J. Inf. Technol. Appl. Manag. 25(2): 113~146, June 2018
https://doi.org/10.21219/jitam.2018.25.2.133

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

개인정보보호법제 관점에서 본 블록체인의 법적 쟁점 GDPR 및 국내 개인정보보호법을 바탕으로

박민정* · 채상미** · 이명준***

Legal Issues of Blockchain in Personal Information Protection : Based on GDPR and Personal Information Protection Act

Minjung Park* · Sangmi Chai** · Myoung Jun Lee***

Abstract

The technical definition of Blockchain is commonly known 'distributed ledger', however, there is no legal definition for being accepted in worldwide. Therefore, unless legal definitions and concepts of Blockchain are presented, there is a possibility that various legal disputes will occur in the future in Blockchain environment. The purpose of this study is to derive legal issues related to personal information protection that can be conflicted in Blockchain environment based on domestic Privacy Act and GDPR. The outcomes of this study can prevent various legal disputes and provide solutions that may occur due to the spread of Blockchain. It also suggests the foundation for the improvement of Privacy Act. Finally, it contributes to activate of Blockchain, industry, in Korea.

Keywords : Blockchain, Distributed Ledger, GDPR, Personal Information Protection, Privacy Act

Received : 2018. 06. 16. Revised : 2018. 06. 25. Final Acceptance : 2018. 06. 26

* Department of Business in the Graduate Student of Ewha Womans University, e-mail : mjpark67@ewhain.net
** Corresponding Author, Associate professor, Department of Business, Ewha Womans University, 52, Ewhayeodae-gil, Seodaemun-gu, Seoul, 03760, Korea, Tel : +82-2-3277-2780, e-mail : smchai@ewha.ac.kr
*** Attorney at law, Harmony Law Office, e-mail : badook98@naver.com

1. 서 론

2016년, 세계경제포럼(World Economic Forum, WEF)은 4차 산업혁명 시대의 핵심기술로 블록체인을 선정하였으며 올해까지 전 세계 은행의 80%가 블록체인 기술을 도입할 것으로 전망하였다. 이와 같이 블록체인 기술은 금융 분야를 비롯하여 제조 및 유통, 공공서비스, 사회・문화 부문의 전 영역에 걸쳐 혁신적인 변화를 일으키는 새로운 패러다임이다[Morabito, 2017].

블록체인은 참가자 사이에 발생한 거래정보가 담긴 원장을 특정 기관의 중앙 서버가 아닌 네트워크에 분산하여 참여자가 공동으로 기록하고 관리하는 분산 장부 기술(Distributed Ledger Technology)인 특징을 갖는다[Maull et al., 2017]. 즉, 하나의 분산원장 시스템인 블록체인은 중앙화된 기관의 개입이 없는 Peer-to-Peer 네트워크이다[Lee et al., 2018]. 따라서 노드 간 통신이 이루어지며 네트워크에 참여한 모든 노드가 동일한 장부를 소유하는 동시에 데이터를 공유하게 된다. 이렇게 공유된 데이터를 바탕으로 블록체인은 발생된 거래를 검증하기 때문에 데이터의 위・변조가 어렵다[Oh and Lee, 2017]. 이와 같이 블록체인은 한번 저장된 데이터의 수정 및 삭제가 어려운 특징을 갖기 때문에, 이러한 특징을 기반으로 현재, 블록체인 기술이 다양한 분야에서 적용되고 있다. 먼저, 의료분야에서 IBM Waston Health 사업부는 미국 식품의약청(FDA)과 블록체인 기술을 이용하여 의료 연구 목적 등으로 환자 데이터를 공유할 수 있는 공동기술 개발을 체결하였다[ComputerWorld, IBM Waston, 2017]. 이는 임상실험 결과 등을 비롯하여 관련된 다양한 데이터의 위, 변조를 방지하여 보다 투명한 연구 결과의 보존과 원활한 교환을 블록체인 프레임워크에서 가능하게 하는 것에 주된 목적이 있다. 이외에 추가적으로 세계 여러 국가에서 전자의무기록(EMR) 관리의 효율성 및 보안성 강화를 위한 방법으로 블록체인 기술 도입을 고려하고 있다. 의료분야뿐만 아니라, 국내 은행 및 카드사는 블록체인의 적용을 통한 모바일 쿠폰을 발행하기 시작하였다. 이는 블록체인 플랫폼 안에서 발행된 쿠폰을 지속적으로 추적, 관찰하여 위・변조를 통한 부정사용 및 도용을 방지하고 제휴가맹점의 쿠폰 발행, 정산 과정을 간소화하기 위하여 도입되었다. 위와 같은 사례는 공통적으로 블록체인 기술의 비가역성을 통하여 이전에 발생 가능하였던 각종 문제를 방지하고 해당 서비스의 효율성을 향상시키고자 하는 목적을 가지고 개발 및 도입되었으나 모두 민감정보를 비롯한 개인정보가 주된 저장 및 수집 대상의 데이터임에 따라, 본 연구는 블록체인 기술이 개인정보보호 측면에서 갖는 이슈를 살펴볼 필요성이 있다고 판단하였다.

블록체인은 기술적으로는 '분산원장'이라는 개념으로 통용되지만 국내 현행법을 비롯하여 전 세계적으로 합의된 법률적 정의 및 성격은 존재하지 않는다. 이에 따라 국내를 비롯하여 전 세계적으로 블록체인과 관련된 입법 추진 활동을 시작하였으나, 블록체인의 법적 지위 및 권한을 명확히 하기 어려운 실정이다. 이에 따라, 국외에서는 블록체인을 '탈중앙화된 자율 조직(DAO, Decentralized Autonomous Organization)으로 정의하여 사전에 결정된 규칙에 의하여 작동하고 인간의 개입이 매우 제한되거나 사실상 없는 자율 조직의 상태로 간주하는 것이 일반적이다[Yook, 2018]. 그러나 이러한 조직의 경우, 법률에 의한 적절한 법적 지위 및 권한을 부여 받지 못하거나 계약 등에 의한 참여자 사이의 책임 관계를 분명히 하지 않는다면, 블록체인을 처음 구축한 자와 블록체인의 노드를 구성하는 참여자 모두가 무한책임을 지는 문제가 발생할 수 있다[Seo et al., 2016]. 즉, 블록체인에게 부여되는 법적 지위와 권한에 따라, 참여자의 손해배상의 책임 여부 및 범위가 결정된다. 따라서 블록체인의 법적 속성을 정의하고 이에

