https://doi.org/10.7840/kics.2023.48.2.206

블록체인에서 안전한 다자간 서명이 가능한 DID 인증 기법

김 준 석◆, 김 근 영*, 류 재 철°

DID Authentication Method for Secure Multi-Party Signature in Blockchain

Junseok Kim◆, Geunyoung Kim*, Jaecheol Ryou°

요 약

DID(Decentralized IDentifiers)는 개인정보를 직접 관리할 수 있는 탈중앙화 신원 관리 체계이다. 블록체인 기반 DID 시스템에서의 전자서명은 VC(Verifiable Credential)를 서명하는데 사용된다. 그러나 현재 DID 표준에서는 단일 서명 방식만을 지원하여 키 관리에 어려움이 있으며, 단일 지점 장애가 발생할 수 있고 VC를 다자간 서명하는 것이 어렵다. 본 논문에서는 안전하게 다자간 서명이 가능한 블록체인 기반 DID 시스템을 제안한다. W3C DID와 VC 표준에 따라 임계 서명 기법을 사용 가능하고, 블록체인을 활용하여 DID 문서를 관리하며, ECDSA 임계 서명 기법을 통해 다자간 서명이 가능하도록 설계하였다. Universal Resolver와 MPECDSA 라이브러리를 활용하여 구현하였고, 주요 성능을 제시하였다. 결과 분석을 통해 제안된 기법이 실현 가능함을 확인하였다.

키워드 : 블록체인, 분산ID, 임계 서명 기법, 다자간 계산, 검증가능한 자격증명
Key Words : Blockchain, DID, Threshold Signature Scheme, Multi-Party Computation, Verifiable Credential

ABSTRACT

DID (Decentralized IDentifiers) is a decentralized identity management system that can directly manage personal information. The digital signature in the blockchain-based DID system is used to sign the VC (Verifiable Credential). However, the current DID standard supports only a single signature method, so it is difficult to manage keys, a single point of failure may occur, and multi-party signing of VCs is impossible. In this paper, we propose a blockchain-based DID system that can secure multi-party signatures. It is designed to enable the use of critical signature techniques according to the W3C DID and VC standards, manage DID documents using blockchain, and enable multi-party signatures through the ECDSA critical signature technique. It was implemented using Universal Resolver and MPECDSA library, and the main performance was presented. Through the analysis of the results, it was confirmed that the proposed technique is feasible.

※ 본 연구는 2022년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2020R1A2C2008864)
◆ First Author : Department of Computer Science and Engineering, Chungnam National University, jkim@o.cnu.ac.kr, 학생회원
° Corresponding Author : Department of Computer Convergence, Chungnam National University, jcryou@cnu.ac.kr, 정회원
* Department of Computer Science and Engineering, Chungnam National University, gykim@cnu.ac.kr
논문번호 : 202205-095-C-RE, Received May 8, 2022; Revised July 22, 2022; Accepted November 13, 2022

Ⅰ. 서 론

디지털 ID는 인터넷 중심의 상호 연결되고 디지털화된 사회에서 중요한 역할을 한다. 사용자들은 개인 정보, 직장, 기타 활동 등 많은 디지털 ID를 보유하고 있으며 소셜 미디어, 온라인 플랫폼 등의 시스템의 범위와 유형이 크게 증가하고 있다. 이에 따라 빅테크 기업의 ID 관리 시스템의 중앙집중화와 정보관리 구조에 의해 데이터의 주권이 침해되고 있어 ID 관리는 매우 중요해졌다. 이는 ID 정보의 관리 및 보호를 위해 설계된 ID 관리 시스템에 대한 필요로 이어지고 있다. 따라서, 최근 탈중앙화, 투명성, 접근성이 특징인 블록체인 등장으로 인해 블록체인이 통합된 ID 관리 시스템 설계가 주목받고 있다[5,6]. 블록체인 기반 신원 관리 시스템은 사용자에게 안전하고 신뢰성이 있으며 통제가 가능한 디지털 ID를 제공한다[13,14,23]. 또한, 블록체인 기반 ID 관리를 통해 중앙집중형 기관에 의존하지 않고 정보 주체가 신원 주체가 되어 프라이버시를 보호할 수 있으며 자주적으로 직접 관리할 수 있다.

블록체인 기반 DID 시스템은 자기주권 신원(Self-Sovereign Identity)를 바탕으로 설계되어 개인의 프라이버시와 개인정보를 정보주체가 직접 관리하므로 주권이 강화되고 본인의 식별자가 블록체인에 저장된다. 또한, 데이터의 무결성을 유지하면서 높은 가용성이 있으며, 본인 인증과 함께 자격 증명 기능도 제공하기 때문에 각광받고 있다[1-3]. 블록체인 기반 DID 시스템의 핵심 요소 중 하나는 무결성, 인증, 부인 방지를 제공하는 전자서명[4]이다. 블록체인 기반 DID 시스템은 비대칭 키쌍(비밀키와 공개키)을 활용하여 전자서명을 수행한다. 비밀키는 비밀키 보유자의 신원 확인과 메시지에 서명하여 메시지의 서명자가 본인임을 증명하는데 사용된다.

하지만, 기존 블록체인 기반 DID 시스템은 한계점을 가진다. DID 시스템 표준에서의 전자서명은 단일 서명 방식만을 제시하고 있다. W3C 표준[1,2]에서 제시되는 전자서명은 RSA[8], ECDSA[9], BBS+[10]이 있다. 따라서, 이들은 모두 단일 서명이기 때문에 키 관리에 어려움이 있고, 단일 지점 장애가 발생할 수 있어 보안에 취약하다. 또한, 복수 당사자의 서명이 공동 자격 증명, 다중 계약, 공금 관리 등에 있어 신원 및 자격 증명의 보안 문제에 어려움이 있다[32]. 그러므로 사용자 중심의 정보 관리가 가능하면서 다자간 활용이 가능한 DID 시스템이 필요하다.

