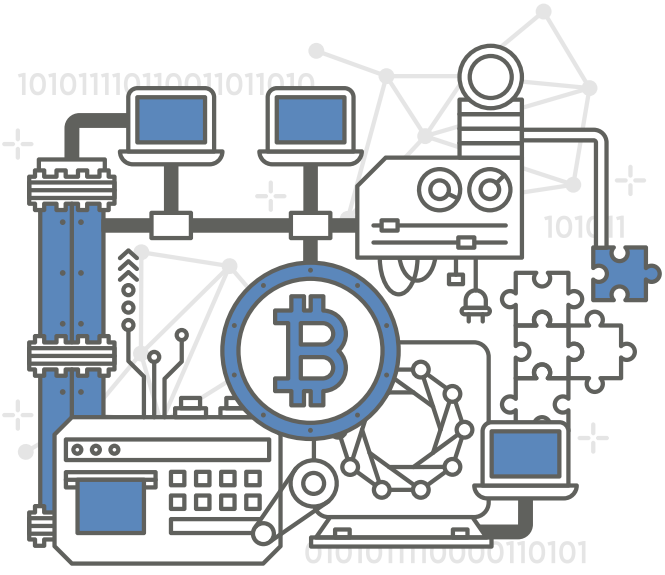
발간 | 충북블록체인진흥센터

2020_1 (통권 제1호)

2020년

블록체인 ISSUE PAPER

정보보호



cbist 충북과학기술혁신원

충북과학기술혁신원장
노 근 호

안녕하십니까? 충북과학기술혁신원장 노근호입니다.

충북과학기술혁신원은 2003년 충북지식산업진흥원으로 설립된 이래 4차 산업혁명을 이끌 전문기관으로서 2020년 6월 '충북과학기술혁신원'으로 새롭게 출범하였습니다. 지역 주도의 과학기술 정책 수립과 신성장 산업의 R&D 기획을 수행하는 전담기관으로서의 면모를 일신하고 있습니다.

특히, 블록체인 산업 생태계 조성을 위해 국내 최초로 원내 충북블록체인진흥센터를 구축하여 블록체인 산업진흥에 이바지하고 있으며, 4차 산업혁명 시대에 대응하는 혁신적 변화와 발전의 기반을 다지고 있습니다.

신뢰성, 무결성, 투명성, 공유성 등의 장점을 지닌 블록체인 기술은 4차 산업혁명시대의 핵심기술 중 하나로 주목받고 있습니다. 블록체인 ISSUE-PAPER에서는 이러한 환경 흐름을 파악하여 지역의 산·학·연·관 관계자들에게 정보를 제공하는 역할과 동시에 블록체인 저변 확산에 초석이 되고자 합니다. 이와 더불어 블록체인에 관심이 있는 모든 분에게 조금이나마 도움이 되었으면 합니다. 또한, 이 순간에도 변화하고 있는 블록체인 산업에 새로운 기회의 발판을 마련하는 계기가 되었으면 하는 바람입니다.

앞으로도 저희 충북과학기술혁신원 블록체인진흥센터에 지속적인 관심과 성원 부탁드리며, 향후 블록체인 산업의 성장과 발전이 초기에 실현되도록 최선을 다하겠습니다.

감사합니다.

블록체인 기술은 가상화폐부터 시작해 P2P, 대출 및 금융 서비스 등 우리 생활에 이미 널리 퍼져있다. 특히, 4차 산업혁명 시대를 맞아 블록체인 기술의 활용 분야와 그 범위로 우리가 아는 금융 서비스뿐 만이 아닌 의료 분야, 유통 산업, 여론조사, 선거 등 다양한 분야에 접목시킬 수 있다.

