정 보 보 호 학 회 지
제 29 권 제4호, 2019. 8

ISO 블록체인 정보보호 표준기술 동향

나 재 훈*, 안 개 일*, 전 해 숙*

요 약

ISO/TC 307(블록체인/분산원장) 표준기술위원회는 2016년 9월 신설되었으며, 호주에서 사무국을 담당하고 있다. 영국, 미국, 프랑스, 독일등 서방국가들이 적극적으로 표준화 활동을 하며, 기업 측면에서는 IBM, MS사의 활동이 두각을 나타내고 있다. 아직 위원회의 구조와 표준화가 초기 단계에 있지만, 블록체인 기술을 기반으로 활용사례 표준 개발을 병행하여, 표준의 효용성을 높이려는 시도가 진행되고 있다. 중앙집중식의 구조에서 탈중앙구조로 패러다임 전환이 순조롭게 추진되기 위해서는 이제 학문적 기초가 필요하다는 의견이 국제컨퍼런스를 통하여 제시되었으며, 이러한 초기 단계에 한국도 적극적으로 활동하여 경쟁력 있는 특화 부분을 선점하는 전략이 필요하다고 사료되며, 지난 5월 더블린에서 개최된 블록체인/분산원장 기술위원회의 표준화 동향을 살펴본다.

Ⅰ. 서 론

블록체인/분산원장 기술은 그 태동이 암호 메커니즘으로 시작된 기술이다. 암호화폐를 기반으로 그 응용을 넓히고 있으나, 산업에서 시작하여 이제 학문적 기반을 구축하고 있는 초기 상태의 기술이라고 하겠다. 현재 1, 2세대 블록체인이 직면한 기술적 한계의 대표적인 예로 네트워크가 확장됨에 따라 초당 거래 처리속도 (TPS: Transaction Per Second)가 느려지는 확장성 (Scalability) 문제를 꼽을 수 있다. 하지만 블록체인 기술의 확장성 문제를 해결하는 데에 있어서 발목을 잡는 요소는 두 가지가 존재한다. 바로 탈중앙화 (Decentralization)와 정보보호(Security) 문제이다. 이러한 확장성, 탈중앙화, 안전성 문제를 포괄한 개념이 블록체인 트릴레마(Trilemma)이다[1]. 이는 시중에 나와 있는 암호화폐들이 사용하는 블록체인은 대부분 위의 세 꼭지점 중에서 하나 또는 최대 두 개까지 해결할 수 있고, 세 가지를 동시에 만족시키는 것은 현재로서는 물리적으로 불가능하다고 이더리움의 창시자 비탈릭 부테린이 언급을 하였다.

블록체인/분산원장에서 PoW(Proof of Work) 합의 알고리즘은 하나의 블록을 생성하기 위하여 최소한의 시간을 보장하고 있다. 이것은 이중지불을 방지하기 위한 고안된 탈중앙의 핵심 메커니즘이다. 즉 서비스를 제공하기 위하여 순기능 만을 설계하다가 후에 보안 기능을 추가하였던 시스템 개발 접근방법에서 서비스를 제공하기에 안전을 동시 우선적으로 고려한 후에 성능개선을 하는 형국이라고 볼 수 있다. 결국 중앙집중식 시스템 구축 방식에서 탈중앙 시스템으로 패러다임 전환이 이슈이며, 중앙집중식 사고와 기술을 탈중앙 인프라에 단순 이주로는 해결할 수 없는 기술로 판단된다.

본 논문에서 블록체인/분산원장 기반의 안전한 서비스 제공을 위하여 상용되고 있는 기술과 상호운용을 위한 표준화의 동향에 대하여 살펴본다[2].

