Check for updates

Journal of KIIT. Vol. 22, No. 9, pp. 133-144, Sep. 30, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.9.133

블록체인 기반 NFT 전자 헌혈 증서 관리 시스템

최희민*, 김희열**

A Blockchain-based NFT Blood Donation Certificate Management System

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.2020R1A6A1A03040583)

요 약

현재, 혈액원은 종이 형태의 헌혈 증서를 수혈의 증명 및 보상의 목적으로 혈액 기증자에게 제공한다. 그러나 물리적 헌혈 증서는 훼손 및 분실의 위험이 있으며, 재발급 시스템도 단 1회에 한정되어 있어 헌혈 증서의 영속성 문제를 해결하지 못한다. 이러한 문제를 해결하기 위해, 본 논문에서는 공개 블록체인 이더리움 네트워크 기반의 디지털 형태 NFT(Non-Fungible Token) 헌혈 증서 관리 시스템을 제안한다. 제안하는 시스템은 NFT 헌혈 증서를 발급함으로써 증서의 영속성을 보장하고, 쉽게 양도 및 관리할 수 있다. 제안 시스템의 주요 참여자는 혈액원, 혈액 기증자, 의료 기관으로 구성되며, 세 가지 시나리오를 통해 구현된 시스템의 정상적인 수행을 검증했다. 실험 결과, NFT 헌혈 증서의 발행, 양도, 폐기에 대한 전체 주기가 원활하게 작동함을 확인했다. 디지털 헌혈 증서를 통해 헌혈 증서의 관리 효율성을 높이고, 헌혈 증서의 활용률을 크게 향상할 수 있다.

Abstract

Currently, blood centers issue physical donation certificates to blood donors as proof of donation and for reward purposes. However, physical certificates are prone to damage and loss, and the reissue system is limited to only one instance, failing to address the issue of certificate permanence. To solve this problem, this paper proposes a digital donation certificate management system based on Non-Fungible Tokens(NFTs) using the public Ethereum blockchain network. The proposed system guarantees the permanence of certificates by issuing NFT donation certificates, making them easy to transfer and manage. The primary participants in the system are blood centers, blood donors, and medical institutions, and the system's functionality was verified through three different scenarios. Experimental results confirm the smooth operation of the full cycle of NFT donation certificate issuance, transfer, and disposal. The digital donation certificates enhance the efficiency of certificate management and significantly increase their utilization.

Keywords
blockchain, blood donation certificate, ethereum, non-fungible token

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

· Received: Apr. 29, 2024, Revised: Sep. 19, 2024, Accepted: Sep. 22, 2024
· 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

1970년대, 매혈 체제에서 무상헌혈 체제로 전환하고 지속적인 헌혈자 수를 유치하기 위하여 헌혈 보상의 대가로 헌혈 증서 제도가 도입되었다[1]. 종이 형태로 지급되는 헌혈 증서를 의료기관에 제출할 시 무상으로 수혈 혜택을 받을 수 있다. 그러나 대한적십자사의 '헌혈환급적립금 제도 통계'에 따르면, 전체 발급 총량 대비 사용률이 12.7%에 불과하며[2], 사용되지 않은 헌혈환급적립금 누적액이 500억을 넘어선 것으로 집계되었다[3]. 이와 같이 낮은 사용률의 원인은 재발급 시스템이 구축되지 않았기 때문이다. 헌혈 증서를 훼손하거나 분실할 경우 이를 대체할 방법이 없어, 헌혈 증서의 활용이 제한되었다.

해당 문제를 해결하기 위해서 헌혈 증서 재발급 시스템 구축과 디지털 헌혈 증서 시스템 개발의 필요성이 제기되었다. 혈액관리법을 개정하여 2022년 9월 24일 이후부터 발급받은 헌혈 증서에만 재발급 서비스를 받을 수 있게 되었다[4]. 또한 대한적십자사 혈액관리본부는 자체 애플리케이션 '레드커넥트'를 출시하였다[5]. 이 애플리케이션을 통해 헌혈 증서 발급 내역 조회와 재발급 신청 서비스를 이용할 수 있지만, 재발급은 단 1회만 가능하며, 2022년 9월 23일 이전에 발급된 헌혈 증서는 재발급 대상에서 제외된다. 또한, 재발행된 헌혈 증서는 여전히 종이 형태로 발급되어 영구적인 보존이 어렵다는 문제점이 지속되고 있다.

현물 증서의 영속성 문제는 블록체인(Blockchain) 기술의 도입으로 해결할 수 있다. 블록체인은 한 번 기록된 데이터를 변경할 수 없기 때문에 데이터의 불변성과 신뢰성을 제공하며, 데이터의 투명성과 보안성을 강화한다. 또한, 스마트 컨트랙트 기술을 통해 자동화된 기능을 수행할 수 있다. 블록체인 기술의 이러한 특성을 활용한 사례로 블록체인 기반 기부 시스템에 대한 연구가 있다. H. Saleh et al.[6]는 기부금 흐름을 투명하게 보장하는 모델을 제안하였다. 모든 네트워크 참여자는 기부금의 흐름을 공개적으로 확인할 수 있으며, 중간 단계에서의 개입 및 위조를 방지할 수 있다. B. Hu et al.[7]는 기부금 흐름 공개 및 스마트 컨트랙트 기능을 통해 비정부기관이 개설한 캠페인을 정부 기관이 승인 또는 거절할 수 있는 모델을 제안하였다. A. Almaghrabi et al.[8]는 이더리움 블록체인 기반 기부 추적 프레임워크(BBDT)를 제안하였다. 스마트 컨트랙트의 다양한 기능을 활용하여 수혜자가 캠페인을 생성할 경우, 관리자에 의해 승인 또는 거절 단계를 거치며, 스마트 컨트랙트의 withdraw 함수를 통해 잉여 금액을 환불받을 수 있다. A. Singh et al.[9]는 스마트 컨트랙트를 사용하여 기부금을 에스크로 형태로 보관한 후 관리자의 승인 또는 거절 판단을 거쳐 기부금을 집행하는 모델을 제안하였다.

