영남대학교 법학연구소
「영남법학」 제47(2018.12) 199~237면.
Yeungnam Univ. Law Journal
Vol.47 (December. 2018) pp.199~237.

블록체인과 개인정보보호
- 블록체인의 매직(Magic)과 법적 도전 -

박 진 아*

< 목 차 >

Ⅰ. 서론

4차 산업혁명의 기반 기술의 하나로 알려진 블록체인 기술은 최근 집중형 온라인 서비스가 안고 있는 많은 문제를 해결할 수 있는 분산형 인터넷으로 기대를 모으고 있다. 세계 스타트업들은 블록체인을 사용하는 소프트웨어를 개발하고 개념 증명(Proof-of-Concept, PoC)을 수행하기 위해 전통적인 자금 조달과 토큰 발급 방법을 사용하고 있다.

블록체인 기술의 주요 장점으로는 개인간 거래를 가능하게 하는 탈중개성(脫仲介性), 손쉽게 활용할 수 있는 확장성(scalability), 모든 사용자가 거래장부를 분산, 저장 관리하는데 따른 뛰어난 보안성(security), 높은 투명성(transparency)을 들 수 있다.[1] 그러나, 모든 노드에서 블록체인을 통과하는 정

* 기술과법연구소 소장, 법학박사 · SJD.
1) 정승화, "블록체인 기술기반의 분산원장 도입을 위한 법적 과제-금융산업을 중심으로-", 「

보를 볼 수 있고 블록에 저장된 정보는 제거할 수 없다는 특징이 개인정보보호의 중요한 원칙을 규정한 개인정보보호법과 충돌할 수밖에 없다. 많은 클라우드 환경에서 그렇듯이 블록체인 관리자는 개인 데이터가 블록체인에 있는지, 그리고 그 데이터가 중요한지를 알 수 없다. 블록체인은 이전 블록을 가리키는 해시, 암호화된 거래 데이터 및/또는 체인 외부에 저장된 데이터를 가리키는 해시를 표시하기 때문이다. 데이터 보호의 관점에서 볼 때 블록체인의 특징은 시스템 고유의 것이 아니며 기술 설계가 수정될 경우 어느 정도 회피될 수 있다. 그러나 개인정보침해를 회피하는 설계는 블록체인의 장점을 훼손하는 딜레마가 있다.

블록체인 기술의 활용을 고려하는 회사는 블록체인 DB 및 응용 비즈니스 모델의 법적 준수를 위하여 고심하고 있으나, 아직 우리나라를 비롯한 세계주요국의 개인정보보호법제는 블록체인 기술개발자에 대한 명확한 법적 가이드라인을 제시하고 있지는 못한 실정이다.

이에 본 논문은 현행 개인정보보호원칙과 블록체인 기술의 충돌가능성을 중심으로 해석론과 함께 개선방안을 제시함으로써 블록체인 기술의 장점을 최대한 활용하면서도 프라이버시를 보호하는 방안을 모색해 보도록 할 것이다. 구체적 논의 순서는 첫째, 블록체인 개념, 특징 및 유형(Ⅱ)에서는 블록체인 일반론을 개인정보보호 문제와 관련된 부분을 중심으로 개괄적으로 다루고, 둘째, 블록체인과 개인정보보호에 관한 일반적 쟁점(Ⅲ)에서는 블록체인과 개인정보보호법과의 충돌, 주요국의 개인정보보호법제 개관, 블록체인의 개인정보 포함 여부를 중심으로 검토하고, 셋째, 블록체인과 개인정보보호에 관한 개별적 쟁점(Ⅳ)에서는 블록체인과 개인정보 보호의 충돌에 따른 개인정보보호법의 개별적 이슈들을 검토할 것이다. 넷째, 블록체인을 고려한 현행법제에 대한 개선방안(Ⅴ)에서는 블록체인기술을 개인정보보호법 내부로 수용할 수 있는 구체적 개선방안을 제안할 것이다.

금융법연구」 제13권 제2호, 한국금융법학회, 2016, 116면.

Ⅱ. 블록체인의 개념, 특징 및 유형

1. 블록체인의 개념

가. 기본 개념

블록체인(Blockchain)은 중앙 서버에 저장되는 대신 여러 컴퓨터 간에 공유되는 거래 목록인 분산 원장이다.[2] 2008년 나카모토 사토시(Nakamoto Satoshi)라는 익명의 개발자가 비트코인(Bitcoin)이라는 공개키(public key) 암호방식과 작업증명(proof-of-work)으로 구성된 합의 알고리즘을 결합하여 암호화폐(crypto-currency)를 만들면서 세상에 알려지게 되었다.[3] 이는 다수의 참가자가 일련의 동기화된 원장을 공동으로 관리하는 탈중앙적인 분산원장구조로 되어 있으므로, 분산원장기술(Distributed Ledger Technology, DLT)이라고도 한다. 블록체인이 적용된 대표적인 예로서 비트코인의 경우 블록체인은 가상비트코인 양도인의 권리가 유효한지, 즉 Bitcoin이 불법 복제 또는 도난당하지 않았는지 보장하는 데 필요한 신뢰할 수 있는 제3자를 대신한다. 비트코인 거래에서 블록체인은 거래되는 모든 비트코인의 지불 내역을 포함하는 데이터베이스로 기능하며 특정 시점에서 누가 소유하는지에 대한 증거를 제공한다. 블록체인 데이터베이스의 견고성과 보안성은 합법적인 비트코인 전송 후 시스템의 다양한 컴퓨터가 블록체인을 업데이트하는 데 동의해야하는 정교한 "합의 메커니즘"에 의해 보장된다. 블록체인에 합법적인 거래가 영구히(irreversibly) 기록되기 때문에, 불법 거래가 어려운 구조로 되어 있다. 블록체인 네트워크 참가자의 성격, 범위 등에 따라 여러 가지 형태가 존재하고 사용용도에 맞게 응용이 가능하다.

나. 전통적인 블록체인 기술

전통적인 블록체인 기술은 비트코인 또는 이더리움과 같이 공개되고 투명한

---

2) Anthony Lewis, A Gentle Introduction to Blockchain Technology 4, https://perma.cc/H3AX-XJXX (archived Oct. 27, 2017).

3) 정승화, 전게 논문, 109면.

퍼블릭 블록체인 기술을 의미한다. 전통적인 블록체인 기술의 구성요소는 p2p 네트워크, 합의 알고리즘, 전자서명·해시함수, 스마트계약으로 이루어진다.[4] 각 블록에는 1) 날짜 스탬프, 데이터 주소(ID) 및 이전 블록의 헤더 해시를 포함하는 (암호화되지 않는) 헤더 및 2) 저장되는 데이터인 (보통 암호화되는) 페이로드(payload)가 있다.[5] 헤더의 해시는 블록의 불변 체인을 생성하기 위한 이전 블록의 해시이며, 페이로드는 일반적으로 문서에 대한 설명(메타 데이터)과 실제 문서를 가리키는 해시이다.[6]

다. 새로운 블록체인 기술과 그 한계

블록체인 기술은 빠르게 발전하고 있기 때문에 새로운 기술들은 더 높은 수준의 익명성을 가지고 이용자의 프라이버시를 보호하면서 작업을 수행할 수 있게 한다. 예컨대, 거래 내역을 섞어 추적을 어렵게 만드는 Dash와 같은 프로토콜은 암호화 추적을 불가능하게 하고, 제로지식증명(Zero Knowledge Proofs: ZKP) 기술은 거래의 세부 사항을 알지 못하고도 거래를 검증할 수 있도록 한다.[7] 즉 ZKP기술은 실제로 데이터를 공개하지 않고 데이터에 대한 계산 사실을 증명한다. ZKP 기술은 거래 생성자가 발신자의 주소, 수신자의 주소 및 거래 금액을 밝히지 않고 거래가 사실임을 증명할 수 있도록 함으로써 전통적 퍼블릭 블록체인에서 모든 항목을 암호화하면 채굴자가 거래가 유효한지를 확인하지 못하기 때문에 거래 검증을 할 수 없다는 문제를 해결한다.

이러한 ZKP기술을 사용하는 예로서 Zcash는 공개 블록체인에 개인 데이터를 저장하기 위한 암호화 프로토콜을 사용하는 암호화된 개방/공개형 복제 원장이다. Zcash는 zk-SNARK(zero-knowledge Succinct Non-Interactive Arguments of Knowledge)를 사용하여 모든 데이터를 암호화하고 인증된 당사자에게만 복호화키를 제공하여 거래를 확인할 수 있도록 한다.[8] 그러나 증명 작업은 광범위하며(extensive) 상당한 계산 비용이 소요되어 결과적으로 확장성

---

4) 아카바네 요시하루 외(양현 역), 「블록체인 구조와 이론」, 위키북스, 2017, 89-90면 참조.
5) Winston Maxwell & John Salmon, A guide to blockchain and data protection, at 20.
6) Id.
7) Lukas Schor of The Argon Group, On Zero-Knowledge Proofs in Blockchains, https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd.
8) Zcash, What are zk-SNARKs? https://z.cash/technology/zksnarks.html.

(scalability) 문제가 있다.[9] Zcash의 문제점을 극복하기 위한 대안은 Hyperledger Fabric 프로젝트인데, 여기서도 키를 발급하는 기관은 중앙집중적이다.[10]

2. 특징

블록체인 기술의 주요 특징으로 개인간 거래를 가능하게 하는 탈중개성(脫仲介性), 손쉽게 활용할 수 있는 확장성(scalability), 모든 사용자가 거래장부를 분산, 저장 관리하는데 따른 뛰어난 보안성(security), 블록체인 내 모든 거래의 세부 사항을 볼 수 있는 높은 투명성(transparency)이 들어진다.[11] 블록체인 구조의 특징 상 높은 투명성 때문에 개인들이 각 거래마다 동일한 공개키를 사용한다고 가정하면 해당 거래에서 개인식별이 가능하며, 공개키와 관련 거래가 식별된 후 이러한 정보가 블록체인의 일부가 되어 정보 삭제가 불가능하게 된다.[12] 이 중 개인정보와 관련하여 중요한 특징은 a) 블록체인을 통과하는 정보는 모든 노드에서 볼 수 있으며, b) 정보는 블록체인에서 제거될 수 없다는 것이다.[13] 첫번째 특징은 사용자의 익명성을 대중에게 알릴 수 있게 하여 모든 거래를 공개적으로 문서화한다. 두번째 특징은 변조 방지 방식으로 문서화하기 때문에 거래 기록을 변경하거나 삭제할 수 없다는 것이다. 이러한 특징은 개인정보보호와 관련하여 데이터 최소화(data minimisation) 및 저장 제한(the storage limitation) 원칙과 충돌한다. 이러한 개인정보보호원칙과의 충돌을 어

9) 아카바네 요시하루 외(양현 역), 앞의 책, 174면; Winston Maxwell & John Salmon, supra note 5, at 21.

10) 아카바네 요시하루 외(양현 역), 앞의 책, 174-175면. 분산형 프레임 워크 중 하나는 Hyperledger Fabric("HLF")이라고 불리는데, Hyperledger 우산 프로젝트 내의 오픈 소스 프로젝트이다. 또한 HLF는 비공개 블록체인을 위한 분산형 운영체제로 볼 수 있는 모듈식 범용 비공개 블록체인 시스템이다. www.hyperledger.org. 개별 거래를 위하여 동일한 개인키를 사용하나, 공개키는 각 거래에 대하여 새로이 생성되는 것을 사용하는 방식으로 이 작업은 일부 공개키에 대해서만 가능하며 핵심 개인키에 대해 각 거래별로 다른 키를 생성하는 키 발급 기관(비록 여러 개라고 하더라도 중앙 집중식이어야 함)이 필요하다. 핵심 키와 거래 키 간의 매핑은 다른 참여자들에게 공개되지 않으며 그들은 개별 거래키만 볼 수 있다. Winston Maxwell & John Salmon, supra note 5, at 21.

11) 정승화, 앞의 논문, 116면.