Ⅱ. ISO TC 307 구조 및 개요

2.1. ISO TC 307 (블록체인/분산원장) 구조

2016년 승인된 ISO TC 307 블록체인 및 분산원장 기술(Blockchain and distributed ledger technology)은 2019년 현재 5개의 작업반(working group)과 2개의 연구반(study group)을 구성하여 작업 중에 있다. WG1(Foundation)은 영국의 Geff Goodell이 맡고 있으며, 블록체인 시스템 및 서비스를 위한 기초적인 용어, 플랫폼 구조, 텍사노미 및 온톨로지등의 표준화를 추진

본 논문은 2019년도 산업자원통산부부의 재원으로 국가표준기술력향상사업의 일환으로 수행되었음.[20005255, 블록체인 기술을 활용한 적합성업무 관리 참조모델 운영 및 표준화 전략]
* 한국전자통신연구원 정보보호연구본부(jhnah,fogone,hsjeon88@etri.re.kr)

하고 있으며, WG2(Security, Privacy and Identity)&WG4는 프랑스의 Julien Bringer가 맡고 있으며, 자가주권 신원관리 개요, 거래소 정보보호 위협, 취약점 및 위기, 프라이버시와 개인식별정보 고려사항, 스마트계약의 정보보호 이슈 등의 표준화를 추진하며, WG3(Smart contract)은 독일의 Volker Skwarek이 맡고 있으며, 적법한 스마트계약, 스마트계약간 상호작용 개요 등의 표준화를 추진 중이며, WG5(Governance)은 덴마크 Roman Beck이 맡고 있으며, 조직을 관리하는 것이 아닌 블록체인 시스템과 프로그램의 상호동작을 관리하는 거너번스를 위한 지침을 표준화 하고 있다. 그리고 지난 5월 더블린 회의에서 WG 6(Use Cases, Caroline Tomas 영국)가 신설되어, SG 2(상호운용성)를 폐지하는 것을 영국에서 제안하였으며, 유스케이스 DTR 문서 승인을 조건으로 WG6의 신설을 합의하였다. 그리고 WG 7(상호운용성: Interoperability)의 신설에 관하여는 신규과제 TR 상호운용성 프레임워크(Interoperability Framework) 승인을 조건으로 합의 하였으며 차기 회기 이전에 투표를 진행하기로 하였다. 그리고 ISO/TC 46/SC 11(기록관리)에서 보내온 JWG 신설에 대한 연락문서에 대하여, 이번 TC 307회의에서 JWG 신설을 찬성하였다.

2.2. ISO TC 307 (블록체인/분산원장) 현황

지난 더블린 회의에서는 인도에서 제안하였던 블록체인 확장성 및 성능관련 SG (Non-funtional Requirements, 컨비너: Jay BOTHRA)은 미국을 제외한 다수 국가의 반대로 SG 신설하는 것은 반려되었고, WG 6 내의 6개월 사전연구(Study)로 승인되었다.

그리고 WG 1의 텍사노미 및 온톨로지 (TS Taxonomy and Ontology) 프로젝트 리더인 중국 Peter Luo가 사임하여, ETRI의 이원석 박사가 후임 프로제트 리더로 선임되었으며, 참조구조(IS 23257)의 프로젝트 리더가 건강상의 이유로 사임을 하여 신규 프로젝트 리더를 공모한 상태이다. 기록관리 분과위원회(ISO/TC 46/SC 11)와의 JWG의 공동컨비너로 영국의 Geff Goodell이, JWG 4(정보보호 관련)에 미국의 SAL Francomacaro가 공동컨비너로 선임되었다.

2.2.1. 블록체인 및 분산원장 기반기술 (WG1)

블록체인 및 분산원장 기술의 기반이 되는 용어표준(IS 22739)이 현재 두 번째 CD 단계에 있으며, 허가형(permissioned)과 비허가형(permissionless), 공적(public)과 사적(private), 포크(fork)/하드포크(hard fork)/소프트포크(soft fork) 등 주요 용어에 대해 산업계의 용례를 검토하여 반영할 것에 대하여 재논의 할 것을 협의하였다. 참조구조 표준은(IS 23257) 플랫폼의 개념, 구조, 기능 컴포넌트, 역할, 액티비티 및 이들의 관계에 대한 표준을 개발 중이며, 이번 회의에서는 첫 번째 CD 투표 코멘트에 대한 이슈 협의 및 문서 작업을 수행하였다. 텍사노미 및 온톨로지 표준안은(TS 23258) “블록체인 및 분산원장기술의 용어, DLT 시스템, 유즈케이스“의 텍사노미와 “클래스, 속성, 그리고 용어들의 관계“를 설명하는 온톨로지를 개발 중이며, 중국의 프로젝트 리더 Peter Luo의 사임으로, 한국의 이원석 박사가 새로운 프로젝트 리더로 임명되었다.

