TTA Technical Report

기술보고서

TTAR-xx.xxxx

제정일: 20년 xx월 xx일

*개정인 경우 최종 개정일만 기재

블록체인 등 분산원장기술 용어정의 사례 연구(기술보고서)

Case Study on Terms and Definition for Distributed Ledger Technology including Blockchain (Technical Report)

(앞 표지)

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	오경희	TCA서비스/분산원장 기술표준 포럼	대표/연구책임자	PG 1006 부의장	TTAR-xx.xxxx
기술보고서 초안 작성자	오경희	TCA서비스/분산원장 기술표준 포럼	대표/연구책임자	PG 1006 부의장	TTAR-xx.xxxx
	류재철	충남대학교/분산원장 기술표준 포럼	교수/의장		TTAR-xx.xxxx
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 블록체인을 포함하는 분산원장기술의 이해 및 사용을 돕기 위해 분산원장기술에서 사용되는 용어 정의 사례를 분석하는 것이다. 이 기술보고서의 용어는 분산원장기술 기반의 다양한 서비스 및 플랫폼 등에 활용 가능하다.

2 주요 내용 요약

이 기술보고서는 분산원장기술의 구조, 기능, 구성 요소, 서비스 및 응용 등에 관련된 용어 정의 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 on Distributed ledger technology (DLT) including blockchain terms and definitions to help in understanding and use of distribute ledger technologies. This standard is applicable to various services and platforms based on DLT.

2 Summary

The standard include terms and definitions for DLT areas, such as DLT structure, functions, components, and services/applications.

3 Relationship to Reference Standards

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

목 차

블록체인 등 분산원장기술 용어정의 사례 연구
(Case Study on Terms and Definitions for Distributed ledger Technology including Blockchain)

1 적용 범위

이 기술보고서의 목적은 블록체인을 포함하는 분산원장기술의 이해 및 사용을 돕기 위해 분산원장기술에서 사용되는 용어 정의 사례를 분석하는 것이다. 이 기술보고서의 용어는 분산원장기술 기반의 다양한 서비스 및 플랫폼 등에 활용 가능하다.

2 인용 표준

이 기술보고서는 별도의 표준을 준용하지 않는다.

3 용어 정의 사례

3.1 거래 Transaction
분산원장에 기록되는 가장 작은 단위의 비즈니스 활동.

3.2 거래 수수료 Transaction fee
블록체인에 포함된 블록을 생성한 채굴자가 그 블록에 포함된 거래에 대해 받는 수수료.
출처: [1][2]

3.3 검증자 Validator
유효성 검증을 수행하는 주체.

3.4 경량 노드 Lightweight node
원장 데이터를 보관하지 않고, 완전 노드를 통해 거래를 요청하거나 거래 데이터에 접근하는 노드 유형
출처 :[3]

3.5 권한 증명 Proof of Authority(PoA)
신뢰 가능한 1개 이상의 일부 노드에게 블록을 생성할 권한을 부여하는 합의 방식.
출처 :[3]

3.6 머클 루트 Merkle root
머클 트리에서 최종 생성된 트리 전체의 부모 노드

출처: [2]

3.7 머클 트리 Merkle tree
블록에 포함된 모든 거래를 요약하기 위해 사용되는 자료구조.

3.8 메인체인 Main chain
① 여러 분기 중 합의 알고리즘에 따라 최종 선정된 분기로 구성되는 블록체인.
② '서브체인'에 대비되는 원래의 블록체인.
③ '사이드체인'에서 하나 이상의 블록체인이 연결되어 자산이 다른 체인과 상호운용될 때 이동 자산이 원래 속한 블록체인.

3.9 무허가형 Permissionless
분산원장에 대한 어떤 활동에 승인이 필요하지 않은 특성.

3.10 방향성 비순환 그래프 Directed acyclic graph(DAG)
분산원장 환경에서 레코드들을 연결하는 방식으로써 하나 이상의 선행 레코드들을 비순환적으로, 해시 암호를 사용하여 연결하는 방식.

3.11 분기 Fork
분산원장의 프로토콜 변경이 일부 노드에서만 수용됨으로써 어느 시점 이후 서로 다른 버전의 분산원장이 발생하는 사건 또는 그 변경.

