Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1607

블록체인 기술 적용과 개인정보 삭제 및 제3자 제공의 법적 문제에 관한 연구*

최 용 혁,† 권 헌 영‡
고려대학교 정보보호대학원

A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information*

Yong-hyuk Choi,† Hun-yeong Kwon‡
Graduate School of Information Security, Korea University

요 약

공신력 있는 거래체결을 보장하고 그 거래정보의 위변조를 용납할 수 없는 금융산업은 지금까지 전통적인 중앙집중형 원장 관리 방식을 신봉해 왔다. 그러나 블록체인 기술은 오히려 그동안 상식적으로 안전하지 않다고 여겨 왔던 탈중앙화를 강점으로 내세우면서 더욱 신뢰할 수 있는 거래의 합의방식과 데이터의 무결성 보장을 통해 세계의 금융산업과 IT세상에 파장을 일으키고 있다. 그렇지만 블록체인 내 블록정보의 비가역성 및 블록체인 참여자간 블록의 공유와 같은 블록체인의 고유한 특성은 개인정보 보호법제와의 충돌을 피할 수 없는 상황이다. 본 연구에서는 블록체인의 이 특성들을 중심으로 개인정보의 삭제와 제3자 제공 관련한 문제점을 살펴보고 블록체인 기술 활용을 위한 개인정보 보호법제 개선방향 및 적용 가능한 블록체인의 기술적 대안을 제시하고자 한다.

ABSTRACT

The financial industry, which guarantees a credible transaction and can not permit forgery of its transaction information, has hitherto adhered to a traditional centralized ledger management method. However, the blockchain technology has a decentralization which has been regarded as unsafe for the time being, and the more reliable transaction agreement and data integrity are guaranteed The world's financial industry and the IT world is causing the wave. Nevertheless, the inherent characteristics of the blockchain, such as the irreversibility of block information within a blockchain and the sharing of blocks between blockchain participants, can not avoid conflicts with the privacy laws. The purpose of this study is to investigate the problems related to deletion and the third party supply of personal information by focusing on these characteristics of the blockchain and to suggest the technical alternatives of the applicable blockchain and the improvement direction of the personal information protection law for using of blockchain technology.

Keywords: Blockchain, Deletion of Personal Information, The Third Party Supply of Personal Information

Received(10. 23. 2018), Modified(11. 09. 2018), Accepted(11. 09. 2018)

* 본 논문은 2018년도 하계학술대회에서 구두 발표한 논문의 개선 및 확장 논문임

† 주저자, hyuk_choi@hanmail.net
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

I. 서 론

비트코인의 광풍을 등에 업고 대중의 입에 오르내리기 시작한 블록체인 기술은 4차 산업혁명을 주도할 미래 선도 혁신 기술로 주목받고 있다. 특히 최근 금융권에서는 블록체인 기술을 미래 금융의 핵심 인프라로 활용하기 위한 논의와 연구가 다양하게 전개되고 있으며, 이러한 움직임은 머지않아 다양한 산업으로 확장되어 사회 기반구조에 큰 영향을 끼칠 것으로 전망된다.

기업들이 블록체인 기술을 이용하는 새로운 비즈니스 모델 발굴에 힘을 쏟고 있음에도 불구하고 아직까지 국내 블록체인 기술 활용은 걸음마 수준에 머물러 있으며, 블록체인 기술에 대한 높은 관심에도 불구하고 실제 산업에 어떤 영향을 줄지 확언하기 어려운 상황이다.

기존 IT인프라를 블록체인시스템으로 전환하기 위한 연구가 활발하게 진행 중임에도 불구하고 블록체인 기술 활용의 속도가 빠르지 않은 이유는 무엇일까? 기술적인 측면으로 보면 블록체인 기술은 아직 발전 초기 단계로 다양한 환경에서 안정적인 거래를 담보하기 위해서는 지속적인 발전이 필요하며, 비즈니스 측면으로 보면 비즈니스 모델 발굴 및 검증과정에서 발생하는 경제적 이익 상충 관계를 블록체인 참여로 유도하는 합의를 이끌어내는 것이 쉽지 않기 때문이다. 블록체인의 상용화가 어려운 최대 걸림돌은 비즈니스 측면의 문제라는 주장도 있지만[1] 법·제도 측면에서 기존 법률과의 상충 여부에 대한 구체적인 해석이나 판례 부재로 인한 진입 위험이 해소되지 않거나 기존 법률과의 상충 문제에 대한 대안이 없다면 블록체인의 상용화는 허울뿐인 연구만으로 만족해야 한다.

본 연구에서는 블록체인의 고유한 특징을 확인하고, 이 특징이 블록체인의 상용화에 걸림돌이 되는 법·제도 중에서도 국내 개인정보 보호법제와 어떤 점에서 상충되는지 살펴보고자 한다. 또한 블록체인 기술의 활용을 위한 국내 개인정보 보호법제 개선 방향을 고민해 보고 이 문제점을 해결하기 위한 기술적 대안을 제시하고자 한다.

II. 블록체인 기술과 개인정보 보호법제

2.1 국내 블록체인 기술 활용 현황

국내 블록체인 기술 활용은 금융기관을 중심으로 활발하게 전개 중이다. 블록체인을 이용하여 저비용으로 해외송금 및 자산관리에 활용하는 플랫폼을 운영하는 미국 핀테크 업체 R3 CEV와 컨소시엄을 형성하고 있는 골드만삭스, 바클레이즈, JP모건, UBS 등 42개 글로벌 대형은행과 연합하기 위해 하나금융그룹과 신한은행이 R3 컨소시엄에 참여하고 있는데 이 은행들은 블록체인 시스템의 표준화를 위해 R3와 협업체계를 유지하면서 더 빠르고 효율적인 시스템을 글로벌 금융시장에 도입할 계획을 가지고 있다.

국내 은행들은 송금분야에서 블록체인 기술을 활용하기 위한 경쟁에 뛰어들고 있다[2]. KEB하나은행은 글로벌 MTO(Money Transfer Operator)와의 업무제휴를 통해 중개은행을 거치지 않는 중국 해외송금 서비스와 모바일 앱으로 간편하게 해외송금이 가능한 원큐트랜스퍼(1QTransfer)를 출시해 15개 국가를 대상으로 해외송금을 지원 중이다. 신한은행은 글로벌S뱅크를 활용한 머니그램 특급송금 서비스를 출시하고 실시간으로 해외 송금 서비스를 준비 중이다. 우리은행은 위비 쿽 글로벌송금을 통해 우리은행 해외지점으로 외화 송금시 중개은행을 거치지 않고 현지로 바로 송금이 가능하다. 국민은행은 모바일 서비스 KB스타뱅킹과 리브메이트에 해외송금 기능을 추가하였다.

교보생명은 업계 최초로 블록체인 기술을 이용하여 의무기록 사본 발급 연계를 통해 보험금 지급 절차를 간소화한 스마트 보험금 청구 서비스와 고객이 가입한 모든 보험 가입정보를 수집하여 보장분석 시 활용하도록 하는 스마트 스크래핑 서비스를 시범운영하고 있다.

금융투자업계는 2017년 10월에 금융투자협회가 주축이 되어 세계 최초로 블록체인을 이용한 공동인증서인 체인아이디를 출시하고 9개 증권사를 대상으로 시범운영 중이며 2018년 연말 상용화를 목표로 하고 있다. 증권사 고객이 체인아이디를 발급받게 되면 체인아이디를 서비스하는 증권사에서는 별도의 등록 과정 없이 인증서를 사용할 수 있다. 이와 유사하게 은행업계는 2018년 8월에 은행권 블록체인 공동인증서인 뱅크사인 서비스를 개시하였다. 2018년 10월 현재 15개 은행에서 서비스하고 있으며 고객이

뱅크사인을 발급받게 되면 뱅크사인을 서비스하는 은행에서는 별도의 등록 과정 없이 인증서를 사용할 수 있다.

