

# 분산원장시스템 거버넌스 국제표준화 동향과 이슈

김 정 덕\*, 박 진 상\*\*

## 요 약

블록체인을 포함하는 분산원장기술은 신뢰할 수 없는 네트워크 상에서 공동으로 거래 정보를 검증하고 기록, 보관함으로써 원장의 무결성과 신뢰성을 제공하고 있다. 이러한 분산원장기술을 이용한 제반 응용시스템이 실세계에서 적용되고 확산되기 위해서는 거버넌스 체계가 구축되어야 한다. 일반적으로 거버넌스란 특정 조직내에서의 지시와 통제활동이라고 할 수 있는데, 분산원장시스템의 경우, 다양한 조직 또는 시스템을 포함하고 있으며 거버넌스 체계도 분산 또는 탈중앙화된 형태로 존재하므로 기존의 조직 거버넌스 체계와 다른 특성과 한계를 가지고 있다. 본 연구에서는 ISO TC 307에서 진행하고 있는 분산원장시스템 거버넌스 표준화 활동을 소개하고 향후 전망과 대응방안을 검토한다.

## I. 서 론

분산원장기술과 블록체인 시스템(이하 ‘분산원장시스템’)에 대한 국제표준화 작업은 ISO TC 307에서 수행하고 있다.[1] TC 307은 2019년 5월 더블린 회의 이후 유스케이스 워킹그룹(WG 6)이 신설됨에 따라 총 6개 워킹그룹으로 구성되어 국제표준화 작업을 진행하고 있다. 이 중 WG 5가 분산원장시스템 거버넌스에 대한 국제표준화를 담당하고 있다.

WG 5는 원래 Study Group 6로 2017년에 시작되어 2018년 10월 모스크바 회의 이후 WG 5로 공식화되었다. 현재 WG 5에서는 ‘분산원장시스템 거버넌스 지침’ 프로젝트(TS WD2 23635)에 집중해서 작업하고 있다. TS(Technical Specification)로서 거버넌스 표준화 작업을 수행하는 이유는 아직 분산원장시스템 기술이 계속적으로 발전하고 있지만, 시스템 개발에 있어 현실적인 표준의 필요성에 대응하기 위함이며, 또한 미래에 용이하게 국제표준(IS)으로 전환될 수 있기 때문이다.

본 논문에서는 현재 진행 중인 WD2 23635(이하 거버넌스 지침)를 중심으로 분산원장시스템 거버넌스의 개념 및 필요성을 기술하고, 거버넌스 구현을 위한 원칙과 프레임워크를 서술한다. 또한 분산원장시스템 거버넌스 국제표준화 노력에서의 이슈를 기술하고 향후 활동계획을 소개한다.

## II. 분산원장시스템 거버넌스 필요성 및 개념

### 2.1. 거버넌스 필요성

분산원장시스템을 활용하여 비즈니스를 수행하기 위해서는 분산원장시스템 목표에 따라 온체인(On-chain)과 오프체인(Off-chain) 상의 의사결정권, 책임성, 보상체계와 같은 분산원장시스템 거버넌스’ 요소들을 고려해야 한다[2]. 분산원장시스템 거버넌스가 부재한 상태로 비즈니스를 수행하면 시스템이 추구하는 목표와 전략을 효과적이고 효율적으로 달성할 수 없고, 조직의 이해관계자들의 기대 및 법규 등의 내 외부 요구사항들을 준수하기 어렵다.

### 2.2. 분산원장시스템 유형과 거버넌스 개념

ISO TC 307에서는 분산원장시스템 거버넌스를 중앙 또는 탈중앙화 된 의사결정권 요소를 모두 포함하는 접근방식으로, 책임성이 네트워크 내에 있고, 참여자들이 합의에 도달하도록 인센티브가 제공되어야 효과적, 효율적인 분산원장시스템 구현이 가능하다고 정의하고 있다.

