The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 6, pp.21-26, Dec. 31, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.6.21
JIIBC 2023-6-4

콜드월렛 지갑 보안 강화를 위한 QR코드 기반 백업 방안에 대한 연구

A study on QR code-based backup methods to strengthen the security of Cold wallet Purse

최병훈[*], 이진용[**], 고남현[**], 전삼현[***]

Byoung Hoon Choi[*], JinYong Lee[**], Nam Hyun Koh[**], Sam Hyun Chun[***]

요 약 최근 디지털 자산으로 불리는 이더리움, 비트코인 등의 암호화폐가 자산으로 빠르게 인식되고 있다. 암호화폐는 실물자산과는 전혀다른 특성을 가지고 있어 신중하고 안전하게 다루어야 하지만 디지털 자산의 단점은 지갑의 개인 키를 아는 사람이라면 누구나 쉽게 해당 디지털 자산을 탈취할 수 있다. 시드카드를 분실하거나 도난 당한경우 또는 작성시 노출된 경우 다른사람이 습득한 시드카드를 이용하여 개인키를 복구하여 지갑을 사용 할 수 있기 때문에 보안에 매우 취약하다. 본 논문에서는 시드카드 작성에 필요한 니모닉 단어 제공시 QR코드를 이용하여 시드카드의 노출 및 분실, 도난에 대해 안전하게 작성하는 방식을 제안하므로 암호화된 자산을 안전하게 보호하고자 한다.

Abstract Recently, cryptocurrencies such as Ethereum and Bitcoin, which are called digital assets, Cryptocurrency has completely different characteristics from real assets and must be handled carefully and safely. But The disadvantage of digital assets is that anyone who knows the private key of the wallet can easily steal the digital assets. If the seed card is lost, stolen, or exposed when used, you can use the wallet by recovering the private key using the seed card acquired by someone else. In this paper We aim to safely protect encrypted assets by using QR codes when providing mnemonic words needed to create seed cards.

Key Words : Blockchain, cryptocurrency, Cryptocurrency Wallet, Information Security

Ⅰ. 서 론

1. 연구배경

디지털 자산의 하나인 암호화폐의 기본이 되는 것은 분산원장 기술로 데이터의 투명성과 무결성이 매우 중요하다. 암호화폐 거래의 기본이 되는 블록체인 구조는 많은 기업들이 이용하고 있는 중앙 집중형 시스템의 단점 및 한계성을 극복하기 위해 탈중앙화 시스템으로 되어있다.[1]

이러한 블록체인 자체기술 및 블록체인 기술기반의 서비스는 서버 없이 진행되는 서비스로 되며 이는 신뢰를

[*]정회원, 숭실대학교 정책경영학과 박사과정 IT
[**]정회원, 숭실대학교 정책경영학과 박사과정 IT
[***]정회원, 숭실대학교 정책경영학과 박사과정 IT
[****]정회원, 숭실대학교 정책경영학과 교수
접수일자 2023년 10월 31일, 수정완료 2023년 11월 30일
게재확정일자 2023년 12월 8일

Received: 31 October, 2023 / Revised: 30 November, 2023 / Accepted: 8 December, 2023
[*]Corresponding Author: shchun@ssu.ac.kr
Dept. of it policy and management, soongsil University, Korea

바탕으로 이루어 지고 있다. 특히 개인들의 디지털 자산을 관리하는데 많이 이용되고 있다.

서비스의 기본기술인 블록체인에서 키관리가 매우 중요하다. 키 관리에서 매우 중요한 부분은 개인키의 백업에 대한 보안이다. 개인키는 블록체인에 액세스하는 데 필요한 중요한 정보이지만, 분실하거나 탈취당하면 사용자의 자산이 도난되거나 본인도 모르게 이채가 되는 경우가 발생한다.[2] 개인키를 안전하게 보관하고 관리하기 위한 방법의 이해도가 부족하여 개인키가 손상되기 때문에 콜드월렛을 이용하여 안전하게 보관하는 방법이 개발되고 있다.

그러나 개인키를 안전하게 보관 및 관리하기 위해 사용되는 콜드월렛은 분실 및 파손에 대한 위험이 있다. 이러한 위험을 해결하고자 사용되는 니모닉 코드를 시드카드에 작성하지만 보안에 대한 이해도가 부족하여 니모닉 코드 전체가 노출되어 지갑자체가 탈취되는 경우가 발생할 수 있다.