2.2 블록체인 기술과 개인정보보호 규제의 관계

2.2.1 블록체인의 탈중앙화 속성

블록체인의 개념에 대한 다양한 견해가 존재하는데 거의 모든 개념에서 공통적으로 다루고 있는 내용은 블록체인은 분산 데이터베이스이며, 탈중앙화를 기본 사상으로 하는 분산형 디지털 장부라는 것이다. 국내 정보보호 관련 법률이 대부분 중앙집중형 IT환경을 전제로 구체적인 요건을 정하고 있는 것을 감안할 때 블록체인의 탈중앙화라는 속성은 여러 쟁점을 양산하는 주요 요인이 된다. 또한 블록체인 기술을 이용하는 비즈니스 모델중 상당수가 개인정보의 처리 과정이 수반되는 것을 고려하면, 블록체인의 탈중앙화라는 속성과 국내 개인정보 보호법제의 주요 법적 의무사항 간 상충되는 문제점을 검토하고 그 문제점을 해결하기 위한 대안을 찾는 작업은 피할 수 없는 과제이다.

2.2.2 블록체인 정보의 개인정보성

개인정보 보호법에서는 개인정보란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보로, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다고 정의하고 있다[3]. 개인정보 보호법상 개인정보임을 판단할 수 있는 기준인 '다른 정보와 쉽게 결합한다.'는 것은 결합 대상이 될 다른 정보의 입수 가능성이 있어야 하며 다른 정보와의 결합 가능성이 높아야 함을 의미하는데, 이는 곧 합법적으로 정보를 수집할 수 없거나 결합을 위해 불합리한 정도의 시간, 비용 등이 필요한 경우에는 쉽게 결합할 수 있는 상태라고 볼 수 없다는 것이다[4].

비트코인과 같은 암호화폐의 경우에는 블록체인 상에서 거래를 하기 위해 34자리로 이루어진 지갑주소를 통해 거래 당사자를 식별하는데, 이러한 거래 당사자가 현실 세계에서 누구인지 식별할 수 있는 이름, 성별, 나이 등의 정보는 블록체인 상에 저장되지 않는다. 즉 블록체인 상에는 특정 개인을 식별할 수 있는 정보가 저장되지 않고 지갑주소 등 블록체인 상에서만 통용되는 식별자만 저장되고 있다. 이 정보가 개인정보에 해당하는지에 대해서는 논란의 여지가 전혀 없다고 할 수는 없지만 앞서 살펴본 개인정보의 정의와 쉽게 결합할 수 있는 상태에 대한 의미를 감안한다면 비트코인의 지갑주소 정보를 개인정보라고 판단하는 것은 무리가 있다.

개인을 식별할 수 있는 정보를 활용하여야 하는 블록체인 모델을 고려하는 경우 개인정보를 평문 그대로 블록체인 상에 저장하는 것은 블록체인 거래의 투명성을 보장하기 위한 정보의 공개 측면에서 보면 많은 위험성을 내포하게 된다. 따라서 개인정보의 해시 처리[1]를 통한 암호화 등 비식별화 조치를 통해 특정 개인을 식별할 수 없는 상태로 블록체인 상에 저장하는 방법을 취하게 된다. 그러나 비식별 조치가 이루어졌다고 해도 재식별 가능성이 있거나 다른 정보와의 결합 가능성이 있는 경우에는 식별가능성이 있다고 인정되어 개인정보에 해당한다고 볼 수 있다. 즉 개인정보를 이용하는 블록체인 서비스가 개인에 대한 식별을 통해 특정 서비스를 제공할 필요성이 있다면 블록체인 상에 해시 처리를 통해 암호화된 정보를 저장한다고 하여도 서비스의 특성상 원래의 정보와의 비교를 통한 식별가능성을 배제하기는 어려울 것이며 이러한 경우에는 블록체인에 개인정보를 저장하고 있다고 보는 것이 타당할 것이다.

2.2.3 개인정보보호 규제 검토 현황

앞서 살펴 본 국내 블록체인 기술 활용 분야의 특징은 은행들의 사례에서와 같이 이미 확보하고 있는 자사 고객만을 대상으로 하는 프라이빗(private) 블록체인 서비스이거나 교보생명의 사례와 같이 새로운 비즈니스를 개발하기 위한 규제 샌드박스[2] 환경을 최대한 이용하였다는 것이다. 즉, 아직까지 국내 대다수의 블록체인 기술 활용 분야는 상용화 단계까지 이르지 못했거나 개인정보 보호법제와 상충하는 블록체인의 고유한 특징을 주의 깊게 보지 않고 있는 상황이다.

1) 해시함수를 이용한 일방향 암호화 방식으로 암호화를 통해 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법

2) 신산업, 신기술 분야에서 새로운 제품, 서비스를 내놓을 때 일정 기간 동안 기존의 규제를 면제 또는 유예시켜주는 제도

이에 반해 금융투자업계의 공동인증서 서비스는 컨소시엄(consortium) 블록체인 서비스 형태로 앞서 소개했던 블록체인의 고유한 특징으로 인해 발생하는 국내 개인정보 보호법제와의 충돌을 고민하면서 대안을 찾아본 흔적들이 있다. 그 중, 스마트계약 기술을 활용한 대안은 Ⅳ장에서 설명하기로 한다.

Ⅲ. 블록체인 기술 적용의 한계

3.1 블록체인 기술의 주요 특징

첫 번째 블록체인 기술의 특징은 데이터의 비가역성(irreversibility)이다. 블록체인의 데이터 기록 방식은 Fig.1.에서 볼 수 있듯이 거래정보를 담고 있는 블록이 체인형태로 연결되어 현재 블록에서는 이전 블록의 해시값과 자신의 해시값을 함께 기록하고 순차적으로 배열되도록 하고 있다. 즉 블록들은 이전 블록 해시값을 기준으로 순차적으로 연결되기 때문에 특정 블록의 데이터를 변경할 경우 블록 간 연결이 끊어지게 되고 이 블록 간 연결 유지 여부를 통해 데이터의 조작 여부를 검증할 수 있게 된다. 이렇게 블록연결을 통해 순차적으로 데이터를 기록하는 특징을 블록체인의 비가역성이라고 한다.

두 번째 블록체인의 특징은 데이터의 공유방식이다. 블록체인은 블록체인 플랫폼을 구성하는 각각의 참여자간 플랫폼이 정한 특정한 합의구조에 따라 거래 데이터를 검증하고 검증된 데이터를 모든 참여자가 분산 저장하는 데이터 공유 방식을 취하며 이렇게 모든 참여자에게 공유되는 데이터 블록은 복사본이 아닌 원본(the original copy)으로서 가치를 가지게 된다. 즉 블록체인에 참여하는 모든 참여자는 선택의 여지없이 모두 원본 데이터를 공유하는 특징을 갖는다. Fig.2.는 이와 같은 블록체인의 데이터 공유방식을 잘 보여주고 있다.

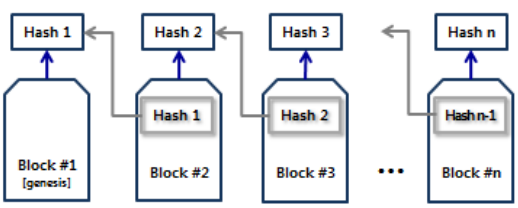

Fig. 1. Linked Listed Block

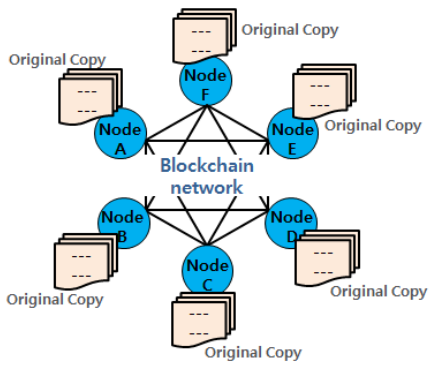

Fig. 2. Distributed Ledger - The Sharing of Original Copy

3.2 국내 개인정보 보호법제와의 충돌

3.2.1 퍼블릭 블록체인의 개인정보처리자

블록체인은 활용 목적과 데이터 관리 방식, 참여자의 범위에 따라 퍼블릭(public) 블록체인과 프라이빗(private) 블록체인, 그리고 컨소시엄(consortium) 블록체인으로 구분할 수 있다.