본 논문에서는 기존 DID 시스템에 비해 보안성이 높고 안전하게 다자간 서명이 가능한 새로운 DID 시스템을 제안한다. 제안된 시스템은 DID 표준을 기본으로 일부 요소를 추가하여 기존의 단일 서명 방식보다 높은 보안성과 성능 및 효율성을 제공하는 곳이 목표이다. 이를 위해 제안된 방식은 ECDSA 기반 임계 서명 기법[11]을 이용하여 블록체인 기반 DID 시스템을 설계한다. 기존의 방식과 달리 제안된 방식은 임계 서명 기법을 이용하여 여러 참가자들이 DID 시스템을 바탕으로 서명을 재구성하여 단일 서명으로 생성하고 이를 검증자가 검증할 수 있도록 한다. 결과적으로 서명을 생성하기 위한 비밀키가 여러 참가자로 분산되어 DID로 관리되고 서명값이 단일 서명이기 때문에 높은 보안성과 성능을 제공할 수 있다.

제안하는 시스템은 오픈소스 프로젝트인 MPECDSA[12]과 Doerner et al.[11]를 활용하여 구현 및 설계하였고, 실험 결과 제안된 DID 시스템은 비밀키를 분산하고 다자간 서명이 가능함을 확인하였다.

본 논문의 나머지 부분은 다음과 같이 구성된다. 2장에서는 관련 연구를 설명한다. 3장에서는 제안된 시스템의 설계에 관하여 설명한다. 4장에서는 실험 결과를 보이고 결과를 분석한다. 5장에서는 관련 연구에 대해 논의하고 6장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1 DID(Decentralized Identifiers)

DID는 검증가능하고 분산된 신원을 위한 새로운 유형의 탈중앙화된 전역 고유 식별자이다[1]. 이러한 식별자는 중앙집중 구조가 아닌 블록체인과 같은 분산 원장과 함께 사용되도록 설계되어 사용자가 DID 주체에 대해 완전 제어가 가능하다. DID 표준의 상세 사양은 현재 W3C 그룹 주도하에 제정하여 유지 및 관리한다.

DID는 웹에 적합한 URI 체계이며 세 가지 필수 항목인 URI 체계 식별자(ex: did), DID 메서드를 위한 식별자(ex: example), DID 메서드별 식별자(ex: 123abc)로 구성된 문자열(did:example:123abc)이다. DID 메서드는 DID와 DID 문서가 생성, 해석, 업데이트 및 비활성화되는 방식을 지정한다. DID 문서는 DID 주체가 DID의 통제권을 증명하기 위한 메커니즘에 필요한 요소들이 포함된다. DID는 보유자(Holder)의 신원 증명하는데 사용되며 VC (Verifiable Credential)와 결합하여 자격 증명이 가능하도록 설계되었다.

2.2 블록체인 기반 DID 플랫폼

블록체인 기반의 DID 플랫폼은 비트코인, 이더리움 등 기존 블록체인을 활용할 수도 있고, DID에 특화된 블록체인 플랫폼인 하이퍼레저 인디(Hyperledger Indy)[24], Microsoft ION[25], Serto[26] 등을 통해 DID 시스템을 구축할 수 있다.

비트코인, 이더리움과 같은 범용 블록체인의 경우 DID 문서를 생성하고 트랜잭션과 스마트 컨트랙트를 이용하여 DID 문서를 블록체인에 저장하고, Universal Resolver[27]를 이용하여 DID 문서를 찾는다. DID에 특화된 블록체인은 DID 시스템을 위한 라이브러리, 처리 성능, 암호화를 제공하기 때문에 DID를 구현하는데 용이하다. 제안된 시스템은 이더리움을 활용하여 DID 시스템을 구현하였다.

2.3 탈중앙화 신원 관리

탈중앙화 신원 관리는 신뢰할 수 있는 데이터 교환을 가능하게 하고 특정 서비스 공급자에 의존하지 않으며 사람들이 자신의 디지털 ID를 제어하는 ID 관리 방식이다. 본 방식에서 사용자는 DID 소유권을 증명하기 위한 값과 자격 증명을 주체가 직접 제어하는 전자지갑에 저장하여 보관한다. 탈중앙화 신원 관리는 기존 신원 관리 방법과 달리 편의성과 개인 정보보호 측면에서 이점이 있고, 분산 원장 시스템을 기반으로 하기 때문에 유효성 검사, 추적 등이 용이하다.

탈중앙화 신원 관리 체계는 W3C의 DID[1], VC[2], DIF[29] 표준을 토대로 활발히 연구가 진행되고 있다. 하지만, 기존 블록체인 기반 DID 시스템은 한계점을 가진다. W3C의 탈중앙화 신원 관리 체계 관련 표준[1,2]에서 제시된 전자서명 방식으로 단일 서명 방식만을 제시하고 있다. 따라서, 이들은 모두 단일 서명이기 때문에 키 관리에 어려움이 있고, 단일 지점 장애가 발생할 수 있어 보안에 취약하다. 그러므로 사용자 중심의 다자간 활용이 가능한 DID 시스템이 필요하다.

