Journal of KIIT. Vol. 23, No. 9, pp. 161-171, Sep. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.9.161

DIDonate: 블록체인과 DID를 활용한 고신뢰성 기부 플랫폼

최희민*, 김희열**

DIDonate: A High-Reliability Donation Platform using Blockchain and DID

Heemin Choi*, Heeyoul Kim**

본 연구는 2024학년도 경기대학교 대학원 연구원장학생 장학금 지원에 의하여 수행되었음. 이 논문은 2024년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. RS-2020-NR049579)

요 약

기존 중앙집중형 기부 시스템은 운영 기관의 신뢰를 전제로 운영된다. 이러한 구조적 특성으로 인해 기부 내역과 집행 과정의 투명성이 부족하여 기부금 횡령 및 사기 문제가 발생한다. 이를 해결하기 위해 블록체인의 불변성, 투명성, 추적 가능성을 활용한 기부 시스템 연구가 활발히 진행되었으나, 대부분 수혜자 자격 검증 메커니즘 부재하거나 오프체인 데이터에 의존하여 신뢰성과 효율성의 측면에서 한계가 존재한다. 본 논문에서는 공개형 블록체인 이더리움과 하이퍼레저 인디 기반의 분산 신원 식별자(DID)를 활용하여, 수혜자의 자격을 온체인 데이터 기반으로 검증하는 방법을 제안한다. 특히, DID-이더리움 계정 바인딩 정보를 스마트 컨트랙트에 등록하고 검증하는 메커니즘을 도입함으로써 기존 연구의 한계를 보완한다. 프로토타입 구현과 테스트를 통해 제안 시스템의 기능적 유효성과 실용성을 입증했다.

Abstract

Conventional centralized donation systems operate on the assumption of trust in the managing organization. However, this structural dependency often leads to a lack of transparency in donation records and fund execution, resulting in risks of embezzlement and fraud. To address these issues, various studies have proposed blockchain-based donation systems leveraging immutability, transparency, and traceability. Nevertheless, most of these approaches either lack beneficiary eligibility verification mechanisms or rely heavily on off-chain data, which limits their trustworthiness and efficiency. In this paper, we propose a method that utilizes Decentralized Identifiers (DIDs) based on Hyperledger Indy in conjunction with the public Ethereum blockchain to enable on-chain verification of beneficiary eligibility. In particular, we introduce a mechanism for registering and validating DID-Ethereum account binding information within smart contracts, thereby overcoming the limitations of prior research. A prototype implementation and evaluation demonstrate the functional validity and practical feasibility of the proposed system.

Keywords

blockchain, ethereum, self-sovereign identity, Hyperledger Indy, ACA-Py

* 경기대학교 SW안전보안학과 석사과정
- ORCID: https://orcid.org/0009-0000-5006-3243
** 경기대학교 컴퓨터과학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0001-6341-580X

· Received: Jun. 17, 2025, Revised: Sep. 09, 2025, Accepted: Sep. 12, 2025
· Corresponding Author: Heeyoul Kim
Dept. of AI Computer science, kyonggi University, 154-42, Gwanggyosan-ro, Korea
Tel.: +82-31-249-9607, Email: heeyoul.kim@kgu.ac.kr

Ⅰ. 서 론

전통적인 중앙집중형 기부 시스템에서는 운영 단체가 전권을 가지고 기부 캠페인의 기획·모금·집행 전 과정을 독점적으로 관리한다. 이러한 운영 방식은 투명성을 저해하며 기부 내역과 집행 과정을 외부에서 검증하기 어렵게 만든다. 그 결과 단체 내 불법 횡령과 사기 사례가 발생하여 기부금이 본래 목적과 다르게 사용되는 심각한 문제로 이어진다. 기빙코리아(2022)의 자료에 따르면, 기부하지 않는 주요 이유로 응답자의 41.8%가 기부처에 대한 불신을 꼽았다[1].

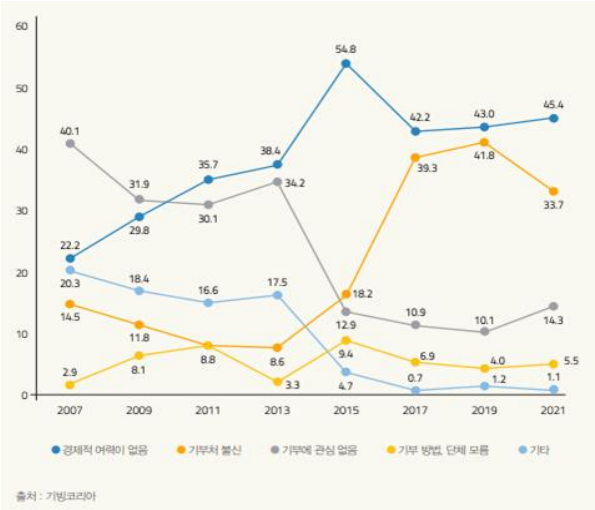


그림 1. 기부하지 않은 이유 그래프 (기빙 코리아)
Fig. 1. Reasons for not donating (Giving Korea)

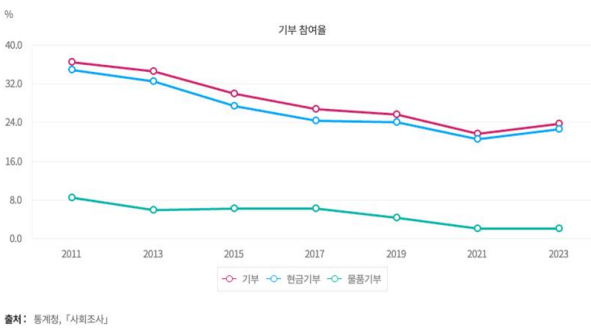


그림 2. 기부 참여율 그래프 (통계청)
Fig. 2. Donation participation rates (Statistics Korea)

또한 통계청 사회조사 결과에 따르면, 13세 이상 인구 중 지난 1년간 현금 또는 물품을 기부한 경험이 있는 비율은 2011년부터 지속적으로 감소하여 2023년까지 하락세를 보인다[2].

