충북블록체인진흥센터
2020_2(통권 제2호)

2020 블록체인 이슈페이퍼

정보보호 / 데이터베이스

cbist 충북과학기술혁신원

지금 왜 블록체인인가

블록체인은 '블록'이라고 하는 소규모 데이터들이 *P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경결과를 열람할 수 있는 원장 관리 기술이다. 절대적인 보안과 신뢰 제공 모델을 바탕으로 구축되었고, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다.

블록체인의 장점으로 크게 3가지(분산화, 불변성, 익명성)로 나누어 볼 수 있다.

분산화

중앙집중식 시스템과는 달리 제3의 신뢰 기관을 요구하지 않는다.

불변성

유효하지 않은 *트랜잭션은 블록체인의 노드들에 의해 받아들여지지 않고 트랜잭션이 블록체인에 기록되면 해당 내용을 삭제하거나 되돌리는 것이 불가능하다.

익명성

각 사용자는 자신의 유사 익명 주소로 블록체인과 상호 동작한다. 이 주소는 사용자 실체 신원 식별 정보가 포함되지 않기 때문에, 사용자 익명성은 보존될 수 있다. 그러나 블록체인은 트랜잭션 내용을 모두 공개하므로 *트랜잭션 익명성은 보장될 수 없다.

반면에, 블록체인 기술에는 부정적인 측면들도 존재한다. 익명 거래로 인한 범죄 활용, 고성능 컴퓨팅 파워를 이용한 거래 조작 등 꽤 심각한 문제들이 존재한다. 더군다나 블록체인은 네트워크에 참여하는 모든 노드가 모든 트랜잭션을 독립적으로 처리한다는 기본 가정을 전제로 하고 한번 등록된 데이터는 지울 수 없는 특성 때문에 시간이 지날수록 블록체인 용량은 커지게 된다. 이로써 트랜잭션의 처리 시간이 느려지는 문제가 발생하는 등 블록체인 기술에는 다양한 단점도 보여지고 있다.

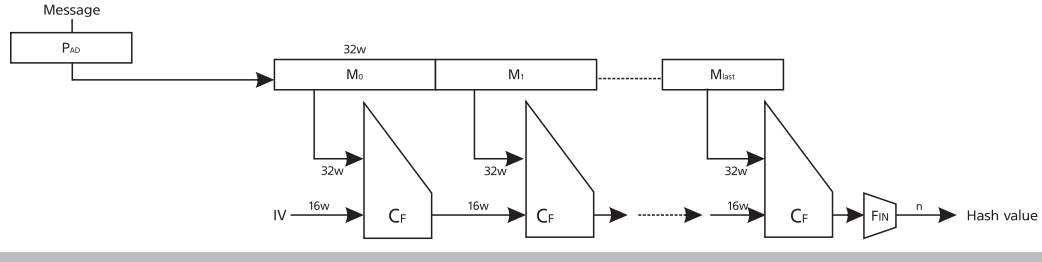
블록체인 기술은 금융권, 의료권, 부동산, 유통, 자율주행 자동차 등 다양한 산업 분야에 사용되어지고 있다. 다만, 블록체인 속성 중 하나인 저장된 정보(데이터)를 네트워크에 참여하는 노드들이 함께 공유할 수 있는 분산 데이터베이스가 국내 개인정보보호법에 위반되는 문제가 발생한다. 이에 블록체인과 접목시킬 수 있는 통상적인 주제로 정보보호와 데이터베이스의 역할이라고 생각하여, 이번 호에서는 위 두 가지 주제를 다루어 보려고 한다.

블록체인 기술과 정보보호·데이터베이스 관계

첫째로 정보보호란 정보를 보호하고 보안을 유지하는 것을 말하며 정보보안과 동의어로 쓸 수 있다. 대부분 문서에서 인정하는 필수적 성질은 기밀성, 무결성, 가용성인데, 자격이 없으면 볼 수 없고 틀린 정보는 취급하지 않는다. 하지만 이러한 정의로 보았을 때, 정보보호의 측면에서도 정보 유출에 대한 책임을 회피할 수 있다는 등의 단점이 존재하고 있다.

블록체인은 데이터 보안을 달성하기 위해 암호화 기술에 크게 의존하고 있는데, 그중에서 가장 중요한 암호화 기능 중 하나는 *해싱으로 볼 수 있다. 입력 크기와 관계없이 출력은 항상 동일한 길이를 나타내는데 입력이 변경되면 출력은 완전히 달라지게 된다. 그러나 입력 내용이 변경되지 않으면, 해시함수를 아무리 많이 실행하더라도 결과는 동일하다.

