Journal of KIIT. Vol. 18, No. 4, pp. 89-99, Apr. 30, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.4.89

블록체인 기반의 분실물 보상 및 회수 모델

홍성호*, 이상윤**[1], 박지우**[2], 김희열***

A Blockchain Based Claim and Reward Model for Lost Property

Seongho Hong*, Sangyun Lee**[1], Jiwoo Park**[2], and Heeyoul Kim***

본 연구는 경기도의 경기도 지역협력연구센터 사업의 일환으로 수행하였음. [GRRC경기2017-B04, 영상 및 네트워크 기반 지능정보 제조 서비스 연구]

요 약

본 논문은 블록체인을 이용하여 사용자 간에 분실물을 돌려주고 이에 대한 적절한 보상금을 받을 수 있는 모델을 제시한다. 분실물은 습득자에게 자발적 선행을 요구하여 분실물 회수를 어렵게 한다. 유실물 관리 서비스를 운영하거나 물건에 전화번호를 기록하여 문제 상황을 개선할 수 있으나, 쌓여가는 분실물을 관리할 기관이 필요하고 분실물 회수에 대한 동기 유발을 할 수 없다. 제안하는 모델은 기기에 QR 코드를 부착하고 QR 정보를 블록체인에 기록하여 습득 알림을 전달해줄 수 있는 방법을 제공하고, 습득자가 중재자 컨트랙트를 통해 보상을 받을 수 있도록 한다. 본 모델은 상호 간의 신뢰 없이 분실물과 보상을 교환할 수 있도록 하고 기관을 통하지 않은 비대면 방식의 교환을 가능하게 한다. 또한 중앙 집중형 모델을 탈피한 에스크로 방식으로 신뢰성을 확보할 수 있다.

Abstract

This paper propose a model that can return lost property between users and receive appropriate reward to acquirer using blockchain. Lost property makes it difficult for the acquirer to voluntarily get ahead of the purpose of recovering lost property by requiring voluntary good deeds. There were precede solutions proposed to solve the problem by operating a lost or found ware house or recording a phone number on the property, but it require to manage the accumulation of lost properties and cannot motivate user to give back lost items. The proposed model attaches a QR code to device and records it on the blockchain, providing a method for sending notifications, and allowing the acquirer to be rewarded through the contract. This model offer exchange methodology of lost and found properties without mutual trust, non-face-to-face exchange, and offer reliable escrow in decentralized environment.

Keywords

blockchain, smart contract, lost item, reward, escrow

* 경기대학교 컴퓨터과학과 석사과정
- ORCID: http://orcid.org/0000-0002-6677-3466
** 경기대학교 컴퓨터과학과 학부생
- ORCID[1]: http://orcid.org/0000-0003-3321-9626
- ORCID[2]: http://orcid.org/0000-0002-5058-8709
*** 경기대학교 컴퓨터과학부 교수(교신저자)
- ORCID: https://orcid.org/0000-0001-8776-5185

• Received: Jan. 09, 2020, Revised: Feb. 26, 2020, Accepted: Feb. 29, 2020
• Corresponding Author: Heeyoul Kim
Dept. of Computer Science, Kyonggi University, 94-6 Iuidong, Yeongtonggu, Suwon, Gyeonggi, 443-760, Korea,
Tel.: +82-31-249-9675, Email: heeyoul.kim@kgu.ac.kr

Ⅰ. 서 론

대다수의 분실물은 분실 시간이나 위치와 같은 부가 정보를 통해 소유자를 특정하기 어렵다. 이는 분실물을 획득한 습득자가 물건을 돌려줄 방법을 실행하기 어렵게 하는 원인이 되며, 과정 또한 습득자의 노력을 요구하기 때문에 분실물 회수에 대한 동기를 저하시킨다. 분실물 회수를 위해 개인의 전화 번호를 분실가능성이 있는 소유물에 부착할 수 있으나, 이는 소유자의 개인 정보가 공개되므로 정보 보호 측면에서 취약하다. 국가 기관에서 분실물에 대한 처리를 습득자로부터 위임받고 소유자를 찾기 위해 지원하는 방안도 있으나, 습득자는 위임 이후 분실물 회수 기여에 대한 보상을 청구하기 어려워지고, 이는 분실물 회수 노력에 대한 동기 유발 감소로 이어진다[1]. 분실물 회수 방법도 웹사이트에 분실물 보관 사실과 분실물에 대한 특징을 고지하는 수준 머물고 있기 때문에 다양한 분실물들 사이에서 자신의 분실물을 조회하기 위해 많은 시간을 소비해야 한다.

분실물을 관리하는 입장에서도 비용과 관리의 어려움 문제를 갖는다. 분실물들은 소유자가 분실을 인지하고 실제로 물품을 찾아가기 위한 시간을 필요로 한다. 이 시간동안 관리자는 이를 보관 창고에 두고 관리하게 되는데 모든 분실물이 반드시 소유자가 찾아가는 것이 아니므로 지속적으로 쌓이는 분실물들이 생겨나게 된다[2]. 이 과정이 반복되면 관리자는 늘어나는 분실물들에 대한 보관 만료 일자와 창고 내 분실물 위치를 관리하기 어려워지고 새로 유입되는 분실물들을 보관할 공간이 부족해지는 문제에 직면한다.

분실물 회수와 관리의 어려움을 해결하고자 다양한 방법으로 문제를 해결하려는 시도들이 존재했다. 이들은 RFID[3]나 저전력 블루투스 기술[4] 등을 이용하여 분실물을 쉽게 회수할 수 있도록 하거나 위치를 특정할 수 있도록 하였다. 그러나 이들 방법은 지속적인 서비스를 위한 관리자를 필요로 하고 실제로 사용하기 위해서 사용자가 준비해야 할 것이 많거나 제약이 커서 통용되기 어려웠다.