12) 비트뱅크, 블록체인의 충격 편집위원회 (김응수, 이두원 역), 「블록체인의 충격-비트코인, 핀테크에서 IoT까지 사회 구조를 바꾸는 파괴적인 기술」, 북스타, 2017, 31면.

13) 아카바네 요시하루 외(양현 역), 앞의 책, 31면 참조.

떻게 회피하고 조화를 이룰 것인가가 블록체인 기술의 서비스 분야에의 응용에 있어서 중요한 과제이기도 하다.

3. 다양한 유형

가. 일반

인터넷과 달리 블록체인 시스템은 거의 무한대로 다양한 구성으로 개발가능하므로 그 유형이 다양하다. 이하에서는 데이터 유형에 의한 구분, 퍼블릭(Public) 및 프라이빗(Private) 블록체인, 공개형(Non-Permissioned)과 폐쇄형(Permissioned) 블록체인, 전통적 블록체인과 변형 블록체인으로 구분하여 그 특징을 설명하고자 한다.

나. 데이터 유형에 의한 구분

블록체인에서 처리하는 데이터의 유형에 제한이 있는지 여부에 따라 일반 블록체인 시스템과 특수 블록체인 시스템으로 나눌 수 있다. 일반 블록체인 시스템은 모든 데이터를 처리하도록 설계된 것이므로 처리에 있어서 개인정보와 비개인정보를 구분하지 않는다. 반면 특수 블록체인 시스템은 특정 데이터 유형만을 처리하도록 설계된 것인데, 이 중 개인정보를 처리하도록 설계된 특수 블록체인의 경우에는 개인정보보호 차원에서 특히 문제된다.[14]

다. 퍼블릭(Public)과 프라이빗(Private) 블록체인

퍼블릭(Public) 및 프라이빗(Private) 블록체인은 개인정보 보호 관점에서 볼 때, 블록체인이 일반적으로 접근 가능한지, 폐쇄 그룹의 구성원인 경우에만 접근할 수 있는지 여부에 따른 구분이다. 즉 퍼블릭(Public) 및 프라이빗(Private) 블록체인은 읽기가 가능한지에 따른 구분이다. 블록체인을 통해 저장된 정보에 “접근”하는 것을 제한하는 것은 암호화를 통해 이루어지며, 이것이 어떻게 제

14) 유럽 GDPR에서는 인간의 권리와 자유에 높은 위험을 초래할 수 있는 데이터 처리에는 데이터 보호 영향 평가를 의무적으로 하도록 하고 있다.

공되는지에 따라 개인정보 보호 문제가 발생한다.

라. 비허락형(Non-Permissioned)과 허락형(Permissioned) 블록체인

비허락형(Non-Permissioned)은 사전허락이나 동의없이 누구나 참여할 수 있는 블록체인을 의미하는 반면, 허락형(Permissioned) 블록체인은 정해진 구성원만으로 네트워크의 노드가 구성된 블록체인을 말한다.[15] 다시 말해 퍼블릭(Public) 및 프라이빗(Private) 블록체인의 차이가 읽기가 가능한지에 따른 구분이라면 비허락형(Non-Permissioned)과 허락형(Permissioned) 블록체인은 쓰기가 가능한지에 따른 구분이다. 당사자가 비허락형 블록체인 을 사용하는 경우 기본적으로 블록체인에 정보를 자유롭게 추가할 수 있다. 반면에 허락형 블록체인을 사용하면 접근이 제한되며 시스템에 대한 통제권(allocation of control)에 영향을 미치는 신뢰받는 중개자가 시스템에 필요하게 된다. 처리 수단 및 목적을 결정하는 당사자는 개인정보보호 규칙을 고려해야 하므로 비허락형 또는 허락형 블록체인 간의 선택은 당사자가 어떤 프라이버시 요건을 준수해야 하는지에 영향을 미치게 된다.

마. 전통적 블록체인과 변형체인

전통적인 블록체인은 비트코인과 이더리움과 같이 공개되고 투명한 퍼블릭 블록체인 기술을 사용하는 경우이고, 변형체인은 블록체인의 공개성에 변형을 가한 것으로서 그 예로 접근이 제한된 다른 시스템에 기밀 정보를 별도로 저장하는 오프체인(Off-Chain)과 원 블록체인과 나란히 존재하는 병렬 블록체인(parallel blockchain)인 사이드체인(Sidechains)이 있다.[16] 정보를 오프체인으로 저장하면 거래 세부 사항에 대한 접근을 권한 있는 당사자에게만 제한하도록 설정할 수 있으므로 거래 내역의 프라이버시가 보장되는 반면 더 이상 거래기록을 공유하게 할 수 없으며 대부분의 경우 거래 양당사자는 각자 자신의 기록

15) 조성훈, 「자본시장에서의 블록체인 기술의 활용전망 및 시사점」, 자본시장연구원 조사보고서 16-07, 2016.11, 14면 참조.
16) 사이드체인은 작업을 각 사이드체인에 분산하여 처리하므로 효율이 높아지고, 속도, 연산능력 등 용도에 따라 필요한 기능을 갖출 수 있다.

을 관리해야 하므로 블록체인을 사용할 때 얻을 수 있는 여러 가지 이점이 사라진다.[17] 사이드 체인에서 발생하는 거래에 대해 제공되는 기밀성 및 프라이버시의 정도는 사이드 체인이 사용하는 기술에 따라 다르다.[18] 그러나 변형 체인에 대해서는 블록체인의 기본적 특성을 갖지 않으므로 엄밀한 의미에서 블록체인으로 분류하기 어렵다는 반론도 가능할 것으로 생각한다.

Ⅲ. 블록체인에 있어서 개인정보보호에 관한 일반적 쟁점

1. 개인정보보호법과 블록체인간의 충돌

우리 개인정보보호법을 비롯한 제외국의 현행 개인정보보호법은 페이스북(Facebook), 구글(Google) 또는 아마존(Amazon)과 같이 인터넷 서비스를 하는 전통적인 중앙집중 관리자에 의하여 개인데이터가 저장, 관리 및 제어된다는 전제하에서 제정된 법이다. 이러한 전제는 분산된 네트워크에 의해 저장, 관리 및 제어되는 변경불능의 데이터베이스인 블록체인의 핵심기술과 충돌한다. 앞에서 설명한 공개 분산원장 방식으로 운용되는 블록체인 기술은 한번 저장된 정보는 블록체인 특성상 파기하기 어렵다는 점에서 기존 개인데이터보호법제가 미리 상정하지 못한 새로운 개념과 모델로 발전하고 있다.

본 논문에서 논의하는 블록체인과 개인정보 보호 이슈의 전제에는 블록체인이 개인정보보호법의 적용을 받는지의 문제가 있다. 블록체인기술이 구현되는 모델이 다양하기 때문에 일반화하여 단정적으로 말하기 어려운 한계가 있으나, 전통적 블록체인 모델에 따라서 논의를 전개하기로 한다.

이하에서는 주요국의 개인정보보호법제 동향에 대하여 간단하게 살펴본 후, 블록체인시스템이 개인정보를 처리하는지 여부, 즉 해시(hash)와 공개키(public key)가 개인정보인지 여부, 개인정보를 처리한다고 볼 수 있는지를 먼저 살펴보고자 한다.

---

17) Winston Maxwell & John Salmon, supra note 5, at 16.
18) Id.

2. 주요국의 개인정보보호법제

가. 유럽

2000년대 들어오면서 유럽연합이 기본권헌장에 개인정보보호권을 명문화하면서 기본권으로 격상되었다. 이를 구체화하기 위하여 1995년부터 시행된 정보보호지침을 대체하는 유럽연합 일반정보보호규정(General Data Protection Regulation: GDPR)을 2015년 12월 제정하는데, 개인정보보호를 위한 새로운 기준을 제시하고 있다.[19] 기존에 정보보호 지침이 유럽 회원국의 입법을 위한 지침이었다면, GDPR은 모든 EU 회원국이 별도의 입법을 제정하지 않아도 법적 구속력을 가지는 규정이다. 2018. 5. 25.부터 시행되고 있어 전세계적으로 관심이 집중되고 각국이 대응책 마련에 고심하고 있다.

아울러 비개인데이터의 자유로운 유통을 수립하는 것을 목적으로 2017년 9월 비개인데이터의 자유로운 유통을 위한 규정초안을 제안하였다.[20] 동 규정초안에서는 비개인정보의 유통에 관한 규칙의 부재가 중소기업의 성장과 혁신의 저해요인이 된다고 판단하여 “비개인데이터의 EU 역내에서의 자유유통을 위한 방침”을 제시하였는데, 비개인데이터의 자유유통을 담보하고 데이터의 안전한 보관에 대해서도 언급하고 있다.

나. 일본

일본은 2017년 5월 30일 개인정보보호법을 개정하면서 포괄적인 개인데이터에 대한 규제를 완화시키고 그 활용성을 증진시켰다. 즉 개인정보에 관한 개념과 범주를 보다 명확하게 하는 한편, 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻을 수 있는 정보로, 복원이 불가능하도록 만든 ‘익명가공정보’라는 개념(일본 개인정보보호법 제2조 제9항)을 새로이 도입하면서[21] 익명가공정

19) European General Data Protection Regulation 2016/679 (GDPR).

20) EUROPEAN COMMISSION, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the free flow of non-personal data in the European Union, Brussels, 13.9.2017 COM(2017) 495 final 2017/0228 (COD).

21) 국내 소개자료로서 장세균, “정밀의료에서 개인정보보호 방안 -미국・EU・일본과의 비교

보로 처리한 이후에는 목적 범위에 제한없이 다른 처리자들과 공유가 자유롭도록 하고 있다.

아울러 의료데이터의 활용성을 증진시키기 위하여 개인데이터 중에서도 의료데이터에 대한 규제 완화와 더불어 이용 가능성을 증진시키기 위하여 의료데이터 활용에 관한 특별법을 새로 입법하였다. 즉 2017년 4월 28일 의료의 특수한 상황을 감안하여 치료에 관한 정보 등을 익명으로 가공하여 의료기관 외에서도 연구할 수 있도록 하는 차세대의료기반법을 통과시키고 2018년 5월부터 시행하고 있다.[22] 동법의 제정으로 지금까지 개별적으로 취득·관리되고 있는 의료데이터를 의료기관 간 공유하여 이용할 수 있게 되고, 별도로 규정된 개인정보보호 안전기준을 충족하는 '인정사업자'가 보건의료기관이 보유하고 있는 의료데이터를 '익명가공'하여 보건의료기관 외의 제약회사 등에게 제공할 수 있게 되었다. 또한 실효적인 의료데이터 규제 완화를 위하여 이와 같은 의료데이터의 이용은 환자 개인이 '정보제공에 대한 동의'를 거부하지 않으면 제공할 수 있도록 하는 옵트아웃(opt-out) 방식을 채용하였다.

다. 미국

미국 연방헌법은 프라이버시권에 대해 명문 규정은 두고 있지 않으나 Griswold v. Conneticut 사건[23]에서 헌법상 권리로 승인하였다. 그러나 정보 프라이버시의 헌법적 권리를 인정하는지는 명확하지 않다.[24] 개인정보 보호에 관한 법률 제정 형식에 있어서, 미국은 우리나라와 달리 개인정보 보호에 관한 일반법이 존재하지 않고 개별영역의 법들이 산재하고 있다.[25] 그 밖에 소비자

법제도 분석을 중심으로-", 연세대학교 보건대학원, 석사학위논문, 2017.6, 49-50면 참조.

22) 次世代医療基盤法 平成 30年5月 施行 (内閣官房健康·医療戦略室). 개인정보보호법의 개정에 의해, 병력 등을 포함한 배려가 요구되는 개인정보에 대해 소위 옵트아웃에 의한 제3자 제공이 금지됨으로써 동의 취득 및 익명화를 포함하는 데이터 처리시스템 구축·운영비용 부담이 커짐에 따라 개인의 권리 이익의 보호를 배려하면서 익명가공된 의료정보를 안심하고 원활하게 활용할 수 있도록 하는 것을 주요 내용으로 한다.

