정 보 보 호 학 회 지
제34권 제4호, 2024. 8

국제 표준 ISO TC307 23353에 대한 고찰

유 순 덕*

요 약

ISO TC307에서 개발 중인 23353(Blockchain and distributed ledger technologies - Auditing guidelines: 블록체인과 분산원장 기술 감리 가이드라인) 표준은 기존 IT 시스템 감리와 달리 블록체인(BC, BlockChain)과 분산원장 기술(DLT, Distributed Ledger Technology) 기반 시스템에 대한 감리이다. ISO 23353의 주요 내용은 감리 원칙, BC/DLT 시스템의 위험, 감리 프레임워크, BC/DLT 감리 프로그램 관리 및 수행 절차 등이며. BC/DLT 감리에 있어 고려해야 할 위험, 통제 목표 및 통제 식별 방안 등에 대한 가이드 제공을 목적으로 한다. 한국이 주도적으로 개발하고 있는 ISO 23353은 블록체인 산업 활성화 촉진과 더불어 디지털 금융 산업에서 주도적 위치를 확보하는 데 긍정적으로 작용할 것이다.

Ⅰ. 서 론

블록체인과 분산원장 기술(DLT, Distributed Ledger Technology)이 여러 산업 분야에서 빠르게 확산 되고 있으며, 이에 이종 기술 간 상호운용성을 보장하고 보안성과 신뢰성을 확보하기 위해 관련 표준화의 중요성이 더욱 커지고 있다. 이러한 요구에 따라 블록체인 기술의 표준화를 위해 다양한 노력들을 기울이고 있으며 이러한 노력의 결과로, ISO TC307이 블록체인 및 분산원장 기술 표준화를 전담하는 기술위원회로 한국이 주도권을 가지게 되었고, 2016년 설립 이후 블록체인 분야의 국제 표준 개발을 주도하고 있다. ISO TC307은 현재 66개 ISO 회원국이 참여하여 블록체인 영역에 대한 표준을 개발하고 있다.

ISO TS23353 (Blockchain and distributed ledger technologies - Auditing guidelines: 블록체인과 분산원장 기술 감리 가이드라인)[1] 표준은 블록체인 시스템의 안전성과 신뢰성을 확보하기 위한 감리 가이드라인을 정의하며, 2023년 3월에 표준 개발을 시작하여 현재 WD(Working Draft) 개발 단계를 진행하고 있다.

본 논문을 통해 국내 기업들과 ISO 23353 표준 내용과 관련 정보를 공유함으로써 국내 블록체인 산업 발전 및 글로벌 시장 경쟁력 강화를 도모하고 나아가 블록체인 국제 표준 개발에 기여 하고자 한다.

Ⅱ. 블록체인과 분산원장 기술 감리

2.1. 블록체인과 분산원장

블록체인(BlockChain)과 분산원장(Distributed Ledger)은 종종 혼용되어 사용되지만, 서로 다른 개념이다.

블록체인은 분산원장의 한 종류로, 데이터를 블록 단위로 묶어 순차적으로 연결한 형태다. 각 블록은 이전 블록의 해시값을 포함하고 있어 데이터의 무결성을 보장하며, 합의 알고리즘을 통해 네트워크의 일관성을 유지한다. 블록체인은 체인 구조, 해시 링크, 합의 알고리즘 등의 특징을 가지고 있으며, 비트코인, 이더리움과 같은 암호화폐뿐만 아니라 스마트 계약, 공급망 관리 등 다양한 분야에서 활용된다.

분산원장은 중앙 서버 없이 여러 노드에 분산되어 저장하고 관리되는 데이터 베이스를 의미한다. 모든 참여자가 동일한 원장의 복사본을 가지고 있으며, 이 원장은 네트워크 전체에 걸쳐 동기화된다. 분산원장은 탈중앙화, 불변성, 투명성, 보안성을 특징으로 하며, 블록체인 외에도 해시그래프, DAG(Directed Acyclic Graph) 등 다양한 형태로 구현될 수 있다.

따라서 모든 블록체인은 분산원장이지만, 모든 분산원장이 블록체인은 아니다. 블록체인은 분산원장의 특징을 가지면서도 특유의 체인 구조와 해시 링크를 통해 더 높은 수준의 보안성과 투명성을 제공한다.

