

# 블록체인과 DLT 상호운용성 표준 및 기술 동향

이원석 한국전자통신연구원(ETRI) 서비스표준연구실 선임연구원  
이강찬 한국전자통신연구원(ETRI) 서비스표준연구실 실장



## 1. 머리말

국제 공적표준화 기구인 ISO에서는 2016년 11월에 블록체인의 표준 용어와 사용자, 애플리케이션, 그리고 시스템 간 상호운용성 및 데이터 교환을 위한 표준 개발을 목적으로 TC 307[1]을 신설하였다. 그 후 2017년 4월 1차회의에서 ‘블록체인과 분산원장기술’ 표준 개발 범위를 확정하고 표준화 항목 선정과 작업반(WG1) 및 5개 연구반을 신설하였으며, WG1은 블록체인 관련 용어에 대한 신규 워크 아이탬을 채택하여 개발 중에 있다. 또한 2017년 11월 2차 회의에서 3개 작업반(WG1/2/3)과 3개 연구반으로 재편 후 표준 개발을 진행 중에 있다. 3개 작업반은 블록체인 참조구조 및 데이터 교환 등 분산원장 기반기술 표준화(WG1), 블록체인 보안 및 식별 체계(WG2), 스마트 컨트랙트 표준화(WG3)이고, 3개 연구반은 유즈케이스(SG2), 블록체인 거버넌스(SG6), 블록체인 상호운용성(SG7)이다. 본고에서는 ISO/TC 307의 SG7에서 진행하고 있는 블록체인과 분산원장기술에 대한 상호운용성 표준화 동향에 대해서 소개하며, 또한 블록체인 간의 상호운용성 기

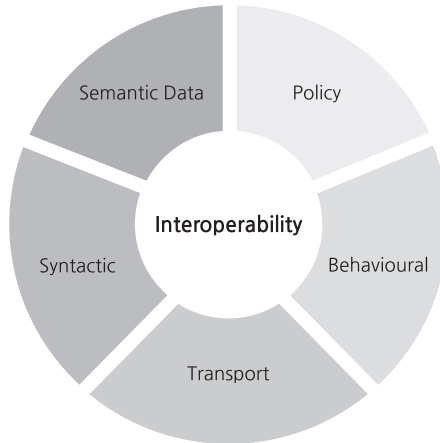
술로 개발 중인 사이드체인, 코스모스 기술에 대해서도 소개한다.

## 2. ISO/TC 307 SG7 활동 현황 및 계획

### 2.1 블록체인 및 DLT 상호운용성 현황

SG7은 블록체인 및 DLT의 상호운용성 표준화를 담당하고 있으며 현재 블록체인 및 DLT 상호운용성과 관련하여 표준화 아이탬에 대한 논의 및 기술문서 개발을 진행 중에 있다. 본 활동은 2017년 11월 도쿄회의 이후부터 2018년 5월 런던회의 종료일까지 진행되나 런던회의에서의 결정에 따라서 연장될 수 있다.

SG7의 블록체인 및 DLT 상호운용성은 ‘ISO/IEC 19941 Cloud computing - Interoperability and Portability’[2] 표준 및 ‘ISO/IEC AWI 21823 Internet of things (IoT) – Interoperability for internet of things systems’ 표준안에서 사용하고 있는 [그림 1]과 같은 5-facet 모델을 기반으로 확장하여 접근하고 있다.



[그림 1] 상호운용성에 대한 5-facet 모델[2]

5-facet 모델 중 3가지 측면에서의 블록체인 및 DLT 상호운용성에 대한 세부적인 내용과 추가적으로 고려하고 있는 발견(Discovery) 측면의 상호운용성에 대한 내용은 아래와 같이 정리할 수 있다. 참고로 5-facet 모델의 Policy 측면에서의 블록체인 및 DLT 상호운용성과 행동(Behavioural) 측면에서의 블록체인 및 DLT 상호운용성은 아직 정리 중에 있다.