23) Griswold v. Conneticut 381 U.S.479 (1965).

24) 미국 버클리 로스쿨의 Schwartz교수는 Whalen v. Roe 사건에서 연방대법원은 실질적인 적법절차(substantive due process)에 근거한 정보 프라이버시의 헌법적 권리를 확인했다고 보고 있다. Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815, 828(1999); Whalen v. Roe, 429 U.S. 589 (1977); Paul v. Davis, 424 U.S. 693 (1976).

25) 프라이버시법(Privacy Act), 금융프라이버시법(The Financial Privacy Act), 케이블통신정책법(Cable Communications Policy Act), 전자통신프라이버시법(Electronic Communication

프라이버시 권리장전, FTC에 의한 개인정보 자율규제가 있다.

의료서비스제공자와 더불어 보험회사가 개인의 의료정보를 접근하고 취득하는데 필요한 사항들을 규정하는 건강보험의 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act, 이하 'HIPAA')[26]과 개인정보보호규칙의 경우[27] HIPAA 개인정보보호규칙의 기준에 따라 건강보험공급자, 보건의료서비스제공자, 보건의료정보센터의 보호의무자들은 개인을 식별할 수 있는 의료정보(individually identifiable health information)는 모두 보호해야 하는데,[28] 식별 가능하지 않도록 처리된 의료정보(de-identified health information)의 이용 및 공개에는 제한이 없다.[29] 여기에서 식별 가능하지 않도록 처리하는 방법에는 두 가지가 있다. 하나는 인정받은 통계 전문가에 의한 공식적인 확인을 받는 것이고, 다른 하나는 그 개인과 개인의 친척, 가구 내 구성원, 고용주 등의 고유 식별자(identifier)들을 삭제하는 것이다.

3. 블록체인의 개인정보 포함 여부

가. 개인정보의 법상 개념

블록체인에 개인정보보호법이 적용되는지 여부를 결정하려면 블록체인 기술

Privacy Act), 비디오프라이버시보호법(Video Privacy Protection Act), 건강보험의 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act), 공정신용보고법(Fair Credit Reporting Act) 등이 이에 해당한다.

26) 그 명칭에서 보듯이 일반적인 의료데이터에 관한 사항을 정한 법률이라기보다는 피보험자에게 이직 등 일신상의 변동 사항이 있을 경우에도 건강보험의 이전과 책무성을 보장하기 위한 사항들을 정한 법률이다.

27) HIPAA가 1996년 제정되고 난 후 그 이행을 위하여 미국 보건복지부는 의료정보의 보호를 위한 국가기준으로 개인 식별 가능한 의료정보의 보호를 위한 기준("개인정보보호규칙")을 제정하였다. 이 기준은 개인의료정보를 수집하고 이용·관리하는 적용 대상인 보호의무자들에게 그 보호의무자의 구성원들로 하여금 개인의 의료정보를 운용하는 방법을 이해하고 적용케 하는 동시에 그 보호의무자 조직을 통제할 수 있는 표준으로 기능한다. 또한 이 기준은 미국 보건복지부 내 인권 부서(Office of Civil Rights, OCR)에서 위의 자발적인 준수활동에 관한 규제 및 위반사항에 관한 처벌을 구현하는 근거가 되고 있다.

28) 이러한 사항은 전자적인 방법이나 서면, 구전 그 어떤 방법으로든 마찬가지다. 개인을 식별할 수 있는 의료정보는 1) 그 개인의 과거, 현재 또는 미래의 신체 또는 정신 건강 또는 상태에 관한 것, 2) 그 개인에 대한 의료 제공, 3) 그 개인의 의료 제공을 위한 과거, 현재 또는 미래의 비용에 관한 사항을 포함한다. 또한 성명, 주소, 생년월일, 사회보장번호도 포함된다.

29) 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

을 사용할 때 개인정보가 처리되는지 여부를 판단해야한다.

우리나라 개인정보보호법은 개인정보를 “살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보라고 하고, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함하는 것”으로 정의하고 있다(동법 제2조 제1호). 일본개인정보보호법도 우리나라와 비슷하게 정의하고 있다.[30] GDPR의 경우, 우리나라나 일본의 경우보다 개인정보를 상세하게 정의하고 있다. 즉 ‘개인정보’를 “식별되거나 식별가능한 자연인에 관한 모든 정보”이고, ‘식별가능한 자연인’은 “특히 성명, 식별번호, 위치 데이터, 온라인 식별자와 같은 식별자, 또는 해당 자연인에 관한 물리적, 생리적, 유전자적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특유한 하나 또는 복수의 요소를 참조하는 것에 의하여 직접적 또는 간접적으로 식별할 수 있는 자”를 말한다고 정의하여(제4조 제1항)[31] 우리나라나 일본의 개인정보보호법상의 개인정보 정의와 달리 위치, IP 주소, 쿠키 데이터, RFID 태그 등 웹 정보의 경우에도 개인정보의 범위에 포함됨을 명시하고 있는 점에서 차이가 있다.

데이터 보호의 관점에서 볼 때 블록체인 DB는 일견 계약 당사자 또는 공중에게 직접 자신의 신원을 공개하지 않아도 최소한 이론적으로 당사자 간의 거래를 허용하기 때문에 관련 거래 당사자가 추적될 수 없는 경우, 개인정보에

---

30) 일본개인정보보호법 상 개인정보는 살아있는 개인에 관한 정보로서 1) 해당 정보에 포함되어있는 성명, 생년월일 기타 기술 등에 기재 또는 기록되거나 음성, 동작 기타 방법을 사용하여 표현된 일체의 사항에 의하여 특정 개인을 식별할 수 있는 것 (다른 정보와 용이하게 조합할 수 있으며, 그로 인하여 특정 개인을 식별할 수 있게 되는 것을 포함한다) 또는 2) 개인식별부호가 포함되는 것을 의미한다(제2조 제1항).
개인식별부호란 다음 각 호의 어느 하나에 해당하는 문자, 번호, 기호 기타의 부호 중 시행령으로 정하는 것을 말한다. 1) 특정 개인의 신체의 일부 특징을 전자계산기용으로 제공하기 위하여 변환한 문자, 번호, 기호 기타의 부호가 해당 특정 개인을 식별할 수 있는 것, 2) 개인에게 제공되는 용역의 이용 또는 개인에게 판매되는 제품의 구입에 관해 할당되거나 또는 개인에게 발급되는 카드 기타 서류에 기재되거나 또는 전자적 방식에 의해 기록된 문자, 번호, 기호 기타의 부호가 그 이용자 또는 구입자 또는 발급을 받는 자마다 다른 것이 되도록 할당 또는 기재되거나 또는 기록됨으로써 특정 이용자 또는 구입자 또는 발행받을 자를 식별할 수 있는 것(제2조 제2항).

31) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

관한 권리는 침해되지 않고, 블록체인의 데이터 처리는 가능하다고도 볼 수 있다. 우리 개인정보보호법에 의하면 개인을 식별할 수 없는 정보는 보호대상이 되지 않으므로 블록체인 데이터 처리는 개인정보보호법의 대상이 되지 않는다고도 볼 수 있는 것이다. 유럽의 GDPR도 단순한 (거래) 데이터에 대해서는 적용되지 않는다고 규정한다(GDPR 서문 26 참조).[32] 따라서 블록체인과 관련한 데이터가 관련 개인을 추적할 수 없는 단순히 거래데이터에 그친다면 특정 데이터를 보호해야 할 의무를 지지 않고 이러한 데이터를 사용하고 처리할 수 있는 법적 권한이 있다.

위와 같은 개인정보의 정의에 따를 때, 상당한 노력 없이 참가자를 쉽게 식별할 수 있게 하는 이름, 주소, 전화 번호 또는 기타 유사한 정보가 블록체인의 해당 거래 데이터 항목에 캡처되지 않는다는 것은 사실이지만, 해당 항목이 식별화될 다양한 가능성이 있다. 예를 들어 블록체인에 문서화된 서비스 이용자의 비트코인 주소로 해당 IP 주소를 추적할 수 있으며, 이 IP 주소는 특정 인터넷 연결 또는 연결 소유자를 추적할 수 있다. 또 이용자 및 거래 네트워크는 비트코인 원장에 공개적으로 접근할 수 있는 블록체인 항목을 기반으로 만들어질 수 있고 익명의 거래들을 통해 특정 이용자들을 추적할 수 있음을 입증할 수 있다.

우리 개인정보보호법은 그 자체로는 개인 식별이 어려우나 다른 정보와 쉽게

---

32) Recital 26 Not applicable to anonymous data. 1. The principles of data protection should apply to any information concerning an identified or identifiable natural person.
2. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
3. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
4. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.
5. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
6. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

결합하여 알아볼 수 있는 경우 개인정보에 해당하는 것으로 보고 있고, GDPR의 경우 위치, IP 주소, 쿠키 데이터, RFID 태그 등 웹 정보의 경우에도 개인정보의 범위에 포함됨을 명시하고 있으므로 해당 정보 그 자체로는 개인 식별이 어려우나 IP주소 등과 쉽게 결합하여 개인식별이 가능하게 된다면 개인정보에 해당되게 될 것이다.

결국 우리 개인정보보호법 상 용이한 정보 결합으로 개인식별이 되는지가 개인정보성을 판단하는 기준이 될 것이므로, 블록체인이 개인정보를 취급하는지를 살펴보기 위하여 아래에서는 구체적으로 해시와 공개키의 개인정보성에 대하여 살펴보기로 한다.

나. 해시의 개인정보 해당 여부

먼저, 블록체인 시스템에서 가장 중요한 역할을 하는 해시가 개인데이터인지 여부를 검토할 필요가 있다. 해시는 그 길이에 관계없이 주어진 디지털 정보 부분에 대해 고정된 길이의 코드를 생성하는데 데이터의 내용마다 고유값을 가진다는 점에서 인간의 지문에 비유된다.[33] 이는 주어진 디지털정보 부분이 원래 해시된 디지털 정보와 동일하다는 것을 증명한다.[34] 그러나 해시는 원본 디지털정보에서 해시에 이르는 일방향으로만 작동하므로 원본 디지털정보를 발견하기 위해 역분석될 수 없다.[35]

그럼에도 불구하고, 제29조 실무그룹(Working Party)은 해시가 익명화(anonymisation)가 아니라 가명화(pseudonymisation) 기술이라는 의견을 내놓았다.[36] 제29조 실무 당국에 따르면, 기록을 나타내는 해시가 개인정보를 구성하는 정보 부분에 연결가능하고, 이 “연결 가능성”만으로 개인정보로 간주될 수 있다고 한다. 따라서 해시 자체를 원래 개인정보로 역분석할 수는 없더라도 개인의 ID 카드 또는 의료 기록을 나타내는 해시는 개인정보로 간주될 수 있다.[37]

---

33) 아카바네 요시하루 외(양현 역), 앞의 책, 118면 참조.

34) Id.

35) 업계의 기본적인 방향은 블록체인에 개인정보를 두지 않고, 이를 편집 가능한 데이터베이스에 저장한 후 데이터의 일방향 해시만이 블록체인에 저장되도록 한다는 것이다. http://www.itworld.co.kr/news/109231#csidx960b9a71673c195a5941c95f2b7cc5b.

36) Opinion 05/2014.

37) Winston Maxwell & John Salmon, supra note 5, at 9. 반면 선하 증권에 개인 데이터가 포함되어 있지 않으므로 선하증권과 연결된다는 이유 때문에 해시는 개인데이터로 간주

이 기준은 유럽 일반 데이터 보호 규정(GDPR)에 의하여 계속 적용될 것인 바, 해시는 기록이 연결되도록 하기 때문에 일반적으로 익명화 기술이 아닌 가명화 기술로 간주된다. 우리 개인정보보호법에 의하더라도 식별가능성이 있는 정보는 개인정보 정의에 포함되므로 해시는 개인정보에 해당할 수 있다.

