블록체인

블록체인 기술은 일찍이 없었던 방식으로 디지털 기술을 경제와 접목시키고 있다. 블록체인은 금융서비스를 제공하기 위한 새로운 수단을 가능케 했을 뿐만 아니라 정부, 법적 서비스, 책임성, 공급망 및 에너지 분배를 재정의하고 있다.[1] 블록체인은 중개자 없이 네트워크를 통해 거래 기록을 변경 없이 유지할 수 있게끔 함으로써 협력과 공유를 통한 디지털 자산 서비스를 제공한다. 즉 개인 간에 자산과 에너지 등을 더 유연하게, 더 적은 수수료로 거래할 수 있는 시장을 형성할 수 있게 해주며, 자산의 유래를 투명하게 공유함으로써 문제의 소재를 더 빠르고 정확하게 확인하게 해준다. 이러한 변화는 법이 적용되는 방식, 정부가 경제와 정책 프레임워크를 관리하고 시민에게 서비스를 제공하는 방식, 그리고 시민권의 작동 방식에 근본적인 영향을 미칠 것이며, 사회적 신뢰를 재정의하게 될 것이다.

이 전세계적인 인프라가 구성, 운영되기 위해서 표준화는 필수적인 요건이다. 아직 블록체인이라는 용어 자체도 정확한 정의가 합의되지 못한 상태다. 블록체인 기술이 지역과 국제 공급망을 연결하고 다양한 응용들을 상호 연계하기 위해서는 기본적인 참조 모델과 이에 기반한 기술적, 정책적 연동표준이 필요하다. 2017년부터 ISO와 ITU-T를 중심으로 국제 표준화가 빠르게 진행되고 있다. 본 특집이 현재의 동향을 공유하고 향후의 방향을 수립하는데 작은 도움이 되기를 바란다.

1) World Economic Forum, Blockchain 4th industrial revolution Summary, https://toplink.weforum.org/knowledge/insight/a1Gb00000038qmPEAQ/explore/summary

오경희 ITU-T SG 17 Q14 DLT 보안 라포처
TCA서비스 대표

블록체인에 대한 개념을 설명해 주신다면...

블록체인은 분산원장을 생성하고 유지하기 위한 기술 중의 하나입니다. 분산원장은 네트워크상의 노드들이 공유하는 원장입니다. 블록체인에서 원장의 레코드는 블록으로 구성됩니다. 이용자들이 트랜잭션을 생성하여 노드에 기록을 요청하면 노드들은 트랜잭션을 검증하고, 여러 트랜잭션들을 모아 일정 크기의 블록으로 만들고 이전 블록의 해시값을 새로 만든 블록의 헤더에 기록하여 연결하는 방식으로 분산원장에 새로운 레코드를 추가합니다. 이런 구조에서는 과거의 블록 내용을 수정하게 되면 해시값이 변경되므로 연결이 끊어지게 됩니다. 그래서 과거의 블록을 수정하지 못하고 새로운 블록을 덧붙이는 방식으로만 원장을 유지하게 됩니다.

노드가 새로운 블록을 생성하게 되면 다른 노드들에게 이 블록을 네트워크를 통해 공유합니다. 새로운 블록이 전달되면 각 노드들은 이를 검증하고 합의 알고리즘에 따라 채택하거나 기각합니다. 일반적으로 알려진 것은 더 길이가 긴 체인을 더 많은 작업량이 이루어진 것으로 간주하여 채택하는 작업 검증(PoW, Proof of Work) 방식이지만 지분 방식 등 다른 합의 알고리즘도 있습니다. 어떤 합의 알고리즘을 채택하느냐에 따라 해당 블록체인이 가지는 특성들이 달라질 수 있습니다. 이러한 과정을 통해서 네트워크상의 모든 노드들이 일련의 블록들의 연결로 이루어진 하나의 원장을 합의된 방식으로 공유하는 것이 블록체인입니다.