* 한세대학교 (교수, koreasally@gmail.com)

ISO 22739:2024 표준에서 이러한 차이점을 명확하게 제시하고 있다.

ISO 22739:2024, 3.6[2]에 따르면 블록체인(Blockchain)을 “distributed ledger with confirmed blocks organized in an append-only, sequential chain using hash links”로 정의하고 있다. 즉 해시 링크를 사용하여 추가 전용 순차 체인으로 구성된 블록이 있는 분산원장으로 정의하고 있다.

구조적으로 블록체인은 일련의 블록들로 구성되며, 각 블록은 이전 블록의 해시값을 포함하고 있어 변경이 어렵기 때문에 데이터의 무결성과 보안을 강화한다.

기술적으로 체인 구조를 이루고 있어 블록들이 선형으로 연결되어 있으며, 각 블록은 이전 블록과 암호학적으로 연결되어 있다. 또한, 탈중앙화 방식으로 모든 참가자가 동일한 사본을 가지며, 중앙 권한이 없고 한 번 기록된 데이터는 불변성을 가지므로 변경이 불가능하다. 또한, PoW(Proof of Work), PoS(Proof of Stake) 등의 합의 알고리즘을 사용하여 네트워크의 일치를 보장한다.

블록체인 주요 활용 사례로는, 비트코인, 이더리움과 같은 암호화폐, 스마트 계약, 공급망 관리 등 다양한 서비스가 있다.

ISO 22739:2024, 3.23[2]에 따르면 분산원장(distributed ledger)은 “ledger that is shared across a set of distributed ledger technology (DLT) nodes and synchronized between the DLT nodes using a consensus mechanism” 으로 정의하고 있다. 즉 분산원장(DL) 노드 집합에서 공유되고 합의 메커니즘을 사용하여 DL 노드 간에 동기화되는 원장으로 분산원장은 불변성, 변조 방지, 변조 방지 및 추가 전용으로 설계되었으며, 확인되고 검증된 거래의 최종 원장 기록을 포함한다.

구조적으로 분산원장(Distributed Ledger)은 중앙 데이터베이스 없이 여러 노드에 분산된 형태로 데이터를 저장하고 관리하는 시스템으로서 모든 참가자가 동일한 원장의 복사본을 보유하며, 이 원장은 네트워크 전체에 걸쳐 동기화된다.

분산원장은 항상 블록체인 형태를 취하지 않을 수 있고 블록체인 외에도 다양한 데이터 구조를 사용할 수 있다.

기술적으로 분산원장은 블록체인, 해시그래프, DAG(Directed Acyclic Graph) 등 다양한 형태로 구현

〔표 1〕 블록체인과 분산원장의 차이

구분	블록체인	분산원장
정의	• 분산원장의 한 종류로, 블록 단위로 연결된 형태	• 중앙 서버 없이 분산된 데이터베이스
구조	• 블록체인 구조인 데이터가 블록 단위로 묶여 순차적으로 연결된 체인 구조	• 블록체인 외 다양한 데이터 구조 허용 • 다양한 구조 (블록체인, 해시그래프 등)
유연성	• 특정한 체인 구조로 인해 고정적 구조	• 더 유연하고 다양한 구조 가능
활용 범위	• 주로 암호화폐와 스마트 계약에 사용	• 금융, 의료, 에너지 등 광범위하게 사용

될 수 있고 탈중앙화 형태로서 중앙 서버 없이 네트워크에 분산되어 관리 된다.

특히, 블록체인과 마찬가지로 다양한 합의 알고리즘을 사용하지만, 블록체인에 비해 더 다양한 접근 기술이 가능하고 특정한 구조에 제한되지 않으며, 다양한 방식으로 데이터를 관리할 수 있다. 블록체인 외에도 다양한 분산원장 기술이 금융, 의료, 에너지 등 다양한 산업에서 사용될 수 있다.

2.2. 감리와 감사

ISO 19011:2018, 3.1[3]에 따르면, 감리(감사, audit)는 “systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled“ 라고 정의하고 있다. 즉, 감리(감사)는 객관적인 증거를 획득하고 이를 객관적으로 평가하여 감리(감사) 기준이 어느 정도 충족하는지 결정하기 위한 체계적이고 독립적이며 문서화된 프로세스로 정의하고 있다.

