정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

ISO/TC 307 블록체인 정보보호 표준기술 동향

나 재 훈*

요 약

ISO/TC 307(블록체인/분산원장) 기술위원회는 영국, 미국, 프랑스, 독일등 서방국가들이 적극적으로 표준화 활동을 하고 있으며, 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 병행하여, 표준의 효용성을 높이려는 시도가 진행되고 있다. 인도 하이데라바드 (2019.11) 회의와 COVID-19로 인하여 온라인으로 개최한 2020년 6월 회의를 중심으로 ISO/TC 307 기술위원회의 표준화 동향을 살펴본다.

Ⅰ. 서 론

인도 하이데라바드 회의(2019년 11월)에서는 인도가 하이데라바드를 IT기반의 중심도시로 육성을 계획하며, 블록체인/분산원장 분야에 중심 역할을 하고자 심혈을 기울였던 회의였으며, 블록체인/분산원장 기술 관련하여 성능개선을 위하여 노력을 집중하고 있음을 감지할 수 있었다.

블록체인/분산원장에서 PoW(Proof of Work) 합의 알고리즘은 하나의 블록을 생성하기 위하여 최소한의 시간을 보장하고 있다. 이것은 이중지불을 방지하기 위하여 고안된 탈중앙의 핵심 메커니즘이다. 즉 서비스를 제공하기 위하여 순기능을 설계하다가 후에 보안 기능을 추가하였던 시스템 개발 접근 방법에서 서비스를 제공하기에 안전을 우선적으로 고려한 후에 성능개선을 추구하는 형국이라고 볼 수 있다. 이러한 근본적인 성능 문제를 안고 있지만, 블록체인/분산원장은 암호화폐를 통하여 탈중앙성과 안전성을 보여주었다. 그리고 이더리움을 개발한 비탈릭 부테린은 블록체인 트릴레마 문제를 제기하였다[1].

본 논문에서 블록체인/분산원장 기반의 안전한 서비스를 위하여 제공되고 있는 기술과 상호운용을 위한 표준화의 동향에 대하여 살펴본다[2-4].

Ⅱ. ISO TC 307 구조 및 개요

2.1. ISO TC 307 (블록체인/분산원장) 구조

2016년 설립된 ISO TC 307 블록체인/분산원장기술(Blockchain and distributed ledger technology) 기술위원회는 2020년 7월 현재 6개의 작업반 (Working group)과 1개의 연구반 (Study group)이 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 표준화를 추진하고 있으며, WG2 (Security, Privacy and Identity)는 프랑스의 Julien Bringer가 맡고 있으며, 거래소 안전관리, 스마트계약의 정보보호 이슈 등의 표준화를 추진하며, WG3 (Smart contract)은 독일의 Volker Skwarek이 맡고 있으며, 적법한 스마트계약, 스마트계약간 상호작용 등의 표준화를 추진 중이며, WG4는 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, WG5 (Governance)은 덴마크 Roman Beck이 맡고 있으며, 거버넌스에 대하여 일반적으로 알려진 것과 같이

본 논문은 2020년도 산업자원통산부부의 재원으로 국가표준기술력향상사업의 일환으로 수행되었음.[20005255, 블록체인 기술을 활용한 적합성업무 관리 참조모델 운영 및 표준화 전략]
* 한국전자통신연구원 정보보호연구본부 (전문위원/책임연구원, jhnah@etri.re.kr)

조직을 관리하는 것이 아니고, 블록체인 시스템과 프로그램의 상호동작을 관리하는 거버넌스(관리)를 위한 지침의 표준화가 진행되고 있다. 그리고 지난 2019년 5월 더블린 회의에서 승인된 WG 6 (Use Cases, Caroline Tomas 영국)가 유스케이스 관련 표준문서를 개발 중에 있다. 그리고 SG 7(상호운용성: Interoperability)의 신설에 관하여는 신규과제 TR 상호운용성 프레임워크 (Interoperability Framework) 승인을 2019년 5월 회의에서 조건으로 합의 하였으나, 컨비너가 인도 하이데라바드 회의에 미참 함으로 진행이 원활하지 못한 상태에 있다.