3.12 분산 애플리케이션 Decentralized application(DApp)
분산원장에서 실행되는 탈중앙화된 애플리케이션.
출처: [1]

3.13 분산원장 Distributed ledger
네트워크의 노드들 간의 합의를 통하여 일련의 노드에 걸쳐 분산되어 공유 및 보관되는 원장.
출처 :[4][5]

3.14 분산원장기술 Distributed ledger technologies(DLT)
분산원장을 생성, 운영 및 이용할 수 있게 해 주는 기술.

3.15 분산원장 네트워크 Distributed ledger network
분산원장시스템을 구성하는 노드들의 네트워크.

3.16 분산원장 노드 Distributed ledger Node
분산원장을 생성, 운영 및 이용하기 위한 기능을 제공하는 분산원장 네트워크의 구성요소.

3.17 분산원장 운영자 Distributed ledger operator
분산원장 시스템 운영 프로그램 운영자 및 운영 서버의 운영체제 운영자.

3.18 불변성 Immutability
처리가 완료된 거래가 더 이상 변경되지 않는 속성.

3.19 블록 Block
블록체인형 분산원장에서의 원장 기록의 단위로서 하나 이상의 거래 데이터의 묶음.
출처 :[6][7]

3.20 블록 생성 주기 Block time
한 블록이 새로 생성되는 시간 간격.
출처: [8]

3.21 블록체인 Blockchain
분산원장의 한 종류로써 검증되고 확정된 블록들을 순차적으로 연결하여 구성되는 분산원장.

3.22 블록체인 운영 데이터 Blockchain operation data
분산원장을 운영하는데 사용되는 데이터.

3.23 블록체인 운영 서버 Blockchain operation server
블록체인 시스템 운영 프로그램이 동작하는 서버.

3.24 블록체인 운영자 Blockchain operator
블록체인 시스템 운영 프로그램 운영자 및 운영 서버의 운영체제 운영자.

3.25 블록 헤더 Block header
블록의 메타정보가 기록된 자료구조.
출처: [1]

3.26 비잔틴 장애 허용 Byzantine fault tolerance(BFT)
일부 노드에 결함이 있거나 장애를 발생하여도 이를 허용하고 운영에 차질을 빚지 않을 수 있는 합의 방식 또는 그러한 특성.
출처: [16][17]

3.27 사용자 User
원장의 기록을 읽고 이용하거나 기록 추가를 요청하는 개체.

3.28 사이드체인 Sidechain
① 한 블록체인의 자산을 다른 독립적인 블록체인으로 전송하고 필요한 기능을 수행한 후 다시 원래의 블록체인으로 전송하기 위한 방식 또는 기술.
② 자산이 임시로 이동된 블록체인.

3.29 상태 State
프로그램 변수 값, 기타 관련 데이터로 구성되는 스마트 계약의 실행 상태.

3.30 상태 기계 복제 State machine replication
서버를 복제하고 클라이언트 상호 작용을 서버 복제본과 조정하여 내부 결함이 있어도 정상적으로 서비스를 구현하는 방식.

3.31 서브체인 Subchain
속도, 확장성, 보안 등 특정 기능을 수행하기 위해 원장의 일부를 국지적으로 관리하는 기술 또는 그렇게 관리되는 원장의 부분집합

3.32 선행 블록 Previous block
어떤 블록의 직전 블록.
출처: [1][2]

3.33 소포트 포크 Soft fork
이전 버전의 프로토콜에 따라 만들어진 원장 데이터가 새로운 버전의 프로토콜에서 유효한 것으로 승인되지 않는 프로토콜의 변경.

3.34 스마트 계옉 Smart contract
분산원장에 기록된 컴퓨터 프로그램으로써 그 실행 결과가 다시 분산원장에 기록되는 프로그램.
출처 :[9][3]

3.35 안전한 실행 환경 Secure execution environment
스마트 컨트랙트 코드가 실행되는 안전한 환경.

3.36 앵커링 Anchoring
합의된 거래 및 블록의 무결성 보장을 강화하기 위해 타 분산원장을 활용하는 기술.

