ITU-T에서 분산원장기술 표준화 동향

Standard Status on ITU-T Distributed Ledger Technology

권동승 (D.S. Kwon, dskwon@etri.re.kr) 지능형고밀집스몰셀연구실 책임연구원
박종대 (J.D. Park, parkjd@etri.re.kr) 블록체인기술연구센터 책임연구원

ABSTRACT

Distributed Ledger Technology (DLT) refers to a process and related technologies that enable a person to safely suggest, verify, and record state changes (usually updates) to synchronize ledgers distributed across network nodes. DLTs are becoming increasingly important as data management requirements evolve. Therefore, they need to understand the current state of standards (such as distributed storage and access technologies) to address future requirements. This paper provides ITU-T FG-DLT standard activities, such as standardization ization trends, use cases, reference architectures, platform evaluation criteria and future prospects.

KEYWORDS Blockchain, Distributed Ledger

Ⅰ. 서론

인류를 지구상의 다른 모든 생물과 구별하는 주요 특징 중 하나는 가능한 한 많은 역사를 기록하고 지식을 다음 세대에 전달하는 능력이다. 이 역사는 돌, 대나무, 옷, 종이에 기록되었으며, 현재는 도서관 등에 보관되어 있다. 그럼에도 불구하고 이 역사는 완전하지 않으며, 불가피하게 귀중한 문화·체험·지식이 상실되었다. 앞으로는 분산원장기술(DLT: Distributed Ledger Technology) 덕분에 더 많은 데이터를 교차 인증된 것으로 기록할 수 있게 된다. DLT는 네트워크 노드에 분산되어 있는 원장을 동기화하기 위해 상태 변경(일반적으로 업데이트)을 안전하게 제안, 검증 및 기록할 수 있게 하는 프로세스 및 관련 기술을 말한다. 데이터 관리 요구사항의 발전에 따라 DLT가 중요한 역할을 수행해야 한다면, 미래 요구사항을 해결하기 위해 데이터의 분산 저장, 액세스 기술 등의 현 표준 현황을 파악할 필요가 있다.

블록체인 관련 공적 표준은 ISO 및 ITU-T

* DOI: https://doi.org/10.22648/ETRI.2020.J.350205
* 이 논문은 2019년도 정부의 지원을 받아 ETRI에서 수행된 연구임[19ZH1200, 데이터 안심사회를 위한 트러스트 데이터 커넥톰 원천기술개발].

가, 사실 표준은 W3C 및 IEEE가 담당하고 있다. ITU-T는 2017년부터 표준화 연구를 시작하였고, 그 중 ITU-T FG-DLT(Focus Group on application of Distributed Ledger Technology)는 2019년 8월 DLT 관련 8개 기술 보고서를 발간하였다. 이 보고서는 DLT 용어 정의, 개념과 생태계, 표준화 현황, 유즈 케이스, 참고 아키텍처, 플랫폼 평가 기준, 규제 프레임워크 그리고 전망에 대한 것이다[1-8].

제시된 유즈 케이스를 보면 대부분의 경우 응용 개발에 대한 표준화된 접근 방식을 채택하면 도움이 될 것임을 알 수 있다. 즉 모든 응용은 비용 절감 및 표준화된 인터페이스 고유의 상호운용성을 이용하므로, 표준 인터페이스로 서비스 제공업체 간 솔루션 이식성의 이득을 얻을 수 있다.

현 DLT들은 특정 유즈 케이스별로 합의 메커니즘, 스마트 컨트랙트 코딩 언어, 자원 요구사항 등 기능에 따라 서로 다른 원장 유형이 있으므로 원장 수준에서 실제로 표준화가 필요한지 의문이 제기된다. 따라서 원장 계층 표준화는 모든 원장 유형을 하나의 공통 원장 유형 또는 하나의 공통 체인 유형으로 줄이는 것보다 서로 다른 원장 간 상호운용성 촉진에 중점을 두고 있다. 이는 다른 원장에 의해 작성된 다른 체인에 존재하는 기록을 링크 혹은 참조하는 표준화가 필요하다는 것이다.

DLT 응용 프로그램 수준에서 표준화는 집중해야 할 부분이지만, 현재 모든 응용 프로그램은 개발자가 독점 개발하므로 응용 프로그램이 개발자에 종속되고, 다양성을 줄이며, 운영 위험을 증가시키므로 표준화로 실질적인 이익을 가져올 수 있다. 표준화의 또 다른 중요한 측면은 원장 유형 간 응용 프로그램의 이식성이 있다.

본 논문에서는 ITU-T FG-DLT에서 2019년 8월에 발간한 기술보고서 중 표준화 동향[3], 유즈 케이스[4], 참조 아키텍처[5], 플랫폼 평가 기준[6]과 미래 전망[8]에 대해 분석 정리하였다.

Ⅱ. 국내외 표준화 동향

1. ISO

ISO는 2016년 11월 호주 제안으로 용어와 사용자, 응용, 그리고 시스템 간 상호운용성 및 데이터 교환을 위한 표준 개발을 목적으로 TC 307 블록체인과 DLT를 신설했다. 2017년 4월 1차 회의에서 블록체인과 분산원장의 표준 개발 범위 확정, 표준화 항목 선정과 작업반(WG1)과 5개 연구반을 신설했다. 2019년 5월, 6개 작업반으로 재편 후, 블록체인 참조 구조 및 데이터 교환 등 DLT기반기술 표준화, 블록체인 보안 및 식별체계, 스마트 컨트랙트 표준화, 거버넌스, 블록체인 유즈 케이스와 블록체인 상호운용성을 표준화 중이다.

2. ITU-T

ITU-T는 2017년부터 SG-13/16/17/20에서 블록체인 표준화를 시작했고, 정보보호 연구그룹인 SG-17과 FG-DLT가 가장 활발하게 활동 중이다.

SG-17은 2017년 9월 DLT 정보보호 표준화 작업 그룹인 Q14/17을 설립하였고, DLT를 위한 정보보호, DLT에 의한 정보보호, 그리고 정보보호 관리에 대한 작업으로 10개 표준 권고를 작업 중이다. DLT기반 데이터 액세스와 공유 관리 시스템을 위한 정보보호 프레임워크, 아이덴티티 관리에서 DLT 사용을 위한 정보보호 고려사항, DLT를 위한 정보보호 보증, DLT를 위한 정보보호 위협, DLT 정보보호 프레임워크, DLT기반 IP관리를 위한 정보보호 요구사항, DLT기반 정보보호 서비스, DLT를 사용한 온라인 투표에 대한 정보보호 위협, DLT기반 디지털 지불 서비스를 위한 정보보호 위

협과 요구사항, DLT기반의 안전한 SW 프로그램 배분 메커니즘을 위한 기술적 프레임워크이다.

FG-DLT는 DLT 응용과 서비스의 식별과 분석하고 구현을 위한 모범 사례 및 지침을 도출하며, ITU-T SG에 DLT 표준화 작업을 제안하기 위해 2017년 5월 신설되었고, 2019년 8월 8개 기술보고서를 완료하였다. DLT 용어 및 정의, DLT 개요·개념·생태계, DLT 표준화 현황, DLT 유즈 케이스, DLT 레퍼런스 아키텍처, DLT 플랫폼 평가 기준, DLT 규제 프레임워크, DLT 전망이다.

SG-16은 2018년 하반기 DLT와 E-Service를 위한 표준화 작업 그룹인 Q22/16과 Q24/16을 설립했고, 각각 표준 권고 4개와 3개 작업 중이다. Q22/16은 DLT 요구사항, DLT 평가 기준, DLT 레퍼런스 프레임워크, DLT기반 디지털 증거 서비스를, Q24/16은 휴먼 케어 서비스를 위한 DLT 요구사항, 개인 건강 기록을 위한 DLT 서비스 모델, 블록체인 기반의 휴먼 팩터 서비스 모델 요구사항과 프레임워크이다.

SG-13도 소프트웨어 정의 네트워크와 네트워크 기능 가상화를 포함하는 차세대 네트워크 진화를 담당하는 Q2/13과 클라우드 컴퓨팅과 빅데이터를 위한 요구사항·생태계·일반 능력을 담당하는 Q17/13에서 DLT 관련된 작업을 하고 있다. Q2/13은 차세대 네트워크 진화에서 블록체인 시나리오와 능력 요구사항을, Q17/13은 Blockchain as a Service를 위한 클라우드 컴퓨팅 기능 요구사항을 개발 중이다.

IoT와 스마트 시티 및 커뮤니티 표준화를 담당하는 SG20도 DLT 관련 5종의 표준 권고를 개발 중이다.

2017년 5월 Digital Fiat Currency(DFC)를 포함한 디지털 화폐 도입이 모바일 머니에 미치는 영향을 분석하였고, DFC의 잠재적인 유즈 케이스와 표준화 영역의 윤곽을 그리는 Focus group on Digital Financial Service(FG-DFC)가 신설됐고, 2019년 6월 7개의 표준 권고를 완료하였다. 중앙은행 보고를 위한 디지털 화폐의 체크리스트, 중앙은행 디지털 화폐를 위한 규제적인 도전과 위험, DFC의 거버넌스 관점에 대한 레퍼런스 다큐멘테이션, DFC 분류법과 용어 정의, 레퍼런스 아키텍처와 유즈 케이스, 디지털 화폐를 위한 보호 보증, 지불 거래를 위한 보호 보증 유즈 케이스이다.