블록체인 기반 기부 플랫폼과 같이 블록체인 기술을 활용하면 헌혈 증서의 발급 및 소유자 이전 내역을 변조 불가능한 형태로 기록할 수 있어, 증서의 영구적인 보존과 투명성을 보장할 수 있다. 다음은 물리적 헌혈 증서의 영속성 문제를 해결하기 위해 블록체인 기술을 활용한 헌혈 증서 연구 사례이다. 변재형 et al. 는 블록체인 기반 분산 신원 인증 기술 DID(Decentralized Identity)를 활용한 프라이빗 블록체인 하이퍼레저 패브릭 기반의 전자 헌혈증서비스를 제안하였다[10]. 디지털 헌혈 증서 발급 및 증서 기부 기능을 제공하지만, 발급 단계에만 중점을 두어 다양한 기능적 요소에 대한 부족으로 한계가 있다. 유안지 et al. 는 퍼블릭 블록체인 이더리움 기반의 전자 혈액 관리 시스템을 제안하였다[11]. 헌혈부터 수혈까지 모든 혈액 유통 과정을 블록체인 원장에 기록하는 방식이지만, 혈액 유통에 중점을 두고 있어 실제 헌혈 증서 사용률을 높이기 어려운 문제가 있다.

이와 같은 연구의 한계점으로 인해, 헌혈 증서가 발급된 이후에도 다양한 기능들을 제공함으로써 헌혈 증서의 유용성과 활용을 증진하는 연구가 필요하다.

본 논문에서는 공개 블록체인 이더리움을 기반으로 하는 새로운 헌혈 증서 관리 시스템을 제안한다. 제안된 시스템은 헌혈 증서를 NFT(Non-Fungible Token)로 발행하여 블록체인 네트워크에 영구적으로 기록함으로써, 헌혈 증서의 훼손 및 분실 문제를 완전히 해결한다. NFT로 발행된 헌혈 증서에 고유성과 검증 가능성을 부여하여 각 증서의 진위를 쉽게 확인할 수 있으며, 투명하고 안전한 소유권 양도 및 이전을 보장한다.

제안된 시스템은 헌혈 증서의 영구적 보존과 즉각적 접근성을 제공하며, 헌혈 증서의 활용도를 크게 향상하는데 기여한다.

본 논문의 구성은 2장에서 제안 시스템과 관련한 배경 기술에 관해 기술하고, 3장에서는 제안하는 블록체인 NFT 헌혈 증서 시스템을 상세 설명한다. 4장에서는 구현 및 시나리오 검증을 기술한다. 마지막 5장에서 결론을 맺는다.

II. 배경 기술

2.1 블록체인

2008년, 익명의 개발자 나카모토 사토시(Satoshi Nakamoto)에 의해 P2P 네트워크 기반 전자 현금 결제 시스템인 비트코인(Bitcoin)이 제안되었다[12]. 비트코인은 최초의 암호화폐(Cryptocurrency)로 블록체인 기술 기반으로 동작한다. 블록체인은 데이터를 블록 단위 형태로 저장하고 블록체인 네트워크를 구성하는 모든 노드가 동일한 원장(Ledger)을 분산해 저장하는 기술이다[13]. 각 블록은 머리(Header)와 몸통(Body)으로 구성되어 있고, 머리에는 블록의 고유 정부가 저장되어 있고, 몸통에는 거래 정보가 저장되어 있다. 상세한 블록의 구조는 다음 그림 1과 같다. 각 블록은 고유한 해시값과 이전 블록의 해시값을 가지고 있어 이를 통해 서로 체인 구조로 연결된다. 해시값을 통해 이전 블록과 연결되기 때문에, 악의적인 공격자가 블록체인의 데이터를 위변조하려면 그 이후의 모든 블록도 변경해야 하고, 블록체인 네트워크에 있는 모든 노드의 원장 사본들도 변경해야 한다.

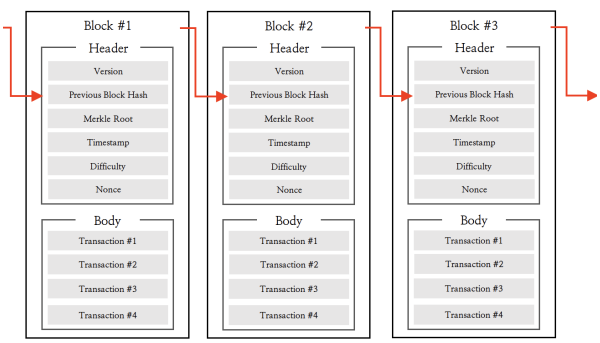


그림 1. 블록체인 구조
Fig. 1. Blockchain structure

이는 사실상 불가능하기 때문에 블록체인을 불변성과 무결성을 갖는다.

블록체인의 합의(Consensus)는 블록체인 네트워크의 모든 참여자 간 단일 원장을 기록하기 위해서 통일된 의사결정을 하기 위한 메커니즘이다. 새로운 블록이 생성되면 블록의 유효성을 검증하고 다수결의 합의에 도달해야 블록을 체인에 추가한다. 이에 사용되는 알고리즘이 합의 알고리즘(Consensus Algorithm)이다. 합의 알고리즘의 종류는 작업 증명 방식(PoW, Proof of Work), 지분 증명 방식(PoS, Proof of Stake), 위임지분증명(DPoS, Delegated Proof of Stake) 등이 있다. 작업 증명 방식은 블록의 해시값을 찾는 과정을 컴퓨팅 파워를 통해 무수히 반복함으로써 해당 작업에 참여했다는 것을 증명하는 방식이다[14]. 지분 증명 방식은 해당 블록체인의 암호화폐를 보유하고 있는 지분율에 따라 의사결정 권한을 주는 방식이다[15]. 위임 지분 증명 방식은 암호화폐 소유자들이 각자의 지분율에 따라 투표권을 행사하여 자신들의 대표자를 선정하고, 대표자들 간의 합의를 통해 의사결정을 내리는 방식이다[16].

블록체인 네트워크의 종류는 크게 두 가지로 구분된다. 공개형 블록체인(Public), 비공개 형 블록체인(Private)가 있다. 공개형 블록체인은 네트워크가 완전히 개방되어 있어 누구나 참여할 수 있는 형태로, 비트코인과 이더리움이 대표적이다. 비공개 블록체인은 소수의 허가 받은 참여자들만이 네트워크에 참여할 수 있으며, 주로 특정 조직이나 기업 내부에서 사용된다. 대표적으로 Hyperledger Fabric이 있다.

