TTA Technical Report

기술보고서

TTAR-xx.xxxx

제정일: 20년 xx월 xx일

*개정인 경우 최종 개정일만 기재

분산원장기술 참조구조 사례 연구(기술보고서)

Case Study on Reference Architecture for Distributed Ledger Technologies (Technical Report)

한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 블록체인기반기술 프로젝트그룹 (PG1006)

기술보고서안 심의 위원회 지능정보기반 기술위원회(TC10)

	성명	소 속	직위	위원회 및 직위	기술보고서번호
기술보고서(과제) 제안	박현제	소프트웨어정책연구소	소장		TTAR-xx.xxxx
기술보고서 초안 작성자	오경희	TCA서비스/분산원장기술 표준포럼	대표/연구책임자	PG 1006 부의장	TTAR-xx.xxxx
	이영주	서강대학교	교수		
	신동환	마크애니	팀장		
	이공근	서강대학교	연구원		
	강호준	서강대학교	연구원		
	장민오	서강대학교	연구원		
	류재철	충남대학교/분산원장기술 표준포럼	교수/의장		
사무국 담당	오정엽	TTA	선임	-	

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 기술보고서의 목적

이 기술보고서의 목적은 다양한 응용을 지원하고 확장성 및 상호운용성을 지원할 수 있는 분산원장 시스템 및 솔루션 공통의 참조 구조 사례를 연구함으로써 이러한 특성을 갖는 분산원장 시스템 및 응용을 개발할 수 있도록 지원하고, 분산원장 기술 분야의 사용자, 서비스 제공자, 개발자, 관리자, 감독기관 등이 그들이 의도하는 바를 명확하고 효과적으로 소통할 수 있도록 지원하는 것이다.

2 주요 내용 요약

이 기술보고서는 블록체인을 포함하는 분산원장시스템의 위한 참조 구조를 정의하고 참조 구조를 구성하는 기능적 계층, 계층 별 기능, 핵심 모듈의 기능 사례를 분석한다.

3 인용 기술보고서와의 비교

3.1 인용 기술보고서와의 관련성

이 기술보고서는 타 기술보고서를 인용하지 않는다.

3.2 인용 표준과 본 기술보고서의 비교표

TTAK.xx-xx.xxxx/R1		비고

Preface

1 Purpose

The standard is to provide study the common reference architecture for distributed ledger systems and solutions in order to support the development of distributed ledger platform being able to support various applications and having scalability and interoperability. The standard is also to help users, customers, service providers, developers, administrators, regulators of distributed ledger technologies to communicate clearly and effectively what they mean by defining reference architecture used for distributed ledger technologies including blockchain technologies.

2 Summary

The standard include reference architecture of general distributed ledger system including blockchain technologies field. This standards also provides functional layers, functions of layers and core modules consisting the reference architecture.

3 Relationship to Reference Standards

The standard does not have any reference standard or technical report.

목 차

분산원장기술 참조 구조 사례 연구
(Case Study on Reference architecture for distributed ledger technologies)

1 적용 범위

이 기술보고서의 목적은 다양한 응용을 지원하고 확장성 및 상호운용성을 지원할 수 있는 분산원장 시스템 및 솔루션 공통의 참조 구조 사례를 연구함으로써 이러한 특성을 갖는 분산원장 시스템 및 응용을 개발할 수 있도록 지원하고, 분산원장 기술 분야의 사용자, 서비스 제공자, 개발자, 관리자, 감독기관 등이 그들이 의도하는 바를 명확하고 효과적으로 소통할 수 있도록 지원하는 것이다.

2 인용 표준

이 기술보고서는 별도의 표준을 준용하지 않는다.

3 용어 정의

이 기술보고서에서 사용되는 용어는 TTAK.KO-12.3006 블록체인 용어 정의를 따른다.

4 약어

이 기술보고서에서는 다음의 약어를 사용한다.

DLT	Distributed Ledger Technologies
DAG	Directed Acyclic Graph
DApp	Decentralized Application
P2P	Peer to Peer

5 분산원장기술 개요

원장은 오래 전부터 금융권에서 회계 기록에 사용해 온 용어이다. 정보기술 분야에서 원장이라 함은 금융권 뿐만 아니라 다양한 종류의 확정된 거래 기록을 저장하기 위한 데이터 구조 및 그에 기록된 데이터를 의미한다. 예를 들어 물리적 객체의 이동과 전송의 기록도 원장이라고 부를 수 있다. 기록을 신뢰하고 업무에 활용하기 위해서 원장은 변경되지 않아야 한다.

분산원장은 분산되고 탈중앙화된 방식으로 유지되는 원장이다. 즉 원장의 데이터는 한 곳에 저장되지 않고 네트워크 내의 여러 노드에 걸쳐 분산된 방식으로 저장된다. 네트워크 내의 다양한 노드들은 여러 당사자가 소유할 수 있으며, 다른 당사자가 가진 노드들과 상호작용한다.

이렇게 네트워크 상에서 서로 다른 참여자들이 하나의 원장을 합의하에 생성, 기록, 유지하기 위하여 사용되는 기술을 분산원장기술이라고 부른다. 분산원장기술은 중앙의 신뢰할 수 있는 제3자가 없이 당사자 간에 안전하고 부인이 불가능한 온라인 거래를 제공하는 것을 목표로 한다. 분산원장 내의 기록은 검증 가능해야 하고 감사가 가능해야 한다.

이를 달성하기 위해서는 어떤 거래가 그것이 처리되는 모든 노드에서 동일한 내용을 가지며, 그 거래에 관련된 당사자들이 그 내용에 합의했음을 보장하기 위한 프로세스가 포함된다. 즉, 새로운 거래를 모든 노드들에 분배하기 위한 메커니즘, 거래를 검증하기 위한 분산 메커니즘, 그리고 블록체인의 모든 사본의 일관성을 궁극적으로 보장하기 위한 메커니즘이 필요하다.