분산원장시스템은 트랜잭션 검증 권한과 트랜잭션 생성 및 읽기 권한, 두 가지의 접근 권한에 따라 [표 1]

\* 중앙대학교 경영경제대학 산업보안학과 교수(jdkimsac@cau.ac.kr)

\*\* 중앙대학교 일반대학원 융합보안학과 석사과정(ponoboy516@gmail.com)

[표 1] 분산원장시스템 유형

	Permissioned	Permissionless
Public	<ul style="list-style-type: none"> <li>· 모든 노드가 트랜잭션을 읽고 생성</li> <li>· 사전 등록된 노드만 트랜잭션을 검증</li> </ul>	<ul style="list-style-type: none"> <li>· 모든 노드가 트랜잭션을 읽고, 생성, 검증</li> </ul>
Private	<ul style="list-style-type: none"> <li>· 사전 등록된 노드만 트랜잭션을 읽고, 생성, 검증</li> </ul>	<ul style="list-style-type: none"> <li>· 해당 없음</li> </ul>

과 같이 세 가지의 유형으로 분류된다. Public/permissioned 시스템은 공동의 최상위 조직에 소속된 별도의 조직에 의해 노드가 운영되는 경우이다. Public/permissionless 시스템은 서로를 인식하지 못하고 공통된 이해관계가 없는 개별 주체들에 의해 운영되는 경우이다. Private/permissioned 시스템은 모든 노드가 단일 조직에서 소유하는 별도의 IT 시스템인 경우이다.

분산원장시스템의 탈중앙화 된 의사결정 프로세스는 중앙 제어 메커니즘 없이 수많은 의사결정권자와 투표자들을 통해 이루어진다. 분산원장시스템은 불확실한 환경에서 신뢰를 보장하기 위해 중앙 제어 메커니즘이나 신뢰 당국이 필요하지 않으며 전통적인 중앙 집중식 시스템과 차별화 되어 권력 집중을 지양한다. 따라서 많은 전문가들은 분산원장시스템을 ‘기술 거버넌스’로 인식하기도 한다.

거버넌스 지침 문서에 의하면, 분산원장시스템 거버넌스는 세 가지의 유형에 따라 다른 거버넌스 메커니즘을 구축해야 한다. Public/permissioned 시스템에서는 거버넌스 규칙이 사전에 설정되어 있기 때문에, 거버넌스 집행 주체의 선정과 거버넌스 규칙 변경 프로세스가 주요 이슈이다. 중앙 당국이나 컨소시엄이 거버넌스 집행 주체로 결정되면, 이들은 주어진 권한을 기반으로 거버넌스를 집행하며 의견 불일치 시, 포킹(forking)을 통해 의견 조율을 한다.

Public/permissionless 시스템은 전통적인 중앙집중식 시스템과 다르게, 참여자들의 공유되고 상호식 합의 를 통해 거버넌스가 수행된다. 초기에는 중앙당국이나 위원회가 시스템의 목적에 따라 거버넌스 시스템을 설계하고 구축하지만, 구현단계에서는 참여자들이 투표 메커니즘과 하드/소프트 포크와 같은 민주적인 의사결정 프로세스를 통해 온체인과 오프체인 상의 거버넌스를 수행한다. 즉, public/permissionless 시스템의 거버넌스 설계단계에서는 중앙당국에 의해 거버넌스 규칙이

설정되지만 시간이 경과함에 따라 다양한 참여자들의 상호식 의사결정을 통해 거버넌스 규칙이 변경되고 집행되어 진다.

Private/permissioned 시스템의 거버넌스는 IT 거버넌스와 같이 전통적인 계층구조 환경의 거버넌스 체계와 유사하다. 중앙 집중식 시스템이기 때문에 탈중앙화 된 책임, 책임성과 의사결정이 필요하지 않다. 전통적인 시스템과 차별화되지 않았기 때문에 분산원장시스템만의 장점을 활용하기에는 부족하지만 기존 거버넌스 시스템을 조직에 적용함에 있어 수월하다는 장점을 가진다.