본 연구에서는 이더리움 네트워크를 채택하였다. 공개 네트워크이기 때문에, 일반 사용자가 쉽게 참여할 수 있으며, 스마트 컨트랙트 기능을 지원하여 분산 애플리케이션(DApp, Decentralized Application)을 개발할 수 있는 환경을 제공하기 때문이다.

2.2 스마트 컨트랙트(Smart contract)

이더리움은 1세대 블록체인 비트코인의 한계점을 극복하기 위해 스마트 계약 기술을 도입했다[17]. 스마트 계약은 블록체인에서 작동하는 프로그래밍 언어(Solidity)로 작성된 디지털 계약서이다.

중앙 서버 없이 모든 계약 조건이 충족되면 자동으로 계약 내용이 이행되도록 하는 기술이다.

스마트 컨트랙트 작동 방식은 다음과 같다. 먼저, 솔리디티 언어로 작성된 컨트랙트를 컴파일(Compile)하여 바이트 코드(Byte code) 형태로 변환하고, 이와 함께 ABI(Application Binary Interface)를 생성한다. 이후, 컴파일된 스마트 컨트랙트를 배포하는 트랜잭션을 생성하여 이더리움 블록체인 네트워크상에 브로드캐스트한다. 브로드캐스트된 컨트랙트 배포 트랜잭션이 블록에 포함되어 채굴되면, 스마트 컨트랙트는 내용은 암호화되어 블록체인 네트워크에 영구적으로 저장된다. 분산 원장에 기록되므로 계약 내용 위변조가 불가하며 누구든 계약의 상태를 검증할 수 있다.

또한 제 3의 중개자 없이 거래 당사자 간 거래가 진행되기 때문에, 중개 수수료를 지불하지 않아 비용 절감이 된다. 또한 가스(Gas) 수수료 메커니즘을 통해 블록체인 플랫폼에 대한 DDoS 공격을 방지할 수 있다. 스마트 계약 실행에 필요한 계산량에 비례하여 수수료가 부과되기 때문에, 악의적인 공격자들이 무차별적으로 네트워크를 공격하는 것을 방지한다. 스마트 계약을 활용하여 금융 서비스, 부동산 거래, 공급망 관리, 전자 투표 시스템 등 다양한 서비스를 구현할 수 있다.

스마트 계약의 기본 구조는 SPDX 라이선스, 컴파일러 버전, 계약 내용으로 이루어진다. 표 1은 “Hello World!” 메시지를 출력하는 간단한 스마트 컨트랙트 예제 코드이다. 해당 컨트랙트를 블록체인 네트워크에 배포한 후, getMessage 함수를 호출하면 “Hello World!” 메시지를 확인할 수 있다.

