정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

ISO TC307 블록체인 정보보호 표준기술 동향

나 재 훈*

요 약

ISO/TC 307(블록체인/분산원장) 기술위원회에도 금융 이슈가 두각을 나타내고 있다. 영국이 TC 307에서의 활동은 조직적이고 열정적이다. 그 이면에는 지향하는 목표가 있다. 금융 대국 영국이 신기술 분야에서 핀테크를 어우르는 블록체인 기반 산업에서 선두 지위를 확보하고자 노력하고 있다는 것을 피부로 느낄 수 있는 활동이라고 판단이 된다. COVID-19 팬데믹의 어려움에도 불구하고 AG3 (Digital currencies)와 AHG3 (pNFT) 임시 그룹의 신설은 TC307 위원회에 신선한 자극을 주고 있다. 2022년 6월 온라인 총회를 중심으로 ISO/TC 307 기술위원회의 국제표준화 동향을 살펴본다.

Ⅰ. 서 론

ISO TC307 6월 총회의 정보보호 주요 결과로는 TR 23249 “Overview of existing DLT systems for identity management” 가 제정되었고, TR 23644 “Overview of trust anchors for DLT-based identity management (TADIM)” 표준 아이템이 2022년 제정을 예정하고 있다. 2021년 11월 회의에서 임시그룹으로 승인된 AG3 (Digital currencies)와 AHG3(Representation of physical assets as non-fungible tokens (NFT))은 중간보고를 통하여 활동 기간을 반기를 연장하여 차기 회의에서 신규표준 아이템을 제안하여 목표 설정을 명확히 할 것을 합의하였다. 스마트 컨트랙트를 관장하는 WG3의 신임 컨비너의 노력으로 사전아이템(PWI Preliminary Work Item)으로 “Smart contract classification (Project Leader: Ismael Arribas)” 표준안을 승인하므로 향후 활동을 격려하였다. ISO TC 307 사무국측은 COVID-19에 대하여 매우 보수적인 견해를 표출하며, 내년(2023년) 하반기에나 하이브리드 형태로 대면 회의를 계획하고 있다. 본 논문에서 블록체인/분산원장 국제표준화를 주관하고 있는 ISO TC307의 각 워킹그룹별로 개발하고 있는 국제표준화 동향에 대하여 살펴본다[1].

Ⅱ. ISO TC 307 구조 및 개요

2.1. ISO TC 307 (블록체인/분산원장) 구조

2022년 6월 기준으로 ISO TC 307 블록체인/분산원장기술 (Blockchain and distributed ledger technology) 기술위원회는 6개의 작업반 (Working group)으로 구성되어 표준화 작업이 진행 중이다. WG1 (Foundation)은 영국의 Geff Goodell이 맡고 있으며, 블록체인 시스템 및 서비스를 위한 기초적인 용어, 플랫폼 참조구조, 텍사노미 및 온톨로지 등의 표준을 제정하였고, 용어정의를 개정을 진행하고 있다. WG3 (Smart contract and their applicatioins)은 후임 컨비너로 스페인의 Ismael Arribas가 선출되었으며, 스마트계약 분류라는 신규표준 개발을 사전아이템을 채택받아 WG3를 이끌어가고자 노력중에 있다, 스마트계약간 상호작용 등의 표준화를 추진 중이다. JWG4 (Security, privacy and identity for Blockchain and DLT)는 TR 23249를 제정하였으며, TR 23644 분산원장 기반 신원관리를 위한 신뢰 앵커, TR 23642 스마트계약 보안 모범사례와 이슈 개요 등의 표준화를 추진하며, JTC 1/SC 27 (Infomation security, cybersecurity and privacy protection)과의 조인트 WG으로 프랑스의 Julien Bringer가 맡고 있으며, JTC 1/SC 27과 공동 관심을 갖는 프라이버시, 정보보호 취약점, 자가주권 신원관리 등의 표준화를 추진하며 (WG2는 TC307 내의 정보보호 표준개발을 목표로 활

* 한국전자통신연구원 정보보호연구본부 (전문위원/책임연구원, jhnah@etri.re.kr)