### III. 분산원장시스템 거버넌스 원칙

일반적으로 거버넌스는 규칙 기반(Rule-based) 방식과 원칙 기반(Principle-based) 방식을 통해 조직의 목적을 달성한다[3]. 규칙 기반의 거버넌스는 각 조직들이 수행해야 할 거버넌스의 최소 기준을 구체적으로 세우고 강력하게 조직들이 해당 기준을 따르도록 규제하는 것이다. 원칙 기반의 거버넌스는 규칙 기반 거버넌스의 한계를 극복하기 위한 대안으로, 시간이 경과함에 따라 조직 상황이 달라져도 일관되게 적용할 수 있는 상위 기준을 제시하는 것이다[4]. 분산원장시스템 기술 및 응용분야가 계속 발전, 확대되고 있으며 관련 거버넌스 체계가 아직 정립되지 않은 현 상황에서는 분산원장시스템이 처한 다양한 내 외부 환경변화에 유연하게 대처하기 위해서는 규칙 기반 보다는 원칙 기반의 거버넌스가 필요하다고 할 수 있다. 이에 한국대표인 김정덕 교수는 효과적, 효율적 분산원장시스템 활용을 위해 행위 기반(Action-oriented)의 거버넌스 원칙을 수립하였다. 또한 수립된 6 가지 각 원칙별로 What과 Why의 측면에서 세부설명을 하였다. 분산원장시스템의 거버넌스 원칙은 [표 2]와 같다.

분산원장시스템 거버넌스 원칙은 기존의 기업 거버넌스, IT 거버넌스, 정보보호 거버넌스, 각 거버넌스의 원칙 및 목표를 비교분석하여 도출하였다[5][6][7]. 또한 선행연구 분석을 통해 전통적인 중앙집중식 시스템과 차별화하여 분산원장시스템만의 특성을 반영하여 6 가지 원칙의 키워드를 도출하였다[8-16].

[표 2] 분산원장시스템 거버넌스 원칙

제1원칙: 탈중앙화 된 접근 방식으로 의사결정 촉진
키워드: 탈중앙화, 의사결정
<ul style="list-style-type: none"> <li>• 분산원장시스템은 탈중앙화와 권한 분산을 하는 것이며, Public/permissionless 시스템의 요소는 누구나 거버넌스에 참여할 수 있다는 가능성이고, 이를 포괄성이라고 한다.</li> <li>• 분산원장시스템 활용의 탈중앙화 정도는 현재 및 향후 네트워크 목적을 충족해야 하며, 시스템의 현재 및 미래 역량이 고려되어야 한다.</li> </ul>
제2원칙: 참여자 간의 협력 및 조정을 지원
키워드: 조정
<ul style="list-style-type: none"> <li>• 분산원장시스템 생명주기 동안 네트워크 내의 개인 및 그룹은 명확하고 투명하며 동의된 의사결정에 따라 협력하여 시스템을 운영하고 관리해야 한다.</li> <li>• 협력과 조정은 다른 목적을 가진 참여자들이 서로를 신뢰하지 않아도 비즈니스 목적을 공동으로 달성하도록 한다.</li> </ul>
제 3원칙: 바람직한 행동과 인센티브와의 연계
키워드: 인센티브, 바람직한 행동
<ul style="list-style-type: none"> <li>• 분산원장시스템의 인센티브는 의사결정권자 간의 합의 달성, 갈등해소, 지속적인 거버넌스 집행과 시스템 설계 및 운영을 유도한다.</li> <li>• 분산원장시스템의 인센티브는 다양한 참여자와 이해관계자들의 바람직한 행동을 유도하는데 있어 핵심 역할을 한다.</li> </ul>
제4원칙: 분산원장시스템이 현재 및 미래의 확장성 요구사항을 만족하도록 보장
키워드: 성과, 확장성
<ul style="list-style-type: none"> <li>• 분산원장시스템 거버넌스는 주어진 기간 동안 많은 의사결정을 처리해야 하며, 네트워크에 더 많은 참여자들이 참여함에 따라 의사결정 처리 양을 증가시켜야 한다.</li> <li>• 분산원장시스템 활용은 비즈니스 성과를 달성하면서 확장될 수 있도록 효과적이고 효율적이어야 한다.</li> </ul>
제5원칙: 정보보호와 데이터 프라이버시를 보장하여 내부 및 외부 요구사항 충족
키워드: 정보보호, 데이터 프라이버시 보호
<ul style="list-style-type: none"> <li>• 분산원장시스템의 정보보호 범위는 분산원장시스템 및 비 분산원장시스템에 대한 모든 정보보호를 포함한다.</li> <li>• 분산원장시스템의 이사회 및 경영진은 정보의 기밀성, 무결성 및 가용성을 보장해야 한다. 또한, 시스템 활용 시 정보의 무결성과 가용성을 유지하는 것 외에도, 개인식별정보 보호 또는 프라이버시 보호와 같은 정보의 기밀성도 보완해야 한다.</li> </ul>
제6원칙: 분산원장시스템과 기타 시스템 간의 상호 운용성 보장
키워드: 상호 운용성
<ul style="list-style-type: none"> <li>• 분산원장시스템은 다른 분산원장시스템 및 기타 시스템과 상호 운용되도록 보장되어야 한다.</li> <li>• 서로 다른 시스템이 상호 운용되도록 효율적인 정보 교환에 초점을 둔다.</li> </ul>