본 논문은 기존의 모델들보다 소유자의 개인정보를 보호할 수 있음과 동시에 분실물 검색을 위한 노력을 최소로 할 수 있는 방안을 제시하며, 기존 방식에서는 불가능했던 분실물에 대한 보상 모델을 제안한다. 제안하는 모델은 QR코드를 이용하여 분실물에 대한 정보에 접근할 수 있도록 하며, 분실물에 대한 정보로 소유자가 가진 이더리움 주소와 분실물에 대한 보상 금액 정보를 블록체인상에 기록되어 누구나 확인할 수 있다. 분실물에 대한 보상이 실현될 수 있도록 하기 위해, 본 모델은 기존의 전자상거래에서 사용되던 에스크로를 스마트 컨트랙트에 구현하여 금융 기관과 같은 중앙 기관의 중재자 역할을 컨트랙트가 수행하도록 한다. 이로 인해 기관의 보증 없이도 투명하게 분실물 보상 서비스가 운영된다. 소유자는 분실 가능성이 있는 물건에 본 서비스에서 생성한 QR코드를 부착하여 분실 시 소유자의 개인 정보 없이 분실 사실을 고지받을 수 있으며 습득자는 분실물 회수 프로세스를 진행하면서 부가적인 노력이 없더라도 보상을 획득할 수 있게 된다.

본 논문의 제 2장에서는 기존의 분실물 회수 모델들에 대하여 분석하고 에스크로 서비스와 이더리움 블록체인에 대하여 설명한다. 제 3장에서는 제안하고자 하는 모델과 모델의 운영 원리에 대하여 기술하였으며, 제 4장에서는 제안된 모델의 보안 분석을 통한 안전성을 설명한다. 제 5장에서는 결론으로 본 모델을 사용함으로써 얻을 수 있는 자체적인 이점과 기존 모델들로부터의 개선점에 대하여 서술한다.

Ⅱ. 관련 연구

2.1 기존의 분실물 회수 모델

RFID를 이용한 분실물 회수 모델은 RFID 칩 소유자는 자신이 분실 시 되찾고 싶은 물건에 칩을 부착하고 칩에 자신의 개인 정보를 기록한다[3]. RFID 칩에 기록한 개인정보와 RFID의 고유 ID, 그리고 분실물에 대한 설명을 분실물 중개 웹서버에 전달하고 웹서버에서 만들어낸 ID값을 자신의 RFID에 추가한다. 이 과정을 마치면 소유물 등록이 완료된다. 소유물이 분실되면 분실물 습득자는 소유자에게 수신자 부담 형태의 전화로 습득 사실을 고지하고 분실물을 교환할 지점을 협의한다. 보상은 분실 물품의 종류에 따라 최소치가 정해져 있으나

양자 간 협의를 통해 보상 금액을 줄이는 것이 가능하다. 직접적으로 연락하는 방식을 취하기 때문에 습득 사실을 즉각적으로 알 수 있고, 교환 과정이 짧아지기 때문에 중요한 물건일수록 간소화된 과정이 가지는 의의가 크다. 그러나 보상에 대한 최소치가 정해졌더라도 실제로 소유자가 보상을 지급할 것이라는 것을 보장할 수 없으며 분실물마다 한 개의 RFID가 필요하므로 관리의 어려움이 발생할 수 있다. 교환 과정에서 대면이 필요하므로 상대적 약자의 경우 교환을 위한 만남 자체에 부담을 가질 수 있으며, 주거지와 분실 지역의 차이가 클수록, 상대와 생활 패턴이 다를수록 대면 교환 시점을 잡기 어려워진다.

Bluetooth LE를 이용한 회수 모델은 Bluetooth Low Energy 기술을 이용하여 물품에 Bluetooth Tag를 부착하고 휴대 전화와 연동 및 사용자 등록을 선행한다[4]. 등록 과정을 마치게 되면 소유자는 해당 물품을 분실하더라도 분실물의 위치를 알 수 있게 되는데, 태그는 블루투스가 지원되는 다른 기기들과 통신을 하게 되며 분실물일 경우 해당 물건의 위치를 서버에 송신한다. 서버는 소유자에게 등록했던 분실물의 태그가 마지막으로 다른 블루투스 기기들과 통신한 위치를 소유자에게 송신한다. 해당 방식은 소유자가 분실물의 위치를 비용 없이 알 수 있다는 장점을 가지나 블루투스가 지원되는 앱이 설치된 휴대전화가 분실물의 통신가능 반경 안에 위치해야 분실물 자신의 위치를 전송할 수 있다는 한계가 존재하므로 블루투스 기기를 사용하는 사용자가 적은 오지, 또는 시간대일수록 분실물 위치 특정 기능의 효과가 감소한다.

2.2 블록체인

블록체인은 여러 노드들이 참여하여 체인처럼 엮인 형태로 존재하는 데이터를 복제하여 갖는 원장 관리 기술이다. 참여자들은 다른 노드들로부터 발생한 거래를 검증하고 이들을 모아 하나의 블록을 생성한다. 생성된 블록은 이전 블록이 가지는 해시 값을 포함하기 때문에, 이전 블록의 특정 값을 바꾸게 될 경우 이후의 블록들이 가지는 이전 블록의 해시 값을 바꿔야 하므로 누군가 임의로 데이터를 수정 및 삭제하는 것이 불가하다. 블록은 전파되는 과정에서 해시 값이 다른 여러 블록이 동시에 전파되는 경우가 발생할 수 있다. 발생한 순간에는 모두 정상 블록으로 인정하지만 시간이 지나서 이들을 부모로 갖는 블록 중 가장 최근까지 이어지는 한 체인에 속한 블록들만 정상 블록으로 인정된다[5].

개별 노드들이 운영의 주체가 된다는 점과 영구적으로 데이터가 기록된다는 성질 덕분에 초기에는 비트코인처럼 전자 상거래를 위한 형태로 초점이 맞춰졌으나[6], 이더리움의 등장으로 다양한 작업을 수행할 수 있게 되었다[7]. 이더리움 플랫폼은 스마트 컨트랙트라는 프로그램을 생성하고 실행할 수 있도록 지원한다. 솔리디티라는 독자적인 언어를 통해 블록체인 플랫폼 위에서 동작하는 컨트랙트를 개발할 수 있고, 이를 웹 또는 앱에서 실행할 수 있도록 web3라는 인터페이스를 제공하여 사용자가 일반 응용 프로그램에서 상호작용이 가능하도록 지원한다. 컨트랙트는 블록체인에서 실행되기 때문에 블록체인에 기록된 정보들처럼 쉽게 컨트랙트의 상태를 변경할 수 없고, 튜링 완전하기 때문에 일반적인 프로그램처럼 조건과 반복을 통해 원하는 플로우를 작성할 수 있다[8]. 이더리움은 공개 블록체인이기 때문에 기록된 컨트랙트는 누구나 접근하고 사용할 수 있으므로[9] 컨트랙트에 사용되는 데이터가 민감할 경우 보안을 개별적으로 신경써야 한다[10].