다. 공개키의 개인정보해당 여부

공개블록체인의 특성상 모든 거래가 공개되어 특정 이용자를 나타내는 공개키에 연결된다. 이 키는 암호화되어있어 블록체인을 들여다보더라도 이용자인 개인 또는 법인을 직접 식별할 수 없으나 공개키를 재이용하면 개인을 직접 확인할 수 없더라도 공개키를 참조하여 개인을 특정할 수 있다.[38] 실제로 공개키의 직접적 목적은 거래가 올바른 사람에게 귀속되는 것을 보장하기 위해 주어진 거래의 작성자를 특정하는 것이다. 공개키가 표시되면 서비스 제공업체가 보유하고 있거나 누군가가 공개키를 개인이나 조직에 연결할 수 있기 때문에 (예컨대, IP 주소 또는 웹 사이트와의 연결을 통해) 개인을 식별할 수 있는 정보를 얻을 수 있으며, 이 시점에서 관련 개인이 한 모든 거래가 공개된다.[39]

2014년에 제29조 작업반은 가명화된 데이터와 익명화된 데이터의 차이에 대한 지침을 작성하였다.[40] 익명화된 데이터는 살아있는 개인을 추적할 수 없기 때문에 익명화된 데이터에 GDPR이 적용되지 않으므로 이 구별은 블록체인과 관련하여 중요하다. 그러나 익명화된 것으로 인정하는 기준이 매우 엄격한 바, 지침에서는 “익명화는 재식별화되지 않도록 개인 데이터를 처리함으로써 이루어진다”라고 명시하였다. 암호화된 개인데이터는 전문가나 다른 사람이 암호해독키를 가지고 충분한 노력을 기울이면 추적 가능하므로, 암호화된 데이터는 익명의 데이터가 아닌 개인 데이터에 해당할 수 있다.[41] 우리 개인정보보호법에 의하더라도 식별가능성이 있는 정보는 개인정보 정의에 포함되므로 공개키는 개인정보에 해당할 수 있다. 이와 같이 볼 때, 개인정보보호법은 블록체인

되지 아니다.

38) 아카바네 요시하루 외(양현 역), 앞의 책, 116~118면 참조; Winston Maxwell & John Salmon, supra note 5, at 7.

39) Id.

40) Opinion 05/2014 (WP 216).

41) Winston Maxwell & John Salmon, supra note 5 at 7.

시스템과 관련된 데이터 중 일부에 적용 가능하게 된다.

라. IP주소의 개인정보 해당 여부

웹 사이트 방문자의 IP 주소를 저장하는 것이 개인정보보호법 위반에 해당되는지 문제된다. 유럽사법재판소(Court of Justice of the European Union: CJEU)는 2016. 10. 19. 네트워크에 연결될 때 컴퓨팅 장치에 할당된 임시 IP 주소인 동적(dynamic) IP 주소에 관한 Patrick Breyer v Bundesrepublik Deutschland 사건에 대하여 최종 판결을 내렸다.[42] 이 사건에서 동적 IP 주소의 '개인 데이터' 해당성에 대한 법원의 판단은 블록체인 환경에서 '개인 데이터'를 정의하는 방법에도 영향을 미치므로 동사건을 주목할 필요가 있다.

동 사건은 독일 국민인 패트릭 브레이어(Patrick Breyer)가 독일정부를 상대로 제소한 사건이다. 브레이어는 독일의 공공기관이 시사 정보를 제공하는 (공개적으로 접근가능한) 웹 사이트의 운영자이다. 그는 독일정부가 사이버 보안상의 이유로 웹 사이트 방문자의 IP 주소를 저장하는 것이 독일 데이터보호법에 위반됨을 근거로 법원에 그 금지를 청구하였다. 독일 연방대법원(German Federal Court of Justice, Bundesgerichtshof – BGH)은 동사건을 유럽사법재판소에 회부하면서 질문사항 중 하나로 웹 사이트 방문자의 동적 IP 주소가 웹 사이트 운영자를 위한 개인 데이터에 해당하는지 여부를 물었다.[43] 동 재판소는 온라인미디어서비스 제공업체가 수집한 동적인 IP 주소가 제3자(예컨대, 사용자의 인터넷 서비스 제공업체)가 보유한 웹 사이트의 사용자를 식별하는 데 필요한 데이터와 결합할 가능성이 있다면 개인 또는 제3자를 식별하는 데 합리적으로 사용되는 수단에 해당한다고 판시하였다. 그러나 데이터 주체의 식별이 법률로 금지되었거나 시간, 비용 및 인력 측면에서 과도한 노력이 필요하여 실질적으로 불가능한 경우 및 식별의 위험이 현저하게 드러나지 않는 경우에는 개인식별정보로 판단할 수 없다는 예외를 인정하였다.[44]

---

42) Case C-582/14.

43) 그리고 독일 텔레미디어법의 특정 데이터 보호 조항은 합법적인 이익에 근거한 정당성(지침 7 (f))을 기본적으로 배제하고 있는데, 동조가 EU법과 조화하는지 여부를 질문하였다.

44) 따라서 CJEU는 인용된 독일 연방사법재판소의 최종 평가에 따라 다음과 같이 가정했다. "온라인 미디어 서비스 제공업체는 관할 기관 및 인터넷 서비스 제공업체의 도움을 받아 저장된 IP 주소에 기초해서 데이터 주체를 식별하는데 합리적으로 사용될 수 있는 수단

Breyer 판결에서 '개인 데이터'의 개념 내지 요건에 대한 법원의 판단은 GDPR 체제에서도 계속 적용되므로 블록체인 환경에서 '개인 데이터'의 정의에도 영향을 미친다고 할 것이다. 따라서 GDPR에서 블록체인이 개인데이터를 포함하는가의 판단에 있어서 식별력이 있는지를 판단하는 기준으로서 식별에 소요되는 시간, 비용, 인력에 과도한 노력이 드는지, 법에서 식별을 금지하고 있는지, 식별의 위험이 현저한지가 종합적으로 사용될 것으로 보인다. 이러한 기준은 우리 개인정보보호법에서 식별력을 판단하는 기준으로도 참조가 된다.

마. 소결

이상에서 살펴본 바와 같이 블록체인의 해시와 공개키, IP주소는 개인과 연결될 가능성이 있다. 따라서 해당 정보만으로는 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우도 개인정보의 범위에 포함하는 우리나라 개인정보보호법이나 개인정보를 식별되거나 식별가능한 자연인에 관한 모든 정보로서 IP 주소, 쿠키 데이터, RFID 태그 등 웹 정보의 경우에도 개인정보의 범위에 포함시키는 유럽 GDPR에 따르면, 블록체인의 해시와 공개키, IP주소는 개인 데이터에 해당할 가능성이 있다. 그러나 유럽의 경우에도 식별이 가능한지를 판단하는 기준으로서 Breyer 판결에서의 판단기준인 식별에 소요되는 시간, 비용, 인력에 과도한 노력이 드는지, 법에서 식별을 금지하고 있는지, 식별의 위험이 현저한지를 종합적으로 사용할 것으로 보이고, 우리 개인정보보호법 상으로도 다른 정보와 쉽게 결합하여 식별력이 있는지를 판단하게 되므로 "쉽게" 결합이 가능한지를 판단하는데 있어서 Breyer 판결이 참조가능할 것으로 보인다. 아울러 이러한 식별기준에 따라 개인데이터에 해당한다고 하더라도, 일부 새로운 블록체인 기술을 사용하면 개인데이터에 해당하지 않게 될 가능성도 배제할 수 없다.

을 가지고 있다."

Ⅳ. 블록체인에 있어서 개인정보보호에 관한 개별적 쟁점

1. 일반

블록체인에 개인정보가 포함되고 블록체인을 통해 처리된다고 가정할 때, 블록체인과 개인정보보호의 개별적 쟁점들로서 블록체인 차원에서 개인정보처리자는 누구인지의 문제, 개인정보처리의 원칙, 동의요건, 블록체인 시스템에서 개인정보삭제의 문제, 설계에 의한 개인정보 보호, 개인데이터 보호 영향 평가, 블록체인에 대한 재판관할과 준거법의 문제를 검토하기로 한다.

2. 책임의 주체

위에서 다룬 바와 같이 블록체인이 개인데이터를 취급하여 개인정보보호법의 적용대상이 된다고 할 때, 블록체인 이용자가 개인정보처리자 또는 위탁관리자에 해당하는 지 등 책임 주체의 문제가 발생한다. 그런데 개인정보 보호의 주요원칙 중 하나인 책임성의 원칙(the principle of accountability)과 관련하여 블록체인의 전세계적으로 분산된 네트워크에서 누가 책임을 지고 개인정보보호법을 준수할 수 있을지는 아직 불분명하다.

우리나라 개인정보보호법은 개인정보 관리자를 “개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물인 개인정보 화일을 업무상 운용하기 위하여 개인정보를 처리하는 자(법 제2조 제4호, 제5호)”라고 하고 일본법은 “개인정보를 포함하는 정보의 집합물로서 특정의 개인정보를 전자계산기를 사용하여 검색할 수 있도록 체계적으로 구성되거나 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성된 개인정보 데이터베이스 등을 사업에 이용하는 자(법 제2조 제4항, 제5항)”로 정의하고 있으며,[45] 유럽 GDPR의 경우는 데이터 관리자(data controller)라고 하고 “단독으로 또는 다른 사람과 공동으로 개인정보의 처리의 목적과 수단을 결정하는 자연인, 법인, 공공기관, 행정기관 또는 기타 단체”로 정의하고 있다.[46] 또한 공

45) 일본법은 개인정보취급사업자라는 용어를 사용하고 있다.

46) 관리자(controller)와 처리자(processor)로 나뉜다. 우리법의 개인정보위탁자에 해당하는 용어로 처리자(processor)가 있는데, “관리자를 위하여 개인데이터의 처리를 하는 자연인,

동관리자에 대하여도 규정을 두고 있는데 2인 이상의 관리자가 공동으로 취급 목적 및 수단을 결정하는 경우 당해 관리자를 공동관리자라 하고, 공동관리자는 투명한 방법으로 본 규칙에 기초한 관리자 공동의 협정에 따라서 개별 책임을 정하도록 하고 있다(제26조 제1항 1문). 특히 데이터 주체의 권리행사에 관한 사항 및 정보를 제공하는 당해 개별 관리자의 의무를 결정하여야 한다(2문).

GDPR의 경우는 개인정보관리자를 정의함에 있어서 개인정보 처리의 목적과 수단을 결정하는 것에 포커스를 맞추고 있고 공동관리자에 대하여도 규정을 두고 있어, 우리 개인정보보호법보다는 블록체인과 같은 새로운 기술에 좀더 유연하게 대응할 수 있지 않을까 생각한다. 그러나 어느 법제의 경우도 블록체인 시스템을 염두에 두고 제정된 것이 아니기 때문에 블록체인에 있어서 개인정보처리자가 있는지 여부와 있다면 주체가 누구인지는 해석을 필요로 한다고 할 것이다. 위에서 살펴본 개인정보관리자의 정의에서 개인정보 처리를 하는 자에 포커스를 두는 경우, 처리 개념에 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 포함하고 있어(동법 제2조 제2호) 개인정보처리자가 있을 수 있고, 개인정보처리자는 p2p 방식으로 컴퓨팅 자원을 사용하며, 자신의 컴퓨터에 분산원장의 전체 사본을 갖고 있는 블록체인의 각 이용자로 볼 수 있을 것이다. 결과적으로, 블록체인 이용자는 자신이 블록체인에 데이터를 업로드하고 자신의 컴퓨터에 블록체인의 전체 복사본을 저장함으로써 개인정보처리자에 해당하게 될 것이다.

