TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx

제정일: 2018년 12월 XX일

블록체인 용어정의

Terms and Definitions for Blockchain

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회	개인정보보호 및 ID관리, 블록체인 보안 프로젝트그룹 (PG502)
표준안 심의 위원회	정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김미연	순천향대학교	연구원	PG 502 참관위원	
표준 초안 작성자	김지혜	순천향대학교	연구원	PG 502 참관위원	
	김미연	순천향대학교	연구원	PG 502 참관위원	
	염흥열	순천향대학교/개인정보보호 표준포럼	교수/의장	PG 502 위원	
	오경희	TCA서비스/분산원장기술표준포럼	대표/연구책임자	PG 502 위원	
	임형진	금융보안원	팀장	PG 502 위원	
사무국 담당	박수정	TTA	책임	사무국	

본 문서에 대한 저작권은 TTA에 있으며, TTA와 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 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 : 2018.12.

서 문

1 표준의 목적

이 표준의 목적은 블록체인의 이해 및 사용을 돕기 위해 블록체인 용어를 정의한다. 본 표준은 블록체인 기반의 다양한 서비스 및 플랫폼 등에 적용 가능하다. 본 표준은 해외 관련 기관 웹페이지, 국제 표준 등을 근거해 국내 블록체인 용어를 정의한다.

2 주요 내용 요약

이 표준은 블록체인 이용사례, 블록체인 구조, 블록체인 기능, 블록체인 구성 요소, 서비스 및 응용 등의 용어 정의를 포함한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 타 표준 또는 기술보고서를 인용하지 않는다.

3.2 인용 표준과 본 기술보고서의 비교표

해당사항 없음

Preface

1 Purpose

The purpose of this standard is to define Blockchain terms and definitions to help in understanding and use of Blockchain technologies. This standard is applicable to various services and platforms based on Blockchain. This standard defines key terms and definitions for Blockchain taking into account website of related organizations and international standards for Blockchain.

2 Summary

The main contents of this standard include terms and definitions for Blockchain areas, such as Blockchain use cases, Blockchain structure, Blockchain functions, Blockchain components, and Blockchain services/applications.

3 Relationship to Reference Standards

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

목 차

블록체인 용어정의
(Terms and Definitions for Blockchain)

1 적용 범위

이 표준의 목적은 블록체인의 이해 및 사용을 돕기 위해 블록체인 용어를 정의한다. 본 표준은 블록체인 기반의 다양한 서비스 및 플랫폼 등에 적용 가능하다. 본 표준은 해외 관련 기관 웹페이지, 국제 표준 등을 근거해 국내 블록체인 용어를 정의한다.

이 표준은 블록체인 이용사례, 구조, 블록체인 기능, 블록체인 구성 요소, 서비스 및 응용 등의 분야의 정의를 포함한다.

2 인용 표준

이 표준은 별도의 표준을 인용하지 않는다.

3 용어 정의

3.1 원장(Ledger)
참가자 간의 자산을 이전한 기록의 데이터나, 모든 비즈니스 활동을 거래로 기록한 데이터를 모은 집합을 말한다.
출처:[1]

3.2 분산원장(Distributed ledger)
네트워크의 노드들 간의 합의를 통하여 일련의 노드에 걸쳐 분산되어 보관되는 원장을 말한다.
출처 :[2][3]

3.3 블록(Block)
거래 데이터의 묶음이며, 블록은 이전 블록과 해시로 연결되어 블록체인을 형성한다.
출처 :[4][5]

3.4 블록체인 데이터(Blockchain data)
블록을 시간 순으로 구성한 것이다. 공인된 제3자 없이 거래 기록의 무결성 및 신뢰성을 확보 가능한 탈중앙화된 분산원장 내 데이터이다.
출처 :[5][6][7][8]

3.5 블록체인(Blockchain)

동일한 목적을 가진 주체들이 운영하는 노드로 구성된 블록체인 네트워크 또는 시스템이다. 일반적으로 모든 노드는 동일한 블록체인 데이터를 공유한다.