2017년 3월 IoT와 Smart Cities & Communities(SC&C) 지원을 위한 데이터 처리와 관리에 표준화 로드맵을 개발하는 Focus group on Data Processing and Management to support IoT and Smart Cities & Communities(FG-DPM)가 신설되었고, 3개의 표준 권고를 완료하였다. DPM 관점에서 IoT와 SC&C 지원을 위한 블록체인 개요, 블록체인 기반 데이터 교환과 공유 기술, IoT와 SC&C 지원을 위한 블록체인 기반 데이터 관리이다.

3. W3C와 IEEE

2016년부터 W3C, IEEE에서 블록체인 기술표준 개발 활동을 시작하였으나, 미흡한 수준이다.

W3C는 현재 3개의 드래프트 문서[Verifiable Credentials Data Model 1.0, The Web Ledger Protocol 1.0, Decentralized Identifiers(DIDs) v0.13]를 출판하였다.

IEEE는 암호화폐 교환 작업그룹(P2140.1/2/3/4/5), 부패에 대한 블록체인 작업그룹(P2141.1), 블록체인 기술을 사용한 E-invoice 비즈니스 작업그룹(P2142.1), 암호화폐 지불 작업그룹(P.2143.1/2/3), 신뢰 IoT 데이터 관리 작업그룹(P.2144.1/2/3)이 활동 중이다. 특히 "사물인터넷에서의 블록체인 활용 프레임워크(P2418)"는 2021

년까지 표준 완료 예정인데, IoT에서 블록체인 사용 프레임워크, 블록체인 시스템을 위한 데이터 포맷 표준, 농업에서 DLT 사용 표준 프레임워크, Connected & Autonomous Vehicles에서 DLT 사용 표준 프레임워크, 에너지에서 블록체인 표준, Healthcare and the Life and Social Sciences에서 DLT 사용 표준 프레임워크, 공급체인 금융에서 블록체인 표준 프레임워크, 정부에서 블록체인 응용 표준, 암호화폐기반의 security token 표준, 블록체인 기반 디지털 자신 관리 표준이다.

4. 유럽

ETSI는 2018년 허가형 분산원장에서 산업 규격 그룹(ISG-PDL: Industry Specification Group-Permissioned Distributed Ledger)을 설립하고, 표준과 기술의 PDL 현황, 연결된 기계를 위한 데이터 처리 요구사항에 대한 PDL 적용과 규정 준수, PDL 응용 시나리오의 3개 표준을 진행 중이다.

2017년 유럽표준화기구와 유럽전기표준화위원회는 유럽을 위한 블록체인과 DLT 표준에서 갭을 식별하고, 그것을 ISO/TC 307 작업에 매핑하기 위해 공동으로 블록체인과 DLT에 대한 포커스 그룹(FG-BDLT: Focus Group-Blockchain and Distributed Ledger Technology)을 만들었다. FG-BDLT는 2018년 유럽에서 블록체인과 DLT 표준화를 위한 권고안을 포함한 백서 출판 후 2019년 이머징 기술을 반영해서 보완 작업 중이다.

미국 상무성 산하의 NIST는 2017년 Industrial Applications Community of Interest(BIA COI)을 위한 블록체인을 설립했고, 2018년 10월 블록체인 기술의 상위 레벨 기술적 개요를 제공하면서 암호화폐로 적용성을 다룬 NIST.IR.8202을 발간했다.

독일 표준화 단체인 The German Institute for Standardization(DIN)은 ISO/TC 307 멤버로서 DLT 관련 표준화에 참여하며, Industries 4.0을 위한 응용 시나리오에서 블록체인과 DLT(DIN SPEC 3103)을 완료했고, 블록체인 기술을 사용하여 개인 데이터 처리를 위한 표준화 모델[Privacy by Blockchain design(DIN SPEC 4997)]을 작업 중이다.

5. 국내

2017년부터 TTA는 개인정보보호·ID 관리와 블록체인 정보보호 프로젝트 그룹(PG 502)을 중심으로 블록체인 표준 개발을 시작하였고, 2019년 블록체인 표준을 담당하는 블록체인 기반 프로젝트 그룹(PG1006)을 신설하여 본격적인 국내 표준 개발을 시작하였다.

Ⅲ. DLT 유즈 케이스

ITU-T FG-DLT는 2017~2019년 7월 동안 전 세계 블록체인 개발업체가 제출한 DLT 중 2019년 7월 현재 개념 증명 단계의 유즈 케이스기반으로 응용 프로그램과 서비스 정보를 기술보고서[4]로 발간했다. 이 보고서는 DLT기반 응용과 서비스의 잠재적 경쟁우위, 수직 및 수평 도메인의 유즈 케이스, DLT 채택 시 주요 장애요소, 그리고 수집된 유즈 케이스의 국제 표준화로 얻는 이점 등을 포함하였다.

1. DLT기반 응용과 서비스의 잠재적 경쟁우위

DLT 사용으로 얻는 이점은 사용 사례, 환경, 이벤트, 프로세스 및 산업에 따라 다르며, 일반적으로 얻는 공통적인 혜택으로 다음 네 가지를 언급하

였다.

첫째, DLT는 전 세계적으로 확장 가능한 서비스로서 안전하고 비용 효율적인 기술이라는 견해이다. 기존 솔루션을 개선하고 새로운 제품 및 서비스 개발을 추진할 수 있는 다양한 혁신을 지원한다는 것이다.

둘째, DLT는 시스템 고장에 저항하는 변조 방지 및 감사 가능한 기술이고, 또한 사기를 감지하고 완화하는 효과적인 도구이다.

셋째, DLT는 범용 기술 형태로 볼 수 있다. 특히 DLT는 신뢰, 익명성, 스토리지, 처리 측면에서 데이터를 보는 방식을 혁신하므로, "데이터가 모든 것"인 정보 시대에서 DLT 정보처리 방식과 처리 데이터 유형에 관계없이 많은 분야에서 유용한 도구가 될 수 있다.

넷째, DLT는 상호작용 및 트랜잭션을 이해 가능하고, 추적 가능하며, 인증 가능하고, 책임감 있게 만드는 신뢰와 투명한 정보 공유 리소스로 인식되고 있다. 주요 수혜자는 데이터를 안전하고 책임감 있게 공유할 수 있는 신뢰할 수 있는 인프라를 구축하려는 신뢰할 수 없는 이해관계자를 포함하는 유즈 케이스이다.

DLT기반 정보보호는 데이터 암호화, 액세스 제어, 변조 방지된 데이터, 신원 관리, 결함 저항성을 제공할 수 있다. 따라서 DLT는 안전한 데이터 출처를 제공하며, 이는 데이터 진위, 법의학 및 개인정보보호에 중요하고, 개인정보보호를 강화한다. 도난 또는 데이터 조작으로부터 소비자와 기업을 보호하여 변조 방지 기록을 보장할 수 있으며, 사기와 싸우는 데 중요한 역할을 하며, 잘못된 바인딩을 감지하고 수정하는 데 도움이 되며, 신원 정보 자체를 공개하지 않고 신원 정보의 검증을 위한 효과적인 도구로서 기능할 가능성을 보여 주고 있다.

2. 수직 도메인에서 유즈 케이스

수직 영역에는 금융, 의료, 정보 및 통신 기술, 엔터테인먼트, 산업, 정부 및 공공 부문에서 DLT가 지원하는 애플리케이션 및 서비스를 포함한다.

가. 금융

DLT가 가장 성숙한 사용 사례 중 하나가 금융 서비스 산업이다. 금융결제에서 명백한 사용(비트코인)에서 복잡한 결제(ASX와 Digital Assets 파트너십)까지 초기부터 기술 시험을 해왔다. 사내 기술 개발(JP Morgan's Quorum), 전략적 투자(Goldman's Circle에 대한 투자)가 진행 중이며 많은 업체가 기술 컨소시엄(R3 CEV)에 참여하고 있다. 현 금융시장 시스템을 고려할 때 DLT는 다음 문제를 해결할 수 있다.

- 데이터 사일로에서 발생하는 정보 조정에 많은 시간과 비용이 소요되는 프로세스
- 서로 다른 이해관계자 간 신뢰 부족
- 개별 플레이어가 호스팅하는 데이터의 대규모 손상 위험을 포함한 중앙 데이터베이스의 사이버 공격 취약성
- 사용자가 실제로 데이터의 소유자가 아닌 상황
- 24/7/365 작업에 적합하지 않은 프로세스

나. 건강

환자 데이터의 사일로화는 정보 비대칭성에 기여하며, 시장 경쟁의 불균형과 적절한 환자 진단을 위한 정보 공유 부족을 유발하며, 진단 속도가 느려지고 시험 비용이 비싸진다. 건강 데이터는 민감한 개인정보이므로 수집, 기록 및 분석이 훨씬 더 정교해야 하는 문제를 해결해야 한다. 그리고 상호운용성은 환자중심 모델 지원에서 근본적으로 정

보보호를 강화하는 동시에 서비스 제공업체 간 신뢰의 필요성을 줄인다.