동하였으나, JWG4와의 중복성과 컨비너의 업무과다의 이유로 JWG4로 합병하고 WG2는 업무를 종료하는 것으로 합의), WG5 (Governance)은 덴마크 Roman Beck이 맡고 있으며, 거버넌스에 대하여 일반적으로 알려진 것과 같이 조직을 관리하는 것과 달리, 블록체인 시스템과 프로그램의 상호동작을 관리하는 거버넌스(관리)를 위한 지침의 표준화를 진행되어 표준 제정 (TS 23635 Guidelines for governance) 하였으며 홍보와 차기 아이템 발굴을 진행하고 있다. WG 6 (Use Cases, Caroline Tomas 영국)는 컨비너 재임용에 대하여 승인받아 3년 임기 연장이 되었다. 유스케이스 관련 표준문서를 개발 중에 있으며, 블록체인을 이용한 각 국가의 다양한 사례들을 규격화하여 분산원장 활용도를 높이기 위하여 노력하고 있다. 그리고 WG 7(상호운용성: Interoperability)은 신규과제 TS 23516 상호운용성 프레임워크 (Interoperability Framework) 승인을 득하여 SG (Study group)에서 WG으로 승격되었으며, 컨비너로 영국의 Gilbert Verdian이 임명되었다.

AHG3 (Representation of physical assets as non-fungible tokens (NFT)) 애드혹그룹은 2021년 11월 미국에서 신규 아이템 제안과 더불어 임시 그룹 신설을 승인 받아 2022년 6월회의에서 중간 보고를 하였으며, 연구기간을 6개월 연장받아 차기 회의에서 신규 아이템 제안을 계획하고 있다. AHG3의 컨비너로 Sal Francomacaro (US)가 신규 아이템 PL로는 Rohi Sukhia (US)가 임명되었다. 미국 OBADA Foundation 사의 기술결과물을 바탕으로 디지털 자산의 처분 (판매, 임대, 양도, 손실 등)을 위한 에코시스템 제안으로 물리적 자산과 디지털 자산 간의 연동을 NFT (대체 불가능 토큰)를 활용을 기반으로 차기회의에서 NP 제안을 하는 것을 합의하였다.

AG3 (Digital currencies) 자문그룹은 2021년 11월 영국 Geoff Goodell (현 WG1 컨비너)이 제안하여 임시 컨비너로 임명되었으며(적임으로 컨비너가 임명되기까지) ISO TC 307 범위를 넘어서 ISO 산하 기술위원회와 타 SDO로부터 정보를 교환하여 (Category A liaision) 현재의 기술 수준 및 표준의 현황을 조사하여 향후 표준화 전략을 수립을 목표로 활동할 것과 승인받았으며, 이를 근거로 전문가들의 지원을 요청하였다. 2022년 6월회의에서 중간보고가 있었으며, 활동기간을 연장받아 차기회의에서 결과를 보고할 것을 합의하였다. 디지털 화폐, 디지털 지불, 디지털 결제 등을 위한 정의, 요구사항, 특징, 분류 등의 분야에서 갭 분석, 방향성 제시를 논의하기 위한 디지털 화폐 자문 그룹으로 보고서의 목차가 제시되었으며, TC68과 리에종을 수립하였고, Joint AG를 추진하자는 의견이 있었으나, ISO에서는 공식적으로 Joint AG를 허용하지 않으므로 독립적 AG3로 진행할 것이며, 신규표준 아이템 차기 회의에서 제안을 예정하고 있다.

2.2. ISO TC 307 (블록체인/분산원장) 표준동향

2.2.1. 블록체인 및 분산원장 기반기술 (WG1)[2]

참조구조 표준은 (IS 23257) 블록체인/분산원장 참조구조를 개발하며, 참조구조의 개념, 구조, 기능 컴포넌트, 역할, 액티비티 및 이들의 관계에 대한 내용으로 한국의 오경희 위원이 에디터로 활동하여 2022년 술의 기반이 되는 용어(Vocaburary, IS 22739) 표준이 2020년 11월 제정이 되었으나, 주요 WG에서 신규 용어가 추가되어야 한다는 요구에 부응하여 개정(2021년 4월)이 바로 착수가 되었으며, 프로젝트 리더는 카나다의 Vitoria Lemieux가 계속적으로 역임하기로 하며, 24개월의 프로젝트 개발기간을 36개월로 연장 요청이 결의되어, 2023년 11월에 표준 제정을 목표로 개발 중에 있다.