2.3 에스크로 서비스

에스크로는 거래의 신뢰도를 높이기 위해 생긴 서비스로 개인 간 중고매매, 소규모 쇼핑몰에서의 허위주문, 물품 미배송 등을 방지하여 안전한 전자 상거래가 이뤄질 수 있도록 고안된 서비스이다[11]. 결제 방식은 신용 카드가 아닌 실시간 계좌 이체, 또는 가상 계좌를 이용한 현금 거래 방식이어야 한다. 에스크로 서비스의 절차는 그림 1과 같다.

에스크로 서비스는 배송 확인을 소비자로부터 받는다. 대부분의 소비자는 배송을 확정짓는 작업을 생략하는 경향이 있기 때문에, 에스크로는 입금 후 일정 기간 이후에도 배송 확인이 되지 않았다면 배송이 정상적으로 되었다고 가정하고 자동으로 대금을 지급한다.

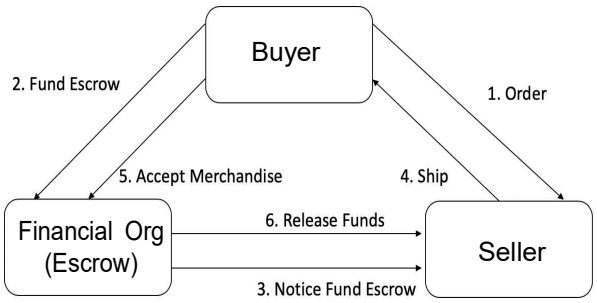

그림 1. 에스크로 서비스 흐름도
Fig. 1. Escrow service flow

이 과정은 판매자가 구매자에게 배송 자동정산 시점까지 대기하여 배송 없이 정산 금액을 빼돌리는 사기가 발생할 소지를 내포한다.

에스크로는 공신력을 필요로 하며 금융 기관이 이 역할을 일임한다. 이들은 에스크로에 참여하는 대가로 일정량의 수수료를 요구하는데, 이는 판매자에게 안전한 거래를 위한 지불 비용이자 거래마다 발생하는 지속적인 부담이다.

블록체인 환경에서 에스크로를 구현한 거래 중개 시스템으로 Lenatos가 있다[12]. 해당 모델은 블록체인을 사용하며 구매자, 판매자, 중개자, 그리고 배송 회사가 자신에게 필요한 정보만을 사용하여 안전한 물품 구매를 보장한다. 구매자는 사전에 Lenatos에서 제공하는 웹서비스에 가입해야 하고, lenatos와 제휴한 쇼핑몰에서 물품을 구매하기 위해 컨트랙트에 구매 요청을 트랜잭션으로 생성하고 물품 금액에 해당하는 돈을 컨트랙트에 전달한다. 판매자는 요청을 확인하고 Lenatos 서버에 해당 사용자가 요청한 것이 맞는지 확인하고 물품을 배송 회사에 전달한다. 배송 회사는 Lenatos 서버에 사용자 주소를 요청하여 물품을 배송하고 안전하게 배송하였으면 구매자에게 구매자 개인키로 서명된 수취 확인을 받는다. 수취 확인은 트랜잭션으로 컨트랙트에 기록되고, 수취 확인을 통해 구매 요청 때 전달된 물품 금액을 판매자가 받게 된다. Lenatos는 서로 다른 역할을 가진 참여자들이 안전한 에스크로를 만들 수 있음을 보여준다.

.

III. 블록체인 기반 분실물 보상 및 회수 모델

3.1 제안하는 모델의 개요

제안 모델은 Web3[13]를 통해 이더리움 블록체인 노드와 연결할 수 있는 애플리케이션을 이용하여 자신의 이더리움 계정을 추가하고 분실가능한 물품의 정보를 블록체인에 등록할 수 있다. 습득한 물품을 소유자에게 전달하여 보상받을 수 있다.

그림 2와 같이 이더리움에는 Escrow Contract가 업로드 되어 있는데, 컨트랙트는 Device와 Escrow 두 가지 역할을 가지며 이들을 Device Component와 Escrow Component로 표현한다. Device Component는 사용자가 분실물 등록 및 확인기능과 관련된 CRUD 컴포넌트이며, Escrow Component는 분실물을 회수하고 보상하는 기능과 관련된 컴포넌트이다.

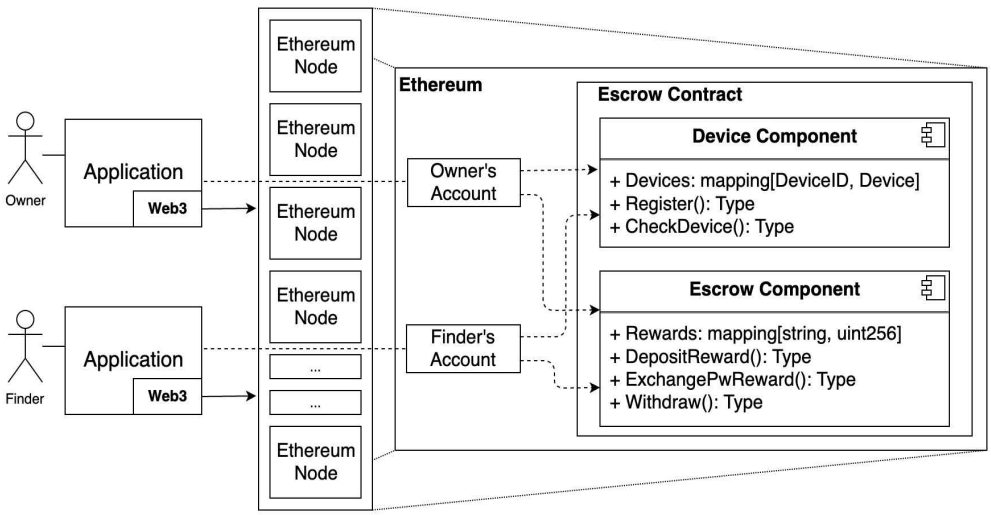

그림 2. 제안하는 분실물 보상 및 회수 모델 구조
Fig. 2. Structure of proposed lost property claim and reward model