2.2.2. 블록체인의 킬러앱으로 개발이 시급한 스마트계약 (WG3)

스마트계약 상호작용 및 개요 표준안은(TR 23455) 기술보고서 발행을 위하여 DTR 투표 코멘트를 최종 반영하는 작업이 진행되었으며, TC 307에 기술보고서 최종 발행을 요청하기로 합의하였다. 법적 구속력 있는 스마트계약 표준안은(TS 23259) 향후 기술규격 작업 방향을 구체화하기 위한 프레임워크가 제안되어 논의되었으며, 보편적 계약 규범에 의거하여 계약 수립에 필요한 단위 구성요소를 먼저 정의하고, 그 관계를 기반으로 온톨로지 및 텍사노미를 구축하고, 일반화된 블록체인 소프트웨어 설계 패턴으로 변환하기로 합의하였다.

2.2.3. 블록체인의 안전한 사용과 적용을 위한 거버넌스 (WG5)

블록체인 시스템의 거버넌스를 위한 지침 (2WD TS 23635) 초안 개정 작업이 진행 중에 있으며, 6개의 타스크포스(생명주기, 거버넌스 레이어, 상호운영성, 결정권한 등)를 구성하여 개정 작업한 결과를 논의하였으며, 한국이 제시한 “블록체인 거버넌스 원칙”을 수용하여,

거버넌스 레이어 대신 콘텍스트(데이터, 프로토콜, 응용, 조직)로 결정하여, 생명주기(수립, 운영, 종료)에 따른 거버넌스 활동을 프레임워크로서 정리하였다.

2.2.4. 블록체인의 다양한 응용을 위한 유스케이스 개발 (SG2)

유스케이스를 연구하는 SG2는 일본의 컨비너가 사임한 이후 영국의 Caroline Thomas가 컨비너로서 운영하였고, 그 동안의 SG 활동을 종료하고 신규 WG(WG 6) 설립을 제안하였다. 이번 회의에서 블록체인 및 분산원장의 유스케이스 기술보고서를 포함한 활동 현황을 보고하였고, 유스케이스 요약보고서에 대한 코멘트 작업을 진행하는 등, 7개의 유스케이스(국경통제를 위한 신원관리, M2M지불을 위한 암호화폐 등) 검토하고, 회의결과 문서로 제출하였으며, 이 문서를 근거로 새로운 WG 신설을 위하여 웹투표를 통하여 승인할 것을 합의하였다.

2.2.5. 다양한 플랫폼 및 서비스간의 상호운용성 연구 (SG7)

상호운용성 스터디그룹은 그 동안의 활동을 종료하고 신규 WG(WG 7, 컨비너: Gilbert Verdian, UK) 설립을 제안하였다. 신규 WG 신설의 필요조건인 필수 표준아이템으로 “블록체인 상호운용성 프레임워크” 개발을 위한 기술규격 문서를 신규제안하기로 하였으며, 문서 범위로는 분산원장 시스템 간, 분산원장 시스템과 비분산원장 시스템 간 등의 상호운용성 프레임워크를 제공하는 것을 목표로 하며 웹투표를 통하여 승인할 것을 합의하였다.

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 자산의 관리를 위한 가이드라인의 내용을 담고 있다. 지난 더블린 회의에서 한국은 거래소에서 자금세탁방지 의무지침에 대하여 FATF (Financial Action Task Force)의 서비스 제공자의 의무사항 등의 내용을 제안하여 반영하였다. 이 기술보고서는 일본의 암호화폐 거래소 MtGox의 도난사고를 분석하여 거래소의 디지털 자산의 관리를 위한 정보보호 가이드라인 개발을 목표로 한다. 제목을 Security management of digital asset custodians로 수정을 합의하였으며, 거래소의 안전성 제고를 목표하기에 많은 관심을 갖고 있지만, MtGox의 해킹에 대하여 확실하게 원인규명이 안됐다는 것이 일본 에디터의 상황설명이 있었다.