2.2.2. 스마트계약 및 응용 (WG3)

합법 스마트계약 표준안은 (TS 23259) 공급체인(Supply chain)의 구성과 관련 법적인 내용이 포함될 것으로 예측하며, 유스케이스에 대한 더 많은 전문가가 활동하기를 독려하였지만 WG3의 전 컨비너의 사임과 맞물려 개발 진행이 원활하지 않아 이번 회의에서 삭제가 결의되었다. 컨비너 후임으로 스페인의 Ismael Arribas가 임명되었고, 신규 아이템으로 PWI Smart contract classification 이 승인되었고, 표준 개발이 원활히 진행되기를 응원하였다.

2.2.3. 거버넌스 (WG5)[4]

블록체인 시스템의 거버넌스를 위한 지침 (TS 23635) 문서는 2022년 2월 최종 표준으로 제정되었으며, DLT 시스템의 거버넌스를 위한 원칙 및 프레임워

크에 대한 가이드라인으로 의사 결정 권한과 책임 및 인센티브와 같은 주요 거버넌스 속성이 분산원장 시스템에서 효과적이고 효율적으로 작동하는 방법에 대한 내용을 포함되었다. 발간된 표준에 대해 산업계 홍보 방안 논의 하였으며(전문가들의 활용을 돕기 위한 프리젠테이션 슬라이드를 작성), 6월 27일 홍보를 위한 웨비나를 개최하였다.
(https://www.eventbrite.com/e/new-governance-standard-for-blockchain-and-distributed-ledger-technologies-tickets-346992202017)

2.2.4. 유스케이스 (WG6)[5]

ISO/DTR 3242(유즈케이스) 문서는 다양한 Blockchain/DLT 적용 사례에서 축적된 지식과 기술의 공유를 통해 기술 표준을 발전시킬 수 있는 공통된 역량, 활용 패턴 및 기술 속성에 대한 분석의 틀을 제공하며, 새로운 Use Case Pipeline을 검토 중이며, 2022년 제정을 예정하고 있으며, 그 후속 작업으로 임시 그룹 AG3와 AHG3의 유스케이스를 추가하는 것을 고려하고 있다.

ISO/WD TR 6277(블록체인과 DLT 유즈케이스를 위한 데이터 흐름) 문서는 블록체인 시스템 설계에 있어 식별자(Identifiers) 정의는 이종 간 시스템 연계를 위해 매우 중요, 식별자로써 주체와 객체를 판단할 수 있는 기준 제시를 위한 프레임워크 제시(블록체인/DLT Application 설계상의 상호호환성에 충분한 설명 제시)하며, Data flow 설계의 원칙으로써 Framework, Life Cycle, Data classification 및 specific data format requirements에 대한 논의 중에 있다.

2.2.5. 상호운용성 WG7[6]

ISO/PWI TS 23516(상호운용성 프레임워크)는 ISO/IEC 19941:2017 (Information technology − Cloud computing − Interoperability and portability) 표준과 ISO 23257:2022 (Blockchain and distributed ledger technologies − Reference architecture) 표준을 기반으로 초안 작성 중에 있으며, TS 승인을 2023년 11월 목표로 하고 있다. 4장 상호운용성 개요 작성 중, 다섯 가지 관점에서의 상호운용성 부분은 ISO/IEC 19941:2017의 내용을 기반으로 작성하고 있으며, 블록체인 및 DLT 시스템과 관련 상호운용성 부분은 ISO 23257:2022을 기반으로 DLT 시스템 간 상호운용성, 외부 Non-DLT 시스템과의 상호운용성, 클라이언트 애플리케이션 상호운용성, 관리자 애플리케이션 상호운용성에 대한 구성으로 표준 개발이 진행중에 있다.

