논문 20-45-08-04 The Journal of Korean Institute of Communications and Information Sciences '20-08 Vol.45 No.08
https://doi.org/10.7840/kics.2020.45.8.1342

블록체인 기반 개인정보 활용 동의에 대한 상호 신뢰 시스템 연구 및 구현

이 정 현◆, 김 지 원*, 김 철 수*, 양 진 홍°

Research and Implementation of Mutual Trust System for Consent to Use Personal Information Based on Blockchain

Jeong-Hyeon Lee◆, Ji-Won Kim*, Chul-Soo Kim*, Jinhong Yang°

요 약

현재의 온라인 서비스 사용자들은 서비스를 이용하기 위해 해당 서비스의 약관에 동의함으로써 자신의 개인정보를 서비스사업자에게 제공하고 있다. 사용자의 약관 동의에 관련한 내용은 서비스 사업자가 보유 및 관리하고 있으며, 변경 있을 시 이메일 또는 문자서비스 등을 통해 사용자에게 알려주고 있다. 하지만 개인정보 제공자인 서비스 사용자의 입장에서는 과거에 어떠한 내용에 동의를 했었는지, 그리고 자신의 최초 약관 동의 시점 대비 어떠한 내용이 변경되었는지를 손쉽게 확인하기 어려운 실정이다. 이러한 문제에 대해 EU의 GDPR 규정에서는 개인정보 활용과 관련된 '동의의 조건'을 명시하고 있으며, 정보주체가 정보처리방식에 동의하였음을 정보처리자가 입증할 수 있어야 한다는 것을 명시하여 개인정보 수집 및 활용 방안을 강화하고 있다. 따라서 현재 온라인 서비스 사용자의 개인정보보호를 위해 사업자가 취득한 사용자의 개인정보 활용'동의'에 대한 보다 더 강화된 관리 모델이 필요하다. 본 연구에서는 블록체인을 활용하여 온라인 서비스를 활용하는 사용자가 서비스 약관 동의 시 개인정보에 대한 이용 권한을 명시적으로 기록, 관리, 확인이 가능하도록 하는 것을 목적으로 하는 블록체인 기반 가입 약관 증명 시스템을 설계 및 구현하였다. 이를 통해 온라인 서비스사업자와 사용자가 상호 신뢰 할 수 있는 서비스 이용 동의 정보 관리를 가능하게 하였으며, 기존의 개인정보 동의 확인의 문제점을 평가하고, 제안한 시스템이 기존의 문제점을 해소할 수 있는지에 대하여 평가하였다.

Key Words : GDPR, User Contents, Consent Providing Verification, Blockchain, Mutual trust

ABSTRACT

Current online service users provide their personal information to service providers by agreeing to the terms of the service in order to use the service. The contents of the terms and conditions agreement are maintained and managed by the service provider, but it is difficult for the user, who is the personal information provider, to agree on what contents they have agreed to and what contents have been changed compared to the time of their initial agreement. In response to these issues, the EU's GDPR regulations strengthen the methods for collecting and using personal information by stating that the data controller must be able to prove that the data subject has

※ 이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2018-0-00261, IoT 환경에서 일반개인정보보호규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)
◆ First Author : Inje University Department of Computer Engineering, jeonghyeon8367@oasis.inje.ac.kr, 학생(석사), 학생회원
° Corresponding Author : Inje University Department of Healthcare IT, jinhong@inje.ac.kr, 정회원
* Inje University Department of Computer Engineering, jeon4107@oasis.inje.ac.kr, 학생회원; charles@inje.ac.kr, 종신회원
논문번호 : 202005-113-C-RU.R1, Received May 27, 2020; Revised June 16, 2020; Accepted June 23, 2020

agreed to the processing method. Therefore, in order to protect the personal information of users of online services, it is necessary to strengthen the management model for 'agreement' of the use of personal information users acquired by the operator. This study designs and implements a blockchain-based subscription agreement verification system that allows users who use online services to explicitly manage access to personal information when agreeing to the terms of service, and that mutual trust between online service providers and users is possible.

Ⅰ. 서 론

온라인 서비스 제공업체 중 사용자에게 서비스를 무상으로 제공하는 사업자들의 경우, 서비스의 제공 대가로 사용자의 정보에 기반 한 광고를 통해 주요 수익을 창출하고 있다. 특히 맞춤형 실시간 광고 비딩 서비스가 활성화됨에 따라, 개인정보에 기반 한 맞춤형 광고는 온라인 서비스 제공업체의 연간 매출을 20%이상 성장시키고 있으며, 해당 분야의 대표 격인 Google과 Facebook의 경우 서비스 수익의 90%이상을 맞춤형 광고를 통해 올리고 있다.[1] 개인정보에 기반 한 맞춤형 광고를 위해 온라인 서비스 제공업체는 서비스를 제공하는 과정에서 사용자에게 가입 절차를 요구하고 있으며 그 과정에서 사용자 약관 동의를 통해 개인정보를 취득하는 방식을 취하고 있다.[2,3]

하지만 서비스 이용을 위한 사용자의 개인정보 활용 동의와 관련해 가장 중요한 단계인 약관 동의 과정의 경우, 사용자는 1) 약관의 내용이 많고, 2) 일괄적 동의 없이 서비스 이용이 어려움 점을 들어 동의서를 읽지 않고 있다고 조사되었다.[4] 즉 온라인 서비스 사용자들은 정보제공 및 활용 동의 항목을 제대로 인지하지 못한 채 정보 제공에 동의함으로써 개인정보가 어디에 활용되고 있는지 파악하지 못하고 있다. 또한 서비스 이용을 위해서는 반드시 개인정보 활용 동의를 진행해야만 서비스 제공 방식은 개인정보 활용에 있어 정보주체의 자율적인 선택이 보장되는가에 대한 의문 및 개인정보 관리 이슈들을 발생시키고 있다.