블록체인 내에서 해시라고 하는 출력값은 데이터 블록의 고유식별자로 활용되는데, 각 블록의 해시는 이전 블록의 해시와 관련되어 생성되며, 이를 통해 블록은 서로 연결되어 블록체인을 형성한다. 블록 해시는 해당 블록에 포함된 데이터에 의존하므로, 데이터를 변경하려면 블록 해시를 변경해야 하기 때문에 각 블록 해시는 해당 블록에 포함된 데이터와 이전 블록의 해시를 기반으로 생성된다. 이러한 해시 식별자는 블록체인 보안과 불변성을 유지하는 데 중요한 역할을 한다. 해시함수는 초기화, 압축, 완료 등 3가지 단계로 구성되어 있다.



해시 함수 LSH 전체 구조 * 출처 : “해시함수”, 위키백과

둘째로 데이터베이스란 여러 사람이 공유하여 사용할 목적으로 체계화해 통합, 관리하는 데이터의 집합이다. 작성된 목록으로써 여러 응용 시스템들의 통합된 정보들을 저장하여 운영할 수 있는 공용 데이터들의 묶음이다.

누구든 블록체인과 데이터베이스를 같은 개념이라고 생각할 수 있다. 하지만 블록체인과 데이터베이스의 차이점은 핵심적인 면에서 다르다. 블록체인은 P2P 네트워크 아키텍처를 기반으로 실행되지만 데이터베이스는 클라이언트-서버 네트워크 아키텍처를 기반으로 실행되어진다. 또한, 데이터베이스는 고도로 중앙화된 시스템이므로 관리자가 이를 잘 관리하도록 신뢰할 수 있다. 데이터베이스에 저장된 데이터를 읽고 쓸 수 있는 권리를 부여하는 것은 관리자이며, 중앙 집중식이기 때문에 데이터베이스 유지 관리가 매우 쉽다. 반면에 블록체인은 고도로 분산된 시스템이며 제3자와 관련없이 중요한 정보를 공유할 수 있는 중앙 집중식 제어 시스템의 필요성을 제거한다는 것이 큰 차이점으로 보여진다.

이미 블록체인을 기존 관계형 데이터베이스를 보완할 수 있는 데이터베이스 시스템으로 활용하려는 시도가 다양한 분야에서 이루어지고 있다. 하지만 이러한 시도가 효율성 측면에서 옳지 않다는 부정적인 시선도 있다. 나아가 이와 관련된 주제들에 대해 전문가의 소견을 통해 고찰하고자 한다.

---

*P2P(peer to peer) : 비교적 소수의 서버에 집중하기보다는 망 구성에 참여하는 기계들의 계산과 대역폭 성능에 의존하여 구성되는 통신망

*트랜잭션 : 데이터통신 시스템에서 관리의 대상이 되는 기본적인 정보를 기록한 기본파일에 대해 내용추가, 삭제 및 갱신 등의 정보를 가져오도록 하는 행위 또는 이동정보라고도 한다.

*해싱 : 해시함수로 알려진 알고리즘이 데이터 입력을 수신하고 고정 길이 값을 포함하는 정해진 출력을 반환하는 과정

전문가 소견 1

• 김태성 교수(충북대학교)

정보보호는 기밀성, 무결성, 가용성의 보장을 목표로 수행하는 기술적, 관리적, 물리적 활동을 통칭한다. 기밀성은 인가된 사람에게만 접근할 수 있도록 보장하는 것이고, 무결성은 정보와 정보처리 방식의 정확성과 완전성을 보장하는 것이고, 가용성은 인가된 사용자가 필요한 때에는 정보 및 이에 관련된 자산에 접근할 수 있는 것을 보장하는 것이다.

네이버 지식백과에 따르면 블록체인은 "누구나 열람할 수 있는 장부에 거래 내역을 투명하게 기록하고, 여러 대의 컴퓨터에 이를 복제해 저장하는 분산형 데이터 저장기술이다. 여러 대의 컴퓨터가 기록을 검증하여 해킹을 막는다."라고 정의되어 있고, 영어로 Blockchain Security Technology로 표기한다고 되어 있다. 복사한 데이터 사본을 분산 저장함으로써 데이터 무결성을 보장하기 위한 기술인 것이다.