2.2. ISO TC 307 (블록체인/분산원장) 현황

2.2.1. 블록체인 및 분산원장 기반기술 (WG1)

블록체인 및 분산원장 기술의 기반이 되는 용어표준 (IS 22739)이 FDIS 투표를 통과하여 제정을 앞두고 있으며, 7월 최종 코멘트 해결을 진행하여 2020년 내에 발행을 계획하고 있다. 참조구조 표준은 (IS 23257) 블록체인/분산원장 참조구조를 개발하며, 참조구조의 개념, 구조, 기능 컴포넌트, 역할, 액티비티 및 이들의 관계에 대한 표준을 개발 중이며, 이번 회의에서는 세 번째 CD 투표 코멘트에 대한 이슈 해결 및 문서 작업을 수행하였으며, 이번 6월 회의에서는 DIS 투표 준비를 진행하였으며, 내년 (2021년) 표준문서 발행을 계획하고 있다. 택사노미 및 온톨로지 표준안은 (TS 23258) “블록체인 및 분산원장기술의 용어, DLT 시스템, 유즈케이스“의 텍사노미와 “클래스, 속성, 그리고 용어들의 관계“를 설명하는 온톨로지를 개발 중이며, 용어 및 양식 제공, 유스케이즈 택사노미 개발을 위하여 WG6와의 협력을 진행하여, 2022년 표준문서 제정을 계획하고 있다.

2.2.2. 스마트계약 및 응용 (WG3)

인도 하이데라바드 회의에서 이미 발행된 스마트계약 상호작용 및 개요 표준 (TR 23455)에 그림 8과 그림 9가 동일한 그림이 중복 삽입되어 있음을 한국 전문가가 지적하여, 2월 웹 미팅에 보고되어 TC 307 사무국 및 ISO 편집위원회에서 후속대응을 논의 중에 있으며, 오류정정 발행이 예상 되고 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. 이 문서를 기술규격서 (Technical Specification)로 진행하는 것에 대하여 논의하였으나, 기술규격으로 개발하기로 결정 하였다. 이와 유사한 표준안이 BSI 개발되고 있음을 3월 웹미팅에서 공유되었다 (BSI PAS 333 “Smart legal contract - Specification”).

2.2.3. 거버넌스 (WG5)

블록체인 시스템의 거버넌스를 위한 지침 (TS 23635) 문서는 CD 상태이며, DTS (Draft TS) 투표를 위한 표준문서 작성을 목표로 6개월 동안 4번의 회의를 개최하였다. 주요 이슈로서 온체인과 오프체인 거버넌스에 대한 논의가 있었으며, 한국이 제시한 “블록체인 거버넌스 원칙”을 수용하여, 거버넌스 콘텍스트(데이터, 프로토콜, 응용, 조직)를 기반으로, 생명주기(수립, 운영, 종료)에 따른 거버넌스 활동을 작성중에 있다.

2.2.4. 유스케이스 (WG6)

유스케이스를 연구하는 WG6는 영국의 Caroline Thomas가 컨비너로서 취임한 이후 약 20여 개의 유스케이스에 대한 코멘트 해결을 완료하고, 차기 10월 회의에서 WD 투표를 진행하기고 합의하였다. 신규 유스케이스 아이템으로는 인증, 에너지 트레이딩, 공급망등 8개가 진행 중이며, 한국에서는 블록체인/분산원장 시범사업의 결과중 탈중앙화 기부 플랫폼에 대하여 협의하여, 하반기에 기고를 준비 중에 있다.

유스케이스의 아이템들에 대한 카테고리 분류 (Classification) 관련하여 도메인과 서브도메인간에 혼선 발생에 대하여 WG1 과 WG6 간에 협의중에 있다.