개인정보보호법에서는 온라인 서비스의 정보제공 및 활용 동의 내역이 변경, 추가, 삭제가 이루어지는 경우 사용자에게 문자 또는 이메일 등을 통해 반드시 통지하도록 하고 있다.[5] 하지만 이러한 방법에도 불구하고 그림 1과 같이 온라인 서비스 사용자는 약관 동의 정보에 대해 1) 온라인 서비스별 어떠한 개인정보 제공 및 활용에 동의했는지 기억하기가 어려운 점과 2) 온라인 서비스사업자가 동의 내역을 임의로 변경, 추가, 삭제한 경우 이를 개인이 인지하고 판단하기가 어려운 문제를 가진다.

유럽연합(EU)에서는 자국민의 온라인 개인 데이터를 보호하고, 개인정보에 대한 권리를 정보주체가 가질 수 있도록 GDPR(General Data Protection Regulations)을 2018년 5월에 발효하였다. GDPR은 기업의 무분별한 데이터 수집과 활용을 경계하고 정보의 주체가 동의한 내용과 관련해 제시된 조건을 수락할 것인지, 불이익 없이 거절할 것인가에 대해 정확히 인지할 수 있도록 조건을 강화하고 있으며, 정보주체가 정보처리방식에 동의하였음을 정보처리자가 입증할 수 있어야 한다는 조건을 명시하고 있다.[6]

따라서 본 논문에서는 GDPR에서 규정한 '인지된 사용자 동의'와 '정보처리방식 동의 내용 증명'을 만족 시 킬 수 있도록 상호 신뢰에 기반 한 블록체인 기반 약관 동의 증명 시스템을 제안 및 구현하였다. 본 연구를 통해서 1) 사용자가 서비스 이용의 대가로 온

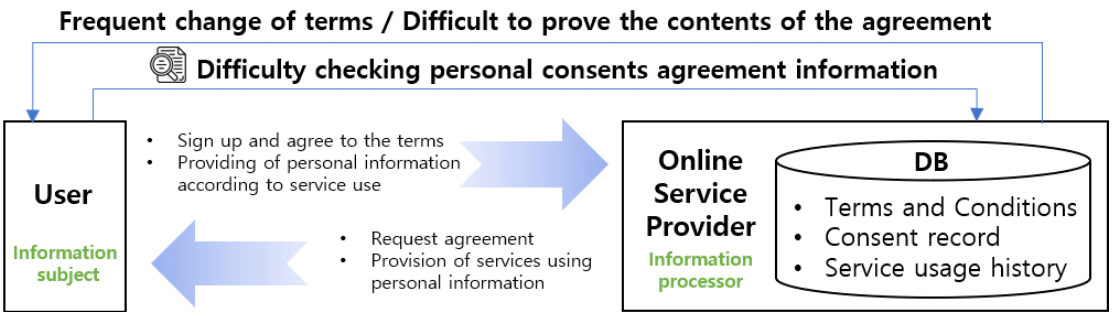


그림 1. 현재 온라인 서비스제공업체의 회원가입 절차 및 사용자 개인정보 동의 확인 방법
Fig. 1. The current membership procedures of online service providers and how to verify user personal information consent

라인 서비스 사업자에게 제공한 개인정보를 안전하게 저장 및 관리하는 시스템 모델을 제안하고, 2) 사용자가 온라인 서비스의 회원가입 시 자신이 선택했던 서비스 제공 방식 및 약관 동의 내용을 확인할 수 있도록 하는 시스템 구조 및 3) 정보주체가 개인정보처리 방식에 동의했다는 것을 입증할 수 있는 시스템 모델을 제시하고 온라인 서비스 사용자와 사업자 간의 신뢰성 있는 관계를 위한 시스템을 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서는 약관 동의 획득 및 관리 측면에서의 개인정보보호 이슈 및 블록체인 활용 연구에 대하여 분석하고 이에 대한 문제점 및 한계점을 살핀다. 3장에서는 제안하는 블록체인 기반 약관 동의 증명 시스템 설계 및 구조에 대하여 서술한다. 4장에서는 블록체인 기반의 개인정보 동의 관리 시스템의 구현 환경과 결과를 기술한다. 5장에서는 기존의 서비스 사업자 정보 저장 방식과 구현된 블록체인 시스템을 비교 분석하였다. 6장에서는 본 논문의 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 약관 동의 획득 및 관리 측면에서의 개인정보보호 이슈 및 블록체인 활용 연구

2.1 약관 동의 획득 방식에 대한 연구

현재 정보주체자들은 온라인 서비스 사용을 위해 회원가입을 전제로 개인정보 수집 및 활용에 관한 동의를 제공하고 있다. 서비스 사업자의 동의 정보 취득 방식은 옵트인, 옵트아웃 두 가지로 볼 수 있으며, 각각의 특징이 존재한다.