제약업체는 개발한 제품의 특허 추적, 그리고 백신과 자가 면역질환 같은 특정 약물 생산을 위해 정부로부터 지원받은 자금 이동과 공급망을 통한 의료 상품 이동 등에서 결제와 제품의 투명성과 추적성 확보를 위해 DLT를 적용하고 있다. 생명공학 회사는 업무에 민감한 유전자 데이터와 자료를 사용하므로 데이터 무결성, 개인정보보호와 액세스 제어에서 DLT를 적용하고 있다.

의료 서비스는 환자 중심으로 전환되고 있으며, 환자의 민감한 의료 데이터는 사이버 공격으로부터 보호하는 것이 중요하다. DLT기반으로 건강 시스템은 환자가 자신의 건강 기록에 대한 통제력을 유지하므로 환자 데이터의 안전성과 신뢰성을 높일 수 있다. DLT는 환자의 건강 이력과 의료 기록을 더 잘 제어할 수 있어서 더 나은 의사결정 및 예방 조치를 적용할 수 있게 한다.

다. 예술, 설계 그리고 문화 영역

DLT는 예술적 창작 및 생산을 위한 새로운 매체 및 재료로 역할을 할 수 있다. 즉 예술가들은 다양한 영역(음악, 예술, 유형 및 무형의 대상)에서 공동 소유권, 예술적 암호화폐와 협동에 DLT를 적용하고 있다. DLT를 사용하면 새로운 형태의 미술 경매를 지원하고, 미술품과 컬렉션의 공동 소유권을 지원하게 하여 작품을 디지털로 조각화하여 미술 작품을 공유하게 할 수 있다.

공연자와 창작자의 협업을 추적해서 경력과 업적에 대한 전문 자격과 경험 기록을 만드는 방식으로 전문 업적을 조합해서 실제 예술 실무 에코시스템에서 평판 관리, 차트 네트워크, 협업과 게스트 공연을 용이하게 한다. 또한 많은 공연자들이 자신의 작업을 텍스트, 이미지, 비디오, AR/VR, 움직임 분석 및 센서 데이터 등을 디지털 데이터를 DLT기반으로 만들면 디지털 아카이브를 만들면 디지털 공연물을 이용하는 경우, 소유권과 로열티를 DLT를 통해 주장할 수 있다.

지적재산권 도난의 맥락과 광고 소재의 저작권 및 소득 보호에 대해서도 DLT기반 온라인 아웃렛이 나타나고 있다.

라. e-Sports와 게임

e-Sports와 게임은 가상화폐 사용의 선구자로 DLT를 기존 게임에 적용 시 진입 장벽은 적다. 이전에는 소수 엘리트 플레이어만 토너먼트에서 상금을 놓고 경쟁할 수 있었으나, 이제 게이머와 회사가 스마트 컨트랙트의 안전한 방식으로 장을 만들고 상을 제공하는 DLT기반 플랫폼에서 플레이어는 자신의 소규모 P2P 토너먼트를 운영할 수 있다. 아마추어 선수나 신입 선수는 전통적인 자금 이체, 재정 규정 및 부패와 중개인의 부패에 의존하지 않고 참여하고 기술을 시험하며 게임에 베팅할 수 있다. 베팅은 e-Sports 토너먼트의 매우 인기 있는 부산물이며 해당 공간에서 많은 수입을 차지한다. DLT는 중앙의 통제를 벗어난 저비용 베팅을 위한 신뢰할 수 있는 안전한 생태계를 만들 수 있으므로, 한 번도 왜곡된 확률로 인해 주저하거나 참여를 두려워하는 사람도 스마트 컨트랙트 덕분에 안심하고 마음대로 할 수 있다.

마. 산업

제품과 서비스별 요구사항에 따라 DLT 구성 요소를 최적화하여 투명하며 분산되고 효율적이며 안전한 DLT 시스템을 만들 수 있다. 대부분은 다자 간 데이터 교환, 물류 조정, 자동 결제 및 계약, 감사와 규정 준수 요구사항 등에서 DLT는 비용 효율적인 정보, 운영 및 재무 관리를 위한 실용적인

솔루션을 제공할 수 있다.

상품, 데이터와 돈의 흐름을 효율적으로 관리하는 공급망의 핵심 요구사항은 DLT 강점인 신뢰성과 무결성이고, DLT 분산 합의는 체인의 모든 엔티티가 독립적으로 검증된 원장에 액세스할 수 있으므로 공급망 분쟁 해결에 적합하다. DLT는 운송 전체 프로세스에서 변조 방지, 추적 가능 기록, 간소화된 클레임 정산, 자동 결제 거래, 투명한 가격과 소유권 정보를 제공한다. DLT는 식품 공급망에서 추적성 개선과 동시에 생산원, 품질과 안전 관리를 포함하여 식품 생산의 전체 공정에 걸쳐 데이터 기록에 사용될 수 있으며, 동시에 농민, 유통 업체 등을 위한 효율적이고 공정한 지불 솔루션을 가능하게 한다. 또한 DLT는 직원의 전체 고용 이력(또는 개인정보보호를 위한 개인 정보의 해시) 및 법인 관련 활동을 포함하여 변조 방지 정보를 저장할 수 있다.

바. 정부 및 공공 부문

디지털화 수준이 높은 정부에서도 위조 및 변조를 방지하기 위해 DLT를 사용할 수 있다. DLT는 신뢰할 수 있는 정보 관리를 단순화하여 정부기관이 중요한 공공 부문 데이터에 쉽게 액세스하고 사용할 수 있도록 하면서 이 정보를 보호할 수 있다. 그동안 정부는 정부 업무에 대한 책임, 투명성과 효율성을 높이기 위해 DLT 실험을 시작했다.

DLT는 투명하고 분산된 디지털 네트워크를 통해 정부가 데이터를 효과적으로 수집·저장하여 데이터 관리 프로세스 개선과 정부 신뢰를 높일 수 있다. DLT의 가장 중요한 기능 중 하나는 신원, 소유권·자산 등록, 건강 관리, 교육 인증, 전자 투표 등을 언급하는 다양한 종류의 데이터 기록 및 공유에 관한 것이다. 일회성 원칙은 시민과 기업은 공공 행정 부서와 접촉 시 한 번만 다양한 데이터를 제공하면, 공공기관은 데이터 보호 규정과 기타 제약 조건하에 국경을 넘어도 이 데이터를 내부적으로 공유하고 재사용되는 조치를 취한다는 것이다. EU는 전자 정부 행동 계획 2016–2020에서 이 원칙을 시행하기 시작했으며 유럽 디지털 단일 시장과 관련된 여러 이니셔티브의 일부로, SCOOP4C 및 TOOP가 있다.

3. 수평 도메인에서 유즈 케이스

수평 도메인으로는 아이덴티티 관리, 정보보호 관리, 데이터 관리, 거버넌스와 DAO(Distributed Autonomous Organization), 그리고 크립토 인프라가 있다.

DLT기반 디지털 아이덴티티 솔루션은 보안, 개인정보와 이식성 세 가지 주요 과제에 중점을 두고 있다. 개인과 기업은 DLT에 자신의 아이덴티티를 저장하고 인증할 수 있고, DLT기반 아이덴티티 관리는 개인의 아이덴티티를 밝히지 않고 개인과 기능을 연결할 수 있으며, 염탐자에게 민감 정보를 유출하지 않고, 신원 도용을 방지할 수 있다.

정보보호 관리는 조직의 자산(사람, 건물, 기계, 시스템 및 정보 자산 등)을 식별한 후 이 자산을 보호하기 위한 정책 및 절차의 개발, 문서화 및 구현을 의미한다. DLT는 기밀성, 무결성 및 가용성을 제공하므로 복원성, 암호화, 감사 및 투명성이 향상될 수 있다.

DLT는 네트워크 노드 간에 분산된 네트워크 활동 기록에 대한 인증된 레코드이므로, 개인 키 집합을 확보하여 네트워크 내에서 임의의 정보를 안전하게 저장할 수 있다. 향후 DLT는 임의의 데이터를 저장하고 분산된 가상머신이 수행하는 자체 관리와 자체 실행 스크립트를 통해 해당 데이터의 수정 권한을 설정할 수 있게 된다. 이 스크립트(스

마트 컨트랙트)는 플랫폼 운영자가 DLT과 사용자와의 상호작용을 제어하는 복잡하고 완전히 사용자 정의 가능한 규칙을 정의할 수 있다.

DLT는 인터넷상에서 자치권을 가진 분산된 글로벌 공공 유틸리티에 대한 거버넌스를 실현하는 새로운 도구인 DAO를 만드는 데 사용될 수 있다.

4. DLT 채택 시 장애 요인

DLT 채택에 대한 주요 장벽으로 일반적인 기술적 위험, DLT 지식부족으로 인한 위험, 생태계 장벽, 고유 기능에서 야기되는 장벽과 법적인 고려사항이 있다. 일반적인 기술 위험은 현 인프라에서 DLT 인프라로 전환 위험, 탈중앙화·확장성·보안의 Trilemma 문제, 비표준 문제, 데이터 보호 문제, 현 비트코인에서도 존재하는 장애, DLT 채택의 비활성화로 타 이머징 기술 대비 느린 투자수익율 문제, 잠재적인 고비용 구현, 프라이버시 문제 등이다.

