

블록체인 및 분산원장 국제 표준화 현황

-ISO TC 307 중심-



박성준 동국대학교 국제정보보호대학원 블록체인연구센터 센터장
ISO TC 307 전문위원회 한국 대표위원

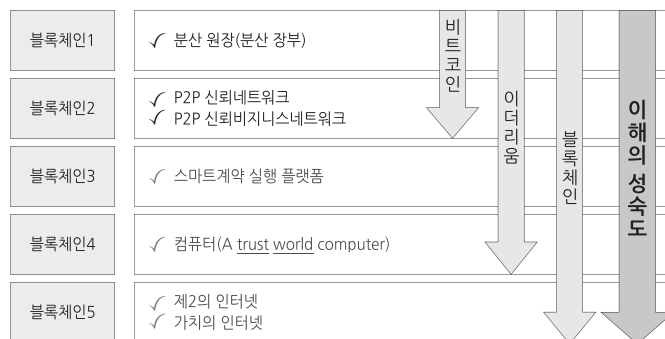
1. 머리말

블록체인(blockchain) 기술은 2008년 익명의 사토시 나카모토에 의해 창안된 P2P 전자화폐시스템 비트코인(bitcoin)에서 사용한 분산원장(distributed ledger) 개념에서 출발한다. 그러나 엄격히 분류하면 블록체인 기술은 분산원장 개념과 서로 다른 개념으로써, 2014년 이더리움에 와서야 확립된 개념이다. 일반적으로 많은 사람들이 오해하고 있는 사실이 비트코인에서 사용한 분산원장 기술과 블록체인 기술을 혼용하고 있는 것이다.

비트코인에서 사용한 분산원장 개념은 P2P 암호화폐 시스템의 가장 중요한 문제인 이중지불(double spending) 문제를 해결하기 위해 기존에 제3의 신뢰

기관(TTP, Trusted Third Party)이 중앙집중 방식으로 관리하던 거래 원장 개념을 제3의 신뢰기관 없이 P2P 모델로 참여자들이 함께 관리하는 방식으로 전환한 것이다. 그리고 상호 신뢰하지 않는 개인 간의 합의를 위한 합의 방식(consensus mechanism)으로 작업증명(PoW, Proof of Work)을 사용하였다. 작업증명 방식의 의미는 기존에 제3의 신뢰기관이 독점적으로 관리하던 원장을 참여자 모두가 원장을 갖게 하고(분산 원장), 각 참여자들이 갖고 있는 분산원장의 동일성을 확보하는 과정이라고 생각할 수 있다.

그러나 블록체인 기술은 분산원장 기술 이상의 개념을 포함하고 있으며, 블록체인의 정의는 ‘글로벌 신뢰컴퓨터’로 간주할 수 있다. [그림 1]은 블록체인



[그림 1]블록체인 기술의 5가지 정의

을 정의하는 5가지 방법을 요약하였으며, 가장 적절한 정의는 3번째 ‘스마트계약 실행 플랫폼’과 4번째 ‘글로벌 신뢰컴퓨터’로 볼 수 있다. 여기서 스마트계약이란 블록체인 컴퓨터에서 실행되는 소프트웨어로 간주할 수 있다.

많은 전문가들이 블록체인 기술을 제4차 산업혁명 시대의 핵심 기반 기술과 제2의 인터넷으로 간주하고 있으며, 현재 각국은 분산원장 및 블록체인 기술의 중요성과 미래 영향력을 깊이 인지하여 국제 표준화 활동에서도 자국의 기술이 선택되도록 각고의 노력을 기울이고 있다.

분산원장 및 블록체인 기술의 국제표준화 활동은 양대 국제표준기구인 ITU-T와 ISO에서 모두 다루고 있다. 블록체인 및 분산원장 국제 표준은 ISO TC 307에서 추진하고 있으며, 블록체인 정보보호 분야 국제 표준은 ITU-T SG17에서 다루고 있다(위원장: 순천향대 염홍렬 교수). 또한 ISO TC 307 국내표준위원회 전문위원인 오경희 위원(TCA 서비스 대표)과 나재훈 위원(ETRI) 등이 ITU-T와의 표준 협력을 위해 ITU-T SG17에서도 활동하고 있다. 블록체인 및 분산원장 기술 분야의 국제 표준을 주도하기 위해 ISO TC 307 국내 전문위원회와 ITU-T SG17과 긴밀한 협력체계를 구축하고 있으며, 올해에는 합동 회의도 개최할 예정이다. 본고에서는 ISO TC 307를 중심으로 국제 표준화 현황을 살펴보고자 한다.