2.2.6. 블록체인을 이용한 공동연구1 (TC 46/SC 11/JWG 1)

이 JWG1은 TC307의 구조에 속하지는 않으나, 한국 전문가들의 제안으로 JWG가 승인되어 공동연구가 진행되고 있으며, 국가기록관리 관련 시스템에 블록체인/DLT를 적용했을 때, 발생하는 도전, 고려사항, 잠재적 이점이 있는지를, 기록관리 관점에서 분석을 위하여 ISO TC 46/SC 11내에 조인트 WG 설립이 2019년 6월에 있었다. 이를 근거로 TR 24332 문서는 2020년 1월에 카나다 밴쿠버에서 합동회의 결의로 제목: Blockchain and DLT in relation to authorative records, records systems, and records management과 범위: 기록관리 관련 시스템에 블록체인 또는 DLT를 적용했을 때, 어떠한 도전, 고려사항, 잠재적 이점이 있는지를 기록관리 관점에서 분석이라는 측면에서 표준개발이 진행되고 있으며 90%의 완성도를 이루고 있다.

Ⅲ. 정보보호, 프라이버시, 신원관리 표준화 (JWG4)[4]

신원관리를 위한 분산원장기술 시스템 (ISO TR 23249)은 신원 관리를 위해 현시점에 존재하는 DLT 시스템의 개요(개체의 신원 속성 집합을 생성, 수신, 수정, 사용, 폐기하는 매커니즘 등)를 제공하는 문서로서 2022년 5월에 표준 제정되었다.

TR 23642(스마트계약 보안 모범사례와 이슈 개요)는 WG3와 공동작업하는 아이템으로, 블록체인 서비스에서 가장 중요한 보안이슈 사항인 스마트계약의 보안 관련 이슈와 보안성 확보를 위한 모범 사례를 제공하는 문서이며, 10차 총회에서 본 문서의 범위(Scope)이 이더리움 컨트랙트 개발 언어인 Solidity에 치중되어 있으며 하이퍼레저의 체인코드 등 허가형 블록체인을 포함하는 타 플랫폼의 언어도 다루어야 된다는 의견이 제시되었다. 프로젝트 리더는 본 문서의 범위에 적합한 추가 정보들을 적절하게 반영하기 위해 WG3와의 joint

〔표 1〕 ISO/TC307/JWG4 표준 목록

표준번호	제목	표준화 단계	Progject Leader
TR 23244: 2020	Privacy and personally identifiable information protection considerations	TR	Holmes Stephen (UK)
TR 23249: 2022	Overview of existing systems for identity management	TR	Paolo (IT), Ignacio Alamillo (ES)
TR 23642	Overview of smart contract security good practice and issues	WD	Stephen Holmes (UK)
TR 23644	Trust Anchors for Decentralised Identity Management	DTR	Ignacio Alamillo(ES), Patrick Curry(UK), Jae Hoon NAH(KR)
IS 7603	Decentralized Identity standard for the identification of subjects and objects	AWI	StClair Jim
TR 12833	Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies	PWI	Robin Renwick (IE)

meeting을 진행하기로 하였다.

분산원장기술 기반 신원관리를 위한 신뢰 앵커 개요(ISO TR 23644)는 분산 신원관리에서 신원인증서를 발급하는 신원증명 서비스에 반드시 필요한 Trust Anchors를 유형별로 구분 및 정의하고, 현재 산업에 공개된 DLT 기반 신원증명 기술에 적용된 트러스트 앵커의 사례를 제공하는 문서로서, 이번 10차회의에서 1차 DTR에 대한 코멘트 논의를 완료하였고 하반기에 표준 제정을 목표로 절차가 진행중에 있다. 분산 신원관리 도입을 위하여 필수적 요소 표준으로 향후 TS 표준개발을 계획하고 있다.

블록체인에서 재식별, 프라이버시 취약성 및 완화 방법 (PWI 12833) 문서는 사전 연구를 거치지 않고 JWG4에서 짧게 논의를 거쳐 바로 8회 총회 (2021년 11월)에 제기되어 승인된 아이템으로 재식별, 프라이버시 취약성 및 이를 완화하기 위한 DLT 구조에 대한 정보를 제공하는 내용으로 아일랜드의 Robin Renwick가 프로젝트 리더가 주관하여 수정된 제목 “Technical specification and guidelines for privacy capability assessment and management of privacy-preserving approaches for DLT systems”과 참조 표준으로 ISO/IEC 29190, 20889, DIS 27559을 고려하고, 본문의 Pseudo-anonymization의 내용은 타 표준으로의 통합 등에 대한 논의를 위해 추가적인 회의를 진행하기로 하였다.