그러나 모든 노드가 거래 기록의 정확히 똑같은 집합을 저장해야 하는 것은 아니다. 어떤 분산원장은 그런 경우가 있지만 항상 그렇지는 않다. 또한 분산원장에 참여하는 모든 당사자가 모든 거래 기록에 접근 가능한 것도 아니다. 어떤 당사자는 그들이 관여하지 않은 거래 기록에 대해서는 접근하지 못할 수 있다.

분산원장 시스템의 유형과 구조를 이해하기 위해 이들을 원장의 저장 구조, 통제 구조, 원장의 분할 여부, 허가의 필요 여부, 구현 방식 등의 측면에서 분류할 수 있다.

이 표준에서는 분산원장 기술의 핵심 개념, 필수적 특성, 블록체인의 유형, 구조 고려사항, 역할 및 기능적 참조 구조에 대해 설명한다.

6 분산원장기술 기본 개념 및 특성

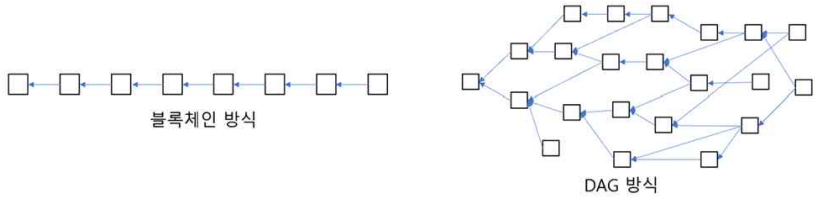
6.1 변경 저항성

변경에 대한 저항성(tamper-resistant)은 원장에 매우 필요한 속성이다. 즉, 거래 기록은 한번 원장에 포함되고 나면 변경될 수 없거나, 조사를 통해 명확히 검증되지 않고는 변경될 수 없어야 한다. 변경은 의도적으로 또는 우연히 발생할 수 있으며, 악성일 수도 있고 무해할 수도 있다.

모든 유형의 변경을 예방하는 것은 극히 어려울 수 있기 때문에, “변경 저항성”은 “변경 증명(tamper-proof)”보다 더 적절한 용어다. “변경 저항성”은 모든 인가되지 않은 변경이 명확히 가시화되도록 하는 특성을 갖는 시스템을 설명하는 데 사용될 수 있다. 실제로 필요한 것은 모든 변경 시도를 탐지하는 것이다. 때때로 분산원장 시스템을 설명할 때 사용되는 “변경 불가능성(immutable)”이란 용어는 어떤 변경도 절대로 일어나지 않는다는 것을 의미하는데 이는 100% 보장될 수 있는 것이 아니기 때문에 오해를 살 수 있다.

6.2 분산원장의 데이터 구조

분산원장을 구성하는 방법은 원장의 레코드를 블록체인 형태로 구성하는 방법과 방향성을 갖는 비순환적 그래프(DAG)로 구성하는 방법으로 크게 나누어진다.



(그림 6-1) 블록체인 방식과 DAG 방식

블록체인 방식은 하나 이상의 거래를 모아 블록의 몸체를 구성하고 선행 블록의 암호학적 해시를 블록 헤더에 포함시켜 두 블록을 연결함으로써 원장을 구성한다. DAG에서는 새로운 거래에 하나 이상의 선행 거래들을 암호학적 해시를 사용하여 연결함으로써 방향은 있지만 순환되지 않는 그래프의 형태로 원장을 구성한다.

두 방식 모두 새로운 거래를 네트워크에 배포하고, 검증하기 위한 프로토콜과 이를 포함하는 레코드를 원장에 추가할 지 결정하기 위한 탈중앙화된 방식의 합의 알고리즘이 필요하다. 일반적으로 각각의 방식에서 사용되는 검증 및 합의 알고리즘에 따라 서로 다른 특성이 나타난다.

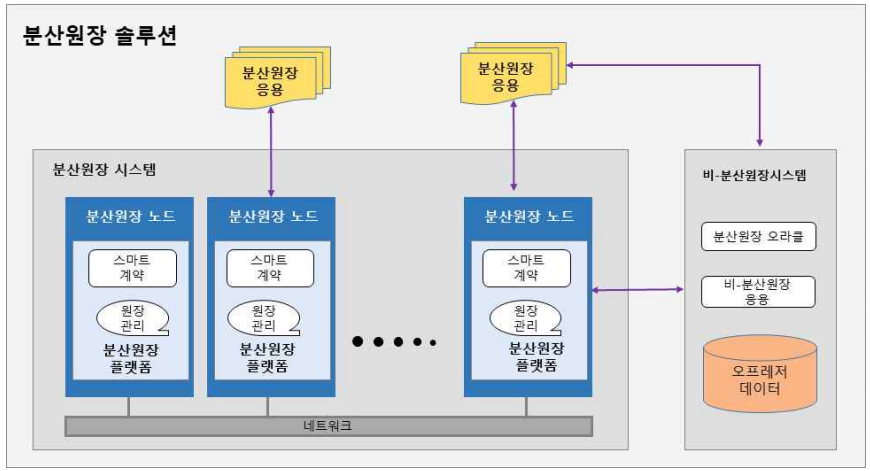
블록체인이라는 용어는 특정 분산원장 내에서 데이터의 저장 구조를 지칭할 때도 사용되고 이러한 구조를 사용하는 특정한 분산원장 전체를 지칭하기 위해 사용되기도 한다.

현실에서는 분산원장을 구현하기 위한 기술로서 블록체인 방식이 가장 먼저 개발되었으며 현재까지 광범위하게 사용되고 있기 때문에 블록체인을 분산원장기술을 포함하는 대표 용어로 사용하는 경우가 종종 발견된다.

6.3 분산원장 시스템, 노드, 플랫폼, 응용, 솔루션의 관계

분산원장 솔루션은 특정 업무 목적을 달성하기 위한 분산원장 시스템, 그 분산원장 응용

및 관련된 비-분산원장 시스템의 총체로 생각할 수 있다.