그러나 블록체인 형태뿐 아니라 트리 형태 등의 다양한 방식으로 트랜잭션들을 연결해서 관리할 수 있습니다. 대표적인 것이 R3 Corda나 IOTA입니다. 이런 기술을 블록체인이라고 부르는 것은 적절치 않기 때문에, 형태에 국한되지 않는 더 포괄적인 용어로 채택된 것이 '분산원장기술(DLT, Distributed Ledger Technology)'입니다. 해시, 전자서명 등 암호기술을 사용하여 네트워크 노드들상에 분산된 원장 데이터를 최종적이고 변경이 어려운 방식으로 유지하는 기술입니다. 그런데 아직은 분산원장기술이라고 하면 잘 모르시는 분들이 많습니다. 한 때 '제록스'가 '복사기'라는 뜻으로 통용된 시절이 있었는데 지금 블록체인이 그렇달까요.

블록체인 기술이 최근 주목받는 이유가 무엇인지...

P2P는 통신 프로토콜이지 그 통신으로 주고 받는 데이터를 통제하지는 않습니다. 그러나 분산원장기술은 P2P 통신 프로토콜을 이용하지만 이 네트워크에 참가하는 노드들이 하나의 가상원장을 유지하게끔 하는 기술입니다. 또한 블록체인 형태로 시작되긴 했지만 더 다양한 형태의 분산원장기술이 개발되었듯이 분산원장기술이 P2P 기술을 이용하여 시작되기는 했지만 이제는 반드시 P2P상에서 운영되어야 하는 것은 아닙니다. 브로드캐스트 등의 통신 방식을 사용한다고 해서 분산원장시스템이 아니라고 말할 수는 없습니다.

분산 DB의 경우 물리적인 저장소는 분산되어 있지만 DB의 통제는 중앙집중화되어 있습니다. 즉 어떤 데이터를 추가할 것인지 말 것인지, 데이터를 어디에 어느 정도로 중복하여 저장할 것인지를 한 곳에서 결정합니다. 그러나 분산원장기술에서는 데이터 추가의 결정을 모든 노드들이 정해진 알고리즘에 따라 각자 수행합니다. 그래서 가장 최근의 원장 데이터는 노드들마다 다를 수 있습니다. 그러나 통신을 통해 다른 노드들의 정보를 얻으면서 동일한 원칙의 알고리즘에 따라 원장 데이터를 조정하기 때문에 일정 시간이 지난 데이터들은 모든 노드들이 일관성 있는 하나의 가상원장을 유지하게 됩니다.

중앙의 중개자 없이 네트워크상에서 변경되지 않는 동일한 합의된 원장을 유지할 수 있다는 것이 핵심 장점이라고 봅니다. 기존의 분산 모델에서는 모든 노드가 동일한 기록을 변경 없이 유지한다는 보장을 받기 어려웠고 이를 위해 모든 노드가 신뢰할 수 있는 중개자를 수립하고 유지하기 위한 비용이 높았습니다. 분산원장기술은 해시, 전자서명 등의 암호와 컨센서스 알고리즘에 기초하여 기존의 조직에 대한 신뢰를 기술에 대한 신뢰로 대체하였습니다. 이는 특히 상호신뢰가 어려운 상황에서 큰 장점이 됩니다.

블록체인 기술의 국내외 표준화 현황 및 시험인증기술을 말씀해 주신다면...

대표적인 국제 표준화 기구로서 ISO TC 307, ITU-T SG 17에서 분산원장기술 관련 표준화를 진행하고 있습니다. ISO TC 307 '블록체인 및 분산원장기술'에서는 분산원장기술 전반에 걸쳐 표준화를 진행하고 있고, ITU-T SG 17에서는 분산원장기술의 보안측면에 초점을 맞춘 연구가 진행되고 있습니다. 그 외에도 IEEE나 W3C에서도 작업이 이루어지고 있습니다. 상세한 내용은 〈표 1〉을 참조해 주시기 바랍니다.

국내에서는 TTA의 PG 502에서 블록체인 보안 관련 단체표준을 개발하고 있고, 금융보안연구원의 블록체인분과에서 금융권 블록체인을 위한 표준을 개발하고 있습니다. 작년에는 개인정보보호포럼이나 사물인터넷포럼에서 블록체인 관련 표준을 개발한 바 있고, 올해 시작한 분산원장기술표준포럼도 이런 국내 여러 기구 및 포럼과 연계하여 용어, 활용사례, 플랫폼 표준 등을 개발하고 있습니다.