정보시스템은 중앙집중화와 분산화가 주기적으로 반복되면서 진화해왔다. 초기의 정보시스템은 고가의 메인프레임을 중심에 두고 저속의 단말기들이 연결하여 사용하는 중앙집중화 방식이었고, 그 이후에 개인용 컴퓨터가 보급되면서 분산화되기 시작하였다. 1990년대에 인터넷 기술을 이용한 네트워크 서비스의 폭발적인 발달로 인해 데이터의 중앙집중화와 데이터의 분산저장이 동시에 발전하게 되었다. 사물인터넷 기기와 센서에서 산출되는 데이터의 규모가 중앙집중화하여 처리할 수 있는 규모를 상회하게 되면서 개별 조직이 관리할 수 없는 정보인프라를 위탁 제공하는 클라우드 서비스나 이용자 간에 정보자원을 공유할 수 있는 P2P (Peer-to-Peer) 서비스가 각광받게 되었다.

2000년대에 등장하게 된 블록체인 기술은 기존의 중앙집중화 정보처리 환경에서 서버에 저장되어 있던 데이터를 정보소유자의 컴퓨터에 분산 저장할 수 있도록 하여 데이터 변조를 방지하고 정보소유자의 정보 주권을 강화하게 되었다. 데이터의 유형에 따라서 이러한 정보서비스 이용환경은 다양하게 발전하고 있는데, 생체

정보를 이용한 본인확인 기술의 일종인 FIDO(Fast IDentity Online)는 온라인 환경에서 ID, 비밀번호 없이 생체인식 기술을 활용하여 보다 편리하고 안전하게 개인 인증을 수행한다. 개인정보 보호법상의 고유식별정보는 아니지만, 개인을 고유하게 식별할 수 있으며 유출시 원정보의 교체 또는 재발급이 어려운 생체정보의 특성상 정보소유자의 정보 주권에 대한 고려가 중요한 이슈이다. FIDO 인증을 위한 개인의 생체정보도 개인 소유의 컴퓨터(또는 정보단말기)에 저장하는 것이 상기한 내용과 유사한 목적의 달성을 위해 추진되고 있다.

블록체인이 정보보호의 무결성 목적의 달성을 위해서는 '효과적'인 수단이지만, 정보보호의 가용성 목적 측면에서는 '효율적'인 수단이 되기는 어렵다. 사본을 사용자의 컴퓨터에 분산 저장한다는 것부터 자원이용의 효율성에 적합하지 않고, 합의 과정을 거쳐서 수정 여부를 결정하는 절차가 필요하기 때문에 중앙집중화된 정보이용환경에서 효율성을 강조하던 기존의 서비스제공자의 반발을 유도할 수 있다. 한국처럼 중앙집중화된 정보인프라가 발달하고 이용자들이 신속한 정보서비스에 익숙한 국가의 경우에는 블록체인의 고유한 특성을 살려서 정보보호 목적을 달성하는 것은 더욱 어려울 것이다.

개발도상국의 경제발전 · 사회발전 · 복지증진 등을 주목적으로 제공되는 공적개발원조(Official Development Assistance, ODA)를 제공하는 경우, 레거시 인프라가 구축되어 있지 않은 부문, 특히 정보주권자의 데이터 무결성이 중요한 의료, 금융, 행정 등의 분야를 대상으로 신규 IT서비스를 블록체인으로 구축하는 방식으로 진행되는 것이 바람직할 것이다. 블록체인 분야는 산업 초기부터 글로벌 시장을 대상으로 추진함으로써 블록체인 고유의 특성을 달성할 수 있을 뿐만 아니라 국내 블록체인 관련 산업체의 육성에도 도움이 될 것이다.

전문가 소견 2

• 이해영 교수(청주대학교)

» 암호화폐를 넘어선 블록체인 기술

블록체인은 4차 산업혁명 신성장 산업을 견인하는 기반 기술 중 하나로 주목받고 있다. 블록체인은 데이터가 담긴 블록들을 암호기술을 사용하여 체인처럼 연결한다. 새로운 데이터를 담은 블록은 데이터와 관련된 참가자들의 합의(consensus)를 통해 기존 블록들과 연결된다. 연결된 블록들은 분산되어 저장되고, 참가자들에게 투명하게 공개된다. 암호기술을 사용하여 연결된 블록들을 분산하여 저장하고 공개하므로 블록들에 담긴 데이터를 조작하거나 삭제하기는 사실상 불가능하다. 또한, 블록들을 분산하여 저장하므로 안전한 데이터 저장소로 활용할 수 있다. 마지막으로, 참가자들의 합의를 통해 새로운 블록이 연결되므로, 별도 중재자(제삼자)의 개입이 불필요하다. 초기 블록체인은 암호화폐(cryptocurrency)와 같은 제한적인 분야에서만 사용되었다. 그러나 지금은 다양한 분야에서 중재자의 개입 없이 데이터를 안전하게 저장하고 검증할 수 있는 기반 기술로 블록체인을 활용하거나 활용을 시도하고 있다.