2. 연구목적

개인키 복구의 방법인 니모닉은 사람들이 정보를 기억하는 데 도움이 되는 기억 보조 도구이다. 단어 목록부터 복잡한 공식까지 무엇이든 기억하는 데 사용된다.

니모닉은 각 줄의 첫 글자가 목록에 있는 단어를 나타내는 시나 문구인 Acrostic방법과 숫자와 관련된 단어를 제시하는 페그 단어, 기억하고 싶은 정보에 대한 이미지를 저장하는 시각적 이미지 등 다양한 유형이 있다. 다양한 유형 중 니모닉단어의 장점으로는 사용자가 암호화키와 같은 복잡한 정보를 친숙한 단어나 문구와 연관시켜 보다 쉽게 기억할 수 있도록 한다. 또한 많은 암호화폐 지갑과 플랫폼은 표준화된 니모닉 단어 목록(BIP-39)을 따라 다양한 서비스 간의 호환성과 복구를 보장하는 장점이 있다.

그러나 누군가 작성된 니모닉 단어에 접근할 수 있는 잠재적 리스크와 안전하게 보관하지 않을 경우 물리적 도난이나 분실의 위험으로 인한 디지털 자산을 훔칠 수 리스크를 가지고 있다. 이러한 니모닉 단어를 기반으로 작성된 시드카드를 이용한 백업의 형태는 콜드월렛뿐만 아니라 메타마스크나 이더월렛등과 같은 소프트지갑의 백업용도로도 사용되고 있다. 각종지갑의 백업을 위해 사용되는 니모니 단어가 적혀있는 시드카드를 사진찍거나 화면 캡처 등 웹사이트에 입력하여 전자 데이터 저장소에 기록할 경우 랜섬웨어의 위협 및 악성코드등을 통한 유출이 될 수 있다. 암호화폐 지갑의 백업을 위해 이용되는 백업방식 중 개인 키의 백업 방식은 암호키 자체, 또는 키를 암호화 하여 보관하는 방식에 대해 사용자에게 위임하는 한계가 있다.[3] 암호화폐 지갑의 백업을 위해 사용되는 시드카드의 관리의 절차상 복잡도 높여 유출에 대한 리스크 해결방식은 다양하게 연구가 되고 있다. 그러나 기술적인 백업형태에 대해 다양한 연구가 미흡하여 니모닉 단어의 노출부터 보관까지의 과정을 기술적인 측면으로 연구하고자 한다. 이를기반으로 백업방식에 사용되는 시드카드를 안전하게 작성하여 암호화폐 지갑의 백업을 안전하게 사용할 수 있도록 기여하고자 한다.

II. 관련연구

1. 암호화폐 지갑의 기능적 정의

암호화폐를 보유하기 위한 지갑은 전통적인 은행 계좌에 돈을 보유하는 것과 유사한 과정이다. 새로운 암호화폐 소유자는 각각의 암호화폐 지갑을 등록해야 하며. 암호화폐 지갑을 등록하는 과정은 전통적인 은행에서의 신규계좌 등록과는 다르다. 전통적 은행과는 다르게 암호화폐를 보관 및 관리하는 지갑의 경우 기존 은행계좌 개설과는 다르게 분산형 네트워크를 기반으로 암호화폐 지갑을 만든다. 또한 개인의 신원을 검토할 관리주체가 없이 분산네트워크에 저장된다. 보유중인 암호화폐 지갑의 소유권을 주장하려면 해당 암호화폐 지갑의 개인 키가 있어야 한다. 암호화폐 지갑의 개인 키는 본질적으로 암호화폐의 소유권을 정의하므로, 안전하게 보호되어야 한다. 개인 키는 컴퓨터나 인터넷을 통해서만 액세스할 수 있고 일반적으로 핫 스토리지라고 하는 컴퓨터 파일에 개인키 암호화 보관 및 분산 보관, 키관리 솔루션 도입하여 보관한다.[4] 그러나 핫 스토리의 보안이슈가 발생하여 USB 드라이브나 종이에 쓰여진 것과 같이 오프라인으로 유지되는 소위 콜드월렛를 사용한다. 콜드월렛을 사용하는 경우 해커가 비트코인 지갑의 키를 얻을 수 없고 분실 및 노출에 대한 보안 침해의 위험을 최소화하기 때문이다.[5] 콜드월렛의 개인키는 여러방식으로 저장이 되어지며 개인키의 가용성을 위해 파일의 백업방식 및 니모닉 단어등을 통해 키를 저장하기도 한다. 개인키를 복구하기 위한 방식으로 시드카드에 니모닉 단어를 작성 및 보관하여 지갑의 복호화가 필요시 시드카드에 작성된 니모닉 단어를 지갑 설정 단계에서 입력하여 지갑을 재사용할 수 있다.