따른 블록체인 기술을 감독하고 관련 법적 분쟁을 해결하기 위한 법적 보호장치가 필요함에도 불구하고 아직 이에 대한 준비는 전 세계적으로 미비한 실정이다[Kiviat, 2015]. 이에 본 연구는 기존 법률에 따라 블록체인 기술을 적용하는 경우, 부합되지 않는 일부 흠결을 보완하거나 새로운 제도의 선행을 통하여 블록체인의 정착 및 관련 기술의 활성화를 기대할 수 있을 것으로 보았다. 이에 다음과 같은 연구 목적을 제시한다. 첫째, 국내 개인정보보호법 등을 비롯한 관련 현행법 및 GDPR (General Data Protection Regulation, 유럽연합 개인정보보호 일반법)의 관점에서 블록체인 기술의 적용에 따라 위반의 소지가 있는 개인정보보호 관련 쟁점을 도출하고자 한다. 블록체인 기술은 최근 도입됨에 따라, 국내 개인정보보호법과 더불어 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 및 전자금융거래법 등에 의거하여 블록체인 사항을 모두 규제하기 위한 관련 법규가 존재하지 않거나 일부 상충될 것으로 판단된다. 이와 더불어 2018년 5월, 시행을 앞두고 있는 GDPR의 관점에서 블록체인 기술의 GDPR 조항 준수 여부를 살펴본다. GDPR은 유럽연합 회원국과 더불어 유럽연합 정보주체에게 서비스를 제공하거나 유럽 내 거주하는 정보주체에 대한 모니터링을 실시하는 국내를 비롯한 전 세계 기업 등이 적용 대상이 되는 유럽연합의 개인정보보호법이다[Park et al., 2018]. 둘째, 본 연구는 블록체인 기술의 적용에 따라 발생 가능한 개인정보보호 관련 주요 법적 쟁점을 도출함에 따라 이를 기반으로 법제적 대응방안을 제안하고자 한다.

국내 개인정보보호법 등의 주요 관련 법규와 GDPR의 관점에서 블록체인 기술 적용에 따라 발생 가능한 법률적 쟁점을 도출하는 것은 다음과 같은 시사점을 갖는다. 첫째, 블록체인 환경에서 발생 가능한 법률적 위반 소지가 있는 사항을 미리 살펴봄에 따라 향후, 국내 환경에 블록체인의 안정적인 정착을 위하여 법적 보호장치와 같은 국가적 조치의 마련이 필요함을 제시한다. 구체적으로, 본 연구의 결과는 블록체인 확산에 따른 국내 관련 법안의 개정 및 제정을 위한 토대가 된다. 둘째, 본 연구는 GDPR의 환경에서 블록체인 기술의 적용이 위반 가능한 조항을 제시함에 따라, 블록체인 산업 관련 기업의 대비 전략 형성에 기여한다. GDPR의 위반은 최대 약 270억 원 혹은 글로벌 매출액의 4% 중 높은 금액의 벌금이 적용됨에 따라, 이는 기업의 심각한 경제적 손실 및 경영 지속의 어려움을 초래할 수 있기 때문에 GDPR의 적용이 되는 글로벌 기업은 반드시 이를 준수하여야 한다. 특히, GDPR 준수의 적용이 되는 기업은 앞서 제시한 바와 같이, 유럽연합에 사업장을 보유하였거나 유럽 거주 시민의 개인정보를 처리하는 모든 기업에게 적용됨에 따라, 유럽연합 회원국을 비롯하여 국내 기업 및 다수의 글로벌 기업이 영향을 받기 때문에 이에 대한 대비가 반드시 필요하다. 따라서 블록체인 기술 환경에서 발생 가능한 GDPR 위반 소지가 있는 각 쟁점의 도출은 현재 블록체인 관련 기술을 도입한 기업 및 블록체인 관련 기술을 적용할 다양한 산업군의 GDPR 준수에 기여한다.

2. 블록체인의 개인정보보호 법적 쟁점

개인정보 관련 사고의 규모가 점차 대형화되고 피해 형태가 다양해짐에 따라, 각 국은 관련 법규를 제정하거나 제도를 신설하여 개인정보 주체의 권리를 보호하기 시작하였다. 국내의 경우, 1995년 개인정보보호법의 제정 및 시행을 주축으로, 정보통신망법, 신용정보법, 전자금융거래법 등을 통하여 개인정보를 보호하고 있다. 본 연구에서는 국내 관련법과 GDPR의 환경에 블록체인 기술이 적용되었을 때, 상충 가능한 이슈 8가지를 다음과 같이 도출하였다.

2.1 개인정보 수정 및 삭제

개인정보보호법 제36조는 다른 법령에 명시되어 있는 경우를 제외하고 개인정보 처리자에게 개인정보의 정정 및 삭제를 요구할 수 있음을 규정한다. 이와 유사하게 GDPR은 16,17조의 정정권 및 삭제권을 명시하여 개인정보 주체가 원하는 경우, 개인정보 데이터를 수정하거나 삭제할 수 있도록 하였다. 즉, 국내 개인정보보호법과 GDPR은 공통적으로 개인정보의 수정 및 삭제를 요구할 수 있는 개인정보 주체의 권리를 보장하고 있다. 하지만 블록체인상에 저장된 데이터는 수정과 삭제가 어렵기 때문에 개인정보 주체의 수정 및 삭제에 대한 권리를 블록체인 환경에서 확보하는 것은 현실적으로 불가능하다. 블록체인에 저장된 데이터를 수정 및 삭제하기 위해서는 블록체인 내에 있는 모든 참여자가 '포크'를 만드는 것에 동의하여야 하는 과정이 선행되어야 한다. 포크는 개발자들이 하나의 소프트웨어 소스를 복사하여 독립적이면서 새로운 소프트웨어를 개발하는 것이다. 따라서 처음 블록체인이 형성되는 시점 이후부터 기존 데이터를 수정 및 삭제하거나 새로운 데이터를 추가하기 위해서는 모든 참여자들이 매번 이에 대하여 동의하여야 한다. 이와 같이 기술적으로는 블록체인상에 이전에 저장된 데이터를 수정 및 삭제하는 것이 가능할 수 있으나, 다수의 참여자가존재하는 블록체인 환경에서 모두의 합의를 유도하는 것은 실질적으로 불가능하다. 특히, 퍼블릭 블록체인과 같이 익명의 참여자로 구성되는 경우, 이는 더욱 더 어려워진다. 따라서 블록체인 환경에서는 기등록된 거래정보에 대한 수정 및 삭제 기능이 제공되지 않음에 따라, 개인이 한 번 제공한 정보에 대하여 이를 수정 및 삭제하여 새로운 정보를 대체할 수 없다. 예를 들어, 현재 시장이 확장되기 시작한 블록체인 기반의 전자상거래 이용자들은 본인의 의사에 따라 쉽게 거래 철회를 할 수 없으며, 배송 주소, 연락처 등 기본적인 개인정보의 수정도 모든 블록에 기록을 남기며 이루어져야 하는 단점이 있다. 이에 개인의 '잊혀질 권리'의 보장이 블록체인 환경에서는 불가능하다. 결론적으로 GDPR 및 국내 개인정보보호법에서는 정보 주체가 요구하면 정보를 삭제해야 하나, 블록체인 기술 환경에서 주체의 요구에 따라 정보를 삭제 및 수정하여 거래에 매번 반영하는 것은 어렵기 때문에 법률 위반의 소지가 있다.

