[정보보호] 블록 체인 및 관련 보안 표준화 추진 동향

블록 체인(Blockchain)이란 거래 내역이 담긴 장부를 한 곳에 모아서 저장하는 것이 아니라 거래에 참여한 모든 이가 나눠 가지는 것으로, 하나의 가상 원장(Virtual Ledger)을 만들고 관리하는 분산 원장 기술(DLT : Distributed Ledger Technology) 이라고도 불린다. 보안성이 좋고, 데이터 보호에 드는 비용을 줄이는 효과가 있다.

블록 체인은 2009년에 등장한 첫번째 암호 화폐였던 비트 코인에서 처음 나타난 개념으로, 모든 암호 화폐는 각각의 블록 체인을 가지고 있다. 암호 화폐는 화폐를 따로 조폐하는 중앙은행이 존재하지 않고 일정한 주기마다 블록(Block)을 찾아내고 보상을 받아가는 식으로 화폐가 생성된다. 블록은 해당 암호 화폐가 사용하는 해시 함수로 이루어져 있으며 사용자는 컴퓨터의 연산 능력을 이용해 일일이 맞는 함수를 대입하는 식으로 해시를 찾게 된다. 이러한 과정을 채굴(Mining)이라 한다.

블록에는 해당 블록이 발견되기 이전에 사용자들에게 전파되었던 모든 거래 내역이 기록되어 있고, 이것은 P2P 방식으로 모든 사용자에게 똑같이 전송되므로 거래 내역을 임의로 수정하거나 누락시킬 수 없다. 블록은 발견된 날짜와 이전 블록에 대한 연결고리를 가지고 있으며 이러한 블록들의 집합을 블록 체인이라 칭한다. 기존의 중앙 서버에 거래기록을 보관하는 것과는 달리, 블록 체인은 모든 사용자에게 거래기록을 보여주며 서로 비교해 위조를 막는다.

블록 체인 아키텍처의 기술적 장점은 다음과 같다.

첫째, 대규모의 노드들 사이에서 각 노드에 분산 저장된 장부의 데이터를 항상 최신 버전으로 유지할 수 있도록 하는 합의 수렴 알고리즘으로 볼 수 있다. 이러한 능력은 노드가 익명으로 실행되거나, 연결이 좋지 않거나, 심지어 신뢰할 수 없는 운영자가 참여하는 것도 가능하게 한다.

둘째, 모든 탈중앙 암호화폐의 노드는 부분 또는 전체의 블록 체인을 가지고 있다. 이것이 페이팔과 같은 시스템에서 필요로 하는, 중앙 집중형 데이터베이스를 가지고 있을 필요를 없게 한다. 일반적인 장부에는 수표나 영수증 또는 약속어음의 교환내역이 기록되는 반면에, 블록 체인은 그것 자체가 거래장부인 동시에 거래증서(수표, 영수증, 약속어음)이다. 비트 코인에서는 거래들의 지불되지 않은 결과의 형태로 존재한다고 표현한다. "지불인 갑이 00원을 수취인 을에게 보내다" 형식의 거래는 소프트웨어 앱(비트코인 지갑앱 등)을 통해 블록 체인 네트워크에 뿌려진다. 블록 체인 네트워크의 노드들은 거래를 검증한 다음, 자신의 장부에 거래를 추가한다. 그리고 이 거래가 추가된 장부를 네트워크의 다른 노드들에게 뿌린다.

셋째, 암호 화폐들은 신뢰할 수 있는 제3자에 의한 시간표시거래를 블록체인에 추가하는 것을 피하기 위해, 작업 증명(proof-of-work) 또는 소유 증명(proof-of-take) 같은 다양한 시간표시 방법들을 사용한다. 이것은 누구나 쉽게 이중 지불되는 돈의 문제를 회피할 수 있게 한다.

