[정보보호] 블록 체인 보안

2017년 3월 ITU-T SG 17에서는 블록체인의 보안 측면에 관한 1일 세미나를 개최하고 이를 통해 제안된 표준화 현안을 다루기 위한 특별 세션을 진행하였다. 본 고에서는 블록체인 보안 세미나에서 다루어진 내용과 이에 관한 SG 17의 논의 사항을 소개하고 기타 국내외 현황과 향후의 대응 방향을 제안한다.

1. 블록체인의 보안 측면 세미나

ITU-T SG 17의 블록체인 세미나는 5개의 세션으로 이루어졌다. 제1 세션은 블록체인의 기술적 개요를 다루었다. 블록체인과 분산 원장 기술의 개요와 응용분야, 그리고 블록체인과 보안의 상호적 상승작용에 관한 발표가 이루어졌다.

제2세션에서는 블록체인의 응용 및 유즈케이스와 이에 관련된 보안 기술의 필요성이 다루어졌다. Hyperledger 그룹에서는 로열티 플랫폼 유즈케이스를 소개하고 이 모델에서 참여자들의 privacy 측면과 보안 측면의 장단점을 제시하였다. 또한 G-클라우드 상의 블록체인 플랫폼인 Credits에서는 자신들의 플랫폼을 소개하고, 기반 기술에 따라 가상화폐의 유즈케이스를 분류하고 관련 규제 및 표준화 현황 및 관련 현안을 소개하였다. Blockchain Hub에서는 블록체인에 관련된 보안 사고를 소개하고 블록체인 기술 자체는 안전하지만 이를 운영하는 시스템 상의 취약점 및 기술에 대한 오해가 문제가 될 수 있음을 설명하였다.

제3세션에서는 블록체인을 위한 정책 및 규제 측면에 관한 발표가 이루어졌다. EC의 DG-CONNECT에서는 블록체인과 금융 시장에 관한 EU 및 유럽 의회의 정책 전망을 소개하였다. 두 번째 발표에서는 Tunisia의 e-Dinar와 MobiPoste 이용 현황이 소개되었다. 이들 블록체인 기반의 전자화폐와 송금은 널리 이용되고 있으나, 돈세탁을 방지하기 위한 강력한 Tunisia 금융 규제에 따라 Tunisia에 거주하는 Tunisia 국민에게는 사용이 불허되고 있는 현실을 소개하면서 이러한 Fintech 기술과 법적 요건에 대한 주의를 환기시켰다. 세 번째 발표자인 Columbia University의 Leon J. Perlman은 분산원장기술의 규제 및 법적 측면에 대해 발표하면서 현재의 강력한 법적 규제로 인해 신기술의 가능성 시험이 이루어지기 힘든 현실을 극복하기 위한 방안으로서 특정 범위 내에서 규제 적용을 완화하는 "Regulatory sandbox(모래상자 규제)"의 필요성을 제기하였다.

제4세션에서는 블록체인에서의 보안, 프라이버시 및 온라인 신뢰측면에 대한 발표가 이루어졌다. 특히 프라이버시에 관해서는 블록체인 기술의 실제 구현 상의 통제 방법에 따라 달라지는 부분이 많으므로 이에 대해서는 더 많은 논의가 필요하다는 점이 강조되었다. 또한 블록체인의 연합

네트워크를 통한 인증과 인가의 결합을 설명하고 블록체인 보안의 핵심은 키관리에 있으며 이를 관리하기 위한 하드웨어 보안 모듈과 신뢰할 수 있는 플랫폼 및 실행환경, 보안 환경에 대한 연구의 필요성이 제시되었다. 이러한 보안 문제는 블록체인 3.0에서 도입된 하이브리드 모델로 가면서 점점 더 복잡해지는 추세이다.

마지막으로 제5세션에서는 블록체인 용어조차 공통된 정의가 없음을 강조하면서 공개 블록체인 이용 시 유의 사항, FIDO 포럼에서 수행 중인 연합 기반의 인증 관련 블록체인 연구 방향 등이 소개되었으며 이에 기초한 블록체인 보안 표준화 활동의 향후 방향에 대해 패널 토론이 이루어졌다.

2. SG 17에서의 후속 논의

SG 17은 이러한 세미나의 결과를 향후의 표준화 작업에 반영하기 위하여 특별 세션을 마련하고 방안을 논의하였다. 이 세션에서는 블록체인의 보안을 SG 17에서 다루기 위한 방법 및 가능한 신규 아이템을 논의하였다. 그러나 미국 등 일부 국가는 블록체인에 대한 논의는 차기 회의에서 지속할 것을 제안하였다. 당 세션에서 완료하지 못한 논의는 디지털 금융 서비스의 보안 측면에 관한 포커스 그룹 결과에 관한 특별 세션에서 지속하기로 하였다.