위와 같이 책임의 주체를 특정하는 것은 중요하다고 할 것이나, GDPR이나 우리 개인정보보호법 모두 기본적으로 중앙집중형 네트워크를 전제로 하고 있으므로 블록체인 시스템에 적용하기 어렵다는 한계가 있다. 프랑스의 CNIL(정보자유국가위원회)의 권고처럼 개인정보관리자의 특정이 필요하다는 점에 동의할 수 있지만, 퍼블릭 블록체인의 경우 블록체인에 관여하는 여러 주체 중 누가 관리자에 해당하는지를 정하는 것이 쉽지 않다. EU집행위원회가 2018. 2. 유럽의회의 지원 하에 발족시킨 블록체인 관련 정책 및 전문지식을 모니터링·분석하고 소통하는 EU Blockchain Observatory and Forum에서 발표한 Blockchain and the GDPR 보고서에서는 “퍼블릭 블록체인에 있어서 블록체인

법인, 공공기관, 행정기관 또는 기타 단체”를 말한다고 정의하고 있다.

에 관여하는 여러 주체의 개인정보관리자 해당성"에 관하여 논의하고 있는데,[47] 최소한 검증노드 또는 참여 노드와 네트워크 유저가 개인정보관리자가 될 수 있다고 하더라도 이들이 과연 기술에 대한 정교한 지식이 있고 기술의 위험으로부터 자신을 보호하는 기술을 알고 있다고 전제할 수 있는지는 의문이다. 이에 블록체인 시스템 운영자에게 일정 책임을 지우거나[48] 보험제도를 활용하는 방안도 생각해 보아야 할 것이다. 물론 보다 구체적으로는 블록체인 기술의 발전과 가능한 서비스 모델별 접근, 해설례, 구체적 판결의 축적을 기다려야 할 것이다.

3. 개인정보처리의 원칙

블록체인의 해시와 공개키가 개인정보에 해당하고, 블록체인의 각 이용자가 개인정보처리자에 해당한다면 개인정보의 처리와 관련하여 데이터최소화의 원칙(the principle of data minimization)과 저장 제한의 원칙(the principle of storage limitation)이 블록체인 데이터베이스에서도 준수될 수 있는지가 문제된다. 데이터를 영구저장한다는 블록체인의 특징은 개인 데이터를 "처리 목적에 필요한 범위를 넘어서 데이터 주체를 식별할 수 있는 형태로 유지하여서는 안된다"는 저장제한의 원칙과 조화되기 어렵다. 또한 이용자 모두가 사본을 저장한다는 점에서 개인정보 처리에 있어서 데이터를 최소화해야 하는 데이터 최소화 원칙과도 조화하기 어렵다.[49]

그러나 현행 개인정보처리에 관한 원칙들은 양보의 가능성이 있다. 예컨대, 저장제한의 원칙에서 저장의 목적범위가 p2p 블록체인 시스템의 올바른 작동까지 포괄할 수 있다면 블록체인 시스템에서의 데이터의 영구 저장을 정당화하는 것도 가능할 것이다.

---

47) EU Blockchain Observatory and Forum, Blockchain and the GDPR, 2018 at 18.

48) 블록체인 시스템 운영자에게 일정 책임을 지우는 것을 제안하는 입장으로는 김현경, "블록체인과 개인정보 규제 합리화 방안 검토", 「법학논집」 제23권 제1호, 이화여자대학교 법학연구소, 2018 참조.

49) 우리 개인정보보호법에서는 처리목적을 명확히 하고 그 목적 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 하며 그 목적 외의 용도로 활용하여서는 아니한다고 규정하고 있는바(제3조 제1항, 제2항), 이는 블록체인 데이터베이스를 사용할 수 있는 범위에도 적용할 수 있을 것이다. 이는 GDPR에서도 명시된 목적 제한 원칙에 따라서 개인 정보는 명확하고 합법적인 목적으로만 수집되며 이러한 목적과 양립할 수 없는 방식으로 추가 처리되지 않도록 규정하고 있다(GDPR 제25조, 제5조(1)(b) 참조).

4. 동의 요건

우리 개인정보보호법에 따르면 개인정보 수집, 이용에 있어서 정보주체의 동의가 개인정보의 처리를 정당화시켜준다. 즉 개인정보의 수집 · 이용 목적, 개인정보를 제공받는 자, 수집, 이용하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간 등을 알리고 동의를 받도록 하고 있고(제15조 제2항, 제17조 제2항), 개인정보의 목적 외 이용·제공 범위를 통계작성 및 학술 연구 등으로 제한하고 있다(제18조 제2항 제4호). GDPR에도 마찬가지의 규정이 있다(제7조, 제13조, 제14조).

그러나 블록체인 중에서도 특히 퍼블릭 블록체인의 경우 원장을 보유하는 블록체인의 참여자도 명확하지 않고, 블록체인 원장의 불변성을 고려할 때 개인정보의 보유 및 이용 기간을 적시하는 것이 무의미하다는 점 등 현행 개인정보보호법 상의 동의 요건을 적용하기 적합하지 않다는 문제가 있다.

5. 블록체인에서의 개인정보의 삭제 가부

앞에서 살펴본 바와 같이 블록체인은 변조 방지 기능(tamper-proofness)을 본질적인 특징으로 하고 있으나, 이는 개인정보 보호에 대한 잠재적 위협이기도 하다. 즉, 블록체인의 주요 특징 중 하나인 블록체인 원장의 불변성(immutability) 내지 데이터 변경불가성은 개인정보의 삭제권(the right to erasure) 보장과 관련하여 문제된다. 해당 거래자는 정보의 정확성을 비롯한 개인데이터 보호와 관련된 사유로 원장에 저장된 정보를 변경할 필요가 있는바, 이는 관련 서비스 제공자에게 데이터베이스 전체의 데이터 무결성을 파괴하고 그 동안 쓸모없어진 데이터 항목을 삭제하거나 수정할 의무를 지울 수 있는지의 문제로 귀결된다.

이와 관련하여 2014년 5월 유럽사법재판소의 판결을 주목할 필요가 있다. 동 사건에서는 유럽시민의 개인정보가 공익을 위하여 필요한 경우가 아닌 한, 인터넷 검색엔진 운영자에게 검색결과 색인에서 검색가능한 콘텐츠를 삭제하도록 요구할 권리가 있는지 여부를 다루었다. 이러한 “탈색인화”될 권리로부터 유럽 입법자는 데이터 관리자에 대해 집행할 수 있는 좀 더 일반적인 "잊힐 권리"를 파생시켰으며 현재 GDPR 제17조[50]에서 규정하고 있다. 즉 GDPR은 계속 처리

해야하는 불가피한 이유가 없는 한 개인에게 개인 데이터의 삭제할 권리(right to erasure)를 인정하며, 구체적으로 해당하는 경우를 동조 제1항 (a)호 내지 (f)호에서 규정한다. 그 외에도 GDPR에서는 개인데이터에 대한 정정권(rights to rectification 제16조, GDPR)을 규정하는데, 블록체인에서는 이러한 권리를 행사하는데 장애가 있다.

우리나라의 경우 개인정보보호법, 전자금융거래법과 신용정보의 이용 및 보호에 관한 법률은 목적이 달성된 개인정보 또는 최장 5년이 경과한 금융거래기록이나 개인신용정보를 파기하도록 하고 있으나[51] 블록체인 기술을 통하여 분산원장으로 개인정보를 보유하고 있는 경우에 블록체인의 특성상 특정 블록을

---

50) 제17조 삭제권 (잊힐 권리, Right to erasure('right to be forgotten') 1. 데이터 주체는 해당 데이터 주체에 관한 개인 데이터에 대해 관리자에게 부당하게 지체하지 않고 소거시킬 권리를 갖는다. 관리자는 다음 각 호의 근거 중 하나가 적용되는 경우 개인 데이터를 부당하게 지체하지 않고 삭제할 의무를 부담한다.
(a) 개인 데이터가 수집된 또는 기타 취급의 목적에 대해 해당 개인 데이터가 더 이상 필요하지 않은 경우.
(b) 데이터 주체가 제6조 제1항 (a)호 또는 제9조제2항 (a)호에 의거한 동의에 따라 취급 동의를 철회하고 취급에 관하여 다른 법적 근거가 없는 경우.
(c) 데이터 주체가 제21조제1항에 따라 이의를 신청하고 취급에 대해 우선하는 법적 근거가 없는 경우 또는 데이터 주체가 제21조제2항에 따라 이의를 신청하는 경우.
(d) 개인 데이터가 불법으로 취급된 경우.
(e) 개인 데이터가 관리자가 따라야 할 EU법 또는 회원국의 국내법의 법적 의무 준수를 위해 삭제해야하는 경우.
(f) 개인 데이터가 제8조 제1항에서 규정하는 정보사회서비스의 제공에 대해 수집된 경우.
2. 관리자가 개인 정보를 공개하고, 제1항에 따른 개인 데이터를 삭제할 의무를 지는 경우 그 관리자는 이용가능한 기술 및 실시 비용을 고려하여 당해 개인 정보를 취급하고 있는 관리자들에게 데이터 주체가 해당 개인 데이터의 모든 링크 또는 복사 또는 복제의 삭제를 요구하는 취지를 통지하기 위해 기술적 조치를 포함한 합리적인 수단을 취해야한다.
3. 제1항 및 제2항은 취급이 다음 각호의 어느 하나에 필요한 경우 적용되지 않는다.
(a) 표현과 정보의 자유의 권리 행사에 필요한 경우.
(b) 관리자가 따르는 EU법 또는 회원국의 국내법에 의해 취급이 요구되는 법적 의무를 준수하는 데 필요한 경우 또는 공공의 이익 또는 관리자에게 주어진 공적 권한의 행사를 위해 행해지는 업무 수행에 필요한 경우.
(c) 제9조 제2항 (h)호 및 (i)호 및 제9조제3항에 따라 공중 보건 분야의 공공의 이익을 위해 필요한 경우.
(d) 제89조제1항에 따라 공공이익 목적, 과학적 또는 역사적 연구 목적 또는 통계 목적의 달성을 위하여 취급이 필요한 경우. 다만, 제1항에 명시된 권리가 실시할 수 있을 것 같지 않거나 또는 그 취급의 목적 달성이 손상되는 경우에 한한다.
(e) 법적 주장시의 입증, 행사 또는 항변에 필요한 경우.

51) 전자금융거래법 제22조, 동시행령 제12조 제5항, 신용정보법 제18조, 동시행령 제17조의2, 개인정보보호법 제21조 제1항, 동시행령 제16조 제1항 제1호 각 참조.

파기하기 어려운 점이 있어 충돌의 여지가 있다.[52]

문제는 블록체인 시스템은 삭제를 방지하도록 설계되어 있으므로 삭제는 기술적으로 불가능하다는 것이다. 이론적으로는 과거 거래 기록을 삭제할 수 있다고 하더라도 이 작업은 해당 거래 이전에 영향을 받는 거래의 유효성 검증 및 다음 거래(블록)의 재구성과 아울러, 각 거래의 노드 중 51%의 협력(cooperation)이 필요하다. 실질적으로 이러한 조치는 불가능하며, 만일 삭제가 가능하도록 블록체인을 설계한다면, 삭제불가능한 데이터를 이용자가 모두 나누어 가짐으로써 별도의 신뢰할 수 있는 관리자를 필요로 하지 않는 블록체인의 장점이 빛을 잃게 된다.[53] 신뢰성을 유지하면서도 데이터 기록을 나중에 편집 가능하도록 하려면 미리 정의된 규칙들에 따라서 블록체인의 원장을 변경할 권한이 있는 신뢰할 수 있는 관리자를 지명하는 것이 필요하므로, 분산형 P2P 형태의 블록체인의 필수 특성 가운데 일부는 유지하기 어려워지기 때문이다.[54]

대안으로 우리법상의 “파기”나 GDPR의 “삭제”의 의미가 법문 상 정의되고 있지 않으므로, 접근권한을 취소하는 것까지 포함하는 것으로 유연하고 포괄적으로 해석하는 방안도 생각해 볼 수 있다. 즉 “삭제”의 의미와 관련하여 불가역적인 암호화(irreversible encryption)를 삭제에 해당한다고 보는 것이다. 접근권한을 관리하는 메커니즘이 포함되어 있는 스마트 계약에서는 모든 접근 권한을 취소할 수 있고 삭제는 하지 않지만 내용이 다른 사람에게 보이지 않게 할 수 있으므로,[55] 스마트계약에서처럼 삭제 대신 접근권한을 취소하는 것으로 대체하는 방안과 같이 블록체인 기술에 적합한 개인정보 파기를 인정하는 입법에 대한 고민이 뒤따라야 할 것이다. 최근 우리 개인정보보호법 상 개인정보 삭제 시 복구나 재생이 불가능하게 삭제해야 한다는 규정을 개정하기 위한 블록체인 관련법 제개정안이 나와 있다. 즉 2018.4.6 제안된 개인정보보호법 일부개정안{권은희의원 등 27인, 제2012932호, 제359회 국회(임시회)} 제21조 제1항에서

52) 김경환, 블록체인의 법률ㆍ제도 동향, 2017.11.23. ‘제4차 산업혁명 시대의 블록체인 기술과 프라이버시’ 심포지움 발표문 참조.