#### IV. 분산원장시스템 거버넌스 프레임워크

ISO/IEC 38500에서 기술하는 전통적인 IT 거버넌스는 단일 조직 내에서의 거버넌스 기능과 책임성을 다룬다. 하지만 분산원장시스템은 일반 IT 시스템과 달리 참여 노드들이 여러 조직이나 개인에 의해 운영되는 분산된 컴퓨팅과 탈중앙화된 시스템이다. 분산원장시스템의 확장성으로 인해 시스템에 참여하는 조직과 신뢰의 경계가 지속적으로 확대된다. 따라서 분산원장시스템 거버넌스는 ISO/IEC 38500에서 기술한 단일 조직 내에서의 거버넌스 접근방식을 초월하여 다양한 조직 및 개인을 포함해야 한다.

분산원장시스템 거버넌스는 의사결정권, 책임성과 인센티브, 위 3가지 차원으로 분류된다[17]. 첫째, 의사결정 통제에 관한 권한(Decision control rights)과 의사결정 관리에 대한 권한(Decision management rights)으로 구별할 수 있다. 전자는 의사결정의 승인 및 모니터링에 관한 것이며, 후자는 의사결정을 제안하고 결정된 사안을 실행 및 구현하는 것이다. 이러한 의사결정권의 분배는 분산원장시스템을 활용함에 있어 시스템의 탈중앙화 정도에 따라 결정되어야 하며 이해관계자들은 이러한 의사결정권 분배되는 방식에 따라 영향을 받는다. 또한 의사결정권은 온체인과 오프체인 상에서의 의사결정을 모두 고려하여 분배되어야 한다. 온체인 의사결정은 분산원장시스템 운영에 필요로 한 합의나 내부규정에 관한 것으로 시스템에 내재되어 있는 사안이라면, 오프체인 의사결정은 법규준수 및 외부 이해관계자들의 기대 충족, 비 분산원장시스템과의 상호운용성과 시스템의 유연성을 위한 사안이다.

두 번째, 책임성은 분산원장시스템 활용에서 참여자의 책임소재에 관한 차원이다. 분산원장시스템은 신뢰하는 제 3자의 개입이 없고 각자 다른 목적을 가지고 있는 참여자들에 의해 운영된다. 이러한 참여자들이 시스템 목적을 공동으로 달성하게 하기 위해서는 역할 및 책임을 명확히 해야 하고 그에 따른 책임성을 규정해야 한다. 분산원장시스템의 전략과 목적 달성을 위해 강력한 책임소재 규명은 필수적이고 이를 집행하는 체계가 필요로 하다. 자가 보상, 자가 처벌, 자가 모니터링을 피하기 위해 분산원장시스템의 통제와 관리는 분리되어야 하며 책임성은 조직의 규정 및 법적 프레임워크를 통해 제정, 명백하게 시행되어야 한다. 또한 분산원장시스템

의 책임성은 온체인 상에서 시스템 규칙에 따라 규정할 수 있으며 오프체인 상에서도 외부 법규로 규정할 수 있다.