2.2 개인정보 파기

블록체인상에 저장된 데이터는 파기 및 거래 내용의 취소가 불가능하다. 블록체인 네트워크상에서는 모든 거래참여자가 거래 내역을 볼 수 있으며, 이는 원장이 아닌 거래참여자를 포함하여 거래의 전체 내역을 별도의 허가 없이 열람이 가능하다. 이러한 블록체인의 비가역성은 블록체인 장부에서 정보를 삭제하는 기능의 구현이 어려움과 동시에 일반적으로 다수의 거래참여자가 원장의 데이터를 소유하고 있기 때문에 모든 데이터가 삭제되었음을 입증하는 것이 어렵다[Lee et al., 2018]. '개인정보의 파기'는 앞서 제시한 '개인정보 삭제'와 유사한 개념으로 혼동될 수 있으나 다음과 같은 이유에서 구분된다. 먼저, '개인정보 삭제'는 이미 제공한 개인정보에 대하여 개인정보 주체가 개인정보의 위험성 등을 인식하여 개인정보를 삭제해줄 것을 제공받은 개인정보 처리자 등을 대상으로 요구하는 권리인 반면에 '개인정보의 파기'는 개인정보 처리자 및 서비스 제공자가 이미 수집 및 보관한 개인정보에 대하여 보유기간의 경과, 수집 목적의 달성, 거래의 종료 등과 같이 법적으로 명시된 사항이 충족되는 경우, 개인정보 처리자가 이를 파기하여야 하는 의무이다. 따라서 개인정보의 파기는 국내 법 및 GDPR에 의거하여 개인정보 처리자 및 프로세서에게 귀속되는 법적

의무사항이나, 개인정보의 삭제와 관련된 사항은 개인정보 주체가 갖는 법적 권한이다.

블록체인상에 저장된 데이터의 파기가 불가능한 것에 반하여, 국내 관련법과 GDPR은 각각 개인정보 처리자 등의 개인정보 파기 의무에 대하여 규정하고 있다. 이를 각각 살펴보면 다음과 같다. 먼저, 개인정보보호법 제21조의 내용을 살펴보면, 개인정보 처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 다른 법령에 따른 예외 사항을 제외하고서는 지체 없이 그 개인정보를 파기할 것을 명시하고 있다. 이와 유사하게 전자금융거래법 제22조의 2항에 따르면 금융회사 등은 보존 기간이 경과하고 금융거래 등 상거래관계가 종료된 경우에는 5년 이내에 전자금융거래기록의 파기, 신용정보법 제20조의 2는 다른 법률에 명시된 불가피한 경우를 제외하고 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제할 것을 규정한다. 구체적으로, 국내 신용정보법은 신용정보주체에게 불이익을 줄 수 있는 연체 정보 등의 신용정보는 5년이 경과되는 경우, 개인의 요청과 관계 없이 해당 정보를 수집 및 보관하고 있는 신용정보회사 등은 이를 파기하여야 하는 의무가 있으나, 블록체인 환경에서는 이미 수집 및 저장된 정보에 대하여 삭제가 불가능함에 따라 해당 사안에 대하여 법적 위반 소지가 있을 것으로 판단된다. 또한 정보통신서비스 제공자 등 역시 개인정보의 수집 및 이용 목적이 달성된 경우, 개인정보의 보유 및 이용기간이 끝난 경우 등을 비롯하여 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보 파기 등 필요한 조치를 취할 것을 제시한다. 즉, 목적된 거래의 성립 등과 같은 파기 사유를 명시한 신용정보법 및 전자금융거래법과 다르게 정보통신망법은 보다 적극적으로 개인정보 파기의 필요성을 인정하고 있다. 이는 일회성의 거래 이행이 주로 이루어는 금융 서비스와 다른 정보통신서비스의 특징을 반영한 것으로 판단된다. GDPR은 '보관기관 제한 원칙'에 의거하여, 개인정보 처리 목적에 필요한 기간이 지난 후의 개인정보 보관을 금지함에 따라, 프로세서는 컨트롤러의 선택에 따라 관련 개인정보를 반환 또는 파기하여야 하는 의무를 명시하고 있다.

국내 개인정보보호법, 신용정보법, 전자금융거래법 및 정보통신망법과 GDPR을 살펴보았을 때, 개인정보 처리자 및 서비스 제공사 등에게 요구되는 개인정보의 파기 시점 및 파기 사유는 상이하나 공통적으로 개인정보를 파기하여야 하는 의무를 갖는다. 하지만 블록체인의 기술적 특성에 따라 한번 원장에 기록된 정보에 대해서는 파기가 불가능함에 따라 정보통신, 전자금융 등의 서비스 제공업체의 파기 의무 이행이 불가능할 것으로 예측된다.

2.3 손해배상책임

최근, 국내를 비롯하여 전 세계적으로 가상화폐 거래소를 대상으로 발생한 해킹 사건은 이용자의 코인 도난에 따른 재산상의 손해를 발생하게 하였음에도 불구하고 이에 대한 명확한 배상 원칙이 부재하여 해당 사건에 대한 책임의 구분이 명확하게 이루어지고 있지 않다. 이에 따라, 사건의 책임 소재에 대하여 다양한 의견이 존재하는데, 거래소의 약관에 해킹에 따른 배상책임이 명시되어 있지 않음에 따라 해당 거래소의 책임이 없다는 것이 대표적이다. 이에 이용자의 관리 주의의무 소홀에 따른 이용자의 우선 책임으로 인정되어야 한다는 것이다. 이외에 해당 사항에 대한 약관의 수정을 통하여 이용자 보호를 우선시해야 한다는 상반된 의견이 함께 제기됨에 따라 가상화폐 거래소를 비롯하여 블록체인 환경에서의 명확한 배상 원칙 마련의 필요한 시점이다.