먼저 옵트인(Opt-in) 방식은 일반적으로 웹사이트 회원가입 과정에서 개인정보 제공 및 활용에 관한 동의를 제공하는 방식으로 이후 서비스 상에서 제공하게 될 정보들에 대해 일괄 동의를 제공하는 형태이다.

옵트아웃(Opt-out) 방식은 사용자의 동의를 받지 않고 개인정보를 처리하되, 사용자가 거부 의사를 밝힌 경우는 개인정보 처리를 중단하는 방식이다.

하지만 대부분의 사용자들은 옵트인(Opt-in)/ 옵트아웃(Opt-out) 방식과 별개의 문제로 개인정보 수집·이용 동의서, 약관 동의 등 동의체크를 읽지 않거나, 가볍게 보고 넘기는 것으로 나타났다.[7]

이러한 문제점을 해결하고자 약관 동의 획득 방식의 법 규정들은 강화되고 있으나, 사용자 입장에서의 약관 동의 정보에 대한 확인 및 관리 부분은 실질적인 개선이 이루어지지 않고 있다.[8]

2.2 법령에서의 약관 동의 관련 규제

2.2.1 EU GDPR

2016년 5월 EU는 일반개인정보보호법 GDPR을 제정하였으며 2018년 5월 시행하였다. GDPR은 데이터 자체가 자산이 되고, 축적된 데이터가 새로운 자산을 창출함에 따라 데이터 유출, 개인정보 침해 등 문제의 심각성이 증가하면서 EU시민의 개인데이터를 처리하는 전 세계 모든 기업들을 대상으로부터 EU의 시민을 보호하기 위해 제정되었다. 이 규정으로 인해 EU시민을 대상으로 서비스하는 기업들은 정보주체로부터 동의의 획득 및 동의했음을 입증하는 것이 필수가 되었다. 이러한 GDPR 규정은 데이터 및 기업을 적극적으로 관리하게 함으로써 개인정보를 보호하는 목적을 띄고 있다.[9]

2.2.2 EU의 GDPR의'동의조항'

GDPR은 전문 총 173개항, 본문 11장 99개 조항으로 구성되어 있으며, 본문 99개 조항 중 19개의 항이 정보주체의 동의에 관해 다루고 있다.[3,10] 그 중 핵심적인 부분으로 '정보주체는 본인이 유효한 동의 획득에 대한 모든 요건을 충족시키는지 여부를 평가할 의무'를 가지고 있는 점이다. 즉 GDPR을 준수하여 동의를 얻고자 하는 온라인 서비스 사업자의 경우 정보주체가 본인에 관한 개인정보의 처리 여부에 대한 통제권을 가질 수 있도록 도구를 제공하여야 한다. 이뿐 아니라 GDPR에서는 개인정보처리자가 정보주체를 개인정보처리에 대해 동의하고 인지시켰음을 입증해야 한다는 조항을 포함하고 있다. 즉 온라인 서비스 사업자는 서비스 이용 동의 획득 시 사용자에게 충분한 약관에 대한 이해를 제공할 수 있어야 한다. '동의' 관련 조항 중 '인지된 동의' 관련 주요 항은 표 1과 같다.[11]

이처럼 EU GDPR에서는 정보주체의 입장에서 '인지된 동의' 획득 및 '동의의 입증'을 위한 방안을 정보처리자에게 제시하도록 명시되어 있다.

따라서 온라인 서비스 사업자는 합법적이고 합리적인 개인정보 수집 및 활용을 위해 GDPR 규정에서의 '사용자 동의' 획득 및 관리와 관련된 사항에 대해 보다 주의를 기울여야 할 뿐 아니라 정보주체에게 사용자 동의 내용을 인지시키고, 동의 받았음을 입증할 수 있는 시스템적인 방안 모색이 필요하다.

표 1. EU GDPR '동의'관련 조항 발췌 내용
Table 1. EU GDPR 'Consent' Excerpts

article	Main Content
32	· The information subject should be able to freely agree to the processing of personal information. · Checking the web site's consent to the processing of personal information, and the technical setting of the service include the actions of the information subject and other statements that mean the user's choice or permission to process personal information. · Personal information processing agreements or omissions, such as silence and automatic advance checks, do not constitute consent. · When requesting the consent of the data subject, if provided, it should be concise and clear.
33	· In the case of using information for research purposes, only the part of the research must be approved by the data subject as long as the data subject agrees and allows it for the intended purpose.
42	· If the consent is based on the fact that the personal information was processed by the data subject, the data controller must be able to prove that the data subject has obtained consent. · At a minimum, the data subject should be aware of the identity of the data controller and the purpose of processing the personal data.
43	· With regard to the processing of personal information, free consent cannot be given unless the subject of the information has obtained separate consent.