3.37 엉클 블록 Uncle block
같은 선행 블록을 가진 블록.
출처: [1]

3.38 오프레저 Off-ledger
분산원장 외부에서 이루어진 프로세스 혹은 분산원장 외부에 저장된 데이터.

3.39 오프체인 Off-chain
블록체인 외부에서 이루어진 프로세스 혹은 블록체인 외부에 저장된 데이터.

3.40 온레저 On-ledger
분산원장 내에서 이루어진 프로세스 혹은 분산원장 내의 데이터.

3.41 온체인 On-chain
블록체인 내에서 이루어진 프로세스 혹은 블록체인 내의 데이터.

3.42 완전 노드 Full node
모든 원장 데이터를 보관하는 분산원장 노드의 한 유형.
출처 :[10][11]

3.43 원장 Ledger
참가자 간의 자산을 이전한 기록의 데이터나, 모든 비즈니스 활동을 거래로 기록한 데이터를 모은 집합.
출처:[12]

3.44 원장 데이터 Ledger data
분산원장 네트워크 내에서 합의를 통해 분산원장에 포함된 기록 또는 그 기록의 한 단위,

3.45 유효성 검증 Validating
어떤 거래 또는 블록이 기 수립된 유효성 검증 기준에 부합하는지의 여부를 확인하는 과정.

3.46 이중 지불 Double spending
분산원장 내에 상충하는 거래가 존재하는 상황.

3.47 이진 해시 트리 Binary hash tree
블록에 포함된 모든 거래를 요약하기 위해 사용되는 자료구조.

3.48 작업 증명 Proof of work(PoW)
특정 조건을 충족해야하는 해시 연산 등, 풀기는 어렵지만 검증하기는 용이한 문제를 통해 가장 높은 비용 및 자원을 소모한 블록(들)을 채택하는 합의 방식.
출처 :[9][2][13]

3.49 지분 증명 Proof of stake(PoS)
노드의 화폐 보유량, 거래량 등의 지분에 따라 블록 생성의 난이도를 조정하는 합의 방식.
출처 :[3][14]

3.50 참여자 Participant
원장의 기록 추가를 합의하는 의사결정 과정에 참여하는 노드 운영 주체.

3.51 채굴 Mining
유효성이 검증된 블록 또는 원장 데이터를 생성하는 활동.
출처: [10][1][2]

3.52 채널 Channel
분산원장 네트워크의 일부 노드들로 구성된 하위 분산원장.
출처 :[6]

3.53 최종성 Finality
처리가 완료된 거래가 더 이상 변경되지 않는 속성.

3.54 최초 블록 Genesis block
블록체인의 가장 첫 번째 블록.
출처: [6][3][1]

3.55 트리 노드 Tree Node
머클 트리 등 트리 형태의 데이터 구조에서 한 데이터 요소.

3.56 하드 포크 Hard fork
신규 버전의 프로토콜에 따라 만들어진 원장 데이터가 구 버전의 프로토콜에서 유효한 것으로 승인되지 않는 프로토콜의 변경.

3.57 합의 Consensus
분산원장 노드 간에 이루어지는 공동의 결정.
출처 :[6][1]

3.58 합의 가로채기 Consensus hijacking
분산원장에서 발생할 수 있는 공격 유형 중 하나로, 공격자가 합의 참여자 중 과반수, 또는 합의에 요구되는 최소 지분을 장악하여 거래 유효성 검증 프로세스를 조작하는 공격.

3.59 허가형 Permissioned
분산원장에 대한 어떤 활동을 위해 승인이 필요한 특성.

3.60 확정 Confirmed
거래가 합의에 따라 분산원장에 안정적으로 포함된 상태.

3.61 회원 Member
허가형, 사설 또는 컨소시엄 분산원장 네트워크에서 노드, 응용 프로그램 등을 운영하는 회사 혹은 조직 등, 법적으로 독립된 개체

4 약어
DAG Directed Acyclic Graph
Dapp Decentralized Application
DLT Distributed Ledger Technologies
PoA Proof of Authority
PoS Proof of Stake
PoW Proof of Work

부 록 I

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

용어 해설

I-1 블록체인의 구성

블록체인은 분산원장의 일종으로서, 원장 데이터가 여러 거래를 포함하는 블록으로 구성되며, 하나의 선행 블록을 갖는 형태로 구성된 것이다. 분산원장에는 블록체인 외에도 원장 데이터가 단일 거래로 이루어지며, 하나 이상의 선행 및 후행 거래를 갖는 등의 다양한 구성 방식이 존재할 수 있다. 블록체인 형태가 아닌 분산원장의 사례로는 R3 Corda, IOTA, Hashgraph 등이 있다.