손해 배상과 관련하여 GDPR은 불법적인 개인정보 처리 결과로 인하여 손해를 입은 정보주체는 컨트롤러 또는 프로세서에게 해당 손해에 상응하는 배상 받을 수 있는 권리를 보장하고 있다. 또한 국내 개인정보호법 및 정보통신망법은 개인정보처리자 및 처리 기관 등에 의하여 수집된 개인정보가 변조, 유출됨에 따라 개인정보 주체가 손실을 입는 경우, 이에 대한 손해배상을 청구할 수 있음을 규정하였다. 신용정보회사 및 금융회사, 전자금융업자 등의 과실 혹은 고의로 인하여 개인정보 주체에게 손해가 발생하는 경우, 이에 대한 손해를 배상할 책임 의무가 있음이 신용정보법 제43조 및 전자금융거래법 제9조에 명시되어 있다. 이에 따라 블록체인에서 개인정보가 유출되어 재산상의 손실 등이 발생하는 경우, 개인정보 주체는 손해에 대한 배상을 요구할 수 있는 권리가 있다. 하지만 책임의 소재가 분명한 중앙집중적 시스템과는 달리 공유를 기본으로 하는 블록체인 시스템에서는 손해배상을 청구할 주체가 불명확하여 개인정보 주체의 권리를 행사하는데 한계가 있다. 즉, 블록체인 환경에서 책임 의무를 수반하는 주체 및 매개체가 존재하지 않는다. 따라서 블록체인에서는 블록체인을 처음 구축한 자와 블록체인의 노드를 구성하는 참여자 모두가 책임을 지는 무한책임의 문제가 발생할 수 있다. 특히, 프라이빗 블록체인에 비하여 익명성을 기반으로 다수의 참여자로 구성된 퍼블릭 블록체인의 환경에서는 책임 소재의 규명이 더욱 어려운 특징을 갖는다. 하지만 퍼블릭 블록체인의 거래소를 전자금융법이 인정하는 금융회사 및 전자금융업자로 적용되는 경우, 거래소의 관리부실, 주의 소홀에 따른 손해 배상의 책임 의무가 수반될 가능성이 있다. 전자금융법에 따라, 블록체인 기술을 통해 전자금융거래를 하고 거래 자료를 공유 및 보관하는 자 모두가 '전자금융업자'로 간주될 경우 모든 거래 참가자는 손해배상 책임을 부담해야 하는 것이 타당하나 실질적으로 불가능하다.

2.4 민감정보 처리 제한

국내 개인정보보호법 제23조 및 신용정보법 제16조와 더불어 GDPR은 공통적으로 유전자 정보, 정치적 견해, 종교 신념 등을 비롯하여 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 '민감정보'로 분류하였다. 이들은 공통적으로 모두 민감정보의 처리는 예외의 사항으로 명시된 경우를 제외하고는 원칙적으로 처리를 금지하고 있다. 특히, 신용정보법은 신용정보와 관계 없는 개인의 사생활에 관련된 사항에 대해서는 정보를 수집, 조사, 처리해서는 아니됨을 규정하였다. GDPR의 경우, 유사하게 민감정보의 처리를 원칙적으로 금지하나, 개인정보 주체의 명시적 동의가 있는 경우에 한하여서 처리를 인정하고 있다. 그러나 블록체인에 관한 규정이 국내・외 모두 아직 마련되지 않음에 따라 블록체인 환경에서의 민감정보에 대한 정의가 마련되지 않기 때문에 이에 대한 처리의 규정도 현재 존재하지 않는다. 향후, 블록체인 기술을 활용한 금융거래 및 블록체인 기반의 스마트 계약이 다양한 분야에서 적용될 것으로 예상됨에 따라 블록체인이 수집 및 처리하는 민감정보에 대한 정의 및 규정은 반드시 필요하다. 부동산 거래 계약서 작성 중, 거래당사자들의 인적 사항은 필수 기입 항목임에 따라 주민등록번호와 같은 고유식별정보 등의 처리 제한 가능성 및 이에 대한 수집 및 처리 방법의 고려가 요구된다. 또한 전자서명 등을 비롯하여 블록체인에 저장 및 관리되는 개인정보는 민감성을 수반함에 따라 이에 대한 별도의 규제 조항 마련 및 기존의 일반 개인정보 처리 규정의 적용 여부에 대한 합의가 필요할 것으로 판단된다. 예를 들어, 의료 분야에 적용된 블록체인은 환자의 진료 기록을 비롯한 다양한 환자의 신체 정보를 처리할 수밖에 없음에 따라 블록체인에 의하여 처리

되는 환자의 민감 정보를 어떠한 규정에 의거하여 처리할지에 대한 기준의 마련이 필요하다.

2.5 개인정보 수집, 이용, 제공 동의

블록체인은 노드 사이의 개인정보의 교환, 거래 등의 공유 활동을 전제로 함에 따라 개인정보의 이동에서 블록체인은 자유로울 수 없다. 따라서 이와 같은 블록체인 사이의 개인정보 거래 등의 이동이 안전하게 이루어지기 위해서는 국내 개인정보보호법 및 GDPR이 명시하는 '개인정보 동의'의 준수가 반드시 필요하다. 국내 개인정보호보법은 제15, 17, 18조를 통하여 개인정보의 수집, 이용 및 제 3자에게의 제공은 정보주체의 동의가 있는 경우에 한하여 가능함을 명시한다. 또한 동법 제23조, 제24조는 각각 민감정보 및 고유식별정보의 처리 역시 개인정보 주체의 동의가 있는 경우에 이루어질 수 있음을 규정한다. GDPR은 적법한 개인정보 처리 여부를 판단하는 기준으로 동의는 적법한 개인정보 처리(lawful processing) 근거이다. 따라서 GDPR은 개인정보 처리에 동의를 표시한 경우에 한하여 개인정보 처리가 가능하며 이에 대한 동의 방법과 동의 조건을 구체적으로 기술하였다. GDPR은 동의는 자유로운 의사에 의해 이루어져야 함을 강조한다. 또한 동의는 정보주체의 진술 또는 적극적 행동을 통한 모호하지 않은 의사표시이며 동의 획득 시에는 구체적이고 명확한 정보가 제공되어야 한다. 이는 정보주체가 동의했다는 사실과 동의한 내용이 분명하여야 하는 것으로 정보 주체가 단순히 동의 조건을 읽었음을 확인하는 것만으로는 동의의 의사표시가 될 수 없으며 동의를 한다는 명확한 신호(clear signal)가 있을 때, 동의한 것으로 성립된다. 이에 GDPR은 해당 서비스에 필요하지 않은 동의를 서비스 제공 조건으로 묶어 정보 주체에게 제공하는 것은 적절치 못한 것으로 판단한다. 즉, GDPR은 모든 동의가 사전 동의(opt-in consent)여야 함을 가정하며 침묵(silence), 부작위(inactivity), 디폴트 세팅(default setting) 또는 미리 체크 된 박스(pre-ticked boxes)는 유효한 동의로 인정하지 않는다.

