Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.341

블록체인 기반의 개인정보 관리를 위한 사용자 중심의 접근제어 서비스*

김 승 현,[1†‡] 김 수 형[2]
[1]한국교원대학교 컴퓨터교육과 (조교수), [2]한국전자통신연구원 정보보호연구본부 (책임연구원)

User-Centric Access Control Service for Blockchain-Based Private Information Management*

Seung-Hyun Kim,[1†‡] Soohyung Kim[2]
[1]Korea National University of Education (Assistant professor),
[2]Electronics and Telecommunication Research Institute (Senior researcher)

요 약

최근에 분산ID관리처럼 개인정보를 주체적으로 관리하는 기술이 주목받고 있지만, 기존에 제시된 블록체인 기반의 접근제어 연구들은 사용자에게 충분한 수준의 개인정보 접근제어 방안을 제공하지 못하고 있다. 본 논문은 퍼미션 블록체인 기술과 표준화된 프라이버시 보호 기술을 결합한 방안을 제안한다. 사용자의 접근제어 개입을 위해 프라이버시 제어 표준인 UMA2를 준용하는 토큰 기반의 사용자 접근제어 서비스를 블록체인 분산어플리케이션에 적용하였다. 블록체인과 UMA2를 연동함으로써 기존 블록체인이 제공하지 못했던 사용자 중심의 접근제어 기능을 제공한다. 또한 UMA2의 단점인 엔터티의 프라이버시 문제와 보안성, 가용성 이슈를 해결하였다.

ABSTRACT

Recently, user-driven privacy control technology, such as distributed ID management, has been gaining attention. However, the existing blockchain-based access control studies have not provided a sufficient level of privacy control method to users. This paper proposes a method that combines permissioned blockchain technology and a recent privacy control standard. To allow users to participate in privacy control, a token-based user access control service that conforms to the UMA2 standard was applied to the blockchain dApp. By combining the blockchain and UMA2, the proposed method provides a user-centered privacy control function that the existing blockchain could not provide. In addition, we solved the problem of privacy, security, and availability of entities, which are the disadvantages of UMA2.

Keywords: Blockchain, Access Control, UMA, Hyperledger Fabric, privacy

I. 서 론

최근에 분산ID관리(DID: Distributed IDentity)라는 개념이 등장하면서 개인정보를 주체적으로 관리하는 기술이 주목받고 있다. 이러한 개인정보 기반 기술의 성공은 서비스의 편의성과 프라이버시 보호라는 두 가지 주요 과제를 균형 있게 제공하는가에 따라 결정된다. 특히 2016년도 유럽의

Received(12. 17. 2020), Modified(03. 31. 2021), Accepted(03. 31. 2021)
* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00321, 5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및 보안 기술 개발)
† 주저자, kimsh@knue.ac.kr
‡ 교신저자, kimsh@knue.ac.kr(Corresponding author)

GDPR 채택으로 인해, 개인정보 보호를 위한 접근제어 체계의 필요성이 강조된다[1]. GDPR (General Data Protection Regulation)의 핵심 개념에 따르면, 개인정보를 처리하기 전에 서비스 제공 업체는 사용자 동의를 받아야 하고, 필요한 개인정보의 범위를 정확히 고지해야 한다. 모든 서비스 제공 업체는 데이터 처리가 사용자의 동의에 부합함을 입증해야 한다.

Pew 리서치센터가 수행한 개인정보 보호 연구에서 응답자의 74%는 개인정보 수집 주체를 제어하는 것이 매우 중요하다고 말했으며, 65%는 개인정보의 수집을 제어하는 것이 매우 중요하다고 응답했다[2]. 이처럼 사용자는 프라이버시 보호를 매우 중요하게 고려하고 있지만, 서비스 제공업체는 서비스의 편의성만을 강조하며 개인정보 보호에는 소극적이다. 초연결시대의 잠재력을 달성하기 위해서는 공공의 이익을 위해 필요한 자료가 즉시 이용 가능하고 동시에 시민을 보호할 수 있는 새로운 방식의 개인정보 거래 방식이 요구된다.

기존에 제시된 블록체인 기반의 접근제어 연구들은 블록체인의 안정성을 통해 신뢰있고 확장성있는 접근제어 기술을 제시한다. 하지만 사용자에게 충분한 수준의 개인정보 접근제어 방안을 제공하지 못하고 있다. 사용자가 요구할 수 있는 접근제어의 자동화, 동기식/비동기식 접근제어, 사용자가 정의한 다양한 수준의 프라이버시 정책을 기반으로 한 접근제어를 모두 지원하는 연구가 없다. 심지어 기존 연구의 대다수는 블록체인 환경에서 구현되지 않아서 실제로 동작 가능 여부가 검증되지 못했다.

본 논문에서 제안하는 블록체인 UMA 기술은 퍼미션 블록체인 기술과 표준화된 프라이버시 보호 기술을 결합한 것으로, 각 기술의 장점을 유지하면서 동시에 각 기술에 존재하는 단점을 극복한다. 사용자의 접근제어 개입을 위해 프라이버시 제어 표준인 UMA2[3]를 준용하는 토큰 기반의 사용자 접근제어 서비스를 블록체인 분산어플리케이션 형태로 설계하였다. 이를 통해 기존의 규칙 기반의 자동화된 접근제어 뿐만 아니라, 동기식/비동기식 접근제어와 같은 다양한 접근제어 유즈케이스를 제공한다. 블록체인 UMA 기술은 대표적인 퍼미션 블록체인인 Hyperledger Fabric에 구현했고, 처리 속도와 가용성 측면에서 정상적으로 동작함을 보였다.

본 연구의 기여는 다음과 같다. 첫째, 블록체인과 UMA2를 연동하는 방안을 제시함으로써 기존 블록체인이 제공하지 못했던 사용자 중심의 접근제어 기능을 제공했다. 둘째, UMA2의 단점인 엔터티의 프라이버시 문제와 보안성, 가용성 문제를 블록체인 기술을 적용하여 해결하였다. 셋째, 상용 오픈소스인 Hyperledger Fabric에 제안 기법이 실제로 동작함을 보였다. 우리가 알기로는 본 연구가 블록체인과 UMA2를 연동하여 각 방식의 단점을 극복한 최초의 연구이다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 배경이 되는 기술을 간략히 소개하고 해결할 문제를 제시한다. 3장에서 제안 방안인 블록체인 UMA 기술의 개념을 설명하고, 아키텍처의 구성 및 동작을 상세하게 제시한다. 4장은 제안 방안의 구현 내역을 설명한다. 5장은 성능 및 기능 측면에서 제안 방안을 고찰하고, 관련 연구와의 차별성을 보인다. 마지막으로 6장에서 결론 및 향후 연구를 제시한다.