2.3 개인정보보호와 관점에서의 블록체인 활용 연구

2.3.1 블록체인에서 개인정보 이슈

개인정보보호를 위한 방안으로 블록체인 기술이 떠오르면서 개인정보보호 관점의 블록체인 연구들이 활발히 이루어지고 있다. 국외 동향으로는 GDPR 시행 국가인 EU에서도 개인정보보호 관점의 블록체인관련 이슈를 다루고 있으며, 국내는 데이터3법이 개정됨에 따라 블록체인 기술 활용이 다시 이슈로 떠오르고 있다.[12-14]

블록체인 상에서 개인정보를 다루는 것은 일반적으로 대다수의 개인정보보호법과 대비된다. 대표적인 예로 유럽 거주자의 개인정보를 블록체인에 저장 시(데이터의 국외 이전에 대한 별도의 동의 없이 GDPR 규정의 '데이터 국외 이전방지 준수' 조항에 위배 된다.[15] 이 외에도 블록체인의 개념과 GDPR 조항이 서로 상충하기 때문에 이에 따른 연구들이 이루어지고 있다.[16-18]

다음 표 2는 블록체인의 특징과 GDPR의 개인정보보호 내용과 상충하는 조항들을 나타낸 것이다.

블록체인에서는 정보 삭제와 관련된 잊혀질 권리의 구현이 어렵고, 다른 참여자들 또한 데이터를 가지고 있어 데이터 삭제에 대한 보장을 할 수 없기 때문이다. 이러한 문제점을 해결하기 위한 노력으로 아래 표 3에서와 같이 개인정보 관리 측면에서의 문제 해결을 위해 블록체인 활용 연구들이 이루어지고 있다.[19]

표 2. 개인정보보호 관련 블록체인 특징과 GDPR 조항 비교
Table 2. Comparison of personal information protection-related blockchain concepts and GDPR provisions

Blockchain Concept	GDPR article
The block chain is stored in the block by consensus	Article 7 'Conditions for consent'
Blockchain ensures data immutability	Article 16 'Right to rectification'
Unable to delete when block chain transaction is complete	Article 16 Right to erasure ('right to be forgotten')
Blockchain is distributed network architecture	Article 16 'Right to data portability'

표. 3. 블록체인에서의 프라이버시 이슈 대응방안
Table 3. Countermeasures for privacy issues in blockchain

Issue	Countermeasure
Block chain privacy prohibited	A method for ensuring the forgotten right required by the Personal Information Protection Act is not to enter the personal information of the data subject into the blockchain. In this case, the usability of the blockchain is poor in the system handling personal information.
Non-identification Personal Information storage	If the non-identifying information is stored on the blockchain and the participants can receive a reasonable reward accordingly, the ecosystem will be able to return.

Issue	Countermeasure
Data encryption	In the process of encrypting all personal information stored in the blockchain, a key is inserted so that it can be verified with a key file that only you have.
Storage of encrypted personal information through external database reference	Personal information is stored in a database through an encryption method, and only Hash values of the data are stored in the blockchain. Through this, since personal information does not exist in the blockchain, it can correspond to the Personal Information Protection Act.
Objection to automated decision making	Blockchain smart contracts are written in code to automate the process of contract execution and verification.By using on-chain governance, explicit consent can be verified by including in the code so that the subject of personal information can Included the transaction that has already been performed.

2.3.2 블록체인에서 개인정보보호 관련 연구 사례

블록체인 기술은 분산형 구조로 구성원이 합의·공유하는 블록에 저장·관리를 함으로써 데이터의 무결성을 보장하여 신뢰성을 확보할 수 있다. 이를 바탕으로 블록체인에 저장된 데이터가 위/증명의 증거자료로 활용이 가능하게 되었다. 대표적인 사례들 가운데 IBM-식품 공급망[20], 한국조폐공사-착(chak) 플랫폼[21]들이 신뢰를 기반으로 서비스가 이루어지고 있다.

이러한 블록체인을 개인정보 관리 시스템에서 활용 시 필연적으로 개인정보보호 규정준수와 같은 확장성 및 보안이슈가 발생하게 된다.[22,23] 이에 따른 문제점 해결을 위해 블록체인 기술 방식 중 온체인(on-chain), 오프체인(off-chain), 수정이 가능한 블록체인 등의 문제 해결 방법 등이 제시되고 있다.

먼저 (1) 일반적인 블록체인의 거래형태인 온체인(on-chain)은 온라인 서비스에서 활용하기에 트랜잭션 확정 소요시간이 길어 확장성의 문제 및 참여된 모든 사람들이 원치 않는 개인정보 또한 노출될 수 있는 가능성이 있다.[24,25] 이를 보완하는 방법으로 개인정보 등을 암호화시켜 트랜잭션 확정 시간 및 노출을 최소화시키는 방안들이 연구되고 있다.[26]

(2) 오프체인(offchain) 방식의 경우 메인 블록체인에 정보를 등록하는 것이 아니라 암호화된 정보를 오프체인에 저장하고 해당 해쉬 값을 온체인상에 저장하는 구조를 가진다. 이를 통해 확장성 및 개인정보보호에 대한 이점을 가지고 있다.[27,28]

(3) 블록체인에서 데이터의 변조 방지 및 비가역성에 대한 서비스 한계를 극복하기 위해 수정 가능한 블록체인 방식의 연구들이 이루어지고 있다.[29] 개인정보의 내용이 저장된 블록의 수정 시에도 블록의 무결성을 유지하는 방식을 택함으로써 EU의 GDPR의 주요 규정들을 만족시키는 방식을 제안하고 있다.[27] 하지만 기존의 블록체인 방식 대비 안정성에 대한 이슈가 존재한다.

따라서 정보처리자는 블록체인의 무결성 및 불변성의 특징을 활용하여 정보주체의 개인정보를 보호하면서, 합법적으로 개인의 정보를 처리하기 위한 연구가 필요하다.