탈중앙화 신원 관리 연구 중 보안 및 프라이버시를 위한 연구[20-22,30,31]를 분석하였다. Wang et al.[20]은 그리드 서비스에서 교차 도메인의 자산 교환 방식을 위해 블록체인 기반 DID 시스템에 다중 서명 기법을 도입하였다. Soltani et al.[21]에서는 탈중앙화 신원 기반의 디지털 온보딩 및 고객확인절차(KYC)을 위한 프레임워크를 개발하였고 프라이버시를 위하여 영지식 증명을 도입하였다. Lauinger et al.[22]은 탈중앙화 신원의 발급자의 탈중앙화 및 익명 인증을 위해 암호학적 누산기와 영지식 증명을 활용하였다. Halpin[30]은 분산형 서비스 생태계에서 프라이버시 문제를 해결하기 위해 익명 인증이 가능한 자격 증명으로 사용자 개인 정보를 관리하는 ID 시스템을 제안하였고, Tu et al.[31]은 기존 PKI 시스템에서의 사용자 키 갱신의 어려움을 해결하기 위해 블록체인 기술을 이용한 탈중앙화 신원 체계를 위한 인증 및 키 관리 기법을 제시하였다.

본 연구는 블록체인 기반 탈중앙화 신원 시스템에서 각 참여자들의 키에 대한 보안성과 프라이버시를 위해 안전한 다자간 계산 기반의 임계 서명 기법을 도입하였다는 점에서 유사하다.

2.4 임계 서명 기법

임계 서명 기법(Threshold Signature Scheme, TSS)[15]을 사용하면 n명의 참가자가 임계값 t를 설정하고 함께 공동 공개키를 생성하여 권한을 공유할 수 있다. t명의 참가자가 모이면 서명이 가능하지만 그보다 적은 수의 참가자끼리는 서명이 불가능하도록 접근 구조가 구성된다. TSS는 메시지 m에 대한 서명 요청이 있을 때 n명 중 t명의 참가자가 개별적으로 서명 공유값을 계산하고 계산된 서명 공유값을 결합하여 메시지 m에 대한 서명값을 구성할 수 있다. 이러한 기법은 다음과 같은 알고리즘으로 구성된다.

ThresKeyGen() → (P, S) : 임계 키 생성 알고리즘이며, 키쌍(P, S)를 생성하고 집합 $S = \{S_1, S_2, \cdots, S_n\}$는 n개의 비밀키 공유이며. P는 서명 검증을 위한 공개키이다. 또한, 서명 공유 검증을 위한 검증키 V도 생성한다.

ThresSign(m, S_i) → σ_i : 임계 서명 알고리즘이며, 각 참가자에게 메시지 m과 비밀키 공유 S_i가 주어졌을때 서명 공유 σ_i을 생성한다.

SigShareVrf(m, σ_i, P, V) → valid : 서명 공유 검증 알고리즘이며, 공개키 P와 검증키 V를 적절히 사용하여 각 참가자의 서명 공유 σ_i를 검증한다.

SigShareCom($\sigma_1, \sigma_2, \cdots, \sigma_t$) → σ : 서명 공유 조합 알고리즘이며, t개의 유효한 서명 공유값 집합 $\{\sigma_1, \sigma_2, \cdots, \sigma_t\}$을 통해 서명값 σ을 생성한다.

Vrf(m, σ, P) → valid : 서명 검증 알고리즘이며 단일 서명 방식과 동일하고 메시지 m에 대한 서명 값을 공개키 P를 통해 검증한다.

이전 연구[17-19,24]에서 Gennaro et al.[17]은 딜러가 없는 효율적인 키 생성으로 ECDSA 기반 임계 서명 기법을 지원하는 최초의 프로토콜을 제안하였다. 따라서 키 생성 및 서명 시간을 단축하며 통신 복잡도를 줄이면서도 안전함을 증명하였다. Gennaro et al.[18]은 효율적이고 최적인 DSA 기반의 임계 서명 기법을 제

안하였다. 악의적 공격을 최소화하면서 비트코인 지갑을 보호하는 유용하다는 특징이 있다. Lindell et al.[19]은 두 당사자 간의 다자간 서명이라는 특정 경우에 대한 임계값 ECDSA 서명 기법을 제시하였다. 영지식 증명과 모듈러 연산이 이용됐으며 게임 기반 정의를 사용하여 보안성을 증명하였다. Doerner et al.[23]은 랜덤 오라클 모델의 CDH 가정하에 t-of-n ECDSA 임계 서명 기법을 제시하고 안전성을 증명하였다. 통신과 연산 오버헤드를 줄여 IoT 디바이스에서 사용하기에 충분히 효율적이라는 것을 보였다.

본 연구는 보안성 및 서명 시간을 줄이기 위해 DID 시스템에서 임계 서명 기법을 활용한다는 점에서 기존 접근 방식[17-19,23]과 일치한다. 제안된 시스템에서 활용된 알고리즘[11]은 n-of-t Threshold ECDSA이며, DID 시스템에 적용하기 위해 필요한 요소들을 추가하여 설계하였다.

Ⅲ. 제안된 시스템 설계

안전한 키 관리와 다자간 서명을 위한 새로운 블록체인 기반 DID 시스템을 제안한다. 본 시스템은 단일 서명 기반의 기존 DID 시스템에 비해 안전한 키 관리 메커니즘을 지원하고 높은 성능의 서명을 지원하는 것을 목표로 한다. 이를 위해 ECDSA 기반의 임계 서명 기법을 활용한 DID 시스템을 고안하여 설계 및 구현하였다.

제안된 시스템은 임계 서명 기법을 사용하여 Holder들의 서명을 재구성하여 단일 서명값을 생성하고 생성된 서명값을 VC와 합하여 VP를 생성하고 이를 Verifier가 검증할 수 있다. 또한, 임계 서명 기법을 지원하기 위해 필요한 추가 변수를 위해 DID 표준에 부합하는 DID 문서를 작성하였다. 마지막으로 제안된 DID 시스템은 W3C DID 표준을 바탕으로 하기 때문에 모든 기존의 블록체인 기반 DID 시스템에서 적용이 가능하다.