1. 금융분야

블록체인은 전자화폐, 해외송금, 금융거래기록저장, 메시지 보호 및 전달 등의 형태로 가장 널리 활용되고 있다.
전자화폐의 경우, 제3자의 보증 없이도 개인 간의 거래가 안전하게 이루어진다. 암호화된 키 값을 사용하고, 새로운 블록과 기존 블록이 결합하면서 데이터 수정이 어려워지기 때문에 보안 능력이 매우 뛰어나다는 장점 또한, 금융기관이라는 중간 관리자를 배제한 거래가 이루어지므로, 금융 거래 속도가 매우 빠르다는 특징도 있다. 그래서 블록체인 기술을 포함한 여러 간편 결제 시스템도 많이 생겨나고 있는 추세이다. 중앙 서버와 시스템에 대한 관리가 불필요하기 때문에 비용적인 측면에서도 우수하다는 평가를 받고 있다.

2. 의료분야

의료 분야에도 블록체인 기술을 적용시킬 수 있다. 보통 환자의 기록은 해당 병원의 서버에 기록되어 별도로 관리되고 있다. 그래서 환자가 다른 병원에 방문해야 하거나 추가 진료를 받게 되는 경우에는 진료 관련 기록을 서류로 제출해야 하는 번거로움이 있다.
하지만 여기서 블록체인의 기술을 결합시키면, 환자에 대한 정보를 여러 병원이 함께 공유할 수 있다는 장점이 있다. 환자가 직접 자신의 몸 상태를 설명하지 않아도 되고, 환자가 설명했을 때 놓칠 수 있는 전문 정보들을 하나도 빠뜨리지 않고 공유할 수 있다. 또한, 블록체인에 저장된 정보는 수정이나 조작이 어렵기 때문에 무엇보다 객관적이어야 할 의료정보에 대한 신뢰성도 확보된다. 이와 더불어, 의료 연구에도 큰 도움이 된다. 연구소가 원하는 표본을 장소의 제한 없이 수집할 수 있을 것이다.

3. 사회분야

우리 정치/사회 분야에도 블록체인 기술을 도입할 수 있다. 각종 여론조사부터 선거까지 보안성이 뛰어난 블록체인 기술을 활용하면 결과를 조작하거나 수정할 수 없기 때문에 공정한 여론조사와 선거가 진행될 수 있다.
그리고 중앙 시스템에서 관리하는 공공 정보를 블록체인 기술을 통해 저장한다면, 해킹의 우려가 감소하여 보다 안전하게 관리할 수 있다. 향후에는 세금과 정부 예산을 관리하는 일에도 블록체인 기술이 도입되어 더욱 투명한 공공예산 관리가 이루어질 것이라는 기대도 있다.

4. 물류/유통 산업 분야

중국의 월마트의 경우에는 IBM의 블록체인 기술을 이미 도입하여, 특정 제품의 유통과 물류의 전 과정을 추적한다고 한다. 이 뿐만 아니라 영국의 또 다른 신생기업도 제품의 원산지 추적과 인증 과정에 있어 IBM의 블록체인 기술을 활용한다. 송하인부터 포워더, 세관, 수하인까지 공유해야 하는 서류가 많은 물류/유통 산업의 경우 블록체인을 통해 문서를 공유한다면 업무의 효율성은 더욱 증진될 것으로 보인다.
현재 블록체인 기술은 금융이나 의료 분야 등 여러 산업군에 활용되고 있지만, 블록체인 기술 적용에 따른 개인정보 침해 등의 문제점이 나타난다. 특히, 국내 현행 개인정보보호법상 제3자의 제공은 엄격한 사전 동의 방식을 취하고 있어, 개인정보 처리가 정보를 제공하는 주체로부터 사전에 동의를 받지 못하면 제3자에게 제공할 수 없다. 이에 블록체인에 참여하게 되어 이용자 모두에게 개인정보를 제공한다고 가정할 시, 개인정보 주체로부터 모두에게 개인정보 이전과 관련된 개별 동의를 받아야 하나 현실적으로 불가능하다.

결과적으로 블록체인 기술은 아직까지 시범 단계일 뿐이고 실생활에 녹아들기 위해 다양한 검증과 노력들이 필요하다고 생각한다. 블록체인 기술의 핵심 장점인 보안성과 안정성을 제대로 부각시켜 더 투명한 사회를 만드는 일에 기여되었으면 하는 바람이다.