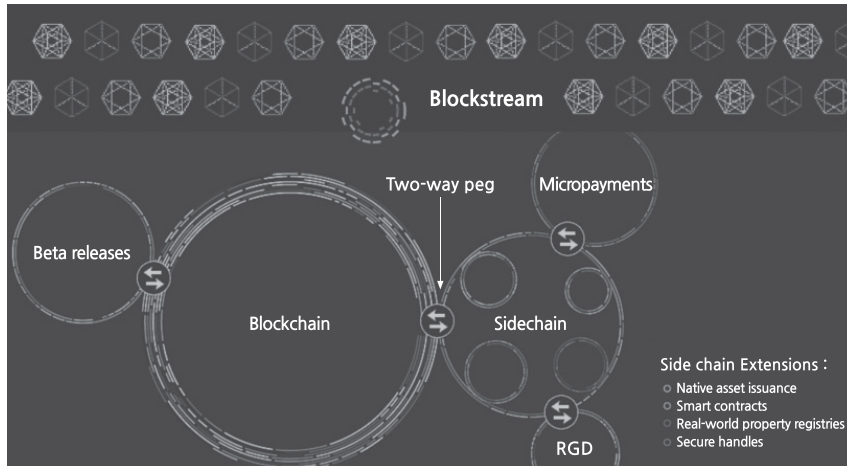
- **Transport 측면에서의 블록체인 및 DLT 상호운용성:** 이더넷, Wi-Fi, 위성 등 다양한 네트워크 환경에서 HTTP(S), MQTT, AMQP 등 다양한 전송 프로토콜이 활용될 것이기 때문에 Transport 레이어에서의 상호호환성을 위한 프로토콜 변환이 필요할 수 있다.
- **구문적 데이터(Syntactic data) 측면에서의 블록체인 및 DLT 상호운용성:** DLT 시스템 간에 이해할 수 있는 정보 교환에 대한 표준 포맷을 의미한다. 이는 데이터를 표현하는 문법을 의미하며 예로 JSON, XML 등이 될 수 있다. DLT 시스템에서 데이터를 요청한 측과 데이터를 제공하는 측 간에 처리할 수 있는 데이터 포맷이 다르다면 이에 대한 변환을 통해서 상호운용성을 유지할 수 있다.
- **의미적 데이터(Semantic data) 측면에서의 블록체인 및 DLT 상호운용성:** 서로 다른 DLT 시스템 간의 의미적인 데이터 상호운용성을 의미하며 일반적으로 서로 다른 블록체인 및 DLT 시스템 간 일관성 있는 데이터 의미를 유지하기 위

해서 온톨로지를 사용할 수 있다. 온톨로지는 간단하게 서로 다른 시스템 간의 의미를 공유할 수 있도록 함으로써 블록체인 시스템의 복잡성을 줄일 수 있으며 또한 이종의 블록체인 시스템 연계에 대한 확장성을 크게 개선한다.

- **발견(Discovery) 측면에서의 블록체인 및 DLT 상호운용성:** 서로 다른 DLT 시스템 간에 원하는 블록체인 플랫폼을 찾고, 평가하고 자율적으로 연동할 수 있도록 지원하기 위해서는 발견(discovery) 기능에 대한 상호운용성 표준이 필요하다. 즉, 블록체인 플랫폼에 대한 기본적인 정보를 다른 블록체인 플랫폼에서 검색 가능하도록 공개해야 하며 또한 이러한 정보에 연동을 위해 기본적으로 확인이 필요한 내용을 평가하고 최종적으로 연동을 실행할 수 있어야 한다. 따라서 이러한 모든 정보들에 대한 표준화와 발견 기능과 관련된 프로토콜에 대한 표준화가 필요하다.

## 2.2 SG7 추후 활동 계획

2018년 5월 런던회의에서 SG7은 구문적 데이터 및 의미적 데이터 측면에서의 블록체인 및 DLT 시스템 상호운용성에 대한 기술문서와 발견(Discovery) 측면에서의 블록체인 및 DLT 상호운용성 기술문서는 WG1으로 이관하여 개발할 것을 제안하여 의결되었다. 따라서 앞으로 WG1에서 본 2건의 기술문서 개발이 이루어질 예정이다. 또한



[그림 2] Blockstream의 사이드체인[3]

SG7은 2018년 모스크바 회의까지 SG7의 활동을 연장하여 암호자산 상호운용성에 대한 논의 및 기술보고서 개발을 진행하기로 제안하여 TC 307 총회에서 의결되었다.