Table 1.은 블록체인의 유형별 특징을 정리한 것이다. 퍼블릭 블록체인은 누구나 접근 가능한 개방형 블록체인으로 채굴 등 알고리즘을 통해 거래를 증명하면서 거래 신뢰도를 높이고 익명성을 보장한다는 장점이 있어 비트코인 등 암호화폐 시장의 기반 플랫폼으로 활용되고 있고, 프라이빗 블록체인은 허가받은 사용자만 접근이 가능하도록 중앙기관에서 통제하는 형태로 기업들의 요구에 맞게 적용 가능한 기업형 블록체인이라고 할 수 있다. 컨소시엄 블록체인은 허가받은 기관 등이 공동으로 참여하여 사전 합의된 규칙으로 거래를 증명하며 권한 부여 차별화를 통해 민감한 정보를 관리할 수 있는 장점이 있다.

개인정보 보호법에서는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 개인정보처리자로 정의하고 있다[5]. 프라이빗 블록체인이나 컨소시엄 블록체인에서 개인정보를 처리하게 되는 경우 블록체인에 참여하는 업체 또는 기관들이 블록체인 운영의 주체가 되므로 이들이 블록체인에서 처리되는 개인정보에 대한 개인정보처리자로서 개인정보의 수집·이용·제공·삭제·안전조치의무 등 개인정보 보호법상의 각종 의무를 준수하여야 한다. 물론 해당 업체나 기관의 정보보호 관련 인력

Table 1. Characteristics of Type of Blockchain

Classification	Public Blockchain	Private Blockchain	Consortium Blockchain
Form	Open(Decentralization)	Personal Type	Semi-centralization
Access	Accessible to anyone	Access only to authorized users (Utilize independently in one institution)	Access only to authorized users (Cooperative participation by authorized organizations)
Proof	Algorithm based(Anonymous transaction proof such as mining)	Proof of transaction by central agency	Pre-agreed rule base(Proof of authenticated user)
Advantage	Stability, Reliability, Transparency (Decentralization, seeking decentralization)	Efficiency, scalability, and agility (Can be specialized by company)	Similar to private but differentiated by user privilege management for sensitive information
Disadvantage	Low scalability and slow trading	Less secure than public	Intervention and sustainable coordination with R & R issues per user
Application	Crypto-currency, etc.	General companies, etc.	R3CEV, etc.

또는 인프라 환경에 따라 그 수준은 달라질 수 있으나 법적 의무를 준수할 수 없다고 말하기는 어려울 것이다. 그러나 불특정 다수의 참여자들이 개인정보의 주체이자 개인정보처리자가 되는 퍼블릭 블록체인의 경우 이들에게 동일한 개인정보 보호법상의 각종 의무를 부과하는 것은 공공연하게 범법자를 양산하는 행위가 될 수 있음을 충분히 예상할 수 있다. 개인정보를 처리하여야 하는 암호화폐가 등장한다면 그 암호화폐의 거래 또는 채굴을 위해서 개인 PC를 활용하는 사람에게 개인정보처리자의 법적의무를 준수하라고 강제할 수는 없을 것이다. 결국 현행 국내 개인정보 보호법제들을 감안할 때 퍼블릭 블록체인의 경우에는 블록체인망에서 개인정보를 처리하지 않도록 주의하여야 한다.

3.2.2 개인정보의 삭제에 관한 문제점

국내 주요 개인정보 보호법제들은 모두 보유기간이 경과하거나 처리 목적이 달성된 개인정보는 파기하도록 정하고 있다[6]. 개인정보 보호법에서는 목적 달성이 된 개인정보는 데이터가 복원되지 않도록 초기화 또는 덮어쓰기를 수행하여 파기하도록 하고 있으며, 신용정보의 이용 및 보호에 관한 법률에서는 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하도록 하고 있다. 또한 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 개인정보의 수집·이용 목적을 달성하였거나 개인정보의 보유 및 이용기간이 끝난 경우, 그리고 정보통신서비스를 1년 동안 이용하지 않은 이용자의 경우에는 해당 이용자의 개인정보를 파기하도록 규정하고 있다.

그러나 블록체인에서 개인정보를 이용하는 경우에는 블록체인 데이터의 비가역성으로 인해 데이터의 삭제나 변조가 불가능하다. 체인형태로 연결되어 있는 블록체인 상에서 어떤 블록의 내용이 변경되면 그 이후의 모든 블록의 해시값이 순차적으로 변경되어야 하는데 블록체인의 데이터 저장방식은 이렇게 블록체인에 기록된 정보의 변경을 매우 어렵게, 즉 현실적으로 불가능하도록 함으로써 정보의 무결성을 보장하고 있다.

3.2.3 개인정보의 제3자 제공에 관한 문제점

국내 개인정보 보호법제들은 개인정보처리자가 수집한 개인정보를 제3자에게 제공할 경우 ① 개인정

보를 제공받는 자, ② 개인정보를 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목, ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 고지하고 정보주체의 동의를 받아야 한다[7].

제3자 제공에 대한 동의 방식은 엄격한 사전 동의를 요구하는 opt-in 방식으로 정보주체로부터 사전 동의를 받지 못한 경우에는 절대로 제3자에게 개인정보를 제공할 수 없다. 프라이빗 블록체인은 블록체인망 참여자가 중앙에서 통제하는 특정 업체나 기관으로 한정되기 때문에 제3자 제공에 대한 사전 동의에 문제가 없다. 퍼블릭 블록체인과 컨소시엄 블록체인의 경우에도 블록체인에 참여하는 개인 또는 업체가 블록체인을 이용한 서비스 개시 전에 확정되고 고정된다면 해당 참여자들을 개인정보를 제공받는 자로 특정하여 제3자 동의를 받을 수 있다. 그러나 이렇게 참여자를 한정해야 하는 비즈니스를 위해 블록체인 기술을 이용하지는 않을 것이다.

일반적인 퍼블릭 블록체인 또는 컨소시엄 블록체인의 경우 블록체인 서비스 개시 전에 고정된 참여자로 제한할 수 없기 때문에 신규 참여자가 발생할 경우 앞서 살펴본 블록체인의 데이터 공유방식은 블록체인 참여자가 블록체인에 참여를 결정하고 블록체인망에 참여노드를 연결하는 순간부터 다른 기존 참여자의 블록정보를 원본 데이터로 공유하게 된다. 따라서 국내 개인정보 보호법제의 사전 동의 의무를 준수하기 위해서는 사실상 블록체인망에 신규 참여를 결정하고 참여노드로 연결하기 전에 모든 정보주체로부터 제3자 제공에 대한 동의를 받아야 하는데 블록체인의 기존 참여자가 많을수록 컨소시엄 블록체인의 경우에는 블록체인 참여자의 거래고객이 많을수록 사전 동의는 더욱 현실적으로 불가능하다.

IV. 한계 극복을 위한 개선 방안

4.1 개인정보 보호법제 개선 방향

4.1.1 개인정보 보호법제 개선의 노력

2018년 4월 6일 권은희 의원은 거래의 기록 및 관리에 대한 권한을 중앙기관 없이 P2P 네트워크를 통해 분산하여 기록하고 저장하는 블록체인 기술의 특성 상 개별 블록에 저장된 데이터를 완전히 삭제하는 경우 블록체인 연결고리가 끊어져 시스템이 가동되지 않는 문제가 있음에도 현행 개인정보 보호법은 개인정보의 처리 목적이 달성 된 경우 정보를 파기한다고 정하고 있어, 블록체인 기술의 적용이 제한되고 있다고 지적하고 이 문제점을 개선하기 위해 Table 2.와 같이 개인정보 보호법 일부개정법률안을 대표 발의하였다[8].

Table 2. Personal Information Protection Act Revision Bill

Current	Revision bill
Article 21(Destruction of personal information) ① The personal information processor **shall destroy the personal information** without delay when the personal information becomes unnecessary, such as the elapse of the holding period and the purpose of processing the personal information. Provided, however, that this shall not apply in cases where it must be preserved in accordance with other laws.	Article 21(Destruction of personal information) ① ---------- ---------- **shall destory of the personal information or dispose the contents in a form that can not be confirmed through technical measures** ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------.

이 개정안은 개인정보 파기에 대한 의무 규정을 “기술적 조치를 통해 내용을 확인할 수 없는 형태로 폐기하는 것도 가능하도록 함”으로써, 전자적 파일에 기록된 개인정보에 대한 접근을 차단하거나 읽을 수 없는 정보로 변환하는 등 기술적 조치를 통해 개인정보를 복원이 불가능한 방법으로 영구 삭제하여 파기하지 않아도 동일한 법적 효과를 낼 수 있는 대안을 제시하였다는 데에 의의가 있다고 할 수 있다. 그러나 이 ‘기술적 조치’의 범위나 내용이 명확하지 않기 때문에 어느 수준까지가 허용되는 기술적 조치인지 블록체인 기술을 이용하려는 기업과 규제당국 간 이견 발생으로 인해 생기는 혼란은 풀어야 하는 또 다른 숙제가 될 수 있다.