또한, 개인정보 보호를 침해하지 않고 블록체인 기술을 적용시킬 수 있는 방안 마련이 필요하다. 이처럼 블록체인 기술과 정보보호는 밀접한 관계를 지니고 있어 정보보호와 블록체인 관계에 대해 살펴볼 필요가 있다. 이와 관련된 시사점·이슈를 전문가의 소견을 통해 고찰해 보고자 한다.

전문가 소견 1

강필용 센터장 | 한국인터넷진흥원
2020.10

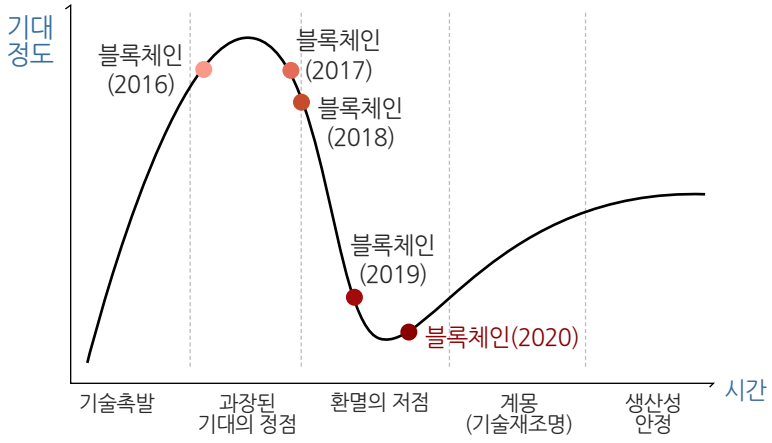
4차 산업혁명의 핵심기술로 주목받고 있는 블록체인

비트코인, 이더리움 등 암호화폐 거래 플랫폼에 적용되어 많은 주목을 받은 블록체인은 제3자 대신 참여자에 의한 검증 · 합의 등에 기반한 작동으로 탈중앙성, 투명성, 무결성, 가용성을 제공하는 기술이다.

무엇보다 블록체인은 분산처리를 통한 거래비용 감소와 데이터 위변조 방지가 장점이며, 다양한 산업과 결합하여 효율성을 높이고 새로운 경제적 가치 창출이 가능하기에 4차 산업혁명 시대에 핵심기술로 활약할 것으로 기대되고 있다.

그러나 이러한 장점 및 기대에도 불구하고, 암호 화폐를 제외하고는 일반 국민이 체감할 수 있는 수준의 블록체인 기반 응용서비스는 아직까지 미흡한 실정이다.

가트너 보고서에 의하면, 블록체인 기술은 현재 환멸의 저점에 도달해 있는 것으로 평가되고 있다. 즉, 다양한 실험 및 구현이 의미 있는 결과물을 내놓는 데 실패함에 따라 관심이 시들해지고, 도입을 시도한 주체들은 다수가 포기하거나 실패한 상황이다. 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속되는 등 옥석을 가리는 시기를 거치고 있으며, 가상자산 거래 및 분산 아이디(Distributed ID) 분야에서 많은 기대를 받고 있다.



〈 가트너 하이프 사이클 상에서의 블록체인 위치변화 〉

최근 국내에서도 공공·민간 분야에서 다양한 도입을 시도하고 있지만, 대다수가 파일럿 단계에 머물러 있으며, 블록체인 표준의 부재, 기술의 미성숙도, 기술에 대한 이해 부족으로 블록체인을 적용할 필요가 없는 분야에 적용하는 등 만족스러운 실사용 사례를 만들지 못해 난항을 겪고 있는 것으로 파악되고 있다. 본 내용에서는 최근의 블록체인 기술이 환멸의 저점을 거쳐 재조명되는 시점에 정보보호를 중심으로 기술적 이슈에 대해 살펴보고자 한다.