블록체인의 블록은 블록 데이터와 블록헤더로 구성된다. 블록 데이터에는 하나 이상의 거래 데이터가 포함되며, 블록헤더에는 이들에 대한 메타정보가 포함된다. 블록헤더에 포함되는 메타정보에는 생성시간, 블록에 포함된 거래의 해시 값(머클 루트), 선행 블록의 해시 값 등이 있다.

블록체인에서의 각 블록들은 선행 블록의 해시 값을 포함함으로써 순차적으로 연결된다. 최초 블록은 블록체인을 시작하는 첫 블록이며, 따라서 선행 블록의 해시 값이 없다. 비트코인의 최초 블록의 선행 해시 값은 0으로 설정되어 있다.

블록 내의 거래 검색 경로를 최소화하기 위하여 블록에 포함된 거래들의 해시 값으로 머클 트리를 구성하여 머클 루트 값을 블록 헤더에 저장한다. 즉, 블록 내의 각각의 거래의 해시값을 머클 트리의 최종 리프(leaf) 노드에 할당하고, 두 개의 리프 노드의 데이터를 연결하여 해시한 값을 그 부모 노드에 할당한다. 이 과정을 상향식으로 반복적으로 수행하여 최종적으로 하나의 루트 값을 계산한다. 머클 루트의 데이터는 블록에 포함된 모든 거래를 하나로 요약한 해시 값이다.

I-2 분산원장의 유형 분류

분산원장의 유형을 분류하는 다양한 방식이 있다. 이중에는 사설(private) 및 공개(public), 허가형(permissioned) 및 무허가형(permissionless)[15] 등이 있다. 이런 용어들은 아직 그 의미가 시장에서 완전히 합의되지 못하고 서로 다른 방식으로 사용되고 있다.

분산원장에 관련된 활동은 크게 참여(participation)와 이용(use)으로 분류될 수 있다. 참

여는 분산원장의 생성, 변경, 유지 관리에 관련되는 활동이며 이용은 분산원장에 기록되어야 할 거래의 생성 및 기록 요청, 분산원장에 기록된 거래의 검색 등의 활동이다. 이러한 활동에 대한 제한 또는 허가의 여부에 따라 분산원장의 유형을 분류하는 것이 일반적이다. 비트코인과 같은 초기 분산원장은 이용과 참여에 전혀 제한이 없는 공개/무허가 형이었으며 이에 대비되는 IBM Fabric 등의 분산원장을 사설 또는 허가형으로 부르는 경향이 있다.

한편 EOS와 같이 참여는 제한하지만 이용에는 제한을 두지 않는 형태의 분산원장이 나타나면서 사설/공개, 허가/무허가라는 용어의 의미를 별도로 분류하고자 하는 시도가 나타나고 있다.

사설 및 공개 분산원장이라는 용어를 통제 측면에서 분류하는 입장이 있다. 즉 비트코인과 같이 운영 주체가 정해지지 않고 참여 및 이용이 자유로운 경우 공개 분산원장이라고 부른다. 이 경우 노드를 검증하거나 신뢰하지 않는다. 이와 대조적으로 하나 또는 여러 주체가 통제하는 경우를 사설 분산원장이라고 부르는 경향이 있다. 이들은 참여자를 승인하는 과정을 통해서 참여자에 대한 신뢰를 높인다. 단일 운영주체에 의한 분산원장의 경우 탈 중앙화 특성이 약화되므로 분산원장의 운영 철학에 대한 문제제기가 있다. 한편 여러 조직이 연합하여 운영하는 경우를 특정하여 컨소시엄(consortium) 분산원장으로 부르기도 한다. 컨소시엄 분산원장에서는 각 운영 주체 별로 사용자를 허가할 수도 있다.