2.2.5. 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 또는 DLT를 적용했을 때, 발생하는 도전, 고려사항, 잠재적 이점이 있는지를, 기록관리 관점에서 분석을 위하

여 ISO TC 46/SC 11내에 조인트 WG 설립이 2019년 6월에 있었다. 이를 근거로 TR 24332 문서 개발을 위하여 올해 1월에 카나다 밴쿠버에서 합동회의가 있었으며, 제목 및 스코프를 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 (WG2,4)

암호화폐 거래소 정보보호 가이드라인 기술보고서(TR 23576 Security of digital asset custodians) 표준개발은 일본에서 제안한 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 원인규명이 안됐다는 것에 실망이 전문가들에서 표명되었다. 이러한 이유로 개정을 진행하는 이슈가 제기되었으며, 6월 회의에서 일본의 Shinichiro Matsuo와 영국의 Aldo Lo Castro가 프로젝트 리더로 선임되었다.

합의 모델에 대한 정보보호 평가에 대한 사전연구(Security evaluation of consensus models : SECM)는 현존하는 합의 알고리즘을 대상으로 리스크 평가(Evaluation)와 리스크를 완화 하고자 하는 기술적 조치 및 평가 방안에 대한 기술조사를 통하여 표준문서 개발 착수를 위한 사전연구를 2년간 진행하였으나, 이해도 및 전략의 부족으로 연구를 종료 하기로 결정하였다.

스마트계약의 정보보호 이슈 (Security issues on smart contract) 사전연구는 WG2 (Security, Privacy and Identity)와 WG3 (Smart Contract)간의 협력 개발 표준으로 스마트계약을 활용 함에 있어서 현존하는 정보보호 이슈와 분산원장(DLT)-오라클과 같은 요소들에 대한 특정 정보보호 이슈들을 분류하는 것이 목표였으며, 6월 회의에서 사전연구의 결과가 우수하여 기술규격(Technical Specification)으로 추진하는 방안이 논의되었으나, 최종 기술보고서(Techinal Report)로 표준개발 트랙을 밟는 것으로 합의하였다. 제목은 “Overview of smart contract security good practice and issues”이며, 한국의 스마트계약 샌드박스 기고가 반영되었다. 프로젝트 리더로 영국의 Stephan Holmes가 선임되었으며, 차기 회의에 첫 번째 WD를 작성하고 코멘트를 논의할 계획을 수립하였다.

탈중앙형 아이덴티티 관리를 위한 Trust Anchors에 대한 사전연구가 종료하여 기술보고서 작성을 승인 받았다. 제목은 “Overivew of Trust Anchors for DLT-based Identity Management”로 결정되었으며, 프로젝트 리더로 스페인의 Ignacio Alamillo, 영국의

〔표 1〕 ISO/TC307/WG2와 JWG4 표준화 현황

표준번호	제목	WG/단계	Progject Leader
ISO TR xxxx*	Security management of digital asset custodians	WG2/ NP	Shin’ichiro Matsuo (JP), Alodo Lo Castro (UK)
ISO TR xxxx*	Overview of smart contract security good practice and issues	WG2&3/ NP	Stephen Holmes(UK)
ISO TR xxxx*	Security risks, threats and vulnerabilities	JWG4/ NP	Julien Bringer(FR)
ISO/IEC TR 23249	Overview of existing systems for identity management	JWG4/ WD	Paolo (IT), Ignacio Alamillo (ES)
ISO TR xxxx*	Trust Anchors for Decentralised Identity Management (TADIM)	JWG4/ NP	Ignacio Alamillo(ES), Patrick Curry(UK), Jae Hoon NAH(KR)

* 번호 할당을 기다리는 표준

Patrick Curry, 한국의 나재훈이 선임되었으며, 8월 말에 첫 번째 WD을 발행하고, 차기 10월 회의에서 코멘트를 논의하기로 합의하였다.

보안 위험(Risk), 위협과 취약점 프로젝트 (TR 23245)가 하이데라바드 회의에서 문서의 질적 수준이 낮다는 미국의 이슈 제기에 의하여 투표에 회부 되었으며, 투표결과 종료하고 재시작하는 것으로 결의하였고, JWG4 코컨비너 Julien Bringer가 임시(Acting) 프로젝트 리더로 선임되었다.