현 DLT 플랫폼은 탈중앙화, 확장성 및 정보보호 세 가지 목표를 동시에 만족시키는 기술은 없으나, 두 가지까지는 동시에 효과적으로 달성할 수 있다. 정보보호 문제는 DLT 네트워크 결함으로 인해 사용자에게 심각한 영향을 주고, 확장성 문제는 합의 메커니즘, 노드 수 및 네트워크 성능의 영향을 받는 처리량 및 처리 속도 병목 현상을 유발할 수 있다. 탈중앙화는 중앙집중식 엔티티 없이 중개 및 자율적 운영을 가능하게 하지만, 탈중앙화는 엄격하고 리소스 소비가 많은 합의 메커니즘을 통한 관리가 필요하며 노드가 오래되거나 해킹된 코드 사용 시 정보보호 위험이 발생할 수 있다. 공개 DLT에 암호화된 개인 데이터를 저장하면 비용이 많이 들고 여전히 데이터 보호 문제가 발생한다. 새로운 암호화 기술, 제로 지식 증명 및 다자 간 계산은 일단 성숙되면 이 문제를 해결할 수 있다. 잠재적인 보안 취약점과 데이터 개인정보보호에 대한 우려는 특히 사용자가 개인 데이터로 DLT 솔루션을 위임하는 경우 중요한 과제이다.

DLT 지식부족으로 인한 위험은 DLT 이해 부족, DLT와 암호화폐 및 토큰 차이점 이해 부족, DLT 사기와 해킹 등의 나쁜 평판, 광범위한 채택을 제한하는 상호운용 불가능한 여러 DLT를 극복하는 기술 부족, 탈중앙화 거버넌스 메커니즘과 관련된 경험 부족 등이 있다. 한편으로, “블록체인으로 문제를 해결할 수 있다”고 하지만, 다른 한편으로, DLT 사용으로 이익을 얻을 수 있는 복잡한 시스템이 그 기술에 대한 지식이나 이해 부족으로 인해 기술을 채택하지 않는 경우가 많다.

생태계 장벽으로는 지배적인 DLT 플랫폼이 없고, 대안 솔루션이 많은 데, 개별 DLT을 연동시키는 상호운용성 미흡, 미개발된 프론트엔드, 지원하는 인프라 부족, DLT 제공 업체의 신뢰성 등이 있다. 허가 및 비허가 플랫폼 시장 경쟁 상황에서 많은 회사들은 사용가능한 솔루션 품질 평가, 기존 IT 환경에 솔루션을 통합 방법 등 불확실성으로 투자 결정이 어려워 주요 플랫폼과 응용 출현을 기다리고 있다. 개별 DLT 플랫폼 간 상호호환성 문제는 일부 DLT 플랫폼이 사이드 체인 및 원자 교환과 같은 대체 방법을 연구개발 등으로 체인 간 상호운용성 발전에도 불구하고 여전히 채택 장벽으로 남아 있다. 제품의 사용 편의성을 위한 프런트엔드는 기술과 백엔드가 성숙에 따라 UI와 UX는 계속 개발되고 있지만, 현재는 여전히 사람들이 응용 프로그램을 사용하고 채택하는 것은 매우 어렵다. 많은 ICT 관심 기업들은 대부분의 DLT 제공업체가 재무 안정성 및 제품 로드맵이 불확실한 신생기업이라 수명이 길고 안정적인 공급업체 식별에 어려움이 있다.

고유 기능에서 야기되는 장벽으로는 DLT를 하나로 통합 시 복잡도로 인한 어려움, 지적 재산권 문제, 불변성, 대규모 DLT 플랫폼을 업그레이드하고 발전시키는 데 어려움, 새로운 형태의 사이버 공격 대응 등이 있다. DLT 채택은 중앙에서 관리되는 단일 조직에서도 충분히 복잡한데, 중앙에서 관리되지 않는 다중 엔티티 환경에 DLT 도입 시 더욱 복잡해진다. 분산 시스템은 플랫폼 업그레이드 시 모든 참가자의 동의가 필요하며, 특히 새로운 개인정보보호 및 확장성 기능 도입 작업도 중앙집중식 시스템에 비해 훨씬 복잡하므로 대규모 DLT 플랫폼의 업그레이드에 위험과 어려움이 있다.

Ⅳ. DLT 참조 아키텍처[5]

1. 개요

참고문헌 [5]의 3쪽 그림 1은 Ethereum과 Bitcoin 퍼블릭 체인, Hyperledger Fabric 프라이빗 체인과 비블록 체인 분산원장을 포괄하는 상위 레벨의 아키텍처로서, 자원 및 인프라 기능, 프로토콜/거버번스 및 규정 준수 기술, 분산 응용(DApp) 기능, 운용·유지 기능, 외부 상호작용 관리 기능과 외부 시스템 확장 기능으로 구성된다.

자원 및 인프라 기능은 DLT 시스템이 의존하는 자원의 지원을 담당하는 기본 계층으로 네트워크, 스토리지와 컴퓨팅 서비스를 포함한다. 네트워크 관리 기능, 스토리지 관리 기능, 유틸리티 기능과 노드 관리 기능으로 구분된다. 네트워크 관리 기능은 각 DLT 시스템이 현 네트워크 기반으로 분산 시스템 모델이 되도록 한다. 스토리지 관리 기능은 각 DLT 시스템에 데이터를 유지하고 데이터 보호 및 프라이버시를 보장하는 표준 스토리지가 있으며, 특히 스토리지 관리는 비용과 데이터 보호의 균형을 유지하기 위해 온 체인 비즈니스를 위한 솔루션을 제공할 수 있다. 유틸리티 기능은 DLT에 원시 데이터와 데이터 전송까지 데이터를 보호하는 것이다. 노드 관리 기능은 DLT 시스템 내부의 각 노드가 노드 소유자·운영자에 의해 유지되게 하는 것으로 DLT 시스템 내에서 단일 노드의 리소스를 관리한다.

DLT 각 노드는 시스템 기술 사양에 따라 자체 기술을 가질 수 있으나, 프로토콜 계층은 DLT 노드의 기술 사양을 제공하는 개념적 계층으로 거버넌스 및 규정 준수, 합의, 리더 관리와 메시징을 포함한다. 거버넌스 및 규정 준수에는 노드 관리, AAA 관리(계정과 권한 관리)가 포함하고, 시스템 거버넌스 관리(신뢰 보증)과 다른 구성 요소의 AAA 기능 관리를 지원한다. 합의 메커니즘은 DLT 핵심 구성 요소로 데이터 일관성 알고리즘, 데이터 유효성 검사, 데이터 배포 및 동기화가 포함된다. 합의 메커니즘을 사용하여 DLT 시스템은 네트워크 가설에 의존한 신뢰 메커니즘을 설정하고, 인센티브 메커니즘과 같은 신뢰 보증 모듈은 그 위에 구현되며, 퍼블릭 체인 데이터를 유지·관리한다. 원장 관리기능은 분산원장의 기본 데이터 관리와 네트워크상의 원장 데이터의 분산 관리를 제공하는 것으로, 원장의 로컬 데이터 저장 방법과 노드 간 동기화 메커니즘을 정의하고, 합의 메커니즘을 사용하여 권한 관리에 대응한다.

분산 응용(DApp) 기능은 런타임 관리, 스마트 컨트랙트 메커니즘 기능과 개방형 DApp 관리가 포함된다. 런타임 관리를 기반으로 DApp은 분산 네트워크 환경에서 다양한 비즈니스 요구사항을 충족하도록 구축된다. 스마트 컨트랙트 메커니즘에는 언어 정의, 코드 컴파일과 실행이 포함되며, 서로 다른 DLT에 대한 스마트 컨트랙트는 간단한 해석 스크립트 또는 프로그래밍 언어를 사용

하여 구현할 수 있다. 개방형 DApp 관리 계층은 DLT 네트워크를 DApp 비즈니스와 연결하는 미들웨어로서 DApp 개발자가 DApp을 작성·유지 보수할 수 있는 DApp 프레임워크와 DApp 호스트가 DApp을 쉽게 관리할 수 있는 스마트 컨트랙트 관리 메커니즘이 포함된다. DApp 프레임워크 내의 인터페이스는 DApp 개발자가 분산원장에 액세스하며, DApp 사용자는 인터페이스를 통해 DLT 서비스에 액세스한다.

운영·유지 보수 기능에는 로그, 모니터링, 노드·네트워크 관리와 스케일링 라이브러리 등 다양한 라이브러리가 포함된다. 각 DLT에는 자체 네트워크 가설, 신뢰 보증 가설·거버넌스 모델이 있으므로, 개방형 네트워크 가설이 있는 DLT는 외부 시스템과 상호작용할 수 있다.