이러한 신뢰 문제를 해결하기 위한 대안으로 블록체인 기술을 활용한 기부 시스템 연구가 활발히 진행됐다. 기부금 거래 내역을 블록체인에 기록함으로써 투명성과 정당성을 확보할 수 있게 되었으나, 기존 접근 방식은 기부금의 흐름 관리에 국한되어 수혜자 자격 검증을 위한 체계적인 메커니즘이 부족하다는 한계를 지닌다.

본 논문의 핵심 기여는 정부 발급 검증 가능한 증명서(VC, Verifiable Credential)을 활용하여 수혜자의 자격을 온체인 상에서 검증하는 방법을 제시하는 것이다. 이를 통해 자격이 확인된 사용자만 기부금 캠페인의 생성·모금·집행 활동에 참여할 수 있도록 설계된 자기주권신원 인증(SSI, Self-Sovereign Identity) 기반 기부 플랫폼 ‘DIDonate’를 제안한다.

제안 시스템은 세 가지 핵심 구성 요소로 구성된다. 첫째, 공개형 이더리움 블록체인은 캠페인 정보와 분산 식별자 DID(DID, Decentralized Identifier) 정보를 온체인에 기록하여 불변성과 투명성을 보장한다. 둘째, Hyperledger Aries의 ACA-Py 에이전트는 DID 생성 및 VC·VP 관리를 수행한다. 셋째, 스마트 컨트랙트는 검증된 사용자만 캠페인 기능을 호출할 수 있도록 제어한다. 세 요소가 유기적으로 연동되어 수혜 자격 검증부터 캠페인 생성, 모금 집행에 이르는 전 과정을 완전한 투명성 아래 운영할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구에서 활용한 관련 기술을 설명한다. 3장에서는 기존 블록체인 기반 기부 시스템을 분석하고 그 한계점을 제시한다. 4장에서는 제안 시스템의 아키텍처와 핵심 설계 및 구현 방법에 관해 서술한다. 5장에서는 네 가지 시나리오 기반의 실험을 통해 시스템 유효성을 입증한다. 6장에서는 연구 결과를 정리하고 향후 연구 방향을 제시한다.

Ⅱ. 관련 기술

2.1 이더리움 블록체인

블록체인 기술은 분산 원장 저장 기술로, 블록체인 네트워크상에서 발생한 모든 거래 내역을 블록

단위로 기록하고 네트워크 참여자들의 검증과 합의를 통해 원장에 저장된다[3]. 블록체인 네트워크는 공개형(Public)과 비공개형(Private)으로 구분된다. 공개형 블록체인은 누구나 네트워크에 참여하여 저장된 데이터에 접근할 수 있으며, 블록 생성 권한에도 참여할 수 있다.

공개형 블록체인 중 이더리움 블록체인(Ethereum blockchain)은 스마트 컨트랙트(Smart contract) 기능을 제공한다[4]. 스마트 컨트랙트는 전용 프로그래밍 언어인 솔리디티(Solidity)로 작성되어 블록체인에 배포되며, 설정된 프로그램 조건이 충족되면 제3자의 개입 없이 사전에 정의된 규칙에 따라 자동으로 실행된다. 이더리움의 스마트 컨트랙트를 기반으로 개발되는 애플리케이션을 탈중앙화 애플리케이션(DApp, Decentralized Application)이라고 하며, 탈중앙화 금융(DeFi), 게임, 공공 서비스 등 다양한 분야에서 활용되고 있다.

또한 이더리움은 초기에는 작업 증명(PoW) 기반의 합의 알고리즘을 사용했으나, 현재는 지분 증명(PoS) 방식으로 전환했다. 기존 PoW 대비 에너지 소비를 줄이면서도 네트워크의 보안성과 신뢰성을 유지할 수 있는 장점이 있다.

2.2 하이퍼레저 인디

하이퍼레저 인디(Hyperledger Indy)는 리눅스 재단의 블록체인 프로젝트 중 하나로, 분산 신원 인증을 지원하는 오픈 소스 프로젝트이다[5]. 인디는 분산 신원 관리를 위해 특화된 공개형 퍼미션드(Public-Permissioned) 분산 원장으로, 분산 식별자(DID), 분산 식별자 문서(DID document), 자격 증명 스키마(Credential schema), 자격 증명 정의(Credential definition) 등이 저장되고, 이를 기반으로 분산 신원 인증에 필요한 핵심 기능을 제공한다. 또한 합의 알고리즘으로 RBFT(Redundant Byzantine Fault Tolerance)를 채택하여 원장의 안정성과 무결성을 보장한다.

표 1은 DID의 구성 예를 보여준다. did 접두어로 시작하여, DID가 생성된 블록체인 네트워크 메소드 이름과 중복되지 않는 고유 문자열 값으로 구성된다.

표 1. 분산 식별자 구조
Table 1. Decentralized identifier structure

Did	Method	Specific identifier
did	indy	123456789abcdef

DID Document는 DID와 관련된 메타데이터를 담은 문서로, DID의 소유권을 증명할 수 있는 공개키가 포함되어 블록체인에 저장된다. 검증자는 블록체인에 저장된 DID Document 내 공개 키를 사용하여 해당 DID 소유자가 생성한 디지털 서명의 유효성을 확인하여 해당 소유자의 신원을 암호학적으로 검증할 수 있다.