(그림 6-2) 분산원장 솔루션 구조

분산원장 시스템은 분산원장을 구현하는 시스템을 말한다. 분산원장 시스템은 분산원장 플랫폼이 운영되는 노드 및 이들의 네트워크로 구성된다. 분산원장 플랫폼은 분산원장 노드 상에서 분산원장 시스템의 기능을 제공하는 처리, 저장 및 통신 장치의 집합을 말한다.

분산원장 노드는 분산원장을 지원하기 위해 통신하고 원장의 복제본을 저장할 수 있는 소프트웨어 구성 요소를 실행하는 P2P 네트워크 상의 한 요소이다. 노드는 물리적인 장치이거나 하나 이상의 가상 머신 또는 컨테이너와 같은 가상 실행 환경의 형태일 수 있다. 즉, 노드가 클라우드 컴퓨팅을 사용하여 구현되는 경우 가상 환경을 사용할 수 있다. 일반적으로 분산원장 시스템 내의 각각의 노드들은 서로 다른 조직 또는 개인에 속한다. 분산원장 플랫폼은 분산원장 네트워크 상의 노드에서 분산원장 시스템의 기능을 제공하는 소프트웨어 및 저장 장치 집합에 사용되는 용어이다.

분산원장 응용은 분산원장 시스템을 이용하기 위한 응용 프로그램이다. 이들은 노드와 통신하며, 노드가 속한 조직과 그 사용자의 활동을 지원하기 위한 기능을 갖는다. 따라서 서로 다른 노드들은 서로 다른 분산원장 응용에 이용될 수 있다. 한편, 같은 활동이 여러 조직과 사용자에게 필요하다면 동일한 분산원장 응용이 여러 조직 및 그 사용자들에게 이용될 수 있다. 예를 들면 동일한 지갑 응용은 이를 지원하는 여러 분산원장 시스템, 노드, 이용자에게 사용될 수 있다.

분산원장 응용은 분산 애플리케이션(Decentralized application, DApp)과는 구분되어야

한다. 분산 애플리케이션은 원장에서 실행되는 탈중앙화된 응용으로 스마트 계약을 포함한다.

암호화폐 등 특정 단일 목적으로 구현되는 분산원장 시스템이거나, 개념 검증을 위해 구현되는 분산원장 시스템의 경우 분산원장 노드의 단독 네트워크로 구성된다. 이런 경우 분산원장 시스템 자체의 능력은 원장의 거래 처리 및 기록 추가를 담당하는 노드의 플랫폼 상에서 운영되는 스마트 계약에 따라 결정된다. 분산원장 응용은 거래를 개시하기 위해 플랫폼의 I/F를 통해 하나 이상의 스마트 계약을 호출하게 된다.

그러나 다양한 업무 목적을 달성하기 위한 분산원장 시스템은 일반적으로 기존의 전통적인 IT 시스템, 즉 비-분산원장 시스템(non-DLT system)들과 연동할 필요가 있다. 비-분산원장 시스템의 데이터에 문제가 있는 경우 분산원장 시스템의 무결성에 영향을 미칠 수 있기 때문에 신뢰할 수 있는 데이터를 안전하게 연동하기 위한 서비스가 필요하다. 이런 서비스를 분산원장 오라클(DLT oracle)이라고 한다. 이러한 비-분산원장시스템은 또한 분산원장 응용과 연동할 수 있다.

7 전반적 구조

기존의 분산원장 구현 방식 중에는 목표 서비스에 필요한 응용 기능을 플랫폼과 통합하여 구현한 경우들이 있다. 이런 경우 추가적인 기능 확장이나 연계가 어려운 문제가 발생할 수 있다.

본 표준에서는 범용성, 확장성과 상호운용성을 보장하기 위한 분산원장 플랫폼 및 관리 기능을 위한 참조 구조를 제시한다.

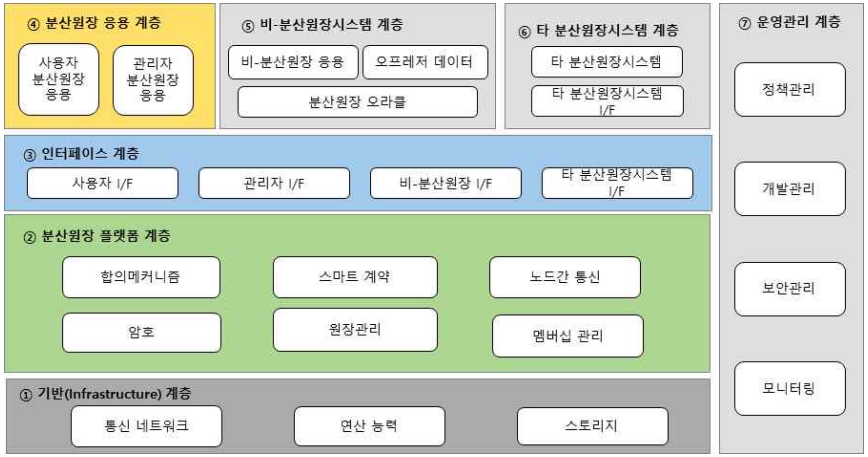
범용성을 제공하기 위해서는 분산원장을 구성하는 핵심 기능과 응용 별로 달라지는 어플리케이션과 구분할 필요가 있다. 이러한 구분을 통해 구성되는 분산원장 시스템은 분산원장의 핵심 기능을 제공하면서 별도의 분산원장 응용 또는 기존의 IT 시스템과 연동하면서 다양한 분야의 서비스를 제공할 수 있다.

분산원장기술 참조 구조는 분산원장 플랫폼을 구성하는 3개 계층(Layer)과 분산원장 플랫폼의 운영, 타 시스템과의 상호운용에 필요한 3개 기능블록(Functional block)으로 구성된다.

8 구성 요소 및 기능

8.1 기반 계층 (Infrastructure Layer)

분산원장을 구성하기 위한 기술 및 물리적인 기반을 제공하는 계층으로서 통신 네트워크



(그림 7-1) 분산원장기술 참조 구조

와 연산 능력, 스토리지로 구성된다.