4.1.2 개인정보자기결정권과 개인정보의 삭제

정보주체가 되는 개인 자신과 관련한 개인정보를 삭제하거나 그 개인정보의 처리를 제한하는 것을 주된 내용으로 하는 '잊힐 권리[3]'는 개인정보자기결정권의 하나로 간주된다[9]. 개인정보자기결정권은 특히 온라인을 통한 개인정보의 데이터베이스화를 통해 시간과 공간에 구속되지 않고 빠르고 편리하게 개인정보의 수집·이용 등 처리과정이 가능하게 되었고, 정보처리의 자동화 및 개인정보가 포함된 파일의 결합 과정을 통해 서로 다른 기관간의 정보교류가 쉬워짐에 따라 특정 기관이 수집하여 보유하고 있는 개인정보를 여러 기관이 동시에 활용하는 것이 가능하게 되었으며, 개인을 식별할 수 있는 인적 사항뿐 아니라 생활공간에서 생성되는 다양한 개인에 관한 정보를 정보주체의 의사와 전혀 무관하게 제3의 개인 또는 단체가 무한대로 축적하여 이용하거나 공개할 수 있는 새로운 정보환경에 놓이게 되었다[10].

이러한 환경의 변화는 개인정보자기결정권의 범주가 워낙 방대해지고 있다는 표현이기도 하다. 물론 끊임없이 다양해지고 범위가 확대되는 개인정보자기결정권의 영역을 정보주체가 잘 행사할 수 있도록 법적인 보장을 하는 것이 바람직한 일이라 하겠다. 그러나 오늘날 정보화 사회에서는 정보주체가 개인정보자기결정권을 잘 행사할 수 있도록 법적인 보장을 잘해 주는 것이 정보주체에게 자신의 개인정보자기결정권을 행사할 수 있는 권리를 보장하는 것과 일치한다고 주장하기는 어려울 것이다. 개인정보결정권의 권한 행사 영역이 넓어질수록 오히려 정보주체는 개인정보처리자의 개인정보처리 목적을 제대로 인지하지 못하고 어느 순간 개인정보자기결정권 행사를 위한 요청과 동의를 기계적으로 반복하는 자신을 보게 될지도 모른다.

개인정보자기결정권은 정보주체인 자신에 관한 정보가 언제, 어떤 수준으로, 무슨 목적을 위해서 타인에게 제공되고 이용될 수 있는지, 언제까지 보유할 수 있는지를 정보주체가 스스로 결정할 수 있도록 보장하는 권리이다. 즉 개인정보자기결정권은 정보주체가 스스로 자신과 관련된 개인정보를 생산한다는 의미로 이해하기보다 정보주체가 자신의 개인정보를 누가 어떤 목적으로 어느 정도의 정보를 이용할 수 있는지를 정보주체가 직접 결정할 수 있다는 의미로 이해하여야 한다. 여기서 간과하면 안 되는 것은 개인정보자기결정권은 자신과 관련한 개인정보에 타인이 접근하거나 처리하려는 것을 제한하는 데에만 그치지 않고, 일정한 범위의 사람들이 접근하여 이용할 수 있도록 허용하는 것도 포함한다는 것이다. 이러한 관점에서 개인정보와 관련한 헌법적 보호는 '개인정보' 그 자체보다는 개인정보에 대한 '자율적 통제'에 초점을 두고 이해되어야 하며, 개인정보자기결정권의 보장은 개인정보의 성격이나 개인정보를 보유하고 있는 주체 또는 개인정보를 이용하는 형태보다도 정보주체의 통제가 미치지 않는 개인정보 처리의 위험성을 더 중요하게 고려하여야 한다[11].

블록체인의 비가역성은 데이터의 위변조를 불가능하도록 하기 위한 기술적 장치이며, 이 장치를 통해 블록체인에 저장되는 데이터는 무결성과 함께 안전한 저장이라는 신뢰를 블록체인 참여자에게 제공한다. 이와 같은 블록체인의 장점을 필요로 하는 정보주체가 블록체인 기술의 선택 대신 개인정보의 삭제에 대한 '잊힐 권리'를 일부 포기하는 것은 스스로의 '자율적 통제'의 영역으로 볼 수 있으며, 이 자율적 통제에 관한 정보주체의 권리는 개인정보자기결정권의 영역으로 보장받을 수 있어야 한다.

4.1.3 개인정보권과 이익형량

개인정보는 '보호'와 '활용'의 균형점을 찾는 것이 중요하다. 특히 '대량 생산 및 대량 소비'를 특징으로 하는 기존의 산업구조를 데이터 처리 기술의 혁신을 바탕으로 '맞춤 생산 및 맞춤 소비'로 전환하게 하는 4차 산업혁명시대에서는 개인정보의 활용이 더욱 강조되기 때문에 이러한 균형점을 찾기 위한 논쟁과 연구가 더 많이 요구된다. 이 때문에 개인정보자기결정권은 자신과 관련한 개인정보에 타인이 접근하거나 처리하려는 것을 제한하는 데에만 그치지 않고, 일정한 범위의 사람들이 접근하여 이용할 수 있도록 허용하는 것도 포함한다는 것에 한 번 더 주목해 볼 필요가 있다. 다른 말로 표현해 보면 개인정보자기결정권은 또 다른 헌법적 권리에 해당하는 '알 권리'와의 충돌을 피할 수 없다는 것이다.

개인정보를 둘러싼 권리관계는 개인정보를 정보주체의 권리 대상으로 정의하는 것에서 출발하여 정당

3) 국내에 이 용어가 번역되어서 소개될 당시 '잊혀질 권리'로 전해져 통용되고 있지만 문법상 '잊혀질 권리'는 표준어가 아니다. '잊다'의 피동형은 '잊히다'이고 피동형에 '~ㄹ' 형용사형 어미를 붙여 조어를 하면 '잊힐 권리'가 바른 표현이므로 여기서는 '잊힐 권리'로 사용하도록 한다.

한 권리를 가진 개인정보 이용자도 법적 보호 대상으로 삼아야 할 필요가 있다. 개인정보자기결정권만으로 개인정보를 둘러싼 권리관계를 수용하기 어렵다는 이유로 '개인정보권'이라는 중립적 개념이 제시되었다. 개인정보권은 "개인정보에 관한 권리로서 정보주체의 자신의 정보에 대한 결정권과 타인의 개인정보에 대한 접근 및 활용 등 처리에 관한 권리"라고 정의하고, 기본적으로 개인정보자기결정권의 개념을 그대로 인정하면서 개인정보를 정당하게 이용하는 타인의 권리 또한 정보주체의 개인정보자기결정권이 제한됨에 따른 반사적인 이익이 아닌 타인의 법적 권리에 해당하는 대상임을 분명히 하였다[12].

개인정보권은 개인정보자기결정권에서 정보주체의 권리를 폭넓게 인정하게 됨에 따라 적법한 개인정보의 이용권을 부여 받은 타인의 권리가 침해되거나 무시될 수 있음을 고려하여 이러한 적법한 타인의 권리를 보장할 수 있도록 개인정보자기결정권에서 편향된 권리의 무한확장에 한계를 두는 개념이라고 볼 수 있다. 4차 산업혁명시대에 맞닥뜨린 오늘날 정보화 사회는 정보주체가 인지하고 본인이 생산한 개인정보는 물론 상거래를 비롯한 다양한 경제활동의 흔적으로 정보주체의 의사와 무관하게 생성되어 온라인에 기록되는 개인정보까지 모든 경우에 대하여 '잊힐 권리'를 보장하라는 정보주체의 요구를 현실적으로 완벽히 수용할 수 없으며, 정보주체의 의사표시를 이미 확인한 제3자의 '기억할 수 있는 권리'조차 보장할 수 있어야 한다. 블록체인 환경에서 블록체인 트랜잭션을 기록하는 개별 블록을 기억할 수 있는 권리를 가지는 주체로 인정할 수 있다면 데이터의 비가역성에 따른 개인정보의 삭제 불가 문제점에 대한 실마리를 풀 수 있을 것이다.