신원관리를 위한 분산원장기술 시스템 기술보고서 (TR 23249: Overivew of existing DLT systems for identity management)는 6월 말까지 두 번째 WD를 완료하고, 코멘트 요청을 8월 말에 마감하여 10월에 코멘트 논의하기로 합의하였다. [표 1]은 정보보호 관련 WG2와 JWG4에서 추진중인 표준 아이템 목록을 보여준다.

Ⅳ. 결 론

2016년 9월에 설립된 ISO/TC 307 (블록체인/분산원장) 기술위원회는 만 4년이 경과 하고 있는 새내기 기술위원회라고 평가할 수 있다. 그리고 블록체인/분산원장을 논하는 기초 표준인 용어와 참조구조 표준이 제정할 것을 예정하고 있다. 탈중앙이라는 네트워크 인프라의 전환은 매우 조심스럽다. 이 인프라는 OSI 7 계층의 응용단에 놓여있는 논리적, 가상적 네트워크이다. 이러한 구조로 인하여 하부의 물리적 프로토콜 스택의 한계점을 품고 있으며, 그 상위에서 논리적 연계와 서비스 제공은 하부구조의 고성능과 고기능을 필요로 한다. 더 나아가 사람과의 인터페이스를 포함하고 있기 때문에 지능화에 대한 요구도 대두되고 있다.

이 영역은 아직 학문적 체계를 갖추지 못한 기술로 회자 되고 있다. 암호화폐로 세간에 알려지면서 이론적 역량에 대한 준비가 아직 구체적이지 않은 상태에서 탄생되어, 단지 익명환경에서 화폐거래 서비스를 제공하여 사회적 순기능과 역기능이 공존하는 기술로 평가되고 있다.

이번 6월 회의의 분위기는 영국이 매우 적극적으로 대응을 하고 있으며, 기업 중에는 IBM과 마이크로소프트가 정보보호 분야에서 각축을 벌이고 있는 상황이다. TR 23246 (Overview of identity management using blockchain and DLT)이 하이데라바드 회의에서 IBM의 프로젝트 리더가 사임을 표명하면서 종료되었으며, 그 후속으로 TR 23249 (Overivew of existing DLT systems for identity management)가 동시에 승인되었다. 그 배경에는 마이크로소프트의 블록체인 신원관리 시스템 ION (Identity over network)의 출시와 무관하지는 않아 보이며, 표준화의 치열한 경쟁의 한 면을 보이는 사례로 사료된다.

이러한 표준화 환경에서 한국의 탈중앙화 기부 플랫폼 유스케이스 아이템을 유스케이스(TR 3242) 표준에 추가한 것은 산업적 검증을 통한 기술결과물의 표준화라는 측면에서 의의가 있다. 한국의 기술이 국제표준의 기준을 마련하기 위한 기술적 성숙도 마련되었고, 이를 국제표준에 반영하는 선순환적인 접근방법은 향후 기술과 표준화의 발전에 순기능으로 작용할 것으로 사료된다.

참 고 문 헌

[1] 블록체인 트릴레마 http://wiki.hash.kr/index.php/트릴레마
[2] ISO/TC307 Meeting 06 Report 2019,11.
[3] ISO/TC307 WG2 Resolution 2020,07.
[4] ISO/TC307 JWG4 Resolution 2020,07.

〈저자소개〉

나 재 훈 (Jae Hoon NAH)
증신회원
1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 정보공학 박사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원
2019년~현재 : 글로벌ICT표준마에스트로
2009년~현재 : ITU-T SG17 WP4 공동의장, Q7 라포처
2018년 7월~현재 : TC307 대표전문위원
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
2011년~현재 : 한국정보보호학회 학회지 정보보호 국제표준 특집호 책임 편집위원
<관심분야> 블록체인보안, 핀테크보안, 웹메쉬업보안, 스마트시티보안, 익명인증