다양한 보안기술이 적용되어야 안전성을 보장

블록체인 자체가 보안기술이고, 비트코인 등으로 대표되는 암호화폐 거래 분야에서 오랫동안 안정적으로 사용되고 있는 관계로 일부에서는 기술적 이해 없이 블록체인을 사용하면, 무조건 안전성을 보장할 수 있다고 믿기도 한다.
그러나 안전하다고 생각하는 암호화폐도 국내외 거래소에서 해킹에 의한 보안사고가 꾸준히 발생하고 있다.

〈 암호화폐 거래소 주요 해킹사고 동향 〉

국내	년도	국외
코인레일/500억, 빗썸/350억(6월) 올스타빗/확인불가(10월)	2018	코인체크/5,700억(1월) 자이프/667억(9월) 비트그레일/1,921억(2월)
빗썸/220억(3월) 업비트/580억(11월)	2019	크리토피아/188억(1월) 바이낸스/470억(5월) 비트포인트/380억(7월)
-	2020	쿠코인/1,760억(9월)

※ 출처 : 국내외 언론보도 재구성

물론, 암호화폐 거래소가 해킹되었다고 해서 블록체인 자체가 보안에 취약한 것은 아니며, 그렇다고 블록체인이 완전무결한 것도 아니므로 다양한 분야에 접목하기 위해서는 정보보호 관점에서의 특성 및 제약사항에 대한 정확한 이해가 필요하다.

전체 서비스에 대한 안전성은 적절한 블록체인 모델의 적용 여부는 물론, 다양한 주변 보안기술의 적정성 등을 고려해 종합적으로 판단하여야 한다.

예컨대, 블록체인은 블록(분산 원장)에 정보를 기록한 이후부터 무결성을 보장하는 것이지, 기록하기 전에 위변조된 경우엔 신뢰성을 보장할 수 없다. 즉, 블록에 정보를 기록하기 이전에 작성자의 신원확인 및 기록될 정보의 신뢰성은 다양한 다른 보안기술이 접목되어야 보장될 수 있다.

특히, 블록체인은 공개키 암호기술에 기반하고 있으므로, 참여자가 개인키(비밀키)를 잘못 관리하여 잃어버리거나 유출되면 백약이 무용하다. 실제 개인의 전자지갑 관리의 허점을 노린 많은 해킹 시도가 성공하고 있다.

또한, 블록에 기록된 내용은 참여자는 누구나 조회할 수 있으므로, 개인정보와 같은 민감한 사항은 별도의 보안 조치(비식별조치, 분리저장 등)가 필요하다. 프라이버시 보호를 위해 일정한 기간이 지나면 삭제를 요구할 수 있는 잊혀질 권리도 보장해야 한다.

검증되지 않은 스마트 콘트랙트(smart contract)는 분산된 다수의 노드에서 자동 실행되면서 보안 취약점을 유발할 수 있으므로 선제적 보안 조치가 필요하다.

블록체인 도입시 다양한 측면에서의 고려사항 검토 필요

블록체인은 개발이 완료된 기술이 아니라 계속해서 진화 · 확장되고 있는 기술로서, 다양한 응용 분야에 적용되기 위해서는 기반 및 확장, 서비스 기술 등 다양한 요소기술들이 결합되어야 한다.

블록체인 기술을 도입 및 적용, 구현하려는 기관은 제공하려는 서비스를 위한 요구사항을 도출하고, 보안 및 성능 관점에서 관련 사항들을 면밀히 분석한 이후 도입을 진행해야 의미 있는 결과물을 얻을 수 있다. 요컨대, 블록체인을 도입해 조직의 핵심 역량을 증대시킬 수 있다는 확증이 없다면 블록체인 기술 도입을 서두르지 않는 게 바람직하다.