개인정보 침해사건을 다루는 법정에서 종종 등장하는 법적용어로 이익형량이라는 말이 있다. 이익형량이란 충돌하는 이익 중 어느 이익이 더 우월한지를 밝히는 것을 의미하며 이익형량을 위법성 판단내지 위법성조각의 원칙으로 내세우는 견해를 이익형량설이라고 한다[13]. 이익형량을 고려한다는 것은 개인정보의 보호와 활용의 균형점을 찾는 것으로 이해할 수 있다. 오늘날 정보사회는 개인정보를 보호하기 위한 획일적인 기준을 제시하기보다 개별 사안에 따라 개인정보 침해 위험의 경감과 같이 법적 규제로 얻을 수 있는 이익과 블록체인 기술을 활용할 수 있는 산업의 위축과 같은 법적 규제로 제한되는 이익의 형량(balancing)을 충분히 고려하여야 한다.

4.1.4 개인정보 이동권

유럽은 GDPR(General Data Protection Regulation)에서 개인정보 이동권 또는 데이터 이동권(right to data portability)을 보장하는 내용을 신설하였는데 개인정보 이동권이란 정보주체인 개인이 자신의 목적을 위해 여러 서비스에 흩어져 있는 개인 데이터를 이동시킴으로써 재사용 할 수 있게 요구할 수 있는 권리로 정의할 수 있다. GDPR의 개인정보 이동권은 국내 개인정보 보호법의 제17조(제3자 제공 관련), 제18조(목적외 이용·제공 관련), 제19조(국외 이전 관련)와 관련성이 있는 것으로 생각해 볼 수 있으나, GDPR은 빅데이터의 활성화의 영향으로 온라인 서비스에서의 정보주체의 선택권을 확대하기 위해 신설된 조항이라는 점에서 그것들과는 다르다고 할 수 있다[14]. 즉 국내 개인정보 보호법은 개인정보처리자가 정보주체의 동의 등에 의해 개인정보를 처리하도록 하고 있는데 반해 GDPR의 개인정보 이동권은 자동화된 수단에 의해 처리되는 것을 전제로 정보주체가 선택권을 가지고 주도적으로 자신의 정보를 제3자에게 제공할 것을 요청할 수 있다는 점에서 차이가 있다.

금융분야 빅데이터 활성화를 위한 '금융분야 데이터활용 및 정보보호 종합방안'을 발표하고 금융분야 데이터산업 경쟁력 강화를 추진하고 있는 금융위원회는 2018년 7월 19일 '금융분야 마이데이터 산업[4] 도입방안 발표'라는 보도자료를 통해 GDPR의 개인정보 이동권을 국내 신용정보의 이용 및 보호에 관한 법률 체계에 맞추어 국내에서 수용하기로 하였으며, 이를 위해 정보주체가 본인정보를 능동적·적극적으로 활용할 수 있도록 '개인신용정보 이동권'을 도입하기로 하였다. 2018년 10월 현재 정부는 신용정보의 이용 및 보호에 관한 법률 개정 등 관련 세부과제를 추진 중이다.

GDPR의 개인정보 이동권이나 신용정보의 이용 및 보호에 관한 법률의 개정을 통해 도입하려고 하는 개인신용정보 이동권은 결국 그동안 국내의 개인정보

4) 금융 분야의 '마이데이터 서비스'는 국내 핀테크산업의 활성화를 위해 제안되었으며 정보주체가 개인신용정보 이동에 동의하는 경우 은행·카드·통신회사에 흩어져 있는 개인의 신용정보를 마이데이터 사업자에게 이동시켜서 한 번에 쉽게 조회하고 신용관리까지 할 수 있도록 하는 서비스이다. 마이데이터 서비스를 통해 본인 신용정보의 체계적인 관리를 지원하고 소비패턴 등을 분석하여 개인의 신용관리·자산관리 서비스를 제공한다.

보호법제가 정보주체의 개인정보를 보호하기 위해 개인정보처리자에게 정보주체의 동의를 요구하던 방식에서 정보주체가 자신의 개인정보의 이동을 개인정보처리자에게 주도적으로 요구하는 형태로 바뀌는 것이라고 할 수 있다. 이러한 개인정보 이동권 또는 개인신용정보 이동권을 블록체인 기술에 적용한다면 블록체인 서비스를 이용하고자 하는 정보주체는 블록체인 기술을 통한 더욱 효과적인 서비스를 위해 블록체인에 참여하는 모든 참여자에 대해(그것이 기존 참여자이든지 신규 참여자이든지 상관없이) 단 한 번의 동의로 자신의 개인정보를 이동시킬 수 있도록 할 수 있을 것이다.

4.1.5 개인정보의 위수탁 여부와 공동관리

국내 개인정보 보호법제는 개인정보처리자가 개인정보를 처리함에 있어서 본인의 이익과 목적을 위해 개인정보를 제3자에게 이전하는 행위는 '개인정보의 위수탁'으로 정의하고 있으며, 제3자의 이익과 목적을 위해 개인정보를 제공하는 행위는 '개인정보의 제3자 제공'으로 규정하고 있다. 개인정보의 위수탁인 경우에는 위탁 내용을 개인정보처리방침 등을 통해 공개하는 것만으로도 정보주체에 대한 통지의무를 다하는 것으로 볼 수 있지만, 제3자 제공인 경우에는 개인정보처리자가 정보주체로부터 '사전 동의'를 받아야 한다.

이와 같이 개인정보의 공동사용에 대해서 위수탁 또는 제3자 제공으로 구분하여 각기 다른 법률적 요건을 규정하고 있는 것은 바람직하다고 볼 수 있다. 그러나 국내 개인정보 보호법제의 개인정보 공동사용에 대한 접근은 동일한 목적을 가지고 동일한 개인정보를 공동으로 관리하는 복수의 개인정보처리자에 대한 고려사항이 없다는 문제점이 있다. 해외 개인정보 보호법제에서는 개인정보 공동관리에 대한 개념을 규정하고 있는 것과 대조적이라고 할 수 있다.

EU GDPR은 제26조에서 '공동 컨트롤러(joint controller)'라는 개념을 정의하고 있다. 둘 이상의 컨트롤러가 공동으로 개인정보 처리 목적과 수단을 정하는 경우 공동 컨트롤러가 되고, 공동 컨트롤러는 당사자 간 합의를 통하여 정보주체의 권리 보장 등 GDPR에 따른 책임에 대하여 각자의 의무를 투명하게 결정하여야 하는데 이러한 컨트롤러 간 합의의 본질적 내용은 정보주체에게 공개되어야 한다[15]. 예를 들어 여행사, 항공사, 호텔이 여행·항공·숙박을 결합한 형태의 인터넷 사이트를 공동으로 운영하고 개인정보를 공동으로 활용하며, 보호책임을 상호 분배하는 형식으로 운영하는 경우에는 공동 컨트롤러에 해당한다. 컨소시엄 블록체인의 경우 블록체인 서비스 별 블록체인 참여자들은 GDPR의 공동 컨트롤러의 자격요건이 가능하므로 GDPR 관점에서는 블록체인의 원본데이터 공유방식에 따른 제3자 제공에 대한 문제점을 해결할 수 있을 것으로 판단된다.

일본의 개정 개인정보 보호법에서도 개인정보의 공동관리에 대한 개념을 찾아볼 수 있다. 제23조제5항제3호를 보면 "특정한 자와의 사이에서 공동으로 이용하는 개인데이터가 당해 특정한 자에게 제공되는 경우로서, 그 취지 및 공동으로 이용되는 개인데이터의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인데이터의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때"에는 제3자 제공으로 보지 않는다[16]. 이런 경우에 해당하는 복수의 개인정보처리자를 '공동이용자'라고 하며 공동이용자는 정보주체의 동의 없이 개인정보를 제공 받을 수 있다. EU GDPR처럼 일본의 개정 개인정보 보호법의 공동이용자의 개념으로도 컨소시엄 블록체인의 경우 원본데이터 공유방식에 따른 제3자 제공에 대한 문제점을 해결할 수 있을 것으로 판단된다.