2. ISO TC 307 국제 표준화 추진 연혁

2016년 9월, ISO/TMB 결의안에 의해 블록체인 기술 및 분산원장 기술 표준화를 목표로 TC 307를 설립하였으며, 제1차 총회가 2017년 4월 호주 시드니에서, 제2차 총회는 11월 일본 도쿄에서 개최되었다. 그리고 제3차 회의가 2018년 5월 14일부터 18일

까지 5일간 영국 런던에서 개최되었다.

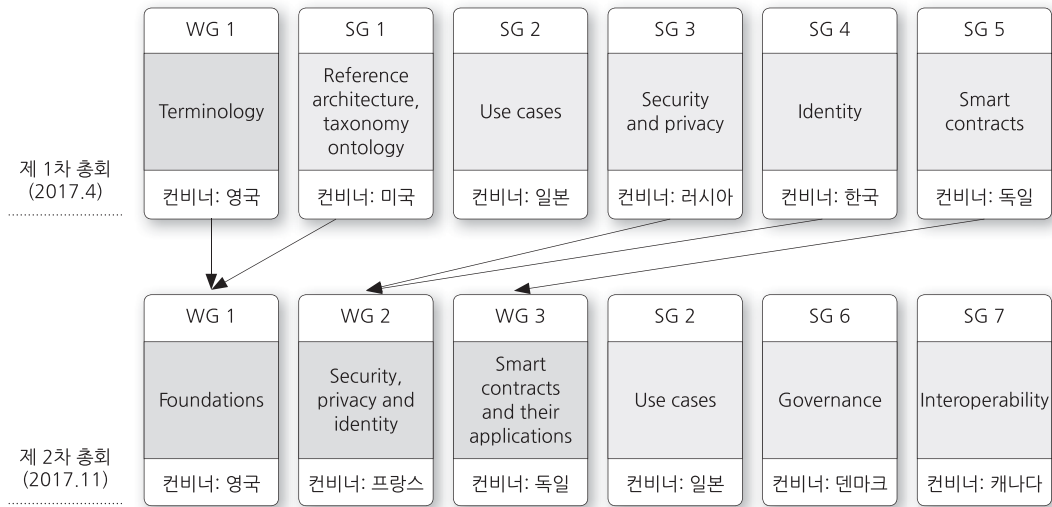
2017년 4월 1차 ISO TC 307 총회를 시작으로 분산원장 및 블록체인 기술 표준화는 1개의 WG(Working Group)과 5개의 SG(Study Group)를 구성하였다.

분류	분야	리더십
WG 1	용어(Terminology)	영국
SG 1	참조구조 및 분류체계 (RA, Taxonomy and Ontology)	미국
SG 2	유스케이스(Use Cases)	일본
SG 3	보안 및 정보보호(Security & Privacy)	러시아
SG 4	식별(Identity)	한국
SG 5	스마트계약(Smart Contracts)	독일

그리고 제2차 총회에서 상호 연관성이 높은 SG 통합과 신규 연구 활동 아이템 제안 등으로 TC 307은 대대적인 조직 개편을 추진하였다.

조직개편 주요 사항을 살펴보면 다음과 같다.

기존의 용어를 맡고 있는 WG1과 참조구조 및 분류체계를 맡고 있었던 SG1을 블록체인 및 분산원장 기술 기반(Blockchain/Distributed Ledger Technology Foundation)으로 명명한 WG1으로 통합하였다. 보안 및 정보보호를 맡고 있는 SG3와 식별을 맡고 있는 SG4를 정보보호, 개인정보보호 및 개인식별(Security, Privacy and identity)로 명명한 WG2로 통합하였다. WG2에서 다루어야 하는 표준화 내용이 방대해지는 부담이 있다는 의견도 있었으나, 참여 전문가의 인적자원 한계를 해결하고 정보보호가 여러 WG으로 분리되어 협력(Collaboration) 장애가 발생하는 것을 방지하고 효율적인 표준화 작업 진행 추진을 위해 통합하자는 의견에 따라 결정되었다. 또한 스마트계약을 맡고 있던 SG5를 스마트계약의 중요성으로 인해 WG3로



[그림 2] TC 307 조직개편 현황

승격하였다([그림 2]).