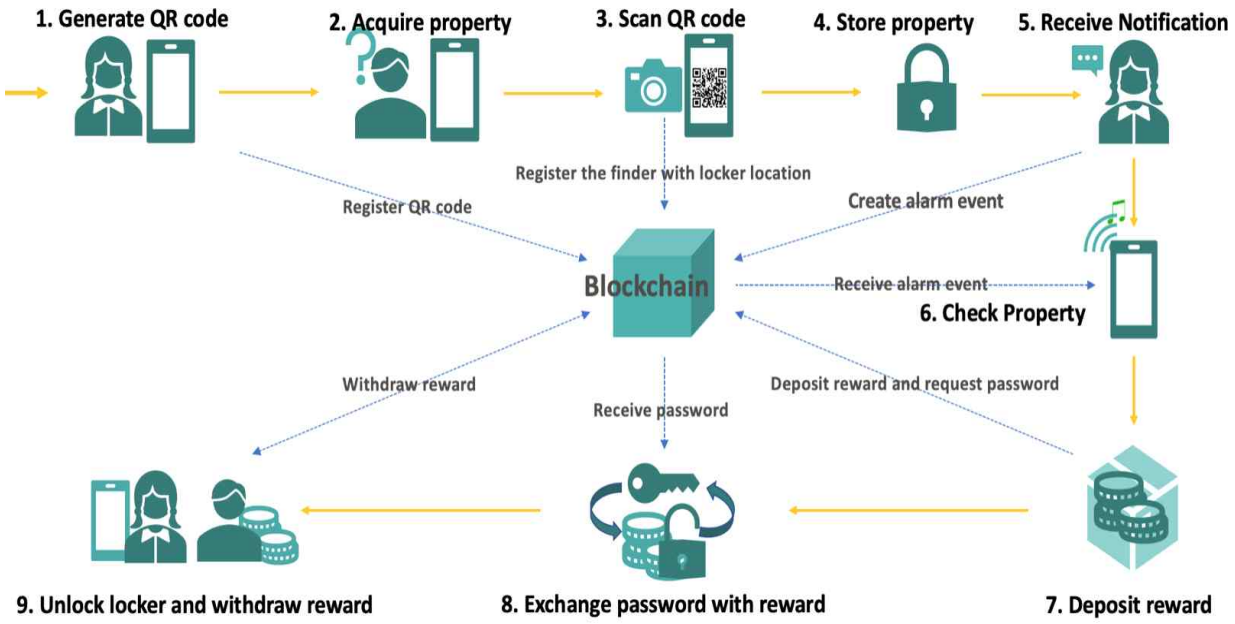

그림 3. 스마트 컨트랙트와 사용자 간에 연계된 활동과 이에 따른 상태 변화
Fig. 3. Activity associated with the smart contract and the user

At step. 1

Key	Value
575343e2951...	h(secret)='3b7d90..', item_name='S2 LTE', reward=0.8

At step. 5

Key	Value
575343e2951...	h(secret)='3b7d90..', item_name='S2 LTE', reward=0.8
6361168Efa9...	location='Suwon station, A-23'

At step. 8

Key	Value
575343e2951...	h(secret)='3b7d90..', item_name='S2 LTE', reward=0.8
6361168Efa9...	location='Suwon station, A-23', password=[1, 6, 2, 1]

575343e2951... = Device ID

6361168Efa9... = finder's account

그림 4. 시나리오 흐름에 따른 상태 변화
Fig. 4. State changes as the scenario progresses

그림 3은 소유자와 습득자의 행위를 표현하고 그림 4는 행위에 따라 변화되는 상태를 표현한 그림이다. 소유자는 애플리케이션을 통해 컨트랙트에 분실 가능한 물품에 대한 정보와 보상 금액을 기록한다. 분실물은 습득자에 의해 컨트랙트에 습득 사실이 기록되고 이를 통해 소유자는 분실물에 대한 위치를 안내 받는다.

표 1. 사례 및 회수 과정에 대한 요약
Table 1. Summarized flow of claim and reward

Seq in flow	Actor	Action
1	owner	Create QR code and register property
2	finder	Acquire the lost property
3	finder	Send message 'where it will be stored'
4	finder	Store property
5	owner	Receive message from ethereum
6	owner	Check 'is property stored'
7	owner	Deposit reward
8	finder	Share reward and send password
9-1	owner	read pw and unlock the locker
9-2	owner	release reward
9-3	finder	withdraw reward

분실물을 확인한 소유자는 보상을 예치하고 분실물 습득을 위한 비밀번호를 습득자가 입력하면 보상이 전달되게 된다. 소유자는 전달받은 비밀번호로 보관함을 열고 자신의 물건을 회수할 수 있다. 각 과정에 대한 행위 주체와 행위는 표 1에서 확인할 수 있다. 표 1은 행동을 번호가 배정되는 기준으로 삼았기 때문에 9와 같이 보상을 교환하는 행동은 같은 번호로 여러 flow를 갖는다.

3.2 Device 등록 및 QR코드 생성

사용자는 앱에서 분실물에 부착할 QR코드를 생성한다. QR코드에는 소유자 이더리움 계정과 보상 금액, 물건 이름, 그리고 비밀 값을 입력한다. 이들은 owner, reward, item_name, secret으로 명명되어 그림 5와 같은 형태의 QR코드에 JSON 형식으로 저장된다.

QR 코드에 저장되는 값들을 기반으로, 이더리움 블록체인에 분실물에 대한 정보들을 기록해야 한다. Device.register 함수를 통해 기록할 수 있으며 QR코드에서 사용했던 secret 값을 두 번 해싱한 후 기록한다는 점이 다르다. 블록체인에 올라간 QR코드 정보를 Device, Device 값에 접근할 수 있는 키 값을 DeviceID라고 명명한다.

Device = {owner, h(h(secret)), item_name, reward}
DeviceID = h(h(h(secret)) + {owner, reward})

블록체인에 등록된 해싱된 비밀 값의 원 값은 소유자와 QR코드를 읽은 사람만 알 수 있는 값이다. 해시 되지 않은 비밀 값은 습득자가 습득 사실을 증명할 때 사용하게 된다.

3.3 분실물 습득 신고 및 확인

이 과정에서 습득자는 분실물을 습득하면 블록체인에 습득 사실과 보관할 장소를 등록하고 이를 소유자가 확인한다. 그림 3에서 5~6번 단계가 3.3에 해당된다.