< 블록체인 도입시 주요 고려사항 >

구분	고려사항	비고
일반 사항	블록 크기, 거래 참여자, 거래기록 열람자, 거래 승인 및 블록생성 권한, 승인 및 합의 방식, 보상 및 벌칙, 자체코인 발행여부 및 방식, 룰 개정 방식 등	모델 선택 (퍼블릭·프라이빗 등)
추가 사항	계정 및 노드의 정당성 검증, 개인정보 보호, 정보의 기밀성, 네트워크 단절·지연 및 악의적 참가자 대응, 취약점 진단 및 조치, 실시간 처리, 블록체인 호환성 등	성능·보안 이슈

전문가 소견 2

이덕규 교수 | 서원대학교
2020.10

블록체인 기술의 가능성

블록체인과 관련된 기술은 최근 4차 산업혁명 기술에서 플랫폼 기술로 역할이 점차 확대되고 있다. 금융에서 가장 크게 적용되고 있으며, 의료, 물류, 공공서비스 등으로 확장되어 사회시스템 변화에 활력을 넣고 있다. 추가로 공유 경제에 해당하는 부분에서 충청북도에서는 비즈니스 모델(농산물 유통, 화장품 불법 차단), 의류·물류 정보 등에 관해 확장연구가 진행되고 있다.

기존 블록체인은 공유 경제에서 서비스 측면으로 많은 접근을 이뤄왔으며, 다양한 응용서비스가 제시되고 있다. 이미 블록체인은 핀테크, 보험, 의료정보, 부동산, 게임, 미디어, 결제, 자동차 등 실생활에 적용된 예는 많이 있다. 이러한 블록체인 분야에서 최근 정보보안에서도 새로운 시장으로 주목받고 있다. 블록체인에서의 분산 원장 기술은 데이터 무결성 보장이라는 장점이, 정보보안을 제공하는 기업·연구소·학계는 블록체인을 이력 관리, 문서 원본 증명, 사용자 인증, 보안 강화 등의 분야에 적용하고 있다.

블록체인 보안 분야에서 향후 연구가 중요시되는 부분은 블록체인에서 사용되는 SW에 대한 문제점과 개인정보가 활용되는 서비스, 예를 들어 전자투표, 의료 융합 서비스, 재난재해 등의 서비스에서의 개인정보 침해가 될 수 있다.
블록체인 중 비트코인으로 예를 본다면 소스 코드가 라이트코인, 대시코인 등의 다른 블록체인에서 사용된 소스 코드가 많은 부분 재사용되고 있다. 이러한 재사용에 높은 비중은 블록체인 소프트웨어에 있어 보안성 관점에서 주목할 만하다.

블록체인 기술의 문제발생 및 해결방안

블록체인에서 사용되고 있는 소프트웨어의 내부 구조를 보면, 이미 개발된 다른 블록체인 소프트웨어에 추가로 제공하는 부분에서 수정·보완하여 제공하는 경우가 많이 있다. 수정된 공개 코드에 새롭게 개발되는 블록체인에서 소프트웨어의 재사용과 함께 DB, 암호화, 파서, 압축 등을 위해 다양한 공개 소스를 포함하고 있음을 확인해야 한다. 이런 재사용에 대한 부분은 블록체인 소스 코드를 개발하는 데 있어 이미 개발되어 공개된 공개 소스를 기반으로 개발하고, 개발된 소스 코드를 다시 공개하여 재사용함으로써 재사용 비

율이 현저히 높아지는 원인이 문제이다. 공개 소스를 공개하고 코드를 재사용하는 것은 현재의 소프트웨어 개발 트렌드로 그 자체에는 문제가 없으나, 보안을 고려한 소프트웨어 개발, 코드 관리를 해야 하는데 간과될 경우들이 문제가 되고 있다.

이러한 보안 위협을 예방하기 위해 시스템 레벨에서의 블록체인의 취약코드 탐지와 블록체인 공개 소스 구성요소 탐지에 대한 보안성 검증 기술이 필요로 하고 있다. 블록체인 개발에 있어 타사 공개 소스 코드 베이스의 일부만 수정해서 재사용하더라도 탐지하고 개발자에게 알려주는 연구가 필요로 할 것이다. 앞에서 언급한 취약코드 탐지와 공개 소스 구성요소 탐지가 이뤄질 수 있다면 실제로 블록체인 코드 베이스에 포함된 취약코드들을 탐지·패치 할 수 있고, 취약점을 내포하고 있거나 라이선스 충돌 가능성이 존재하는 타사 공개 소스 구성요소 식별 후 바로 패치/업데이트가 이뤄질 수 있을 것이며, 이는 향후 블록체인 서비스의 보안성 검증을 지원할 수 있을 것이다.