2. 개인키 관리기술

ECDSA를 이용하여 암호화폐에 많이 사용되는 각종 클라이언트 지갑들의 키에 대해 생성 및 저장과 키 사용 영역에서 사용하는 키 관리 기술들을 정리하였다.[6] 암호화폐 영역에서 사용되는 클라이언트의 지갑에 대해서 공개된 자료도 제한적 이기에 때문에 수집이 가능한 암호화폐 영역에서의 키 관련 자료를 표1과 같이 조사를 수행하였다.

표 1. 암호화폐 클라이언트 지갑의 개인키 관리 기법
Table 1. Private key management of cryptocurrency client wallet

지갑구분	키 저장소		키 사용
	키저장소 가용성측면	키저장소 기밀성측면	
Bitcoin Core (S/W)	FileBackup	Password	-
MetaMask (WEB)	Mnemonic Code	Password	-
Ledger Nano (ColdWallet)	Mnemonic Code	Secure Element	Secure Element
TREZOR (ColdWallet)	Mnemonic Code	Secure Element	Secure Element
Electrum (S/W)	Mnemonic Code	Password	MultiSig
Wemix Wallet(S/W)	FileBackup	Password	

암호화폐 클라이언트 지갑의 개인 키 관리 기법에서 주요 내용인 키 저장은 가용성 및 기밀성이 중요하다.

키 저장소(가용성) : 사용중인 클라이언트에서 키 복구 솔루션을 이용한 가용성을 확보하기 위해 니모닉 코드를 사용 하였다. 각 지갑의 구체적인 사용동작은 다르지만 근본적으로 지갑 사용자를 통해 BIP39를 사용하여 키 생성에 사용되는 시드를 일련의 단어 조합으로 추가 및 변경하고 해당 단어를 보관하도록 하였다.

키 저장소(기밀성): 기밀성과 무결성 보장을 위한 개인키의 저장 기술은 일반적으로 하드웨어 클라이언트에서 동일한 기술을 사용 함께 제공되었다. 개인키는 암호화되어 저장소에 보관는 소프트웨어 타입에서는 서명생성 과정에서 사용자가 직접 입력하는 패스워드로 복호화하여 사용하는 패스워드 방식을 사용하였다.[7]

3. 콜드월렛 개인 키 백업의 보안 위험성

핫월렛보다 상대적으로 보안에 안전하다는 판단되는 콜드월렛의 경우 개인 키 백업 방법으로 가장 기본적인 방법은 사용자의 개인키를 출력된 종이에 작성하여 보관함에 넣어 보관한다. 이러한 방식은 네트워크등을 통한 해킹 공격을 근본적으로 차단할 수 있다.

콜드월렛 내에서 생성되는 모든 키는 하나의 정보인 마스터 시드로부터 생성하도록 구성된다. 마스터 시드를 사용자가 읽을 수 있는 단어로 치환하여 제공해주고, 콜드월렛을 잃어버려도 단어만 알면 복구할 수 있도록 돕기위한 방법이 바로 니모닉 단어(mnemonic code)이다.[8] 니모닉 단어는 기존 종이로 출력하여 백업을 하던 방식보다 발전하여 개인키를 쉽고 편리하게 사용자가 관리할 수 있도록 사전에 정해진 단어들의 조합으로 개인키로 변환시킨다. 개인키는 주변에서 쉽게 기억될 수 있는 여러개의 단어들의 조합으로 변환되어 사용자 입장에서 쉽게 개인키를 관리할 수 있다. 이러한 방식은 그림1과 같이 대다수 콜드월렛의 복구 수단 및 메타마스크, 이더월렛등과 같은 지갑서비스의 개인 키 복구용으로 사용한다.