II. 배경 기술

2.1 블록체인 접근제어 기술

블록체인을 활용한 접근제어 기술은 IoT와 같은 특정 환경에서 많은 주목을 받고 있으며, 대표적으로는 FairAccess와 PrivacyGuard가 있다. FairAccess[4]는 암호화폐와 유사하게 사용자가 지갑 어플리케이션을 통해 개인정보를 관리한다. 또한 OrBAC이라는 접근제어 기법을 적용하여, 사용자가 중앙에서 직접 정의한 정책과 각 조직이 P2P 방식으로 정의한 정책을 결합하여 접근제어를 수행한다. FairAccess는 개념증명(PoC) 수준의 구현이 이루어졌지만, 트랜잭션이 성립되기 위한 대기시간이 길고 사용자가 직접 정의한 다양한 수준의 접근제어는 어렵다는 단점이 존재한다.

PrivacyGuard[5]는 클라우드 저장소에 암호화된 개인정보를 관리하고 TEE(Trusted Execution Environment)라는 보안 영역에서 개인정보의 암복호화 작업을 처리한다. 블록체인은 사용자가 직접 정의한 다양한 수준의 접근제어 정책을 스마트 컨트랙트로 표현하거나 개인정보의 접근 이력을 저장하는 용도로 활용된다.

Zyskind와 Kaaniche는 블록체인 접근제어 기술에 높은 수준의 보안을 제공하기 위한 방식을 제안하였다. Zyskind[6]는 블록체인에서 접근제어용 트랜잭션과 개인정보 관리용 트랜잭션을 분리하여 수행하는 기법을 제

안하였다. 개인정보는 오프체인에 별도로 암호화되어 관리되며, 접근제어 정책에서 승인된 노드는 암호화된 개인정보를 수신하고 자신의 보안키로 복호화할 수 있다. 블록체인에는 해시 포인터만 저장되고, 개인정보는 서명키와 암호키로 보호받는다.

Kaaniche[7]는 블록체인 접근제어를 위해 계층적 ID 기반의 암호화 메커니즘을 적용하였다. 사용자가 직접 정의한 다양한 수준의 접근제어 정책을 스마트 컨트랙트로 표현하고 개인정보를 함께 전달함으로써, 접근제어 정책에서 승인된 노드만 개인정보를 얻을 수 있도록 하였다.

2.2 UMA2

OAuth는 토큰 기반 인증을 제공하는 접근제어 프로토콜로, Google이나 Facebook 등 업계 전반에 걸쳐 많은 기업들이 OAuth를 기반으로 독자적인 인증 소프트웨어를 구현했다. 하지만 IoT 장치처럼 통신 및 처리 오버헤드가 제한된 환경에서는 모든 OAuth 프로토콜을 수행할 수 없다는 한계가 있었다. 또한 특정 타입의 개인정보 전체를 지속적으로 공유할지 여부만 제어할 수 있기 때문에, 상황에 따라 사용자가 세밀하게 접근제어를 결정할 수 없다.

UMA(User-Managed Access) 2 [3]는 미국의 Kantara Initiative가 개발한 접근제어 프로토콜이다. 리소스 소유자의 관점에서 리소스 사용 권한 제어의 제어 지점을 통합하는 OAuth 기반 프로토콜로, 위에 제시된 OAuth의 단점을 모두 해결했다.

그림 1과 같이, UMA2는 리소스 소유자 (Resource Owner), 리소스 서버 (Resource Server), 인가 서버 (Authorization Server) 및 클라이언트의 네 가지 유형의 엔터티로 구성된다. 리소스 소유자는 리소스 서버 내의 리소스(즉, 사용자의 개인정보)을 제공하고 인가 서버 내에서 이 리소스에 대한 접근여부를 제어한다. 클라이언트는 토큰을 인가 서버에 요청하고 이 토큰을 사용하여 리소스 서버의 리소스에 접근할 수 있다[3].

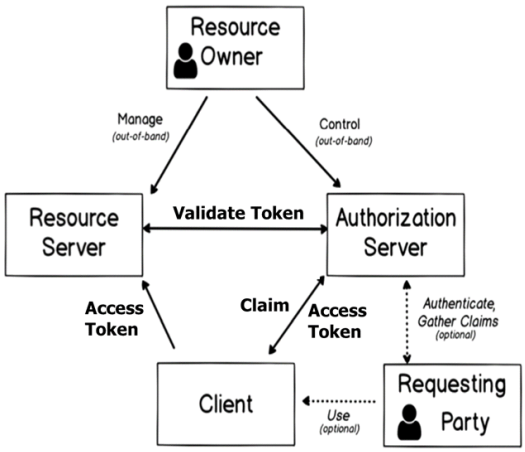

Fig. 1. UMA2 Architecture [3]

UMA2는 다음의 3가지 특징이 있다.

- 프라이버시 정책 기반: 동기식 승인을 위해 고안된 OAuth와 달리, UMA는 사용자가 미리 설정한 프라이버시 정책을 기반으로 접근제어를 처리할 수 있다.
- 오프라인 모드: UMA는 개인정보 접근 요청시 사용자가 오프라인일 때 해당 요청을 비동기식으로 처리한다.
- 사용자 중심 접근제어: UMA는 사용자를 모델의 핵심 부분으로 포함시켜, 접근제어 과정에서 사용자가 직접 개입할 수 있다.

2.3 해결할 문제

Hyperledger Fabric[8]은 가장 인기있는 오픈소스 블록체인 프로젝트 중 하나로, 합의 알고리즘, 체인코드, 멤버십 서비스 등의 각 핵심요소를 모듈형태로 탈부착 가능한 확장형 아키텍처를 가진다. 또한 적절한 최적화를 통해, 초당 수천 건의 트랜잭션 처리 성능을 보장한다[9]. Hyperledger Fabric에는 사용자가 블록체인 네트워크에 저장된 자신의 개인정보를 직접 제어할 수 있는 기능이 존재하지 않는다. 0.6 버전에서의 멤버십 서비스와 1.0 버전에서의 Fabric-CA는 블록체인 노드를 관리하는 목적을 가진다. 1.1 버전에서의 속성 기반의 체인코드 접근제어와 클라이언트 ID 확인 기능, 1.2 버전과 1.4 버전에서의 Private Data 기능은 체인코드를 구동 요청한 사용자 신원에 따라 개인정보의 접근제어를 수행할 수 있다. 하지만, 체인코드에 사용자ID 또는 속성 기반의 접근제어를 하드코딩으로 설정해야 하며, 사용자가 직접 정의한 다양한 수준의 접근제어가 어렵다. 2.0 버전 이상에서는 Private Data 기능에 대한 검증, 보증, 사용 기능이 개선되었지만 여전히 사용자가 직접 정의한 다양한 수준의 접근제어는 제공하지 않고 있다[10].