» 데이터를 조작할 수 없는 데이터 저장소

블록체인의 데이터를 조작하거나 삭제하기는 사실상 불가능하다. 이러한 특성이 필요한 정보보호 분야에서 블록체인을 활용할 수 있다. 예를 들어, 리눅스나 윈도우와 같은 운영체제의 사건 기록(logging) 기능에 블록체인 기술을 적용할 수 있다. 대부분 운영체제는 문제 발생, 사용자 로그인 등의 주요 사건들을 기록하는 기능을 기본적으로 제공한다. 그러나 고도로 숙련된 해커는 해킹 사실의 인지와 추적을 방해하기 위하여 해킹과 관련된 기록을 삭제한다. 블록체인 기술을 활용하여 주요 사건들을 기록한다면, 해킹 사실을 보다 빨리 인지할 수 있으며 해커의 추적 가능성 또한 높아질 것이다. 또한, 디지털 미디어의 저작권 관리에도 블록체인 기술을 적용할 수 있다. 디지털 미디어의 저작권자와 이용자 추적을 위해 블록체인을 활용할 수 있으며, 저작권, 이용 등의 관리에도 활용할 수 있다.

» 안전한 분산형 데이터 저장소

블록체인의 데이터는 여러 컴퓨터에 분산되어 저장되므로 특정 지점에 장애가 생기면 전체가 중단되는 단일 장애점(single point of failure; SPOF) 문제에서 벗어난다. 단일 장애점이 없는 정보보호 기술이 필요할 때 블록체인을 활용 수 있다.

예를 들어, 소프트웨어의 안전한 업데이트를 위해 블록체인 기술을 적용할 수 있다. 특히 스마트카와 같이 안전이 극히 중요한 시스템(safety-critical system)의 소프트웨어를 원격으로 업데이트할 때 단일 장애점 있다면 치명적인 사고로 이어질 가능성이 있다. 블록체인 기술을 활용하여 소프트웨어를 제공하고 점검한다면, 단일 장애점으로 인한 사고를 근본적으로 방지할 수 있다.

» 중재자가 불필요한 데이터 저장소

블록체인은 별도의 중재자가 필요하지 않으므로 높은 확장성(scalability)을 가진다. 그러므로 높은 확장성이 필요한 정보보호 분야에서 블록체인을 활용할 수 있다. 예를 들어, 안전한 통신을 위한 암호 키 관리를 위해 블록체인 기술을 적용할 수 있다. 안전한 통신을 위해서는 보낼 데이터를 암호화해야 하며, 암호화에는 암호 키가 필요하다. 현재는 소수의 중재자가 암호화 키를 관리하고 있으나, 향후 수많은 기기가 연결되는 사물인터넷(IoT) 시대가 본격적으로 도래한다면 현재의 중앙집중식 키 관리 모델은 한계를 가질 수밖에 없다. 중재자가 불필요한 블록체인은 IoT 시대에서 현재 모델의 확장성 문제를 해결하는 기술로 활용될 수 있다.

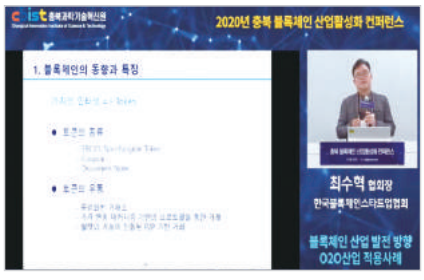
» 블록체인 보안기술

앞서 소개한 예제들은 정보보호 분야에서 블록체인의 적용 가능성을 극히 일부만 보인 것이다. 지금도 정보보호 분야에서 블록체인 기술을 응용하는 연구·개발이 진행 중이며, 앞으로도 블록체인 응용이 끊임없이 개발될 것이다. 정보보호 분야에서 획기적인 응용 개발은 기업과 국가의 경쟁력을 한층 높이는 계기가 될 수 있으므로, 이를 위한 투자가 필요하다. 또한, 블록체인을 가동하는 토대를 안전하게 만드는 블록체인 보안기술에도 지속해서 관심을 둘 필요가 있다.