DLT 플랫폼의 확장 기능은 데이터 상호운용성의 서로 다른 요구사항 해결을 목적으로 하며, 외부 시스템(멀티/사이드/오프 체인) 또는 내부 시스템(차일드 체인, 샤딩)의 데이터 상호운용을 위한 프로토콜과 사양이 포함된다. 각 DLT에는 하나의 거버넌스 모델이 있고, 내부 시스템 확장은 동일한 거버넌스 모델을 사용하여 하나의 DLT 생태계에 대한 확장성 문제를 해결하는 것을 목표로 한다. 차일드 체인은 스마트 컨트랙트 배포, 자산 발행, 투표 및 메시지 전송과 같은 운영 트랜잭션을 담당하는 고유 토큰이 있는 개별 원장으로 모든 차일드 체인은 네트워크의 부모 체인과 동일한 소스 코드를 통해 합의하고 공유하므로 네트워크의 모든 차일드 체인은 상호운용 가능하다.

외부 시스템 확장 기능은 대부분 비즈니스에서 데이터 상호운용성은 시스템 간 요구사항이므로 외부 시스템에 액세스하도록 하는 것이다. 오프 체인 시스템과 상호운용하는 것은 대부분 유즈 케이스이고, 또한 온 체인과 오프 체인 기술의 조합으로 2 계층 솔루션을 사용하여 DLT 시스템 성능과 확장성을 최적화한다.

2. 기능적 요소

DLT 플랫폼은 상위 레벨 아키텍처에서 일관성이 높지만 세부 아키텍처는 다를 수 있다. 참고문헌 [5]의 6쪽 그림 2의 기능적 아키텍처를 보면 크게 핵심 계층, 서비스 계층, 응용 서비스 플랫폼, DLT 응용, 그리고 외부 서비스로 구분된다. 핵심 계층은 자원과 프로토콜 기능, 서비스 계층은 프로토콜과 거버넌스 기능, 응용 서비스 플랫폼은 응용과 운용·유지 기능, 분산원장 응용은 응용 기능, 그리고 외부 서비스는 외부 상호작용과 확장 기능이다.

가. 핵심 계층

핵심 계층은 세부적으로 자원계층과 프로토콜 계층으로 구성된다. 자원 계층에는 안전한 HW, 네트워크 및 인프라, 스토리지 기능, 확장 가능한 통신, P2P 네트워크가 있고, 프로토콜 계층에는 신뢰하는 스토리지, 원장, 합의 메커니즘, 데이터 보호, 스마트 컨트랙트 메커니즘, 계정 관리, 그리고 시스템 관리로 구성된다.

DLT 시스템은 신뢰할 수 있고 안전한 하드웨어 환경에서 데이터 보호 및 프라이버시를 보장하면서 고성능으로 동작해야 한다. 확장 가능한 프로토콜 통신은 분산 시스템의 네트워크 가설을 기반으로 스케일러블 프로토콜 통신 모듈로서 가능하다면 동종 분산원장 네트워크를 위해 계층 7 필터링을 가진 서로 다른 체인 네트워크와 데이터 교환 기능을 제공하는 것을 목표로 한다. DLT 시스템은 네트워크 가설을 기반으로 하므로 네트워크 관리가 필요한데, 특히 비허가형 DLT 시스템에서 각

노드는 동일한 권한을 가지며, 노드 소유자는 노드 자체의 기여를 결정하며, 네트워크 관리는 노드 네트워크를 제어하는 기본 기능을 한다. 각 노드는 네트워크 발견 프로토콜로 인접 노드를 감지하고 링크를 설정하며, 이 프로토콜은 sybil 공격 등 다양한 공격을 방지하기 위해 노드 ID를 식별 인증해야 한다. 노드가 이웃 노드에 연결되면, 데이터 송수신기 모듈은 다른 노드와 데이터 교환(트랜잭션 브로드캐스트, 합의 메시지, 데이터 동기화)을 완료한다. 데이터 트랜시버 설계는 일련 번호, 확인 및 암호화 등 요구사항을 고려해야 한다.

DLT는 블록 데이터, 트랜잭션 데이터, 상태 데이터 및 로컬 계정의 개인 데이터 등 다양한 데이터를 지속 저장해야 한다. 데이터 유형과 DLT 설계에 따라 다른 저장 모드를 사용할 수 있고, 저장 모드에는 관계형·비관계형 데이터베이스와 자체 구성 파일이 포함된다.

합의 메커니즘은 데이터 동기화와 적법한 검증 기능을 한다. 데이터 동기화 모듈은 분산원장의 일관된 원장여부 확인 후, 서로 다른 노드 간 원장의 새로운 부분을 전송하고, 동기화된 데이터의 정확성과 일관성 보장을 위해 동기화된 데이터 유효성을 검사한다. 다른 유형의 노드는 모든 트랜잭션, 블록과 상태 데이터 동기화, 모든 트랜잭션과 블록 데이터 동기화, 부분 트랜잭션 데이터 동기화 등을 포함하는 서로 다른 동기화 방법이 있다. 합의 목적은 회계와 관련된 많은 노드가 공동의 계정을 공동으로 유지하는 것이고, 합의 알고리즘은 거래 데이터 자체의 검증이 아니라 거래 주문에 동의하는 알고리즘만을 지칭한다. 합의 알고리즘 설계 시 일관성, 적시성과 정보보호를 보장해야 한다. 합의 노드는 결국 데이터에 동의하고, 합의 노드는 가능한 한 빨리 데이터 합의를 완료하며, 일관성을 손상시키는 데 많은 비용이 들도록 쉽게 공격당하지 않아야 한다.

스마트 컨트랙트 메커니즘은 DLT 시스템에 작성된 프로그램으로, 특정 조건에 의해 유효성이 검증되고 트리거되는 방식으로 특정 유형의 DLT 시스템 트랜잭션에 대한 규칙을 인코딩하는 것으로 검증 모듈 언어 및 컴파일러 그리고 실행 엔진으로 구성된다.

스마트 컨트랙트 설계에는 일반적으로 컨트랙트 엔진, 컨트랙트 관리와 컨트랙트 데이터 관리가 포함된다. 컨트랙트 엔진은 그 코드를 실행하고 코드에 따라 컨트랙트 데이터를 유지하며, 그 코드 관리는 코드의 배포 및 저장 작업을 담당하며, 데이터 관리는 데이터를 유지 관리하고 컨트랙트 엔진에 대한 액세스 인터페이스를 제공한다.

검증 모듈에는 분산원장 및 기본 트랜잭션 확인을 위한 트랜잭션 버퍼 풀이 있고, 분산원장은 일반적으로 보낸 사람의 거래 잔액, 거래 번호 등을 확인한 후 DLT 시스템에 트랜잭션을 저장한다. 검증 모듈은 다양한 공격을 효과적으로 방지하고 분산원장의 안정적 작동을 보장해야 한다.

언어와 컴파일러는 컨트랙트 문법 사양과 컴파일 사양을 제공하며, 트랜잭션은 실행 엔진에 의해 처리된다. 비즈니스 요구사항이 매우 제한적인 경우 스크립트를 사용하여 컨트랙트를 구현할 수 있고, 가벼운 비즈니스에는 효율성이 높고 배포 복잡성을 줄이는 인라인 컨트랙트 엔진을, 대규모 기업에게는 더 많은 리소스와 더 높은 실행 효율성을 갖춘 외부 실행 환경을 권장한다.

실행 엔진은 외부 컨트랙트 실행 환경, 인라인 컨트랙트 엔진, 스크립팅·유한 상태 머신으로 구성된다. 외부 컨트랙트 실행 환경을 사용하여 컨트랙트 코드를 실행하고 일반적으로 외부 컨테이너 또는 가상 머신을 사용하여 모든 노드에 대해 일관된 실행 환경을 보장한다. 컨트랙트 데이터 유지

보수는 외부 환경에서 에이전트 프로세스와 통신하는 분산원장 프로세스로 수행된다.

인라인 컨트랙트 엔진은 프로세스에 임베드되며 컨트랙트 코드는 실행 중에 해석되거나 컴파일된 후에 구현된다. 이 엔진의 장점은 튜링 완전성, 빠른 컨트랙트 배포, 향상된 데이터 액세스 속도, 엔진 보안 강화, 컨트랙트 엔진 컴퓨팅 리소스의 편리한 관리 및 사용자 정의 기능이고, 단점은 컨트랙트가 메모리에 상주하지 않아서 무거운 비즈니스 수행 시 덜 효율적인 것이다.

스크립팅·유한 상태 머신은 일련의 실행 명령이 분산 원장에 사전 설정되어 있으며, 상태 머신에 의해 해석되는 컨트랙트 코드를 형성한다. 명령어의 복잡성과 코드 크기로 인해 스크립팅은 일반적으로 기능이 약하고 튜링 불완전해서 기본 작업만 수행한다. 스크립팅 기술은 구현하기 쉽고 그 기능이 효과적으로 제어되며 강력한 공격 방지 완화 기능이 있지만, 단점은 복잡한 스크립트 개발, 비 튜링 완전성 및 스크립트 규모가 작아서 기능이 제한적인 것이다.

원장은 모든 트랜잭션 데이터와 컨트랙트 데이터를 저장해야 하므로 트랜잭션과 프로세싱, 색인 작성과 콘트랙트 저장을 완료해야 한다. 원장 관리에는 원장 메커니즘과 신뢰하는 스토리지가 필요하며, 원장 메커니즘은 P2P 네트워킹과 확장된 스토리지 서비스에 의존하는 합의 메커니즘을 기반으로 하고, 신뢰하는 스토리지는 원장을 위한 확장된 스토리지 서비스를 제공한다.