가) 통신 네트워크

분산원장 시스템의 통신망은 노드를 연결하는 통신망으로써 일반적으로 동등 계층 통신망(peer-to-peer network) 프로토콜을 사용한다. 또한 노드와 분산원장 업무 응용 시스템 간을 연결하는 통신망, 그리고 분산원장 업무 응용과 사용자 기기를 연결하는 통신망이 포함된다.

나) 연산 능력

분산원장 시스템의 실행 환경은 분산원장 시스템 운영을 위한 연산 능력을 제공한다. 이 실행환경은 일반적으로 노드를 운영하기 위한 것으로서 일반 컴퓨터, 컨테이너, 가상 머신, 클라우드 등이 될 수 있다.

다) 스토리지

분산원장 시스템의 데이터 저장소는 원장 및 기타 분산원장 플랫폼 운영에 필요한 데이터를 저장하는 물리적 위치이다. 저장소는 분산되거나 국지적(local)일 수 있다.

8.2 분산원장 플랫폼 계층

분산원장을 구성하는 노드에서 실행해야 하는 다양한 기능을 제공하는 계층이다. 합의

메커니즘, 거래 및 원장 레코드에 관련된 프로토콜, 스마트 계약 실행, 원장 관리 등의 기능을 포함한다.

가) 합의(Consensus)메커니즘

합의는 트랜잭션의 유효성을 검사하고 분산원장에 일관성있는 트랜잭션 집합 및 순서가 포함되도록하는 분산원장 노드 간의 동의(Agreement)를 의미한다. 이는 모든 분산원장 노드가 동의한다는 의미는 아니다. 일단 합의에 따라 분산원장에 기록된 거래는 최종적이고 결정적이며 불변인 것으로 간주된다. 이를 위해서는 분산원장 시스템이 분산원장을 유지 및 변경하고 원장의 기록 신뢰성, 진위성 및 정확성을 보장하고 다양한 규칙 및 절차를 포함한 합의 메커니즘이 필요하다. 합의 메커니즘의 예로는 작업증명 (PoW), 상태증명(PoS, DPoS), 중요성 증명, 비잔틴 합의(pBFT, FBT, Paxos) 등이 있다.

나) 암호

기밀성, 무결성 등의 보호를 제공하기 위해 암호화, 전자서명, 해시 계산 등을 수행한다. 해시 함수는 원장을 변경하지 않았음을 보장하고, 전자서명은 수신자가 트랜잭션의 내용이 위변조되지 않고 권한이 있는 사람만 접근할 수 있음을 보장한다.

이 기능은 플랫폼 계층 내의 합의 모듈, 멤버십 관리 기능 등 다양한 기능과 연결되어 필요한 암호 기능을 제공한다.

다) 스마트 계약(Smart Contract)

원장에 연결된 컴퓨터 프로그램을 이벤트 기반으로 실행하고 그 결과를 다시 분산원장에 기록한다. 필요한 경우 스마트 계약을 실행하기 위한 안전한 실행환경을 포함한다.

안전한 실행환경은 코드를 수행하기 위한 가상 머신 또는 안전한 운영 시스템, 분산원장 지원 프로그래밍 언어를 위한 라이브러리, 관련 실행코드 등의 집합을 포함하는 안전한 컨테이너 등이 될 수 있다.

라) 원장관리

원장은 최종적이고 결정적인 거래 기록을 보관하는 정보 저장소이다. 원장관리 구성요소는 원장, 거래 정보, 운영 데이터 등과 같은 분산원장 시스템의 작동 중에 생성되는 다양한 유형의 데이터를 작성하고 스토리지에 기록하고 질의할 수 있도록 지원한다. 여기에는 원장에 저장된 자산의 상태에 대한 추적, 새로운 트랜잭션이 수행될 때의 상태 갱신 등 상태 관리 기능이 포함될 수 있다. 구현방법은 관계형 데이터베이스, 키-값 쌍 데이터베이스, 파일 데이터베이스 등이 될 수 있다. 분산 컴퓨팅 시스템에서 많은 양의데이터

를 처리하기 위한 방법인 샤딩(Sharding)을 지원하기 위해서는 데이터 단편화 및 라우팅 기능이 필요하다.

마) 노드 간 통신

통신망을 통해 노드 간의 거래, 블록, 사건 등을 통신하기 위한 통신 프로토콜을 수행한다. 거래 및 스마트 계약 실행에 따라 발생된 사건들을 노드들에 배포하고 받은 사건을 처리하는 이벤트 분배 및 처리 기능을 포함한다.

바) 멤버십 관리

분산원장 사용자 및 노드의 신원과 그에 해당하는 공개키 정보를 관리한다. 접근 관리 및 권한 관리가 필요한 경우, 이 멤버십 관리 기능을 이용하여 수행된다. 기밀성을 제공하기 위해 특정 노드 간에서만 거래 정보를 공유하도록 하는 경우에도 멤버십 관리의 신원 정보를 활용한다. 또한 감사를 위해 신원에 기반한 활동 기록을 유지할 필요가 있을 경우 이 멤버십 관리 기능을 활용할 수 있다.

멤버십 관리는 신원에 따라 활동을 제한하는 허가형(permissioned) 분산원장 시스템에만 적용된다. 무허가형(permissionless) 분산원장 시스템에서는 공개키 자체가 신원의 역할을 하므로 별도의 멤버십 관리가 불필요하다.

8.3 인터페이스 계층

내·외부 시스템과의 상호운용과 관련된 계층으로 '사용자 I/F', '관리자 I/F', '비-분산원장 시스템 I/F', '타 분산원장 시스템 I/F'로 구성된다. 인터페이스 계층은 분산원장 플랫폼 계층 내의 기능 구성 요소를 호출하여 분산원장 시스템에 대한 안정적이고 효율적인 접근을 '분산원장 응용 계층' 및 '비-분산원장 시스템 계층'과 '타 분산원장 시스템'에 제공하는 기능이다. 또한 통합 접근 및 노드 관리 기능을 제공한다.

가) 사용자 I/F

도메인 특유의 기능에 대한 접근을 제공하는 응용 프로그래밍 인터페이스이다. 이것은 기업 또는 컨소시엄과 관련이 있을 수도 있고 그렇지 않을 수도 있다.