충북블록체인진흥센터 연혁 및 성과

2020. 12. 충북 블록체인 산업활성화 컨퍼런스 개최

- 일 시 : 12. 4(금) 10:00~
- 장 소 : 충북과학기술혁신원 제1관
- 참석자 : 33명
- 방 법 : 온·오프라인 동시 진행



2020. 12. 충북 블록체인 신규 과제기획 발굴 (2과제)

- 화장품 용기 사용 블록체인 플랫폼 구축
- 블록체인 기반 소프트웨어 업데이트 아키텍처 분석 및 설계

2020. 11. 블록체인 이슈페이퍼(통권 2호) 발행 (정보보호와 데이터베이스)

2020. 10. 블록체인 이슈페이퍼(통권 1호) 발행 (정보보호)

2020. 09. 충북 블록체인 기술창업 경진대회 개최

- 공고기간 : 2020. 9. 28 ~ 10. 30.
- 시 상 식 : 2020. 12. 04(금)

2020. 07. **다부처공동기획 연구지원 사업 선정 (전담: KISTEP)**

- 과 제 명 : 골든타임 확보를 위한 블록체인 의료 데이터 공유 플랫폼
- 사업기간 : 2020. 7. 3. ~ 2020. 12. 31.(6개월)
- 사 업 비 : 총 60,000천원

2020. 06. **'20년 산업혁신기반 구축사업 선정 (전담: KIAT)**

- 과 제 명 : P2P 분산거래 유통 플랫폼 구축 및 현지 실증사업
- 사업기간 : 2020. 6. 1. ~ 2022. 12. 31.(31개월)
- 사 업 비 : 총 3,000,000천원 / 정부 2,400,000천원, 민간 600,000천원

2020. 03. **SOS랩 구축 및 SW서비스 개발사업 선정 (전담: NIPA)**

- 과 제 명 : 도시안전 SOS랩 구축 및 SW서비스 개발
- 사업기간 : 2020. 04. 01. ~ 2024. 12. 31.(57개월)
- 사 업 비 : 9,339,000천원 / 정부 5,539,000천원, 지방비 3,800,000천원

2019. 12. **블록체인 산업인의 밤 개최**

- 일시 : 12. 17(화) 18:00
- 장소 : 쿠우쿠우(오창점)
- 참석자 : 33명
- 내용 : 주제발표 및 네트워킹

2019. 11. 충북 블록체인 기본계획 수립 최종보고서 발간

2019. 11. 충청북도 블록체인산업 진흥조례의 제정 계획 수립

2019. 10. 제1차 충북 블록체인 활성화 세미나 개최

- 일 시 : 10. 23(수) 14:00 ~
- 장 소 : 서원대학교 제1자연관
- 참석자 : 60명
- 방 법 : 주제발표 및 패널토론

2019. 10. 충북 블록체인 진흥을 위한 업무협약 체결

- 일 시 : 10. 23(수) 14:00
- 장 소 : 서원대학교 제1자연관
- 대 상 : 충북과학기술혁신원↔한국블록체인산업진흥협회 ↔충북ICT산업협회

2019. 04. 블록체인 기술컨설팅 지원사업 선정 (전담: NIPA)

- 과 제 명 : 블록체인 기반 응급의료 정보 공유 플랫폼 구축
- 사업기간 : 2019. 08. 01. ~ 2019. 11. 30.(4개월)

2018. 10. 충북블록체인진흥센터 개소식

- 일　시 : 10. 22(월) 11:00 ~
- 장　소 : 충북과학기술혁신원 제1관
- 참석자 : 120명
- 방　법 : 개회선언 및 발표

참고문헌

- 블록체인, **구글**(https://www.google.com)
- 블록체인, **위키백과**(https://ko.wikipedia.org), 2020. 10. 22.
- 블록체인, **한국과학기술정보연구원**(https://www.kisti.re.kr), 2018. 12. 4.
- P2P, **위키백과**(https://ko.wikipedia.org), 2020. 9. 18.
- 트랜잭션, **네이버 지식백과**(https://terms.naver.com), 2020. 1. 31.
- 정보보호, **나무위키**(https://namu.wiki), 2020. 8. 4.
- 해시함수, **위키백과**(https://ko.wikipedia.org), 2020. 6. 19.
- 데이터베이스, **위키백과**(https://ko.wikipedia.org), 2020. 9. 24.
- 데이터베이스, **구글**(https://www.google.com)

2020 블록체인 이슈페이퍼 2020_2(통권 제2호)

정보보호 / 데이터베이스

- 발행일 : 2020년 11월 30일
- 발행처 : 충북과학기술혁신원 블록체인진흥센터
- 편집자 : 정재욱 센터장, 유혜인 주임, 이영훈 사원
- 주　소 : 충북 청주시 청원구 오창읍 각리1길 7
- 홈페이지 : http://www.cbist.or.kr/

www.cbist.or.kr