<표 1> 국제 표준화기구 분산원장기술 표준화 현황

개발기구	표준	비고
ISO TC 307	• ISO 22739 Terminology • ISO 23257 Reference architecture • TR 23258 Taxonomy and ontology • TR Discovery issues related to interoperability • Study on "Data flow and data taxonomy for blockchain and distributed ledger technologies"	WG 01: Foundations
	• TR Use cases	SG 02: Use cases
	• TR 23245 Security risks and vulnerabilities • TR Security of digital asset custodians • Study on "Security evaluation of consensus models"	WG 02: Security, Privacy and Identity
	• TS 23259 Legally binding smart contracts • TR 23455 Overview of and interactions between smart contracts	WG 03: Smart contract and their applications
	• TS Guidelines for governance	SG 06: Governance
	• Interoperability issues related to cryptocurrencies' platform, utility and transaction tokens and other cryptographically supported digital assets or proxies for physical and intangible assets	SG 07: Interoperability
	• TR 23244 Overview of privacy and personally identifiable information (PII) protection • TR 23246 Overview of identity management using blockchain and DLT	Joint working group with ISO/IEC JTC1 SC27
ISO TC 215	• NP 22228 Healthcare applications of Blockchain technologies	
ITU-T SG 17	• X.dltsec Privacy and security considerations for using DLT data in identity management • X.sct-dlt Security capabilities and threats of DLT • X.sradlt Security framework for DLT • X.sadlt Security assurance for DLT • X.strdlt Security threats and requirements for digital payment services based on DLT • X.stov Security threats to online voting using DLT • X.ss-dlt Security services based on DLT • X.das-mat Security framework for the data access and sharing management system based on DLT • X.tf-spd-dlt Technical framework for secure software distribution mechanism	Q14 Security aspects for DLT
ITU-T SG 13	• Y.NGNe-BC-reqts Scenarios and capability requirements of blockchain in next generation network evolution • Y.BaaS-reqts Cloud computing - Functional requirements for blockchain as a service	
ITU-T SG 16	• F.DLS Requirements and capabilities of decentralized ledger services	
ITU-T SG 20	• Y.IoT-BoT-fw Framework of blockchain of things as decentralized service platform	
IEEE	• Standard for the framework of blockchain use in Internet of Things	blockchain wg
W3C	• Verifiable claims use cases	

우리가 주목해야 하는 표준이나 핵심원천 기술은 무엇이 있는지...

현재는 표준화가 막 시작된 단계라 아직 용어나 참조구조가 확정되지 않은 상태여서 이런 것들이 이슈가 되고 있습니다만 곧 플랫폼이나 서비스 간의 상호운용을 위한 표준들이 시작되면 이런 것들이 실제 기술을 구현하고 시장을 넓히기 위해 중요한 요소가 될 것입니다. 국내에서도 ETRI 등에서 연구가 진행되고 있는 것으로 알고 있습니다.

상업적으로는 암호화폐가 먼저 이루어졌지만 표준 분야에서는 암호화폐 관련 표준의 연구가 이제 시작되려고 하고 있습니다. ITU-T 산하의 FG-DFC는 법정화폐를 포함하는 암호화폐 플랫폼, 관련 법규제, 보안 등에 대해 표준화 선행 연구를 수행하고 있고, TC 307에서는 디지털 자산 관리자의 보안에 대한 기술보고서 개발을 개시하기로 하였습니다. 암호화폐 거래소가 자산 관리자의 예가 될 수 있습니다.

한편 기술 관련 특허도 매우 빠르게 출원, 등록되고 있습니다. 블록체인의 기본 개념은 오픈 소스로 공개되어 있지만 보안, 운용, 활용 등에 관련된 기술 특허가 이루어지고 있습니다. 블록체인 기술 관련 특허는 2013년부터 시작되어 2016년까지 총 1200여 건의 특허가 출원되었다고 알려져 있는데 미공개 건이나 '블록체인'이라는 용어를 사용하지 않은 특허까지 생각하면 실제 관련 특허는 더 많을 것이고, 앞으로 물류, 의료, 공공 서비스 등 활용 분야가 넓어지면서 더 많은 특허가 쏟아질 것으로 예상됩니다. 미국, 중국이 대부분이지만 국내에서도 많은 특허가 출원되고 있습니다. 특허 기술이 표준에 반영되면 시장 확보에 큰 도움이 될 것입니다.

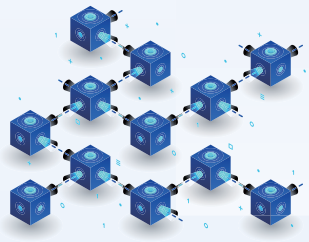
국가별 상용화 추세 및 사례 등을 소개해 주신다면...