나) 관리자 I/F

관리자 및 운영자 기능에 대한 접근을 제공하는 인터페이스이다.

다) 비-분산원장 I/F

분산원장 시스템과 비-분산원장 시스템 간의 통신을 위한 안전한 수단을 제공한다.

라) 타 분산원장 시스템 I/F

분산원장 시스템과 타 분산원장 시스템 연계 시 필요한 데이터 형식, 통신 프로토콜, 자산 이전 등에 관련된 상호운용성 및 보안을 보장하기 위한 기능을 수행한다.

8.4 응용 서비스 계층

분산원장에 기반한 업무 응용 시스템을 운영하는 계층. 분산원장에 관련된 데이터를 제공하는 분산원장 외부의 데이터 저장소 및 응용 프로그램이 포함되며, 사용자 및 관리자용의 프로그램이 포함된다.

가) 사용자 분산원장 응용

사용자 분산원장 응용은 분산원장 시스템의 클라이언트로서 사용자가 특정 업무 기능을 수행하기 위해 이용하는 응용 프로그램이다.

나) 관리자 분산원장 응용

관리자 분산원장 응용은 분산원장 시스템의 클라이언트로서 관리자가 응용 및 시스템을 관리하기 위한 능력을 제공하는 응용 프로그램이다.

8.5 비-분산원장 시스템 계층

비-분산원장 시스템에는 분산원장 오라클, 비-분산원장 응용 및 오프레저(Off-Ledger) 데이터가 포함된다. 이들은 '비-분산원장 시스템 I/F' 구성 요소를 사용하여 분산원장 노드에 연결된다.

비-분산원장 시스템 계층에는 비즈니스 목표를 달성하기 위해 분산원장 시스템이 통신하는 분산원장 시스템 외부의 시스템이 포함된다.

가) 분산원장 오라클

분산원장 오라클은 외부 데이터를 분산원장 시스템에 제공하거나 분산원장 시스템의 이벤트에 응답하도록 고안된 시스템이다. 변환 논리 및 서비스를 사용하여 분산원장 시스템과 비-분산원장 시스템 간에 데이터를 교환하는 데 필요한 변환을 수행할 수 있다. 스

마트 계약을 통해 코드 실행 중에 실제 데이터를 안전하게 수집하기 위해 분산원장 오라클을 사용한다.

나) 비-분산원장 응용

비-분산원장 응용은 분산원장 시스템 외부에서 데이터 송수신을 위해 통신하는 응용 프로그램이다. 이러한 응용 프로그램은 응용 프로그래밍 인터페이스를 통해 분산원장 응용 프로그램에 데이터 및 서비스를 제공하거나 보조 서비스를 제공하기 위해 분산원장에서 데이터를 수집 할 수 있다.

다) 오프레저 데이터

오프레저 데이터는 분산원장 시스템과 관련된 데이터를 저장할 수 있는 분산원장 시스템 외부의 모든 데이터 저장소이다. 예를 들어 원장에 보관된 거래와 관련된 추가 데이터가 들어있는 데이터베이스가 있을 수 있다.

8.6 타 분산원장 시스템 계층

타 분산원장 시스템은 독립적으로 운용되는 별도의 분산원장 시스템이다. 이들은 인터페이스 계층의 '타 분산원장 시스템 I/F' 구성 요소를 사용하여 분산원장 노드에 연결된다.

8.7 운영·관리 계층

분산원장의 운영과 관련되어 모든 계층에 걸쳐 작동하는 기능이다. '정책 관리', '개발 관리', '보안 관리', '모니터링'으로 구성된다.

완전 공개형 분산원장의 경우 관련 기능은 거의 존재하지 않을 수 있으며, 플랫폼 관리 기능의 일부로 작동된다. 승인형 분산원장의 경우 정책에 따라 각 관련 기능들이 요구될 수 있으며, 이들은 각 노드 상에서, 또는 일부 노드들과 연결된 형태로 분산되어 작동하 할 수 있다. 특히 사설 분산원장에서 이 기능의 일부는 별도의 물리적 기계에서 중앙집중화된 형태로 관리되고 통신을 통해 각 노드와 연결되어 작동할 수 있다.

가) 정책 관리

분산원장 시스템의 구성요소 및 기능에 대한 정책을 수립 ·관리한다. 여기에는 서비스 디렉토리 관리, 사고 대응, 분산원장 시스템 관리, 노드 관리, 원장 관리 등 전반적인 분산원장 시스템 관리를 위한 다양한 기능에 관련된 세부 정책이 포함된다.

- 서비스 디렉토리는 분산원장이 제공하는 다양한 서비스, 스마트 계약, 운영자, 노드 등의 대상을 검색하기 위해 제공된다.

- 사고 대응은 모니터링 기능과 연계하여 분산원장 시스템 전체에서 발생하는 다양한 사고 및 문제를 탐지, 보고, 분석, 대응 및 관리한다. 이 결과는 정책에 따라 분산원장 노드의 운영자 또는 사용자들에게 보고된다. 법 및 규제 대응은 모니터링 기능을 참조하라.
- 분산원장 시스템 관리는 분산원장의 성능 및 가용성을 포함하는 전반적인 서비스를 관리한다. 여기에는 분산원장 시스템의 서비스 접근점에서의 서비스 제공 수준을 관리하는 서비스 제공관리가 포함될 수 있다.
- 노드 관리는 모니터링 시스템과 연결되어 분산원장 네트워크를 구성하는 노드 및 이들의 성능과 가용성을 관리한다.
- 원장 관리는 분산원장의 구성 및 저장을 관리한다. 정책에 따라 분산원장은 일부 노드에만 저장될 수도 있으며 노드에 따라 원장의 일부만이 저장될 수도 있다.

나) 개발 관리

플랫폼 소프트웨어 및 스마트 계약의 개발 관리, 코드의 보안성을 포함하는 테스트, 빌드, 배포 및 패치 등의 관리 기능을 수행한다. 정책관리에 연결되어 업데이트 및 버전관리를 제공할 수 있다.