한편, Hyperledger 진영은 사설 및 공개 여부를 이용에 대한 제한 여부에 따라 정의하고자 한다. 이들은 원장의 기록 추가와 같은 활동은 참여에 대한 제한이 있지만 일반 거래의 기록 요청 및 검색은 제한 없이 가능한 경우를 공개 허가형(public permissioned)이라고 부른다. 이 분류에 따르면 이용에는 제한이 있지만 참여에는 제한이 없는(private permissionless) 분산원장은 존재하지 않는다.

I-3 분산원장의 데이터 공유

한 분산원장 네트워크 내의 노드는 동일한 원장 데이터를 공유하는 것이 일반적이다. 그러나 데이터의 기밀성이나 처리의 효율성을 위해 노드에 따라 원장의 일부만을 저장하는 경우도 존재한다. 예를 들어 거래의 기밀성을 보장하기 위해 거래 당사자 중심으로 일부 노드들 간에서만 특정 원장 데이터를 공유하는 채널을 구성할 수 있다. 이 경우 그 원장 데이터에 포함된 거래의 유효성 검증, 합의 등의 거래 처리 절차는 해당 채널 내에서 수행 및 완료된다.

일반적으로 완전 노드는 분산원장의 전체 사본을 보관할 뿐만 아니라 유효성 검증, 합의 등의 기능도 수행한다. 이러한 노드의 기능을 수행하는 주체를 참여자(participants)라고 부른다. 참여자에는 검증자, 블록 생성자 등이 포함된다. 허가형 블록체인에서는 회원이

라고 부르기도 한다. 경량 노드는 일반적으로 유효성 검증, 합의 등의 기능은 수행하지 않는다. 거래의 기록을 요청하고 분산원장 내의 기록을 검색하는 등 이용만 하는 경우에는 사용자라고 부르기도 한다.

경량 노드는 이 블록 헤더만을 저장함으로써 원장의 용량을 최소한으로 유지하고 검색 시에는 완전 노드에 해당 블록 데이터를 요청함으로써 검색을 수행한다.

I-4 합의 알고리즘과 거래 기록의 최종성

합의 과정에는 어떤 거래 (및 블록)의 유효성 검증과 유효성이 검증된 거래들의 순서 및 원장 포함 여부의 결정이 포함된다. 유효성 검증에는 일반적으로 거래의 경우 거래 요청자가 정당한 권리를 보유(예: 암호화폐 소유자인지 여부)하였는지 여부, 이미 사용한 자산을 재사용하는 것인지 여부 등의 검증이 포함된다. 블록의 경우 블록 생성자가 합의 방식의 블록 생성 조건(작업, 지분, 권한 증명)을 만족하는지 여부를 검증한다.

작업 증명(PoW), 지분 증명(PoS) 알고리즘은 일반적으로 노드 간의 신뢰성이 낮은 공개 블록체인에서 주로 사용된다. 권한 증명(PoA), 실용적 비잔틴 장애허용(PBFT) 알고리즘은 일반적으로 노드 간의 신뢰성이 높은 사설 또는 컨소시엄 블록체인에서 사용된다.

채굴은 작업 증명 등의 합의 방식을 채택하는 블록체인에서 특정 조건을 충족해야하는 해시 연산 등 높은 비용/자원이 필요한 작업을 하는 행위를 말한다. 블록 생성을 촉진하기 위해 채굴자(miner) 에게 보상을 제공하기도 한다. 한 채굴자가 블록을 생성했을 때, 다른 채굴자가 같은 선행 블록을 가진 다른 블록을 생성한다면 이는 생성된 블록의 엉클 블록이다.

이중 지불은 악의적인 사용자가 특정 자산에 대한 거래가 블록체인 내에서 완전히 확정되기 전에 해당 거래의 결과물을 수취하고 거래를 취소하거나, 해당 자산을 재사용함으로써 발생할 수 있다. 이 두 개의 거래는 상충하지만, 서로 멀리 떨어진 다른 블록에 포함되어 일시적으로 서로 다른 노드 집단 사이에서 부분적으로 합의된 상태로 존재할 수 있다. 합의된 블록들이 전체 네트워크로 전파되면서 전체 노드의 최종 합의가 이루어지는 과정에서 한 거래는 폐기 된다.