나. 서비스 계층

서비스 계층은 상위 응용, 데이터 보호, 데이터 처리 관리, 데이터 AAA 관리 및 인프라 관리를 위한 기본 서비스를 제공하며, 분산원장 핵심계층과 DApp 간 미들웨어 역할을 한다.

분산 계정 시스템은 DLT 시스템에서 모든 종류의 엔티티와 데이터를 제공하며, 주소와 아이덴티티를 제어한다. 주소는 트러스트 데이터에 바인딩되며, 아이덴티티는 엔티티와 바인딩되고, 분산 아이덴티티와 다차원 인증 프로토콜을 기반으로 노드 운영자, 신뢰 보증 규제 역할, DApp 운영자, 최종 사용자와 확장된 IoT 액세스 엔티티의 관리를 제공한다. 분산 아이덴티티는 DLT 시스템에서 비즈니스 엔티티에 대한 암호화 기반 디지털 아이덴티티를 설정한다.

인증과 권한 부여를 위해 AAA 솔루션은 계정 관리의 전체 사용을 지원한다. 다양한 분산원장마다 다른 응용 프로그램 시나리오가 있으므로 권한 관리에 대한 접근 방식이 다를 수 있다.

노드(시스템) 관리는 보안 통신, 신뢰할 수 있는 데이터 전송, 관련 노드 운영과 네트워크 거버넌스 서비스이다. DLT 시스템 내부의 노드 관리는 네트워크 상태, 통신 채널 모니터링, 경보와 추적, 신뢰 보증, 노드 장애 모니터링 등을 포함한 노드 거버넌스 제어와 DLT 시스템의 거버넌스 제어이다.

서비스 계층에서 스마트 컨트랙트 메커니즘은 컨트랙트 등록, 컨트랙트 템플리트, 컨트랙트 컴파일러 및 VM 런타임을 위한 컴포넌트이다.

데이터 보호는 정책 구성, 액세스 제어, 데이터 정보보호와 프라이버시, 데이터 모니터링과 감사이다. 분산 시스템의 다양한 신뢰 승인 방법에 따라서 신뢰 보증 관리는 거버넌스 모델을 충족시키는 데 사용된다.

다. 응용 서비스 플랫폼

응용 서비스 플랫폼은 DApp 프레임워크, AAA, 데이터 프라이버시, 데이터 저장과 동기화 그리고 운영과 유지 관리를 담당한다.

DApp 프레임워크에는 DApp 개발, 분산원장 데

이터 관리가 분산원장 계정 관리를 지원하는 인터페이스가 있다. AAA 시스템은 DApp 사용자가 데이터에 액세스하고 처리하며, 트랜잭션 기반으로 데이터 교환을 수행할 수 있는 기능을 관리한다.

온 체인 사용자 데이터를 보호하고 응용에서 데이터 프라이버시 요구사항 충족을 위해 암호화 기술을 사용해야 한다. 프라이버시는 항상 DLT 적용 시 장애물 중 하나였으며, 규제 요구사항을 충족하고 데이터 프라이버시를 침해하지 않는 방법은 DLT 산업의 핵심이다. 따라서 프라이버시는 익명 제어, 고성능, 투명한 감독의 요구사항을 충족해야 한다.

DLT 관점에서 외부 서비스는 외부 시스템과 협력하기 위한 솔루션 제공으로, 확장한다는 것은 DLT 이외의 시스템, 타사 DLT 시스템 및/또는 레이어 2 블록체인 기술과 상호작용한다는 것을 말한다.

V. DLT 플랫폼 평가 기준

본고에서는 DLT 플랫폼의 핵심 기술, 응용 지원 기능과 동작 기능을 포함하여 DLT 플랫폼 평가 기준을 서술하였다[6].

1. 핵심 기술

DLT에서 사용자 계정은 공개키와 개인키로서 그 이름이 고유해야 하며, 사용자 또는 스마트 컨트랙트에 의해 생성되며, 개인 키는 클라이언트에만 보관한다.

트랜잭션 처리 기능은 자산 이전 트랜잭션과 비자산 이전 트랜잭션이 있으나, 이 두 가지 트랜잭션을 모두 지원할 필요는 없고, 사용자는 성공적으로 트랜잭션을 수행한 후 DLT의 모든 노드에서 결과를 확인할 수 있어야 한다.

쿼리는 사용자가 정보 요청으로 결과를 얻는 것으로, 잔액 조회와 조건부 쿼리가 있고, 조건부 쿼리는 사용자는 기간 지정 또는 지정된 사용자 계정과 같은 검색 조건으로 DLT 플랫폼에서 기록 정보를 검색하는 것이다.

합의 메커니즘 효과를 보장하려면 블록체인 플랫폼의 목표와 부합되도록 합의 프로세스에 참여하는 노드가 충분해야 한다. 합의 메커니즘은 합의에 도달하는 일련의 규칙과 절차로서, 분산 프로세스나 다중 에이전트 시스템 간에 단일 데이터 값 또는 단일 네트워크 상태에 대해 필요한 동의를 얻기 위해 DLT 플랫폼에 사용되는 데이터 일관성 메커니즘이다. 데이터 동기화 모듈은 동기화된 데이터의 유효성을 검사하여 즉각적 또는 최종적인 최종성에 관계없이 정확성과 일관성을 보장하는 것이다. 악의적 동작이나 시스템 오류가 있는 일부 노드에도 불구하고 DLT 시스템은 계속 작동해야 한다. 허용된 악의적 또한 충돌된 노드에 대한 임계값은 선택된 합의 메커니즘과 DLT 플랫폼 설계에 의해 결정된다.

DLT에서 개인 키 관리는 사용자 경험과 정보보호 조치에 중요한 기능으로 사용자의 개인키를 유지하는 안정적이고 안전한 방법을 제공한다. 개인키의 저장 및 사용은 분리될 수 있고, 사용자는 개인키 사용을 완전히 제어할 수 있어야 한다. 개인키의 저장 방법에는 소프트웨어 지갑 방법과 하드웨어 지갑 방법이 있다.

스마트 컨트랙트 메커니즘에는 언어 정의, 코드 컴파일과 실행이 포함되며, 서로 다른 DLT 시스템에 대한 스마트 컨트랙트는 간단한 해석 스크립트 또는 프로그래밍 언어를 사용하여 구현할 수 있다. 이 메커니즘에는 참가자 상태 모니터링 기능과 스마트 컨트랙트 수명주기 관리 기능이 있다.

DLT 시스템은 시스템 보안을 최대한 보장하고 정보보호(암호화 선언, 플로그러블 암호화 알고리즘, 암호화 알고리즘의 효과성, 암호화 강도) 측정을 공개해야 한다.

2. 응용 지원

사용자 인증은 사용자 계정 확인, 로그인 상태 관리, 사용자 분류와 관리, 권한 부여와 스마트 컨트랙트 데이터 액세스 제어가 있다. DLT 플랫폼에는 사용자 인증 모듈과 사용자 액세스 제어 관리 모듈이 있어야 하며, 전자 서명은 사용자를 효과적으로 인증하는 방법이고, 그 플랫폼은 사용자의 액세스를 인증하고 제어할 수 있는 스마트 컨트랙트 생성을 허용할 수 있어야 한다. 스마트 컨트랙트 데이터 액세스 제어는 스마트 컨트랙트 데이터가 스마트 컨트랙트 참가자들이 공유하도록 모든 관련 참가자가 이 정보에 액세스하도록 하는 것이다.

시스템 안정성측면에서 플랫폼은 최소한의 노드 관리 안정성, 교차 체인 운영의 안정성, 네트워크 대기 시간, 메모리 사용률, CPU 사용률, 동시성 안정성의 요구사항을 충족해야 한다. 일부 노드는 가입, 탈퇴 또는 업그레이드 시 시스템에 정상적인 작동을 허용하는 노드 관리 안정성, 시스템이 다른 DLT 시스템 또는 클라우드 시스템과 협력 시 정상적인 운영을 허용하는 교차 체인 운영의 안정성을 보장해야 한다. 네트워크 대기 시간, 네트워크 대기 시간, 메모리 사용률, CPU 사용률은 7×24 시간을 실행한 후에도 시스템이 안정적으로 유지해야 하고, 동시 트랜잭션이 급증하더라도 시스템은 안정적으로 유지되어야 한다.

경제 메커니즘 설계는 블록체인 플랫폼 경제와 블록체인 시스템에서 생산되는 토큰에 중점을 두는 것으로 사용자 참여를 장려하는 경제 메커니즘이 있어야 한다. 여기에는 합의 프로토콜, 해결 메커니즘, 투표 프로토콜, 할당 메커니즘, 협상 프로토콜, 토큰의 통화 정책, 거래 수수료가 포함되지만 이에 국한되지는 않는다.