Ⅲ. 블록체인 기반 약관 동의 증명 시스템 개발 설계 및 구조

3.1 블록체인 시스템의 기술 제안 구조

정보처리 주체의 개인정보 이용과 관련된 약관 및 동의 정보 관리를 위해 제안한 블록체인 기반 약관 동의 증명 시스템은 일반적인 온라인 약관 서비스 상에서 정보주체가 약관의 동의 여부를 증명하기 위해 필요한 이해관계자를 중심으로 한 역할로 구성되어 있다.

- User : 온라인 서비스 이용 또는 연동을 위해 서비스에 가입 또는 권한을 위임하는 사용자이며 PII/PPII를 가지고 있는 주체이다.
- Privacy Consumer : 온라인 서비스 사업자로 서비스 제공의 대가로 사용자로부터 개인정보 사용 권한을 위임받아 비즈니스를 영위하는 주체이다.
- Trust Provider : Privacy Consumer가 User의 개인정보 활용을 위해 동의받은 내역을 제 3자 입장에서 안전하게 저장 및 관리하고 증명 서비스를 제공하는 사업자이다.

그림 2는 제안된 플랫폼의 개념을 나타낸다. 주요 이해관계자의 구성은 다음과 같다.

User와 Privacy Consumer의 관계를 보면 Privacy Consumer는 User에게 서비스 공급의 대가로 개인정보를 제공받는다.

Trust Provider와 Privacy Consumer의 관계에서는 Privacy Consumer가 User의 개인정보 동의 시점과 관련된 개인정보 동의 내용을 Trust Provider에게 저장 요청하면 Trust Provider는 User의 동의 내용을 블

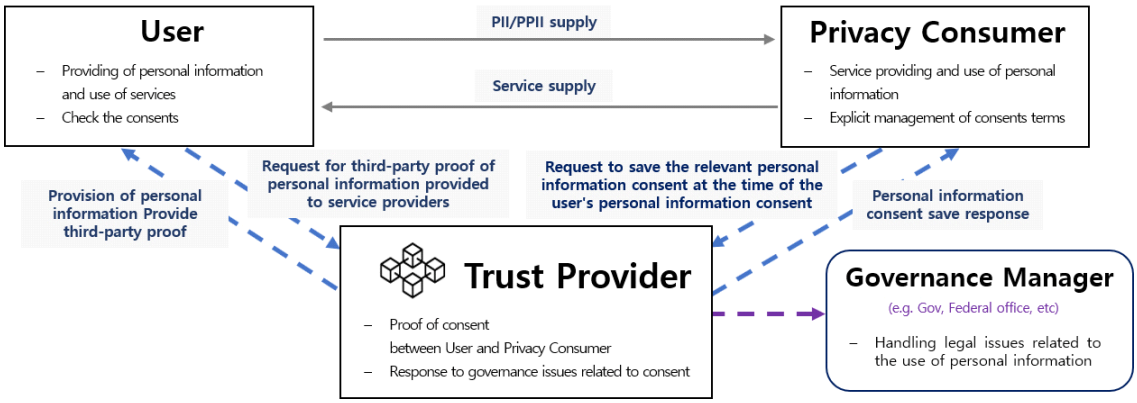


그림 2. 그림 제안된 블록체인 시스템의 모델 구조
Fig. 2. Model Structure of the proposed Blockchain System

록체인에 저장했음을 응답하게 된다.

User가 Privacy Consumer에게 제공한 개인정보 제공 내역을 제3자인 Trust Provider에게 증명 요청을 하게 되면 Trust Provider는 User가 개인정보 활용에 동의한 내용을 알려준다.

각 이해관계자는 블록체인 기반 약관 동의 증명 시스템 이용이 다음과 같이 이루어진다.

위의 과정에서 Privacy Consumer는 Trust Provider의 블록체인 기반의 약관 동의 증명 시스템을 통해 User의 정보처리 방식에 대한 동의 제공 여부를 입증받을 수 있도록 한다. 또한 Privacy Consumer의 경우 개인정보 기반의 서비스 이용에 따른 책임을 Trust Provider와 나눌 수 있는 시스템이 요구된다.

3.2 약관 동의 정보 증명을 위한 주요 프로세스

그림 3에서는 본 논문의 블록체인 기반 약관 동의 증명 시스템 프로세스의 흐름도를 보여주고 있다. 사용자가 Trust Provider 서비스에 이미 가입되어 있음을 가정으로 하고 있으며 블록의 생성 및 저장과 관련된 부분은 점선으로 표시되었다.

먼저 사용자 회원가입 시점에 발생하는 흐름은 ①~⑥번까지의 과정으로 아래와 같다.