UAM2 아키텍처는 광범위한 작업에 사용할 수 있지만, 엔터티의 중앙 집중화로 인한 문제가 존재한다. 각 엔터티의 종속성으로 인해, 단일 지점 장애(Single Point of Failure) 문제에 취약해지고 참여 노드의 증가를 제한할 수 있다. 특히 인가서버가 중단되면 모든 엔터티의 동작이 중지될 수 있다.

또한, UMA 아키텍처는 각 엔터티의 해킹으로 인해 엔터티에서의 사용자 활동 내역과 같은 프라이버시가 공격자에게 노출될 수 있다. 인가 서버는 사용자의 프라이버시 정책을 관리하고 클라이언트의 접근제어를 처리하는 역할을 담당하는데, 인가 서버가 공격당하면 사용자의 실제 신원이 드러나고 모든 온라인 활동 이력이 감시될 수 있다. 또한 인가 서버에 저장된 사용자의 프라이버시 정책을 임의로 변경하거나, 리소스 서버에 저장된 개인정보를 접근할 수 있다.

따라서 제안하는 방법은 다음 문제를 해결할 수 있어야 한다. 첫째, 블록체인에서 적용할 수 있는 사용자 중심의 접근제어 기법을 제공해야 한다. 관리자의 개입 없이 사용자가 직접 정의한 다양한 수준의 프라이버시 정책을 기반으로 개인정보가 제어되어야 한다. 둘째, 단일 지점 장애 문제에 대비하여 참여 노드의 상황 변동이 성능에 미치는 영향이 제한적이어야 한다. 셋째, 참여 노드에 대한 공격으로 인해 사용자의 실제 신원이 드러나거나, 사용자의 프라이버시 정책의 변경, 사용자 동의 없이 이루어지는 개인정보의 불법적인 접근을 방지할 수 있어야 한다.

III. 블록체인 UMA 기술

본 논문에서 제안하는 방법은 UMA2 표준 구조를 블록체인에 모두 이식하고, 개인정보와 프라이버시 정책을 블록체인에서 관리하는 것이다. 구체적으로 인가 서버와 리소스 서버는 블록체인의 체인코드 형태로 포팅한다. 또한 개인정보와 프라이버시 정책은 블록체인의 Private Data 영역에 암호화하여 관리한다. 여기서 Private Data 영역은 Hyperledger Fabric 1.2 버전 이후에 적용된 기능으로, 블록체인 채널에 공개되지 않고 특정 당사자에게만 접근 가능한 특수한 블록체인 영역이다. 저장소의 내용은 암호화되어 있으며 블록체인과는 별도의 통신 방식으로 특정 당사자 간에 공유된다.

그림 2는 제안하는 블록체인 UMA 기술의 개념도를 보인다. 사용자는 개인정보의 소유주이고, 프라이버시 정책을 설정하여 개인정보에 대한 접근을 제

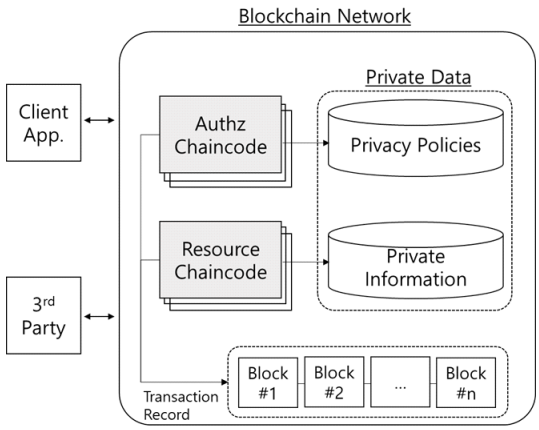

Fig. 2. Blockchain UMA Architecture

한한다. 그림의 좌상단에 위치한 클라이언트 앱은 사용자 단말에 설치되는 전용 어플리케이션으로, 사용자가 개인정보와 프라이버시 정책을 보관 중인 블록체인의 인가 체인코드 및 리소스 체인코드의 엔드포인트를 유지한다. 사용자는 클라이언트 앱을 통해 블록체인에 개인정보를 등록하고 프라이버시 정책을 설정한다.

그림 2의 좌하단에 위치한 서드파티는 사용자의 개인정보를 기반으로 특정 서비스를 제공하는 서비스 프로바이더이다. 사용자가 제시하는 블록체인의 인가 체인코드와 리소스 체인코드의 엔드포인트를 통해 사용자의 개인정보를 요청하고 제공받을 수 있다.

그림 2의 오른쪽에 위치한 블록체인 네트워크에는 인가 체인코드와 리소스 체인코드, 그리고 각 체인코드가 사용하는 Private Data 영역이 존재한다. 인가 체인코드는 사용자의 프라이버시 정책을 Private Data 영역에 등록한다. 그리고 서드파티의 개인정보 요청시, 사용자의 해당 프라이버시 정책에 따라 개인정보 요청을 승인/거부하고 토큰을 발급한다. 리소스 체인코드는 인가 체인코드가 발급한 토큰의 유효성을 확인한 다음, Private Data 영역에 저장된 사용자의 개인정보를 서드파티에게 제공한다. 이들 체인코드의 구동 내역은 개별 트랜잭션으로 간주되어, 블록체인의 블록에 이력이 저장된다.

인가 체인코드와 리소스 체인코드는 UMA2 표준에 명시된 RPT(Request Party Token), PCT(Persisted Claims Token), PAT(Protection API Token)를 모두 지원한다. 클라이언트 앱과 서드파티 또한 UMA2 표준에 명시

된 메시지 포맷과 프로토콜을 준용한다. 인가 체인코드와 리소스 체인코드는 엔드포인트로 전달되는 메시지의 헤더 정보에 따라 각 메시지 타입을 구분하고, 메시지의 바디 정보 내용으로 접근 권한 여부를 조회한다.