프라이버시는 DLT 플랫폼 핵심 요구사항으로, 시스템에서 비밀 데이터의 생성, 저장과 전송을 말하며, 특히 사용자 개인정보는 안전하게 저장되어야 한다. 기밀 또는 독점 정보는 보안채널을 통해 전송되어야 하며, 지정된 보안 전송 프로토콜을 통해 얻어야 한다. 법률 또는 정책으로 보호되는 모든 기밀 또는 개인 정보는 보관 또는 운송 중에 적절한 수준의 차등 액세스 제어와 정보보호가 필요하다. DLT 플랫폼은 영 지식 증명, 링 서명, 안전한 다자 간 계산과 동종 암호화와 같은 개인정보보호 알고리즘을 사용하여 개인정보 공개를 피할 수 있다.

DLT 플랫폼은 사용자 친화성 향상을 위한 응용 프로그램 지원 기능을 구현하는데, 쿼리용 사용자 인터페이스, 스마트 컨트랙트를 위한 사용자 인터페이스와 다국어 소프트웨어 개발 키트가 포함된다.

3. 운영 기능

DLT 시스템은 DDoS 공격, Sybil 공격 또는 부정직한 노드에 저항할 수 있어야 하며, 공격이 실패하면 시스템을 이전의 알려진 상태로 복구할 수 있는 위험 관리와 완화가 필요하다. DLT 시스템은 복구, 보안 서비스 등을 다운그레이드하여 장애로부터 복구할 수 있어야 하며, 복구 솔루션은 유연하고 문제 지향적이어야 한다.

DLT 시스템은 단지 추가 전용의 신뢰 원장이므로 그 시스템에 저장된 대량 데이터는 쿼리 성능을 저하시킬 수 있다. 더 이상 적극적으로 사용되지

않는 데이터를 장기 보존을 위해, 특히 권한이 부여된 DLT 시스템의 경우 별도의 저장 장치로 이동해야 한다.

4. 성능

초당 트랜잭션(TPS: Transactions per Second)은 DLT의 표준 성능지표로서 시스템 부팅 또는 종료와 테스트 환경 불안정으로 인해 부정확성이 발생할 수 있으므로 시스템이 안정적일 때 TPS를 측정해야 한다.

$$\text{TPS} = \frac{\text{number of processed transactions}}{\text{time used process transactions}}$$

$$\text{MTD(max transaction delay)} = \max(\text{transaction confirmed tim} - \text{transaction commited time})$$

$$\text{ATD(average transaction delay)} = \frac{\sum(\text{transaction confirmed time} - \text{transaction commited time})}{\text{number of transactions}}$$

성능평가 전제 조건은 테스트 환경, 네트워크 토폴로지, 테스트 시스템 배치, 트랜잭션, 테스트 도구이다. 성능 평가 시 CPU, 메모리, 하드 디스크, 네트워크 등 하드웨어, 네트워크 토폴로지, 테스트 시스템 전개 유형과 트랜잭션 수를 표시해야 한다. 테스트 도구로는 Hyperleder Caliper, Trusted-Bench 등 특별히 설계된 오픈소스 도구가 있다. 스크립트를 사용하여 성능 테스트를 할 수도 있다.

5. 생태계

DLT 생태계 평가 기준에는 플랫폼 성숙도, 오픈소스, 전문가 가용성, DLT 시스템의 운영비용 그리고 벤더 락인 방지가 있다.

DLT 플랫폼 성숙도에는 제작 연도, 프로덕션 버전 출시, 네트워크 배포(메인 넷과 테스트 넷), 프로덕션 네트워크 수, 응용 프로그램 수와 팀 전문지식과 같은 많은 요소가 포함되며, 공급업체는 이 정보를 모든 소비자에게 공개해야 한다. DLT 플랫폼은 그 사용자에게 오픈 소스가 되므로 사용 중인 라이선스 또한 알려야 한다.

DLT 플랫폼은 개인, 회사 또는 비영리 조직에 의해 잘 유지·관리되어야 하므로 소스 리포지토리에 대한 정기적인 업데이트, 플랫폼 관련 커뮤니티의 활발한 토론, 분산된 응용 프로그램과 DAO 플랫폼 업데이트 용이성이 포함된다. DLT 플랫폼별 복합적인 기술적 배경이 필요하다는 것은 시장에서 가용한 전문가 수를 간접적으로 제한하므로 충분한 인재 공급 가능성은 DLT 플랫폼 평가에 중요한 요소이다.

DLT 시스템의 운영 비용 평가는 필수적인 요소로, 지불 수수료, 거래 확인 시간과 서면 비용, 스마트 컨트랙트를 읽고 실행하는 비용이 포함된다. 앞으로 스마트 컨트랙트 보안이 중요하므로 스마트 컨트랙트 감사, 코드 검토와 기타 많은 중간 수수료도 고려해야 한다.

DLT 시스템은 서비스 액세스, 데이터 사전, 통신 프로토콜, 암호화 알고리즘 및 시스템 테스트의 표준화된 API가 있어야 고객이 벤더 락인을 피할 수 있고, 유사한 서비스를 제공하는 여러 공급업체가 있어야 한다.

VI. 분산원장기술 전망

DLT 전망으로 거버넌스와 법적 규제, 계산 네트워크, 아이덴티티와 프라이버시, 정보보호와 복원성 그리고 위험과 감사가 포함되어 있으나[8], 여기서는 계산 네트워크, 아이덴티티와 프라이버시, 정보보호와 복원성만 서술하였다.

1. 계산 네트워크

가. 연결성 능력과 고가용성

현 네트워크 연결성은 분산 비구조화된 토폴로지(비트코인), 분산 구조화된 토폴로지(ETH), 그리고 부분적 분산 토폴로지(패브릭)로 구분된다.

분산 네트워크는 확장성과 유연성 면에서 중앙 네트워크보다 성능이 뛰어나므로 대규모 통신 시나리오에 효과적인 접근 방식이지만, 실제는 더 많은 노드는 더 많은 사본을 의미하므로 네트워크 속도가 느려지게 된다. 분산 네트워크는 로컬 정보를 기반으로 실시간으로 성능과 안정성을 최적화할 수 없으므로 연결 능력과 가용성 성능에 영향을 준다. 반면 중앙집중식 네트워크는 완전한 정보를 사용하여 연결 능력과 고 가용성 모두를 향상시킬 수 있다. 하이브리드 네트워크 아키텍처는 네트워크 성능, 확장성과 유연성 간 균형을 유지할 수 있다. 현재 산업체와 커뮤니티에서는 지연시간을 줄이고 처리량을 높이는 블록체인 스케일링 방법 설계에 전념하고 있다. 연결성 측면에서 고도화된 네트워킹은 비효율적인 DLT 운영 모델을 변화시킬 수 있는 연결을 제공해야 한다. 확장성 관점에서, 중앙 집중화와 탈중앙화 사이의 균형을 이루는 하이브리드 체계가 가까운 시일 내에 더욱 실용적일 수 있다. 확장성 관점에서 중앙집중식 시스템 간 인터페이스 표준화를 하는 것이 성능과 상호운용성 간 균형을 유지하는 방법인지 검토가 필요하다.

나. 프로그램 가능성과 스마트 컨트랙트

스마트 컨트랙트는 여전히 기능이 제한되어 있어서 실용적 사용에는 불충분하지만, 프로그래밍 가능성과 효율성, 의존성, 계층적, 결함 수정 메커니즘, 수명 주기와 진화 향상 방법론 개발에 재원이 투자되고 있다. 가상머신의 개선으로 DLT 프로그래밍 가능성이 발전되고 있고, 그 중 하나가 WebAssembly(Wasm)이다. 일부 DLT 그룹은 Ethereum의 eWasm 프로젝트와 EOS 플랫폼과 같이 적응 가능한 버전의 Wasm을 지원하는 프로젝트를 실행하고 있다.

기존 기술에서 얻은 교훈을 고려하여 DLT 플랫폼을 대상으로 프로그래밍 언어가 개발되고 있다. Vyper는 이더리움 플랫폼(2018년 6월 베타 테스트)의 새로운 언어로 보안, 사람이 읽을 수 있는 코드, 언어와 컴파일러 단순성 제공에 중점을 두고 있다. Simplicity는 가상 시스템의 리소스 사용량을 분석하는 결합기 기반의 저 수준 언어이고, Ergo는 플랫폼에 독립적 의미가 있는 기능 언어로서 Simplicity와 마찬가지로 반복에 대한 제한을 부과하고 컨트랙트 실행의 종료를 보장한다. 2016년 Hyperledger Fabric의 초기 릴리스를 위해 Linux Foundation은 블록체인 플랫폼의 스마트 컨트랙트 Golang을 구현해서 Google은 빠르고 배우기 쉽고 정형화된 언어를 활용했다.

다. 원장 데이터 구조

DLT는 상태(이진 문자열)에 대한 신뢰할 수 없는 노드 그룹과 해당 상태로의 전환에 대해 합의를 달성하는 것을 목표로 한다. 즉 초기 상태 유효성, 악의적 행위자와 비잔틴 노드에 직면한 상태 전환의 합의, 악의적 행위자와 비잔틴 노드에 직면하여 유효한 전환을 수행하는 능력과 참가자의 상태와 전환 정보 제공에 대한 상태와 거래에 대한 유효성 규칙을 충족시켜야 한다. 이를 구현하기 위해 원장 데이터 구조에는 상태 정보, 포함된 유효한 전환 정보, 트랜잭션, 상태와 전환에 대한 합의를 결정하는 합의 알고리즘에 따른 정보가 포함된다.