그림 1. 지갑서비스의 니모닉코드
Fig. 1. Mnemonic code of Wallet Service

콜드월렛으로 사용하는 경우 하드웨어의 손상 또는 하드웨어가 분실을 대비하기 위해 그림 2와 같은 시드카드에 니모닉 코드를 작성한다. 동일한 제품으로 구매 후 지갑 소프트웨어를 다시 다운로드 한 후 백업용으로 기록되어 있는 니모닉 코드를 입력한다. 이후 새로운 암호화폐지갑을 다시 사용할 수 있게 된다.

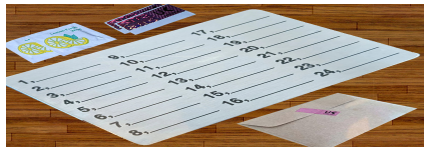

그림 2. 콜드월렛의 니모닉시드
Fig. 2. cold wallet mnemonic seed

그러나 편리하게 백업을 하던 니모닉 코드를 저장한 시드카드의 분실 및 파손, 노출등의 위험이 존재한다. [9] 니모닉 시드가 훼손되거나 분실 후 타인이 니모닉 시드를 발견한 사람이 복구를 할 경우 기존의 지갑에 보관되어 있는 모든 암호화폐 자산에 대해 빼앗거나 임의의 지갑으로 전송하여 사용할 수 있다. 콜드월렛의 백업에 사용되는 시드카드 작성 시 제공되는 단어는 자연어로 보여지는 단어들이므로 작성 시 외부에 노출이 가능한 위험으로부터 안전하지 않다.

기본적인 개인 키의 백업으로 사용되는 방법은 사용자를 식별할 수 있는 개인키를 보관 또는 출력하여 각종 해킹 등 네트워크를 통한 탈취공격을 근본적으로 차단할 수 있다. 복잡한 개인키가 일반적인 단어로 나타내어 쉽게 기억될 수 있는 일정 단어들의 조합으로 이용되기 때문에 사용자들은 개인키를 더 쉽게 관리할 수 있으며 암호화폐 지갑에서 현재 많은 복구 수단으로 니모닉 코드를 이용하고 있다. 니모닉 코드를 이용한 키백업은 사용자에게 안전성을 의존하는 한계가 있다. 이러한 개인키의 안전한 백업방식 및 안전한 복구를 위한 방법에 대해 활발히 연구되고 있다.[10]

이에 본 연구는 자연어로 제공되는 니모닉 코드를 QR코드로 전환하며 개인키가 저장되어 있는 전용 단말기에서만 보여지는 방식을 사용하여 보안을 강화하여 콜드월렛의 가용성 및 기밀성을 강화하고자 한다

Ⅲ. 본 론

본 논문에서는 기존에 콜드월렛에서 백업방식으로 사용하고 있는 니모닉 코드에 대해 QR코드를 이용한 안전한 백업모델 방안을 제언한다.

1. 콜드월렛의 백업방식 및 구성

콜드월렛에서 개인키를 백업할 때 제공되는 니모닉단어 24개를 콜드월렛 화면에서 보여준다. 다음으로 콜드월렛 설정시 콜드월렛회사에서 제공되는 종이로 되어 있는 니모닉단어를 기록하는 니모닉 시드에 각 단어별로 작성하게 된다. 이때 가장많은 시간이 소요되지만 니모닉 단어 기록 시 주변의 사람들로 하여금 노출되는 위험과 기록 후 잘못된 보관으로 인한 니모닉 시드의 분실을 통해 콜드월렛의 모든 암호자산이 분실 또는 암호화폐 전송이라는 리스크가 발생할 수 있다.

이에 대해 백업시 보여주는 니모닉 단어를 노출시키지 않고 QR코드를 이용한 백업키 방식을 이용한다. 해당 단어를 의미하는 QR코드를 보여줌에 따라 주변의 사람들에게 니모닉 단어가 노출되지 않고도 시드카드와 동일한 백업체계를 가지게 된다. QR코드를 통해 백업키를 저장 및 이용은 다음과 같은 특징 및 절차를 보여준다.

가. 니모닉단어의 노출 리스크에 대해서 보안강화를 위해 QR코드로 보여지게 되어 24개 단어가 어떤 단어인지 직관적으로 인식할 수 없게 된다. QR코드를 지정된 스마트폰 또는 테블릿으로 QR코드를 인식 및 저장하게 된다.

나. 분실하거나 파손되기 쉬운 종이로 된 니모닉 시드의 리스크를 해결하기 위해 QR를 통해 저장된 니모닉단어는 스마트폰에서 인식하게 한다.