국내는 감리와 감사라는 용어로 구분하여 사용하고 있지만, 영어는 Audit이라는 용어로 사용하고 있다. 국내의 경우 감리와 감사는 둘 다 조직의 활동을 검토하고 평가하는 과정이지만, 그 목적과 범위, 수행 방법에서 몇 가지 중요한 차이점이 있다.

감리(監理)는 목적 측면에서 프로젝트나 특정 활동이 계획대로 진행되고 있는지 확인하고, 품질과 규정 준수 여부를 검토하는 데 중점을 둔다. 주로 프로젝트 관리, 건설, 소프트웨어 개발 등의 분야에서 사용되고 있으며 특정 프로젝트나 작업의 전반적인 진행 상황을

모니터링 하고, 특정 기술적 사항이나 절차를 점검하는 활동이다.

수행 측면에서 주기적인 점검과 검토를 통해 진행 상태를 파악하고, 문제점을 조기에 발견하여 수정할 수 있도록 하고 종종 프로젝트 관리자나 기술 전문가가 감리를 수행한다.

이와 달리 감사(監査)는 목적 측면에서 조직의 재무 보고서나 운영 절차가 정확하고 신뢰할 수 있는지, 그리고 관련 법규나 규정을 준수하고 있는지를 독립적으로 평가한다. 주로 재무 감사, 내부 감사, 외부 감사 등의 형태로 수행된다. 즉 조직의 전체적인 운영, 재무 상태, 내부 통제 시스템 등을 포괄적으로 검토하고 재무 정보의 신뢰성, 운영의 효율성, 법규 준수 등을 평가한다.

수행 측면에서 감사인은 독립적인 위치에서 객관적으로 검토를 수행하며, 조직 내부나 외부에서 이루어질 수 있으며 감사 보고서를 작성하여 경영진이나 이사회, 주주 등에게 보고한다.

감리와 감사의 차이를 정리하면, 목적 관점에서 감리는 특정 프로젝트나 활동의 진행 상황을 점검하고 품질 관리에 집중하는 반면, 감사는 조직 전체의 운영 및 재무 상태를 평가하고 법규 준수를 검토한다.

범위 관점에서 감리는 특정 프로젝트나 기술적 활동에 집중되는 반면, 감사는 조직 전체를 대상으로 한다.

〔표 2〕 감리와 감사의 차이

구분	감리	감사
대상	• 진행 중인 활동이나 프로세스	• 이미 완료된 활동이나 결과
목적	• 활동이나 프로세스가 적절하게 수행되는지 평가, 개선점 찾음	• 규정 위반이나 부정 행위가 없었는지 확인하고, 책임 소재 규명
방법	• 활동이나 프로세스를 실제로 관찰하거나, 관련자를 면담하는 등 정성적 방법	• 회계 기록이나 증빙 서류 등의 객관적인 증거 검토
결과	• 개선점을 제시 및 개선 권고	• 규정 위반이나 부정 행위 발견 시, 조치 보고서 제공
예시	• 공사 현장의 안전 관리 감리 • IT 시스템에 대한 운용 평가 감리 • 의료기관의 의료 행위 감리	• 기업의 재무제표 감사 • 정부기관의 예산 집행 감사 • 비영리 단체의 운영 감사

수행 관점에서 감리는 주기적인 점검과 현장 검토를 통해 문제를 조기에 발견하고 수정하는 데 중점을 두는 반면, 감사는 독립적이고 체계적인 검토를 통해 포괄적인 평가를 수행한다.

2.3. 테스트와 감리

ISO 23353(Blockchain and distributed ledger technologies – Auditing guidelines:블록체인과 분산원장의 감리 가이드라인) 표준 개발 시 감리와 테스트에 대한 차이를 공식적으로 정리하지 않았지만, 이에 대해 다음과 같이 논의했다.

테스트(Test)는 소프트웨어나 시스템이 요구사항을 충족하는지, 오류가 없는지를 확인하는 것을 목적으로 하며, 주로 소프트웨어나 시스템의 기능과 성능, 보안 등 비기능을 대상으로 한다.

테스트는 소프트웨어 코드나 시스템을 실제로 실행하여 기능을 검증하며 다양한 테스트 단계(예: 단위 테스트, 통합 테스트, 시스템 테스트, 사용자 인수 테스트)를 통해 소프트웨어를 다양한 측면에서 검증한다. 테스트는 주로 소프트웨어 개발자나 품질 보증팀이 수행하며 특정 기능의 작동 여부, 성능, 안정성 등을 확인하는 데 집중한다.