인가 체인코드는 프라이버시 정책 기반의 자동화된 승인/거부뿐만 아니라 UMA2가 제공하는 동기식/비동기식 질의 기능 또한 제공한다. 그림 3은 블록체인 UMA의 동기식 질의 절차를 보인다. 서드파티가 인가 체인코드에게 개인정보 접근 권한을 요청하면(단계1), 인가 체인코드는 사용자가 미리 설정한 프라이버시 정책을 조회하여 해당 서드파티가 개인정보에 접근할 자격이 있는지 검증한다(단계2). 만약 사용자의 프라이버시 정책에 따라 해당 서드파티가 동기식 질의에 해당하는 경우, 즉 해당 접근권한에 대한 프라이버시 정책이 존재하지 않는 경우, 인가 체인코드는 사용자에게 바로 직접 해당 접근 요청을 승인받아야 한다. 인가 체인코드는 동기식 질의 요청을 확인하고 클라이언트 앱으로 서드파티의 개인정보 접근 권한 요청을 전달한다. 사용자는 클라이언트 앱을 통해 개인정보 요청 내역을 조회하고, 해당 요청의 승인 또는 거부를 선택한다(단계3-4). 인가 체인코드는 사용자가 승인한 경우에만 토큰을 발급하여 서드파티에게 전달한다(단계5). 서드파티가 해당 토큰과 함께 개인정보 요청 메시지를 리소스 체인코드에 전달하면(단계6), 리소스 체인코드는 토큰을 검증한 뒤 개인정보를 제공한다(단계7-8).

비동기식 질의인 경우, 즉 사용자가 오프라인 상태인 경우(예. 동기식 질의 요청 후 일정 시간 경과,

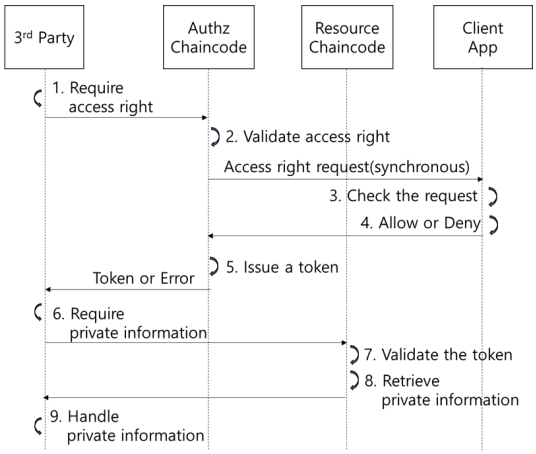

Fig. 3. Synchronous query process

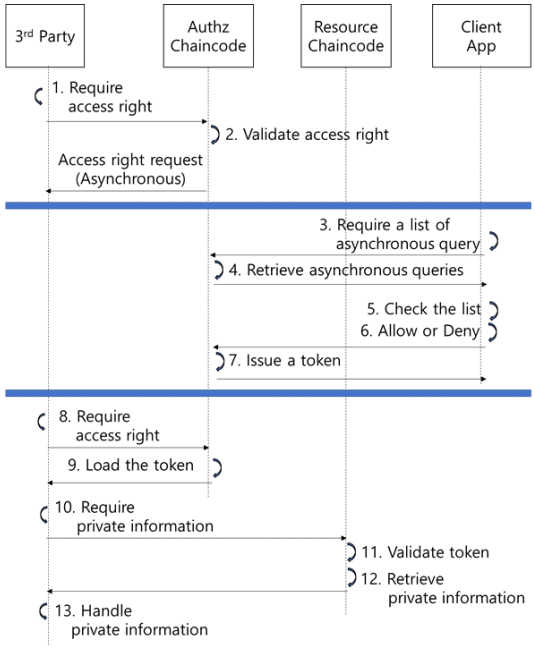

Fig. 4. Asynchronous query process

클라이언트 앱 구동 중지 등), 사용자가 향후에 해당 접근 요청을 승인해야만 서드파티가 개인정보에 접근할 수 있다. 그림 4는 블록체인 UMA의 비동기식 질의 절차를 보인다. 서드파티가 인가 체인코드에게 개인정보 접근 권한을 요청하면(단계1), 인가 체인코드는 사용자의 프라이버시 정책을 조회하고, 비동기식 질의에 해당할 경우 서드파티에게 대기 응답을 내린다(단계2). 임의의 시간이 경과한 이후, 사용자가 클라이언트 앱을 통해 대기 중인 질의 요청을 확인하고(단계3), 인가 체인코드로부터 서드파티의 개인정보 요청 내역을 조회한다(단계4-5). 사용자가 해당 요청의 승인 또는 거부를 선택하면(단계6), 인가 체인코드는 사용자의 선택에 따라 토큰을 발급한다(단계7). 서드파티가 인가 체인코드에게 질의 요청 결과를 확인하고 토큰을 받았다면(단계8-9), 해당 토큰과 함께 개인정보 요청 메시지를 리소스 체인코드에 전달하여 개인정보를 받는다(단계 10-12).

IV. 구 현

본 논문에서 제안한 블록체인 UMA 프레임워크는 Ubuntu 18.04 운영체제, Node.js 8.15.0 버전, Hyperledger Fabric 1.4.8 버전에서 구현했

다. Hyperledger Fabric 1.4 버전은 완성도가 높고 안정적인 최초의 LTS(Long Term Support) 버전이다. 또한 Hyperledger Fabric 버전 중에서 가장 많이 연구[1]되고 있을 뿐만 아니라, Amazon 클라우드[11]와 IBM 클라우드[12] 등 다수의 상용 프로젝트에 적용되었다. 따라서 본 논문에서도 2020년 7월에 공개된 1.4.8 버전을 기반으로 구현하였다.