### 3. 블록체인 상호운용성 기술개발 현황

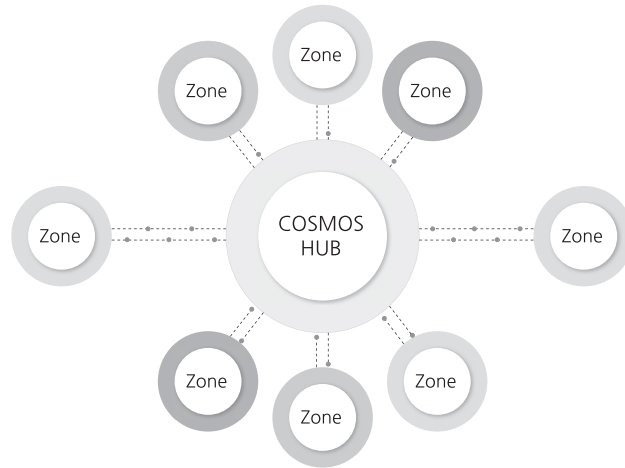
#### 3.1 사이드체인(Sidechain)

사이드체인 기술은 비트코인의 느린 성능, 비트코인 블록체인에서는 비트코인만 사용해야 하는 한계, 스마트 컨트랙트 등 추가적인 기능 확장의 한계 및 모든 거래내용이 공개되는 이슈 등을 해결하기 위한 하나의 방법으로 탄생되었다. 사이드체인은 서로 다른 블록체인에서 사용하는 암호화폐를 서로 안전하게 거래할 수 있는 기술을 의미한다. 즉, 이더리움 블록체인의 스마트 컨트랙트 기능을 사용하는데 비트코인 사용을 가능하게 할 수 있다. 좀 더 구체적인 동작 방식은 다음과 같다.

사이드체인은 부모 블록체인에 양방향 상호작용할 수 있도록 연결된 별도의 블록체인이다. 양방향

상호작용이 가능한 연결은 부모 블록체인과 사이드체인 간에 미리 결정된 비율로 자산 교환을 가능하게 한다. 부모 블록체인의 사용자가 그들의 코인을 목적 주소로 보내면, 목적 주소의 코인은 잠긴 상태가 돼서 사용자는 어디서도 이 코인을 사용할 수 없는 상태가 된다. 트랜잭션이 완료되면 체인을 통해 확인 메시지가 전달되고 추가 보안을 위한 대기 시간이 주어진다. 대기시간이 끝나면 사이드체인에 동등한 수의 코인이 릴리즈되어 사용자가 거기에서 이들을 접근하여 사용할 수 있도록 허용된다. 또한 반대로 사이드체인으로부터 부모 블록체인으로도 자산교환이 가능하다.

대표적인 사이드체인 플랫폼으로 RSK(Rootstock)와 Ardor 블록체인이 있다. RSK는 사이드체인을 위한 오픈소스 테스트넷인 Ginger를 만들었다. 이는 비트코인 블록체인에 대한 양방향 상호작용을 지원하며 통합된 채굴을 통해 비트코인 채굴자에게 리워드를 준다. RSK의 목적은 비트코인 블록체인에 스마트 컨트랙트 기능을 가능하게 하고 또한 결제 처리 속도를 대폭 개선하는데 있다[4]. Ardor 블록체인은 비즈니스를 위한 서비스 플랫폼을 지향한다.



[그림 3] 코스모스 구조

Ardor는 PoS(Proof of Stake) 컨센서스 알고리즘을 지원하며, ‘childchain’이라고 부르는 사이드체인이 부모체인에 긴밀하게 통합되어있다. 자산이나 통화와 같은 체인들의 글로벌 엔티티들은 ‘childchain’을 통해서 접근 가능하다[4].

사이드체인을 선도하고 있는 기업으로 블록스트림(Blockstream)이 있으며 블록체인의 상호운용성을 확장하여 지원하기 위한 텐더민트(Tendermint) 등이 있다.

### 3.2 코스모스(Cosmos)[5]

코스모스도 사이드체인과 유사하게 다양한 블록체인 플랫폼이 등장하고 있으나 파편화되어 있고, PoW 방식의 에너지 비효율성, 처리 성능 및 확장성에 대한 한계 등을 해결하기 위한 방법으로 제안된 기술이다. 위에서 나열한 다양한 이슈들에 대해 가장 적합한 해결방법은 병렬의 블록체인들이 각자의 보안을 유지하면서 호환되도록 하는 것이며, 코스모스는 이것을 목표로 한다.