아직 개인정보의 공동관리에 대한 대비가 부족한 국내 상황에서는 블록체인의 원본데이터 공유방식을 제3자 제공이 아닌 개인정보의 위수탁으로 볼 수 있다면 제3자 제공에 대한 사전 동의 규제를 적용받지 않을 수도 있다. 컨소시엄 블록체인에서 제공하는 서비스에 참여하고 있는 참여자 A, B, C가 있다고 할 때 신규 참여자 D가 등장한 경우 참여자 A의 고객 x의 개인정보는 원본데이터 공유에 따라 자동으로 D의 블록체인 서버에 저장된다. 그러나 참여자 D는 고객 x의 개인정보를 D가 제공하는 블록체인 서비스에 이용하지 않고 단지 A, B, C가 참여하는 블록체인 서비스에 대한 블록 생성작업[5] 및 블록체인의

5) 블록체인은 중앙 통제자가 없기 때문에 블록을 생성할 때 블록의 생성권을 누구에게 주는가가 중요하다. 시빌 공격(sybil attack)은 네트워크 해킹 공격 방법의 일종으로 어떤 특수 목적을 이루기 위해 한 사람이 여러 사람의 행위인 것으로 속여 네트워크를 공격하는 방법이며 이 공격을 통해 블록 생성권을 독점할 수 있기 때문에 이 공격을 방지하기 위해 블록체인은 시빌 통제 메커니즘(sybil control mechanisms)을 가지고 있다. 여기에는 작업증

합의 메커니즘[6]을 수행하는 용도로만 사용한다면 참여자 A의 이익과 서비스 제공을 목적으로 x의 정보를 D에 제공한 것이 되므로 A가 D에게 x의 개인정보를 제공한 행위는 개인정보의 위수탁으로 해석할 수 있다. 결국 A는 개인정보처리방침 등을 통해 D에게 개인정보를 위탁한다고 통지하는 것으로 법의 준수가 가능하다. 다만 신규 참여자 D가 A, B, C가 참여하고 있는 블록체인 서비스에 참여하는 것만으로도 자신의 이익을 발생시킬 수 있다면 A가 D에게 x의 개인정보를 제공한 행위는 개인정보의 위수탁이 아닌 제3자 제공으로 보아야 할 것이며 A는 D에게 x의 개인정보를 제공하기 전에 x로부터 제공에 대한 동의를 받아야 한다. 그러나 일반적으로 D는 A, B, C가 참여하고 있는 블록체인 서비스에 참여하는 것만으로는 x의 개인정보를 처리함으로써 자신이 얻을 수 있는 이익은 없을 것이다. 오히려 D가 x에게 이 컨소시엄 블록체인의 서비스를 제공하는 경우에는 D가 x에게 서비스를 개시하기 전에 x로부터 개인정보의 수집·이용에 대한 동의를 받는 것으로 법적인 의무를 이행할 수 있을 것이다.

4.1.6 포괄적 동의 및 옵트아웃(opt-out)

4차 산업혁명 시대의 중요한 특징 중 하나가 빅데이터 환경이다. 정보주체의 온라인상에서의 관심사와 행동, 모바일 기기를 통한 위치정보, 그리고 사물인터넷 기기의 각종 센서를 통해 방대한 양의 데이터가 실시간으로 축적되고 있으며 현대 정보통신기술의 빠른 발전은 기하급수적으로 데이터의 축적을 늘려가고 있다. 이런 환경에서 정보주체가 인지하지 못하는 정보의 생성과 수집 내역을 정보주체에게 일일이 통지하고 동의를 받는다면 그 양이 워낙 방대하므로 정보주체의 인식 범위를 벗어나게 될 수 있으며, 이 경우 정보주체로서는 자신의 개인정보 처리에 대한 인식을 못한 것과 다를 바가 없게 된다.

개인정보자기결정권의 선택권을 제한한다는 것 때문에 현행법은 '포괄적 동의'를 금지하고 있다. 그러나 EU GDPR에서는 '수령인(recipient)'의 범주에 해당하는 경우 개인정보 제공에 대한 포괄적인 사전 동의가 가능하도록 하고 있다. 수령인은 제3자인지 여부와 관계없이 개인정보를 공개·제공받는 자연인이나 법인, 정부부처 및 관련기관, 기타 단체 등을 의미하며 컨트롤러는 수령인 또는 수령인의 유형을 사전에 식별하여 정보주체에게 그들의 개인정보가 어떤 수령인에게 공개·제공되었는지 알려 주어야 한다[17]. 즉 장래의 예상되는 블록체인 참여자들을 수령인의 범주로서 포괄적으로 기재하여 미리 동의를 받으면 개인정보 제3자 제공에 대한 법적 요건을 갖출 수 있다.

엄격한 사전 동의를 의무화 하고 있는 opt-in 방식의 국내 개인정보보호 규제는 오늘날 정보사회에서 특히 빅데이터 환경을 지향하는 입장에서 현실적으로 불가능하고 규제의 효용성에도 문제가 있다는 의문을 제기한 사례가 있으며[18], 미국의 경우에는 미국의 금융지주회사법에 해당하는 GLB Act(Gramm Leach Bliley Act)에서 포괄적 예외(disclosure pursuant to opt-out)를 통해 제3자 제공을 opt-out이 적용되는 것으로 규정하고 있다. 금융기관은 고객에게 정보가 제3자에게 공개될 수도 있음을 서면으로 알리고, 정보공개를 하지 않을 권리가 고객에게 있음을 알리며, 비공개를 원할 경우 이에 대한 절차를 고객에게 설명함으로써 포괄적 예외로 고객의 정보를 공개할 수 있게 된다[19].

4.1.7 소결

블록체인망에서 개인정보를 이용하려고 할 때 데이터의 비가역성에 따른 개인정보의 삭제 불가 문제점은 우선 개인정보자기결정권에 있어서 개인정보의 성격이나 개인정보를 보유하고 있는 주체 또는 개인정보를 이용하는 형태보다도 정보주체의 통제가 미치지 않는 개인정보 처리의 위험성을 더 중요하게 고려하여 개인정보에 대한 정보주체의 '자율적 통제'의 입장에서 블록체인 기술의 장점을 활용하고자 하는 정보주체가 개인정보의 삭제에 대한 '잊힐 권리'를 일부 포기하는 것은 자율적 통제에 관한 정보주체의 개인정보자기결정권이라는 것을 충분히 고려하는 개인정보 보호법제의 개선 검토가 필요하다. 또한 '잊힐 권

명(PoW, Proof of Work), 지분증명(PoS, Proof of Stake), 위임지분증명(DPoS, Delegated Proof of Stake) 등이 있으며 이 메커니즘을 수행하기 위해서는 블록체인 참여자의 역할이 필요하다.

6) 합의 메커니즘(consensus mechanisms)이란 블록체인에서 생성되는 여러 블록들 중 어떤 블록을 진짜 블록으로 판단할지를 결정하기 위한 의사결정방식이다. heaviest/longest chain selection, PBFT (Practical Byzantine Fault Tolerance), tendermint 등이 있으며 이 합의 메커니즘 수행을 위해서는 블록체인 참여자의 역할이 중요하다.

리'를 보장하라는 정보주체의 요구를 완벽하게 수용할 수 없는 오늘날의 정보화 사회에서 정보주체의 의사표시를 이미 확인한 제3자의 '기억할 수 있는 권리'의 중요성을 제시하고 있는 '개인정보권'의 개념도 적극적으로 검토할 필요가 있다.

블록체인망에서 개인정보를 이용하려고 할 때 원본데이터 공유방식에 따른 개인정보의 제3자 제공에 대한 사전 동의가 불가능한 문제점은 GDPR의 '개인정보 이동권'이나 국내에서 추진 중인 '개인신용정보 이동권'에 대한 적극적인 해석을 통한 해결방안을 검토해 볼 수 있다. 그러나 신규 참여자가 블록체인망에 참여노드를 연결하는 순간 원본데이터의 공유가 발생하므로 그 전에 사전동의를 완료하기 위해서는 이동권을 행사하기 위한 주체를 기존 블록체인 서비스 참여자로 하여야 한다는 입장에서 2018년 10월 현재 정부가 추진 중인 '개인신용정보 이동권' 행사방식과는 다소 차이가 있다. 또한 제3자 제공에 대한 문제점 해결을 위해 GDPR의 '공동 컨트롤러'와 일본 개인정보 보호법의 '공동이용자'의 개념을 국내 개인정보 보호법제에 반영하기 위한 노력도 필요하다. 아울러 GDPR에서 '수령인의 범주'에 대한 포괄적 동의를 허용하고 있는 점과 미국이 제3자 제공을 Opt-out 규제방식으로 채택하고 있는 점은 국내에서도 제공 대상의 범위를 신중하게 고려하여 적용여부를 검토해 볼 필요가 있다.