다) 보안 관리

식별 및 인증, 보안 정책 관리, 접근관리, 분산원장 운영에 필요한 특정 정보에 대한 가용성 관리가 포함된다.

- 허가형 분산원장의 경우 사용자 및 노드에 대한 멤버십관리 기능이 포함된다. 이 기능은 정책에 따라 노드 및 사용자를 검증하고 이들이 사용하는 공개키를 관리한다.
- 노드 및 사용자의 권한 및 접근을 관리하기 위한 권한관리 및 접근 관리 기능이 포함된다.
- 보안 정책에 따라 필요한 경우 저장 데이터 및 통신을 암호화 하고 시스템 무결성을 검증한다.
- 개인정보가 관련된 경우 개인정보보호 정책 및 관리 기능이 포함된다.

라) 모니터링

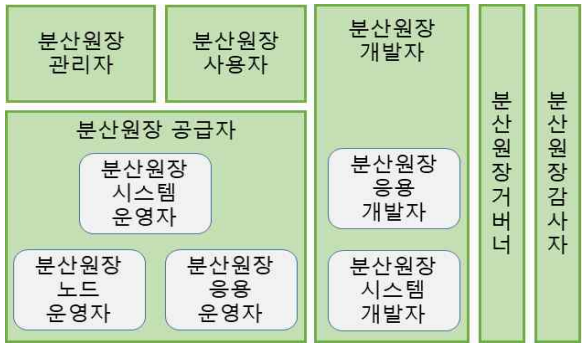
노드 및 네트워크의 상태, 사용자 및 운영자의 활동, 분산원장 시스템에서 발생하는 다양한 이벤트를 모니터링한다. 이 기능은 사고 대응과 연계하여 이상이나 문제를 탐지하고 대응하는 데 이용될 수 있다. 법 및 규제에 대한 모니터링 및 대응을 포함할 수 있다.

분산원장이 제공하는 서비스가 특정 산업 분야의 법 및 규제의 대상이 될 경우 이의 준

수를 위한 기능이 필요할 수 있다. 예를 들어 금융 분야에는 돈세탁, 불법자금 및 범죄 예방 등을 위한 규제가 강제된다. 준수 기능에는 감독 및 감사 지원, 거버넌스 통제, 세부 정책 관리 등이 포함될 수 있다.

9 사용자 역할

이 장에서는 분산원장 시스템의 주요 활동에 연관된 역할과 하위역할에 대해 설명한다. 분산원장 시스템과 관련된 이해관계자들을 그림 3에 정리하였다.



(그림 9-1) 분산원장 시스템 역할

9.1 분산원장 사용자

분산원장 사용자는 분산원장 솔루션을 사용하는 역할로써 개인, 조직, 장치 또는 시스템을 나타낼 수 있다. 일반적으로 분산원장 사용자는 분산원장 노드와 직접 상호 작용하기보다는 분산원장에서 제공하는 사용자 I/F와 상호 작용하는 분산원장 응용 프로그램 또는 오프 체인 코드를 사용하여 분산원장 시스템을 사용한다. 사용자가 사람이 아닌 자동화된 시스템인 분산원장 사용자인 경우 분산원장 응용 프로그램에서 제공하는 인터페이스를 통해 상호작용이 이루어진다.

분산원장 사용자의 주요 활동은 다음을 포함 할 수 있다.

- 분산원장 사용자 응용 프로그램 이용 – 필요한 경우 비즈니스 시스템과 연동
- 사용자 응용 프로그램 설치
- 분산원장 사용자 응용 프로그램 구성
- 분산원장 시스템과 상호 작용할 클라이언트 또는 응용 프로그램 설치
- 예외 또는 실패 처리

9.2 분산원장 관리자

분산원장 관리자는 특히 보안 구성을 위한 작업을 수행한다. 관리자의 업무 범위는 시스템 및 네트워크에 따라 다를 수 있다. 어떤 경우는 일부 분산원장 노드만 관리하는 것으로 제한되며 어떤 경우는 분산원장 솔루션 전체를 관리할 수 있다.

분산원장 관리자의 주요 활동은 다음을 포함 할 수 있다.

- 보안 정책 관리
- 암호화 키 관리
- 예외 처리
- 사용자 응용 프로그램 설치
- 분산원장 사용자 응용 프로그램 구성 (일반 사용자 또는 관리자)
- 스마트 계약 생성 및 배포를 위한 역할 기반 접근 제어 관리
- 특정 스마트 계약 기능 호출을 위한 역할 기반 접근 제어 관리

9.3 분산원장 공급자

분산원장 공급자는 분산원장 시스템 및 분산원장 네트워크에서 하나 이상의 노드를 소유하고 운영하는 역할이며 비즈니스 관계자이다. 분산원장 공급 업체는 노드를 생성 및 인스턴스화하고 네트워크에 가입하며 네트워크에 가입하기 위한 법적 계약을 체결하고 이에 동의한다.

분산원장 공급자 역할은 아래와 같이 세분화 할 수 있다.

가) 분산원장 시스템 운영자

분산원장 시스템 운영자는 분산원장 노드에서 분산원장 시스템 및 플랫폼의 구성 요소를 관리하고 실행하는 실제 및 가상 시스템 및 네트워크를 관리하고 운영하는 역할이다. 네트워크 및 다중 노드 연결, 노드 간의 상호 운용성을 처리하고 노드 간 정책을 적용한다.

분산원장 시스템 운영자의 주요 활동은 다음을 포함할 수 있다.

- 분산원장 통신 네트워크 관리
- 물리적 시스템 및 가상 시스템 배포
- 환경 및 프로세스 수립

나) 분산원장 노드 운영자

분산원장 노드 운영자는 분산원장 공급자를 위해 분산원장 시스템에서 하나 이상의 노드를 관리하고 운영하는 역할이다. 노드 운영자는 비즈니스 책임, 배포 준비, 노드 실행,

노드 관리 및 유지 보수를 포함 하여 노드의 전체수명주기를 관리한다. 노드 운영자는 분산원장 공급자의 하위 역할이다.