이와 달리 감리는 프로젝트의 전반적인 진행 상황과 품질 보증 현황을 검토하는 것을 목적으로 프로젝트의 전반적인 측면(문서화, 절차, 규정 준수 등)을 포괄적으로 점검한다.

〔표 3〕 테스트와 감리의 차이

구분	테스트	감리
목적	• 소프트웨어나 시스템의 기능성과 신뢰성 등 검증	• 프로젝트의 전반적인 진행 상황과 품질 보증 현황 등 검토
범위	• 소프트웨어나 시스템의 기능 및 비기능(신뢰성, 성능, 사용성 등) 특성	• 프로젝트의 전반적 측면(문서화, 절차, 규정 준수 등)
방법	• 소프트웨어 코드나 시스템을 실행	• 문서 검토, 회의, 인터뷰 등
역할	• 개발자나 품질보증팀이 수행	• 프로젝트 관리자나 외부 전문가가 수행

2.4. 블록체인 및 분산원장 기술 시스템 감리와 IT 시스템 감리

블록체인과 분산원장 기술 시스템과 IT 시스템 가장 큰 차이는 중앙화(Centralization), 불변성(Mmutability), 투명성(Transparency)이다.

〔표 4〕 블록체인 및 분산원장 기술 시스템과 IT 시스템 차이

구분	블록체인 및 분산원장 기술 시스템	IT 시스템
중앙화	• 탈중앙화 방식으로 데이터는 단일 권한 없이 컴퓨터 네트워크에 분산	• 중앙 집중화 방식으로 데이터는 일반적으로 단일 엔터티(예: 회사, 조직)가 제어하는 중앙 서버에 저장
불변성	• 데이터가 블록체인에 추가되면 변경 또는 삭제가 매우 어렵거나 불가능 • 특정 DLT에 따라 데이터 불변인 경우 있음	• 데이터는 중앙화된 시스템 내에서 승인된 사용자에 의해 쉽게 수정되거나 삭제
투명성	• 퍼블릭 블록체인에서 사용자를 가명처리할 수 있지만, 누구나 거래 내역 확인 가능	• 중앙당국이 설정한 접근 통제 정책에 의존

Ⅲ. 블록체인과 분산원장 기술 감리 가이드라인 표준 개발 동향

3.1. 블록체인과 분산원장 기술 감리 표준화 개발 경과

ISO 23353 표준은 기존 IT 감리에서 다루지 않는 블록체인과 분산원장 기술을 대상으로 체계적인 감리 가이드라인을 제시하고자 한다.

ISO TC307에서 감리 가이드라인 표준 개발에 대한 요구사항은 인도에서 발의하고 검토를 했으나, 초기 논의 단계에서 논의가 중단되었다. 그 후 다시 캐나다에서 관련 아이디어를 발의를 했으나, 별다른 진척이 없었다. 2022년 국내 전문가들이 블록체인 시스템 감리에 대해 다시 논의를 시작했으며, 결국 2023년 3월부터 한국이 주도적으로 ISO/TC307/WG5에서 블록체인 및 분산원장 기술 감리 표준 개발을 논의하게 되었으며, ISO 23353(Blockchain and distributed ledger technologies - Auditing guidelines: 블록체인과 분산원장 기술 감리 가이드라인) 표준 개발 프로젝트 리더로 한국의 유순덕 교수(한세대)가 선임되었고, 표준안은 2023년 10월 14일 WG 멤버 투표를 통해 WD(Working Draft) 단계로 승인을 받았으며, 현재 WD 단계를 진행 중이다.

현재 블록체인과 분산원장 기술 감리 가이드라인 표준은 많은 국가들이 관심을 거지고 있으며, ISO 오프라인 회의에 가장 많은 국가에서 멤버들이 참여하는 회의 중 하나다. WG 멤버 중 가장 적극적으로 개발에 참여는 국가는 한국을 비롯해 스페인, 독일, 미국, 프랑스 등이 있다. 이 표준은 개발 이후에 감리 등 관련 시 장의에 적지 않은 영향을 미칠 것으로 예상된다.