다. 스마트폰에 저장된 니모닉 단어의 보안성을 강화하기 위해 24개의 니모닉 단어를 의미한 QR코드를 인식 후 설정된 개인키를 통해 다시한번 암호화 처리하여 스마트폰 분실뿐만 아니라 노출의 위험성에도 보안이 강화된다.[11]

2. 니모닉문장의 암호화 처리

가. 니모닉문장의 카이사르 암호화 처리

제공된 니모닉문장에 대해서 카이사르 암호화 방식으로 알파벳과 같은 양의 정수키인 1부터 26까지키를 가지며, 니모닉 단어를 알파벳의 정수 키만큼 떨어진 치환된 알파벳 메시지를 표시한다.

K : 정수키, p: 평문, c는 암호화 된 암호문

c= E(k, p)는 키와 평문을 암호화를 진행할 경우 C가 표현되며 수식으로 나타내면 아래와 같이 나타난다.

$$c = E(k, p) = (p + k) \bmod 26$$
$$p = D(k, c) = (c - k) \bmod 26$$

이렇게 카이사르 암호화 방식을 통해 보안성을 강화하는 연구는 지속적으로 이루어지고 있다.

나. 암호화된 단에 대해서 QR코드 생성

카이사르 암호화 방식으로 변환되어 생성된 단어에 대해 다시한번 QR코드로 생성을 하여 백업을 하는 단계에서는 니모닉 문장이 시각적으로 표시가 되지 않아 외부에 노출되는 보안리스트에 대해서 안전하다.

3. 구현결과

그림 3과 같이 니모닉카드를 작성하기 위해 나노랫저

S를 기반으로 초기 설정시 랫저에서 니모닉 제시단어 24개의 단어 중 1번째 니모닉 제시단어, 13번째 니모닉 제시단어, 20번째 니모닉 제시단어를 이용하였다.

그림 3. 나노랫저 콜드월렛의 니모닉시드 단어
Fig. 3. Nano_ledger Cold Wallet Mnemonic Words

나노랫저에서 제시된 단어를 카이샤르 암호화 처리를 위해 정수키 K는 동일하게 3으로 설정하였다. 이후 카이사르 암호화 처리된 단어를 AES-256알고리즘을 통해 재암호화 처리하였다.

암호화 처리된 문장을 기반으로 QR크로를 저장하여 안전한 시드카드 생성을 하였다. 다만 해당 연구에 대해 24번이 아닌 3회 반복한 실험을 시행하였다

표 2. 니모닉단어에 대한 암호화처리 및 QR코드 생성
Table 2. Encryption processing and QR code generation for mnemonic words

ghost	jkrvw	gAAAAABkwdOSXkFLbwv7w5_PtD36TYGW4MHq-9p-4P0NVBFBCZ3fpLTjYzjZ-kSkXyYmvzalj1f1z5hscmWm6w4eGRcKg==	
summer	vxp phu	gAAAAABkwdPkEVfmhpi60JbFKI8dflmD4ZAS1zmZ8UfytQg3b3ZlRojgWDrpGx41COzm9x7Dg3PEsDh1vhbKvhANJssfcbkIYw==	
secret	vhfuhw	gAAAAABkwdPkEVfmhpi60JbFKI8dflmD4ZAS1zmZ8UfytQg3b3ZlRojgWDrpGx41COzm9x7Dg3PEsDh1vhbKvhANJssfcbkIYw==	

Ⅳ. 결 론

암호화폐 및 암호화폐의 지갑의 사용이 증가하고 있지만 보안사고의 방식도 다양해 지고 있다. 특히 암호화폐 지갑의 도난 및 파손을 방지하기 위해 백업의 형태도 다양해 지고 있다.

이에 본 논문에서는 암호화폐의 보안성을 위해 콜드월렛의 사용시 백업 단계에서 발생할 수 있는 취약점을 나열하고 이에대해 QR코드를 이용한 니모닉 단어의 사용함에 따라 니모닉 단어를 노출하지 않아 보안을 강화하는 방안을 제시하고자 하였다

이를 위해 콜드월렛을 설정 시 필수단계인 니모닉단어를 통한 백업에서 발생가능한 보안리스크에 대해서 나열하였으며 이를 통해 해결방안인 니모닉단어의 노출 및 니모닉카드의 분실을 최소화하는 스마트폰내 QR코드를 암호화 하는 방식을 구현하여 안전한 콜드월렛 사용방식을 제시하였다.