3.1 개 요

그림 1은 제안하는 시스템의 전체 구조를 나타낸다. 시스템의 구성요소는 여러 보유자들, 발급자, 검증자, 블록체인 네 가지로 구성되어 있다.

보유자들은 제안된 블록체인 기반 DID 시스템에서 정보 주체이고, 발급자는 보유자의 요청에 의해 VC를 발행하며, 검증자는 보유자로부터 전달받은 VP를 검증하고 올바르다면 서비스를 제공한다. 블록체인은 보유자가 생성한 DID 문서의 저장소 역할을 한다. 이때,

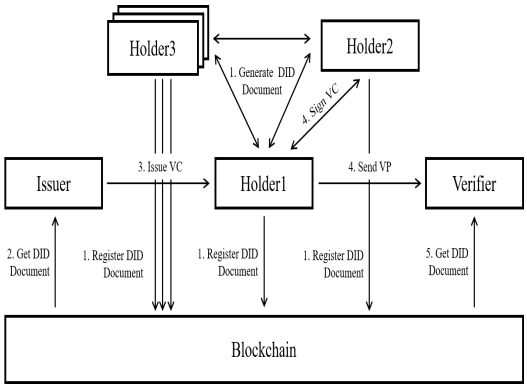

그림 1. 제안된 DID 시스템 구조
Fig. 1. Architecture of proposed DID system

활용되는 블록체인은 검증가능한 데이터 저장소로서 DID 문서 저장이 가능하고 누구나 접근이 가능해야 한다. 그림 1에서 제안된 시스템의 절차는 다음과 같다.

1) DID 문서 생성 및 등록: 다자간 서명을 수행하기 위한 DID 문서가 필요한 보유자들 간에 키 생성을 통해 DID 문서를 각 보유자가 생성하고, DID 문서를 블록체인에 등록한다.
2) DID 문서 획득: 발급자는 보유자로부터 전달받은 정보를 이용하여 블록체인으로부터 DID 문서를 획득한다.
3) VC 발급 : 발급자는 획득한 DID 문서를 바탕으로 보유자들과 인증 과정을 거치고 보유자들에게 VC를 발행한다.
4) VC 서명 및 VP 전달 : 보유자들은 발급받은VC에 다자간 서명을 수행하고 VP를 생성한다. 생성된 VP를 검증자에게 전달한다.
5) DID 문서 획득 및 검증 : 검증자는 보유자로부터 전달받은 를 통해 DID 문서를 획득하고 이를 통해 VP에 있는 서명을 검증하여 VP의 진위 여부를 판별한다.

3.2 DID 생성

보유자들이 다자간 키 생성을 통해 DID를 생성하는 과정이다. 그림 2는 2-of-3 임계 서명의 키 생성하는 절차를 나타내었다. 처음에 보유자1이 보유자2, 보유자3에게 임계값(t) 2와 참가자 수(n) 3을 포함하여 키 생성을 요청한다.

각 보유자는 x를 변수로 하는 1차 지역 다항식 (local polynomial) $p_i(x)$을 생성한 다음, 다른 보유자의 인덱스를 대입하여 개인 다항식 점(local p_point)을 구하여 각 보유자들에게 전달한다. 각 보유자들은

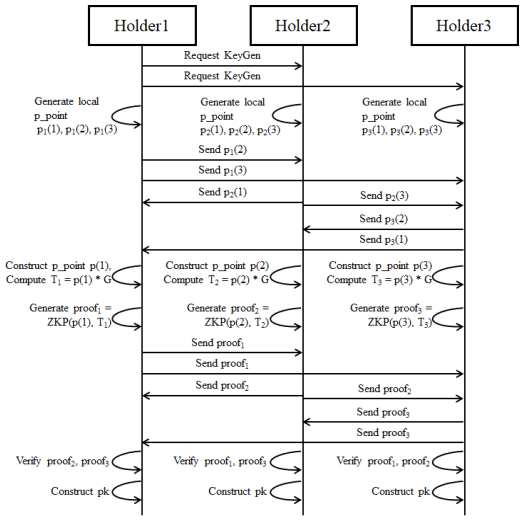

그림 2. 2 대 3 키 생성 절차
Fig. 2. Procedure of 2-of-3 key generation

전달받은 개인 다항식 점들과 같은 인덱스를 갖는 자체 생성한 개인 다항식 점을 더하여 개인키 역할을 하는 다항식 점(p_point)을 구성한다. 구성한 다항식 점에 생성원 G를 곱하여 T_i를 계산하고 p(i)와 함께 영지식 증명[16]을 생성하여 보유자들간에 교환한다. 전달받은 영지식 증명 검증을 통해 올바른 참여자임을 확인한다. 확인 결과가 모두 올바르다면 보유자들은 T_i 값을 이용하여 공동 공개키를 생성한다.

생성된 공개키를 포함하는 DID 문서를 만들어 블록체인에 저장하고 보유자들간에 DID를 서로 교환하면 DID 생성 절차가 완료된다. 이 과정은 그림 3과 같다.

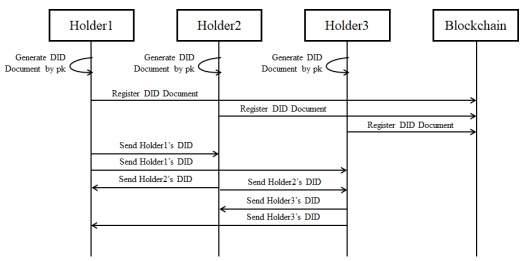

그림 3. DID 문서 생성 절차
Fig. 3. Procedure of DID document generation

3.3 VC 발급

보유자가 발급자에게 VC 발급을 요청하는 과정이며, 그림 4는 3.2절 과정을 마무리한 보유자들이 VC를 발급받는 절차이다. 보유자1이 발급자에게 VC 발급을 요청하면 발급자는 보유자1과 보유자2의 DID 값을 이용하여 블록체인 내에 저장되어있는 DID 문서를 얻고 보유자1과 보유자2에게 DID 인증을 챌린지를 요청한다. 보유자1과 보유자2는 챌린지에 대한 반응값을 계산하여 발급자에게 전달하고 발급자는 반응값을 검증한다. 검증 결과가 올바르면 보유자1과 보유자2에게 VC를 발급한다.