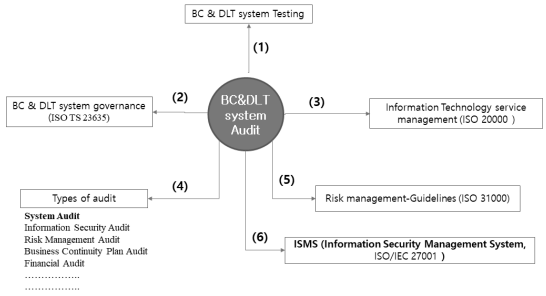
3.2. 블록체인과 분산원장 기술 감리 개발 범위

ISO 23353은 감리 원칙, BC/DLT 시스템의 위험, 감리 프레임워크, BC/DLT 감리 프로그램 관리 및 수행 등으로 구성되어 있으며, 블록체인 및 분산원장 기술(BC/DLT) 시스템 감리에 대한 지침을 제공한다.

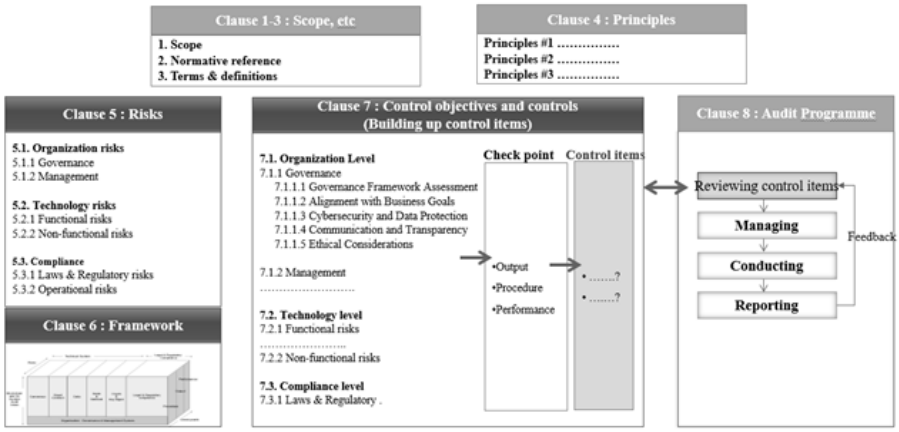
이 표준은 ISO 22739:2020(블록체인 및 분산원장 기술 - 어휘)[2], ISO 23257(블록체인 및 분산원장 기술 - 참조 아키텍처)[4], ISO 19011:2018(경영 시스템 감리 가이드라인)[3], ISO 23635:2022(블록체인 및 분산원장 기술 – 거버넌스 가이드라인)[5]를 참고로 하여 개발하고 있다.

[그림 1]은 23353 표준과 관련된 표준들이다. 블록체인과 분산원장 기술 감리는 테스트, 거버넌스(ISO TS23635), 관리(ISO 20000), 위험관리(ISO 31000) 정보보호(ISMS, ISO/IEC 27001) 등과 연관되어 있다.

[그림 2]는 개발 중인 ISO TC307 23353 표준 구조로서 감리원칙, 감리 위험요인, 감리 프레임워크, 감리 통제방안과 운영방안 및 수행방안으로 나누어 개발하



〔그림 1〕 23353 표준 개발과 관련된 분야



〔그림 2〕 표준 개발 중인 ISO TC307 23353 표준 구조

고 있다.

3.3. 블록체인과 분산원장 기술 감리 원칙

ISO 23353 표준에서 개발하는 감리 원칙은 감리자의 업무 수행 측면과 블록체인과 분산원장 측면으로 나누어 정리하고 있다. 감리 수행 측면에서 성실성, 공정한 발표, 정당한 전문적 관리, 기밀성, 독립성, 증거 기반 접근 방식, 위험 기반 접근 방식 등을 정의하고 있다. 탈중앙화인 DLT의 원장은 네트워크의 여러 노드(컴퓨터)에 의해 운영되고 있으며, 효율성 측면에서 성능과 확장성 제공 문제와 상호운용성 측면에서 상호운용성 대한 요구사항이 있다.

3.4. 블록체인과 분산원장 기술 감리 위험 요인

블록체인과 분산원장 기술 감리 시 고려해야 할 블록체인 및 DLT 시스템의 위험 요인을 정의하고 있다. 위험 요인을 3가지로 분류하여 조직적 위험, 기술적 위험, 규정적 위험으로 구분했다. 조직적 위험의 하위 항목으로 거버넌스 위험과 경영 리스크를 제시하고 기술 위험 하위 항목으로 기능적 위험과 비기능적 위험을 제시했다. 그리고 규정적 위험은 법률 및 규제 위험과 운영 위험 요인 항목을 검토하고 있다.