전 세계가 다 분산원장기술에 뛰어들고 있어서 일일이 말씀드리기가 어려울 정도입니다. 어느 국가가 특별히 뭘 하고 있다기보다는 전반적으로 거의 모든 분야에 걸쳐 사례를 개발하고 있습니다. 아직은 상용화로 성공했다고 할 만한 사례는 일부 암호화폐 정도지만 엄청난 자원이 투자되고 다양한 상용화 노력이 이루어지고 있습니다.

최근의 사례로는 유럽 22개국이 유럽 블록체인 파트너십을 수립하고 전 유럽에 걸친 블록체인 시스템을 만들기 위한 준비를 하고 있습니다. EC의 디지털 경제 사회 위원장은 앞으로 모든 공공서비스는 블록체인 기술을 사용할 것이라고 공언한 바 있습니다. EC는 블록체인 관련 프로젝트에 이미 8천만 유로를 투자했고 향후 3억 유로를 추가 지출할 예정입니다. 이에 관련하여 건강증진을 위한 MHMD와 개인정보보호를 위한 DECODE가 이미 수립되어 진행되고 있습니다.

국내에서도 국제간 송금 등 금융권에서 이미 다양한 사업들을 시작했고 커뮤니티 전자투표시스템, 지역 화폐 등의 시범사업이 이루어졌습니다. 올해는 국가 주도로 부동산종합공부시스템에 기반한 스마트 거래, 축산물 이력관리시스템, 전자투표시스템, 아포스티유 블록체인 등의 시범사업 등을 진행하고 있으며, 의료기록 보관 등 민간 쪽에서도 사례들이 개발되고 있습니다.

이렇게 다양한 활용사례들이 나타나고 있습니다만 분산원장기술이 만능은 아니기 때문에 때로는 굳이 분산원장을 사용할 필요가 없는 경우에도 어떤 시스템을 블록체인으로 개발했다고 마케팅을 하는 경우가 가끔 있는 것 같습니다. 앞서도 말씀드렸지만 분산원장기술이 강점을 갖는 경우는 당사자간의 신뢰에 대한 이슈가 있고 거래의 투명성 및 변경되지 않는 이력 기록이 필요한 경우입니다. 중앙의 관리기관에 대한 신뢰를 유지하는 경우 기록을 분산 검증하고 분산 저장하기 위한 부가적 자원 소모를 정당화하기는 매우 어렵습니다. 실제 상업적 성공에 이르기까지는 시행착오 기간이 좀 걸릴 것으로 예상됩니다.



블록체인 구현을 통해 새로 창출될 비즈니스나 우리가 경험하게 될 서비스에 대해 말씀해 주신다면...

분산원장기술은 인프라이기 때문에 완전히 새로운 서비스라기보다는 기존의 비즈니스를 더 빠르고 더 적은 비용으로 달성하게 되는 부분이 클 것입니다. 스마트 컨트랙트를 이용한 좀 더 다양화된 서비스를 제공받거나, 좀 더 다양한 의사결정 알고리즘이 활용될 수 있을 것입니다. 많은 새로운 서비스들은 블록체인만으로 가능한 것이라기보다는 IoT나 인공지능과 같이 병행 발전하는 IT 기술과 융합되면서 나타납니다. 이런 것들이 블록체인이라는 공통 인프라 위에서 통합되면서 서비스 간 연계가 더 빠르게 이루어짐으로써 사람이 할 일을 현저하게 줄여 줄 수 있을 것입니다.

현재 중점적으로 연구되고 있는 분야 중 하나는 공급망인데요, 고립적으로 이루어졌던 업무들이 다양한 조건에 맞추어 자동으로 진행될 수 있습니다. 예를 들어 고객이 제품을 주문하면 설계자가 설계를 하고, 설계가 승인되면 부품 및 서비스 주문이 자동으로 이루어지고 공장으로 배송되어 단계별 작업이 이루어지고, 결과물의 포장과 배송이 진행되어 주문자에게 배달됩니다. 이런 전 과정이 블록체인에 기록되면서 사용자는 자신의 주문이 지금 설계 중인지 배송 중인지 확인이 되고 이 과정에서 유지되어야 할 조건들이 만족되고 있는지 등을 확인할 수 있습니다. 예를 들어 유기농 라텍스 매트리스가 깔린 아기 침대를 주문했다면 그 매트리스 제조사가 어디이고 유통과정에서 오염이나 낙후를 방지하기 위한 조치가 제대로 취해졌는지 등이 블록체인에 기록되고 관세처리, 인수 승인에 따른 지불 및 기록 등이 자동으로 이루어져서 실시간 확인이 가능한 시스템을 구현할 수 있을 것으로 기대되고 있습니다.