세 번째, 인센티브는 분산원장시스템의 다양한 참여자 및 이해관계자의 행동을 유도하는 핵심적인 역할을 한다. 참여자의 바람직한 행동과 인센티브의 연계는 참여자들이 자신의 행동을 자유롭게 결정할 수 있게 하며 시스템의 목적과 자신들의 행동을 일치하도록 하게 한다. 시스템 참여자들에 대한 인센티브가 잘못 연계되면 궁극적으로 참여자 또는 이해관계자들은 장기적인 관점에서 시스템을 해치는 행동을 할 수 있으며 시스템의 지속 가능한 운영을 위태롭게 할 수 있다. 시스템의 인센티브는 의사결정권자 간의 합의 달성, 분쟁 해결 및 시스템의 지속적인 관리, 설계 및 운영에 대한 결정을 유도한다. 인센티브는 금전적 인센티브와 비금전적 인센티브로 구별할 수 있다. 전자는 참여자의 행동을 금전적인 보상과 연계하는 것이며, 후자는 권한상승, 명예 등과 같은 비금전적인 보상을 참여자의 행동과 연계하는 것이다.

## V. 분산원장시스템 거버넌스 요소

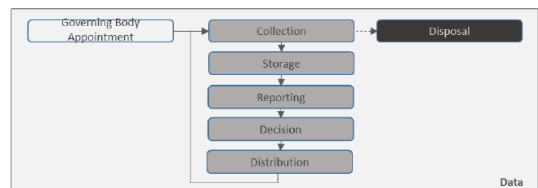
거버넌스 요소에 대해서는 WG 5에서 아직 많은 논의가 이루어지지 않아 초초안 상태라고 볼 수 있느냐, 분산원장시스템 거버넌스의 요소로서 역할, 의사결정권한, 그리고 거버넌스 도구(Instruments)를 포함하고 있다. 분산원장시스템 거버넌스를 위해 11가지 주체별 역할과 각 역할마다의 책임성, 의사결정 권한, 책임을 개발 중에 있다. 예시로, 거버넌스 핵심 주체인 거버너(Governor)는 규칙과 정책을 통해 시스템이 적절히 운영되도록 보장하고 사고가 일어났을 시, 이를 해결하기 위한 중요 의사결정을 내리는 역할이다. 거버너는 모든 시스템 이해관계자들의 요구사항을 충족할 책임성이 있으며, 시스템 업데이트에 관한 의사결정 권한을 갖는다. 또한 거버너는 분산원장 플랫폼이 안전하고 비즈니스 목표에 따라 운영되도록 유지할 책임이 있다.

거버넌스 의사결정 권한은 분산원장시스템 생명주기에 걸쳐 7가지 프로세스를 따른다. 거버넌스 주체인 Governing body가 임명되면 분산원장시스템의 데이터 전송 메커니즘을 결정한다. 데이터 수집은 분산원장시스템 생명주기 동안 여러 조직 및 시스템 상황을 고려

하여 결정된다. 온체인과 오프체인 상의 데이터 저장은 분산원장시스템이 확장함에 따라 추가되는 데이터, 스마트 계약 코드 및 여러 로그들을 포함해야 한다. 데이터 보고는 분산원장시스템의 일반 사용자부터 관리자까지 모든 참여자들의 트랜잭션 및 블록 데이터가 분산원장시스템 간의 상호 운용성이 고려되어 전달되어야 한다. 의사결정은 데이터 보고 결과를 기반으로 분산원장시스템의 개선을 위한 여러 대책 안에 관해 이루어진다. 데이터 유통의 경우 분산원장시스템 상에서의 데이터 접근권한에 따라 데이터가 분배된다. 데이터 폐기는 조직이 준수해야 하는 법적 요구사항을 고려하여 데이터의 완전한 처분 또는 폐기가 결정되어야 한다. 거버넌스 의사결정 프로세스는 [그림 1]과 같다.