표 1. 스마트 컨트랙트 예제 코드
Table 1. Smart contract example code

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract HelloWorld {
    string public message;
    constructor() {
        message = "Hello, World!";
    }
    function getMessage() public view returns (string
memory) {
        return message;
    }
}
```

2.3 NFT(Non-Fungible Token)

이더리움 블록체인은 NFT의 표준화된 규약으로 ERC-721(Ethereum Request for Comment 721)을 사용한다[18]. NFT는 블록체인에 저장된 생성된 희소성 있는 대체 불가한 디지털 가상 자산이다. 각각의 NFT는 식별될 수 있는 고유한 값을 지니기 때문에 서로 다른 토큰으로 대체 될 수 없는 특징이 있다. 즉, 동일한 값을 가진 중복되는 토큰이 존재할 수 없기 때문에 소유권을 증명할 수 있다.

ERC-721 표준을 사용하면 사진, 비디오, 오디오, 문서 등 다양한 디지털 파일을 포함한 디지털 자산을 표현할 수 있다. 각 ERC-721 토큰은 고유한 속성과 메타데이터를 가질 수 있어, 디지털 콘텐츠의 소유권을 투명하게 추적하고, 블록체인상에서 거래할 수 있다. 메타데이터는 블록체인에 불변하게 저장되어 있어 신뢰성과 무결성을 유지한다.

표 2. ERC-20과 ERC-721 비교
Table 2. Comparison between ERC-20 and ERC-721

	ERC-20	ERC-721
Fungibility	Fungible	Non-Fungible
Divisibility	Possible	Impossible
Token ownership	None	Exists
Unique identifier	None	Exists
Usage	Cryptocurrency	Digital art

III. 제안 시스템

이 장에서는 블록체인 기반 NFT 전자 헌혈 증서 관리 제안 시스템을 제안한다. 제안 시스템의 구조와 시스템 참여자, 스마트 컨트랙트, 기능별 프로세스에 관해 설명한다.

3.1 제안 시스템 구조

제안 시스템은 그림 2과 같이 메타마스크 지갑(MetaMask), 웹 인터페이스 (Web Interface), 시스템 참여자를 위한 NFT 헌혈 증서 관리 분산 애플리케이션(Dapp), NFT Blood Certificate 스마트 컨트랙트, IPFS (Inter Planetary File System)로 구성되어 있다.

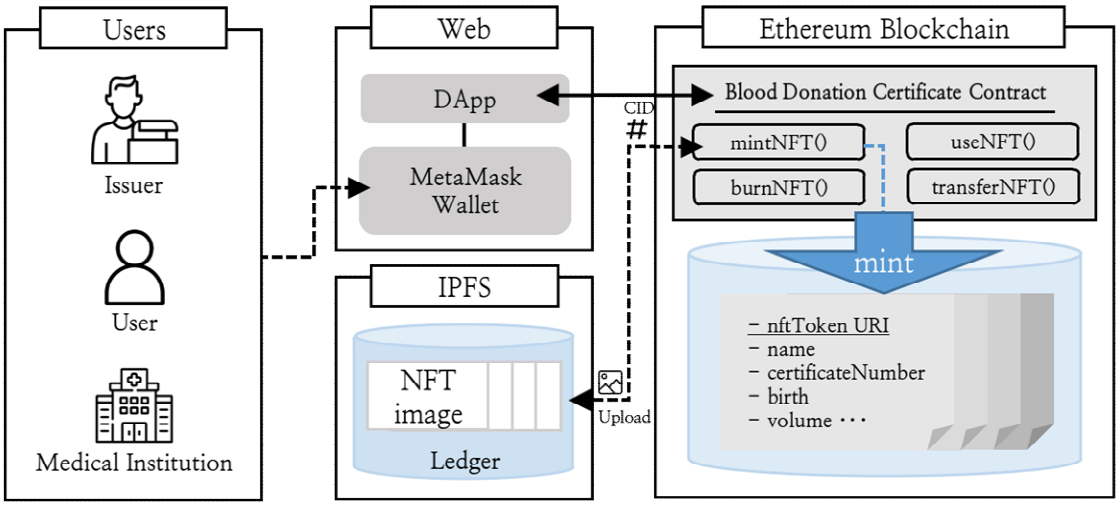


그림 2. 제안 시스템 구성도
Fig. 2. Proposed system architecture

각 시스템 구성의 세부 기능은 다음과 같다.

메타마스크는 사용자가 디지털 자산을 관리할 수 있게 해주는 웹 익스텐션 기반의 블록체인 기반 디지털 지갑이다. 해당 지갑을 통해 사용자는 메타마스크 계정과 관련된 디지털 자산을 조회 및 관리할 수 있다. 이더리움 네트워크와 연결되어, 사용자들이 메타마스크를 통해 이더리움 기반의 애플리케이션과 상호작용을 한다[19].

웹 인터페이스는 시스템 참여자들이 시스템과 상호작용 할 수 있게 한다. 해당 인터페이스를 통해 NFT 헌혈 증서를 생성, 조회, 전송 등의 작업을 수행한다. NFT 헌혈 증서 관리 분산 애플리케이션(DApp)는 시스템 참여자의 서비스 이용을 위한 애플리케이션 플랫폼이다. 메타마스크를 이용해 DApp 로그인 후, 헌혈 증서 발행, 조회 등 서비스 이용이 가능하다.

NFT Blood Certificate 스마트 컨트랙트는 솔리디티 언어로 작성된 컨트랙트는 이더리움 블록체인에 헌혈 증서의 정보를 안전하게 저장하며, 헌혈 증서의 발행, 양도, 사용, 폐기의 프로세스를 자동화한다.

