 마지막으로, 이 모든 과정이 성공적으로 완료되면 최종 결과로 Holder VC List가 응답으로 반환된다.

3.3. Verifiable Credential 인증 요청

시스템은 먼저 요청된 사용자의 유형이 "Holder"인지 확인한다. 유형이 "Holder"가 아니라면, 403 Forbidden 오류를 반환하여 접근을 거부한다. 그 후, Verifier는 요청 본문에서 제공된 VC 목록 ID를 사용하여 Holder의 Verifiable Credential (VC) 목록을 데이터베이스에서 검색한다. 이어서, Verifier는 Holder와 자신 간의 키 페어를 확보하기 위해 Holder 및 Verifier KeyPair를 검색한다. 이 단계에서는 Holder의 개인키와 Verifier의 공개키가 획득된다.

다음으로, Verifier는 Verifiable Presentation (VP)의 페이로드를 생성한다. 이 페이로드는 VC를 포함하며 발급자 및 Holder의 공개키 정보를 담고 있다. 이후, 전자 서명 작업이 진행된다. VP의 원본을 해싱한 후, 해당 해시값을 Holder의 개인 키로 암호화하여 전자 서명을 생성한다. 이 서명은 Verify List에 저장되어 Verifier가 나중에 확인할 수 있도록 한다.

그다음, Verifier는 새로운 Verify List 인스턴스를 생성하고 이를 데이터베이스에 저장한다. 이 인스턴스에는 원본 VP, 암호화된 VP, 요청한 사용자 및 Verifier의 정보 등이 포함되어 있다. 최종적으로, 처리가 성공하면 HTTP 상태 코드 200과 함께 새로운 Verify List의 정보를 JSON 형식으로 반환한다. 이렇게 함으로써 Verifier는 Holder로부터 제시된 자격증에 대한 전자 서명을 검증하고, 관련 정보를 안전하게 저장한다.

3.4. Verifiable Credentail 검증 요청

다음으로 Verifier가 Holder의 인증 요청을 검증하는 일련의 단계를 수행한다. 먼저, Verify List 모델을 통해 검증할 대상인 Verify List를 불러온다. 그 후, 해당 Verify List에 연결된 Holder와 Verifier를 특정하고, 현재 사용자가 해당 Verify List의 소유자(verify Owner)와 같은지를 확인하여 본인에게 요청된 Verify List만을 검증 대상으로 허용한다. 만약 다를 경우 403 Forbidden 오류를 반환한다. 이어서, Holder의 Wallet Address를 사용하여 Holder의 DID Document에 접근하고, 그 Document에서 public Key를 획득한다. 이 정보를 통해 Holder의 전자 서명을 복호화하고 검증한다.

다음으로, Verify List에서 필요한 정보들을 추출하고, Holder의 DID Document에서 가져온 public Key를 디코딩한다. 그 후, Verify List에 담겨 있는 다양한 정보를 이용하여 VP(Verifiable Presentation)의 복호화와 전자 서명의 검증, Issuer의 서명 복호화와 검증, Issuer의 DID Document에서 Holder의 ID 확인, 그리고 Verifier가 검증할 인증서의 종류 일치 여부를 각각

확인한다.

모든 인증 요소를 종합하여, 검증이 성공하면 "success"를 반환하고, 실패할 경우 "failed"를 반환한다. 최종적으로, Verify List의 상태를 업데이트하며 Verifier가 아닌 사용자가 접근하려고 하는 경우 403 Forbidden 오류를 반환한다. 이로써 Verifier는 복잡한 암호화 및 전자 서명 검증 과정을 통해 Holder의 인증 요청을 안전하게 검증하게 된다.

Ⅳ. 결 론

본 연구는 퍼블릭 블록체인 기술을 활용하여 탈중앙화된 디지털 신원 관리 시스템을 구현하고자 했다. 퍼블릭 블록체인의 특성을 활용하여 안전하고 투명한 디지털 인증서 발급 및 검증 프로세스를 설계하고 구현함으로써 사용자들에게 안전하고 신뢰성 있는 식별 정보를 제공하는 데 성공하였다. 또한 컨소시엄 블록체인 형태의 DID에 대한 분석을 통해, Proof-of-Transaction (PoT) 알고리즘과 Transaction-as-a-Vote (TaaV)를 활용하여 블록체인 기여하는 방식을 참조하였고 이를 활용한 Infra Digital Certificates는 안전하고 효율적인 디지털 인증 서비스를 제공하는 방법을 제시했다.

또한 퍼블릭 블록체인 기반의 Verifiable Credential을 통해 사용자가 자신의 신원 정보를 소유하고 제어하는 방안을 제시하였다. Verifiable Credential 생성 및 검증 과정에서 사용자 친화적인 웹앱 디자인을 통해 사용자 경험을 향상하고, 블록체인의 분산화와 퍼블릭 블록체인의 신뢰성을 결합하여 안전하고 효과적인 디지털 인증 서비스를 제공함으로써 디지털 환경에서의 안전한 신원 확인 문제에 기여하고자 했다.

결과적으로, 퍼블릭 블록체인 기반의 디지털 신원 관리 시스템은 컨소시엄 블록체인의 문제를 극복하고 분산화와 안전성을 강화하는 방향으로 발전할 수 있다. 사용자들은 안전하고 효과적으로 자신의 신원을 관리할 수 있으며, 전 세계적으로 분산된 네트워크로 구성된 퍼블릭 블록체인은 중앙 집중화 및 보안 취약성과 같은 문제에 대한 신뢰성 있는 해결책을 제공하여 사용자들에게 안전하고 효율적인 디지털 신원 관리를 제공할 수 있는 기술적 기반을 마련하였다.

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008): 21260.

[2] InfraBlockchain_Technical_White_Paper_Version_2_4_ENG_202008

[3] Casper the Friendly Finality Gadget (2017)

[4] Decentralized identifiers (DiDs) v1.0 (2020)

〈저자소개〉

구 재 욱 (Jae Wook Koo)

2024년 2월 : 경기대학교 컴퓨터 공학부 졸업

<관심분야> 블록체인, 정보보호

김 도 훈 (Dohoon Kim)

2011년 2월 : Bell-Lab Internship(Alcatel-Lucent), New Jersey, USA

2012년 4월 : Agency for Defense and Development, Senior Researcher (前 국방과학연구소 선임연구원, 사이버방호 & 정보보호 팀장)

2018년 3월 : Kyonggi University, Assistant Professor (現 경기대학교 조교수)

<관심분야> 블록체인, 정보보호