블록체인 UMA 프레임워크의 핵심이 되는 인가 체인코드와 리소스 체인코드는 다음과 같이 구현되었다. 첫째, 개인정보 관리는 등록, 업데이트, 삭제기능으로 나뉘고 리소스 체인코드가 처리한다. 각 기능별로 리소스 정보(리소스의 식별자, 이름, 타입)와 리소스 값을 입력 파라미터로 받는다. 개인정보 관리를 위해서는 UMA2 표준에 명시된 Bearer 타입의 PAT(Protection API Token)가 필요한데, 인가 체인코드에 PAT 요청 메시지와 사용자의 id 및 패스워드를 제시하여 획득한다. 둘째, 프라이버시 정책 관리는 정책 등록, 접근 권한 처리 기능으로 나뉘고 인가 체인코드가 처리한다. 프라이버시 정책 등록은 리소스의 식별자와 접근 권한을 입력 파라미터로 받고, 접근 권한은 '읽기' 또는 '수정'을 지원한다. 셋째, 서드파티는 PAT와 리소스의 식별자를 입력으로 받고 인가 체인코드로부터 UMA2 표준에 명시된 RPT(Request Party Token)를 발급받는다. 서드파티는 리소스 체인코드에게 RPT를 제시하고, 리소스 정보와 리소스 값을 받는다.

그림 5는 동기식 질의 과정에서 서드파티와 클라이언트 앱의 UI를 보인다. 왼쪽 그림에서 서드파티는 접근이 거부된 사용자의 주소 정보를 요청하였다. 인가 체인코드는 해당 요청을 수신한 뒤에 연관된 프라이버시 정책이 없는 것을 확인하고 사용자에게 승인을 요청한다. 오른쪽 그림에서 클라이언트 앱이 팝업으로 사용자에게 승인을 요청하는 것을 볼 수 있다. 사용자가 승인한 경우, 서드파티는 사용자의 주소 정보를 조회할 수 있다.

그림 6은 비동기식 질의 과정에서 서드파티와 클라이언트 앱의 UI를 보인다. 왼쪽 그림에서 서드파티는 접근이 거부된 사용자의 주소 정보를 요청하였다. 인가 체인코드는 사용자에게 승인을 요청하지만 사용자가 응답할 수 없는 경우 승인대기 상태로 변경

1) Google Scholar의 검색 결과("Hyperledger Fabric v x.x")에 따르면, 1.4 버전(53 건), 1.1 버전(53 건), 1.2 버전(35 건), 1.3 버전(25 건), 2.1 버전(1 건), 2.0 버전(0 건), 2.3 버전(0 건) 순으로 조회됨.

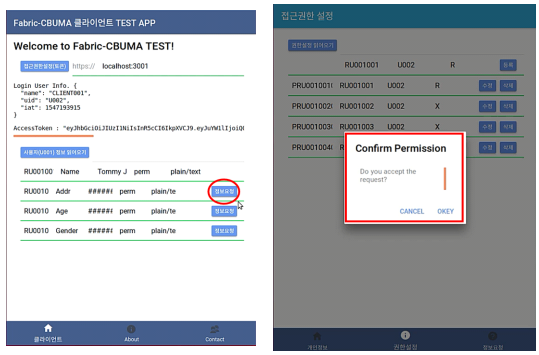

Fig. 5. UI for synchronous query(left: 3rd party, right: client app)

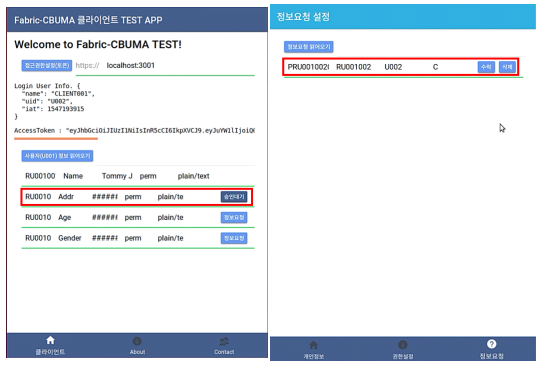

Fig. 6. UI for asynchronous query(left: 3rd party, right: client app)

된 것을 볼 수 있다. 오른쪽 그림에서 사용자는 클라이언트 앱에서 승인 대기 요청을 조회할 수 있다. 사용자가 승인한 경우, 서드파티는 향후 재요청을 통해 사용자의 주소 정보를 조회할 수 있게 된다.

V. 평 가

5.1 성능 분석

본 논문에서 제안한 블록체인 UMA 프레임워크는 Intel i7-7500U CPU 2.9GHz, 16GB RAM, 64비트 버전의 Windows 10 운영체제에서 성능을 분석하였다. 그림 7과 같이, 5개의 블록체인 노드를 각각 VM(Virtual Machine)에서 Ubuntu 18.04 운영체제, Node.js 8.15.0 버전, Hyperledger Fabric 1.4.8 버전에서 구동하도록 네트워크를 구성하였다. 특히 UMA2의 단점인 확장성과 장애 발생 이슈에 대한 대응을 검증하기 위해,