현재 GDPR과 국내 개인정보보호법을 적용하였을 때, 블록체인 노드 사이의 개인정보 교환, 거래 등의 개인정보 이동이 적법성을 보장받고 유효한 처리 과정으로 볼 수 없다. 즉, 개인정보 처리에 대한 적법 및 유효한 이동으로 인정되기 위해서는 개인정보 처리에 대한 개인정보 주체의 동의 필요성 여부 및 범위의 설정이 선행되어야 한다. 하지만 블록체인의 분상원장에 이미 올라간 개인정보는 이에 다수의 참여자가 이미 접근할 수 있음에 따라 노드 사이의 각 이동 마다 개인정보 주체의 동의를 확보할 필요성이 없다. 또한 블록체인 환경에서 개인정보가 이동하는 모든 경우에 익명성을 가진 참여자 및 다수의 참여자를 대상으로 동의를 구하는 것은 불가능하다. 따라서 블록체인 노드 사이에 참여자가 추가되는 경우를 고려하여 '포괄적 동의' 여부 및 묵시적 동의의 가능성에 대한 고려가 필요하다. 현재, 개인정보보호법, 정보통신망법, 신용정보법에 따라, 선택 정보나 마케팅 등 불필요한 제 3자 제공 항목에 대해서 이용자 동의가 없어도 서비스 제공을 거부할 수 없도록 하는 것이 원칙이며 정보제공 대상 회사에 대하여 포괄적으로 동의 받는 것에 대하여 과태료나 과징금을 징수할 수 있다. 즉, 개인정보에 대한 '포괄적 동의'는 인정하지 않는 것으로 판단되나 블록체인의 경우, 포괄적 동의의 인정 혹은 개인정보 이동과 관련된 거래의 처리 횟수에 따른 동의 요구와 같은 특수한 개인정보 관련 동의 프로세스의 방식이 개발되어야 한다. 하지만 블록체인의 기술적 특수성과 참여자의 편의를 우선으로 하여 포괄적인 동의가 인정되는 경우, 기존의 '개인정보 동의' 관련 법규 조항이 확보하고자 하였던 개인정보의 취약성이 훼손되지 않는지에 대한 고려가 필요하다.

2.6 개인정보 국외 이전

블록체인의 확산은 개인정보를 비롯하여 각종 데이터의 이동을 용이하게 하여 국가간의 개인정보 이동을 활발하게 할 것으로 예상된다. 특히, 블록체인의 노드 사이에서 발생하는 데이터의 이동은 이전의 네트워크 기반보다 보안성, 신속성 등을 확보하였기 때문에 금융, 공공, 의료 분야를 막론하여 블록체인 기술이 적용될 것이다. 다양한 분야에서의 블록체인 적용과 활용은 이와 동시에 국가간의 구분 없이 개인정보가 이전되는 사례를 함께 증가시킬 것으로 판단된다. 즉, 국가를 뛰어넘는 개인정보 교환, 거래 등의 증가는 향후 이에 대한 국가간의 법적 분쟁을 발생시킬 수 있다. 기존 국내의 개인정보보호법 및 GDPR은 개인정보의 국가 이전에 대한 규정을 보유하고 있음에도 불구하고 블록체인 기술 적용에 따른 특화된 사항은 반영되지 않았기 때문에 이를 통하여 발생 가능한 분쟁을 해결할 수 없다.

국내 개인정보보호법 제17조 3항과 정보통신망법 제63조는 각각 개인정보를 국외로의 제공, 국외 보관 등의 처리 위탁을 수행하기 위해서는 개인정보 주체의 동의가 원칙적으로 필요하며 예외 사항을 제외하고서는 동의 없이 국외로 개인정보를 이전하는 계약의 체결을 금지하고 있다. 이와 같은 국내의 환경에서 블록체인의 노드를 통하여 발생하는 개인정보의 국외 이전은 무엇보다 적법한 절차에 따라 '개인정보 주체의 동의'가 확보된다면, 국외로 개인정보 제공이 비교적 용이하게 이루어질 수 있다. 단, 블록체인을 통한 개인정보의 국외 이전은 개인정보를 보유한 기업이 이를 정보 주체에게 제공 받아 대리인의 입장으로 처리하는 기존의 정보통신서비스 등과는 다르기 때문에 준거법의 상충 소지가 있다. 현재 국제사법은 당사자가 준거법을 선택 하거나 그러지 아니한 경우에는 가장 밀접한 관련이 있는 국가의 법에 따를 것을 규정하고 있다. 하지만 이에 따라 블록체인에 존재하는 다수의 당사자가 선택하는 단일한 준거법을 설정하거나 가장 관련이 있는 국가의 법을 따르도록 선택하는 것은 수많은 참여자가 존재하는 블록체인 환경에서 현실적으로 불가능하다. 또한 블록체인은 다수의 참여자가 존재하는 동시에 개인정보에 대한 주체가 각각 존재하기 때문에 다수로부터 개인정보를 제공 받은 기업 및 국가와 같은 단일 주체의 대리인이 수행하는 기존의 국내 법규가 규정한 '개인정보 국외 이전'의 문제와는 다른 양상을 갖는다.

GDPR은 개인정보의 국외이전에 비교적 엄격하다. 이는 GDPR은 개인정보 국외 이전을 원칙적으로 금지하기 때문이다. 그러나 1) 개인정보 이전이 예상되는 제 3국 및 국제 조직의 적합한 보호 수준을 보장하는 적정성 평가(Adequacy Decision)를 획득한 경우, 2) 적정성 평가를 획득하지 못한 경우 정보관리자가 적절한 안전 장치(Appropriate safeguards)인 구속력 있는 기업 규칙(Binding Corporate Rules), 표준 개인정보보호 조항 요건(Standard Contractual Clauses)을 갖추거나 관련 표준 인증 획득 여부를 제시하는 경우에 따라 제한적으로 개인정보 국외 이전을 허용하고 있다. 이러한 GDPR의 조항에 의거하여 블록체인에서 발생하는 개인정보의 국가간 이전은 앞서 제시된 요건의 확보를 통한 경우에 허용된다. 즉, 개인정보 이전이 적정성 평가, 표준 인증 등을 확보한 국가를 대상만으로 하는 방식으로 이루어져야 하나, 블록체인의 노드 위에서 거래되는 데이터의 이동을 국가의 기준으로 정확히 통제 및 감시할 수 없는 한계가 존재한다.