합의모델에 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 프레임워크를 제안하였다고 긍정적 평가를 받고 있으며, 지갑에 대한 접근관리 및 자금세탁등에 대한 추가적인 연구를 위해 6개월 연장하는 것에 합의하였다.

스마트계약의 정보보호 이슈 (Security issues on smart contract) 사전연구는 WG2(Security, Privacy and Identity)와 WG3(Smart Contract)간의 협력 개발 표준으로 스마트계약을 활용함에 있어서 현존하는 정보보호 이슈와 분산원장(DLT)-오라클과 같은 요소들에 대한 특정 정보보호 이슈들을 분류하는 것이 주요 목표이다. 2018년 10월 모스크바회의에서 인도의 Rajeev에 의하여 제안되어 수행되었으나, 이번 회의에서 영국의 Stephen Homles로 프로젝트 리더가 변경되고 6개월 연장하여 다음 인도 회의에서 검토하기로 협의하였다.

프라이버시와 개인정보보호 고려사항

기술보고서(TR 23244 Privacy and personally identifiable information (PII) protection consideration)는 프라이버시와 개인정보보호를 블록체인/분산원장 시스템에 적용 할 때에 발생하는 문제를 다루며, 특히 유럽연합의 GDPR(General Data Protection Regulation) 법령(2018년 5월 25일로 시행)과 관련하여 블록체인/분산원장 서비스 환경에서의 잊혀질 권리를 고려하는 조항과, 양자 저항 암호 용어정의를 명확히 하고, 자구 수정을 통하여 DTR 투표를 할 것에 합의하였다.

정보보호 리스크, 위협과 취약점 기술고보고서(TR

〔표 1〕 ISO/TC307/WG2와 JWG4 표준화 현황(2019년 5월)

표준번호	제목	WG/단계	Progject Leader
ISO/IEC TR 23576	Blockchain and distributed ledger technologies – Security management of digital asset custodians	WG2/ DTR	Shin'ichiro Matsuo (일본)
(Study)	Blockchain and distributed ledger technologies – Security evaluation of consensus models (SECM)	WG2/ Study	Stéphane Caporali (프랑스)
(Study)	Security issues on smart contract	WG2&3/ Study	Stephen Holmes(영국)
ISO/IEC TR 23244	Blockchain and distributed ledger technologies – Privacy and personally identifiable information (PII) protection consideration	JWG4/ DTR	Stephen Holmes (UK)
ISO/IEC TR 23245	Blockchain and distributed ledger technologies – Security risks, threats and vulnerabilities	JWG4/ DTR	Shin'ichiro Matsuo (일본)
ISO/IEC TR 23246	Blockchain and distributed ledger technologies – Overview of identity using blockchain and distributed ledger technology	JWG4/ WD	Paul Ferris (영국)
(Study)	Trust Anchors for Decentralised Identity Management (TADIM)	JWG4/ Study	Ignacio Alamillo (스페인)

23245 Security risks, threats and vulnerabilities)는 블록체인/분산원장 시스템에 관련된 보안 위협, 취약점 및 리스크를 연구하고 있으며, 네크워크 보안, 암호 알고리즘 및 프로토콜 구성, 암호키 관리, 보안관리 프로세스, 안전한 구현 및 인증(Certification) 및 가용성 등의 내용을 기반으로 표준안을 작성하고 있다.

신원정보 개요 기술보고서 (TR 23246 Overview of identity using blockchain and distributed ledger technology)는 식별관리 기술의 동향을 분석하는 보고서로서, 블록체인/분산원장 기술을 이용하여 자가주권(Self-sovereign) 식별관리 서비스를 제공에 관한 표준 개발이며, 이번 더블린회의에서 자가주권이라는 용어가 정의되지 않았다는 이유를 들어, 자가주권 용어를 사용하지 않을 것을 미국에서 제안하여, 용어를 식별관리로 통일하는 것과, 6절의 내용에서 ShoCard의 참조모델이 기술되어 있어, 기술보고서의 내용으로 적절하지 못하다는 미국의 코멘트에 의하여, 6절의 내용을 단순 기술 분석 수준으로 기술하여 기술보고서로 진행할 것을 합의하였다.