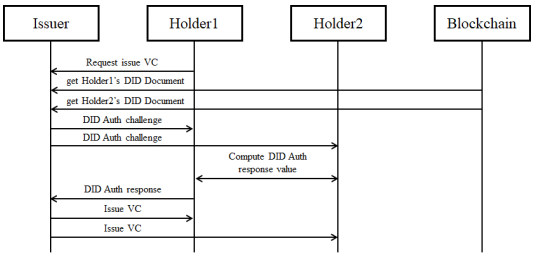

그림 4. VC 발행 절차
Fig. 4. Procedure of issuing VC

3.4 VP 제출

보유자들이 보유하고 있는 VC에 다자간 서명을 통해 서명값을 구하고 이를 이용하여 VP를 생성한다. 그림 5는 2-of-3 임계 서명 기법을 이용하여 설명하였고 그림 6은 VP를 제출 및 검증하는 것을 나타내었다. 상세한 설명은 다음과 같다.

보유자1이 보유자2에게 서명을 요청하면 보유자들간 모듈러 인버스 샘플링 프로토콜을 수행하여 인스턴스 키 공유 u_i, 인스턴스 키 인버스 공유 v_i와 R 값

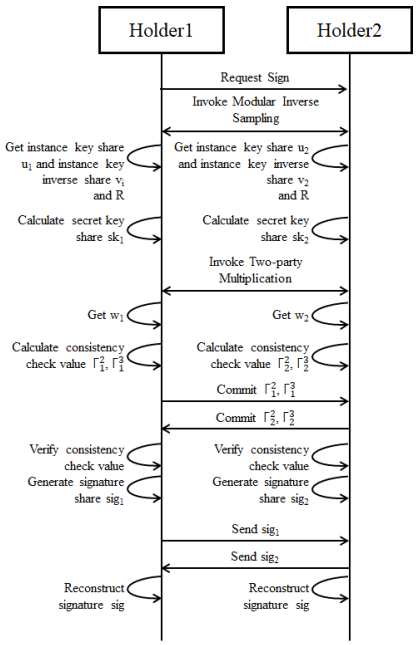

그림 5. 2 대 3 서명 절차
Fig. 5. Procedure of 2-of-3 signature

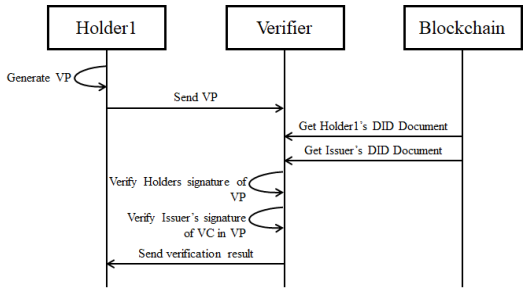

그림 6. VP 제출 절차
Fig. 6. Procedure of present VP

을 구한다[11]. 그 후 보유자들은 키생성 과정에서 생성한 값인 p(i)을 라그랑주 계수와 곱하여 sk_i를 계산한다. 보유자들간에 계산한 sk_i와 v_i를 입력으로 하여 쌍방 곱셈 프로토콜을 1라운드를 실행하고 결과로서 각 보유자가 w_i 값을 얻는다[11].

각 보유자들은 일관성 검사값 I_i^2, I_i^3을 계산하고 이 값을 커밋하여 서로 교환하여 I_j^2, I_j^3을 얻는다. 각 보유자는 얻은 일관성 검사값을 검증하여 올바르다면 VC를 메시지로 하는 서명 공유값 sig_i를 계산하고 서로 교환한다. 마지막으로, 각 보유자는 확보한 서명값들을 더하여 단일 서명값 sig를 구성한다.

보유자1이 VC와 VC의 서명값을 이용하여 VP를 생성하고 검증자에게 제출한다. 검증자는 제공받은 VP에 있는 발급자와 보유자1의 DID를 통해 블록체인으로부터 DID 문서 내 공개키를 확인한다. 이를 통해 보유자들 간에 다자간 서명으로 생성된 서명과 발급자의 서명을 각각 공개키를 이용하여 검증하고 이에 대한 결과를 자에게 전달한다.

3.5 DID와 VC 구성

본 논문에서 제시하는 DID와 VC는 기존 DID 시스템의 표준을 준수하면서 임계 서명 기법을 효율적으로 도입하기 위해 일부 항목이 DID 문서와 VC에 추가된다. 추가된 항목에 대한 설명은 다음과 같다.