어떤 거래가 포함된 원장 데이터(블록)가 전체 노드의 합의를 거쳐 원장에 포함되었다고 하더라도 이후 합의 알고리즘에 더 적합한 블록 집합으로 대체될 가능성이 존재한다. 따라서 일반적으로 특정 원장 데이터에 더 이상의 변경이 일어나지 않을 것으로 예상되는 조건이 발생한 경우 그 원장 데이터에 포함된 거래를 신뢰하여 확정confirm되었다고 말한다. 비트코인의 경우 어떤 블록 이후 6개의 블록이 연결되면 해당 블록이 확정되었다고 보아 블록 생성 노드에 보상을 제공한다.

금융거래의 경우 특히 거래 기록의 최종성 보장이 필요하다. 분산원장기술은 확정된 거래의 최종성 보장을 목적으로 설계되었으나, 신규 기록의 합의 과정이나 포크의 예에서 나타나듯이 항상 완전히 보장되는 것은 아니다. 소프트 포크의 경우 실제 원장이 분기되지 않을 수도 있으나 누적되는 경우 원장의 분기가 발생할 수 있다. 하드 포크의 경우 모든 노드가 새 버전의 프로토콜로 변경되지 않으면 원장이 분기된다.

I-5 스마트 계약과 분산 애플리케이션

스마트 계약은 계약을 프로그램화하여 블록체인에 등록함으로써 계약 내용의 위변조를 방지하고 계약 조건 만족 시 자동으로 계약이 실행되도록 하는 기술이다. 원장의 무결성을 보장하기 위해 스마트 계약 코드 실행 환경은 안전해야 한다.

분산 애플리케이션은 참여자 간의 계약 이외에도 다양한 응용 서비스를 제공하며 일반적으로 분산원장 내의 스마트 계약과 분산원장 외부에서 스마트 계약을 호출하는 사용자 인터페이스까지를 포함하는 용어로 사용된다. 분산 애플리케이션은 분산원장 상에서 분산되어 실행되므로 분산 애플리케이션 및 이를 통해 처리하는 정보의 위변조 방지가 가능하다.

I-6 사설 분산원장의 운영

사설 분산원장에서는 분산원장 운영자가 존재하며 구현 방식에 따라 분산원장 네트워크 운영 서버가 별도로 존재할 수 있다.

분산원장 운영데이터에는 정책, 키, 회원, 스마트 계약 상태 및 분산원장의 노드, 네트워크, 데이터에 대한 메타데이터 등이 포함될 수 있다.

앵커링은 사설 또는 허가형 분산원장의 신뢰도를 제고하기 위해 해시 값과 같은 위변조 확인이 가능한 정보를 타 블록체인, 일반적으로 공개 블록체인에 보관함으로써 필요시 위변조 여부를 확인하고 신뢰도를 제고한다.

부 록 II

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문-국문 용어 대비표

영문	국문	절 번호
Anchoring	앵커링	3.36
Binary hash tree	이진 해시 트리	3.47
Block	블록	3.19
Block header	블록 헤더	3.25
Blockchain	블록체인	3.21
Blockchain operation server	블록체인 운영서버	3.23
Blockchain operator	블록체인 운영자	3.24
Block time	블록 생성 주기	3.20
Byzantine Fault Tolerance	비잔틴 장애 허용	3.26
Channel	채널	3.52
Confirmed	확정	3.60
Consensus	합의	3.57
Consensus hijacking	합의 가로채기	3.58
Decentralized application	분산 애플리케이션	3.12
Directied Acyclic Graph	방향성 비순환 그래프	3.10
Distributed ledger	분산원장	3.13
Distributed ledger network	분산원장 네트워크	3.15
Distributed ledger node	분산원장 노드	3.16
Distributed ledger operator	분산원장 운영자	3.17
Distributed ledger technology	분산원장기술	3.14
Double spending	이중지불	3.46
Finality	최종성	3.53
Fork	분기	3.11
Full node	완전 노드	3.42
Genesis block	최초블록	3.54
Hard fork	하드 포크	3.56
Immutability	불변성	3.18
Ledger	원장	3.43
Ledger data	원장 데이터	3.44
Lightweight node	경량 노드	3.4
Main chain	메인체인	3.8
Member	회원	3.61
Merkle root	머클 루트	3.6
Merkle tree	머클 트리	3.7
Mining	채굴	3.51
Off-chain	오프체인	3.39
Off-ledger	오프레저	3.38
On-chain	온체인	3.41
On-ledger	온레저	3.40
Participant	참여자	3.50
Permissioned	허가형	3.59
Permissionless	무허가형	3.9
Previous block	선행 블록	3.32
Proof of Authority	권한 증명	3.5
Proff of stake	지분 증명	3.49