코스모스는 구조적으로 크게 허브(hub)와 존(zone)으로 구성되어 있다. 존은 다양한 독립된 블록


체인이고 허브는 다중자산 분산 원장을 관리하는 블록체인으로 전체 시스템을 위한 토큰의 ‘중앙 원장’ 역할을 수행한다. 따라서 이종의 블록체인은 존 형태로 코스모스 허브에 연결되어 다른 블록체인과 연동할 수 있는 구조이다. 존은 텐더민트 코어(Tendermint Core)를 통해 작동하는데, 텐더민트 코어는 일관적이고 안전한 고성능의 유사PBFT 합의 엔진을 제공하며, 악의적인 공격자들에게 엄격한 포크 책임(fork-accountability)을 묻는다. 텐더민트 코어의 BFT 합의 알고리즘은 공개형 지분증명 블록체인들의 확장성을 확보하는데 적합하다. 코스모스 네트워크의 허브와 존들은 블록체인 간 통신(IBC, Inter-blockchain communication) 프로토콜을 통해 상호 통신하며, 이 프로토콜은 블록체인들 간의 연동을 위한 가상의 UDP(User Datagram Protocol)와 TCP(Transmission Control Protocol) 역할을 한다. 토큰들은 존들 간 거래소의 유동성(exchange liquidity) 없이도 안전하고 신속하게 하나의 존에서 다른 존으로 전송될 수 있다. 존들 간 토큰 전송은 코스모스 허브를 통과하며, 코스모스 허브는 각 존이 보유한 토큰 총액을 추적한다.

[그림 3]은 코스모스 허브와 존과의 구조를 보여준다.

#### 4. 맺음말

블록체인 기반의 비트코인이 개발된 이후 빠른 속도로 블록체인 플랫폼과 코인이 늘어나고 있어 기술의 발전은 빠르게 이루어지는 것으로 보이나 파편화 또한 빠르게 심각해지고 있는 것이 사실이다. 이러한 문제를 해결하고 블록체인 생태계를 활성화하기 위해서 ISO/TC 307의 SG7에서는 블록체인 및 DLT 상호운용성 표준화에 대한 기술문서를 개발하였고 2018년 5월 런던회의에서 좀 더 세부적으로 구문적 데이터 및 의미적 데이터 측면에서의 블록체인 및 DLT 상호운용성 기술문서와 발견(Discovery) 측면에서의 블록체인 및 DLT 상호운용성 기술문서개발의 필요성을 제안하여 WG1에서 본 두 개의 문서 개발을 시작할 예정이다. 또한 SG7은 암호자산에 대한 상호운용성 연구를 2018년 10월 모스크바 회의까지 개발할 계획이다.

블록체인 산업계에서는 블록체인 상호운용성을 위한 기술로 사이드체인 및 코스모스 등 다양한 아이디어로 기술 개발을 진행 중에 있다. 또한 2017년 말에 아이온(Aion), 완체인(Wanchain), 그리고 아이콘(ICON)은 블록체인 상호운용성 표준을 만드는 것을 목적으로 블록체인 상호운용성 얼라이언스(Blockchain Interoperability Alliance)를 생성하였다[6].

블록체인 및 DLT 기술은 기반이 되는 기술로 금융뿐 아니라 다양한 산업기반 기술로 생태계 활성화를 위해 이종 플랫폼 간 융합을 편리하게 지원할 수 있는 핵심 기반표준 개발이 절실하다. 이뿐 아니라 블록체인 분야의 IPR과 표준화를 전략적으로 선점하기 위한 노력이 절실히 요구되는 시점으로, 특히 우리가 강점을 지닌 분야를 찾아 특화된 블록체인 기술 개발이 필요하며, 더불어 이와 관련된 표준화 병행 필요성에 대한 부분도 새롭게 고민해 볼 시점이라고 할 수 있다. 

---

※이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(2017-0-00472, 안전한 웹기반 개방형 핀테크 플랫폼 표준 개발).

#### [참고문헌]

- [1] ISO/TC 307, 2018, URL: <https://www.iso.org/committee/6266604.html>
- [2] ISO/IEC 19941 Cloud computing – Interoperability and Portability, 2017, URL: <https://www.iso.org/standard/66639.html>
- [3] Blockstream, URL: <https://blockstream.com/technology/>
- [4] Shaan Ray, 'What are Sidechains?', URL: <https://hackernoon.com/what-are-sidechains-1c45ea2daf3>
- [5] Jae Kwon, Ethan Buchman, 'Cosmos', URL: <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md>
- [6] Blockchain Interoperability Alliance (BIA) - Defining Blockchain 3.0, <https://cryptovest.com/education/blockchain-interoperability-alliance-bia---defining-blockchain-30/>