3.6 사설 블록체인(Private Blockchain, Consortium chain, Permissioned ledger)

블록체인의 유형 중 하나이며, 운영주체가 존재하고 검증을 통해 승인된 주체만 참여 가능한 원장으로 노드 간의 신뢰성이 높다. 해외의 경우, 이를 Private Blockchains, Consortium chain, Permissioned ledger 등으로 칭한다.
출처 :[7][8]

3.7 공개 블록체인(Public blockchain, Permissionless blockchain)

블록체인의 유형 중 하나이며, 운영 주체가 불분명하고 누구나 참여 가능한 블록체인으로 노드 간의 신뢰성이 낮다. 해외의 경우, 이를 Public blockchain, Permissionless blockchain으로 칭한다.
출처 :[8][9]

3.8 최초 블록(Genesis block)

블록체인의 가장 첫 번째 블록이다. 블록체인의 초기구성 블록 역할을 한다.
출처: [4][8][10]

3.9 블록 헤더(Block header)

블록의 메타정보(생성시간, 블록에 포함된 거래의 해시 값, 부모 블록의 해시 값 등)가 기록된 자료구조이다.
출처: [10]

3.10 부모 블록(parent)

어떤 블록의 직전 블록이다.
출처: [10][11]

3.11 엉클 블록(uncle)

같은 부모 블록을 가진 블록을 의미한다. 채굴자가 블록을 생성했을 때, 다른 채굴자가 같은 부모 블록을 가진 블록을 생성한다면 이는 생성된 블록의 엉클 블록이다.
출처: [10]

3.12 머클 트리(Merkle tree)

블록에 포함된 모든 거래를 요약하기 위해 사용되는 자료구조로서 '이진 해시 트리'라고도 불린다. 트리의 최종 리프(leaf)데이터는 각 거래의 해시 값이며 부모데이터는 두 개의 리프데이터를 연결하여 해시한 값이다. 이 과정을 상향식으로 반복적으로 수행하여 하나의 트리 구조가 생성된다.

3.13 머클 루트(Merkle root)
머클 트리에서 최종 생성된 부모(루트) 데이터이며 블록에 포함된 모든 거래를 하나로 요약한 해시 값이다.
출처: [11]

3.14 노드(Node)
분산 원장을 생성, 운영 및 이용하기 위한 기능을 제공하는 분산원장 네트워크의 구성요소를 말한다.

3.15 완전 노드(Full node)
모든 블록체인 데이터를 보관하는 노드 유형이다. 일반적으로 전체 노드는 유효성 확인, 합의 등의 기능도 수행한다.
출처 :[6][12]

3.16 경량 노드(Light node)
블록체인 데이터를 보관하지 않고, 일반적으로 거래를 요청하거나 완전 노드를 통해 거래 데이터에 접근하는 노드 유형이다. 일반적으로 유효성 확인, 합의 등의 기능은 수행하지 않는다.
출처 :[8]

3.17 참가자(Participant)
원장에 접근할 수 있는 행위자로 기록을 읽거나 추가하는 역할을 수행한다.
출처 :[7]

3.18 회원(Member)
회사 혹은 조직 등, 법적으로 독립된 엔티티로, 블록체인 네트워크에서 노드, 응용 프로그램 등을 운영한다.
출처 :[4][13]

3.19 채널(Channel)
일부 노드들로 구성된 하위 블록체인이다. 일반적으로 거래의 기밀성을 보장하기 위한 목적으로 거래 당사자 중심으로 구성되며, 해당 네트워크 내에서 유효성 확인, 합의 등의 거래 처리 절차가 수행 및 완료된다.
출처 :[4]

3.20 앵커링(Anchoring)
합의된 거래 및 블록의 무결성 보장을 강화하기 위해 타 블록체인을 활용하는 기술이다. 위변조 확인이 가능한 정보(예: 해시 값)를 타 블록체인에 보관하고 필요시 위변조 여부를 확인한다.

3.21 합의(Consensus)

블록을 생성하여 노드에 전파하고 모든 노드가 이전 블록에 동일한 블록을 연결할 것인지 결정하는 일련의 과정이다.

출처 :[4][10]

3.22 비잔틴 장애 허용(BFT, Byzantine Fault Tolerance)

합의 방식 중 하나로, 일부 노드에 결함이 있거나 장애를 발생하여도 이를 허용할 수 있는 합의 방식들을 통칭한다.

출처 :[14][15]

3.23 작업 증명(PoW, Proof of work)

블록을 생성하는 노드가 작업(예: 특정 조건을 충족해야하는 해시 연산 등 높은 비용/자원이 필요한 작업)을 통해 스스로의 신뢰성을 증명하는 합의 방식이다. 일반적으로 노드 간에 신뢰성이 낮은 공개 블록체인에서 사용된다.