Proof of Work	작업 증명	3.48
Secure execution environment	안전한 실행환경	3.35
Sidechain	사이드체인	3.28
Smart contract	스마트 컨트랙트	3.34
Soft fork	소프트 포크	3.33
State	상태	3.29
State machine replication	상태 기계 복제	3.30
Subchain	서브체인	3.31
Transaction	거래	3.1
Transaction fee	거래 수수료	3.2
Tree node	트리 노드	3.55
Uer	사용자	3.27
Uncle block	엉클 블록	3.37
Validating	유효성 검증	3.45
Validation	검증자	3.3

※ 본 기술보고서를 작성하기 위해 참고 문헌의 용어 외에도 ISO 등에서 검토 중인 용어 등을 참고하였다. 이 중 디지털 서명(digital signature), 실체(entity), 실패(failure), 확정된 거래(confirmed transaction) 등과 같이 다른 분야에서 이미 정의된 용어로서 분산원장기술에서 추가적인 의미 변경이 없는 경우, 또는 이미 정의된 용어로 단순 수식되고 수식된 뜻이 정의된 의미 외에 다른 변경이 없는 경우는 제외하였다.

부 록 III-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

III-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 III-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

III-2.1 시험인증 대상 여부

(해당 사항 없음)

III-2.2 시험표준 제정 현황

(해당 사항 없음)

부 록 III-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

(해당 사항 없음)

부 록 III-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] Ethereum Homestead, "Glossary" [Online] Available: http://ethdocs.org/en/latest/glossary.html

[2] ethereum/wiki, "Glossary", [Online] Available: https://github.com/ethereum/wiki/wiki/Glossary

[3] BlockchainHub, "Glossary" [Online] Available: https://blockchainhub.net/blockchain-glossary/

[4] Sloane Brakevill, Bhargav Perepa, "Blockchain basics: Glossary and usecases", IBM, August 2017.

[5] ITU, "ITU Focus Group on Application of Distributed Ledger Technology" May 2017, [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[6] Hyperledger, "Hyperledger-fabric dos master documentation: Glossary", [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/glossary.html

[7] 홍승필 외 9인, "블록체인기술 금융분야 도입방안을 위한 연구", 성신여대, 금융위원회 2016.6

[8] Muhammad Ghayas. "What does "Block Time" mean in cryptocurrency?", Quora. 2018.01.21.

[9] Blockchain Technology Guide, "Blockchain Glossary", [Online]. Available: https://www.blockchaintechnologies.com/glossary/

[10] Bitcoin, "Vocabulary" [Online]. Available: https://bitcoin.org/en/vocabulary#bit

[11] Andreas M. antonopoulos, "Mastering bitcoin", O'Reily, 2014.12

[12] Christian Cachin, "Blockchain, cryptography, and consensus", ITU Workshop on "Security Aspects of Blockchain", March 2017.

[13] Bitcoin Wiki, "Vocabulary" [Online]. Available: https://en.bitcoin.it/wiki/Vocabulary

[14] 이부형, 임연주, 이종혁, "블록체인 플랫폼에서의 합의 알고리즘", 한국통신학회 2017년도 동계종합학술발표회

[15] Core Dump, "Blockchain - What is Permissioned vs Permissionless?" January 2017.

[16] Chris Colohan, "Byzantine Fault Tolerance", 2016.10.21.

[17] The loop, "BFT기반 합의 알고리즘", 2017.6.21.

부 록 III-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

(해당 사항 없음)

부 록 III-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	블록체인 등 분산원장기술 용어 정의 사례 연구	블록체인기반기술 프로젝트 그룹 (PG1006)