2.3 하이퍼레저 에어리즈

하이퍼레저 에어리즈(Hyperledger Aries)는 인디 분산 원장을 활용하여 탈중앙화 신원 인증 메커니즘을 지원하는 프로토콜을 제공한다[6]. 에어리즈는 에이전트 간의 안전한 메시징(DIDComm), 자격 증명 교환 등 다양한 상호작용 방식을 정의하며, 원장과 애플리케이션 계층을 연결하는 미들웨어 역할을 수행한다. W3C의 DID 및 VC 표준을 지원하여 다양한 블록체인 네트워크와 서비스 환경 간 상호운용성을 보장한다.

ACA-Py(Aries Cloud Agent – Python)는 에어리즈 프로토콜 기반으로 구현된 대표적인 에이전트 소프트웨어이다. ACA-Py는 에이전트 간 메시지 교환, DID 생성 및 관리, 개인 키와 신원 정보를 안전하게 저장할 수 있는 Wallet 기능을 포함한다. 또한, VC 발급 및 관리, 검증할 수 있는 프레젠테이션(VP, Verifiable Presentation) 생성 및 검증 기능을 지원함으로써 분산 신원 인증을 수행한다[7].

III. 선행 연구 비교 및 한계

표 2는 중앙화된 시스템의 한계를 극복하기 위해 블록체인 기술을 도입한 주요 기부 시스템들을 정리한 표이다.

표 2. 기존 블록체인 기부 시스템 분석
Table 2. Analysis of existing blockchain based donation systems

Classification	N. S. Sirisha et al. (2019)	A. Almaghrabi et al. (2022)	A. Singh et al. (2020)	L. Trotter et al. (2020)
Blockchain	Public	Public	Public	Public
Participants	Donor NGO retailer government	Donor beneficiary trustee	Donor beneficiary NGO government	Donor beneficiary NGO data -provider
Smart contract main functions	Create donation request (Campagin)			
	Manage bidding	Approve	Approve	Escrow
	Activate	Reject	Reject	Refund
Verification and approval mechanism	Government review	Trustee review	Government review	Oracle review

N. S. Sirisha et al.[8]은 퍼블릭 이더리움 기반으로 수혜 단체, 기부자, 입찰 참여 소매업체, 정부가 참여한다. 수혜 단체는 필요한 자원과 금액을 템플릿 형태로 제시하고, 소매업체는 입찰에 참여한다. 정부는 입찰 요청의 진위를 오프체인에서 검토한 뒤 스마트 컨트랙트를 활성화하여 기부가 실행되도록 승인한다.

A. Almaghrabi et al.[9]은 이더리움 블록체인 기반의 기부 추적 프레임워크 연구이다. 기부자, 수혜자, 신탁자 세 주체가 참여한다. 수혜자는 자신의 지원 사유(case)를 생성하여 블록체인 네트워크에 트랜잭션으로 기록하고, 신탁자가 수혜자의 case를 심사한 후 승인 여부를 결정한다.

A. Singh et al.[10]은 이더리움 블록체인 기반의 기부 추적 시스템을 다룬 연구이다. 이 시스템은 기부자, NGO, 수혜자, 정부가 네 주체가 참여하며, NGO가 기부 요건(Requirement)을 생성하면 정부가 이를 승인하거나 거절하는 구조를 갖는다.

L. Trotter et al.[11]는 퍼블릭 이더리움 기반으로 기부자, 수혜자, NGO, 데이터 제공자의 네 주체가 참여한다. NGO가 기부 요청 템플릿을 발행한 후, 기부자는 해당 템플릿에 금액과 이벤트 기반 조건을 설정하고 에스크로에 예치한다. 데이터 제공자는 실시간으로 조건 충족 여부를 검증하고 스마트컨트랙트가 조건 만족 시 자동으로 수혜자에게 기부금을 분배한다. 만약 지정 기간 내에 조건이 충족되지 않으면, 남은 잔액은 기부자에게 자동으로 반환된다.

이들 연구는 공통적으로 수혜자 자격 검증 절차를 구체화하지 못했고, 검증 과정이 오프체인 행정 심사에 의존함으로써 기준이 불투명하며 처리 속도가 지연되는 구조적 한계를 갖는다. 이러한 제약은 부정 수혜를 사전에 방지하지 못하고, 기부금 집행 과정의 신뢰성과 효율성을 저해한다.

Ⅳ. 제안 시스템

4.1 제안 시스템의 구조와 참여자 역할

본 장에서는 제안하는 기부 시스템의 구조와 참여자들의 역할을 설명한다. 제안 시스템은 수혜자가 정부 발급 검증 가능한 자격 증명(VC)을 활용하여 DID 기반 분산 신원 인증을 통해 자격을 검증받고, 안전하게 기부금 모금 활동에 참여할 수 있도록 설계되었다.

DID와 이더리움 블록체인을 도입함으로써 온체인 상에서 자격 확인 절차를 지원하고 검증 과정을 투명하게 관리할 수 있다. 그림 3은 제안 시스템의 전체 구조를 나타낸다.

모든 참여 주체는 인디 분산 원장에 DID와 DID Document가 등록되어 있으며, 각자의 ACA-Py 에이전트를 통해 신원 정보를 관리할 수 있다. 시스템 참여자들의 역할은 다음과 같다.

정부(Issuer): 정부는 공신력 있는 발급 기관으로서 수혜자의 자격 요건을 심사한 뒤, 표 3에 정의된 credentialSubject 속성을 포함한 기초생활 수급자 VC를 발행하는 주체이다. VC에는 정부의 DID, 디지털 서명이 함께 기록된다.

수혜자(Holder) : 수혜자는 정부가 발행한 VC를 소유하고, 이를 VP로 가공하여 검증자에게 제출하고 검증을 요청한다. 검증이 완료되면 검증자로부터 받은 디지털 서명을 활용해 DIDAttestation 스마트 컨트랙트에 수혜자의 DID와 이더리움 계정 주소를 매핑하여 온체인에 등록하며, 이후 자신의 수혜 목적에 맞는 기부금 모집 캠페인을 생성하여 기부금을 모금한다.