IPFS는 분산형 파일 저장 시스템으로, P2P 네트워크 방식을 활용하여 대용량의 파일이나 데이터를 공유하기 위해서 사용된다[20]. NFT 헌혈 증서 이미지의 URL을 해시화하여 IPFS에 저장함으로써, 파일의 무결성을 보장하고 안전하게 보관한다.

본 논문에서 제안하는 분산형 애플리케이션 시스템은 기존의 헌혈 증서 시스템을 넘어서, 블록체인 기술을 활용하여 헌혈 증서의 영속성, 무결성, 불변성 그리고 접근성을 강화한 모델을 구현할 수 있다.

3.2 제안 시스템 참여자 관계 정의

NFT 전자 헌혈 증서 관리 시스템 참여자들의 관계는 그림 3과 같으며, 각 참여자의 세부 설명은 아래와 같다.

혈액원 (Issuer)는 혈액 기증자에게 그들의 기여를 인정하는 증서를 NFT 형태로 발행하는 주체이다. 발행자의 권한은 대한적십자사가 설정한 특정한 기준을 충족하는 기관에만 부여된다.

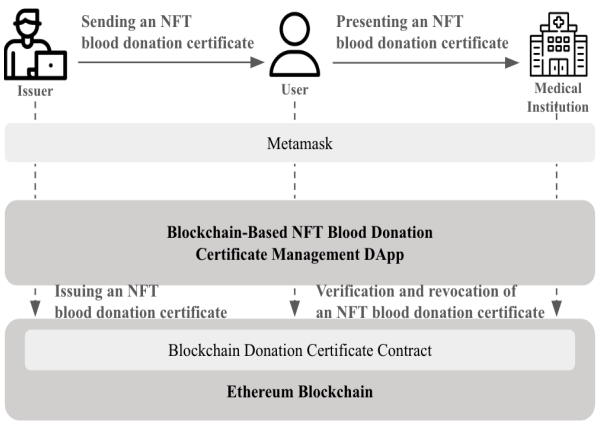


그림 3. 제안 시스템 참여자 관계도
Fig. 3. Participant relationshipi diagram in proposal system

등록된 혈액원은 헌혈 증서 데이터를 이더리움 블록체인의 분산된 네트워크상에 영구적으로 저장하고 관리한다.

혈액 기증자 (User)는 혈액원으로부터 발급받은 NFT 헌혈 증서를 이용하는 주체이다. NFT 헌혈 증서 관리 분산 애플리케이션을 통해 헌혈 증서 조회, 유효성 확인 등 서비스를 이용할 수 있다. 또한 해당 앱을 통해 NFT 헌혈 증서를 의료 기관에 제시하여 무료 수혈 혜택을 받거나, 자신의 헌혈 증서를 또 다른 사용자나 의료 기관에 양도할 수 있다.

의료 기관 (Medical Institution)은 혈액 기증자가 제시한 헌혈 증서를 활용하는 주체로, NFT 헌혈 증서 관리 분산 애플리케이션을 통해 제시된 헌혈 증서의 유효성을 빠르게 확인하고, 무료 수혈 혜택을 제공하며, 폐기한다.

NFT 헌혈 증서가 활용되는 과정은 다음과 같다. 혈액 기증자가 헌혈을 수행하면, 혈액원에 NFT 헌혈 증서 발행을 요청한다. 혈액원은 혈액 기증자의 정보와 헌혈 정보를 스마트 컨트랙트에 입력한다. 스마트 컨트랙트는 이 정보를 기반으로 NFT 전자 헌혈 증서를 생성하고, 이를 혈액원의 메타마스크 지갑 주소로 전달한다. 그다음, 혈액원은 NFT 헌혈 증서를 해당 혈액 기증자의 메타마스크 지갑 주소로 전송하고, 혈액 기증자는 사용할 헌혈 증서를 의료 기관에 제출하여 사용한다.

3.3 헌혈 증서

표 3. NFT 헌혈 증서 메타 데이터
Table 3. NFT blood certificate metadata

Parameter	Data type	Description
name	string	Name
certificateNumber	uint256	Certificate unique number
birth	uint256	Date of birth
volume	string	Type of donation
date	uint256	Donation date
medicalCenter	uint256	Blood bank ID
bloodType	string	Blood type
nftToken_URI	string	Certificate's main image URI
isUsed	bool	Usage status

헌혈 증서는 헌혈자가 헌혈했음을 증명하는 문서이다. 표 3은 헌혈 증서의 메타 데이터를 나타내며, 이는 이더리움 블록체인에 구조체의 형태로 저장된다. 블록체인 기술을 사용하여 헌혈 증서를 저장함으로써 데이터 위변조가 불가능하여 헌혈 증서의 신뢰성을 보장한다. 또한, 모든 기록이 공개적으로 검증할 수 있어 헌혈 증서의 발행 및 사용 이력을 누구나 확인 할 수 있다.

3.4 제안 시스템 스마트 컨트랙트 코드

스마트 컨트랙트는 NFT 헌혈 증서의 발행, 전송, 검증 등을 자동화하는 핵심 요소이다. 제안 시스템의 스마트 컨트랙트는 솔리디티(Solidity) 언어로 작성되었으며, 솔리디티 기반 표준 라이브러리인 OpenZepplin 라이브러리의 ERC-721 표준 컨트랙트를 상속받아 NFT 발행 및 관리 기능을 제공한다.

표 4. 스마트 컨트랙트 발행 코드
Table 4. Smart contract issuance code