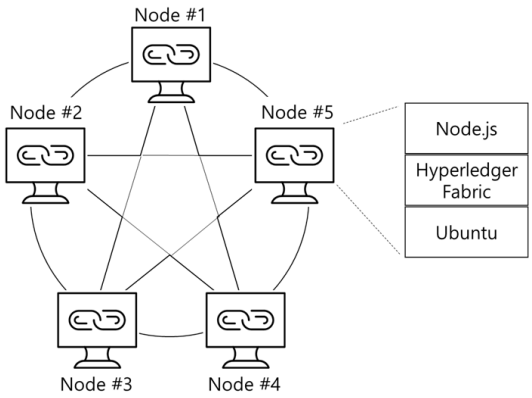

Fig. 7. Blockchain network for evaluation

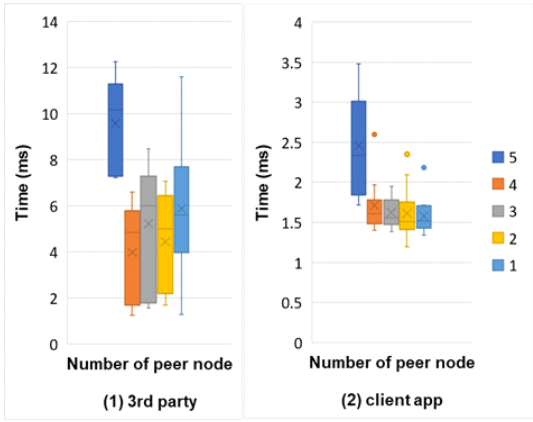

Fig. 8. Chaincode execution time

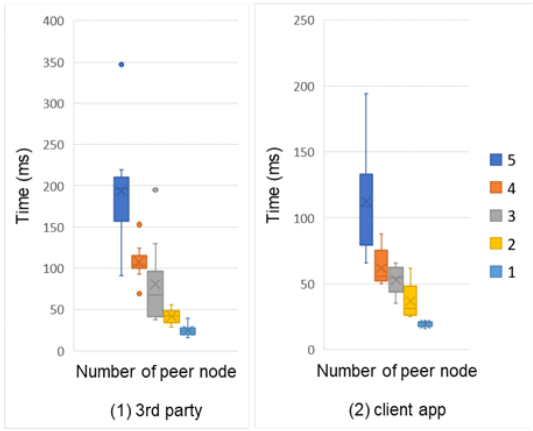

Fig. 9. Block confirmation time

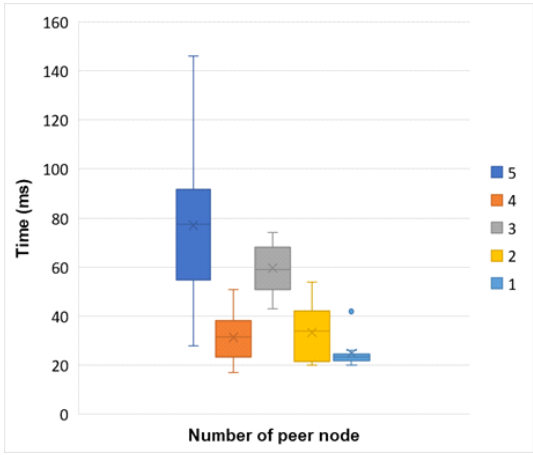

Fig. 10. Latency of user notification

블록체인 네트워크의 노드 수를 변경하면서 전체 프로세스에 소요되는 시간을 측정하였다. 구체적으로, 장애 상황을 재현하기 위해 노드 수를 5개부터 1개까지 순차적으로 1개씩 강제로 중지하였다. 각 상황별로 그림 3의 동기식 질의 프로세스를 10회 측정하였고, 블록체인 네트워크에서 체인코드 실행과 블록 생성에 소요되는 시간은 Hyperledger Fabric 네트워크의 로그 메시지를 통해 도출하였다. 동기식 질의에서 사용자가 클라이언트 앱을 통해 개인정보 요청 내역을 통보받는데 소요되는 시간은 웹브라우저의 개발자 기능을 통해 네트워크 지연 시간을 도출하였다. 성능 분석 결과는 그림8~10과 같이, 성과 그림 그래프의 5가지 요약 수치(최솟값, 제1사분위, 제2사분위, 제3사분위, 최댓값)로 표현하여 데이터의 통계적인 특성을 관찰하였다.

첫 번째로 체인코드의 구동시간을 분석하였다. 체인코드는 호출 주체에 따라 서드파티와 클라이언트 앱으로 구분되는데, 그림 3에서 볼 수 있듯이 서드파티는 1~9 단계까지 구동하여 인가 체인코드와 리소스 체인코드를 모두 실행하고, 클라이언트 앱은 2-4 단계까지만 구동하여 인가 체인코드만 실행한다. 이 때문에, 그림 8에서, 체인코드의 구동시간은 서드파티(평균 5.8 ms)에 비해 클라이언트 앱(평균 1.8 ms)의 구동 시간이 짧은 것을 볼 수 있다. 또한 그림 8(1)에서 서드파티는 노드가 5개인 경우가 가장 느리고(평균 9.5 ms), 나머지 경우는 일정(평균 4 ~ 6 ms)하다. 노드가 1개인 경우, 1.2 ms ~ 11.6 ms 까지 변동폭이 크다. 이는 노드 1개에서 모든 체인코드를 실행해야 하므로, 처리 과정에서 간헐적으로 과부하가 걸리는 것으로 판단된다. 그림 8(2)에서 클라이언트 앱의 경우, 노드 5개를 제외하

면 일부 비정상 수치에 불구하고 평균 1.5 ms 정도로 안정적인 구동 시간을 보인다. 이는 클라이언트 앱이 블록체인 블록 중에서 서드파티의 요청 내역을 검색하고 사용자의 응답을 블록에 추가하는 간단한 작업을 수행하기 때문으로 판단된다.

두 번째로 각 트랜잭션을 블록으로 기록하는데 소요되는 합의시간을 분석하였다. 블록 합의는 트랜잭션 주체에 따라 서드파티와 클라이언트 앱으로 구분된다. 서드파티는 토큰 발급을 위해 사용자의 승인을 요청하는 트랜잭션과 토큰을 사용하여 사용자의 개인정보를 요청하는 트랜잭션을 수행한다. 클라이언트 앱은 서드파티의 승인 요청에 대해 사용자의 응답을 등록하는 트랜잭션을 수행한다. 이 때문에, 그림 9에서 블록 합의시간은 서드파티(평균 89.5 ms)에 비해 클라이언트 앱(평균 56.7 ms)이 짧은 것을 볼 수 있다. 또한 노드 개수가 줄어듬에 따라 블록 합의시간이 줄어들고 편차 또한 줄어드는 것을 볼 수 있다. 이는 블록체인 네트워크의 노드가 증가할수록, 노드들이 합의에 이르기까지의 시간 또한 증가되기 때문이다. 노드가 1개인 경우는 블록 합의시간의 편차가 상대적으로 적은 것을 볼 수 있다.

세 번째로 동기식 질의 과정에서 인가 체인코드가 요청 트랜잭션을 읽은 뒤 클라이언트 앱이 승인 요청 팝업을 열기까지의 시간을 분석하였다. 인가 체인코드가 서드파티의 승인 요청 블록을 확인하고 클라이언트 앱에게 승인 요청 내역을 전달하면, 클라이언트 앱은 팝업으로 해당 내역을 출력한다. 그림 10에서 노드 개수가 줄어들수록 승인 요청 팝업이 열리는 시간이 줄어드는 것을 볼 수 있다. 구체적으로, 노드가 5개인 경우 평균 시간은 77 ms이고 편차가 큰 것을 확인할 수 있다. 반면에 노드가 1개인 경우, 평균 시간은 24.9 ms이며, 1건의 아웃라이어를 제외하고는 편차가 적다. 이는 노드들 간의 블록 합의 및 등록에 걸리는 시간이 인가 체인코드의 블록 확인 시간에 영향을 미치는 것으로 판단된다.