그림 7은 제안하는 DID 문서에 대한 예시를 보여준다. DID 문서의 기본 항목에 참가자 수 parties, 임계값 threshold에 추가되었고, 제어자 controller 항목에 참가자로 참여하는 보유자들의 DID를 모두 나열한다. 본 예시는 2 of 3 서명을 지원하므로 참가자 수는 3, 임계값은 2, 컨트롤러는 세 참가자의 DID 주소(did:example:{ABC, DEF, GHI})들이 들어간다. 공개키는 공동 공개키를 활 용하므로 기존 단일 서명 방식과 같다. 그림 8은 제안하는 시스템 내 활용되는 VC에 대한 예시를 보여준다. VC 기본 항목과 동일하


```
{
 "@context": "https://www.w3.org/ns/did/v1",
 "id": "did:example:ABC",
 "authentication": [{
   "id": "did:example:ABC#keys-1",
   "type": "MultiPartyECDSAVerificationKey2022",
   "parties": "3",
   "threshold": "2",
   "controller": {
      "did:example:ABC",
      "did:example:DEF",
      "did:example:GHI"
   }
   "publicKeyMultibase": "zH3C2AVvLMv6gmMNaaa"
 }]
 "service": [{
  "id":"did:example:ABC",
  "type": "ThresholdSignatureScheme",
  "serviceEndpoint": "https://www.example.com"
 }]
}
```


그림 7. DID 문서 예시
Fig. 7. Example of DID document

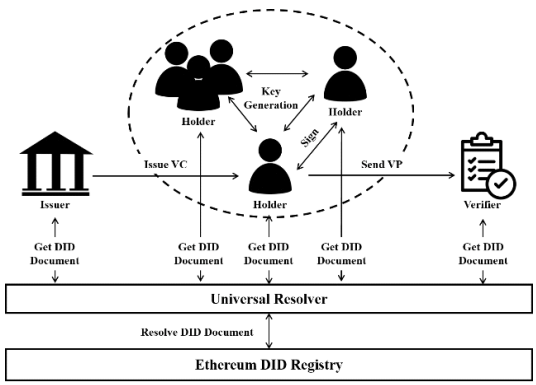

그림 8. VC 예시
Fig. 8. Example of VC

며 자격 내용(credential subject) 내에 있는 id 항목에 DID 문서를 함께 생성한 보유자들의 DID 주소가 포함된다. 그림 8의 경우 그림 7 DID 문서의 controller 항목에 있는 3개의 DID 주소가 포함되도록 한다.

Ⅳ. 구 현

제안하는 시스템을 구현하고 핵심 기능인 다자간 키 생성과 다자간 서명 그리고 서명 검증 시간을 측정하였다. 제안된 시스템의 구현을 위해 시스템의 주요 요소인 블록체인 기반 DID 시스템과 임계 서명 기법을 사용하였다. ethr-did-resolver[28] 6.0.1 버전을 이용하여 DID 관련 시스템을 개발하였고, DID 문서를 생

성하는 기능, Ethereum DID Registry 내에 DID 문서를 저장 및 획득하는 기능이 포함한다. 임계 서명 기법 라이브러리인 MPECDSA[11]를 기반으로 DID 시스템 내에 다자간 키 생성을 포함한 DID 문서 생성과 VC를 발행하는 기능과 다자간 서명을 통한 VP 생성 그리고 VP 내의 서명 검증을 off-chain에서 수행하도록 구현하였다. 제안된 시스템의 구현 결과는 그림 9와 같다.

제안하는 시스템에서 주요 기능의 성능 평가를 위한 실험을 수행하였다. 제안하는 시스템 내의 발급자, 보유자, 검증자, Universal Resolver는 Intel(R) Core(TM) i7-9700F @3.00GHz CPU와 32GB 메모리이며, Debian GNU/Linux 10 운영체제를 갖는 Desktop PC에서 실행되었으며, DID 문서를 관리하기 위한 블록체인으로 Ethereum DID Registry를 활용하였고, 컴파일러는 rustc 1.56.0 버전을 사용하였다. 모든 실험에서 PC는 대역폭이 98.3Mbps/103.1Mbps(down/uplink)인 네트워크 환경 내에서 LAN으로 통신하였다. 본 실험은 제안된 시스템의 핵심 기능인 다자간 키생성과 다자간 서명 시간을 측정하였고, 평가 기준은 키 생성과 서명 생성 참여하는 참가자 수로 하였으며 2 of 2, 2 of 3, 3 of 4, 4 of 5, 5 of 6 경우에 대해 성능을 측정하였다.


```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "id": "http://example/credentials/1873",
 "type": ["VerifiableCredential", "SocialSecurityCredential"],
 "issuer": "https://example.edu/issuers/565039",
 "issuanceDate": "2022-03-30T19:23:24Z",
 "expirationDate": "2023-03-30T19:23:24Z",
 "credentialSubject": {
    "id": {
        "did:example:ABC",
        "did:example:DEF",
        "did:example:GHI",
    },
     "name": {
         "SSN": "111-11-1111",
      }
   }
 },
 "proof": {
   "type": " EcdsaSecp256k1VerificationKey2019",
   "created": "2022-04-30T19:23:24Z ",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "https://example/issuers/12#key-1",
   "jws":"Qktb3rk-BuQy72IFLOqV0G_zS245 kronKb78c"
 }
}
```


그림 9. 제안된 시스템의 구현
Fig. 9. Implementation of proposed system

V. 실험 및 평가

5.1 성능 측정 및 분석

임계 서명 기법의 참가자 수와 임계값에 따른 키 생성과 서명 생성, 서명 검증 기능의 평균 수행 시간을 100회를 기준으로 측정하였다. 실험 결과를 토대로 분석한 결과 그림 10과 같이 키생성 참가자 수가 2명일 때 평균 51.5ms가 소요되고 키 생성 참가자수가 한 명씩 증가할 때마다 1.16배, 1.46배, 1.58배, 2.1배씩 증가하였다. 이를 통해, 다자간 키생성 수행시 임계값은 영향을 주지 않고 키 생성에 참여하는 참가자 수에 따라 선형적으로 증가한다. 그러므로 같은 네트워크 환경 내에서 보유자 간에 DID 문서를 생성한다면 보유자 수에 비례하여 시간이 소요됨을 알 수 있다.