2.7 영향평가

국내 전자금융거래법 제21조의3에 따르면 금융회사 및 전자금융업자는 전자금융거래의 안전

성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대하여 분석·평가하여야 한다. 분석 및 평가는 정보기술부문의 조직, 시설 및 내부통제에 관한 사항, 정보기술부문의 전자적 장치 및 접근매체에 관한 사항, 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항 등에 대해서 이루어져야 한다. 따라서 블록체인에 참여하고 있는 각 노드가 모두 전자금융기반시설로 간주되는 경우, 이에 대하여 취약성 분석 및 평가를 수행하여야 하나 이는 블록체인의 경우 물리적 공간이 한 곳에 집중되어 있지 않아 평가를 수행하는 것이 어렵다. 또한 일정 규모 이상의 개인정보파일을 처리하는 국내 공공기관의 경우, 개인정보보호법 제31조에 따라 영향평가 의무 수행이 요구된다. 이에 따라 국내 공공기관에서 블록체인 기술을 적용한다면, 해당 기관은 블록체인을 대상으로 영향평가를 수행하여야 하는 의무를 갖는다. 그러나 블록체인을 구성하는 모든 노드에 존재하는 위험요인 등을 도출하고자 모든 노드의 취약성 및 위험요인을 파악하는 것은 어렵다. 따라서 국내법에 의거하였을 때, 블록체인의 환경에서 발생하는 모든 전자금융거래를 비롯한 공공기관의 업무 수행은 위반의 소지가 있다.

GDPR은 기업이 개인정보 영향평가를 통해 개인정보 처리 관련 문제점을 조기에 발견 및 해결할 것을 권장하나, 개인정보 처리로 인하여 개인의 권리와 자유에 고위험의 초래 가능성이 있는 경우, 민감정보 등을 비롯한 유죄 판결 및 형사범죄에 대한 대규모의 개인정보를 처리 사항에 대해서는 영향평가의 의무 수행을 요구한다. 즉, 국내의 상황과 비교하였을 때 비교적 영향평가의 의무 적용이 엄격하지 않다. 단, 기업이 신기술을 사용함에 따라 개인정보의 처리 과정에서 개인의 권리와 자유에 위험을 야기할 것으로 판단되는 경우 영향평가를 수행하여야 하기 때문에 블록체인을 도입한 기업 상당수는 영향평가 수행의 적용 대상으로 간주될 수 있다. 이에 국내외에서 현재 수행되는 영향평가의 방식은 블록체인의 환경에서 현실적으로 적용이 어렵기 때문에, 블록체인에 특화된 영향평가의 방식이 마련되어야 한다.

2.8 정보보호책임자 지정

국내 전자금융거래법 제21조 및 동법 시행령 제11조의 3, 정보통신망법 제45조의 3항 등에 의거하여 개인정보관리책임자(CISO, Chief Information Security Officer)를 의무적으로 지정하도록 한다. 또한 개인정보보호법 제31조, 정보통신망법 제27조에서는 정보통신서비스 제공자 등의 국내 일부 기업에 대하여 최고보안책임자(Chief Privacy Officer, CPO)의 의무 임명을 명시하였다. GDPR은 1) 공공기관에 해당되는 경우, 2) 기업 및 단체의 핵심활동이 정보주체의 활동을 대규모로 모니터링 하는 경우, 3) 기업 및 단체의 핵심활동이 민감 정보나 범죄정보의 대규모 처리에 관여된 경우에 대하여 DPO의 임명을 필수적으로 규정하고 있다. 특히, 의료 기관에서 블록체인 기술을 적용하여 환자의 유전자 정보, 생체 정보 및 건강 정보 등의 민감정보를 다루는 경우, DPO임명은 반드시 이루어져야 한다. 하지만 퍼블릭 블록체인과 같이 운영주체가 불분명한 블록체인은 정보보호책임자 등의 해당 블록체인이 수반하는 정보보호 관련을 관리 및 책임질 담당관의 임명이 어려워 GDPR을 비롯한 국내 관련 법규의 준수가 어려운 한계점을 갖는다.

앞서 제시된 개인정보보호 관점에서 상충 가능한 블록체인의 법적 쟁점에 대한 8가지 이슈는 <Table 1>과 같이 정리된다. 다음의 표를 통하여 8가지 쟁점에 대한 국내 개인정보보호법을 비롯한 관련 법률 및 GDPR이 명시한 공통적인 주요 내용을 제시하였으며, 이슈에 따른 각각의 조항을 확인할 수 있다.

〈Table 1〉 Legal Issues in Blockchain

Legal Issue \ Article	GDPR	Personal Information Protection Act	Electronic Financial Transaction Act	Information and Communication Network Act	Use and Protection of Credit Information Act
Amend & Delete of Personal Information	The subjects of personal information can require to amend, replace or delete the personal information to personal information processors.				
	#16, #17	#4, #36	-	-	-
Destruction of Personal Information	The personal information processors should delete or destruct of personal information collected and stored according to certain conditions.				
	#5	#21	#22	#20	#29
Compensation & Liability	The service provider or personal information processor should compensate to damages incurred for to the subjects of personal information				
	#82	#39	#43	#32	#9
Prohibition on Processing Special Categories of Personal Data	Processing of sensitive information is generally prohibited, but can only be done with explicit consents of the subject.				
	#9	#23	-	-	#16
Consents of Collecting & Processing	It is possible to collect, use, and provide personal information only when the consent of the information subject is obtained.				
	#6, #7	#4, #15, #17, #18, #23, #24	-	-	-
Transfers of Personal Data to Third Countries or International Organizations	When the personal information processors transfer personal information to third countries, they should notify to the subjects of personal information and consent is required.				
	#44, #45	#17	-	#63	-
Data Protection Impact Assessment	Data protection impact assessment should be performed before when personal information processing is predicted to have a risk to the personal information subjects.				
	#35	#31	#21	-	-
Designation of the Data Protection Officer	Officer or manager who has responsible for protecting and controlling personal information should be designated in the organization.				
	#37	#31	#21	#27, #45	-

3. 블록체인 환경에서의 국내 개인정보 보호법제 개선 방안

본 연구에서는 블록체인 환경에서 발생 가능한 GDPR 및 국내 관련 법률의 상충 사항을 미리 살펴봄에 따라 향후, 블록체인 확산에 따른 국내 관련 법안의 개정 및 추가적인 법적 장치의 마련이 필요함을 시사하였다. 이러한 본 연구의 결과는 현재 마련되지 않은 블록체인 관련 법률의 기반 형성에 다음과 같이 기여한다.