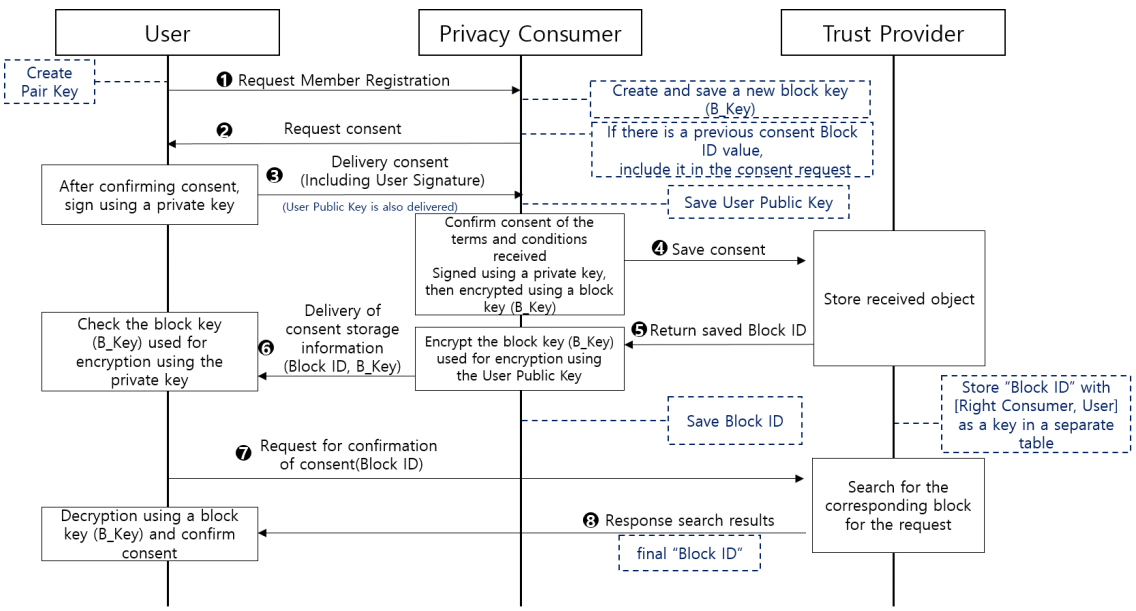


그림 3. 블록체인 기반 약관 동의 증명 시스템 프로세스
Fig. 3. Blockchain-based notarized system processes

① User가 서비스를 이용하기 위해 Privacy Consumer에게 회원가입을 요청한다. 회원가입을 요청한 경우 User에게 Pair Key가 생성된다.

② Privacy Consumer는 User에게 개인정보 활용에 대한 약관 동의를 요청한다. 이전에 Block ID가 등록되어 있는 경우, 동의 요청에 포함 시킨다.

③ User가 개인정보처리활용에 대한 동의 내용을 확인하고, 본인이 약관내용을 인지 하였음을 증명하기 위해 서명 후 Privacy Consumer에게 전달한다.

④ Privacy Consumer는 User로부터 전달받은 약관 동의를 확인하고 블록 Key를 사용하여 암호화시킨다. 그 값을 Trust Provider에게 전달하며 동의 내역을 블록체인 상에 저장 요청한다.

⑤ Trust Provider에서는 저장한 Block ID값을 Privacy Consumer에게 반환시킨다.

⑥ Privacy Consumer에서는 암호화에 사용된 블록 Key를 User의 Public Key로 암호화 후 동의된 저장 정보에 대해 User에게 다시 확인하는 절차를 거친다.

이후 가입된 사용자가 자신의 동의 정보에 대한 증명을 위한 프로세스는 ⑦, ⑧에 해당하며 아래와 같다.

⑦ User가 자신의 약관 동의 내역을 확인하기 위해 Block ID를 활용하여 Trust Provider에게 요청한다.

⑧ Trust Provider는 요청받은 암호화된 동의 내역을 User에게 전달하게 되고, 이는 자신의 블록 Key와 서명을 통해 복호화한 후 확인할 수 있다.

Ⅳ. 제안된 블록체인 시스템 개발 구현

4.1 구현 환경

본 논문에서는 가상머신 2대를 활용해 우분투 기반 개발환경을 사용하였으며, 한 대는 Privacy Consumer 역할을 제공하는 웹 서비스를 구축(PC), 다른 한대 Trust Provider 역할을 제공하는 블록체인 기반 약관 동의 증명 서버(TP)로 구축하였다.

표 4. PC, TP 전체 시스템 개발환경
Table 4. System development environment on PC, TP

Classification	Environment
Compute	Virtual machine (VM Ware Pro 15.5)
OS	ubuntu 18.0.02 LTS
Web Application Server	Express.js, node.js, HTML, Go(chain-code), Java Script
Database	mongoDB
Blockchain	Hyperledger fabric v1.4

PC에는 Node.js의 웹 프레임워크인 Express.js API 기반으로 온라인 서비스 사업자에 해당하는 가상의 웹사이트를 제작하고 사용자 가입 시 약관 동의 환경을 구성하였다. 기본적인 사용자 가입 정보와 약관 동의 내역 저장을 위해 데이터베이스는 mongoDB 사용하였으며, 암호화 및 서명은 JavaScript 이용해 작성되었다.

TP에는 하이퍼레져패브릭 v1.4 기반의 블록체인을 사용했으며, TCP/IP 소켓 통신을 하기 위한 Node.js의 웹 프레임워크인 Express.js API를 사용해 서버를 구축하였다. 그 외 작업으로 체인코드는 go언어 기반으로 작성하였으며, 체인코드 배포, 설치 및 블록조회는 Java Script를 통해 작성되었다. 그리고 블록체인의 노드 역할은 PC, 및 TP가 각각 수행한다.