분산원장 노드 운영자의 주요 활동은 다음을 포함 할 수 있다.

- 고객 관계 및 재무 프로세스, 비즈니스 통계 등 비즈니스 문제 처리.
- 배포 준비 : 배포 프로세스 정의, 시스템 연속성 설계 및 감사 요구 사항 선택 등의 작업
- 시스템 준비, 배포 프로세스 구현, 보안 실행 시간대의 원장 실행, 스마트 계약 및 합의 메커니즘, 시스템 연속성 구현 및 사용자 요청에 응답하기 등의 실행 및 운영
- 관리, 보안 및 운영 : 시스템 운영 및 모니터링, 노드 복구, 자산 관리 및 보안 및 위험 관리
- 분산원장 시스템이 적절히 업데이트되도록 유지 보수

다) 분산원장 응용 운영자

분산원장 응용 프로그램 운영자는 분산원장 사용자에게 직접 또는 간접적으로 분산원장 서비스를 제공하기 위한 분산원장 응용 프로그램 / 비즈니스 시스템을 관리, 소유, 운영 및 유지 보수하는 역할이다.

분산원장 응용 운영자의 주요 활동은 다음을 포함 할 수 있다.

- 분산원장 비즈니스 서비스 제공, 모니터링 및 관리
- 경영 관리
- 개인 정보 보호
- 보안 및 위험 관리
- 감사 보고서 받기
- 문제 처리
- 컴플라이언스 보장

9.4 분산원장 개발자

분산원장 개발자는 분산원장 시스템 또는 응용 프로그램의 모든 부분 또는 구현에 대한 코드 및 특수 장비를 유지 관리하는 역할을 한다. 분산원장 개발자에게는 응용 프로그램 개발자와 분산원장 시스템 개발자라는 두 가지 하위 역할이 있다.

가) 분산원장 응용 개발자

분산원장 응용 개발자는 분산원장 시스템과 함께 실행되는 분산원장 응용 및 스마트 계

약을 생성하고 유지 관리하는 역할이다. 또한 분산원장 시스템의 노드 외부에서 실행되는 응용을 포함 할 수 있으며 노드가 제공하는 사용자 I/F를 통해 응용과 상호 작용할 수 있다. 분산원장 응용은 분산원장 사용자 또는 분산원장 공급자가 사용, 호스팅 및 실행할 수 있다.

스마트 계약 개발은 종종 양 당사자 간의 기본 거래처럼 간단한 업무에서부터 금융 서비스나 공급망과 같은 분야의 매우 복잡한 시나리오에 이르기까지 다양한 비즈니스 프로세스를 구현하기 때문에 때로는 특별한 도구와 기술이 필요하다. 승인된 비즈니스 프로세스 흐름을 따르는 스마트 계약만 배포 가능해야 한다. 이러한 스마트 계약의 메소드는 소유자나 구매자와 같은 도메인 특정 역할에 할당 된 식별자가 스마트 계약 내에서 실행될 수 있는 작업을 나타낸다.

조직에서는 특정 식별자가 응용 프로그램 및 스마트 계약의 새 인스턴스를 원장 이행(implementation)에만 배포하도록 허용 할 수 있다. 스마트 계약 생성은 응용 계층, 분산원장 플랫폼 계층 또는 스마트 계약 기능에서 관리 될 수 있다.

분산원장 응용 프로그램 및 스마트 계약 개발자는 역할 및 접근권한 요구 사항을 고려해야 한다.

분산원장 응용 개발자의 주요 활동은 다음을 포함 할 수 있다.

- 분산원장 시스템을 기반으로 비즈니스 시스템을 설계, 생성, 통합 및 유지 관리
- 분산원장 시스템에서 구성 요소 또는 스마트 계약을 설계, 생성 및 유지 관리

나) 분산원장 시스템 개발자

분산원장 시스템 개발자는 분산원장 노드의 분산원장 시스템 및 플랫폼 구성 요소를 호스트하고 실행하는 실제 및 가상 시스템을 개발하는 역할이다.

주요활동은 다음을 포함 할 수 있다.

- 분산원장 시스템의 기존 구성 요소를 사용하여 분산원장 플랫폼 구성 요소 개발
- 노드 운영자와 노드 사용자를 위한 분산원장 시스템 구성 요소 테스트

9.5 분산원장 거버너

분산원장 거버너는 전체 분산원장 시스템 및 네트워크의 거버넌스를 수행하는 역할이지만 전체 분산원장 솔루션의 거버너일 필요는 없다. 분산원장 시스템은 인프라로 간주 될 수 있고 분산원장 솔루션은 하나의 비즈니스 응용으로 간주된다. 둘 다 각각의 거버넌스를 갖지만 다른 거버넌스 기구에 의해 관리 될 수 있다. 근본적으로 분산된 시스템의 거버넌스는 새로운 거버넌스 구조와 시간이 흐르면서 변화 할 수 있는 능력을 요구할 수

있다. 일부 분산원장에서는 거버넌스가 거버넌스 기구가 아닌 이해 관계자 집단에 의해 수행된다.

분산원장 시스템이 일반적으로 여러 조직이 소유하고 운영하는 여러 노드가 있는 경우 분산원장 시스템 전체를 관리하고 분산원장 시스템이 설정된 작업을 실행할 수 있게 하는 역할이 필요하다.

분산원장 거버너의 주요활동은 다음을 포함 할 수 있다.

- 정책 개발 및 커뮤니케이션
- 분쟁 해결 및 변경 관리
- 합의 메커니즘에 대한 정책 정의
- 최소 보안 요구 사항을 포함하여 분산원장 네트워크에 참여할 수 있는 노드에 대한 정책 정의
- 분산원장 공급 업체와 협력
- 분산원장 노드 운영자와 협력하여 모니터링 및 거버넌스를 보장

9.6 분산원장 감사자

분산원장 감사자는 정책, 거버넌스 및 규정이 분산원장 시스템에서 준수되는지 확인한다. 운영자, 규제 기관, 거버너 등과 함께 작업 할 수 있다.