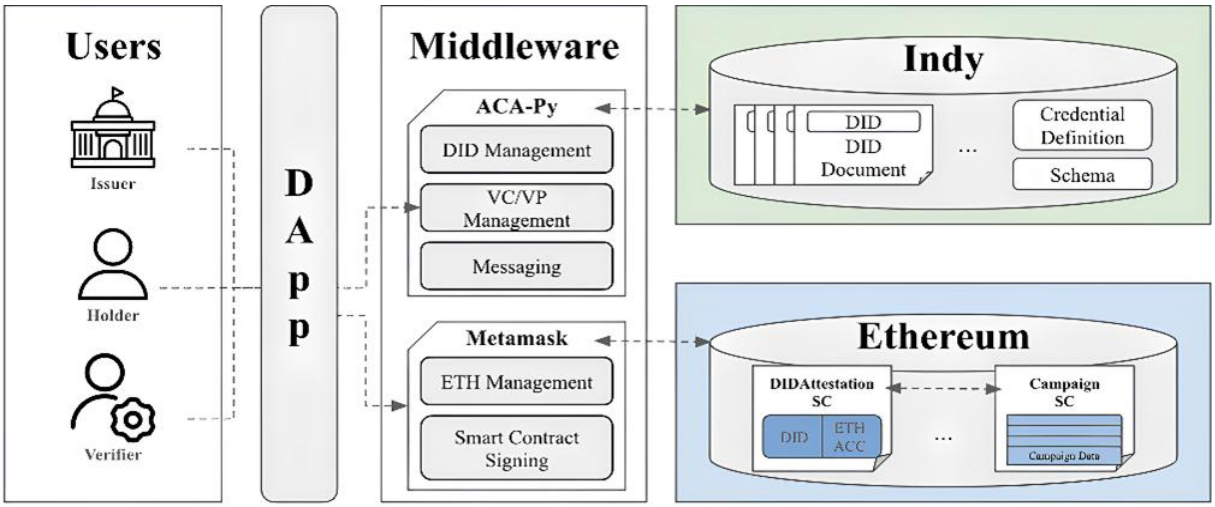


그림 3. 제안 시스템 구조도
Fig. 3. Proposed system architecture

표 3. VC의 CredentialSubject 주요 속성
Table 3. Key Attributes of the VC credentialSubject

Attribute	Description
name	Beneficiary's full name
birthDate	Beneficiary's date of birth
address	Address on resident registration
headOfHouseholdname	Head of Household's name
relationshipToHeadOfHousehold	Relationship to head of household
beneficiaryType	Beneficiary type
issuanceDate	VC issuance date and time
expirationDate	VC expiration date and time

검증자(Verifier) : DIDonate 기부 시스템의 관리자로서, 수혜자가 제출한 VP와 함께 이더리움 공개키 및 DID를 수신한다. 검증자는 VP에 포함된 정부 발급 VC에 담긴 디지털 서명 유효성과 발행일(issuanceDate), 만료일(expirationDate)를 확인하여 검증을 완료한다. 검증이 성공하면, 검증자의 개인 키로 수혜자의 DID와 Ethereum Account 결합한 메시지에 디지털 서명을 생성하여 수혜자에게 반환한다.

4.2 제안 시스템의 스마트 컨트랙트

제안 시스템은 두 가지 스마트 컨트랙트로 구성되어 있다. DIDAttestation 스마트 컨트랙트와 Campaign 스마트 컨트랙트이다. DIDAttestation 스마트 컨트랙트는 검증자로부터 발급된 디지털 서명의 진위를 확인하고, 유효한 서명만 수혜자의 DID와 이더리움 계정 주소를 온체인에 매핑하여 등록하는 역할을 수행한다. 주요 메소드는 다음과 같다.

서명 검증 메소드 : 수혜자의 DID와 이더리움 계정 주소를 결합해 keccak256 해시를 생성하고 이를 EIP-191 표준으로 래핑한 후, 전달된 서명으로 ECDSA.recover를 통해 복원된 서명자 주소가 스마트 컨트랙트에 등록된 검증자의 주소와 일치하는지 확인함으로써, 유효성을 검증한다[12].

수혜자 정보 등록 메소드 : ACA-Py 에이전트와 메타마스크 연동을 통해 수혜자가 검증자로부터 받은 디지털 서명과 수혜자의 DID를 입력값으로 제출하여 온체인에 등록하는 기능을 수행한다. didToAddress 매핑에서 동일한 DID와 Ethereum 계정이 이미 등록되어 있는지 확인한다. 이후 verifyAttestation() 메소드를 호출하여, 제출된 서명이 컨트랙트에 등록된 검증자로부터 발급된 것인지와 서명 대상 주소가 현재 트랜잭션 발신자(msg.sender)와 일치하는지 검증한다. 검증이 성공하면 didToAddress 매핑에 해당 DID와 발신자의 Ethereum 주소를 저장한다. 등록된 매핑은 getDIDHolder(did) 메소드를 통해 조회할 수 있으며, Campaign 컨트랙트는 이를 참조하여 검증된 수혜자 계정만이 캠페인 생성 메소드를 호출할 수 있게 권한을 제한한다.

캠페인 생성 메소드 : 검증된 수혜자는 새로운 기부 캠페인을 등록하는 기능을 수행한다. 표 4와 같이 기부 캠페인의 제목, 설명, 시작 및 종료 시점, 목표 금액 등 핵심 정보를 입력받아 블록체인 네트워크상에 생성한다.