첫째, 클라우드 보안 관련 법규 검토의 필요성을 제기한다. 블록체인의 기술을 적용한 주요 암호화폐 거래소의 시스템은 클라우드 기반에서 운영됨에 따라 이에 대한 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률'에 대한 전반적인 검토가 필요하다. 현재, 클라우드법 내에 블록체인 관련 분쟁을 해결하기 위한 법률이 없기 때문에 동법 내 블록체인 관련 조항의 추가 및 블록체인의 적용 가능성에 대한 판단이 이루어져야 한다.

둘째, 가상화폐 거래소의 망분리 의무화 규정

적용이 고려되어야 한다. 2012년 국내에서 발생한 대규모의 개인정보 유출 사건으로 인하여 개인정보 처리시스템에 접근하는 컴퓨터 등의 외부 인터넷망 차단, 즉 망분리 관련 사항을 정보통신망법 시행령이 신설되었다. 이외에 금융권 망분리 가이드라인, 개인정보보호법 시행령, 전자금융감독 규정을 발표하여 대부분의 금융권을 대상으로 전산센터를 시작으로 영업점까지 2016년 내, 모두 구축을 완료할 것을 권고 받았으나 현재 대다수의 기업에서 망분리 작업이 진행 중이다. 망분리 의무에 해당되는 금융기업은 전년도말 직전 3개월간 일일평균 100만 명 이상의 이용자 개인정보를 보유하거나 전년도 정보통신분야 매출액이 100억 원 이상인 정보통신서비스 제공자이다. 이에 의무적용에 해당되는 금융기업은 개인정보 처리시스템에 접속하는 컴퓨터 등을 외부 인터넷망과 차단해야하는 의무를 갖는다. 다음의 <Table 2>는 관련 시행령 및 행정규칙의 주요 조항과 내용을 제시한다.

금융기업과 더불어 가상화폐 거래소는 이용자의 금융정보를 주로 다룬다. 이와 동시에 기업의 취약한 보안 수준은 해킹 등의 표적이 되기 쉬우며 대규모의 금전 피해를 발생시킬 수 있다. 2017년 1월, 일본의 암호화폐 거래소에서 발생한 해킹 사고는 5,700억 원 상당의 피해액을 발생시켰다. 이와 같은 점을 종합하였을 때, 가상화폐 거래소를 비롯하여 블록체인 환경에서 망분리 의무 적용에 대한 고려가 필요하다.

망분리 작업은 보안수준을 향상시키는 단계에서 다른 기술적 장치의 설치보다 신속하게 이루어질 수 있는 장점이 있다[Cho et al., 2015]. 이에 가상화폐 거래소 역시 금융기업과 같이 망분리의 의무 작업을 법적으로 규제할 타당성이 있다. 실제로 망분리는 서버 보안과 더불어 금융기업의 보안수준을 평가하는데 있어 '준비단계'로 평가된다. 이와 달리, 이용자가 화폐를 보관하는 월렛을 콜드월렛, 핫월렛으로 각각 분리하여 보관하는 '월렛 네트워크 분리' 및 2개 이상의 서명(key)을 승인해야 거래가 이루어지도록 하는 '멀티시그니처'보다 현재의 상용된 기술로 쉽고 빠르게 적용 가능한 방법이 망분리이다. 이에 따라 가상화폐 거래소의 기술적 보호조치 의무를 판단하는 기준으로 망분리가 선행될 필요가 있다. 즉, 특정 보호조치를 적용하는데 지나치게 비용이 많이 들거나, 제한된 영역에만 적용 가능하거나 조속한 시일 내에 도입이 어려운 신기술이 아님에 따라 망분리를 가상화폐 거래소의 법적 의무 사항으로 적용되어야 한다.

망분리 구축 방식은 물리적 망분리와 논리적 망분리로 구분된다[Jee et al., 2012]. 개인의 업무와 사무용 PC를 구분하여 2대의 PC를 사용하는 물리적 망분리는 비효율성이 떨어지는 단점이 있

〈Table 2〉 Administrative Rules of Partitioned-Network for Information Security in Korea

Enforcement Decree of Information and Communications Network Act, *Article 15, Clause 2, paragraph 3* (Protection Measures of Personal Information)	Enforcement Decree of the Personal Information Protection Act, *Article 30, Clause 1, paragraph 2* (Secure Plan of Security in Personal Information)	Regulations for Electronic Financial Supervisory Service, *Article 15, Clause 1, paragraph 3* (Measures to Prevent Hacking)
Blocking of external partitioned-network for personal information processors' computers connected to personal information processing system	Restrict the rights of controlling and accessing to personal information	The internal communication network, including the wireless communication network should be separated from the external communication network

으나, 논리적 망분리의 일종인 CBC(클라이언트 기반 망분리)는 PC 부분 가상화를 통해 인터넷 영역과 업무 영역이 분리되는 동시에 네트워크 게이트웨이 설치만으로 보안 수준을 높일 수 있어 적은 비용으로 망분리 수행이 가능하다. 물리적 망분리의 경우, 서버팜을 구축하여 인터넷 망은 서버를 통해 접속하며 업무망은 PC로 분리하는 방식으로 보안수준은 높으나 필요로 하는 추가 장비가 많아 구축 비용이 큰 단점이 있다. 따라서 국내 가상화폐 거래소의 경우에도 논리적 망분리 형태의 적용을 고려해볼 수 있다. 국내 공공기업의 경우, 개인정보보호법 제33조에 따라, 5만 명 이상의 민감정보 혹은 고유식별정보를 처리하는 공공기관은 개인정보영향평가를 의무적으로 수행하도록 하고 있다. 이러한 법적 조항은 국내 공공기관이 수집 처리하는 개인정보의 안정성을 향상시키는 것에 주된 목적이 있다. 이와 같이 국내의 가상화폐 거래소도 최소한의 기술적 보호조치 의무를 판단하기 위한 관련 법 및 시행령이 마련되어야 한다. 이러한 기술적 보호조치가 마련되지 않는 경우, 보안성 확보에 실패한 가상화폐 거래소 등이 운영되어 국가적 차원의 대규모 손실을 초래할 수 있다.