제2차 총회에서 결정된 개편된 주요 그룹들의 세부 연구 활동 내역은 2018년 3월에 특허전략개발원이 발간한 SEP Inside Vol.17의 블록체인 및 분산원장 기술 분야의 표준화 동향을 참조하길 바란다[1].

3. ISO TC 307 국제 표준화 주요 현황

현재 진행 중인 표준화 주요 활동은 다음과 같다[2].

3.1 WG1(용어 부문)

- 배경: TC 307 1차 회의에서 '용어'에 대한 WG을 관련 NWIP의 성공적 투표를 조건으로 생성 (N0068 Resolution 3)
- 투표문서: NWIP(N0082), outline(N0083)
- 투표결과: 찬성 15개국, 반대 3개국(독일, 네덜란드, 미국), 기권 2개국(핀란드, 스웨덴) (N0108)에 따라 다음의 문서 개발 착수

• 개발 문서

문서타입	제목	최종문서
표준문서	ISO/IEC 22739, 용어 및 개요 (Blockchain and Distributed Ledger Technologies -- Terminology and Concepts)	N0083

• 이슈사항(용어)

- 개요(concept) 포함 반대: 독일, 미국, 캐나다(N0108)
※ 투표기간에 한국은 concept 부분을 명확히 해야 한다는 의견을 제시, 개요 부분은 22739 또는 참조구조 문서에 포함될 것으로 예상. 어느 문서에서 작성되는지의 결정에 따라 문서의 주도권이 예상. 만약 22739에서 개요 부분을 포함하지 않는다면 22739 문서는 용어들의 설명만 있는 문서가 될 것으로 예상
- 현재 outline 문서는 ISO 포맷이 아니며 관련 정의들을 모아놓은 것에 불과함

3.2 SG1(참조구조)

- 배경: TC 307 1차 회의에서 차기 TC 307까지 참조구조, 텍사노미, 온톨로지를 위한 연구그룹 생성 (N0068 Resolution 4)
- 다음 두 문서에 대해서 NIWP 제안 작업 및 보고서 개발 중

문서타입	제목	최종문서
표준문서	참조 구조(Blockchain and distributed ledger technologies — Reference architecture)	draft : SG1/N0046
기술명세	텍사노미 및 온톨로지(Blockchain and distributed ledger technologies — Taxonomy and ontology)	NWIP for: SG1/N0049 outline : SG1/N0047
보고서	Draft Report of the TC307 Study Group 1 on Reference Architecture, Taxonomy and Ontology	SG1/N0028

• 이슈 사항(참조구조)

- 참조 구조 표준 개발에 대한 반대 국가 없음
- 참조 구조에 개요(concept) 부분 포함 제안: 개요 범위 명확치 않음
 - ※ 개요는 General concepts, System organization, Types of DLT System, Consensus, Roles, Applications & Services, Aspects of Distributed Ledgers 등을 포함하고 있음 (2017.9.21)
- 참조구조 문서 – 22739 문서와의 관계, 참조구조 문서-신규 NWIP 문서간의 관계가 불분명

• 이슈 사항(텍사노미 및 온톨로지)

- 텍사노미 및 온톨로지 문서는 ToC 정도만 작성되어 있음(2017.9.1)
- 텍사노미: 개념(용어)의 분류, 블록체인의 분류, 시스템의 분류, 유즈케이스의 분류(2017.9.14)
- 온톨로지: 개념에 대한 클래스, 속성, 그리고 관계 (2017.9.14)
- 아직까지 텍사노미 및 온톨로지에 대해서 NIWP에 대한 공감대가 있는 것은 아니라고 판단됨(2017.8.25)
 - 텍사노미/온톨로지를 RA와 별개로 만들지 말고 RA에 텍사노미를 포함해야 한다는 의견(일본), 텍사노미/온톨로지에 대해서 TS로 만들자는 의견 등이 있음(2017.9.1)
 - 텍사노미/온톨로지에 대해서 TS로 개발 결정(2017.9.15)

• 이슈 사항(SG1 리포트)

- NWIP-Reference Architecture(36개월, IS 목표)
- NWIP-Taxonomy and Ontology(48개월, TS 목표)
- NWIP를 한WG에서 개발 제안
- 신규 WG 제안 'Reference Architecture and

Fundamental Aspects of DLT*

- ToR: Progress work items that relate to the fundamental aspects of distributed ledger technology, including but not limited to a reference architecture, an ontology of DLT systems and a taxonomy of DLT systems.