표 4. 캠페인 데이터 구조체
Table 4. Campaign data struct

Filed name	Description	Type
creator	creator's ethereum account	address
title	campaign title	string
description	campaign detailed description	string
goalAmount	target amount (wei)	uint256
startDate	campaign start date	uint256
endDate	campaign end date	uint256
usagePlan	description of planned use	string
totalDonations	amount raised	uint256
ended	campaign status	bool

캠페인 집행 메소드 : 캠페인에 모인 기부금을 정해진 조건에 따라 자동으로 집행하는 기능을 담당한다. 집행 조건은 목표 금액(goalAmount) 도달이나 캠페인 종료 시점(endDate) 도달이다. 스마트 컨트랙트 내 로직에 따라 기부금이 검증된 수혜자에게 분배된다.

4.3 ECDSA 서명 기반 DID-Ethereum 계정 바인딩 절차

다음은 분산 신원(DID)과 이더리움 계정을 안전하게 연결하기 위해 제안된 전체 검증 절차를 그림 4와 그림 5를 통해 시각적으로 설명한다. 그림 4는 제안 시스템에서 Indy 분산 원장 기반 신원 검증과 Ethereum 온체인 계정 바인딩이 순차적으로 수행되는 과정을 나타낸다.

(i) 수혜자는 정부 기관으로부터 발급받은 VC를 기반으로 VP를 생성하고 자신의 Ethereum 계정 주소와 함께 검증자에게 제출한다.

(ii) 검증자는 Indy 분산 원장에 저장된 스키마, 크리덴셜 정의, 발급자의 DID 문서 등을 조회하여 VC의 발급자 서명, 발급 시간, 만료 시간, 요청된 속성과 조건 충족 여부를 온체인에서 검증한다.

(iii) 검증이 성공하면 검증자는 수혜자의 DID와 Ethereum 계정을 결합한 메시지를 해싱한 뒤, 검증자의 개인 키로 ECDSA 서명을 생성하여 수혜자에게 전달한다.

(iv) 수혜자는 해당 서명을 Ethereum 네트워크의 DIDAttestation 컨트랙트에 제출한다. 컨트랙트는 제출된 DID, Ethereum 계정 주소, 서명 데이터를 기반으로 동일한 해시를 재구성하고, ECDSA.recover() 함수를 통해 서명자의 주소를 복구하여 사전에 등록된 검증자 주소와 일치하는지 확인한다. 검증이 성공하면 Indy 온체인에서 신원 검증 결과를 Ethereum 온체인에 영속화하며, 해당 계정에 캠페인 생성 권한을 부여한다.

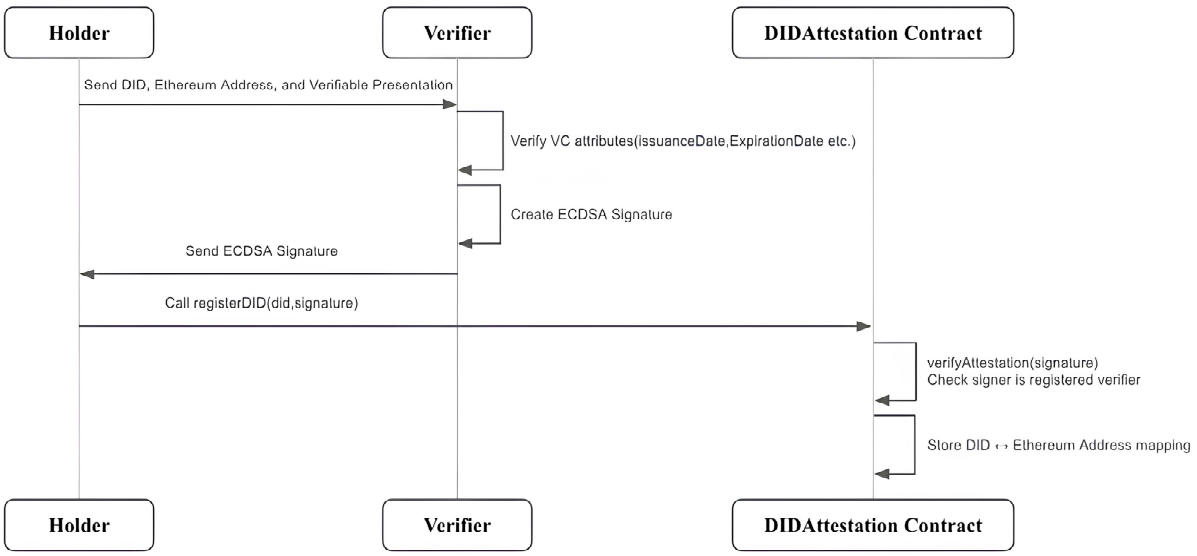


그림 4. DID-Ethereum account 바인딩 시퀀스 다이어그램
Fig. 4. Sequence diagram of DID-Ethereum account binding