53) 실제 이러한 기능을 갖춘 타입은 이미 대규모 은행의 요구에 따라 개발되었지만 상당한 제한이 있다.

54) 이러한 문제 때문에 재편집가능한 블록체인 메커니즘에 대한 개발과 연구가 진행될 수 있을 것으로 보인다.

55) Winston Maxwell & John Salmon, supra note 5, at 11;, https://www.lexology.com/library/detail.aspx?g=918d13f7-92c5-4ef8-bfd1-fbf5f0a648b8; What does privacy mean on a public blockchain? 2018. 4. 16. https://hackernoon.com/what-does-privacy-mean-on-a-public-blockchain-1243776df22f

개인정보 파기의 범위를 내용을 확인할 수 없는 형태로 폐기하는 것으로 규정하고 있으며, 블록체인산업진흥기본법 제정안 제26조 제2항에서도 기술적 조치를 통해 내용을 파악할 수 없는 경우 파기로 간주하는 블록체인 기록 파기의 방법을 규정하여 블록체인 산업 활성화에 장애가 생기지 않도록 하고 있다.

<법안 대비표>

개인정보보호법 현행	개인정보보호법 개정안 (2018.4. 권은희 의원안)	블록체인산업진흥기본법안
제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.	제21조(개인정보의 파기) ① ---------- 파기 또는 기술적 조치를 통해 내용을 확인할 수 없는 형태로 폐기하여야 한다. ----------.	제26조 (블록체인 기록의 효력 및 파기) ① [생략] ② 개인정보가 포함된 블록체인 기록의 파기는 블록체인 기록의 내용을 파악할 수 없도록 하는 기술적 조치로 갈음할 수 있다.

6. 설계에 의한 개인정보 보호

가. 블록체인기술을 활용한 개인정보 보호

현재 알려진 개인정보보호설계기술로 '준동형 암호화(Homomorphic Encryption)'라는 새로운 종류의 암호화는 데이터를 복호할 필요 없이 암호화된 데이터에 대해 계산을 수행할 수 있게 한다. State channel이라는 오프체인 기술은 블록체인과 상호작용하지만 블록체인 밖에서 수행되므로 서비스 제공업체는 사용자 데이터를 비공개로 안전하게 유지할 수 있다. 앞에서도 살펴본 제로지식 증명 프로토콜은 안전한 인증 체계를 구축하거나 민감한 위조불가능한 데이터가 포함된 거래에 대해 더 나은 데이터 프라이버시를 제공하는 데 사용될 수 있으므로 GDPR 환경에서 매우 유용하다.[56] 제로지식증명기술을 실현하는 프로젝트로서 NuCypher와 Nuggets 프로젝트 등이 있다.[57] ZCash의

새로운 형태로 zk-SNARK 구현을 비롯한 여러 가지 변경 및 업그레이드를 가한 Bitcoin Private이 주목받고 있고, Ethereum도 블록체인에 zk-SNARK를 추가했다. 또한 Enigma 프로젝트 및 기타 개인 정보 보호에 집중한 프로젝트가 진행되고 있고, 이들은 블록체인 기술의 미래에 매우 중요하다.

나. 개인정보보호 설계의무의 부과

GDPR은 입법례로서는 세계 최초로 설계에 의한 개인정보보호 내지 개인정보보호의 내재화(Data protection-by-design and by-default, 이하 설계에 의한 개인정보보호라 함) 개념을 도입하고 있다(GDPR 제25조).[58] 즉 관리자는 구체적인 처리 목적에 따른 개인데이터만 처리되도록 보장하는 기술적 및 조직적인 대책을 강구하여야한다. 당해 의무는 수집된 개인 데이터의 양, 처리 범위, 저장 기간 및 접근가능성에 적용되며, 특히 개인 데이터가 개인의 관여 없이 불특정 다수의 자연인에게 접근되지 않도록 대책을 마련하여야 한다.

문제는 GDPR 제25조는 블록체인을 상정하고 마련된 규정이 아니라는 점이다. 앞에서 살펴본 바와 같이 퍼블릭 블록체인과 설계에 의한 개인정보보호원칙(principles of privacy by-design and by-default)은 긴장관계에 있다. 블록체인에 있어서는 데이터 보안(예: 암호화)을 제공하는 보안장치가 있지만 동시에 영구적인 분산저장, 개인에 대한 가명 연결가능성, 민감한 데이터에 대한 특별하고 추가적 보호를 제공하는 처리의 부족 및 개인의 청구를 처리하기 위한 책

56) Michiel Mulders, What is Zero-knowledge Proof? Meet the ZKP Projects, Last Updated On Aug 15, 2018 @ 08:35 UTC. https://cryptopotato.com/zero-knowledge-proofs-a-trend-towards-blockchain-privacy/

57) NuCypher는 프록시 재암호화(proxy re-encryption)를 위한 네트워크를 구축하는 강력한 ICO 프로젝트이다. Nuggets 프로젝트는 상품을 온라인으로 구매할 때 사용자가 주체가 되어 개인 데이터를 소유하고 상품을 구매하는 온라인 상점과 얼마나 많은 데이터를 공유할지 결정하는 방식으로 사용자에게 통제권을 돌려준다.

58) 제25조 제1항에서는 기술수준, 처리의 이행 비용, 성격, 범위, 내용 및 목적 및 처리에 기인한 자연인의 권리와 자유에 대한 일어날 수 있는 중대한 위험들을 고려하여 관리자는 본 규칙의 요건을 충족시키고 데이터 주체의 권리를 보호하기 위해 처리방법을 결정하는 시점 및 처리 시점의 양 시점에서 적절한 기술적 및 조직적 대책(예컨대, 가명화)을 실시해야 하고, 이는 데이터 보호의 원칙(예를 들어, 데이터 최소화)을 효과적인 방법으로 이행하고 필요한 보호 조치를 처리에 내재하도록 설계되어야 함을 규정한다. 제2항에서는 관리자는 기본적으로 각 구체적인 처리 목적에 따른 개인정보처리를 보장하기 위한 적절한 기술적 및 조직적인 대책을 실시하도록 의무지우고, 당해 의무는 수집된 개인 데이터의 양, 처리 범위, 저장 기간 및 접근가능성에 적용된다.

임 있는 제3자의 부재라는 특징 때문에 개인정보원칙을 준수하기 어렵다.퍼블릭 블록체인에 있어서도 제로지식증명기술 등을 활용하여 GDPR을 준수할 수 있도록 전략을 짜는 것이 앞으로의 기술적 과제가 될 것이다.

다. 소결

블록체인 데이터베이스가 어느 정도까지 설계에 의하여 개인정보보호의 기본원칙을 구현할 수 있는지는 기술의 진보에 달려 있다. 우리나라는 아직 입법이 없는 상태이므로, 개인정보를 고려한 기술 설계 내재화 의무를 지우는 GDPR의 예를 검토할 수밖에 없다. 아직 GDPR의 경우도 동 규칙 제25조에 따라 기업에 어떠한 기술적 조치를 의무화해야 하는지 명확하지 않으며 추상적 맥락, 위험, 비용 및 개별 평가 기준만을 제공하는데 그치고 있다. 아직 시행 초기이기 때문에 구체적인 내용은 업계의 이해관계자, 규제 기관 및 시민 단체의 합의에 의하여 정해질 것으로 보이는바, 좀 더 상황의 진전을 지켜보아야 할 것이다.

7. 개인정보보호에 대한 영향평가의무

GDPR 제35조는 개인데이터관리자에 대한 개인데이터보호 영향평가에 대하여 규정하고 있다. 즉 개인데이터관리자에게 신기술을 이용한 개인데이터 취급의 성질, 범위, 내용 및 취급의 목적을 고려하여 자연인의 권리와 자유에 큰 위험을 초래할 가능성이 있는 경우 그 취급 전에 개인데이터 보호에 대한 영향평가를 실시할 의무를 지우고(동조 제1항), 영향평가항목에는 예상되는 처리작업 및 처리목적의 체계적 기술, 처리작업의 필요성 및 비례성 평가, 데이터 주체의 권리 및 자유에 관한 위험 평가, 위험대책을 포함하도록 하고 있다(동조 제7항). 우리 개인정보보호법 제33조에서도 개인정보 영향평가에 대한 규정을 두고 있으나, GDPR과 달리 개인정보처리자가 아니라 공공기관의 장에게 의무를 지우고 있다.[59]

59) 즉 공공기관의 장에게 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하고 그 결과를 행정안전부장관에게 제출할 의무를 지우고(동조 제1항), 영향평가를 함에 있어서는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도 등을 고려하도록 하고 있다(동조 제2항).

아직 개인정보처리자에게 개인정보영향평가의무를 지우고 있지 않은 우리 법과는 달리 GDPR의 경우 개인데이터관리자에게 개인데이터 영향평가의무를 지우고 있으므로, 블록체인도 개인데이터 영향평가의 대상이 될 수 있다. 다양한 블록체인 시스템이 가능함을 고려하면 블록체인 시스템 별로 상이한 취급이 필요할 것이다. 즉, 개인 데이터 처리가 주목적인 블록체인 시스템의 경우 개인데이터 영향평가가 필수적일 수 있으나, 일반 블록체인(Non-specialised blockchains)과 같이 다루어지는 데이터 유형이 위험하다고 볼 수 없는 경우에는 a) 이용자에게 특정 종류의 개인정보의 게시를 금지하고, b) 이용자가 개인정보를 처리하려면 동의를 받거나 다른 법적 근거가 있는 경우로 제한하는 등 이용자에게 준수의무를 부과하는 대신, 관리자에게 별도의 데이터보호 영향평가의무를 지우지 않는 것도 고려할 수 있다.[60] 앞으로 블록체인을 활용한 서비스가 빠르게 늘어날 것으로 보이는바, 우리나라의 경우에도 개인정보 위험이 큰 경우 개인정보처리자에게 개인정보 영향평가의무를 지우는 방식으로 블록체인 기술을 포용하면서 기술적 위험에는 대비할 수 있도록 개인정보보호법을 개정할 필요가 있다.

8. 개인정보보호사건의 재판관할과 준거법

블록체인은 앞에서 정의한 바와 같이 분산형 장부로서 여러 국가들에 위치한 컴퓨터들과 관련될 수 밖에 없다. 따라서 분쟁이 발생하는 경우 기술 특성상 필연적으로 어느 나라의 법을 적용하여 어느 나라의 관할에 따라야 할지가 문제된다. 우리 개인정보보호법은 개인정보 처리를 둘러싼 분쟁에 외국사업자가 관계되는 경우 우리나라에 소재하는 이들의 주된 사무소, 영업소 또는 업무담당자의 주소지 관할을 전속관할로 하는 규정(제52조)을 두고 있는 외에는 외국사업자에 적용되는 규정을 두고 있지 않다.