```
function mintNFT(
    string memory _name,
    uint256 _certificateNumber,
    uint256 _birth,
    string memory _volume,
    uint256 _date,
    uint256 _medicalCenter,
    string memory _bloodtype,
    string memory _tokenURI
)
    public returns (uint256)
{
    _tokenIds.increment();
    uint256 newTokenId = _tokenIds.current();
    nftTokenDetails[newTokenId] = NftTokenData(
        _name,
        _certificateNumber,
        _birth,
        _volume,
        _date,
        _medicalCenter,
        _bloodtype,
        _tokenURI,
        false // isUsed를 false로 초기화
    );
    _mint(msg.sender, newTokenId);
    return newTokenId;
}
```

표 4는 실제 혈액 기증자의 정보와 헌혈 정보를 기반으로 한 NFT 형태 헌혈 증서를 발행하는 솔리디티 코드를 나타낸다. 제안 시스템의 스마트 컨트랙트 구성은 표 5와 같으며, 주요 함수의 세부 기능은 다음과 같다.

표 5. 제안 시스템 스마트 컨트랙트 함수
Table 5. Proposed system smart contract function

	Function
Issuer	mintNFT() getAll_NFT() getNFT_Details() checkNFTUsed() transferNFT()
User	getUsedNFT_Count() getMyNFTDetails() transgerNFT()
Medical institution	useNFT() burnNFT()

mintNFT() 함수는 헌혈증서를 발행하는 역할이다. 이 함수는 헌혈자의 세부 정보를 입력받아 새로운 NFT를 발행하고 그에 대한 고유한 토큰 ID를 반환한다. 발행된 NFT는 NftTokenData 구조체에 저장된다.

getNFT_Details() 함수는 특정 NFT의 세부 정보를 조회하는 데 사용되며, 특정 토큰의 ID에 해당하는 NftTokenData 구조체를 반환한다.

checkNFTUsed() 함수는 특정 NFT의 사용 여부를 확인하고 업데이트하는 데 사용된다. 특정 토큰 ID의 isUsed 속성을 변경한다.

transferNFT() 함수는 특정 NFT를 입력한 지정된 주소로 전송한다. 헌혈 기증자에게 전송할 때나 양도할 때 사용된다. 이를 통해 NFT의 소유권이 변경되고, 블록체인상의 거래 기록에 반영된다.

useNFT() 함수는 의료 기관이 NFT를 사용하는 데에 활용된다. 특정 NFT의 사용 여부를 표시하며 해당 토큰 ID에 대한 isUsed 속성을 true로 변경하여 해당 헌혈 증서가 사용되었음을 나타낸다.

burnNFT() 함수는 사용된 NFT를 폐기하는 데 사용된다. NFT의 isUsed 변수가 'true'인 경우 폐기 프로세스를 진행한다. 해당 NFT를 블랙홀 주소로 전송하여 완전히 제거하여, 재사용 문제를 방지한다.

3.5 제안 시스템 기능별 프로세스

이 절에서는 NFT 헌혈 증서 발행 절차, NFT 헌혈 증서 양도 절차, NFT 헌혈 증사 사용 및 폐기 절차에 대한 프로세스에 관해 설명한다.

3.5.1 사용자 인증

모든 사용자는 NFT 헌혈 증서를 관리하기 위해 메타마스크 웹 익스텐션 프로그램 형태의 소프트웨어 암호화폐 지갑을 사용한다. 각 사용자는 메타마스크 계정(Account)을 생성하고 등록한다. 이를 통해 사용자는 블록체인 클라이언트(Geth) 없이도 블록체인 네트워크와 상호작용을 한다. 메타마스크를 통해 인증을 완료하고 시스템에 로그인한 사용자는 웹(NFT 헌혈 증서 관리 분산 애플리케이션)을 통해 연결된 스마트 컨트랙트(NFT blood certificate smart contract)와 상호작용을 한다. 사용자는 메타마스크의 계정으로 소유하고 있는 헌혈 증서를 간편하게 조회할 수 있다.

3.5.2 헌혈 증서 발행

그림 4는 혈액원이 NFT Blood Certificate 스마트 컨트랙트를 통해 검증할 수 있는 NFT 헌혈 증서를 발행하는 프로세스를 나타낸다. 증서 발행은 표 3과 같은 헌혈 증서 메타 데이터를 포함하여 mintNFT() 함수를 통해 혈액원에 의해 수행된다. 발행된 모든 헌혈 증서는 혈액원에 의해 관리되고 조회된다.

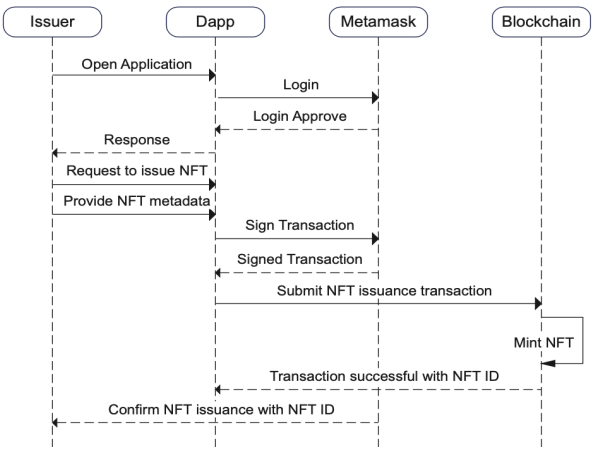


그림 4. NFT 헌혈 증서 발행 프로세스
Fig. 4. NFT blood donation certificate issuance process

해당 헌혈 증서의 사용 여부는 불리언 자료형의 'isUsed' 변수를 통해서 확인된다. 이 변수는 미사용일 경우 0, 사용된 경우 1로 구분되어 있으며, 해당 정보는 그림 5와 같이 GUI에서 '미사용' 또는 '사용됨' 상태로 직관적으로 확인할 수 있다.

그림 5. 혈액원 헌혈 증서 조회 및 관리 GUI
Fig. 5. Iusser's blood donation certificate inquiry and management GUI

3.5.3 헌혈 증서 양도

그림 6은 NFT 헌혈 증서 양도 프로세스를 나타낸다. 모든 사용자는 양도 페이지를 통해 자신의 헌혈 증서를 타인에게 양도할 수 있다. 헌혈 증서 소유자를 추적할 수 있으며 사용 여부도 확인 할 수 있어 스마트 컨트랙트에 의해 제3의 중개자 없이 안전하고 효율적으로 헌혈 증서를 양도할 수 있다. 헌혈 증서는 법적으로 대가나 금품을 요구하는 것이 금지되어 있기 때문에 스마트 컨트랙트 기반 양도 프로세스를 통해 양도 및 사용 기록을 추적하여 불법 매매를 방지할 수 있다. 양도 페이지에 등록된 이더리움 공개키 주소를 통해 양도가 이루어진다.

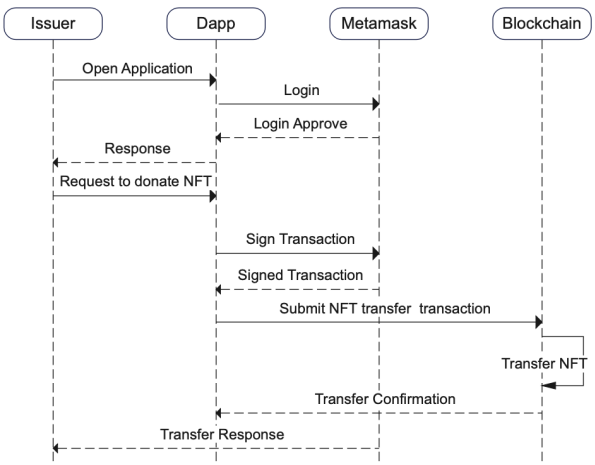


그림 6. NFT 헌혈 증서 양도 프로세스
Fig. 6. NFT blood donation certificate transfer process

3.5.4 헌혈 증서 사용 및 폐기

그림 7과 같이 의료 기관은 사용자가 제시한 헌혈 증서를 사용하고 폐기 처리할 수 있다. 이러한 기능은 스마트 컨트랙트의 useNFT()와 burnNFT() 함수를 통해 수행된다. 그림 8은 의료 기관의 대시보드를 나타낸다. 의료 기관의 대시보드의 '사용하기' 버튼을 클릭하면 useNFT() 함수가 활성화되어 헌혈 증서 구조체의 isUSed 변수 값이 1(사용됨)로 변경된다. 스마트 컨트랙트 내의 사전 정의된 규칙에 따라 burnNFT() 함수가 활성화되어 소각된다. 이더리움 블록체인에는 직접적인 폐기 또는 삭제 기능이 없지만, 상태 변화를 통해 명시적으로 사용 불가 상태로 변경한 후, 영구적으로 사용할 수 없게 블랙홀 주소로 전송된다. 이로써 중복 사용을 방지하며 헌혈 증서의 무결성을 유지한다.