셋째, 전자금융거래법 및 정보통신망법에 의한 블록체인 규제의 적용 가능성을 검토하여야 한다. 블록체인의 공식화된 정의는 없으나, 처음 제시한 사토시 나카모토는 블록체인을 'P2P 네트워크를 이용하여 이중 지불을 막는 기술'로 논문에 제시하였다. 또한 Swan[2015]은 '블록체인'은 인터넷의 또 다른 유형으로 공유된 네트워크를 기반으로 돈(화폐)을 비롯하여 개인의 집, 차 등의 유형 및 정보, 지식과 같은 무형의 자산을 모두 다룰 수 있는 새로운 패러다임으로 명명하였다. 이에 기반하여 블록체인의 정의를 종합적으로 살펴보았을 때, 블록체인은 '네트워크 시스템을 기반으로 온라인 상에서 거래 내용이 담긴 블록이 형성되도록 하는 기술'이다. 따라서, 국내 전자금융거래 및 정보통신서비스로의 인정 가능성을 확인할 수 있다.

전자금융거래법 제2조에 따르면, 전자금융거래는 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다. 또한 전자서명은 블록체인의 보안 수단이 되는 동시에 정보 처리시스템에 의한 전자문서가 송・수신되고 이를 통해 재화나 용역이 거래되기 때문에 전자문서 및 전자거래기본법의 적용 가능성도 존재한다. 정보통신망법은 정보통신서비스를 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것으로 정의하며 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 '전자문서'가 전자적 전송매체를 통하여 이동이 가능함을 규정한다. 위의 각 법이 정의한 전자금융거래와 정보통신서비스가 컴퓨터 등의 전자적 장치를 기반으로 한다는 점(종사자와의 대면이 요구되지 않음), 해당 전자적 장치가 자동화된 방식으로 상품 및 서비스(전자금융거래) 혹은 전자문서(정보통신서비스)의 송수신이 이루어진다는 점에서 블록체인도 해당 거래 및 서비스로의 적용이 가능하다고 판단된다. 이에 따라, 블록체인을 통하여 발생하는 거래의 결과 및 거래 프로세스가 넓은 개념의 전자금융거래 및 정보통신서비스로의 인정이 가능하다면, 이에 따른 법적 지위 및 권한이 발생하여 앞서 제시된 다양한 법적 쟁점을 예방 및 해결할 수 있을 것이다. 전자금융거래법에 따라, 블록체인이 구속받는다면 블록체인의 비가역성(irreversibility)으로 인하여 과거 수집된 고객의 전자금융거래를 파기하는 것이 기술적으로 어려움에 따라, 전자금융거래법의 동 규정을 폐기하는 방식의 고려가 필요하다. 블록체

인의 분산된 노드는 정보주체인 동시에 정보 처리자와 위탁자 역할을 동시에 이행하게 됨에 따라, 블록체인의 환경에서 정보주체, 처리자 및 위탁자 역할의 정립이 필요하다.

References

[1] Cho, B. J., Yun, J. H., and Lee, K. H., "Study of effectiveness for the network separation policy of financial companies", *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 25, No. 1, 2015, pp. 181-195.

[2] Computer World, IBM Waston, *FDA to explore blockchain for secure patient data exchange*, 2017. 01. 11.

[3] Jee, J., Lee, S., Lee, S., Bae, B., and Shin, Y., "A Logical Network Partition Scheme for Cyber Hacking and Terror Attacks", *Journal of KIISE*, Vol. 39, No. 1, 2012, pp. 95-101.

[4] Kiviat, T. I., "Beyond Bitcoin : Issues in Regulating Blockchain Tranactions", *Duke LJ*, 2015, Vol. 65, p. 569.

[5] Lee, J., Park, S., and Hong, S., "A Suggestion on Node Identification and Authentication method on Blockchain Network", *The Conference of Korean Institute of Communications and Information Sciences*, 2018, pp. 476-477.

[6] Lee, S., Kim, H., and Hong, S., "A Study on Blockchain Data Design Considering Personal Information Protection", *The Conference of Korean Institute of Communications and Information Sciences*, 2018, pp. 478-479.

[7] Maull, R., Godsiff, P., Mulligan, C., Brown, A., and Kewell, B., "Distributed Ledger Technology : Applications and Implications", *Strategic Change*, Vol. 26, No. 5, 2017, pp. 481-489.

[8] Morabito, V., *Business Innovation through Blockchain*, Cham : Springer International Publishing, 2017.

[9] Oh, S. and Lee, C., " Block Chain Application Technology to Improve Reliability of Real Estate Market", *The Journal of Society for e-Business Studies*, Vol. 22, No. 1, 2017, pp. 51-64.

[10] Park, M., Chai, S., and Lee, M., "A Study on the Establishment of Data Protection Officer(DPO) Position under GDPR Enactment", *The Journal of Korean Institute of Communications and Information Sciences (J-KICS)*, Vol. 43, No. 2, 2018, pp. 427-438.

[11] Seo, J., Lee, D., and Choi, G., "Policy Issues and Application Cases of Blockchain in the Financial Services Industry", *KIF Financial Report*, Vol. 25, No. 39, 2016, pp. 1-9.

[12] Swan, M., *Blockchain : Blueprint for a new economy*, O'Reilly Media, Inc, 2015.

[13] Yook, T., "Change of Financial Systems by Virtual Currency or Cryptocurrency and its Legal Implications", *Kangwon Law Review*, Vol. 53, 2018, pp. 225-270.

저자소개

Minjung Park

Minjung Park is PhD candidate of Ewha School of Business, Ewha Womans University. She graduated from Ewha Womans University with M.S in Data Analytics and received BS in Sungshin Women's University. Her research interest is behavioral information security, information security management, and cybersecurity.

Myoungjun Lee

Myoungjun Lee is a lawyer in Korea. He graduated from Seoul National University with a law degree. He passed the judicial examination and completed Judicial Research and Training Institute. Currently, he specializes in personal information protection, block chains, taxation, and real estate.

Sangmi Chai

Sangmi Chai is an Associate Professor in Ewha School of Business, Ewha Womans University. She received her PhD in MIS from School of Management, State University of New York at Buffalo. She was an Assistant Professor in College of Business, Information and Social Sciences, Slippery Rock University, PA, USA. She graduated from MBA in Seoul National University and received BS in the Ewha Womans University. Her research interests include information privacy and security, trust and knowledge management, and IT investment.