분산신원관리를 위한 신뢰 앵커 사전연구 (Study Trust Anchors for Decentralized Identity Management : TADIM) 제안이 스페인 Ignacio Alamillo에 의하여 제안되었으며, 분산형, 탈중앙형 아이덴티티 관리를 위한 신뢰 앵커(Trust anchor)의 현존 모델과 유즈케이스 식별, 유형별 분류 및 평가 모델에 대한 연구에 대한 필요성을 인정받아 차기 인도 회의에 사전연구 결과를 보고하는 것에 합의하였다.

Ⅳ. 결 론

2016년 9월에 설립된 ISO/TC 307(블록체인/분산원장) 기술위원회는 아직 내부구조를 정비 중이다. 탈중앙이라는 패러다임 전환을 목표로 하는 기술의 영역으로 아직 학문적 체계를 갖추지 못한 기술로 회자 되고 있다. 암호화폐로 세간에 알려지면서 기술적 역량에 대한 준비가 아직 구체적이지 않은 상태에서 익명환경에서 화폐거래를 가능하게 서비스를 제공하여 사회적 순기능과 역기능이 공존하는 기술로 평가되고 있다.

회의 전반적으로 영국이 매우 적극적으로대응을 하고 있으며, 기업중에는 IBM이 하이퍼레저 기반의 활동을 벌였고, 이후 마이크로소프트가 후발 참여를 하였지만, 정보보호 분야에서 각축을 벌이고 있는 상황이다.

이번 ISO/TC 307 (5월 더블린)회의에서 한국은 총 7건의 기고서를 제출하였으며, 주요 성과로 텍사노미 및 온톨로지(TS 23258) 프로젝트 리더를 수임하였으며, 디지털 자산 거래소 보안 관리 표준에 자금세탁방지 관련한 보안통제를 추가하였다. 그리고 기록관리 분과위원회와의 협력은(ISO/TC 307 와 ISO/TC 46/SC 11 간

의 JWG (Joint WG)) 국가기록관리 업무에 블록체인 기술 활용을 위한 표준으로 향후 국가산업과의 연계 및 파급효과가 크다고 판단되며, 국내 전문가들의 적극 대응이 필요하다고 사료된다.

참 고 문 헌

[1] 블록체인 트릴레마 http://wiki.hash.kr/index.php/트릴레마

[2] ISO/TC307 Meeting 05 Report 2019,07.

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)

종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 학사

1987년 2월 : 중앙대학교 컴퓨터공학과 석사

2005년 2월 : 한국외국어대학교 정보공학 박사

1987년 ~ 현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원

2009년 ~ 현재 : ITU-T SG17 WP4 부의장, Q7 라포처

2018년7월~현재 : TC307 대표전문위원

2011년~2012년 : 한국정보보호학회 학회지 편집위원장

2011년~현재 : 한국정보보호학회 학회지 정보보호 국제표준 특집호 책임 편집위원

<관심분야> 블록체인보안, 핀테크보안, P2P보안, 웹메쉬업 보안

안 개 일 (Ahn Gaeil)

종신회원

1993년 2월 : 충남대학교 컴퓨터공학과 학사

1995년 2월 : 충남대학교 컴퓨터공학과 석사

2001년 8월 : 충남대학교 컴퓨터공학과 박사

2006년 7월~2007년 6월: 미국 Security University 박사후 연구원

2001년 8월~현재: 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> 네트워크보안, 제어시스템보안, 국민생활사이버안전

전 해 숙 (Jeon Hae Sook)

종신회원

1992년 8월 : 충남대학교 전산학과 학사

1995년 2월 : 충남대학교 컴퓨터과학과 석사

2015년 2월 : 충남대학교 컴퓨터공학과 박사

2000년3월~현재 : 정보보호연구본부 책임연구원

2017년10월~현재 : IEC TC80K 전문위원

2017년8월~현재 : 스마트자율운항선박포럼 위원

<관심분야> AI 알고리즘, ISDN 신호처리 프로토콜, SNMP 기반 MPLS 망관리, ATM 스위치 FW, 라우터 QoS, IDNet, VTS 통합게이트웨이, 선박 IEC 항로계획 표준과 선박통신 표준