개인정보처리가 필요한 업무에 블록체인 기술을 적용하려는 기업이나 기관은 블록체인을 통한 원본데이터 공유를 개인정보의 위수탁으로 볼 수 있다는 가능성을 열어 두고 비즈니스 개발과 함께 법적 규제 준수를 위한 방법을 심도 있게 고민해 보아야 한다.

또한 법적 규제에 블록체인 기술 적용에 대한 예외를 적용함으로 블록체인 산업의 부흥이 가져올 이익과 여전한 법적 규제를 통한 개인정보 침해 위험의 경감 사이에 공정하고 객관적인 이익형량을 법정에서만이 아닌 현실적인 규제 적용환경에서 먼저 따져보아야 한다.

4.2 개인정보의 삭제에 대한 기술적 대안

4.2.1 검토 가능한 기술적 대안

지금까지 논의되고 있는 개인정보의 삭제에 대한 기술적인 대안은 오프체인 스토리지(off-chain storage), 블랙리스팅(blacklisting), 하드포크(hard fork) 방식의 세 가지 정도로 요약할 수 있다[20].

오프체인 스토리지는 암호화폐의 거래에서 수수료 비용을 낮추고 트랜잭션 속도를 높이기 위해 활용되는 기술로 블록체인에서 개인정보를 저장할 때 블록 내에 저장하지 않고 블록 밖에 저장하여 필요시 블록체인의 해시값의 일치여부를 확인한 후 사용할 수 있다[21]. 오프체인 스토리지는 개인정보를 블록 외부에 저장하기 때문에 개인정보의 삭제에 대한 법적 요구사항을 충족할 수 있다. 그러나 블록 내 데이터의 저장을 통한 데이터의 무결성을 보장할 수 없기 때문에 해킹이나 정보조작의 위험이 있으며, 블록체인의 탈중앙화 속성을 파괴하면서까지 블록체인 기술을 이용해야 할 필요성이 있을지 의문이 남는다.

블랙리스팅 방식은 블록체인에 개인정보를 저장할 때 사용한 암호키를 파기하여 해당 개인정보에 대한 조회 또는 접근을 할 수 없도록 만드는 기술로 블록체인 내 개인정보를 삭제하지 않고 해당 정보에 대한 접근 자체를 강제로 차단해 버린다. 블랙리스팅 방식은 GDPR에서 규정하고 있는 개인정보의 삭제권(right to erasure) 및 정정권(right to rectification)을 준수하기 위한 블록체인 활용 방안으로 제시된 사례도 찾아볼 수 있다[22]. 그러나, 개인정보의 암호키를 개인별로 관리하여야 하는 어려움과 암호키 관리의 신뢰성에 문제가 될 수 있는 단점이 있으며, 블록체인 내 개인정보의 삭제 없이 접근 자체를 막는 것이 법적인 삭제의 개념으로 인정할 수 있는 행위인지 여전히 의견이 분분하다.

하드포크는 기존 블록체인에서 분기를 통해 새로운 블록체인을 생성하는 기술로 블록체인에 참여하는 각 노드 간 합의에 따라 하드포크를 실시하고 기존의 블록체인은 파기하는 방식이다. 즉, 하드포크 결과를 통해 기존의 블록체인에 저장되어 있는 개인정보는 파기할 수 있게 된다. 그러나 하드포크를 실행하기 위해서는 블록체인 참여자의 전원 합의 과정이 필요하기 때문에 현실적으로 어렵고, 개인정보의 삭제 이슈가 있을 때마다 하드포크를 실행하여야 하는 관리의 비효율성으로 인해 개인정보 삭제에 대한 기술적 대안으로 검토는 해 볼 수 있겠지만 실현 가능성은 현저히 낮다고 보아야 할 것이다.

4.2.2 스마트계약 기술 활용 제안

개인정보의 삭제에 대한 법적 문제를 해결하기 위

한 새로운 기술로 블록체인의 스마트계약(smart contract) 활용 방안을 고려해 볼 수 있다.

스마트계약은 블록체인의 모든 참여자의 장부의 상태를 변경하는 방식으로 블록체인 상에 자동화된 방식으로 실행되는 프로그래밍 코드를 의미한다. 즉 스마트계약은 기록된 계약을 보관하고, 이행하고, 집행하는 컴퓨터 프로그램이다. 스마트계약은 컴퓨터 과학자 닉 자보에 의해 1994년에 최초로 소개되었으며 인터넷에서 낯선 사람들과 전자상거래 프로토콜을 설계하는 것과 이와 관련한 '고도로 진화된' 관행을 도입하려는 목표를 추구했다[23].

본 기술 활용 제안의 전제 조건은 다음과 같다.

1. 블록체인의 블록을 생성하고 저장하는 영역(blockchain storage)의 접근은 스마트계약을 통해서만 가능하다.
2. 스마트계약을 통해 자동 실행된 결과 값은 별도의 저장소(SCORE storage)에 최신정보를 기록하고, 블록체인의 저장공간(blockchain storage)에 이력정보를 기록한다.
3. 스마트계약 실행결과를 기록하는 저장소(SCORE storage)의 접근은 스마트계약을 통해서만 가능하다.
4. Fig.3.과 같은 구성이 가능한 블록체인 플랫폼에서만 적용 가능한 기술이다.

블록체인 저장소와 스마트계약, 그리고 스마트계약 저장소의 구성은 Fig.4.와 같다. 스마트계약에서 사전에 약속된 작업이 수행되면 수행 내역은 블록체인 저장소에 저장되고, 최종 수행 결과 값은 스마트계약 저장소에 기록된다.

개인정보의 삭제절차는 다음과 같다.

1. 특정 정보주체의 개인정보의 삭제요청을 받으면 스마트계약은 블록체인저장소에 삭제요청블록을 생성한다.
2. 이 블록에 의해 스마트계약이 자동으로 실행되어 블록체인저장소에는 삭제이력블록을 생성하고 스마트계약 저장소에서는 해당 개인정보를 완전 삭제 처리한다.

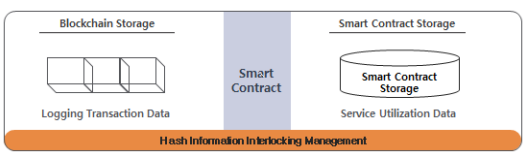

Fig. 3. Blockchain Diagram

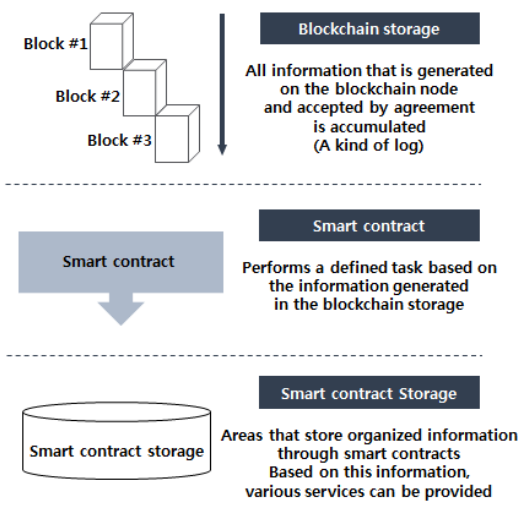

Fig. 4. Relationship of Storage and Smart Contract

이렇게 되면 결과적으로 최종 결과 값을 저장하는 스마트계약저장소에는 삭제 요청된 정보주체의 개인정보는 모두 삭제되고 스마트계약에 의해 삭제 처리된 작업 내용은 블록체인저장소에 기록된다. 실제로는 블록체인저장소에 정보주체의 개인정보가 남아 있으므로 완전 삭제가 아니라고 볼 수 있지만 이 저장소의 접근은 스마트계약에 의해서만 가능하고 스마트계약의 접근은 스마트계약저장소에 있는 정보를 기준으로 이력조회를 할 수 있기 때문에 블록체인저장소에 남아 있는 개인정보는 쓸모없는 정보가 된다.