출처 :[7][11][16]

3.24 지분 증명(PoS, Proof of Stake)

블록을 생성하는 노드가 지분(지분 보유량, 거래량 등)을 통해 스스로의 신뢰성을 증명하는 합의 방식이다. 일반적으로 노드 간에 신뢰성이 낮은 공개 블록체인에서 사용된다.

출처 :[8][17]

3.25 권한 증명(PoA, Proof of Authority)

신뢰 가능한 일부 노드(1개 이상의 노드)에게 블록을 생성할 권한을 부여하는 합의 방식이다. 생성된 블록에 대한 전자서명 검증을 통해 정당한 노드에 의해 생성된 블록인지 확인 가능하다. 일반적으로 노드 간에 신뢰성이 높은 사설 블록체인에서 사용된다.

출처 :[8]

3.26 유효성 확인(Validating)

어떤 거래, 블록이 기 수립된 유효성 검증 기준에 부합하는지 여부를 확인하는 과정이다. 일반적으로 거래의 경우 거래 요청자가 정당한 권리를 보유(예: 가상화폐 소유자인지 여부)하였는지 여부, 이미 사용한 자산을 재사용하는 것인지 여부 등을 확인한다. 블록의 경우 블록 생성자가 합의 방식의 블록생성 조건(작업, 지분, 권한 증명)을 만족하는지 여부를 확인한다.

3.27 검증자(Validator)

‘유효성 확인’을 수행하는 주체이다.

3.28 메인체인(Main chain)

합의 알고리즘에 따라 선정된 블록체인으로 가장 긴 블록체인을 말한다.

출처 :[16]

3.29 사이드체인(Sidechain)
메인 체인에서 분기하여 갈라진 체인으로 메인 체인이 아닌 나머지 체인을 말한다.
출처 :[10]

3.30 온체인(On-chain)
블록체인 내에서 이루어진 프로세스 혹은 블록체인 내의 데이터 등을 수식할 때 사용된다.

3.31 오프체인(Off-chain)
블록체인 외에서 이루어진 프로세스 혹은 블록체인 외부에 저장된 데이터 등을 수식할 때 사용된다.

3.32 스마트 컨트랙트(Smart contracts)
분산 원장에 기록된 컴퓨터 프로그램으로써 그 실행 결과가 다시 분산 원장에 기록되는 프로그램이다. 계약을 프로그램화하여 블록체인에 등록함으로써 계약 내용의 위변조를 방지하고 계약 조건 만족 시 자동으로 계약이 실행되도록 하는 기술이다.
출처 :[7][8]

3.33 분산 애플리케이션(Dapp, Decentralized application)
블록체인에서 실행되는 탈중앙화된 애플리케이션이다. Dapp은 참여자 간의 계약 이외에도 다양한 응용 서비스를 제공하며 일반적으로 스마트 계약을 포함하는 용어로 사용된다. Dapp은 블록체인에서 분산되어 실행되므로 Dapp과 Dapp이 처리하는 정보의 위변조 방지가 가능하다.
출처: [10]

3.34 상태(State)
스마트 컨트랙트의 실행 상태(프로그램 변수 값, 기타 관련 데이터로 구성)이다.

3.35 이중지불(Double spending)
블록체인에서 발생할 수 있는 공격 유형 중 하나로, 악의적인 사용자가 자산에 대한 거래가 확정되기 전에 대가를 제공 받고 거래를 취소하거나 자산을 재사용하는 공격이다.
출처: [10]

3.36 합의 가로채기(Consensus hijacking)
블록체인에서 발생할 수 있는 공격 유형 중 하나로, 공격자가 합의 참여자 중 과반수(또는 합의에 요구되는 최소 지분)를 장악하여 거래 유효성 확인 프로세스를 조작하는 공격이다.

3.37 최종성(Finality)
처리가 완료된 거래가 더 이상 변경되지 않는 속성으로 금융거래의 경우 최종성 보장이 요구된다. 블록체인의 경우 합의 알고리즘에 따라 최종성 보장 여부가 결정된다.

