정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

ISO TC307 블록체인 정보보호 표준기술 동향

나 재 훈*

요 약

ISO TC 307(블록체인/분산원장) 기술위원회는 영국, 미국, 프랑스, 독일등 서방국가들이 적극적으로 표준화 활동을 하고, 기업은 IBM, MS사의 활동이 두각을 나타내고 있다. 위원회의 구조와 표준화가 초기 단계를 지나 표준화 인프라를 구축하였다고 볼 수 있으며, 블록체인 기술을 기반으로 활용사례 표준 개발을 병행하며, 표준의 효용성을 높이려는 시도가 진행되고 있다. 인도 하이데라바드 (2019.11) 회의 이후 COVID-19로 온라인으로 회의가 개최되고 있으며, 2021년 6월 총회를 중심으로 ISO TC 307 기술위원회의 국제표준화 동향을 살펴본다.

Ⅰ. 서 론

다른 많은 국제회의가 그렇듯이 ISO TC307 국제표준화도 인도 하이데라바드 회의(2019년 11월) 이후에는 COVID-19로 인하여 비대면 회의로 진행을 하고 있으며, 지난 2021년 6월에 온라인으로 있었던 총회를 기준으로 진행되고 있다.

ISO TC307 6월 총회의 주요 결과로는 정보보호 관련 “Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies” 라는 제목으로 아일랜드의 Robin Renwick가 제안한 신규아이템 채택에 대한 승인이 있었다. 스마트 컨트랙트를 관장하는 WG3의 컨비너가 사임으로 후임 컨비너의 선출을 위한 투표가 진행되고 있음이 공지되었으며, 다양한 플랫폼간의 서비스 의 상호운용성을 보장하기 위한 필요성이 두각이 되어 “Interoperability Framework” 신규 아이템에 대한 투표가 진행되고 있으며, 이 아이템이 승인되면 SG(Study Group)7이 WG(Working Group) 7으로 정규 그룹으로 승격과, 영국의 Gilbert Verdian이 컨비너로 자동 임명이 예정되어 있다. 이로써 영국출신 컨비너가 WG1, WG6와 더불어 3명이 된다. 국가적 배분이 깨지는 상황이 되이지만, 영국이 블록체인 국제표준화 부분에서 강력한 의지가 표출되는 결과라 판단된다. 그리고 정보보호 관련하여 WG2와 WG4로 두 개로 운영되었던 것인데, WG2가 최종 폐지되고, WG4에서 총괄하여 정보보호 표준 개발을 결의하였다. WG4는 ISO/IEC JTC 1/SC27 과의 협력관계를 가지고 있으며, WG4에서 개발되는 모든 문서를 JTC 1/SC27에서 추가적인 검토와 코멘트를 제출한다는 협정이 체결되어 있어서, 상호협력이 진행되고 있다.

블록체인/분산원장에서 PoW(Proof of Work) 합의 알고리즘은 근본적으로 성능 문제를 안고 있으며, 이를 개선하고자 주도적으로 활동을 표현한 국가는 인도이었다. 그러나 하이데라바드 회의(2019년 11월) 이후에 구체적인 결과가 제시가 되지 않아서, TC307 총회에서는 인도 대표자들이 참석하지 않아 차기 회의에서 재논의 할 것을 결의하였다.

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

2021년 6월 기준으로 ISO TC 307 블록체인/분산원장기술 (Blockchain and distributed ledger technology) 기술위원회는 5개의 작업반 (Working group)과 1개의 연구반 (Study group)이 구성되어 표

본 논문은 2021년도 산업자원통산부의 재원으로 국가표준기술력향상사업의 일환으로 수행되었음.[20005255, 블록체인 기술을 활용한 적합성업무 관리 참조모델 운영 및 표준화 전략]
* 한국전자통신연구원 정보보호연구본부 (전문위원/책임연구원, jhnah@etri.re.kr)