서명 생성 과정에서 두 참가자 간에 다자간 서명을 수행했을 때 평균 12.7ms가 소요되고 서명 참가자수가 증가할 때마다 1.2배, 1.68배, 1.96배씩 증가함을 알 수 있다. 이를 통해, 다자간 서명 수행시 참가자 수에 따라 서명 시간이 선형적으로 증가함을 알 수 있다.

서명 검증 과정은 참가자수와 임계값에 관계없이 평균 2.1ms가 소요되었다. 서명 검증의 경우 검증자가 단독으로 수행하고 ECDSA 서명의 검증 기능과 동일하므로 다자간 계산으로 인한 오버헤드가 발생하지 않는다.

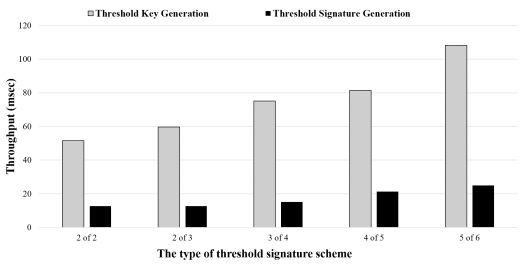

그림 10. 키 생성 및 서명 소요시간
Fig. 10. Elapsed time for key generation and sign

5.2 기능 분석

설계된 시스템을 구현하고, 주요 기능인 DID문서 생성, 블록체인으로부터 DID 문서 저장 및 획득, 다자간 키생성과 다자간 서명이 동작하는지를 검증하였다. 다자간 키생성 및 서명 기능의 소요시간을 측정한 결과, 본 논문에서 제안된 시스템의 기능들은 실현가능하고, 안정적으로 동작함을 알 수 있다. 또한, 두 기능 모두 참여자 수에 비례하여 시간이 증가하는데 이는 통신량 증가에 의한 것으로 볼 수 있다. 따라서, 네트

워크 속도가 향상된다면 소요시간을 낮출 수 있다.

기존 DID 시스템의 경우 한 VC를 바탕으로 보유자가 각각 VP를 생성하여 제출하므로 VP 내에 있는 보유자들의 DID 주소가 보여지게 된다. 제안된 시스템을 활용하는 경우, DID 문서를 함께 생성한 모든 보유자들의 DID 주소는 공개되는 데 반해 VP에 다자간 서명을 수행한 보유자의 DID 주소는 공개되지 않으므로 프라이버시가 보호된다는 장점이 있다.

Ⅵ. 결 론

본 논문에서는 블록체인 기반 DID 인증에서 안전하게 다자간 서명이 가능한 시스템을 설계하여 제안하였다. 제안된 방법은 다자간 키생성을 통해 DID 문서를 만들어 블록체인에 저장하고, DID 인증을 통해 VC를 보유자들에게 전달하여 다자간 서명을 통해 VP를 생성 및 검증하여 여러 보유자가 VP를 함께 제어할 수 있도록 구현하였으며, 안전한 다자간 계산을 위해 임계 서명 기법을 사용하였다. 제안된 방법은 W3C DID/VC 표준[1,2], 이더리움, Universal Resolver[28]와 MPECDSA 라이브러리[12]를 활용하여 구현하였고, 제안된 기법의 다자간 키생성 및 다자간 서명의 성능 측정을 진행하였고 이를 분석하였다.

제안된 방법을 통해 DID 시스템을 구축하면 여러 보유자들이 하나의 공개키의 쌍이 되는 서로 다른 개인키를 직접 관리할 수 있고, 키 분실 시 복구할 수 있으며 단일 지점 장애를 제거할 수 있다. 제안된 방법의 모든 기능은 블록체인의 온체인이 아닌 오프체인에서 진행되어 특정 블록체인 플랫폼에 의존하지 않고 DID 인증 시스템에 적용이 가능하다는 장점이 있다. 향후 연구로 블록체인 기반 DID 인증 기법에 필요한 키 갱신 및 복구 메커니즘을 추가적으로 고려된다면 시스템의 가용성과 보안성이 향상될 것으로 기대된다.

References

[1] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized identifiers (DIDs) v1.0,” *W3C Proposed Recommendation*, Aug. 2021.

[2] M. Sporny, G. Noble, D. Longley, D. Burnett, B. Zundel, and K. D. Hartog, “Verifiable credentials data model 1.1,” *W3C Recommendation*, Mar. 2022.

[3] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, “Self-sovereign and decentralized identity as the future of identity management?,” *Open Identity Summit*, 2020. (https://doi.org/10.18420/ois2020_03)

[4] NIST, Corporate, “The digital signature standard,” *Commun. of the ACM*, vol. 35, no. 7, pp. 36-40, 1992.

[5] T. Andrew and D. Reed, “The inevitable rise of self-sovereign identity,” *The Sovrin Foundation*, Apr. 2016. (http://doi.org/10.1007/978-981-19-0852-1_19)

[6] N. Naik and P. Jenkins, “uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain,” *2020 IEEE ISSE*, pp. 1-7, 2020. (https://doi.org/10.1109/ISSE49799.2020.9272223)

[7] L. Harn, “Group-oriented (t, n) threshold digital signature scheme and digital multisignature,” *IEE Proc.-Comput. and Digital Techniques*, vol. 141, no. 5, pp. 307-313, 1994. (https://doi.org/10.1049/ip-cdt:19941293)

[8] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. of the ACM*, vol. 21, no. 2, pp. 120-126, 1978. (https://doi.org/10.1145/359340.359342)

[9] F. PUB, “Digital Signature Standard (DSS),” *FIPS PUB*, pp. 186-192, 2000. (https://doi.org/10.6028/nist.fips.186-4)

[10] J. Camenisch, M. Drijvers, and A. Lehmann, “Anonymous attestation using the strong diffie hellman assumption revisited,” *9th Int. Conf. Trust and Trustworthy Computing*, Springer, Cham, vol. 9, pp. 1-20, Vienna, Austria, Aug. 2016. (https://doi.org/10.1007/978-3-319-45572-3_1)

[11] J. Doerner, et al., “Threshold ECDSA from ECDSA assumptions: The multiparty case,” *2019 IEEE Symp. Security and Privacy*, pp. 1051-1066, 2019. (https://doi.org/10.1109/SP.2019.00024)

[12] Doerner, *MPECDSA*(2021), Retrieved May 8, 2022. from https://gitlab.com/neucrypt/mpecdsa

[13] D. Allessie, et al., "Blockchain for digital government," *Luxembourg: Publications Office of the European Union*, p. 88, 2019.