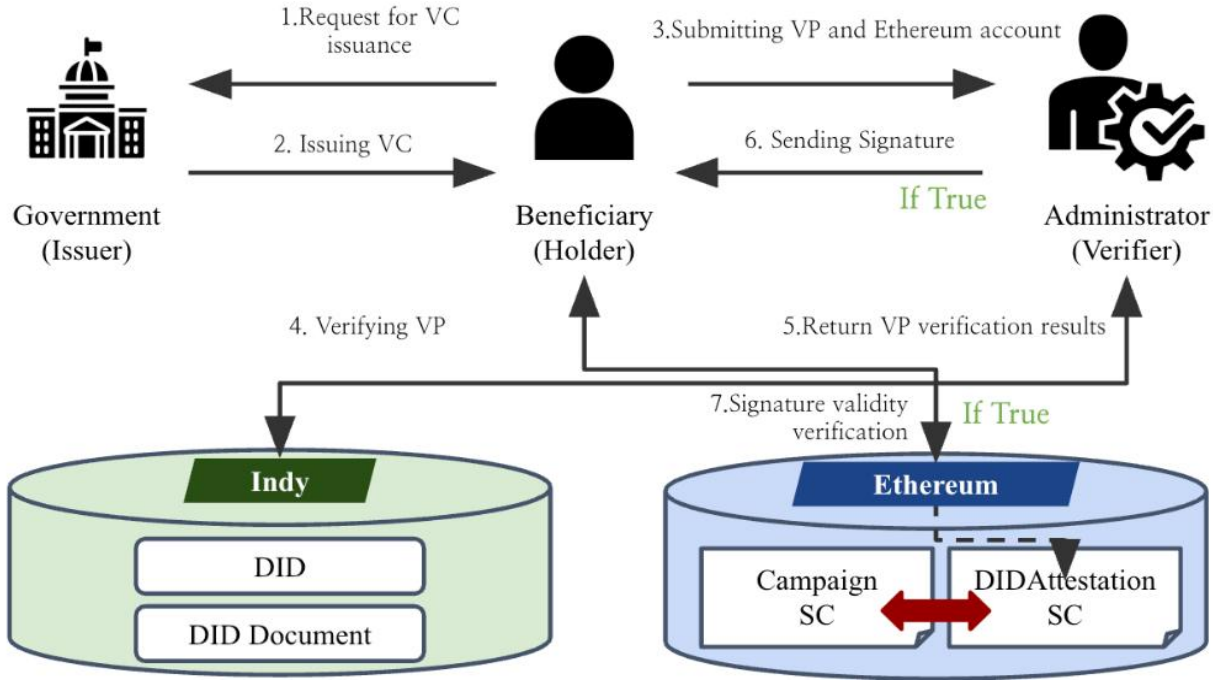


그림 5. DID-Ethereum 계정 바인딩 서명 기반 검증 흐름도
Fig. 5. DID-Ethereum account binding signarue-based verification flowchart

그림 5는 DID-Ethereum 계정 바인딩 절차를 포함하여, 해당 계정이 캠페인 생성 권한을 획득하고 이를 통해 새로운 캠페인을 개설하기까지의 전체 과정을 나타낸다. 수혜자의 DID와 Ethereum 계정이 매핑되어 DIDAttestation 컨트랙트에 저장된다. Campaign 컨트랙트는 새로운 캠페인 생성 요청 시 DIDAttestation을 조회하여 요청 계정이 등록된 계정인지 확인 후, 조건을 충족하는 경우에만 캠페인 생성을 허용한다.

제안된 검증 절차는 정확한 스마트 컨트랙트 배포자로부터의 서명의 진위 확인 및 부인방지, 전송 단계의 기밀성과 무결성, 온체인 불변성 특성을 활용하여 메시지 변조를 원천적으로 차단하고 송신자의 진위를 보증한다. 검증 결과를 영구히 보관함으로써 DID와 Ethereum Account 간의 위·변조 없는 안전한 바인딩을 제공한다.

V. 구 현

제안 시스템은 표 5에 정리된 개발 환경에서 프로토타입을 구현했다. 네 가지 시나리오를 통해 전 과정이 정상적으로 수행되었음을 확인했다.

표 5. 제안 시스템 구현 환경
Table 5. Proposed system implementation environment

Wallet	Metamask Extension v12.10.4
	Hyperledger Aries ACA-Py
Smart contract	Solidity v0.8.0
	Hardhat v2.22.19
Blockchain	Ethereum
	Hyperledger Indy
OS	Ubuntu 18.04.6 LTS

5.1 시나리오 검증

5.1.1 시나리오 1: 기초생활수급자 VC 발행

그림 6은 Issuer인 정부 기관이 기초생활수급자 자격 증명서(VC)를 발행하는 UI 화면이다. Issuer는 Indy 원장에 등록된 해당 증명서의 Schema와 Credential Definition을 기반으로 credentialSubject에 대한 속성값들을 정의한 뒤 VC를 발행한다. credentialSubject의 ACA-Py 에이전트와 Issuer의 에이전트 간 연결(Connection ID)을 통해 VC를 안전하게 전달 할 수 있다. Verifier는 블록체인상의 Schema ID와 Credential Definition ID를 참조하여 해당 VC의

진위와 유효성을 즉시 확인할 수 있다. 그림 7은 발급된 VC가 보관된 Holder의 ACA-Py 지갑에서 해당 VC를 조회했을 때의 화면을 나타낸다.

그림 6. 기초생활수급자 증명서 VC 발행 화면
Fig. 6. Basic livelihood security recipient certificate VC issuance screen

그림 7. Holder의 ACA-Py 지갑에 저장된 기초생활수급자 증명서 VC 조회 화면
Fig. 7. Basic livelihood security recipient certificate VC display in holder's ACA-Py wallet

5.1.2 시나리오 2: 수혜 자격 등록

그림 8은 기초생활수급자 증명서(VC)를 활용해 수혜 자격을 온체인에 등록하는 UI 화면이다. 해당 VC를 기반으로 Verifiable Presentation(VP)을 생성한 뒤 Verifier에 검증을 요청한다. Verifier는 요청받은 VP의 유효성을 검증한 뒤 서명 값을 요청자에게 반환한다. 수혜자는 반환된 서명 값을 스마트 컨트랙트에 제출하면, 스마트 컨트랙트가 이를 검증하고 유효할경우 DID와 Ethereum 주소를 매핑하여 온체인 상에 등록하고 캠페인 생성 권한을 부여한다. 그림 9는 성공적으로 처리된 트랜잭션 결과를 보여준다.