습득자는 분실물을 습득할 때 QR코드를 스캔하여 분실물 ID(deviceID)를 확인하여 분실물 정보를 확인한다. 분실물 ID와 QR코드에 포함된 Secret, 그리고 자신이 분실물을 보관할 위치 정보인 Location과 자신의 이더리움 계정을 분실물 정보에 추가하고 소유자에게 분실 사실을 Escrow.notifyProperty를 호출하여 그림 7의 LostFound 이벤트를 발생시킨다. 이벤트는 스마트 컨트랙트가 수행되었을 때 해당 수행 내용과 관련된 사용자가 인지할 수 있도록 만들어지는 짧은 로그이다. 함수 호출은 그림 6에서 QR Scan 후 Save를 누를 때 발생하게 된다.

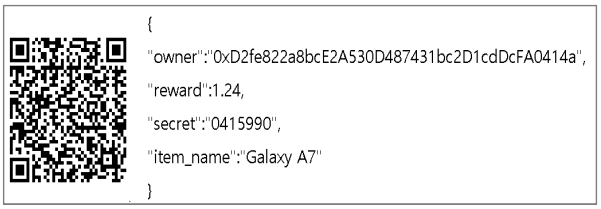

그림 5. 분실물에 부착되는 QR코드 데이터
Fig. 5. QR code data attached to lost property

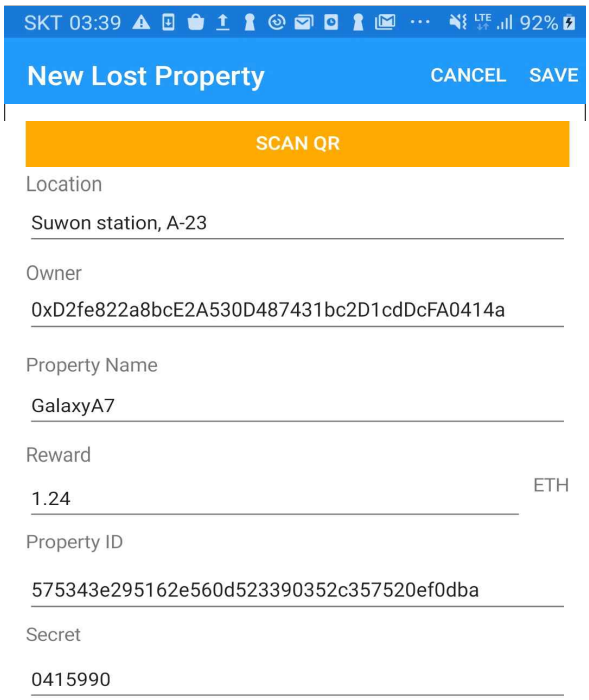

그림 6. 모바일에서 QR코드를 스캔하여 분실물 신고 등록
Fig. 6. Register the lost property by scanning the QR code

Event: LostFound
Arguments:
- deviceID: "575343e295162e560d523390352c357520ef0dba"
- hsecret: "0x745cec...0ad9"
- finder:"6361168Efa922D80bFA320ad019a127b53E3078F"
- location: "Suwon station, A-23"

그림 7 습득자가 최초로 발생시키는 이벤트
Fig. 7. First event raised by finder

이더리움 기반의 앱은 주기적으로 블록체인에서 새로 발생된 이벤트가 존재하는지 폴링(Polling)하여 새롭게 발생한 이벤트들을 감지한다. 소유자는 해당 이벤트를 읽고 이벤트에 표시된 보관함으로 이동하여 자신의 분실물이 들어있음을 확인해야 한다.

소유자는 앱 또는 그림 8과 같은 사전에 자신의 분실물을 기록한 웹에서 분실물의 현황을 살필 수

있다. 분실물이 신고되면 Property Found 상태가 되며 자신의 물품이 어디에 보관되었는지 확인할 수 있다. 보관 장소로 이동한 소유자는 자신의 분실물이 보관되었는지 Check Device로 확인할 수 있는데, 이 버튼은 Device.CheckDevice(deviceID) 함수를 실행시켜 트랜잭션을 발생시킨다.

해당 트랜잭션은 그림 9의 ValidationSound 이벤트를 발생시키게 되어 소유자가 자신의 분실물이 올바르게 보관함에 들어있는지 확인할 수 있다. 이벤트에는 분실물 ID, 분실물이 가진 소리 파일 인덱스 번호가 포함된다. 기기가 이벤트에 기록된 요청에 맞는 소리를 발생시킴으로써 증명된다. 소유자의 상황이나 필요에 따라서 자신의 분실물의 보관 확인 과정을 생략할 수 있다.

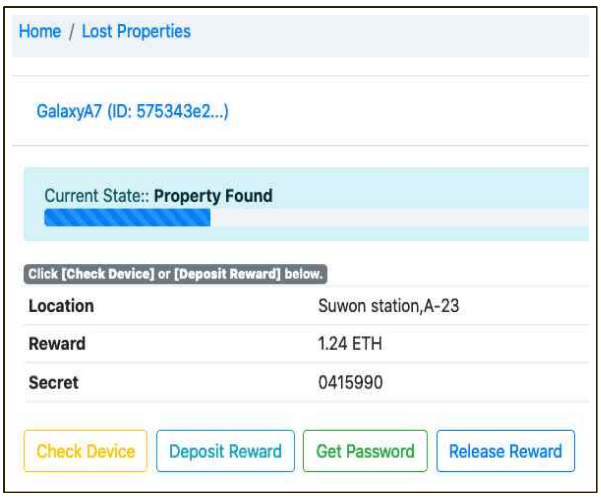

그림 8. 웹에서 분실물에게 신호 발생을 요청
Fig. 8. Request to ring the lost property by itself

Event: ValidationSound
Arguments:
- deviceID: "575343e295162e560d523390352c357520ef0dba"

그림 9. 소유자가 습득물을 확인하기 위한 이벤트
Fig. 9. Event for owner to check the lost property

3.4 분실물 사례 및 회수

소유자는 사례금을 예치하고, 분실물 사례에 대한 예치금이 등록되면 습득자는 분실물을 회수할 수 있도록 한다. 그림 3에서 7번 이후의 과정이 3.4에 해당되며 표 1은 3.4 부분에서 발생하는 흐름에 대한 요약이다.

소유자는 자신의 분실물이 보관된 보관함을 열 수 있는 비밀번호를 습득자에게 요청해야 한다.