준화 작업이 진행 중이다. WG1 (Foundation)은 영국의 Geff Goodell이 맡고 있으며, 블록체인 시스템 및 서비스를 위한 기초적인 용어, 플랫폼 참조구조, 텍사노미 및 온톨로지 등의 표준화를 추진하고 있으며, WG3 (Smart contract)은 독일의 Volker Skwarek이 맡고 있었으나 사임을 표명하여 후임 컨비너 선출을 위하여 투표가 진행중이며, 적법한 스마트계약, 스마트계약간 상호작용 등의 표준화를 추진 중이며, WG4 (Security, Privacy and Identity for Blockchain and DLT)는 분산원장 기반 신원관리를 위한 신뢰 앵커, 스마트계약의 정보보호 이슈 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 공동관심을 갖는 프라이버시, 정보보호 취약점, 자가주권 신원관리 등의 표준화를 추진하며 (WG2는 TC307 내의 정보보호 표준개발을 목표로 활동하였으나, 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 것이 아니고, 블록체인 시스템과 프로그램의 상호동작을 관리하는 거버넌스(관리)를 위한 지침의 표준화가 진행되어 표준 제정을 앞두고 있다. WG 6 (Use Cases, Caroline Tomas 영국)는 유스케이스 관련 표준문서를 개발 중에 있으며, 블록체인을 이용한 각 국가의 다양한 사례들을 규격화하여 분산원장 활용도를 높이기 위하여 노력하고 있다. 그리고 SG 7 (상호운용성: Interoperability)의 신설에 관하여는 신규과제 TS 상호운용성 프레임워크(Interoperability Framework) 승인을 위한 투표중에 있으며, 컨비너로 영국의 Gilbert Verdian이 역임하고 있다.

2.2. ISO TC 307 (블록체인/분산원장) 표준동향

2.2.1. 블록체인 및 분산원장 기반기술 (WG1)[2]

블록체인 및 분산원장 기술의 기반이 되는 용어 (Vocaburary, IS 22739) 표준이 2020년 11월 제정이 되었으나, 주요 WG에서 신규 용어가 추가되어야 한다는 요구에 부응하여 개정(2021년 4월)에 바로 착수가 되었으며, 프로젝트 리더는 카나다의 Vitoria Lemieux가 계속적으로 역임하기로 하며, 24개월의 프로젝트 개발기간을 36개월로 연장 요청이 결의되어, 표준 개발이 진행중에 있다. 참조구조 표준은 (IS 23257) 블록체인/분산원장 참조구조를 개발하며, 참조구조의 개념, 구조, 기능 컴포넌트, 역할, 액티비티 및 이들의 관계에 대한 표준을 개발하여 DIS 통과하였지만, ISO/CS(Central Secretariat)로부터 받은 코멘트를 해결하여 FDIS 거쳐, 2022년 1월 30일경에 표준 제정을 예정하고 있다. 텍사노미 및 온톨로지 표준안은 (TS 23258) “블록체인 및 분산원장기술의 용어, DLT 시스템, 유즈케이스“의 텍사노미와 “클래스, 속성, 그리고 용어들의 관계“를 설명하는 온톨로지를 개발하여 DTS 발행을 위하여 TS 초안을 제출하였으며, ISO/CS의 편집 결과를 최종 검토하여 TS 발행 예정이다.

2.2.2. 스마트계약 및 응용 (WG3)

이미 발행된 스마트계약 상호작용 및 개요 표준 (TR 23455)에 그림 8과 그림 9가 동일한 그림이 중복 삽입되어 있음을 2019년 11월 인도 하이데라바드 회의에서 한국 전문가가 지적하여, 웹 미팅에 보고되어 TC 307 사무국 및 ISO 편집위원회에서 후속대응을 논의중에 있으며, 오류정정 발행이 지연되고 있다. 합법 스마트계약 표준안은 (TS 23259) 공급체인 (Supply chain)의 구성과 관련 법적인 내용이 포함될 것으로 예측하며, 유스케이스에 대한 더 많은 전문가가 활동하기를 독려하고 있다. 이와 유사한 표준안이 BSI에서 개발되고 있음을 웹미팅에서 공유되었다 (BSI PAS 333 “Smart legal contract - Specification”).

2.2.3. 거버넌스 (WG5)[4]

블록체인 시스템의 거버넌스를 위한 지침 (TS 23635) 문서는 DTS (Draft TS) 투표(6월25일)를 거쳐 2021년 내에 제정을 목표하고 있다. DLT 시스템의 거버넌스를 위한 원칙 및 프레임워크에 대한 가이드라인으로 의사 결정 권한과 책임 및 인센티브와 같은 주요 거버넌스 속성이 분산원장 시스템에서 효과적이고 효율적으로 작동하는 방법에 대한 내용을 포한다.

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, 2021년 시작 예정인 2차 Edition 진행에 대하여 논의 중에 있다.