5.2 기능 분석

블록체인 UMA 기술은 사용자가 Hyperledger Fabric에서 본인의 개인정보를 세밀하게 관리하지 못하는 단점을 해소한다. 퍼미션 블록체인에서 사용자 중심으로 세밀하게 개인정보 관리를 제어하는 기능을 제공함으로써, 2장에서 언급했던 문제를 해결한다. 사용자는 리소스 체인코드를 통해 자신의 개인정보와 프라이버시 정책을 블록체인 내에서 관리할 수 있다. 인가 서버에 해당하는 인가 체인코드는 사용자의 프라이버시 정책에 따라 사용자의 개인정보 제공 여부를 다양한 방식(예. 프라이버시 정책, 동기

Table 1. Comparison between the proposed method and the existing studies

	FairAccess [4]	Zyskind's method [6]	PrivacyGuard [5]	Kaaniche's method [7]	Blockchain UMA
Automated access control	x	o	o	o	o
Synchronous access control	o	x	x	x	o
Fine-grained privacy policy	x	x	o	o	o
Storage for private information	IoT	DHT	Cloud	User	DHT
Storage for privacy policy	User	Blockchain	Smart Contract	Smart Contract	DHT
Type of Blockchain	Public	Public	Public	Permissioned	Permissioned
Use of smart contract	x	x	o	o	o
Implementation	o	x	x	x	o
Characteristic	ORBAC	DHT	TEE	HIBE	UMA2

* DHT: Distributed Hash Table
* ORBAC: ORganisation-Based Access Control,
* TEE: Trusted Execution Environment,
* HIBE: Hierarchical Identity Based Encryption

식 질의, 비동기식 질의)으로 결정한다.

또한 블록체인 UMA 기술은 UMA2 표준에서 도출된 안정성, 프라이버시, 보안성 문제를 모두 해결한다. 첫째, 인증 서버와 리소스 서버가 블록체인 노드에 분산된 체인코드 형태를 가지기 때문에, 중앙 엔터티의 단일 지점 장애로부터 안전해진다. 둘째, 사용자의 프라이버시 정책과 개인정보는 Hyperledger Fabric의 Private Data 영역에 암호화되어 저장되기 때문에 안전하다. 셋째, 임의로 블록체인에 저장된 개인정보나 프라이버시 정책의 변경이 시도되더라도 변경 이력이 블록에 기록되어 노드 간에 공유되기 때문에 탐지와 대응이 용이해진다.

2.1 절에서 분석된 기존 블록체인 기반의 접근제어 연구 결과[13]와 비교할 때, 표 1과 같이 본 제안 방안의 특징을 9가지 측면에서 도출할 수 있다.

1. 자동화된 접근제어; 블록체인 UMA 기술을 포함한 나머지 관련 연구는 사용자의 명시적 개입 없는 자동화된 접근제어를 지원한다. 반면에 FairAccess는 사용자가 지갑형태로 관리되는 개인정보를 직접 제공해주어야 하므로 수동 접근제어만 이루어진다.
2. 동기식 접근제어; 사용자의 명시적인 승인에 따른 접근제어는 FairAccess와 블록체인 UMA 기술만 가능하다. 나머지 관련 연구는 사용자가 사전에 수립한 프라이버시 정책에 따라서 비동기적으로 접근제어가 동작한다.
3. 사용자가 정의한 다양한 수준의 프라이버시 정책; FairAccess는 ORBAC이라는 특정 접근제어 정책을 따라야 하고, Zyskind의 방법은 특정 서비스에게 특정 개인정보 타입을 제공한다는 간단한 프라이버시 정책을 사용한다. 반면에 블록체인 UMA 기술을 포함한 나머지 관련 연구는 특정 프라이버시 정책에 의존하지 않기 때문에 사용자가 직접 정의한 다양한 수준의 프라이버시 정책과 연동할 수 있다.
4. 개인정보 저장 위치; 사용자의 개인정보가 저장되어 있는 곳을 의미하며, 관련 연구 별로 차이를 보인다. 블록체인 UMA 기술은 Hyperledger Fabric의 Private Data 영역에 저장되어 있는데, 이 영역은 분산 해시 테이블(DHT)와 동일한 방식으로 동작하기 때문에 DHT로 표기하였다. 나머지 관련 연구는 IoT 장치, 클라우드, 사용자가 직접 개인정보를 보관한다는 특징이 있다.
5. 프라이버시 정책 저장 위치; 사용자의 프라이버시 정책이 저장되어 있는 곳을 의미하며, 관련 연구 별로 차이를 보인다. 블록체인 UMA 기술은 Hyperledger Fabric의 Private Data 영역에 저장되어 있기 때문에 DHT로 표기하였다. FairAccess는 사용자가 직접 제어하고, Zyskind는 블록체인의 블록에 프라이버시 정책을 저장한다. PrivacyGuard와 Kaaniche는 스마트 컨트랙트 내에 프라이버시 정책을 명시한다.
6. 블록체인 타입; 관련 연구가 지원하는 블록체인의 타입을 의미한다. 블록체인 UMA와 Kaaniche의 방법은 퍼미션 블록체인을 지원하며, 나머지 관련 연구는 공개 블록체인을 지원한다.
7. 스마트 컨트랙트 사용; 블록체인 접근제어를 위해 스마트 컨트랙트를 사용하는지 여부를 의미한다. 스마트 컨트랙트를 사용하면 블록체인 노드 간에 접근제어 절차를 투명하게 집행하고 검증할 수 있다. 관련 연구 중에서 블록체인 UMA, PrivacyGuard, Kaaniche의 방법만 스마트 컨트랙트를 사용한다. 하지만 PrivacyGuard와 Kaaniche는 스마트 컨트랙트에 프라이버시 정책이 명시되어 있기 때문에, 정책 수정 등 관리가 불편하다.
8. 실제 구현; 관련 연구 중에서 실제 환경에서 구현을 통해 동작이 검증되었는지 여부를 의미한다. 관련 연구 중에서는 블록체인 UMA와 FairAccess만 실제 블록체인 환경에서 구현되어 정상적으로 동작함을 보였다.
9. 특정 적용기술; 관련 연구들이 접근제어 서비스를 위해 활용하는 기반 기술을 의미한다. FairAccess는 ORBAC이라는 접근제어 기술, Zyskind는 DHT라는 분산 저장소 기술, PrivacyGuard는 TEE라는 하드웨어 신뢰 환경, Kanniche는 HIBE라는 ID 기반 암호화 기술에 기반한다. 블록체인 UMA는 UMA2라는 접근제어 프로토콜에 기반한다.