만약 블록체인저장소에 있는 정보까지 완전삭제를 요구한다면 개별 정보의 삭제는 불가능하지만 특정 시점을 기준으로 그 이전의 블록들은 블록체인 체크아웃 기능을 통해 삭제하고자 하는 블록까지 해시 처리하여 하나의 블록으로 묶고 다음 블록을 새로운 제너시스 블록으로 지정한 후 새로 묶어서 생성한 블록을 완전 삭제하는 방식으로 삭제할 수도 있다.

V. 결 론

5.1 결론

본 연구에서는 먼저 블록체인 기술의 두 가지 특징인 비가역성과 정보의 분산 공유를 살펴보고 이 특징들이 국내 개인정보 보호법제의 내용 중 개인정보

의 삭제와 제3자 제공에 대한 사전 동의에 있어서 이해 상충되고 있음을 분석하였다. 이러한 내재적인 문제점이 국내 블록체인 기술의 상용화 서비스가 아직 많지 않은 이유와 연관성이 있음을 추론해 보았다. 또한 블록체인 기술과 개인정보 보호법제의 충돌을 피하기 위해 개인정보의 삭제와 제3자 제공에 대한 사전 동의 규정에 대한 개선방향을 제시하였다. 블록체인망에서 신규 참여자에 대한 원본데이터의 공유방식이 제3자 제공이 아닌 위수탁으로 볼 수 있다는 논리를 제시한 것과 정보의 삭제가 불가능한 블록체인의 비가역성을 파괴하지 않으면서도 법적인 삭제의 의무를 할 수 있는 기술적 대안을 제시한 것은 신선한 접근이 될 수 있을 것이다.

본 연구를 통해 블록체인 기술의 장점을 최대한 활용할 수 있는 여러 다양한 비즈니스가 발굴되고 4차 산업혁명 시대에 맞는 국내 개인정보 보호법제의 개선방향이 꾸준히 논의되는 계기가 되기를 바란다.

5.2 연구의 한계 및 발전 방향

본 연구는 개인정보 보호법제의 개선방향만을 다루고 있다. 또한 스마트계약 기술을 응용한 개인정보의 삭제 방안도 여러 제약조건을 만족하는 기술구조에서만 가능하다는 것을 전제하고 있다. 따라서 법제에 대한 개선은 실제 관련 분야의 전문가들을 통한 보다 더 심도 있는 논의가 이어져서 본 연구에서 다루지 못한 여러 타 법에 관한 충돌 문제도 해결방안을 마련해 갈 수 있는 계기가 되기를 희망한다. 또한 스마트계약 기술을 이용한 블록체인 서비스의 다양한 시도도 꾸준히 이어져서 국내 블록체인 기술 환경이 4차 산업혁명 시대에 세계를 선도하는 장이 되기를 기대한다.

References

[1] Jung-kyoon Kim, Bo-kyung Kim and Yu-jin Lee, "The effects and implications of blockchain on industry and international trade," IIT TRADE FOCUS-2018-14, pp. 29, April 2018.

[2] Jae-sung Kim and Seong-chul Lim, "A study on possibility of international trade by using of block chain," The International Commerce & Law Review, 75, pp. 140, Aug. 2017.

[3] National Law Information Center, "Personal information protection act article 2," http://www.law.go.kr/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95#undefined, Oct. 2018.

[4] Joint governmental ministry, "Personal information non-identification action guidelines," pp.4, June 2016.

[5] National Law Information Center, "Personal information protection act article 2," http://www.law.go.kr/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95#undefined, Oct. 2018.

[6] National Law Information Center, "Personal information protection act article 21," http://www.law.go.kr/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95#undefined, "Credit information use and protection act article 29," http://www.law.go.kr/LSW/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EC%8B%A0%EC%9A%A9%EC%A0%95%EB%B3%B4%EC%9D%98%20%EC%9D%B4%EC%9A%A9%20%EB%B0%8F%20%EB%B3%B4%ED%98%B8%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0#undefined, "Act on promotion of information and communications network utilization and information protection, etc. article 20-2," http://w

ww.law.go.kr/LSW/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%20%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%20%EB%B0%8F%20%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%20%EB%93%B1%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0#undefined, Oct. 2018.

〔7〕 National Law Information Center, "Personal information protection act article 17," http://www.law.go.kr/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95#undefined, "Credit information use and protection act article 32," http://www.law.go.kr/LSW/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EC%8B%A0%EC%9A%A9%EC%A0%95%EB%B3%B4%EC%9D%98%20%EC%9D%B4%EC%9A%A9%20%EB%B0%8F%20%EB%B3%B4%ED%98%B8%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0#undefined, "Act on promotion of information and communications network utilization and information protection, etc. article 24-2," http://www.law.go.kr/LSW/lsSc.do?tabMenuId=tab18&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%20%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%20%EB%B0%8F%20%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%20%EB%93%B1%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%95%EB%A5%A0#undefined, Oct. 2018.

〔8〕 Bill Information, "〔2012932〕Personal information protection act revision Bill," http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T1K8E0W4H0J6T0N9P4F5F0P4R4I5P6, April 2018.

〔9〕 Chris Conley, "The right to delete," 2010 AAAI(the Association for the Advancement of Artificial Intelligence) Spring Symposium Series, Palo Alto, California: AAAI Publications, pp. 54, http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482, March 2010.

〔10〕 Min-Yeong Lee, "So called 'right to be forgotten' and personal data protection," A Collection of Law Treatises 20.1, pp.70, April 2013.

〔11〕 Geon-Bo Kwon, "A study on the scope of personal information and the right to self-determination over personal information," Public Law Journal, pp.201, Aug. 2017.

〔12〕 Hun-Yeong Kwon, Sang-Pil Yoon and Seung-Jae Jeon, "Conceptual review of PIR and its legal framework in the age of fourth industrial revolution," The Justice, pp.21-23, Feb. 2017.

〔13〕 Ki-Won Lee, "A study on balancing of profit in the cause of fraud sculpture," Journal of Law of Chosun University, 18(2), pp.326, Aug. 2011.

〔14〕 Su-Young Cho, "A study on privacy protection in the EU's GDPR and Korea's personal information protection act," Kyungpook National University Law Journal, 61, pp.137, April 2018.

〔15〕 Ministry of the Interior and Safety, Korea Communications Commission, Korea Internet & Security Agency, "EU GDPR guide book for our companies," pp.70, May 2018.

〔16〕 Kyungsung University Industry-

Academia Collaboration Foundation, Personal Information Protection Commission, "A study on the policy analysis of personal information protection law in Japan," pp. 167-168, Dec. 2017.
〔17〕 Ministry of the Interior and Safety, Korea Communications Commission, Korea Internet & Security Agency, "EU GDPR guide book for our companies," pp.22, May 2018.
〔18〕 Hun-Yeong Kwon, Sang-Pil Yoon and Seung-Jae Jeon, "Conceptual review of PIR and its legal framework in the age of fourth industrial revolution," The Justice, pp. 34-35, Feb. 2017.
〔19〕 Ji-Su Lee, "Introduction to the Gramm-Leach-Bliley Act ('GLB Act') in the United States," Economic Reform Research Institute, pp.11, June 2004.
〔20〕 Kyung-hwan Kim, "Destruction of personal information in a blockchain environment," IT Chosun, http://it.chosun.com/site/data/html_dir/2018/06/19/2018061900075.html, June 2018.
〔21〕 Andries Van Humbeeck, "The blockchain-GDPR paradox," TheLedger, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047, Nov. 2017.
〔22〕 BCDiploma, "When the right to be forgotten becomes possible on the ethereum blockchain," NEWS BTC, https://www.newsbtc.com/press-relea323ses/bcdiploma-right-to-be-forgotten-ethereum-blockchain, Nov. 2017.
〔23〕 Don Tapscott and Alex Tapscott, The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, Portfolio Penguin, May 2016.

〈저자소개〉

최 용 혁 (Yong-hyuk Choi) 정회원
2001년 2월: 숭실대학교 정보통신공학과 졸업
2017년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융보안, 정보보호정책, 개인정보보호, IT감사, 블록체인

권 헌 영 (Hun-yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 졸업
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2015년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부