이에대해 암호화폐 지갑을 안전하게 백업을 하여 다양한 위험으로 부터 암호화폐의 사용할 수 있을 것으로 기대된다

References

[1] Alhazmi, Omar H., Yashwant K. Malaiya, and Indrajit Ray, ."Measuring, analyzing and predicting security vulnerabilities in software systems.", Computers & Security, Vol. 26, No. 3, pp. 219-228, May 2007. DOI:https://doi.org/10.1016/j.cose.2006.10.002

[2] Heeyoul Kim, “Analysis of Security Threats and Countermeasureson Blockchain Platforms”, Journal of KIIT. Vol. 16, No. 5, pp. 103-112, May 31, 2018 http://dx.doi.org/10.14801/jkiit.2018.16.5.103

[3] R. Soltani, U. T. Nguyen, andA. An,“Practical Key Recovery Model forSelf-Sovereign Identity Based DigitalWallets,” Proceedings of the 2019IEEE Intl Conf on Dependable,Autonomic and Secure Computing,Intl Conf on Pervasive Intelligenceand Computing, Intl Conf onCloudand Big Data Computing, Intl Confon Cyber Science and TechnologyCongress, pp. 320-325, Aug. 2019 DOI:https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066

[4] Seounghan Song, Suntae Kim, Jung-Hoon Shin, Jeong-Hyu Lee, “Recovery Phrase Management Scheme for Public Blockchain Wallets based on OTP”, The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 20, No. 1, pp.35-44, Feb. 29, 2020 DOI:https://doi.org/10.7236/JIIBC.2020.20.1.35

[5] Marek Palatinus, Pavol Rusnak, “Mnemonic code for generating deterministic keys”, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[6] Siwan Noh,1† Kyung-Hyune Rhee "A Private Key Management Guideline For Secure Blockchain-Based Services", Journal of The Korea Institute of Information Security & Cryptology, Vol.32, No.5,, pp. 908, Oct. 2022. DOI:https://doi.org/10.13089/JKIISC.2022.32.5.899

[7] G. Maxwell, A. Poelstra, Y. Seurin,and P. Wuille, “Simple Schnorrmulti-signatures with applications toBitcoin,” Designs, Codes andCryptography, vol. 87, no. 9, pp. 2139-2164, Feb. 2019. DOI:https://doi.org/10.1007/s10623-019-00608-x

[8] Buntings, JP (2017). What is a mnemonic seed? Merkle News. https:// themerkle.com/what-is-a-mnemonic-seed/

[9] Nanta Janpitak, Woraphon Lilakiatsakun, "The novel secure testament methodology for cryptocurrency wallet using mnemonic seed", Information Security Journal, A Global Perspective, Vol. 29, No. 4, pp. 169-182, Mar 2020. DOI:https://doi.org/10.1080/19393555.2020.1739788

[10] G. Li and L. You, “AConsortiumBlockchain Wallet Scheme BasedonDual-Threshold Key Sharing,” Symmetry, vol. 13, no. 8, pp. 1444,Aug. 2021 DOI:https://doi.org/10.3390/sym13081444

[11] Liu, Yue, Ju Yang, and Mingjun Liu. "Recognition of QR Code withmobile phones." 2008 Chinese control and decision conference. IEEE,2008. DOI:https://doi.org/10.1109/CCDC.2008.4597299

저 자 소 개

최 병 훈(정회원)

- 2004년 : 숭실대학교 산업정보시스템공학(석사)
- 2022년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 제로 트러스트, 정보보안, 블록체인, E-Commerce

이 진 용(정회원)

- 2008년 : 연세대학교 컴퓨터과학과(석사)
- 2022년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 제로 트러스트, 블록체인, 정보보호 및 개인정보보호 IT 및 정보보호 법률·정책

고 남 현(정회원)

- 2021년 : 연세대학교 IT정보보호법전공(석사)
- 2022년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 블록체인, 행태정보 프로파일링, 정보호호 및 개인정보보호 관리체계, 개인정보 보호 법률·정책

전 삼 현(정회원)

- 1989년 : 숭실대학교 법학과(석사)
- 1992년 : 프랑크푸르트대학교 법학과(박사)
- 1993년 ~ 현재 : 숭실대학교 법학과, IT정책경영학과 교수
- 관심분야 : 블록체인, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책