ISO/WD TR 6277(블록체인과 DLT 유즈케이스를 위한 데이터 흐름) 문서는 블록체인/DLT 애플리케이션 설계 및 시스템 분석을 지원하기 위해 활용 사례 개발에서 데이터 흐름의 설명 프레임워크와 블록체인/DLT 데이터 흐름의 특성을 이해하기 위한 기초 표준을 제공(블록체인/DLT Application 설계상의 상호호환성에 충분한 설명 제시) 하며, Data flow 설계의 원칙으로써 Framework, Life Cycle, Data classification 및 specific data format requirements에 대한 추가를 논의 중에 있다.

2.2.5. 상호운용성 연구그룹

ISO/PWI TS 23516(상호운용성 프레임워크)의 신규 프로젝트(NP)의 승인(~7/2 NP 투표 진행 중) 조건으로 '상호운용성' 표준 개발을 담당하는 WG 7을 신설에 대하여 NP 투표 결과를 차기 11월회의에서 결의가 있을 예정이며, WG7의 컨비너가 정식으로 임명되기 전까지 SG7의 컨비너인 Gilbert Verdian (영국)이 대행하기로 결의하였다.

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 문서 개발을 위하여 2020년 1월에 카나다 밴쿠버에서 합동회의가 있었으며, 제목 및 범위를 다음과 같이 조정하였다.

제목: Blockchain and DLT in relation to authorative records, records systems, and records management

범위: 기록관리 관련 시스템에 블록체인 또는 DLT를 적용했을 때, 어떠한 도전, 고려사항, 잠재적 이점이 있는지를 기록관리 관점에서 분석

Ⅲ. 정보보호, 프라이버시, 신원관리 표준화 (JWG4)[4]

일본 주도로 발간된 ISO TR 23576:2020의 후속조치로, 발간된 문서를 기반으로 TS 제안을 목표로 사전연구가 진행중에 있다. 암호화폐 거래소 정보보호 가이드라인 기술보고서 (TR 23576:2020 Security of digital asset custodians)는 암호화폐 거래소 디지털 자산 관리를 위한 가이드라인의 내용을 담고 있다. 이 기술보고서는 일본의 암호화폐 거래소 MtGox의 도난사고를 분석하여 거래소의 디지털 자산의 관리를 위한 정보보호 가이드라인 개발을 목표로 한다. 거래소의 안전성 제고를 목표하기에 많은 관심을 갖고 있었지만, MtGox의 해킹에 대하여 확실하게 원인 규명이 안됐다는 것에 실망이 전문가들에서 표명되고, 이러한 이유로 개정을 진행하는 이슈가 제기되었으며, 2020년 6월 회의에서 일본의 Shinichiro Matsuo와 영국의 Aldo Lo Castro가 사전연구 아이템 프로젝트 리더로 선임 되었다.

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, 분산 신원관리 도입을 위하여 필수적 요소 표준으로 향후 TS 표준개발을 계획하고 있다.

신원관리를 위한 분산원장기술 시스템 (ISO DTR 23249)은 신원 관리를 위해 현시점에 존재하는 DLT 시스템의 개요(개체의 신원 속성 집합을 생성, 수신, 수정, 사용, 폐기하는 매커니즘 등)를 제공하는 문서로서 JWG4 10차 미팅('21.3)에서 결정된 바에 따라 Final DoC(N206)을 반영한 Final Draft DTR이 ISO/CS 편집자에게 송부되었으며, 향후 발간을 준비중에 있다.

스마트계약 보안 모범사례와 이슈 개요 (ISO/AWI TR 23642 Security issues on smart contract) 블록체

인 서비스에서 가장 중요한 사항인 스마트계약의 보안 관련 이슈와 보안성 확보를 위한 모범 사례를 제공하는 문서로서 WD2에 대한 DoC 작성 완료(~6/11), DoC를 반영한 WD3 개발(~7/9), WD3에 대한 코멘트 요청 및 기고 요청(~9/15) 일정으로 작업이 진행되고 있다.

신규 표준 아이템으로 블록체인과 DLT에서의 재식별, 프라이버시 취약성 및 완화 방법 (PWI Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies) 문서는 사전 연구를 거치지 않고 JWG4에서 짧게 논의를 거쳐 바로 총회에 제기되어 승인된 아이템으로 재식별, 프라이버시 취약성 및 이를 완화하기 위한 DLT 구조에 대한 정보를 제공하는 내용으로 아일랜드의 Robin Renwick가 프로젝트 리더로 임명되어 기고서를 요청하여 작업에 착수하기로 합의하였다.