서비스 측면에서 사례를 통해 살펴본다면, 다음과 같이 두 가지 사례를 통해 개인정보 보호와 연관하여 살펴볼 수 있다. 첫 번째는 온라인 투표 시스템으로 오프라인 투표의 장소 제약적 요인 해소와 기존 온라인 전자투표의 신뢰성 문제를 해결하고 투표결과에 대한 위변조를 예방하기 위해 블록체인 온라인 투표 시스템을 추진하고 있다. 기존 온라인 투표 시스템은 하나의 중앙 시스템을 목표로 하므로 시스템은 늘 위험에 직면해 있으며, 끊임없이 취약점이 발견되고 있다. 블록체인으로 온라인 투표 시스템을 구성하더라도 투표자 본인의 투표를 증명하기 위해 개인 키를 이용하게 되는데 암호키를 생성하는 과정이나 제공하는 과정에서 키 관리에 대한 이슈가 존재하게 된다.

두 번째로 의료 융합 서비스 시스템으로 환자 개인의 의료정보가 병원 중심으로 관리되고 있어 개인 의료정보 활용 한계가 존재하며, 환자 본인의 의료·진료 정보를 개인의 자기 결정권에 따라 다른 의료기관 혹은 다른 기관과의 교류 필요성이 증대되고 있다. 이에 개인 의료정보를 직접 교류하는 과정에서 진료비 청구서, 처방전, 진료 청구서 세부 명세서 및 제 증명서에 대한 위·변조 방지 및 무결성 검증 방법이 필요하게 됨에 따라 블록체인 기술 적용을 통해 의료데이터의 보관, 처리, 가공, 공유 등 환자 중심의 의료정보시스템으로 방안을 모색하고 있다. 이처럼 블록체인 중심으로 의료 융합 서비스 시스템을 구축을 위해 대용량 의료데이터의 형태와 구조가 정의가 필요하며, 블록체인 모든 노드에 정보를 저장하기 위한 처리 속도 및 저장공간의 한계를 극복해야 한다. 특히 개인의 모든 정보가 비가역적으로 저장되어 열람 가능한 형태로 블록체인에 저장된다며 이는 보안에 치명적인 문제가 발생할 수 있다. 해결하려는 방법으로 블록에 실을 온체인 데이터(On-chain Data)와 인덱스 정보를 통해 실제 데이터가 존재하는 오프체인 데이터(Off-chain Data)를 구분하여 개인정보 보호를 침해하지 않는 방안이 필요하다.

블록체인은 기술의 발전과 시장에 따라 급변하고 있다. 블록체인의 신뢰성, 안전성, 개인정보 보호 등에서 많은 정보보안 기술이 적용되고 있으며, 발전을 거듭해 가고 있다. 블록체인에서의 정보보안 이슈는 실제 현장에서도 잘 활용되고 적용하는 방안으로 진행되어야 더욱 안전한 블록체인 서비스 환경을 구축하는데 일조하는 것이다. 블록체인 자체 소스 코드에 대한 위협·침해에 대한 대응과 함께 개인정보에 대한 신뢰성, 보안기술이 적용되어야 할 것이다. 정보보안은 블록체인에서 중요한 화두이며, 향후 블록체인 사업에서 중요한 정보보안에 대한 고려가 필요할 것으로 사료된다.

cbist 충북과학기술혁신원

블록체인 이슈페이퍼 2020_1(통권 제1호) - 정보보호

발행일 2020년 10월 30일
발행처 충북과학기술혁신원 블록체인진흥센터
편집자 정재욱 센터장, 유혜인 주임, 이영훈 사원

충북 청주시 청원구 오창읍 각리1길 7
http://www.cbist.or.kr/