다양한 원장 데이터 구조가 구현되고 있는데, 합의 알고리즘, 상태, 유효성 규칙과 원장 데이터 구

조 사이의 긴밀한 결합으로 원장 데이터 구조를 합의 알고리즘과 혼합하여 일치시킬 수는 없으나, 일부 합의 알고리즘 제품은 유사한 원장 데이터 구조를 공유하며 상호 교환적으로 사용한다.

스토리지 크기와 증가, 전환을 위한 가용성 요구사항, 오더링 강도, 초기 부트스트랩 비용을 사용하여 원장 데이터 구조를 비교하면 특정 유즈 케이스에 적합 여부를 확인할 수 있다.

최근 몇몇 DLT는 폭발적으로 발전했지만 실제 응용에서 고객들은 그들의 특정 요구사항을 충족하고, 혁신과 제어 비용을 촉진하기 위해 벤더와 기술 선택을 여전히 원한다. 다양한 컨소시엄에 참여 조직들은 주기적으로 DLT 간 상호운용성을 요구하므로, 이 방향에서 혁신이 나타날 것이다. 체인 기술 간(및 체인 인스턴스) 상호운용성이 현실화될 때 표준화가 나타날 것이다.

2. 아이덴티티와 프라이버시

가. 아이덴티티와 고객 파악

일상생활에서 기하급수적인 디지털화와 그 영향을 고려하면 아이덴티티와 프라이버시는 개인의 프라이버시와 기밀성에 대한 자율적 통제를 확보하기 위해 중요한 주제이다. 기존 연구로는 2014년 9월 17일에 발효된 EU 규정으로 유럽 단일 시장에서 전자 거래를 위한 최초의 중요한 전자 식별 및 신뢰 서비스 표준인 eIDAS, NIST 보고서[발급(신임 관리) 및 신원 인증], 미국 연방준비은행 보고서(지불에 있어서 합성 신원 사기 위험)가 있다.

레거시 트러스트 모델이 계속될 것이고, 다양한 DLT기반 트러스트 프레임워크가 등장하면, 이 이질적인 시스템의 인접성으로 발생되는 신뢰 등 문제 해소 혹은 격차를 줄이기 위해 상호 호환성, 투명성, 자율, 종단 간 원칙에 초점을 둘 것을 권고한다. 스마트폰 소유자는 쉬운 유지 관리, 효과적 사이버 보안을 달성하기 위해 자체 에이전시를 입증·보호할 수 있는 도구가 필요하다.

이를 위한 새로운 계산 도구는 엔티티의 식별 가능한 특성으로 구성되는 클레임에 대한 자연인의 정확성 입증, 정보 및/또는 화폐 자산의 이전, 저장과 검색에 영향을 미치는 프로세스를 활성화하려는 자연인 의도, 정보 및/또는 화폐 자산의 전송, 저장과 검색에 영향을 미치는 프로세스에서 해석 가능한 변수 사용 등을 위해 자율적 유효성 증명을 해야 한다.

나. 프라이버시를 위한 데이터 스토리지 체계, 최소화

DLT 시스템은 다양한 사용자 커뮤니티의 다양한 요구를 충족하도록 발전할 것인데, 현 모범 사례로 오프 체인 메커니즘, 사이드 체인, 영 지식증명 등이 있다.

충분한 시장력을 가진 민첩한 기업은 데이터 최소화와 사용 제한에 대해 전 세계적으로 일관된 규칙 도입을 준비하고 있다. 11,000개의 개별적으로 관리되는 서브넷에 분산된 데이터 소유자를 보호하는 새로운 정책 적용 지점의 설계 구조를 개발 중에 있다.

오프 체인과 사이드 체인 메커니즘 모두 계속 블록체인 기술이 발전하고, 이 영역에서 표준화가 거의 없는 것으로 보이므로 상호운용 가능한 솔루션을 조장하는 ITU-T 권고를 필요로 한다.

3. 정보보호와 복원성

가. 상황 스탬프

DLT 출현으로 분산적이고 변조방지 방법으로 정보를 안전하게 타임스탬프할 수 있게 되었다. 분

산 타임스탬프는 데이터를 해시하고, 해시를 DLT에 저장된 트랜잭션에 통합할 수 있으며, 이 데이터는 해당 데이터가 존재한 정확한 시간을 안전하게 증명하는 역할을 한다. 미래에는 타임스탬프와 위치 스탬프 간 연결이 필요할 수 있다. 공급망에서 시간과 공간에 물품이 어디에 있는지, 언제 있는지를 DLT기반 저장소에 저장할 수 있다.

블록체인에서, 블록 데이터의 타임스탬프는 로컬 시스템 클록 또는 신뢰할 수 있는 TSA(Time Stamp Authority)에 의해 유지되는 교정된 클록에서 얻는다. 신뢰할 수 있는 타임스탬프는 블록 시퀀스의 유효성을 보다 확실하게 보장한다. TSA 시간은 ISO/IEC 18014 표준의 프로파일 기반인 ITU-T 권고를 활용하면 된다.

나. 합의

지금까지 많은 합의 체계가 제안되어 왔으나, 추가 분석을 위해 정보보호 메트릭과 성능 메트릭으로 구분되어 연구되어 왔다. 정보보호 메트릭은 일관성, 트랜잭션 검열 저항성, 그리고 DDoS 저항성, 성능 메트릭으로는 처리량, 확장성과 지연이다.

DLT를 채택하기 전에 극복할 주요 장애물은 성능, 확장성과 정보보호인데, 개선되었지만 기대 수준에는 미치지 못하고 있다. 이는 블록체인의 핵심 요소인 합의 프로토콜과 깊은 관련이 있으므로 향후 연구가 필요하다. 합의에 대한 정보보호 수준은 다양한 합의 체계 및 관련 정보보호 프로파일을 기반으로 정의된다.

다. 프로그램 가능성의 복원성

시스템 복원력, 공식 검증과 스마트 컨트랙트 테스트 도구를 포함한 방법론을 보장하기 위해 프로그래밍 가능성 복원력이 중요하다.

프로그램 속성을 수학적으로 증명하여 정보보호를 향상시키기 위해 공식 검증 기술이 도입되었다. 이 기술은 분산원장 시스템의 스크립트와 스마트 컨트랙트에 특히 유용하다. 안전한 스마트 컨트랙트 스크립팅을 위한 방법론으로 시스템 설계와 의도된 동작을 모델링하는 프로세스로 Solidity 스마트 컨트랙트를 NuSMV 입력 언어로 변환하기 위한 규칙을 도출하는 것이다. 보다 복잡한 스마트 컨트랙트의 경우 온톨로지와 규칙을 사용하여 가능성을 포착하고 바람직한 행동을 시행하는 것이다. 자율적 환경에 의해 악화된 취약점뿐만 아니라 스마트 컨트랙트 편재성을 인정하고, 이에 대해 스마트 컨트랙트 코드가 전통적인 스크립팅 언어를 넘어 공식적인 논리 대신 고려되는 공식적인 검증을 하는 방법이다. Corda는 실제 시나리오 이후의 트랜잭션을 모델링하는 방법을 제안하였다.

최근 몇 년 동안 Bitcoin과 Ethereum 네트워크에서 많은 계정이 해킹되었다. 대부분은 해커가 잘못 작성된 스마트 컨트랙트 코드 내 허점을 이용했다. Hyperledger Fabric에서 범용 언어로 작성된 스마트 컨트랙트는 튜링 완벽하지만, 반복 메커니즘과 비결정적 실행으로 인해 DoS 및 DoS 공격의 변형에 취약하다. 유연성과 탄력성의 균형은 곧 업계에서 중요해지므로 유연성 기능 개선 노력과 탄력성을 강화 연구가 촉발될 것이다.

약어 정리

AAA	Accounting, Authorization and Authentication
DAO	Distributed Autonomous Organization
eIDAS	electronic IDentification, Authentication and trust Services
FG-DLT	Focus Group on application of Distributed Ledger Technology

NIST	National Institute on Science and Technology
TSA	Time Stamp Authority
W3C	World Wide Web Consortium

참고문헌

[1] ITU-T FG-DLT-D1.1 Distributed ledger technology terms and definitions, 1 Aug. 2019.

[2] ITU-T FG-DLT-D1.2 Distributed ledger technology overview concepts ecosystem, 1 Aug. 2019.

[3] ITU-T FG-DLT-D1.3 Distributed ledger technology standardization landscape, 1 Aug. 2019.

[4] U-T FG-DLT-D2.1 Distributed ledger technology use cases, 1 Aug. 2019.

[5] ITU-T FG-DLT-D3.1 Distributed ledger technology reference architecture, 1 Aug. 2019.

[6] T FG-DLT-D3.3 Assessment criteria for distributed ledger technology platforms, 1 Aug. 2019.

[7] ITU-T FG-DLT-D4.1 Distributed ledger technology regulatory framework, 1 Aug. 2019.

[8] T FG-DLT-D5.1 outlook on Distributed ledger technologies, 1 Aug. 2019.