분산원장시스템의 거버넌스 도구는 온체인과 오프체인 상의 거버넌스 도구로 구성된다. 온체인 거버넌스 도구는 통상적으로 투표 메커니즘을 일컫는다. 분산원장시스템의 의사결정은 프로토콜 상에서 직접 투표를 통한 합의로 이루어진다. 투표 이해관계자는 시스템 설계자, 채굴자와 일반 사용자이며, 각 이해관계자는 동일한 투표권한을 보유한다. 하지만 온체인 거버넌스는 의사결정을 위한 합의에 도달하지 못할 위험이 있으며, 이런 상황 시 하드포크 또는 소프트 포크를 통해 조정된다.

오프체인 거버넌스 도구는 분산원장시스템의 외부 메커니즘을 일컫는다. 오프체인 거버넌스는 분산원장시스템의 기타 시스템, 법규 준수사항, 조직의 여러 기술과 상호 운용되도록 수행된다. 이러한 오프체인 거버넌스 도구는 온체인에서 수행되는 트랜잭션이 의도된 목적대로 운영되도록 유지하는 역할을 한다. 예를 들어, 오프체인 거버넌스는 온체인 원장과 오프체인 정보의 무결성 유지를 위해 트랜잭션의 불변성과 블록 검증 기능을 지원한다. 또한 오프체인 거버넌스 이해관계자는 시스템 개발자, 채굴자, 일반 사용자 및 관련 업체를 포함하며 해당 이해관계자들 마다 상이한 투표권을 보유할 수 있다.



[그림 1] 거버넌스 의사결정 프로세스

표준문서에서는 분산원장시스템의 컴플라이언스 핵심 요소로 위험관리와 프라이버시 보호를 고려하고 있다. 분산원장시스템의 위험관리는 ISO 31000과 ISO/IEC 27005의 위험관리 프로세스를 따라야 하지만, 탈중앙화 된 시스템이기 때문에 다양한 위험관리 이해관계자들을 고려해야 한다. 위험관리를 수행하는 주체 당국이 부재하기 때문에 시스템의 이해관계자들의 동의와 협력을 필요로 한다. Public/permissioned 시스템과 private/permissioned 시스템은 중앙집중식 시스템과 유사하기 때문에 기존 위험관리 방식의 적용이 수월하겠지만 public/permissionless 시스템의 경우, 새로운 위험관리 방안이 개발될 필요가 있다.

분산원장시스템의 프라이버시 보호에 있어, 거버넌스 이해관계자는 시스템의 사용자 데이터를 적절하게 저장하고 관리하도록 대응책을 제시할 필요가 있다. 또한 국제표준(ISO/IEC 29100[18]와 ISO TR 23244[19])를 참조하여 시스템 상의 개인 식별 정보 보호를 위한 대응책을 제시할 필요가 있다.

## VI. 분산원장시스템 거버넌스 국제표준화 이슈

분산원장시스템 거버넌스 국제표준화 작업은 2019년 8월 현재 2nd WD 상태로서 문서의 골격은 어느 정도 갖추어 졌다고 판단되나 아직 내용 면에서는 많은 보완과 수정이 요구된다. 특히 지난 5월 더블린 회의에서 거버넌스 원칙이 처음으로 논의되기 시작하였고 한 국대표인 김정덕 교수 기고문을 기반으로 clause 4를 새롭게 신설하고 거버넌스 원칙 초안을 개발하고 있다.

효과적인 작업 진행을 위해 clause 별로 전문가 그룹을 정해서 초안 개발을 하고 있으며, 차기 인도 회의 이전에 3차례의 줌 미팅을 통해 개발된 초안 내용에 대한 검토를 예정하고 있다. 11월 회의 이후 CD 개발은 가능할 것으로 예상된다.