블록 체인의 첫 구현체 개발은 비트 코인으로 시작되었고, 추가적으로 성능 개선, 익명성 추가, 저장 기능과 스마트 컨트랙(smart contract) 기능들이 개발되었으며, 블록 체인의 주요 구현 사례는 다음과 같다.

o 비트 코인 : 작업 증명(Proof of work)

o 디지털노트 XDN : 블록체인 위에 인스턴트 메신저, 블록 체인 작업 증명에 기반을 둔 뱅킹 예금 시스템

o 네임코인 : 블록 체인에 데이터 저장 기능 제공

o 마스터코인 : 다양한 거래를 처리 가능한 블록 체인

o 피어코인 : 작업 증명의 대안으로 소유 증명 추가

o 이더리움 : 튜링 완전 스마트 컨트랙 및 12초의 블록 생성 주기 지원

블록 체인의 약점도 존재한다. 잘못 입력된 데이터는 분산 원장에서 삭제가 거의 불가능하다. 블록 내 개인정보가 포함되면 프라이버시 침해 소지가 크다. 안전성 강화를 위해선 암호학적 계산을 위한 추가 자원의 소비가 요구된다. 정보가 공개돼 있으므로 정보 훼손에 대한 파급효과가 더 크다. 이에 따른 위험도 도사리고 있다. 블록 내 지문이나 홍채 등의 생체 정보가 해킹되면 되돌릴 수 없고 다시 활용할 수 없게 된다.

블록 체인 서비스나 응용의 안전성 근간인 개인키는 하드웨어 등의 수단으로 안전하게 사용돼야 하며, 개인키를 안전하게 이용할 수 있게 만드는 생체 기반 인증 기술의 적용은 편리성을 향상시킬 수 있다. 블록 체인은 기존 인증 방식을 대체하는 것이 아니고, 공인 인증 기술과 결합돼 안전성을 향상시켜야 한다.

블록 체인의 안전성 검토가 필요하다. 일정 주기마다 블록에서 해시 체인을 확정하기 위해 필요한 암호학적 계산 복잡도도 서비스마다 위험 평가 결과에 근거해 결정돼야 한다. 블록 체인 내에 포함될 개인정보가 침해되지 않도록 운영돼야 한다. 실제 데이터나 암호화된 데이터를 블록에 저장하지 말고 데이터의 존재 사실과 링크만을 블록에 제공해야 한다. 모든 참여자가 블록 정보에 접근케 하는 일괄적인 접근 권한 방식보다는 참여자마다 다른 접근 권한을 부여하는

세부 접근 권한 관리가 필요하다. 블록에 존재하는 개인정보가 무엇이고 어떤 용도로 이용되는지도 파악되어야 한다. 사용자 동의 기반의 블록 내 개인정보의 활용도 기본이다.

블록 체인이 인터넷 상의 기존 문제점을 모두 해결해 줄 것이라는 기대는 무리다. 블록 체인에 기반을 둔 응용 및 서비스를 개발하기 위해서는 차분하게 기술 속성을 살펴보고 그 속성을 만족하는 적절한 서비스 이용 사례의 파악이 먼저다. 다양한 이용 사례를 지원할 수 있는 공통 플랫폼의 개발과 생태계 조성과 견고한 특허 협정이 필요하다. 데이터와 서비스의 호환을 고려한 국내외 표준의 개발도 필요하다. 최근, 블록 체인 표준화를 위해 월드 와이드 웹(WWW) 컨소시엄에서는 블록 체인 연락 그룹(CG)이 만들어 졌다. 또한, 보안과 개인정보보호를 포함한 블록체인 관련 국제 표준을 개발하기 위해 ITU-T 에서는 금년 3월 "블록 체인의 보안성 측면" 워크숍을 개최하였고, 이의 후속 조치로 ITU-T SG 17 (의장 : 염흥열 교수)에서는 "분산 원장 기술(DLT: Distributed Ledger Technology) 포커스 그룹" 구성을 통해 표준 개발을 시작키로 결정하였으며, 현재 고려 중인 주요 표준화 대상은 다음과 같다

o 블록 체인 기술에 기반한 응용 및 서비스를 위한 보안 측면 연구
o 블록 체인 기술에 기반한 응용 및 서비스에서의 보안 이슈 및 위협
o 블록 체인 기술에 기반한 응용 및 서비스를 위한 보안 메커니즘, 프로토콜 및 기술
o 블록 체인 기술에 기반한 응용 및 서비스를 위한 안전한 상호접속 메커니즘
o 블록 체인 기술에 기반한 응용 및 서비스를 위한 개인정보 관리 및 인증
o 블록 체인 기술에 기반한 응용 및 서비스에서의 개인 식별 정보 보호 이슈 및 위협
o 블록 체인 기술에 기반한 응용 및 서비스를 제공하는 조직을 위한 정보관리 시스템 등

블록 체인의 광범위한 도입을 위하여는 국내 및 국제 표준화가 절실하며, 국내 민간 전문가나 정부의 적극적인 참여가 필요하다.

진병문 (두진정보연구원 대표, bmchin@tta.or.kr)