즉, 블록체인 UMA 기술은 사용자의 프라이버시 정책을 기반으로 자동화된 접근제어 뿐만 아니라, UMA2 표준에 기반한 사용자 동기식/비동기식 질의 및 사용자가 직접 정의한 다양한 수준의 프라이버시

정책 적용이 가능하다. 개인정보 데이터와 프라이버시 정책은 DHT에 해당하는 Hyperledger Fabric의 Private Data에 암호화된 상태로 저장된다. 블록체인 UMA는 대표적인 퍼미션 블록체인인 Hyperledger Fabric 1.4버전에서 인가 체인코드와 리소스 체인코드라는 스마트 컨트랙트 형태로 구현하여 성능 및 기능 검증을 완료했다.

VI. 결론 및 향후 연구

본 논문은 퍼미션 블록체인 기술과 표준 프라이버시 보호 기술을 결합한 블록체인 UMA 기술을 제시한다. 본 논문의 가장 큰 컨트리뷰션은 퍼미션 블록체인과 UMA2 표준 각각의 장점을 유지하면서, 동시에 각 방식에 존재하는 단점을 극복한 것이다. 기존 블록체인이 제공하지 못했던 사용자 중심의 접근제어 기능을 제공했고, UMA2 표준의 단점인 중앙 엔터티의 프라이버시/보안성/가용성 문제를 해결하였다. 이를 통해 블록체인 기반의 개인정보 제어 시스템은 사용자의 명시적인 동의를 기반으로 신뢰성이 보장되는 접근제어를 수행할 수 있다. 또한 제안 기술을 Hyperledger Fabric 1.4 버전에 구현하고 실제로 동작함을 검증하였다.

향후에는 접근제어의 편의성을 높이면서 사용자의 프라이버시를 더욱 강화하는 방향의 추가 연구가 필요하다. 첫 번째 연구 방향은, 기계학습으로 사용자의 명시적인 접근제어 개입을 줄이는 방법이다. 사전에 정의된 프라이버시 정책이 없는 경우, 기존 방식은 사용자가 직접 해당 접근제어 요청을 처리해야 하는 부담이 있다. 유사한 성향의 타 사용자 혹은 사용자의 이전 접근제어 이력을 기반으로 사용자의 접근제어 성향을 예측하여 적절한 접근제어를 추천한다면, 제안 방안의 편의성을 개선할 수 있다. 두 번째 연구 방향은 영지식증명과 같이 개인정보 노출없는 검증 방법을 적용하는 것이다. 제안 방안에서는 사용자의 동의에 따라서 개인정보 접근을 제어할 수 있지만, 한 번 제공된 개인정보의 노출 및 활용을 제한할 수는 없다. 하지만 영지식증명과 같이 개인정보를 노출시키지 않는다면, 제안 방안과 접목하여 사용자의 프라이버시 보호를 개선할 수 있다.

References

[1] Voigt, P., and Von dem Bussche, A., "The EU General Data Protection Regulation (GDPR)," A Practical Guide, 1st Ed., Cham: Springer International Publishing, pp. 1-392, Aug. 2017.

[2] Pew Research, "Privacy and Information Sharing," Retrieved May, 2021, from https://www.pewresearch.org/ internet/2016/01/14/privacy-and-information-sharing/.

[3] Maler, E., M. Machulak, and J. Richer., "User-Managed Access (UMA) 2.0.," Kantara Initiative, Kantara Published Specification, Jan. 2017.

[4] Ouaddah, A., Abou Elkalam, A., and Ait Ouahman, A., "FairAccess: A New Blockchain Based Access Control Framework for the Internet of Things," Security Communications. Network, vol. 9, no. 18, pp. 5943-5964, Feb. 2017.

[5] Zhang, N., Li, J., Lou, W., and Hou, Y. T., "PrivacyGuard: Enforcing Private Data Usage with Blockchain and Attested Execution," Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, pp. 345-353, Sep. 2018.

[6] Zyskind, G., and Nathan, O., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security Privacy Workshops, pp. 180-184, May. 2015.

[7] N. Kaaniche and M. Laurent, "A Blockchain-Based Data Usage Auditing Architecture with Enhanced Privacy and Availability," IEEE 16th International Symposium on Network Computing and Applications (NCA), pp. 1-5, Oct. 2017.

[8] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., and Muralidharan, S., "Hyperledger fabric: a distributed operating system for permissioned blockchains," Proceedings of the thirteenth EuroSys

conference, pp. 1-15, Apr. 2018.
〔9〕 Thakkar, P., Nathan, S., and Viswanathan, B., "Performance benchmarking and optimizing hyperledger fabric blockchain platform," IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). pp. 264-276, Sep. 2018.
〔10〕 Hyperledger, "What's new in Hyperledger fabric v2.3", Retrieved May. 2021, from https://hyperledger-fabric.readthedocs.io/en/latest/whatsnew.html#what-s-new-in-hyperledger-fabric-v2-3.
〔11〕 Amazon, "Amazon Managed Blockchain now supports Hyperledger Fabric v1.4", Retrieved May. 2021, from https://aws.amazon.com/about-aws/whats-new/2020/09/amazon-managed-blockchain-now-supports-hyperledger-fabric-v1-4/.
〔12〕 IBM, "IBM Blockchain Platform," Retrieved May. 2021, from https://marketplace.visualstudio.com/items?itemName=IBMBlockchain.ibm-blockchain-platform.
〔13〕 Seung-Hyun Kim and Soohyung Kim, "Analysis of Blockchain-based Access Control Technology," Electronics and Telecommunications Trends, Vol. 34 No. 4, pp. 117-128, Aug. 2019.

〈저자소개〉

김 승 현 (Seung-Hyun Kim) 정회원
2002년: 금오공과대학교 컴퓨터공학과 졸업
2004년: 포항공과대학교 컴퓨터공학과 석사
2004년~2021년: 한국전자통신연구원 책임연구원
2017년: 한국과학기술원 전산학부 박사
2021년~현재: 한국교원대학교 컴퓨터교육과 조교수
〈관심분야〉 블록체인, 개인정보보호, 강화학습, 컴퓨터 교육

김 수 형 (Soohyung Kim) 정회원
1996년 2월: 연세대학교 컴퓨터과학과 졸업
1998년 8월: 연세대학교 컴퓨터과학과 석사
2016년 2월: KAIST 전산학 박사
2000년 11월: 한국정보통신연구원
2000년 12월~현재: 한국전자통신연구원 정보보호연구본부 기술총괄
〈관심분야〉 ID관리, 바이오인증, 핀테크 보안, 모바일 보안, 개인정보보호