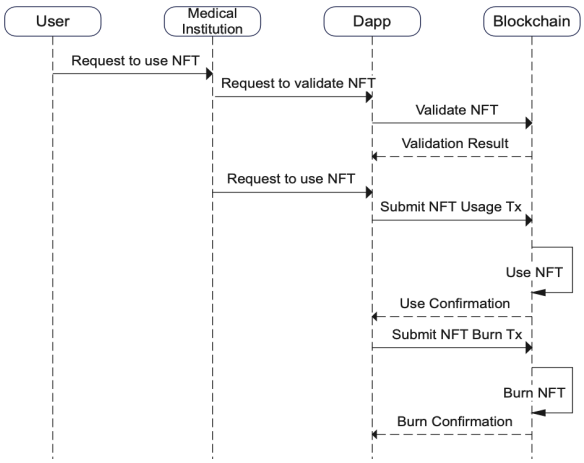


그림 7. NFT 헌혈 증서 사용 및 폐기 프로세스
Fig. 7. Usage and disposal process of NFT blood donation certificate

그림 8. 의료기관 GUI
Fig. 8. Medical institution GUI

Ⅳ. 구 현

제안 시스템은 표 6과 같은 환경에서 구현되었으며, 실험은 이더리움 공개 블록체인의 '세폴리아 테스트넷'을 통해 진행했다.

표 6. 제안 시스템의 실험 환경
Table 6. Proposed system development environment

Blockchain	Ethereum sepolia testnet	
Smart contract	Remix - Ethereum IDE	
	Language	Solidity
Wallet	MetaMask	
Web	Chrome browser	
	Language	Node.js
		Web3.js

사용자 인증과 NFT 헌혈 증서를 관리하기 위하여 메타마스크 크롬 익스텐션을 사용한다. 스마트 컨트랙트는 리믹스 통합개발환경(Remix-IDE)에서 솔리디티 언어로 개발되었다[21]. 우리는 제안 시스템의 구현 실험 결과를 세 가지 시나리오를 통해 검증한다. 시나리오 검증 트랜잭션은 이더 스캔과 같은 블록체인 탐색기를 사용하여 해당 트랜잭션의 해시를 확인할 수 있다[22].

4.1 시나리오 검증

표 7은 참여자의 메타마스크 주소 목록을 나타낸다. 각 시나리오의 참여자를 식별할 수 있다.

표 7. 참여자 메타마스크 주소 목록
Table 7. Participant metamask account list

Classification	Metamask account
Issuer	0x95a8452b45eCAd058b9E81ea40D4364366C6402
User alice	0x5C461f8C23a1A99C7C1eE398c4C5Eb1586f43054
User bob	0x0A27b1e7B347e59f4D92cE19Ceb4d900A222D738
Medical institution	0x67043d193470666d3C00C309D31bC03A13CD5460

4.1.1 시나리오 1 : 민팅

그림 9는 혈액원이 NFT 헌혈 증서를 발행하기 위해 NFT Blood Certificate.sol 스마트 컨트랙트를 블록체인에 배포(Deploy)한 것을 나타낸다. 배포 트랜잭션이 생성되고 블록체인 네트워크에 전송되면, 네트워크 노드들은 받은 트랜잭션의 유효성을 검사하고, 유효성 검사를 마친 노드는 NFT Blood Donation Certificate.sol 스마트 컨트랙트를 블록체인의 새로운 블록에 포함해 네트워크에 저장하고 배포하여 스마트 컨트랙트를 활성화한다.

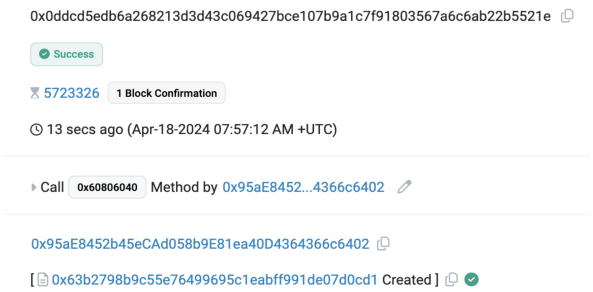


그림 9. 스마트 컨트랙트 배포 트랜잭션
Fig. 9. Smart contract deployment transaction

그림 10은 혈액원이 사용하는 헌혈 증서 발행 GUI를 나타낸다. 혈액 기증자 정보와 헌혈 정보를 기입하고 헌혈 증서를 발행한다. 그림 11은 발행 트랜잭션의 처리 결과를 나타낸다.

그림 10. NFT 헌혈 증서 발행 GUI
Fig. 10. NFT blood donation certificate issuance GUI

4.1.2 시나리오 2 : 양도

헌혈 증서 기증자는 다른 개인이나 의료 기관의 헌혈 증서 양도 요청 글을 확인하고 그림 12와 같이, 해당 양도 수혜자의 메타마스크 공개키를 활용하여 헌혈 증서를 양도를 수행한다. 이 과정은 스마트 컨트랙트를 통해 이루어지므로 헌혈 증서의 소유권 변경 사항 또한 블록체인에 기록된다. 그림 13은 양도 트랜잭션의 처리 결과를 나타낸다.

그림 12. NFT 헌혈 증서 양도 GUI
Fig. 12. NFT blood donation certificate transfer GUI

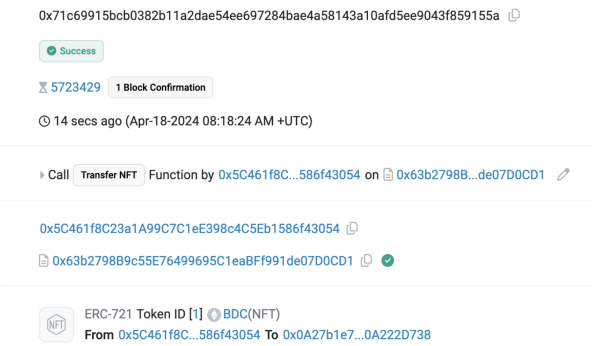


그림 13. NFT 헌혈 증서 양도 트랜잭션
Fig. 13. NFT blood donation certificate transfer transaction

4.1.3 시나리오 3 : 폐기

그림 14는 의료 기관이 NFT 헌혈 증서를 사용하고 폐기하는 과정을 나타낸다. 헌혈 증서 사용자는 무료 수혈 혜택을 받기 위해 의료 기관에 헌혈 증서를 제시한다. 의료 기관에서는 해당 헌혈 증서를 사용하여 제시한 자에게 무료 수혈을 제공한 후, 해당 헌혈 증서의 목적을 완료했다고 판단하여 폐기 프로세스를 진행한다. 의료 기관은 증서의 상태를 '사용됨'으로 업데이트하고 블랙홀 주소로 전송한다.

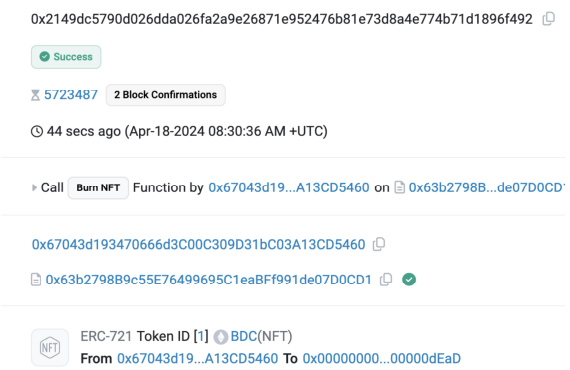


그림 14. NFT 헌혈 증서 폐기 트랜잭션
Fig. 14. NFT blood donation certificate disposal transaction

V. 결 론

본 논문에서는 메타마스크의 연동을 통해 사용자를 신뢰성 있게 인증하며, 이를 기반으로 NFT 헌혈 증서를 안전하게 저장하고 관리하는 블록체인 기반 시스템을 제안하고 구현하였다. 사용자, 디앱, 스마트 컨트랙트로 구성되어 있다. 이를 통하여 사용자는 자신의 NFT 헌혈 증서를 이 시스템에 안전하게 저장할 수 있으며, 블록체인의 분산형 특성으로 무결성과 보안을 보장한다. 헌혈 증서의 양도 및 사용 과정을 투명하게 기록하고 관리하며, 디앱의 핵심 기능인 스마트 컨트랙트를 통해 기증자와 수혜자 간의 양도가 신속하게 이루어진다. 이러한 블록체인 기반 NFT 전자 헌혈 증서 관리 시스템은 헌혈 과정의 투명성과 안전성을 확보하면서, 사용자들이 자유롭게 헌혈 증서를 활용하고 양도할 수 있어 효율성과 신뢰성을 높이며 기존의 문제였던 헌혈 증서 훼손 및 분실 문제, 재발급 제한 문제, 헌혈 환급 적립금 누적 문제를 해결할 수 있을 것으로 기대한다.

References

[1] "Blood Donation Certificate Guide", KOREAN Redcross Blood Services, https://www.bloodinfo.n용et/knrcbs/cm/cntnts/cntntsView.do?mi=1142&cntntsId=1022 [accessed: Jun. 15, 2024]

[2] "Blood Donation Certificates Should Be Managed Electronically; Only 12% of Issued Certificates Used", Minkyu Jo, http://www.kukimedi.com/article/view.asp?gCode=01&sCode=0000&arcid=709582&code=51111102 [accessed: Jun. 15, 2024]

[3] "Blood Insurance Fund Like Gold; 50 Billion Won Blood Donation Refund Fund Lying Dormant", Leeching Stop, https://news.mt.co.kr/mtview.php?no=2023040322164865872 [accessed: Jun. 15, 2024]