- WG1(용어) 과의 관계: collaboration and alignment with on going work in WG1

• 향후 일정

- NWIP 검토(10/5), 수정보완(10/12), SG 결과 최종 승인 (10/19), TC 307로 최종 결과물 전달(10/23)

3.3 SG2(유즈케이스)

- 배경: TC 307 1차 회의에서 차기 TC 307까지 유즈케이스를 위한 연구그룹 생성(N0068 Resolution 5, 컨비너 Takeo Nishikata, Japan)
- 이슈 사항(SG 2 Report & Use case template)
 - 보고서는 마무리 단계로 최종 검토
 - Use cases template을 다른 SG에 회람 중
 - Use cases의 성격 논의 중: SD 또는 TR

• 향후 일정

- 일정 논의 중: 현안 정리 마감(10월 1차주), TC 307로 최종 결과물 전달(10/24)

3.4 SG3(보안 및 프라이버시)

- 배경: TC 307 1차 회의에서 차기 TC 307까지 보안 및 프라이버시를 위한 연구그룹 생성(N0068 Resolution 6, 컨비너(Maksim Shevchenko, Russia))

• 이슈 사항(SG3 리포트)

- 보고서는 마무리 단계로 최종 검토 중
- Security에 관해서는 추가 논의 지속
- No NWIP: Privacy 관련 사항을 TR 또는 TS로 개발 여부 논의 중
- SP 6개월 연장 여부 논의 중

- 향후 일정

- NWIP 검토 및 현안 마무리(10/4), TC 307로 최종 결과물 전달(10/24)

3.5 SG4(식별)

- SG 리포트 초안 논의 후, SG 기간 6개월 연장 제안 예정 (11월 국제회의)

3.6 SG5(스마트 콘트랙트)

- 배경: TC 307 1차 회의에서 차기 TC 307까지 스마트 콘트랙트를 위한 연구그룹 생성(N0068 Resolution 8, 컨비너 Volker Skwarek, Germany)
- 이슈 사항
 - 보고서 마무리 단계 검토 중
 - Goal에 NWIP와 다음 제안을 포함하고 별도 챕터가 존재하는 것으로 보아 NWIP에 대한 논의가 있었을 것으로 예상
 - Use cases Template에 관해 Appendix 형태로 기 제출되어 있는 걸로 보아 회람 또는 성격 논의 등의 활동 전개 중일 것으로 예상
- 향후 일정
 - Webex- CA present finished chapters 참여하여 관련 내용 F/U 예정(10/4), TC 307로 최종 결과물 전달(10/24)

3.7 SG7(상호운용성)

- 배경: TC 307 2차 회의에서 '상호운용성'에 대한 연구그룹(~런던 회의까지) 생성(N0194 Resolution)
- Tasks
 - 클라우드 컴퓨팅 상호운용성 및 이식성(ISO/IEC 19941)의 5개 주요 영역(정책, 트랜스포트, 데이터 구문, 데이터 시맨틱, 행위 시맨틱) 검토
 - 상호운용이 발생할 수 있는 DLT 시스템 인터페이스의 디스커버리 주제 포함
 - 참조구조(N0174), 거버넌스(N117), 거버넌스 덴마크 문서(N119), 영국제안(N120)을 포함한 TC307에 제출되었거나 개발되는 관련 문서 검토

- ISO/IEC 19941을 포함하지만, 이에 국한하지 않는 관련 문서 검토
- 제출된 기고서 검토
- TC 307 3차회의(런던)를 위한 보고서 개발
- DLT 시스템의 상호운용성 영역에 대한 하나 이상의 권고안 개발
- DLT 시스템과 거버넌스를 포함한 TC 307의 다른 작업과 관련

- 다음의 보고서 개발

문서타입	제목	최종문서
보고서	Draft Report of the TC307 Study Group 1 on Interoperability of Blockchain and Distributed Ledger Tehcnologies	SG7/ N0024


- 이슈 사항(리포트)