한편 비트코인이 투기로 인해 문제가 되었듯이 이러한 기술을 사회가 어떻게 받아들이느냐에 따라 달라지는 점들이 있을 것입니다. 일반적으로 국제무역에서는 인수 후에도 일정 기간을 두고 지불을 하는데 이들은 블록체인이 즉각적인 자동화된 지불을 가능하게 하더라도 기존의 관행을 유지하고 싶어 할 것입니다. 한편 공급망의 말단 소규모 공급자들은 이런 체계에 편입되기 위해 현재보다 더 많은 요구를 만족시켜야 할 경우가 생길 수 있고, 스마트 컨트랙트를 이용해서 더 빠르게 인수에 따른 송금이 가능하기는 하지만 반드시 그렇게 구현될 것이라고 보장할 수는 없습니다. UN에서는 분산원장기술이 가져오게 될 변화가 지속가능한 성장이라는 의제에 어떤 영향을 미치게 될 지에 대해서도 관심을 가지고 있습니다. 분산원장기술이 서비스를 빠르고 더 적은 비용으로 제공해주기는 하겠지만, 그만큼 그전에 사람이 해야 했던 일을 줄이게 되고 이는 일자리 감소로 나타날 수 있습니다.

국내 블록체인 시장 활성화와 세계 시장 선점을 위해 선결되어야 할 점이 있다면...

현재까지의 국내 플랫폼은 특정 사례를 위한 기능 제공을 목표로 시스템이 개발된 경우가 많아 확장이나 상호운용에 어려움이 있습니다. 일반적인 플랫폼상에서 API를 통해 응용을 구현하는 형태로 진화하고 있으므로 확장 측면에서의 기술적인 어려움은 차츰 해결될 것으로 전망됩니다. 한편 규제나 기준이 중앙집중화된 시스템을 가정하고 만들어져 분산시스템에 적용할 수 없어서 만족할 수 없는 경우 등이 있습니다. 이런 측면에서의 개선도 필요합니다.

한편 세계시장 진출을 위해서는 상호운용을 위한 표준 작업에 좀 더 유의할 필요가 있습니다. 분산원장기술은 전세계를 연결하는 인프라가 될 것이며 국지적 블록체인들이 국가 또는 국제 블록체인들과 연결되면서 연동되는 형태가 될텐데 이 때 표준의 만족 여부가 관건이 될 것입니다. 표준이 개발되고 난 뒤 대응하기 보다는 적극적으로 표준화 과정에 참여하면서 좀 더 나은 표준이 만들어 질 수 있도록 영향을 미칠 필요가 있습니다. 국제 표준을 만족시키기 위한 기술을 개발하면서 특허까지 취득할 수 있다면 세계 시장 선점에 매우 유리할 것입니다.

보안 및 컴플라이언스 문제도 고려해야 합니다. 얼마 전 중국 북경대학의 한 학생은 대학 측의 정보 규제에 맞서 자신의 상황을 이더리움 트랜잭션에 기록해 올렸습니다. 비탈릭 부테린은 이를 블록체인의 검열 저항성의 사례로 제시하고 있습니다. 반면 인터폴은 블록체인이 포르노 등 불법적인 기록에 사용될 것을 오래전부터 우려하고 있었고 얼마 전 실제로 비트코인상에 아동성학대 이미지가 올라간 사례가 발견되었습니다. 다크웹 서비스에 대한 링크도 발견되었고요. 바이러스가 블록체인을 통해 전파될 가능성도 우려되고 있습니다. DAO 해킹의 사례에서 볼 수 있듯 스마트 컨트랙트 코드의 오류는 큰 피해를 가져올 수 있습니다. 블록체인이 전세계적 인프라로 이용되기 위해서는 이러한 오남용을 막기 위한 기술적, 법적 조치들이 함께 이루어져야 할 것입니다.