AWI 7603(주체와 객체의 식별을 위한 탈중앙형 신원 표준)는 W3C의 DID 및 VC(Verifiable Credentials) 관련 표준 등 탈중앙형 신원과 관련된 표준현황 등을 다루기 위한 신규 아이템으로 프로젝트 리더의 사유로 인해 10차 총회 개최 시점에도 완료되지 않음, 회의에서 일부 전문가들은 6개월간의 기간에도 불구하고 문서 개발에 진척이 없으므로 프로젝트 취소 의견 제시하였으나, Ignacio Alamillo (ES)를 프로젝트 리더로 지명하고 표준개발을 지속하기로 협의 하였다.

Ⅳ. 결 론

제10회 총회에서는 블록체인을 기반으로 금융 자산에 대한 기술이 돋보이는 회의 였다고 판단된다. 아직은 시작에 불과하지만 핀테크와 연관하여 블록체인 기술의 영역을 확고히 하는 것이 매우 의미 있는 행보라 할 수 있다. 미국을 중심으로 NFT의 표현에 대한 표준이 준비중에 있으며, 영국을 중심으로 디지털 화폐에 대한 논의가 진행되고 있다. 이러한 기술 표준들과 분산/탈중앙 신원관리 기술표준은 연계는 필연적인 것이라 판단되며, 국제표준화 기조와 병행하여 국내 기술 및 표준화를 경쟁구도로 진행을 하여야 한다고 판단된다.

ISO/TC 307 (블록체인/분산원장) 기술위원회는 2016년 9월에 설립되어 만 6년이 경과하였으나, 상대적으로 새내기 기술위원회라고 할 수 있다. 금융권에서는

탈중앙이라는 용어보다는 탈중개라는 용어를 선호한다. 즉 중앙집중식에서 분산으로 가는 것을 의미하는 것이 아니라, 중개인이 없는 인프라에서 신뢰를 구축하는 것을 의미한다.

TC 307은 선진국들이 주도적으로 운영하는 위원회라 평가된다. 그 이유는 영국이기술위원회를 주도적으로 운영을 하고자 노력하는 모습이 부각되고 있다. 현재 WG1(Foundation), WG6(Use cases), WG7(Interoperability)의 컨비너가 영국 출신이며, 금융 인프라가 발달된 영국이 블록체인에 많은 관심을 갖고 있다는 것은 매우 고무적인 사항이며, 향후 지속적으로 관심을 가지고, 유대관계를 유지할 필요가 있다고 사료되며, WG3는 스페인 출신의 컨비너, JWG4는 프랑스 출신의 컨비너, WG5는 네덜란드 출신의 컨비너가 회의를 진행하고 있다. JTC 1/SC 27 출신의 미국 Salvatore Francomacaro가 JWG4의 공동 컨비너로 활동하고 있는 것 또한 간과해서는 안될 것으로 사료된다.

이러한 국제표준화 환경에서 한국은 모바일 운전면허증을 시행하는 국가의 측면에서 분산ID의 기술 저변 확대와 상호운용성 측면에서 표준화가 같이 병행되어야 할 것으로 판단되며, 한국에서 추진하고 있는 분산ID를 암호화폐 이후 사회 기반기술로 발전시키기는 전략이 필요한 때라고 사료된다.

참 고 문 헌

[1] ISO/TC307 N908 Meeting 10 Resolutions - Virtual 05-2022, 2022., 06.
[2] ISO/TC307 N868 WG1 Report 2022., 04.
[3] ISO/TC307 N904 JWG4 Report 2022., 06.
[4] ISO/TC307 N905 WG5 Report 2022., 06.
[5] ISO/TC307 N872 WG6 Report 2022., 04.
[6] ISO/TC307 N873 WG7 Report 2022., 06.

〈저 자 소 개〉

나 재 훈 (Jae Hoon NAH)
종신회원
1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 정보공학 박사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원
2019년~현재 : ICT 국제표준화 명장
2018년 7월~현재 : TC307 HoD/대표전문위원
2009년~현재 : ITU-T SG17 WP4의장, Q7 라포처
2011년~현재 : 한국정보보호학회 이사
2011년~현재 : 한국정보보호학회 학회지 정보보호 국제표준 특집호 책임 편집위원/의장
<관심분야> 블록체인보안, 핀테크보안, 웹보안, 스마트시티보안, 익명인증, 6G보안