분산원장 감사자의 주요 활동은 다음을 포함 할 수 있다.

- 감사 증거 수집 (선택된 요구 사항, 기준, 프레임워크 또는 옵션을 충족시키기 위해)
- 분산원장 시스템 및 분산원장 응용 프로그램 감사 수행
- 감사 결과 보고

부 록 I

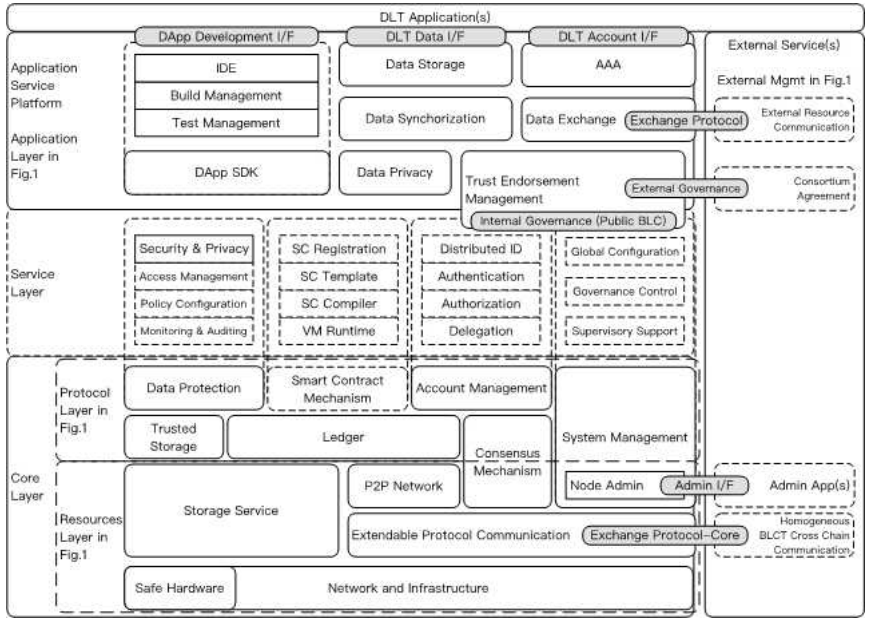
(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

관련 타 참조 구조 소개 및 비교

I-1 ISO TC 307 참조 구조

<table>
<tr><td colspan="2">Non-DLT systsms</td><td>User layer</td><td colspan="4">Cross layer functions</td></tr>
<tr><td colspan="3">API layer</td><td rowspan="3">Development</td><td rowspan="3">Management and Operation</td><td rowspan="3">Security</td><td rowspan="3">Governance & Compliance</td></tr>
<tr><td colspan="3">DLT Platform layer</td></tr>
<tr><td colspan="3">Infrasturcture layer</td></tr>
</table>

I-2 ITU-T FG-DLT 기술 프레임워크



Ⅰ-3 국제 표준 참조 구조와의 비교표

분산원장 시스템 참조 구조	TC 307 Reference architecture	ITU-T Technical framework
기반계층	Infrastructure layer	Core layer - Resources layer
-통신 네트워크	-Peer-to-Peer Network	-P2P network, Net & Infra
-연산 능력	-Compute	- Safe hardware
-스토리지	-Storage	- Storage service
분산원장 플랫폼 계층	DLT platform layer	Core layer - Protocol layer
-합의 메커니즘	-Consensus mechanism	-Consensus mechanism
-스마트 계약	-Smart contract, Secure runtime & state management	-Smart contract mechanisms, Trusted storage
-노드 간 통신	-Secure inter-node communications & Event distribution	-Consensus Mechanism
-암호	-Crypto services	-Data protection
-원장관리	-Ledger	-Ledger
-멤버십 관리	-Membership services	-Account management
인터페이스 계층	API layer	Application service platform (ASP) & External services
-사용자 I/F	-User API	DLT Applications
-관리자 I/F	-Admin API	-System management, Node Admin, Admin I/F (Core layer)
-비-분산원장 I/F	-External I/F	- Data exchange, Exchange protocol (ASP)
-타 분산원장 시스템 I/F	-InterSystem I/F	- Extendable protocol comms (Core layer)
DLT 응용 계층	User Layer	DLT Applications
-사용자 분산원장 응용	-User apps	DLT Applications
-관리자 분산원장 응용	-Admin apps	-Admin Apps(External srvs)
비-분산원장 시스템 계층	Non-DLT systems	-Trust Endorsement Management (ASP)
-분산원장 오라클	-DLT oracles	-External Governace
-비-분산원장 응용	-Non-DLT Applications	-Consortium Agreement
-오프레저 데이터	-Off-ledger data	-Consortium Agreement
타 분산원장 시스템 계층	N/A	Homogeneous BLCT Cross Chain Communication
운영관리 계층	Cross layer functions	Service Layer
-정책 관리	- Management & Operation, Governance & Policy mng	-I&A, Authorization, Delegation, Governance...
-개발 관리	- Development	-Dapp SDK (ASP) -Smart Contract (Srv layer)
-보안 관리	- Security, Risk mng	-Security and Privacy
-모니터링	- Assurance and Audit, Compliance	-Supervisory support -Monitoring and Auditing

부 록 Ⅱ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

Ⅱ-1.1 지식재산권 확약서(1)

(해당 사항 없음)

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 II-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

II-2.1 시험인증 대상 여부

(해당 사항 없음)

II-2.2 시험표준 제정 현황

(해당 사항 없음)

부 록 II-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

(해당 사항 없음)

부 록 II-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] ISO TC 307, ISO 23257 2nd CD, “Reference architecture”, 2nd CD, 9.2019

[2] ITU-T FG-DLT, “Deliverable D3.1 “Distributed Ledger Technology Architecture,” May 2019.

부 록 II-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

(해당 사항 없음)

부 록 II-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2019.XX.XX	제정 TTAx.xx-xx.xxxx	분산원장기술 참조구조 사례 연구	블록체인기반기술 프로젝트 그룹(PG1006)