습득자에게 보상이 지불 가능함을 보이기 위해 QR코드에서 명시한 reward 만큼의 eth를 컨트랙트에 예치하고 Escrow.depositReward(finder, reward) 함수를 통해 트랜잭션을 발생시키고 이를 통해 그림 10과 같은 RewardDeposited 이벤트가 발생된다.

습득자는 그림 12의 RewardDeposited 이벤트를 통해 예치금이 컨트랙트에 등록되었음을 확인할 수 있다. 예치금이 컨트랙트에게 전달되었다면 습득자는 보관함 비밀번호(pwd)를 QR코드의 secret과 XOR 연산한 값을 비밀번호로 제공하고 소유자와 예치금을 공동 소유하는 것으로 변경하여 소유자가 예치금을 인출하지 못하도록 한다.

Event: RewardDeposited
Arguments:
- deviceID: "575343e295162e560d523390352c357520ef0dba"
- finder: "6361168Efa922D80bFA320ad019a127b53E3078F"

그림 10. 보상 예치에 대한 기록을 남기는 이벤트
Fig. 10. Event to record a reward deposit

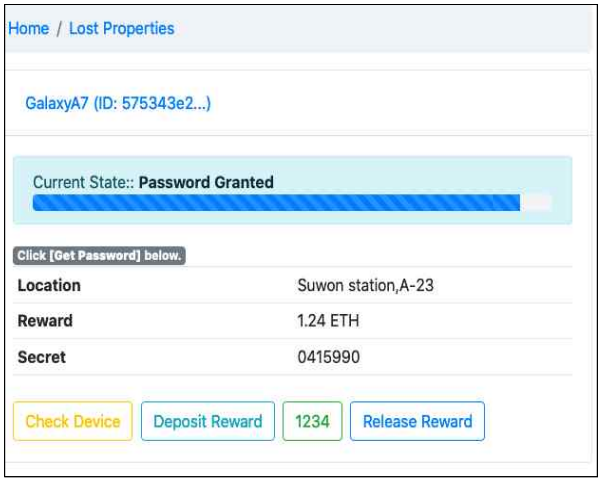

그림 11. 웹에서 비밀번호를 획득
Fig. 11. Acquire the password to open locker

Event: PasswordGranted
Arguments:
- deviceID: "575343e295162e560d523390352c357520ef0dba"
- finder: "6361168Efa922D80bFA320ad019a127b53E3078F"
- xorPassword: pwd XOR secret

그림 12. 비밀번호 제공 사실을 기록하는 이벤트
Fig. 12. Event to record password provided by finder

Escrow.exchangePwReward(xpw)함수 수행을 통해 소유자가 비밀번호가 제공되었음을 알 수 있도록 PasswordGranted 이벤트를 발생시킨다.

소유자는 이벤트에 기록된 비밀번호를 그림 11의 웹에서 확인할 수 있다. 제공된 비밀번호를 이용하여 보관함을 해제하고 분실물을 습득한다.

분실물을 습득한 후, 소유자는 불완전 상태로 습득자에게 전달된 보상을 풀어주어 습득자에게 완전한 형태의 보상을 제공한다. 보상 전달은 습득자가 별도의 행동을 하지 않아도 전달되며 보상을 완전하게 제공하였음을 확인할 수 있도록 Withdraw() 트랜잭션을 발생시켜 그림 13과 같은 RewardGranted 이벤트를 생성한다.

```
Event:  RewardGranted
Arguments:
- deviceID: "575343e295162e560d523390352c357520ef0dba"
- owner: "D2fe822a8bcE2A530D487431bc2D1cdDcFA0414a"
- finder: "6361168Efa922D80bFA320ad019a127b53E3078F"
```

그림 13. 보상 전달 사실을 기록하는 이벤트
Fig. 13. Event to record the released reward

위의 이벤트까지 전달함으로써 소유자와 습득자는 안전하게 분실물을 교환하고 보상을 지급받을 수 있다. 소유자가 RewardGranted 이벤트를 발생시키지 않을 경우, 습득자는 실제 시간으로 약 보름이 경과한 시점에서 강제성을 띈 함수를 통해 보상을 습득할 수 있다.

제안 모델은 그림 1에서의 에스크로와 다른 형태의 흐름을 갖는다. 이는 구매자-판매자 관계가 물건을 소유한 이에게 요청을 전달한다면, 소유자-습득자 관계는 물건을 소유한 이가 먼저 제안하는 형태이기 때문이며 제안 모델의 에스크로는 기존 모델과의 차이점을 인지하고 다른 형태로 흐름을 구성하였다.

그림 14의 흐름 1번과 5번 과정이 가장 큰 차이를 나타내는데, 분실물 보상 및 회수는 습득자로부터 흐름이 시작되기 때문에 진행 방향의 차이를 가진다. 5번에서 소유자는 습득자가 비밀번호를 제공하는 조건으로 보상금을 임시적으로 공동 소유하게 되므로 진행 방향의 차이를 갖게 되며, 기존의 구매자가 물품 확인을 하는 과정 및 보상금 예치가 2번에 포함되어 안전성을 유지하게 된다.

3.5 기존 모델과의 비교

제안 모델은 소유자의 개인정보와 사용성 개선, 그리고 사용자 간에 안전하게 분실물을 회수하는 방법에 중점을 두었으며 표 2가 이를 설명한다.

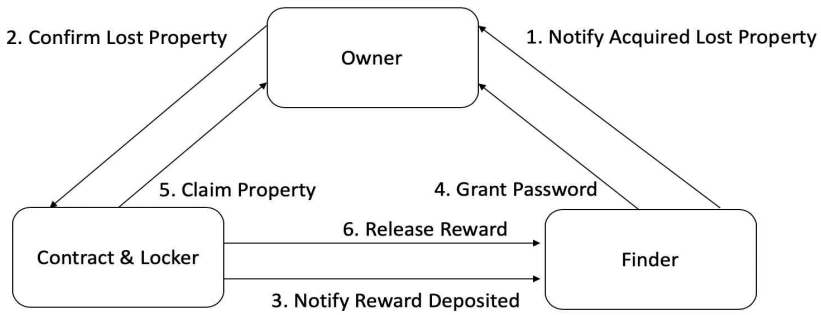

그림 14. 분실물 보상/회수 흐름도
Fig. 14. Lost property claim and reward flow

표 2. 기존 모델과 제안 모델과의 비교
Table 2. Comparison between proposed model and traditional models