3.38 채굴(Mining)
합의 방식 중 '작업 증명' 방식에서 '작업(예: 특정 조건을 충족해야하는 해시 연산 등 높은 비용/자원이 필요한 작업)'을 하는 행위이다.
출처: [6][10][11]

3.39 거래 수수료(Transaction fee)
거래를 블록에 추가하는 작업에 대한 수수료를 의미한다.
출처: [10][11]

3.40 기능 블록(Functional block)
운영 기능과 관련된 블록으로 정책, 키, 멤버쉽, 스마트 계약 관리 및 모니터링 등의 기능을 수행하며, 블록체인의 운영과 타 시스템과의 상호운영 시 요구될 수 있다.

3.41 블록체인 운영 데이터(Blockchain operation data)
블록체인을 운영하는데 사용되는 데이터로 정책, 키, 멤버쉽, 스마트 계약 상태 및 블록체인의 노드, 네트워크, 데이터에 대한 메타데이터 등이 포함될 수 있다.

3.42 실행 환경(Execution environment)
스마트 계약 코드가 실행되는 환경을 의미한다.

3.43 블록생성 주기(Block time)
한 블록이 새로 생성되는 시간 간격을 의미한다.
출처: [18]

3.44 블록체인 운영자(Blockchain operator)
블록체인 / 분산원장 시스템 운영 프로그램 운영자 및 운영 서버의 운영체제 운영자를 뜻한다. 사설 블록체인에서 주로 나타난다.

3.45 블록체인 운영 서버(Blockchain operation server)
블록체인 / 분산원장 시스템 운영 프로그램이 동작하는 서버를 뜻한다. 사설 블록체인에서 주로 나타난다.

3.46 상태 기계 복제(State machine replication)
서버를 복제하고 클라이언트 상호 작용을 서버 복제본과 조정하여 내부 결함이 있어도 정상적으로 서비스를 구현하는 방식이다.

3.47 분산원장기술(DLT, Distributed Ledger Technologies)

분산원장을 생성, 운영 및 이용할 수 있게 해 주는 기술이다.

3.48 방향성 비순환 그래프(DAG, Directed Acyclic Graph)

분산 원장 환경에서 레코드들을 연결하는 방식으로써 하나 이상의 선행 레코드들을 비순환적으로, 암호기법을 사용하여 연결하여 선행 레코드의 변경을 어렵게 한다. 블록체인은 선행 레코드가 하나만 존재하는 방향성 비순환 그래프이다.

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-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1) (스타일 적용-대항목/소항목)

해당 사항 없음

Ⅰ-1.2 지식재산권 확약서(2) (스타일 적용-대항목/소항목)

해당 사항 없음

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 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 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] Christian Cachin, “Blockchain, cryptography, and consensus“, ITU Workshop on “Security Aspects of Blockchain”, March 2017.

[2] Sloane Brakevill, Bhargav Perepa, “Blockchain basics: Glossary and usecases”, IBM, August 2017.

[3] 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

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

[5] 홍승필 외 9인, “블록체인기술 금융분야 도입방안을 위한 연구”, 성신여대, 금융위원회 2016.6

[6] Bitcoin, “Vocabulary” [Online]. Available: https://bitcoin.org/en/vocabulary#bit

[7] Blockchain Technology Guide, “Blockchain Glossary”, [Online]. Available: https://www.blockchaintechnologies.com/glossary/

[8] BlockchainHub, “Glossary” [Online] Available: https://blockchainhub.net/blockchain-glossary/

[9] Core Dump, “Blockchain - What is Permissioned vs Permissionless?” January 2017.

[10] Ethereum Homestead, “Glossary” [Online] Available: http://ethdocs.org/en/latest/glossary.html

[11] ethereum/wiki, “Glossary“, [Online] Available: https://github.com/ethereum/wiki/wiki/Glossary

[12] Andreas M. antonopoulos, “Mastering bitcoin”, O’Reily, 2014.12

[13] Josh Horton, “FAB-2288: Update Doc Glossary”, Hyperledger JIRA, Feburary 2017.

[14] Chris Colohan, “Byzantine Fault Tolerance”, 2016.10.21.

[15] The loop, “BFT기반 합의 알고리즘”, 2017.6.21.

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

[17] 이부형, 임연주, 이종혁, “블록체인 플랫폼에서의 합의 알고리즘”, 한국통신학회 2017년도 동계종합학술발표회

[18] Muhammad Ghayas. “What does ”Block Time” mean in cryptocurrency?”, Quora. 2018.01.21.

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.31	제정 TTAx.xx-xx.xxxx	블록체인 용어정의	개인정보보호/ID 관리, 블록체인 보안 프로젝트그룹 (PG502)