현재 WG 5에서 활발하게 참여하는 전문가는 약 15명 정도로 대부분 유럽 출신이며 아시아권에서는 한국만이 참여하고 있다. 분산원장시스템의 효과적, 효율적 운영을 위해서는 거버넌스 체계가 제대로 실현되어야 함에도 불구하고 아직 관련 기술 및 시스템 개발이 초기 단계인 관계로 많은 전문가들이 참가하지 못하고 있는 실정이다. 한국에서의 분산원장시스템 기술 및 표준 개발의 선도적 역할을 위해서도 좀 더 많은 전문가들의

관심과 참여가 필요하다.

## 참 고 문 헌

- [1] 오경희, “분산원장기술(블록체인) 국제 표준화 현황”, *정보보호학회지*, 28(4), pp. 41-47. August 2018.
- [2] ISO/TC 307 WD2 23635, “*Blockchain and distributed ledger technologies - Guidelines for Governance*”. May 2019.
- [3] K. Reddy, S. Locke, “The efficacy of principle based corporate governance practices and firm financial performance: An empirical investigation”. *International Journal of Managerial Finance*, 6(3), pp. 190-219. June 2010.
- [4] Banff Executive Leadership Inc, “*Improving governance performance rules-based vs. principles-based approaches*”. February 2004.
- [5] ISO/IEC WD4 37000, “*Guidance for the governance of organizations*”. December 2018.
- [6] ISO/IEC 38500, “*Corporate governance of information technology*”. February 2015.
- [7] ISO/IEC WD3 27014, “*Information technology - Security techniques - Governance of information security*”. October 2018.
- [8] R. Beck, C. Bloch, J. King, “Governance in the blockchain economy: A framework and research agenda”. *Journal of the Association for Information Systems*, 19(10), pp. 1020-1034. October 2018.
- [9] M. Verduyn, “*Bitcoin and beyond: cryptocurrencies, blockchains, and global governance*”. Routledge. 2018.
- [10] J. Mattila, T. Seppälä, “Distributed governance in multi-sided platforms, *Translational Systems Sciences*, vol 11. Springer, pp. 183-205. 2018.
- [11] D. Yermack, “*Corporate governance and blockchains*”. Oxford. January 2017.
- [12] V. Shermin, “*Disrupting governance with blockchains and smart contracts*”. John Wiley & Sons. September 2017.
- [13] S. Mills, B. McDowall, “*Responsibility without*

power? The governance of mutual distributed ledgers”. Cardo Foundation. July 2017.

- [14] F. Piazza, “Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses”. *Journal of Law & International Affairs*, 5(2), pp. 262-301. 2017.
- [15] P. Tasca, T. Thanabalasingham, “*Ontology of blockchain technologies. Principles of identification and classification*”. SSRN Electronic Journal. May 2017.
- [16] ISO/TC 307 TR 23245, “*Blockchain and distributed ledger technologies - Security risks, threats and vulnerabilities*”. January 2019.
- [17] P. Weill, “Don’t just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, 3(1), pp. 1-17. March 2004.
- [18] ISO/IEC 29100, “Privacy Framework”, October 2012.
- [19] ISO/TC 307 TR 23244, Blockchain and distributed ledger technologies\_Oview of privacy and PII protection, May, 2019.



### 박진상 (Jinsang Park)

정회원

2017년 8월 : 중앙대학교 경영학과 졸업

2017년 9월~현재 : 중앙대학교 융합보안학과 석사과정  
<관심분야> 정보보호 거버넌스, 보안관리체계, 위협관리

### 〈저자소개〉



### 김정덕 (Jungduk Kim)

종신회원

1979년 2월 : 연세대학교 정치외교학과 졸업

1981년 8월 : 연세대학교 경제학과 석사

1986년 5월 : University of S. Carolina, MBA

1990년 12월 : Texas A&M University, Ph.D. in MIS

1995년 3월~2014년 8월 : 중앙대학교 정보시스템학과 교수

2014년 9월~현재 : 중앙대학교 산업보안학과 교수

2018년 9월~현재 : ISO TC 307 전문위원

<관심분야> 디지털 비즈니스 보안, 사이버보안 거버넌스 및 관리