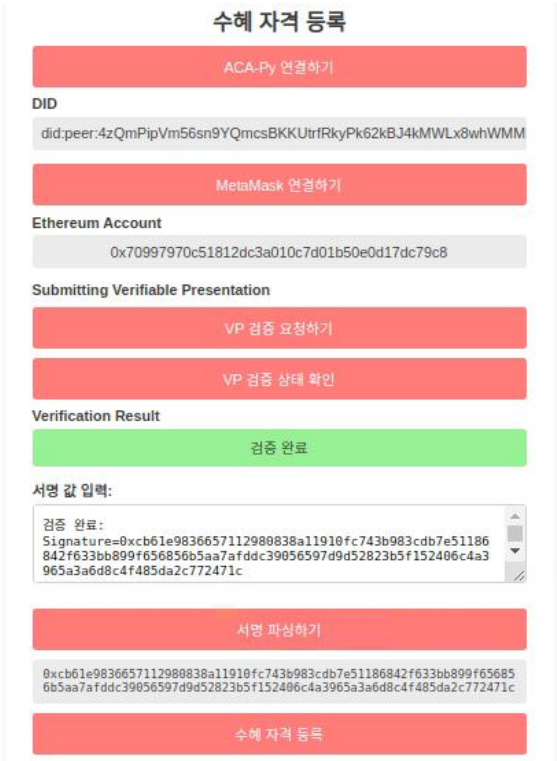


그림 8. 수혜 자격 등록 화면
Fig. 8. Beneficiary eligibility registration screen

그림 9. 수혜 자격 등록 트랜잭션 결과
Fig. 9. Beneficiary eligibility registration transaction result

5.1.3 시나리오 3: 캠페인 생성

그림 10은 수혜자가 캠페인을 생성하는 UI 화면을 나타낸다. 수혜자는 캠페인 제목, 캠페인에 대한 세부 설명, 목표 금액, 캠페인 시작일, 캠페인 종료일, 캠페인 모금액에 대한 사용 계획 필드를 작성한 후 Campaign 스마트 컨트랙트의 createCampagin 메소드를 호출하여 캠페인을 생성하고 온체인에 저장한다. 그림 11은 createCamapgin 메소드가 성공적으로 실행된 뒤 반환된 트랜잭션 결과 화면을 나타낸다.

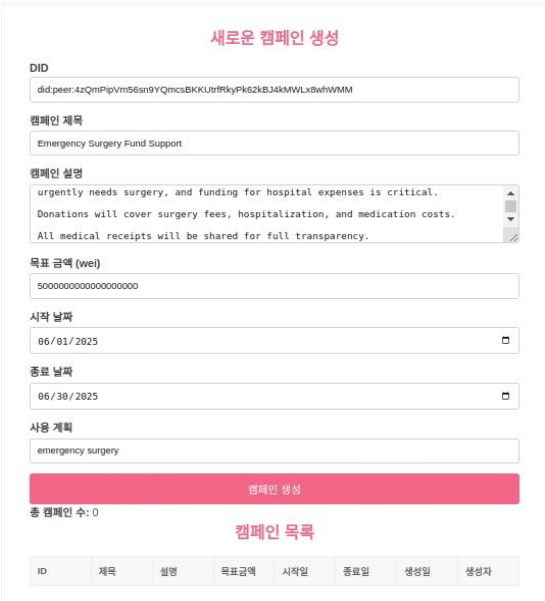


그림 10. 캠페인 생성 화면
Fig. 10. Campaign creation screen

```
net_version (3)
eth_blockNumber
eth_sendRawTransaction
  Contract call:       Campaign#createCampaign
  Transaction:         0x3ab0cdc93c61e9cd87aee988de2d0e6c372c15b408b97d4044628c2c523073d9
  From:                0x70997970c51812dc3a010c7d01b50e0d17dc79c8
  To:                  0xe7f1725e7734ce288f8367e1bb143e90bb3f0512
  Value:               0 ETH
  Gas used:            406973 of 416973
  Block #4:            0x87da35c5213910292c0f0915fb23196e2e306231e85f1ba7df84610df876e601
```

그림 11. 캠페인 생성 트랜잭션 결과
Fig. 11. Campaign creation transaction result

5.1.4 시나리오 4: 캠페인 기부

그림 12는 수혜 자격이 등록된 수혜자가 개설한 기부 캠페인을 조회하는 화면이다. 기부자는 캠페인에 대한 상세 내용을 확인한 후, 기부금을 입력하고 donate() 메소드를 호출하여 해당 캠페인에 기부금을 전송한다. 모금된 기부금은 캠페인의 목표 기간이 종료되거나 목표 금액이 달성되면 자동으로 캠페인 생성자에게 집행된다. 그림 13은 donate 메소드가 성공적으로 실행된 이후 반환된 트랜잭션 결과를 보여준다.

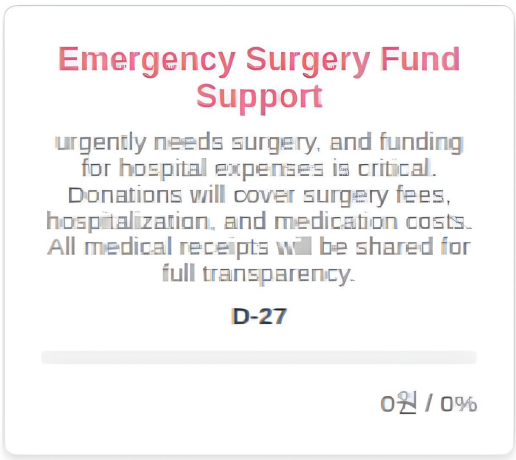


그림 12. 기부 캠페인 조회 화면
Fig. 12. Donation campaign viewing screen

```
eth_sendRawTransaction
  Contract call:       Campaign#donate
  Transaction:         0x60f1a49595bf682e9f0e4eae676d5dde36df3c808cba8fc0daf197fa161e4a44
  From:                0x9965507d1a55bcc2695c58ba16fb37d819b0a4dc
  To:                  0xe7f1725e7734ce288f8367e1bb143e90bb3f0512
  Value:               5. ETH
  Gas used:            184361 of 194361
  Block #5:            0x581d4cd59213cd807bc4be5bf76867b29dcea57c7f6442d9078bc3023e903b63
```

그림 13. 기부금 송금 트랜잭션 결과
Fig. 13. Donation transaction result

VI. 결론 및 향후 방향

본 연구는 수혜자의 자격을 투명하고 신뢰성 있게 검증하기 위해 분산 신원 인증과 공개형 이더리움 블록체인을 결합한 고신뢰성 기부 시스템을 제안했다. DIDAttestation과 Campaign 스마트 컨트랙트를 통해 수혜자 자격 검증과 기부금 집행 과정을 중간 개입자 없이 자동화하고, 데이터의 불변성과 투명성을 기반으로 신뢰할 수 있는 기부 생태계를 구현했다.