Attribute	RFID based model[3]	Bluetooth LE based model[4]	Our model
Architecture	Centralized	Centralized	Decentralized
Cost	RFID&Server management (Medium)	Bluetooth LE module (High)	Transaction fee (Low)
Privacy	Phone number, address (severe)	No privacy leak (safe)	Ethereum account, property ID (safe)
Loss Awareness	Receive notification to acquirer through phone (good)	No notification (bad)	Receive notification to acquirer through blockchain (good)
Escrow	by moderator (Good)	No escrow (Bad)	by contract (Good)

제안 모델은 이더리움 블록체인에 데이터를 업로드할 때 필요로 하는 트랜잭션 수수료뿐이다. 이는 RFID 모듈을 등록하려는 소유물마다 구매해야 하거나 Bluetooth LE처럼 등록하려는 기기가 기능을 지원해야 하는 등의 제약이 존재하지 않는다. 분실물을 돌려받기 위해 제공하는 정보도 중앙화된 기관이 관리하는 형태가 아니며, 주소와 같이 민감한 정보를 제공하는 RFID 기반 모델과 달리 이더리움 계정처럼 특정되기 어려운 정보들이므로 안전하다. 분실물이 발생하는 시점을 인지하는 것 역시 중요한데, 제안 모델은 습득 시점에 이를 고지하는 것이 가능하므로 분실물 회수에 좀 더 기여할 수 있다.

Ⅳ. 제안 모델 보안 분석

제안 모델은 사용자 개인정보 보호와 분실물 습득 사실에 대한 증명, 유실물과 보관 사실에 대한 사기 방지, 그리고 제 3자에 의한 분실물 도난 방지를 수행할 수 있으므로, 사용자 정보를 보호할 수 있고 결함 없이 교환을 수행하게 된다.

4.1 사용자 개인정보 보호

기존 모델들은 분실물을 회수받기 위해 자신의 전화 번호를 이용했다. 제안 모델은 습득자가 사용자에게 돌려주는 과정에서 사용자의 개인 정보를 이용하는 대신 deviceID와 이더리움 계정을 사용하여 소유자와 습득자가 직접적으로 연락할 수 있다. 이더리움 계정은 사용자가 임의로 생성 가능한 ID이므로 실제 사용자를 추론하기 어렵다. deviceID와 device도 임의로 생성 가능하며 실제 분실물에 대한 형태나 개략적인 종류만을 물건명(item_name)에 등록하거나, 다양한 계정을 사용하여 등록하는 방법이 존재하므로 계정 주인의 실제 부를 예측하는 것 또한 불가하다.

4.2 습득 사실에 대한 증명

분실물 습득은 소유자에게 가장 큰 관심사이며 보상을 통해 습득자에게 분실물을 돌려받고자 한다. 보상은 회수를 전제로 하는 행위이기 때문에 습득자는 분실물 소유를 증명할 수 있어야 한다.

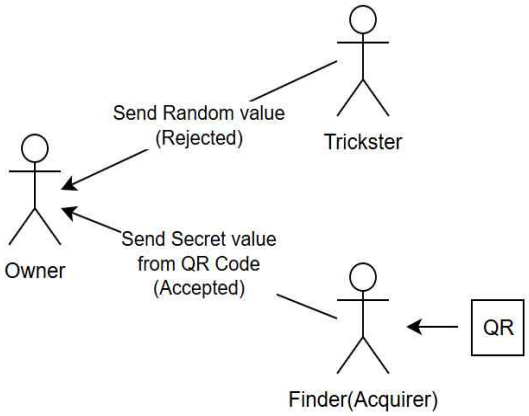

그림 15. 습득 사실에 대한 증명
Fig. 15. Proof about acquisition

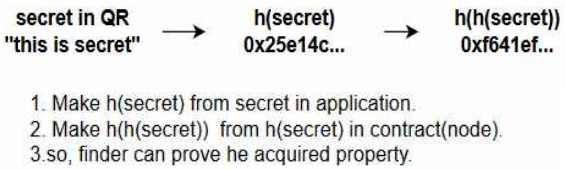

그림 16. hhsecret 생성 과정
Fig 16. Creation method from secret

그림 15에서 습득자는 분실물의 QR코드를 읽고 QR코드에 포함된 비밀 값을 이용하여 소유자만 생성할 수 있는 h(h(secret))를 동일하게 생성할 수 있음을 보임으로써 습득 사실을 증명한다. 공격자는 실제로 QR코드를 확인할 수 없기 때문에 그림 16과 같이 h(h(secret))를 만들기 위해 필요로 하는 비밀 값을 임의로 무작위 대입해야 한다.

무작위로 생성한 h(h(secret))를 트랜잭션으로 이더리움에 전파해야 하는데, hash 함수는 단방향성(one-wayness, preimage resistance)와 충돌 저항성(collision resistance)을 지니기 때문에 이를 위한 공격이 어렵다. 단방향성은 ouput으로부터 input을 예측할 수 없음을 의미하며 hash의 결과로 나온 digest를 아는 것으로 digest의 원본값을 아는 것이 불가함을 뜻한다. 충돌 저항성은 하나의 값을 hash로 만들 때 다른 값을 이용하여 동일한 hash를 만들어내기 어렵고 모든 값들에 대하여 hash값이 균등하게 분포한다.

Keccak256 함수는 상기한 특성들을 만족하므로 [14] 공격자는 secret 없이 hhsecret을 만들 수 없으며 hsecret으로 secret을 유추할 수 없다.