4.2 구현된 시스템

4.2.1 약관 동의 관련 정보 수집

그림 4는 User가 PC를 이용하기 위해 회원가입을 하는 과정을 나타낸 것이다. 회원가입 시 ①~②번은 기존의 회원가입 구조를 나타내고, ③~④번은 블록체인 기반 약관 동의 증명 시스템을 이용하기 위한 구조이다. User가 약관 동의 내용에 서명 후 Key 파일을 내려받아 개인정보 및 약관 동의 내용, PC의 이름 등을 암호화시켜 블록체인 상에 저장시키는 방식으로 구현되었다. 관련 기능의 노드 간 신뢰성 확보를 위해 스마트 컨트랙트 방식의 일종인 하이퍼레저패브릭의 체인코드 기반으로 작성하였다.

① 회원가입 페이지로 전환되었을 때 제너럴 키(General Key)가 발급된다. 이후 User는 개인의 정보를 (ID, Password, Name) 입력한다.

② 개인정보 활용 및 수집에 따른 약관내용을 읽은 후 체크 유/무를 결정한다.

③ 서명을 통해 User의 약관 동의 개수, Privacy Consumer의 이름, User의 서명 등이 RSA-OAER 방법을 통해 암호화된다. User는 개인의 Key 파일을 컴퓨터상에 저장시킨다.

④ 회원가입 버튼을 통해서 Trust Provider에 사용자의 정보(Hashing 된 User의 ID, 약관 동의 내역, 암호화 내용, 시간)들이 블록체인에 저장된다.

4.2.2 약관 동의 내역을 저장하기 위한 블록의 구조

트랜잭션의 구성요소는 User의 ID, User가 동의한 내용, 동의 시간 그리고 서명으로 구성되어있다. 그 중 개인의 정보로 취급될 수 있는 User ID 및 동의 내

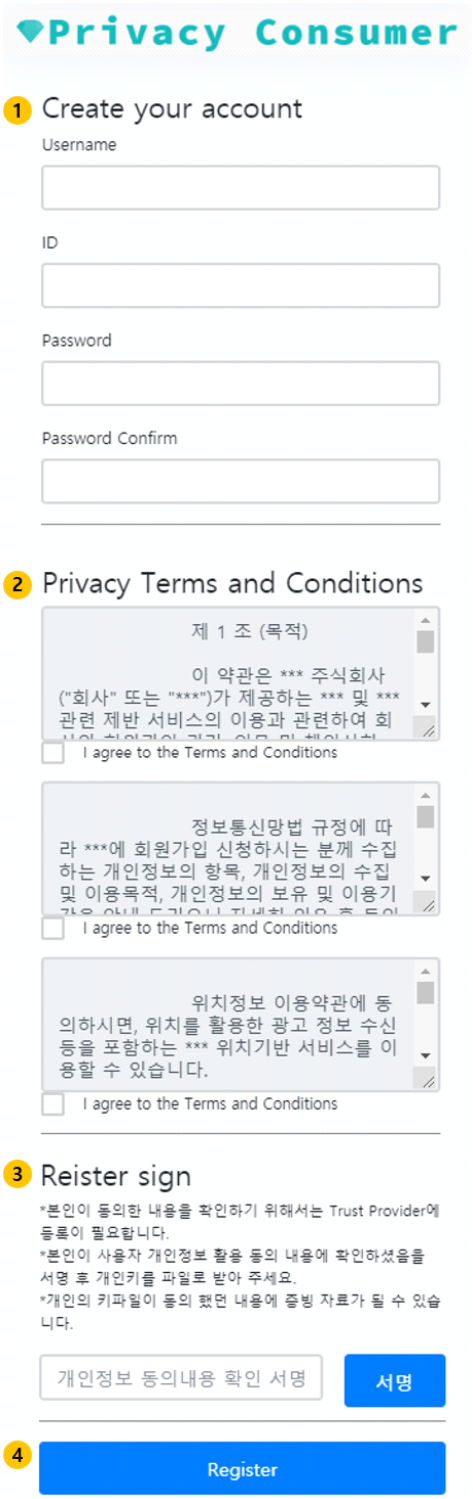


그림 4. User의 회원가입 절차
Fig. 4. Member Registration Process for User

표. 5. 트랜잭션의 구성요소
Table 5. Component of transaction

Variable name	Variable value	Type
User ID	User registered ID	String (Hash)
Block ID	ID issued when the user's consent is successfully registered	String (Hash)
Agreement 1,2,3	User consent	String
Agree time	Time the user agreed to use personal information	String
Encryption Data	Encrypting the details previously agreed by the user, the name of the privacy consumer, and the user's signature	String (Encryption data)

역, 서명 등은 암호화된 후 TP의 블록체인 상에 저장되며 표 5 트랜잭션의 구성요소와 같다.