기존 연구 대비 본 연구의 차별성은 다음과 같다. 첫째, 기존 대부분의 블록체인 기반 기부 시스템은 수혜 자격 검증을 오프체인 데이터와 심사 절차에 의존하는 것과 달리, 본 연구는 하이퍼레저 인디(Hyperledger Indy) 기반의 Verifiable Credential/Presentation을 활용하여 자격 검증 전 과정을 온체인에서 수행했다. 둘째, ECDSA 서명 검

증 기반 DID-Ethereum 계정 바인딩 절차를 도입하여 검증된 수혜자만이 이더리움 네트워크 내에서 캠페인을 생성하고 집행할 수 있도록 권한을 제한한다. 불변 기록과 온체인 검증으로 수혜자 자격 정보의 위·변조 가능성을 차단하여 신뢰성을 강화하고, 기부금의 이동 경로 전체를 블록체인 원장에 기록되고 관리되어 기부자와 수혜자 모두 동일하게 확인 및 검증할 수 있는 투명성을 확보한다.

네 가지의 시나리오 기반 실험 결과, 제안 시스템이 설계된 기능적 요구사항을 안정적으로 동작하며, 수혜 자격 검증과 기부금 집행의 자동화를 통해 기존 시스템의 한계를 극복함을 확인했다.

본 연구는 분산 신원 인증과 공개형 이더리움 블록체인을 통해 기부 시스템의 투명성과 신뢰성을 확보하는 데 중점을 두었으나, 향후 연구에서는 영지식증명(Zero-Knowledge proof) 기술을 적용하여, 수혜자의 VC 항목을 영지식 방식으로 검증함으로써 필요한 속성만 증명하고 불필요한 개인정보는 전혀 노출하지 않는 방안을 제안한다. 또한, DID가 블록체인에 영구적으로 저장되어 발생할 수 있는 개인 프라이버시 문제를 방지하기 위해, 수혜자-검증자-스마트 컨트랙트 다자간의 ZKP 구조를 설계하여 연구를 고도화할 계획이다.

References

[1] Beautiful Fund Research Archive, "Reasons for Not Donating", https://research.beautifulfund.org/13875/. [accessed: Dec. 26, 2024]

[2] Statistics Korea, "Donation Participation Rate", Social Survey, https://www.index.go.kr/unity/potal/indicator/IndexInfo.do?cdNo=2&clasCd=10&idxCd=F0263. [accessed: May 02, 2025]

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", White paper, Oct. 2008. https://bitcoin.org/bitcoin.pdf. [accessed: May 02, 2025]

[4] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", 2014. https://ethereum.org/en/whitepaper/. [accessed: May 08, 2025]

[5] Hyperledger Foundation, "Hyperledger Indy Documentation", https://hyperledger-indy.readthedocs.io/en/latest/. [accessed: Jun. 05, 2025]

[6] Hyperledger Foundation, "Hyperledger Aries Repository", https://github.com/hyperledger/aries. [accessed: Jun. 05, 2025]

[7] OpenWallet Foundation, "acapy Repository", https://github.com/openwallet-foundation/acapy. [accessed: Jun. 05, 2025]

[8] N. S. Sirisha, T. Agarwal, and R. Monde, "Proposed solution for trackable donations using blockchain", Proc. Int. Conf. on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, pp. 1-5, Jan. 2019. https://doi.org/10.1109/ICNTE44896.2019.8946019.

[9] A. Almaghrabi and A. Alhogail, "Blockchain-based donations traceability framework", Journal of King Saud University - Computer and Information Sciences, Vol. 34, No. 10, pp. 9442-9454, Oct. 2022. https://doi.org/10.1016/j.jksuci.2022.09.021.

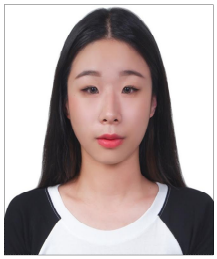
[10] A. Singh, R. Rajak, and H. Mistry, "Aid, charity and donation tracking system using blockchain", Proc. 4th Int. Conf. on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, pp. 457-462, Jun. 2020. https://doi.org/10.1109/ICOEI48184.2020.9143001.

[11] L. Trotter, M. Harding, and P. Shaw, "Smart donations: Event-driven conditional donations using smart contracts on the blockchain", Proc. 32nd Australian Conf. on Human-Computer Interaction, New York, United States, pp. 546-557, Dec. 2020. https://doi.org/10.1145/3441000.3441014.

[12] OpenZeppelin Contributors, "ECDSA.sol", OpenZeppelin Contracts, https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/utils/cryptography/ECDSA.sol. [accessed: May 08, 2025]

저자소개

최 희 민 (Heemin Choi)



2024년 2월 : 경기대학교
컴퓨터공학부(공학사)
2024년 3월 ~ 현재 : 경기대학교
SW안전보안학과 석사과정
관심분야 : 블록체인, 정보보호

김 희 열 (Heeyoul Kim)

2002년 2월 : 한국과학기술원
전산학과(공학석사)
2007년 2월 : 한국과학기술원
전산학과(공학박사)
2009년 3월 ~ 현재 : 경기대학교
컴퓨터공학부 교수
관심분야 : 정보보호, 블록체인