위험 요인에 필요한 보안 제어 정의하기 위해 ISO 23257의 내용을 기반으로 DLT 시스템에 대한 아키텍처 고려사항을 참고하고 있다. 통제 목표별 통제 영역은 다음 표에 따라 분류하고 개발이 진행되고 있다.

〔표 5〕 보안 및 제어 항목

Controls				
General	Public	Private	Permis sionless	Permis sioned

3.5. 블록체인과 분산원장 기술 감리 운영과 수행방안

ISO 23353 표준에서 감리 가이드라인은 감리 운영관리 방안과 감리 수행방안으로 구분하여 제시하고 있다.

감리 운영관리 방안은 하나 이상의 경영시스템 표준 또는 기타 요구사항에 대한 감리를 포함할 수 있는 감리 프로그램을 수립해야 하며, 개별적으로 또는 결합하여(통합 감리) 수행해야 한다.

감리 프로그램의 범위는 감리 대상의 규모와 특징, 기능, 복잡성, 위험과 기회의 유형, 관리 시스템의 성숙도 수준에 따라 결정해야 한다. 이에 따라 감리 수행방안은 조사준비, 감리수행, 수집된 결과 리뷰 등의 단계를 고려하고 있다.

Ⅳ. 결 론

ISO TC307에서 개발 중인 블록체인과 분산원장 기술 감리 가이드라인은 국제 표준으로서 블록체인 서비스에 대한 시장의 신뢰성을 높이는 데 기여할 수 있다. 특히, 한국을 비롯한 미국, 영국, 스페인, 독일 등 여러 국가들이 표준 개발에 적극적으로 참여하고 있으며, 블록체인 기술의 발전과 서비스 활성화에 긍정적인 영

향을 미칠 것이다.

한국이 블록체인 및 분산원장 기술 감리 가이드라인 표준 개발을 주도함으로써, 국제 표준을 선도하는 위치를 공고히 하고 국내 블록체인 기업들의 경쟁력을 강화하고, 글로벌 시장 진출을 지원할 수 있는 긍정적인 효과를 기대할 수 있다. 또한, 블록체인 기술 기반의 디지털 금융 서비스의 신뢰성을 확보하고, 국내 디지털 금융 산업의 경쟁력을 강화할 수 있고, 나아가 국제적인 기술 리더십을 확보함으로써 국가 경쟁력을 높일 수 있다.

따라서 한국은 블록체인 및 분산원장 기술 감리 가이드라인 표준 개발을 통해, 국제 표준 개발의 주도권을 확보하는 동시에 국내 블록체인 기업들의 요구사항을 국제 표준에 적극적으로 반영해야 한다. 그리고 다양한 채널을 통해 표준 개발 현황을 공유하고, 관련 기업들의 의견을 수집함으로써, 국내 기업들이 국제 표준에 대한 이해를 높이고, 표준 개발 과정에 참여할 수 있도록 보다 적극적인 지원이 필요하다.

참 고 문 헌

[1] ISO/TC307 N243 ISO TC307 WG5 TS_23353_B CDLT Auditing guidelines, 2024.06.

[2] ISO 22739:2024, Blockchain and distributed ledger technologies - Vocabulary

[3] ISO 19011:2018, Guidelines for auditing management systems

[4] ISO 23257, Blockchain and distributed ledger technologies - Reference architecture

[5] ISO 23635:2022, Blockchain and distributed ledger technologies - Guidelines for Governance

〈저 자 소 개〉

유 순 덕 (Soonduck Yoo)

1991년 2월 : 국민대학교 수학과 학사

1994년 2월 : 연세대학원 수학과 이학석사

1995년 12월 : 영국뉴카슬 대학 응용수학 석사

2010년 3월~2013년 2월 : 한세대학교 IT융합박사

2013년 9월~현재 : 한세대학교 조교수

2022년~현재 : ISO/TC307 국제표준 전문위원으로 활동

<관심 분야> 인공지능, 블록체인, 전자금융, 창업 및 벤처, 빅데이터, 정부정책, 개인정보 및 보안