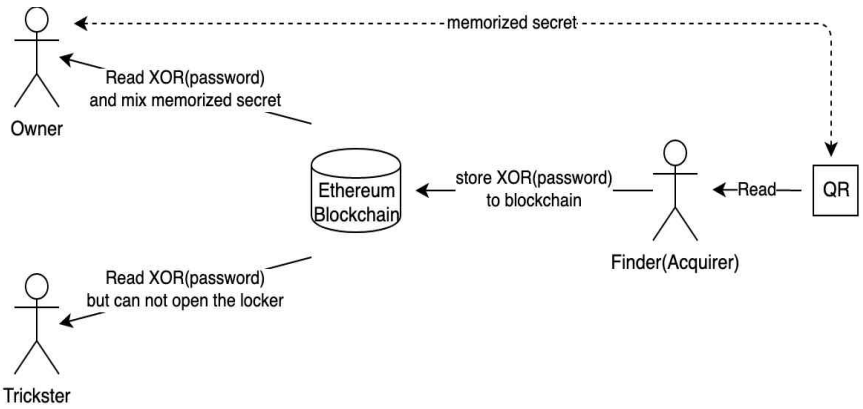

그림 17. 제 3자로 인한 습득물 도난 방지
Fig. 17. Prevention of theft of acquisitions by others

4.3 유실물 및 보관함 비밀번호 속임수 방지

습득자는 사전에 소유자에게 알린 보관함에 분실물을 보관하고 이를 열기 위한 올바른 비밀번호를 소유자에게 전달할 의무가 있다. 소유자는 습득자에게 비밀번호를 전달받음과 동시에 습득자에게 보상금을 지불하기 때문에 이 과정에서 소유자에게 올바르지 않은 비밀번호를 전달할 경우 소유자는 습득자에게 무의미한 보상을 전달하게 된다. 이를 방지하고자 블록체인을 통해 기기에게 특정 소리를 송출하도록 하고, 해당 소리를 근거로 사용자가 보관함 내부에 분실물이 들어있는지 판단할 수 있도록 한다. 소유자는 소리를 근거로 보상을 지불할 것인지 판단해야 하며 실제 분실물이 들어있지 않다고 판단될 경우 보상을 예치하지 않음으로써 무의미한 손실을 줄일 수 있다. 이 과정은 기존 에스크로에서의 물건 확인 과정과 같기 때문에 소유자의 선택에 따라 생략할 수 있다.

4.4 제 3자의 습득물 도난 방지

소유자와 습득자 사이에서 발생하는 컨트랙트의 내용은 공개 블록체인의 특성 때문에 모두가 읽을 수 있다. 제 3자가 컨트랙트 내 이벤트를 지속적으로 모니터링 한다면, 제 3자의 주변에서 발생한 분실물을 가로챌 수 있는 가능성이 있다. 이러한 도난 가능성을 방지하고자 그림 17과 같이 물리적인 QR 코드에 포함된 비밀 값을 사용하여 XOR 연산된 비밀번호(Password XOR secret)를 블록체인에 제공한다. 비밀 값을 모르는 제 3자는 올바른 XOR 연산을 수행할 수 없으므로 보관함을 열 수 없다.

V. 결 론

제안 모델은 블록체인 기반의 기존에는 없는 새로운 형태의 분실물 회수 모델이다. 기존 모델들보다 사용자가 사용하기 위한 금액적 부담이 적으면서 사용자의 개인 정보 없이 습득 사실을 알릴 수 있어 안전하게 분실 인지 시점을 앞당기고 이를 돌려받을 방법을 제공한다.

제안 모델을 활용하면 일련의 과정들을 통해 사용자들은 비대면으로 분실물을 회수하고 보상받을 수 있다. 소유자는 분실물을 습득자에게로부터 개인 정보 제공 없이 습득 사실을 전달받을 수 있고 습득자는 복잡한 과정과 연락 없이도 분실물을 전달하는 과정 속에서 분실물 회수에 대한 보상을 얻을 수 있다. 부가적으로, 모든 과정에서 분실물 처리를 위탁받은 특정 기관이 존재하지 않기 때문에 기존의 기관들이 본 모델을 활용할 경우, 분실물들로 인한 창고 보관 문제와 분실물 처리의 지역성 문제를 해결할 수 있다.

References

[1] National Police of Korea, "National Police Agency Lost and Found Management System", https://lost112.go.kr. [accessed: Nov. 20, 2019]
[2] YNA, "55% SRT Loss Recovery", https://www.

yna.co.kr/view/AKR20180312056400003 [accessed: Nov. 20, 2019]
[3] Elliot S. Klein, "Lost and found system and method", US6259367B1, 2000.
[4] James Buchheim, ArneHennig, "Locator beacon and radar application for mobile device", US9967713B2, 2014.
[5] Zibin Zheng, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 6th IEEE International Congress on Big Data, Honolulu, HI, USA, pp. 558-560, Jun. 2017.
[6] Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf. [accessed: Nov. 20, 2019]
[7] Shailak, Jani, "An Overview of Ethereum & Its Comparison with Bitcoin", International Journal of Scientific & Engineering Research, Vol. 10, No. 8, Feb. 2018
[8] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", https://github.com/ethereum/wiki/wiki/White-Paper. [accessed: Nov. 20, 2019]
[9] Martin Valenta, "Comparison of Ethereum, Hyperledger Fabric and Corda", Frankfurt School Blockchain Center, Jun. 2017.
[10] Andreas Unterweger, "Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum", 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) Paris, France, pp. 847-52 Aug. 2019.
[11] Woori Bank, "About Escrow Service", https://svc.wooribank.com/svc/Dream?withyou=ESSIF0003. [accessed: Nov. 20, 2019]
[12] Riham AlTawy, "Lelantos: A Blockchain-based Anonymous Physical Delivery System", 15th Annual Conference on Privacy, Security and Trust, Calgary, AB, Canada, 12pages, Aug. 2017.
[13] "web3.js", https://web3js.readthedocs.io/en/v1.2.5/ [accessed: Nov. 20, 2019]
[14] Imad Fakhri Al-shaikhli, Mohammad A. Alahmad, Khanssaa Munthir, "Hash Function of Finalist SHA-3: Analysis Study", International Journal of Advanced Computer Science and Information Technology, Vol. 2, No. 2, pp. 1-12, Apr. 2013.

저자소개

홍 성 호 (Seongho Hong)

2019년 2월 : 경기대학교 컴퓨터과학과(공학사)
2019년 3월 ~ 현재 : 경기대학교 컴퓨터과학(공학석사)
관심분야 : 블록체인

이 상 윤 (Sangyun Lee)

2014년 3월 ~ 현재 : 경기대학교 컴퓨터과학과(공학사)
관심분야 : 네트워크

박 지 우 (Jiwoo Park)

2017년 3월 ~ 현재 : 경기대학교 컴퓨터과학과(공학사)
관심분야 : 네트워크

김 희 열 (Heeyoul Kim)

2000년 2월 : 한국과학기술원 전산학사(공학사)
2002년 2월 : 한국과학기술원 전산학사(공학석사)
2002년 2월 : 한국과학기술원 전산학사(공학박사)
2009년 3월 ~ 현재 : 경기대학교 컴퓨터과학과 부교수
관심분야 : 정보보호, 암호학, 블록체인