Ⅳ. 결 론

블록체인은 산업 영역에서 기원되어, 학문적 체계가 필요한 기술영역이다. 특히 2021년에는 DeFi (Decentralized Finance), NFT (Non-fungible Token), CBDC (Central Bank Digital Currency) 등과 같은 기술은 갑자기 부각되고 있으며, NFT의 진본성을 기반으로 하는 디지털 자산의 거래는 산업적 반응을 고무시키고 있다.

ISO TC 307 (블록체인/분산원장) 기술위원회는 2016년 9월에 설립되어 만 5년이 경과한 새내기 기술위원회라고 할 수 있다. 블록체인/분산원장을 논하는 기초 표준인 용어는 발간되었으나, 각 WG별 신규 용어의 추가적인 작업이 요구되어 개정작업에 있으며 참조구조 표준은 제정을 위한 절차를 밟고 있는 상황이다. 탈중앙이라는 네트워크 인프라의 전환은 IT구조를 통째로 바꾸는 것은 아니다. IT 서비스들 중에 탈중앙 구조가 유익하고 효율적인 서비스 영역이 있다. 장부를 기반으로 하는 업무가 이에 속한다고 판단되며, 그 위에서 비즈니스가 처리되는 스마트 계약이 그 업무 영역에 속한다고 할 수 있다. 그리고 탈중앙 네트워크 인프라는 OSI 7 계층의 응용단에 놓여있는 가상적 네트워크이다. 이러한 구조로 인하여 하부의 물리적 프로토콜 스택의 한계점을 품고 있으며, 그 상위에서 논리적 연계와 서비스 제공은 하부구조의 고성능과 고기능이 필요하다. 더 나아가 사람과의 인터페이스를 포함하고 있기 때문에 지능화에 대한 요구가 있어서, 6G 네트워크의 응용서비스의 제로터치(Zero Touch)의 개념과도 상통하는 면이 있다.

이번 6월 총회의 분위기는 여전히 영국이 주도권을

〈표 1〉 ISO TC307/JWG4 표준화 현황

표준번호	제목	표준화 단계	Progject Leader
ISO TR 23576	Security management of digital asset custodians	Study	Shin'ichiro Matsuo (JP), Alodo Lo Castro (UK)
ISO TR 23642	Overview of smart contract security good practice and issues	NP	Stephen Holmes(UK)
ISO TR 23245	Security risks, threats and vulnerabilities	Study	Julien Bringer(FR)
ISO/IEC TR 23249	Overview of existing systems for identity management	DTR	Paolo (IT), Ignacio Alamillo (ES)
ISO TR 23644	Trust Anchors for Decentralised Identity Management	WD	Ignacio Alamillo(ES), Patrick Curry(UK), Jae Hoon NAH(KR)
ISO TR xxxx*	Re-identification and privacy vulnerabilities and mitigation methods in blockchain and distributed ledger technologies	PWI	Robin Renwick (IE)

* 번호 할당을 기다리는 표준

가지고자 노력하는 의도가 부각되고 있다. 현재 WG1, WG6의 컨비너가 영국 출신이며, 차기 회의에서 신규 WG으로 승격이 예상되는 SG7의 현재 컨비너가 영국 출신이다. 금융 인프라가 발달된 영국이 블록체인에 많은 관심을 갖고 있다는 것은 지속적으로 관심을 가지고, 유대관계를 유지할 필요가 있다고 사료되며, 정보보호 측면에서는 WG4의 프랑스 출신이 컨비너를 역임하고 있으며, JTC 1/SC 27에서 활동을 하고 있는 미국의 Salvatore Francomacaro가 코-컨비너로 활동하고 있는 것 또한 간과 해서는 안될 것으로 사료된다.

이러한 국제표준화 환경에서 한국은 운전면허증 및 공무원증을 디지털화 하는 국가의 정책사업의 측면에서 분산ID의 기술 저변확대와 상호운용성 측면에서 표준화가 같이 병행되어야 할 것으로 판단되며, 한국에서 추진하고 있는 분산ID를 암호화폐 이후 사회 기반기술로 발전시키기를 희망한다.

참 고 문 헌

[1] ISO TC307 N763 Meeting 08 Report 2021. 06.

[2] ISO TC307 N733 WG1 Report 2021. 06.

[3] ISO TC307 N735 JWG4 Update-to-TC307-plenary_v2 2021. 06.

[4] ISO TC307 N734 WG5 Gevernance Report for June 2021 Plenary 2021. 06.

[5] ISO TC307 N736 WG6 Report for June 2021 Plenary 2021. 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 : 글로벌ICT표준마에스트로

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