[4] "Request for Reissuance of Blood Donation Certificate", KOREAN Redcross Blood Services, https://bloodinfo.net/knrcbs/cm/cntnts/cntntsView.do?mi=1185&cntntsId=1088 [accessed: Jun. 15, 2024]

[5] "Red Connect (Blood Donation App)",KOREAN

Redcross Blood Services, https://www.bloodinfo.net/knrcbs/cm/cntnts/cntntsView.do?mi=1125&cntntsId=1014 [accessed: Jun. 15, 2024]

[6] H. Saleh, S. Avdoshin, and A. Dzhonov, "Platform for tracking donations of charitable foundations based on blockchain technology", 2019 Actual Problems of Systems and Software Engineering (APSSE), Moscow, Russia, pp. 182-187, Nov. 2019. https://doi.org/10.1109/APSSE47353.2019.00031.

[7] B Hu and H. Li, "Research on Charity System Based on Blockchain", IOP Conference Series. Materials Science and Engineering, Vol. 768, No. 7, 2020. https://doi.org/10.1088/1757-899X/768/7/072020.

[8] 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, Nov. 2022. https://doi.org/10.1016/j.jksuci.2022.09.021.

[9] A. Singh, M. Ahad, and H. M. Malik, "Donation Tracking System using Blockchain", International Research Journal of Engineering and Technology (IRJET), Vol. 10, No. 1, pp 735-739, Jan. 2023.

[10] B. Jaeyoung, et al., "DID-based digital blood donation certification issuance service", Proc. of the Korea Information Processing Society Conference, Vol. 27, No. 2, pp 416-419, Nov. 2020. https://doi.org/10.3745/PKIPS.y2020m11a.416.

[11] Y. Anji and C. Sangyoung, "Implementation of Blockchain-based Blood Management System for Blood Recipient", Korean Institute of Information Scientists and Engineers, pp 1536-1538, Dec. 2020.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Satoshi Nakamoto, 2008.

[13] Y. Yeongjin, K. Hackyoon, and J. Hyunjun, "Career Certificate System using Blockchain-based Smart Contract", Journal of KIIT, Vol. 21, No. 12, pp. 201-209, Dec. 2023. http://dx.doi.org/10.14801/jkiit.2023.21.12.201.

[14] Z. Ouyang, J. Shao, and Y. Zeng, " PoW and PoS and related applications", 2021 International Conferenc.e on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, pp. 59-62, Sep. 2021. https://doi.org/10.1109/EIECS53707.2021.9588080.

[15] H. Sheikh, R. M. Azmathullah, and, F. Rizwan, "Proof-of-work vs proof-of-stake: a comparative analysis and an approach to blockchain consensus mechanism", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 6, No. 12, pp. 786-791, Dec. 2018.

[16] G. Xu, Y. Liu, and P. W. Khan, "Improvement of the DPoS consensus mechanism in blockchain based on vague sets", IEEE Transactions on Industrial Informatics, Vol. 16, No. 6, pp. 4252-4259, Nov. 2019. https://doi.org/10.1109/TII.2019.2955719

[17] W. Zou, D. Lo, P. S. Kochhar, X. B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities", IEEE transactions on software engineering, Vol. 47, No. 10, pp. 2084-2106, Sep. 2019. http://dx.doi.org/10.1109/TSE.2019.2942301.

[18] "ERC-721 NON-FUNGIBLE TOKEN STANDARD", Ethereum, https://ethereum.org/ko/developers/docs/standards/tokens/erc-721 [accessed: Jun. 15, 2024]

[19] MetaMask, https://metamask.io [accessed: Jun. 15, 2024]

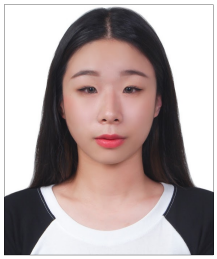
[20] IPFS, https://ipfs.tech [accessed: Jun. 15, 2024]

[21] Remix-IDE, https://remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null [accessed: Jun. 15, 2024]

[22] Sepolia Etherscan, https://sepolia.etherscan.io [accessed: Jun. 15, 2024]

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)

2000년 2월: 한국과학기술원
전산학과 (공학사)
2002년 2월: 한국과학기술원
전산학과 (공학석사)
2007년 2월: 한국과학기술원
전산학과 (공학박사)
2009년 ~ 현재 : 경기대학교
컴퓨터공학부 교수
관심분야 : 블록체인, 정보보호