[14] J. Y. Won, "The era of private certificates... What is the domestic DID status?", Retrieved May, 30, 2022, from "https://dealsite.co.kr/articles/60896"

[15] V. Shoup, "Practical threshold signatures," in *Advances in Cryptology—EUROCRYPT 2000,* Springer, vol. 19, pp. 207-220, Berlin, Heidelberg, May 2000. (https://doi.org/10.1007/3-540-45539-6_15)

[16] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *J. Cryptology*, vol. 7, no. 1, pp. 1-32, 1994. (https://doi.org/10.1007/BF00195207)

[17] R. Gennaro and S. Goldfeder, "Fast multiparty threshold ECDSA with fast trustless setup," in *Proc. 2018 ACM SIGSAC Conf. Comput. and Commun. Secur.*, pp. 1179-1194, 2018. (https://doi.org/10.1145/3243734.3243859)

[18] S. Goldfeder, et al., "Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme," et al., 2015.

[19] Y. Lindell, "Fast secure two-party ECDSA signing," *Annu. Int. Cryptology Conf.*, pp. 613-644, Springer, Cham, 2017. (https://doi.org/10.1007/s00145-021-09409-9)

[20] X. Wang, et al., "A credible transfer method of cross-chain assets based on DID and VC," *2021 IEEE 4th ICISCAE*, pp. 238-242, 2021. (https://doi.org/10.1109/ICISCAE52414.2021.9590718)

[21] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," *2018 IEEE Int. Conf. Internet of Things (iThings) and IEEE Green Comput. and Commun. (GreenCom) and IEEE Cyber, Physic. and Soc. Comput. (CPSCom) and IEEE Smart Data*, pp. 1129-1136, 2018. (https://doi.org/10.1109/Cybermatics_2018.2018.00205)

[22] J. Lauinger, et al., "A-poa: Anonymous proof of authorization for decentralized identity management," *2021 IEEE ICBC*, pp. 1-9, 2021. (https://doi.org/10.1109/ICBC51069.2021.9461082)

[23] S. Kim, S.-H. Lee, Y. Cho, and S. Kim, "A study on blockchain based identity management systems," in *Proc. Symp. KICS*, pp. 730-731, 2019.

[24] M. P. Bhattacharya, P. Zavarsky, and S. Butakov, "Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain," *2020 ISNCC*, pp. 1-7, 2020. (https://doi.org/10.1109/ISNCC49221.2020.9297357)

[25] "*Decentralized identity: Own and control your identity*," 2018, [online] Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY.

[26] A. M. Thomas, R. Ramaguru, and M. Sethumadhavan, "Distributed identity and verifiable claims using ethereum standards," in *Proc. ICICCT 2021*, pp. 621-636, Singapore: Springer Nature Singapore, 2022. (https://doi.org/10.1007/978-981-16-5529-6_48)

[27] M. Sabadello, *A Universal Resolver for self-sovereign identifiers*, 05 2019, [online] Available: https://medium.com/decentralized-identity/a-universalresolver-for-self-sovereign-identifiers-48e6b4a5cc3c.

[28] D. I. Foundation, *DID resolver for Ethereum Addresses with support for key management,* 2020, https://github.com/decentralized-identity/ethr-did-resolver

[29] "*Decentralized Identity Foundation*," 2020, [online] Available: https://identity.foundation/.

[30] H. Halpin, "Nym credentials: Privacy-preserving decentralized identity with blockchains," *2020 CVCBT IEEE*, pp. 56-67, 2020. (https://doi.org/10.1109/CVCBT50464.2020.00010)

[31] Y. Tu, et al., "Decentralized identity authentication and key management scheme,"

2019 IEEE 3rd Conf. Energy Internet and Energy Syst. Integration (EI2), pp. 2697-2702, 2019. (https://doi.org/10.1109/EI247390.2019.9062013)

[32] Z. Omer Shlomovits, "*Threshold Signatures Explained*," Binance Academy, 2021. [online] Available: https://academy.binance.com/en/articles/threshold-signatures-explained

김 준 석 (Junseok Kim)

2021년 2월 : 충남대학교 컴퓨터공학과 학사

2021년 3월~현재 : 충남대학교 컴퓨터공학과 석사과정

<관심분야> 블록체인, 인증, 암호 구현

김 근 영 (Geunyoung Kim)

2018년 2월 : 충남대학교 컴퓨터공학과 학사

2018년 3월~현재 : 충남대학교 컴퓨터공학과 석박사통합과정

<관심분야> 블록체인, DID, 인증

류 재 철 (Jaecheol Ryou)

1985년 2월 : 한양대학교 산업공학과 학사

1988년 5월 : Iowa State University 전산학 석사

1990년 12월 : Northwestern University 전산학 박사

1991년 2월~현재 : 충남대학교 컴퓨터융합학부 교수

<관심분야> 모바일 보안, 금융 보안, 블록체인