반면 GDPR은 EU내에 사업장이 없는 개인데이터 처리자에게도 확대 적용된다고 규정한다. 즉 GDPR은 EU에 사업장이 없지만, EU 거주자에게 재화나 서비스를 제공하는 기업이나 EU 거주자에 대해 EU 내의 행동을 모니터링하는 기업에도 적용된다.[61] 이를 블록체인에 적용하면, 블록체인 시스템이 전세계에

60) Winston Maxwell & John Salmon, supra note 5, 21.
61) 개인정보처리활동이 (a) EU에 거주하는 데이터 주체에 대한 상품 또는 서비스의 제공(데

위치한 복수의 데이터 관리자와 관련될 수 있고 그들 중 일부는 EU내에 사업장이 없고 EU 거주자가 아닌 자이므로 이들이 GDPR의 적용대상에 포함할 수 있어서 재판관할과 준거법 문제는 복잡해질 수 있다.

국제적 분산형 블록체인 환경 하에서 준거법은 거래별로 분석되어야 할 것이다. 데이터 보호 준거법 규칙은 계약 준거법 규칙과 다르기 때문에 거래에 적용될 수 있는 데이터보호법은 계약법에 상응할 수 없다. 준거법은 GDPR 제3조에서 규정하는 요소들에 의해 결정된다. 블록체인의 국제적 성질과 GDPR의 적용의 광범위성을 고려할 때 GDPR은 유럽에 연결점이 부존재하거나 희박한 많은 블록체인에 기초한 거래에 적용될 것이다.[62]

블록체인 환경에서는 국제재판관할의 결정도 용이하지 않다. 중앙 서버 관리자가 있으면 그의 소재지에 국제재판관할이 집중될 수 있겠지만 블록체인에서는 전세계 노드의 위치 모두에 국제재판관할이 인정되는 경우 인터넷상 유비쿼터스 침해와 마찬가지로 관할 결정에 어려움이 있다.[63]

9. 소결

이상에서는 블록체인에 있어서 개인정보보호에 관한 개별적 쟁점으로 누가 개인정보처리 책임을 지는지, 개인정보처리원칙으로서 데이터 최소화의 원칙과 저장 제한의 원칙과의 충돌 문제, 블록체인에 있어서 개인정보 삭제가 가능한지 여부, GDPR의 경우 의무화하고 있는 개인정보보호 설계의무와 관련하여 공공블록체인과 설계에 의한 개인정보 보호와의 긴장관계를 어떻게 해결할 것인지, 개인정보처리자에 대한 개인데이터보호 영향평가의무를 지우는 문제, 개인정보보호사건과 재판관할과 준거법 문제를 중심으로 우리나라와 유럽 GDPR의 해당 규정을 중심으로 비교법적으로 검토해 보았다. 해석론으로 해결하기 어려운 부분들에 대하여는 개인정보보호법의 개정을 필요로 하므로, 이하에서는 개

이터 주체의 지불이 요구되는지 여부에 대해서는 묻지 않는다)이나 (b) EU 역내에서 이루어지는 데이터 주체의 행동 모니터링에 관련되는 경우 유럽연합에서 설립되지 않은 개인정보관리자 또는 처리자가 유럽연합에 있는 데이터 주체의 개인데이터를 처리하는 경우 본 규정이 적용된다. GDPR 제3조 제2항 참조.

62) Winston Maxwell & John Salmon, supra 5, at 11.

63) 국제재판관할을 넘어 역외에도 규제 관할권을 행사할 위험이 지적되기도 한다. 木下信行 · 岩下直行 · 久保田隆 · 本柳祐介, 「ブロックチェーンの法的檢討(下)」, 商事法務, 2017.4.15, 37-39 頁.

선을 위한 방향에 대하여 검토하기로 한다.

Ⅴ. 블록체인을 고려한 개인정보보호법제 개선 방향

1. 일반

위에서 블록체인과 개인정보보호법과의 충돌에 대하여 우리나라 법과 주로 EU의 GDPR의 관련 조항을 중심으로 살펴보면서 해석론만으로 한계가 있는 부분을 지적하였다. 분산형 인터넷으로서의 블록체인기술은 집중형 온라인 서비스를 기준으로 마련되고 제정된 개인정보보호원칙과 개인정보보호법제와 조화할 수 없는 면들이 있다. 단순한 해석론으로 해결될 수 없는 문제들에 대하여 블록체인기술을 상정한 개인정보보호법의 개선이 필요하며 이는 신규 ICT 기술 도입에 따른 단편적인 제도개선이 아닌 개인정보보호법제의 체계 변화를 필요로 한다고 할 것이다.

이하에서는 블록체인의 특성을 반영한 우리나라 개인정보보호법의 개선방안을 블록체인의 해시와 공개키의 개인정보성 명확화, 개인정보처리자 정의의 수정 등, 개인정보 삭제권에의 예외 인정, 설계에 의한 개인정보 보호, 개인정보보호영향평가, 준거법과 재판관할 규정의 설치 문제를 중심으로 검토하기로 한다.

2. 개인정보 개념의 확대

블록체인의 해시와 공개키, IP주소는 이용자의 인터넷 서비스 제공업체가 보유한 웹사이트 이용자를 식별하는데 필요한 데이터와 결합할 가능성이 있다면 개인정보가 될 수 있는바, 해당 정보만으로는 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우를 좀더 명확하게 할 필요가 있다. 유럽 GDPR에 따르면, 개인정보를 식별되거나 식별가능한 자연인에 관한 모든 정보로서 IP 주소, 쿠키 데이터, RFID 태그 등 웹 정보의 경우에도 개인정보의 범위에 포함됨을 명시하고 있으며(제4조), 앞에서 살펴본 Breyer 판결에서 식별이 가능한지를 판단하는 기준을 식별에 소요되는 시간, 비용, 인력에 과도한 노력이 드는지, 법에서 식별을 금지하고 있는지, 식별의 위험이 현저한지를 들고

있는바, 개정에 있어서 참조가능할 것으로 보인다.[64]

3. 개인정보처리자 정의의 수정 등

우리 개인정보보호법은 일본법과 유사하게 개인정보처리자의 개인정보 처리의 목적을 “개인정보 파일 운용”을 위한 경우로 한정하고 있다. 이와 같이 개인정보처리자의 정의를 협의로 하는 경우 다양한 유형의 블록체인 시스템에서 개인정보를 처리하는 자를 그 적용범위에 포섭할 수 없는 문제가 있다. 유럽 GDPR의 경우와 같이 개인정보의 처리를 하는 자로 포괄적으로 정의하고 공동관리자 내지 복수관리자에 대하여도 규정을 둘 필요가 있다고 생각한다. 아울러 블록체인 기술의 발전 동향을 계속 살피면서 개인정보처리자의 책임과 관련하여 보험처리나 블록체인 시스템 운영자에게 일정 부분 책임을 지우는 방안도 함께 고려되어야 할 것이다.

4. 개인정보 삭제·파기의 대체 인정

블록체인 환경에서는 시스템이 삭제를 방지하도록 설계되었으므로 삭제 또는 파기는 기술적으로 불가능하다. 나중에 편집가능한 블록체인 메커니즘은 가능은 하나 경제적 실효성에 문제가 있을 수 있다. 이에 삭제 또는 파기의 개념에 신기술 특성상 삭제 또는 파기가 불가능하다면 이에 대체될 수 있는 있는 되돌릴 수 없는 암호화(irreversible encryption) 또는 접근권한을 취소하는 것도 포함하도록 하여, 블록체인 기술에 적합한 개인정보 삭제 또는 파기를 인정하는 개정 방안을 마련할 필요가 있다.

5. 설계에 의한 개인정보 보호

블록체인에 개인정보보호법이 요구하는 개인정보보호 수준을 설계할 수 있도록 우리나라 개인정보보호법 제29조의 안전조치의무를 넘어서서 GDPR과 같이 개인정보보호의 설계를 내재화하도록 하는 개정을 고려하여야 할 것이다. 즉

64) 아울러 이러한 식별기준에 따라 개인데이터에 해당한다고 하더라도, 일부 새로운 블록체인 기술을 사용하면 개인데이터에 해당하지 않게 될 가능성도 배제할 수 없다.

블록체인 시스템이 개인의 권리와 자유에 대한 위험을 초래하지 않도록 보장하기 위하여 데이터보호 방법의 설계를 내재화하는 개인정보 보호 시스템을 구축하도록 의무 지워야 할 것이다. 개인정보보호원칙을 블록체인에 구현함에 있어서는 블록체인의 장점을 최대한 훼손하지 않도록 블록체인 기술에 적합한 개인정보 침해를 회피하는 설계가 인정될 수 있도록 하고 구체적 가이드라인을 마련할 필요가 있을 것이다.

이를 통해 블록체인기술을 사용하는 회사들은 블록체인 기반 응용 프로그램을 개발하는 초기 단계에서 개인정보보호법을 비롯한 관련 규제 틀을 고려하여 특정기술설계가 해당 법률에 명시된 요구 사항들을 충족하는지 확인하여 법적 안정성을 기할 수 있을 것이다.

6. 개인정보보호영향평가

앞에서 살펴본 바와 같이 현행 개인정보보호법 제33조는 공공기관의 장에게 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가의무를 부과하고 있어 개인데이터 관리자에게 의무를 부과하는 GDPR과는 다르다. GDPR과 같이 우리법도 개인정보처리자에게 영향평가의무를 부과하고, 다양한 블록체인 시스템 중 개인정보 침해의 위험이 큰 경우를 포함할 수 있도록 개인정보보호법 제33조의 개인정보 영향평가에 관한 조항을 개정하여야 할 것이다.

블록체인의 경우 다양한 블록체인 시스템이 가능하므로 블록체인 사업자의 입장에서는 자신의 시스템이 개인정보보호영향평가의 대상인지 확인할 수 있도록 구체적 개인정보보호영향평가 가이드라인을 마련할 필요가 있다.

7. 준거법과 재판관할 규정의 설치

GDPR에서 보는 바와 같이 개인정보보호법의 적용범위와 재판관할에 관한 규정을 설치하여 블록체인과 관련한 개인정보보호법의 적용범위와 그 관할을 명확히 하여야 할 것이다. 국외에서 이루어진 행위라도 국내시장에 영향을 미치는 경우에는 적용함을 명문으로 규정하고 있는 공정거래법 제2조의2 처럼 역외적용을 명시하는 개정 방안도 고려해 볼 수 있을 것이다.

8. 소결

단기적으로는 앞에서와 같이 블록체인의 해시와 공개키의 개인정보성 명확화, 개인정보처리자 정의의 수정, 개인정보 삭제권에의 예외 인정, 설계에 의한 개인정보 보호, 개인정보보호영향평가, 준거법과 재판관할 규정의 설치 등에 대한 개인정보보호법 개선 방안을 마련하는 것이나, 장기적으로 블록체인기술을 상정하여 중앙집중형, 분산형 기술 양자를 포섭하는 기술 중립적인 개인정보보호 법제를 마련함으로써 개인정보보호법제의 체계 변화를 도모할 필요가 있다. 블록체인 시스템을 개인정보보호법 안으로 수용하는 것은 블록체인 프로젝트들이 개인정보보호법을 준수할 수 있도록 지침을 제공하고 이용자에게 개인정보를 제어할 권리를 부여하여 개인이 스스로 자신의 데이터를 저장·관리하고 제3자에 대한 데이터 제공을 통제할 수 있게 하는 것이기 때문이다.

Ⅵ. 결론

블록체인 기술이 4차산업혁명시대에 개인주도 개인데이터 소유와 이용 활성화라는 두 마리 토끼를 잡음으로써 우리사회에 엄청난 매직을 선사할 수도 있다. 그러나 이를 위하여는 먼저 개인정보 보호 문제에 대한 큰 장벽을 넘어야 한다.