한국은 더 구체적인 논의를 진행하기 위하여 블록체인 보안 표준화 수행 방안과 신규 아이템에 대한 제안을 문서화하여 TD로 발행하고 제안하였다. 먼저 SG 17에서 블록체인 보안 표준화를 수행하기 위한 방안으로써 1) 신규 Question 설립, 2) 기존 Question text를 블록체인을 포함하도록 변경, 3) Focus Group 설립 방법을 제안하고 각각에 필요한 텍스트를 제시하였으며, 가능한 신규 아이템 리스트를 제시하고 특히 블록체인 기반 디지털 금융 서비스의 보안 위협 및 요구사항에 관한 신규 아이템을 예로써 제안하였다.

제시된 가능한 신규 아이템 리스트는 다음과 같다.

- 블록체인 용어정의(Block chain terminology)
- 디지털 금융서비스를 위한 블록체인 유즈케이스 및 비 금융 서비스를 위한 유즈케이스 (Blockchain use cases for digital financial services/ non-financial services)
- 블록체인 유즈케이스에 기반한 보안 및 프라이버시 위협 및 요구사항 (Security and privacy threats and requirements based on blockchain use case)
- 블록체인 보안 참조 아키텍처 (Security reference architecture for blockchain)
- 블록체인 기반 신원 관리 (Identity management based on blockchain)
- 블록체인 기반 키 입증 (Key attestation based on blockchain)

- 블록체인 응용 및 서비스를 위한 보안 및 프라이버시 가이드 (Security and privacy guidance for blockcain applications and services)

이어진 논의에서는 디지털 금융 서비스 보안에 관한 포커스 그룹의 결과를 참조하여 추가하도록 하고, 블록체인 기술의 성숙도, 표준화 시점, ISO TC 307 등 타 표준화 기구와의 중복 회피의 필요성을 논의하는 한편, SG 17이 블록체인 보안을 선도할 필요성에 대한 논의가 이루어졌다. 논의는 총회까지 이어져서 총회에서 TSAG 산하의 블록체인 포커스 그룹을 제안하는 것으로 마무리되었다. 이 제안은 TSAG 회의에서 분산 원장 기술 포커스 그룹으로 제목을 변경하여 통과되었다. 이 포커스 그룹은 ITU-T 내 SG 2(운영 측면), 3(경제 및 정책 현안), 5(환경 및 기후변화), 9(광역 케이블 및 TV), 11(프로토콜 및 테스트 스펙), 13(클라우드, 모바일 및 차세대 네트워크를 포함하는 미래 네트워크), 16(멀티미디어), 20(IoT 및 스마트 시티 및 커뮤니티를 포함하는 그 응용)을 포괄하며 각자의 분야에 해당하는 분산원장 및 블록체인 기술을 연구할 때 횡적 소통을 제공하게 될 것이다.

3. 국내외 현황과 향후 표준화 방향

블록체인은 가트너의 하이프 사이클에 따르면 기대의 최정점에 오른 기술이다. ITU-T SG 20에서는 이미 IoT 관련 블록체인 신규 아이템 Framework of blockchain of things as decentralized service platform을 승인하였으며 ISO에서는 4월 초 호주에서 TC 307 블록체인 첫 회의를 개최하고 용어정의(Terminology) 표준 개발을 결정하였다. 한편 R3 CEV, Hyperledger 등의 컨소시엄들이 표준 플랫폼을 개발하고 있으며 사실 표준화 기구인 W3C에서도 표준화 작업이 개시되고 있다. 각 컨소시엄 및 표준화 기구 내에서도 하위 연구 그룹마다 중점을 두는 측면이 있지만, 가장 기초가 되는 용어, 유즈케이스 및 기술 참조 모델의 표준화가 가장 우선적으로 꼽히고 있다. 각 그룹의 표준화 노력이 중복되지 않고 효과적으로 결실을 맺을 수 있도록 기구 간 협력이 필요한 실정이다. ITU-T의 포커스 그룹은 이러한 영역 간 협력을 효과적으로 조정하고 관리할 수 있는 좋은 시발점이 될 수 있을 것이다.

국내에서도 블록체인 표준화 포럼이 발족하였고 사물인터넷포럼에서는 ID 기반 디바이스 및 자원 검색을 위한 보안 프레임워크에 관한 개념적 표준을 제정한 바 있다. 한편 기술 구현 측면에서는 블록체인이 실제 다량의 데이터 처리에 적용될 때 발생하는 퍼포먼스 문제에 대한 우려가 나타나고 있다.

2017년 들어 블록체인 관련 기술 개발 및 표준화 노력들이 국내외를 막론하고 동시 다발적으로 진행되고 있다. 국내에서도 많은 기술 및 표준 개발 노력들이 이루어지고 있는 상황에서, 자칫

이러한 노력들이 중복되고 낭비될 우려가 크다. 국내의 기술이 국제 표준으로 반영되어 국제 시장에서 효과적으로 결실을 얻을 수 있도록 관련 부처의 지도 지원과 산업계 및 학계의 협력이 필요한 실정이다. 관련 부처의 창구를 일원화하고 각 표준화 단체의 국내 위원회 및 산학연의 기술 전문가들이 기술현황과 표준화 전략을 함께 논의할 수 있는 장이 마련된다면 체계적인 협력을 통해 효과적이고 효율적인 기술 개발 및 국제 표준 선도가 가능할 것이다.

오경희(TCA서비스 대표, khoh@tcaservices.kr)