- SG7 권고안
 - (TR) Syntax and Semantics and Interoperability and Blockchain and DLT systems
 - (TR) Discovery and Interoperability and Blockchain and DLT systems
 - 'Cryptoassets and Interoperability and Blockchain and DLT systems' 관련 연구를 위해 4차 TC 307 회의까지 SG7을 연장
- (TR) Syntax and Semantics and Interoperability and Blockchain and DLT systems
 - DLT 시스템 콘텐츠가 내부적으로 또는 외부적으로 모호하게 참조될 경우 표준화된 구문과 시맨틱의 사용이 필요. SG7은 상호운용성에 대해서 DLT 시스템 페이로드에 대해서 외부와 교환을 위한 메타데이터, 전달 방식 등을 고려
 - 관련: 검색엔진(클로킹-인덱싱-검색), 레지스트리-리파지토리, Web Services-WSDL, UDDI(Universal Description, Discovery and Integration), CORBA (Common Object Request Broker Architecture)
 - TR의 scope을 개발하지 못했으며, 런던 회의에서 개발 예상
- (TR) Discovery and Interoperability and Blockchain and DLT systems
 - DLT 시스템간 정보를 찾고, 평가하고, 연결하고 매핑해야 할 때 서로 다른 DLT 시스템을 상호운용 가능하게 만들고 자동화 할 수 있도록 시스템이 속성을 게시하고 다른 시스템에서 확인할 수 있는 검색 메커니즘

- TR의 scope을 개발하지 못했으며, 런던 회의에서 개발 예상
- Cryptoassets and Interoperability and Blockchain and DLT systems
- scope을 개발하지 못했으며, 코인이나 토큰 등의 암호화 화폐에 대한 상호운용성은 아직 논의되지 않았음
- 기타
- TR, TS, IS의 구분이 모호(제안자, 그룹에 따라 각기 다른 기준 존재)
- SG 보고서 제출이 늦게 됨에 따라 NB에서 검토 후 의견 제출이 어려움. 차기 회의부터는 SG보고서는 1차 기고서 제출기한에 따라 제출 필요

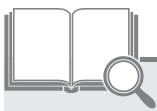
4. 맺음말

현재 블록체인 및 분산원장 기술 관련 표준 활동을 살펴보면 아직은 초기 단계라고 할 수 있으며 ISO TC 307에 제출된 많은 표준 안건들은 표준 문서 형식에서도 미흡한 부분이 많이 있다. 그러나 각국의 국제 표준회의 활동을 보면 블록체인 및 분산원장 기술의 중요성을 깊이 인지하고 있다는 사실은 분명하다.

국내의 경우 아직도 암호화폐 논쟁으로 인해 블록체인 및 분산원장 기술의 발전을 저해하고 있는 안타까운 현실이다. 암호화폐를 포함한 블록체인 및 분산원장 기술의 국제 표준 전쟁에서 조속히 우리나라가 주도적으로 선도하기 위해서는 국제 표준과 연계하여 블록체인 및 분산원장 기술의 국가 발전 로드맵이 마련되어야 할 것이며, 특히 가장 중요한 핵심 기반인 암호화폐 활성화를 조속히 추진해야 할 것이다. 

[참고 자료]

- [1] 박성준, 블록체인 및 분산원장 기술 분야의 표준화 동향, 특허전략 개발원 SEP Inside Vol.17, 2018년 3월.
- [2] ISO_TC 307 국내 표준전문위원회, TC 307 이슈리포트, 2018년 3월.



정보통신 용어 사전

<http://terms.tta.or.kr>

✓ 데이터 채굴 Data mining

인공 지능 기법을 이용하여 대용량의 데이터에서 의미 있는 통계적 패턴이나 규칙, 관계를 찾아내 분석함으로써 유용하고 활용 가능한 정보를 추출하는 기술.

지하에 묻힌 광물을 찾아낸다는 뜻의 채굴(mining)을 데이터 분석의 용어로 사용하게 된 이유는 탄광에서 석탄을 캐거나 대륙붕에서 원유를 채굴하는 작업처럼 데이터에서 숨겨진 가치를 찾아낸다는 동일한 특징 때문이다. 학문적으로는 통계, 전산, 경영 등 다양한 데이터 분석 관련 학문의 융합으로 탄생한 융합 학문이며, 기술적으로는 대용량 데이터를 효율적으로 저장 및 관리하는 기법인 데이터베이스, 데이터 창고(DW: Data Warehouse), 데이터 마트(data mart) 등과, 방대한 규모의 데이터를 분석하는 분산 처리 기술 등이 사용된다. 분석 방법으로는 목표 변수에 따라 진행되는 정형 데이터 채굴 기법과 비정형 데이터 채굴 기법이 있다. 데이터 채굴은 데이터 처리를 위한 다양한 분야에 적용할 수 있으며, 마케팅, 생산, 금융, 미디어, 순수 과학 등 다양한 산업 분야에 활용할 수 있다.