이를 위하여 필자는 먼저 블록체인에 있어서 개인정보보호에 관한 일반적 쟁점으로서 블록체인이 개인정보를 포함하여 블록체인이 개인정보보호법의 적용을 받는지의 문제를 다룬 후, 블록체인에 있어서 개인정보보호에 관한 개별적 쟁점들로서 첫째, 블록체인 차원에서 개인정보처리자는 누구인지의 책임의 주체 문제를 살펴보고, 둘째, 개인정보처리의 원칙을 검토하고, 셋째, 동의문제를 살펴본 후, 넷째, 개인정보 삭제의 문제를 다루고, 다섯째, 설계에 의한 개인정보보호 문제를 다루었으며, 여섯째, 개인정보보호영향평가의 문제를 검토하였으며, 일곱째, 블록체인과 재판관할과 적용법의 문제를 함께 다루었다. 물론 쟁점사항들의 검토에 있어서는 블록체인기술이 구현되는 모델이 다양하기 때문에 일반화하기 어려운 한계가 있음을 감안하였다.[65] 개인정보를 취급하고 있지 않아 최소한의 데이터관리 메커니즘만 필요한 경우가 있는 반면 일부 프로젝트는

개인정보보호영향평가를 위해 고위험 데이터 처리를 필요로 하는 경우도 있어 블록체인 프로젝트별로 다른 취급을 하여야 하기 때문이다.

이러한 검토를 토대로 현행법제에 대한 개선방안으로서 블록체인의 해시와 공개키의 개인정보성을 명확하게 하는 개인정보 개념의 확대, 개인정보처리자 정의의 수정, 개인정보 삭제·파기의 대체 인정, 설계에 의한 개인정보보호, 개인정보보호영향평가, 준거법과 재판관할 규정의 신설 문제를 중심으로 살펴보았다.

블록체인과 개인정보보호법 등의 개선과 관련해서는 국제규범과의 정합성도 함께 검토되어야 할 것이다. 아울러 블록체인기술의 개인정보 보호원칙과의 조화 문제를 넘어서 개인주도의 개인정보 관리에 블록체인이 큰 역할을 할 것으로 보이는바, 향후 몇 년 동안은 개인정보를 포함하는 다양한 종류의 다량의 데이터를 안심하고 안전하게 유통·활용할 수 있는 환경을 정비하기 위하여 개인주도의 개인정보 유통과 보호 기술과 제도에 관한 다양한 실증실험이 진행되어야 할 것이며 이를 지원하는 정부의 정책도 뒷받침되어야 할 것이다.

본고에서의 블록체인과 개인정보보호관련 쟁점 사항 검토와 우리 개인정보보호법의 개선방안 제시가 4차 산업혁명으로 도래한 데이터경제에 있어서 개인정보 보호와 혁신(Innovation)의 양립을 위한 정책개선방안 수립과 개인정보보호법, 정보통신망법 등 관련 법령 개선에 도움이 되기를 바란다.

투고일 : 2018.11.30 / 심사완료일 : 2018.12.8 / 게재확정일 : 2018.12.10

65) 블록체인과 대부분의 클라우드 컴퓨팅 환경의 주요 차이점은 블록체인 시스템의 경우는 하나의 스토리지 또는 컴퓨팅 자원 업체에 의존하지 않는다는 점이다.

[참고문헌]

국회 법제실,「4차산업혁명 대응 입법과제」, 2017.12.

김경환, 블록체인의 법률 · 제도 동향, 2017.11.23. '제4차 산업혁명 시대의 블록체인 기술과 프라이버시' 심포지움 발표문.

김혜리 · 홍승필, "블록체인 네트워크에서의 개인정보보호 방안 연구-개인정보보호 컴플라이언스 중심",「보안공학연구논문지」 제15권 제2호, 보안공학연구지원센터, 2018.

김현경, "블록체인과 개인정보 규제 합리화 방안 검토",「법학논집」 제23권 제1호, 이화여자대학교 법학연구소, 2018.

비트뱅크 · 블록체인의 충격 편집위원회(김응수, 이두원 역),「블록체인의 충격-비트코인, 핀테크에서 IoT까지 사회 구조를 바꾸는 파괴적인 기술」, 북스타, 2017.

정상조 · 남효순,「인터넷과 법률Ⅱ」, 법문사, 2005.

스콧 갤러웨이(이경식 옮김).「플랫폼 제국의 미래」, 비즈니스 북스, 2018.

아카바네 요시하루 외(양현 역),「블록체인 구조와 이론」, 위키북스, 2017.

장세균, "정밀의료에서 개인정보보호 방안-미국・EU・일본과의 비교법제도 분석을 중심으로", 연세대학교 보건대학원, 석사학위논문, 2017.6.

정승화, "블록체인 기술기반의 분산원장 도입을 위한 법적 과제-금융산업을 중심으로-",「금융법연구」 제13권 제2호, 한국금융법학회, 2016.

제355회 국회 제5차 4차 산업혁명 특별위원회, 4차 산업혁명 관련 제3차 공청회-빅테이터, 클라우드, 개인정보, 공공데이터 개방 등 관련-, 2018. 1.23.

조성훈,「자본시장에서의 블록체인 기술의 활용전망 및 시사점」, 자본시장연구원 조사보고서 16-07, 2016.11.

木下信行 · 岩下直行 · 久保田隆 · 本柳祐介,「ブロックチェーンの法的檢討(下)」, 商事法務, 2017. 4.15.

Anthony Lewis, A Gentle Introduction to Blockchain Technology 4, https://perma.cc/H3AX-XJXX (archived Oct. 27, 2017).

Anthony Mandelli, Blockstack Unveils Decentralized Tokenized Blockchain Web Browser, Bitcoin Technology May 27, 2017.

EU Blockchain Observatory and Forum, Blockchain and the GDPR, 2018.

F. Gregory Lastowka & Dan Hunter, The Laws of the Virtual Worlds, 92 Cal. L. Rev. 40 (2004).

Joshua A.T. Fairfield, Virtual Property, 85 B.U.L. REV. 1049~50 (2005).

Klaus Schwab, The Fourth Industrial Revolution: what it means, how to respond, 14 Jan 2016.

Michael A. Carrier & Greg Lastowka, Against Cyberproperty, 22B.T.L.J. 1485(2007).

Nicholas Davis, What is the fourth industrial revolution? 19 Jan 2016.

Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. REV. 2164 (2004).

Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815 (1999).

R. Polk Wagner, On Software Regulation, 78 S. CAL. L. REV. 457 (2005).

Winston Maxwell & John Salmon, A guide to blockchain and data protection.

Winston Maxwell & John Salmon, Blockchain and the right to erasure, January 12 2018.

Raymond Wacks, Law, Morality, and the Privacy Domain, Hong Kong Univ. Press 2000.

[국문초록]

블록체인과 개인정보보호
- 블록체인의 매직(Magic)과 법적 도전 -

박 진 아*

4차 산업혁명의 기반 기술의 하나로 알려진 블록체인 기술은 최근 집중형 온라인 서비스가 안고 있는 많은 문제를 해결할 수 있는 분산형 인터넷으로 기대를 모으고 있다. 세계 스타트업들은 블록체인을 사용하는 소프트웨어를 개발하고 개념 증명(Proof-of-Concept, PoC)을 수행하기 위해 전통적인 자금 조달과 토큰 발급 방법을 사용하고 있다.

블록체인 기술의 주요 장점으로는 개인간 거래를 가능하게 하는 탈중개성(脫仲介性), 손쉽게 활용할 수 있는 확장성(scalability), 모든 사용자가 거래장부를 분산, 저장 관리하는데 따른 뛰어난 보안성(security), 높은 투명성(transparency)을 들 수 있다. 그러나, 모든 노드에서 블록체인을 통과하는 정보를 볼 수 있고 블록에 저장된 정보는 제거할 수 없다는 특징이 개인정보보호의 중요한 원칙을 규정한 개인정보보호법과 충돌할 수 밖에 없다. 많은 클라우드 환경에서 그렇듯이 블록체인 관리자는 개인 데이터가 블록체인에 있는지, 그리고 그 데이터가 중요한지를 알 수 없다. 블록체인은 이전 블록을 가리키는 해시, 암호화된 거래 데이터 및/또는 체인 외부에 저장된 데이터를 가리키는 해시를 표시하기 때문이다. 데이터 보호의 관점에서 볼 때 블록체인의 특징은 시스템 고유의 것이 아니며 기술 설계가 각각 수정될 경우 어느 정도 회피될 수 있다. 그러나 개인정보침해를 회피하는 설계는 블록체인의 장점을 훼손하는 딜레마가 있다.

블록체인 기술의 활용을 고려하는 회사는 블록체인 DB 및 응용 비즈니스 모델의 법적 준수를 위하여 고심하고 있으나, 아직 우리나라를 비롯한 세계주요

* 기술과법연구소 소장, 법학박사 · SJD.

국의 개인정보보호법제는 블록체인 기술개발자에 대한 명확한 법적 가이드라인을 제시하고 있지는 못한 실정이다.

이에 본 논문은 현행 개인정보보호원칙과 블록체인 기술의 충돌가능성을 중심으로 해석론과 함께 개선방안을 제시함으로써 블록체인 기술의 장점을 최대한 활용하면서도 프라이버시를 보호하는 방안을 모색해 보도록 할 것이다. 구체적 논의 순서는 첫째, 블록체인 개념, 특징 및 유형(Ⅱ)에서는 블록체인 일반론을 개인정보보호 문제와 관련된 부분을 중심으로 개괄적으로 다루고, 둘째, 블록체인과 개인정보보호에 관한 일반적 쟁점(Ⅲ)에서는 블록체인과 개인정보보호법과의 충돌, 주요국의 개인정보보호법제 개관, 블록체인의 개인정보 포함 여부를 중심으로 검토하고, 셋째, 블록체인과 개인정보보호에 관한 개별적 쟁점(Ⅳ)에서는 블록체인과 개인정보 보호의 충돌에 따른 개인정보보호법의 개별적 이슈들을 검토할 것이다. 넷째, 블록체인을 고려한 현행법제에 대한 개선방안(Ⅴ)에서는 블록체인기술을 개인정보보호법 내부로 수용할 수 있는 구체적 개선방안을 제안할 것이다.

주제어 : 블록체인, 개인정보(보호), 개인정보처리자, 삭제, 설계

[Abstract]

Blockchain and Personal Data Protection
- Magic of blockchain and challenges to law thereof -

Park, Jina*

The use of blockchain technology can, and will, change our society profoundly. A blockchain as the next big thing for the decentralized internet is in essence a digital ledger containing lines of data or information. Such a ledger can contain different types of data, varying from transaction records, transactional attributes, credentials, or any other piece of data or information. As a matter of principle only lines of data can be added to this digital ledger, and none can be removed or altered.

My aim in this article is to deal with blockchain technology and personal data protection and its use. For this purpose, first of all, I will attempt to answer the question "Is blockchain subject to personal data protection law?" Firstly, I will examine whether hash and public key of a blockchain system are personal data or anonymised data. Secondly, I will deal with the question "Who is the data controller and the data processor in a blockchain context?" Thirdly, the principle of personal data processing will be discussed. Fourthly, the issues of contract will be discussed. Fifthly, the problem of personal data deletion will be addressed. Sixthly, the issues of the applicable law and jurisdiction will be examined. Seventhly, I will discuss the problem of data protection impact assessment. Of course, I will take into account that there are limitations that can not be expressed in general because of the variety of models in which the blockchain technology is implemented. The answers to these questions may lead to the conclusion that a given blockchain project'

* Dr., Korea Institute of Technology And Law.

nexus to personal data is so remote that only minimal data governance mechanisms are required. By contrast, some projects will involve high-risk data processing, requiring a full-blown data protection impact assessment.

Based on the above review and discussion, I will suggest ways to improve the existing personal information protection law. In order to improve the personal information protection law considering the blockchain technology, compatibility with international norms should also be examined. Beyond the harmonization with the privacy principles of the blockchain technology, the blockchain seems to play a big role in the personal information management led by the individual. In the next few years, various personal-led personal information distribution and protection technologies and systems projects should be conducted to ensure that a large amount of data, including personal information, can be distributed and utilized safely and securely. It should also be supported by government policies supporting these projects.

I hope that this paper will help to improve policies for taking balance between privacy and innovation in the data economy coming from the 4th Industrial Revolution, and improve related laws such as the Personal Information Protection Act and the Information and Communication Network Act.

Key words : Blockchain, Personal Data (Protection), data controller, deletion, design.