4.2.3 블록체인 상에 약관 동의 정보 저장

PC는 User의 약관 동의 정보 획득 후 TP에 전달하게 된다. 이때 TP가 전달받은 정보는 User의 정보로 Hashing 된 ID, 약관 동의 시간, 암호화된 서명 및 약

```
1  type SmartContract struct { }
2  // Invoke 함수는 트랙잭션당 한번씩 호출되는 Chaincode API의 함수
3  function (s *SmartContract) Invoke (APIstubshim.ChaincodeStubInterface) sc.Response)
4  // fabric에서 데이터 가져오기 를 위해서 Query 호출
5  IF function == queyUseragreement THEN
6      return s.queryUseragreement(APIstub,args)
7  // 데이터를 초기화 하기위해서 Init 호출
8  ELSE IF function == initUseragreement THEN
9      return s.initUseragree(APIstub)
10 // fabric에서 블록에 데이터를 넣기 위해서 add 호출
11 ELSE IF function == addUseragreement THEN
12     return s.addUseragree(APIstub, args)
13 ENDIF
14 // 잘못된 스마트 계약  함수의 호출 일 경우 에러메시지
15 return shim.Error("Invalid Smart Contract function name.")
16 EXIT
```

그림 5. 약관 정보의 신뢰성 제공을 위한 체인코드 호출 구조
Fig. 5. Chaincode invoke structure for providing reliability of terms and conditions information

관 동의 내역, 약관 동의 개수, PC 정보를 담고 있으며, 이를 블록에 저장한다. 이후 그림 5와 같이 체인코드로 작성해둔 addUseragreement메서드 호출에 의해 해당 트랜잭션 아이디가 생성되고 성공 시 블록체인에 저장되는 구조를 가진다. 블록 상에 저장된 내용 중 일부 암호를 풀어 살펴보면 그림 6과 같이 약관 항목별 동의 여부에 대한 정보 및 약관 동의 내용 등이 저장되어 있음을 확인할 수 있다.

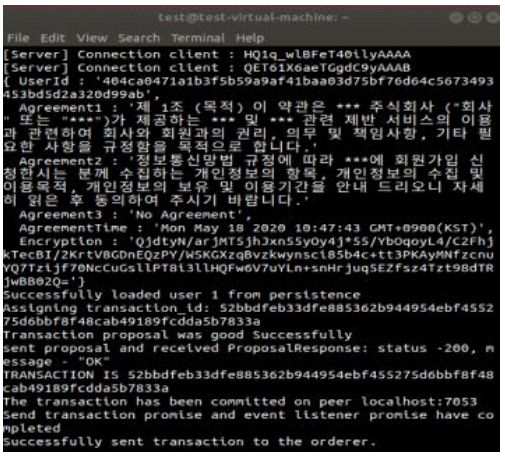


그림 6. 블록체인에 사용자 정보가 저장된 화면
Fig. 6. User information stored in the block chain

4.2.4 약관 동의 정보 저장 결과 반환

TP는 User의 약관 동의 내역 관련 정보를 블록 상에 저장 후, PC에게 해당 정보가 저장된 블록 ID를 반환한다. 이때 반환하는 정보는 JSON 구조를 가지며, Key값은 Block ID, Record는 User의 가입 시 약관 동의 관련 정보(약관 동의 내역, 시간, 암호화된 내역)로 구성된다. 해당 정보를 체인코드 상에서의 queyUseragreement 메서드의 호출을 통해서 이루어지며 결과가 성공적으로 저장되었을 때 그림 7과 같이 나타난다.

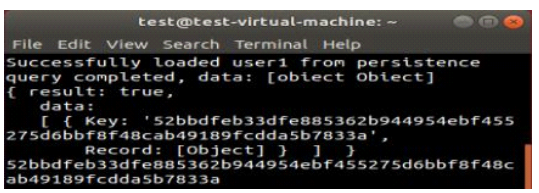


그림 7. 약관 동이 내역이 저장된 블록 ID의 반환
Fig. 7. Return of the block ID where the terms and conditions are saved

4.2.5 저장된 약관 동의 내역의 조회

User는 자신이 동의 한 내용을 조회하고 싶은 경우 TP에게 요청한다. 이때 User는 약관 동의 시 입력한 자신의 서명을 이용하여 블록의 내용을 조회할 수 있다. 검색 결과는 그림 8상에서 Key 파일 불러오기를 클릭하여 Key 파일을 첨부시킨 후 User의 서명확인 과정을 거치면 자신의 블록 내용을 확인할 수 있다.

최종적으로 TP가 User의 블록 ID, 회원가입 시 약관 동의의 체크 유/무, 약관 동의했던 시점의 시간, 개수를 보여주며 그림 9와 같이 나타난다.

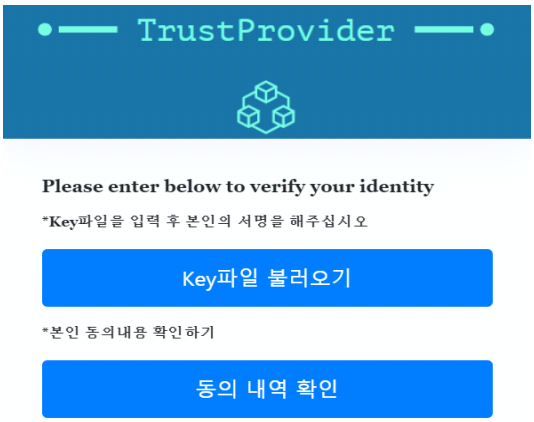


그림 8. 사용자 본인의 동의 내역 확인을 위한 인증 과정
Fig. 8. Certification process to verify your own consent history

Title	Contents
User ID	jiwon
Company Name	Privacy Consumer
Block ID	52bbdfeb33dfe885362b944954ebf455275d6bbf8f48cab49189fcdda5b7833a
Agreement1	제 1 조 (목적) 이 약관은 *** 주식회사 ("회사" 또는 "***")가 제공하는 *** 및 *** 관련 제반 서비스의 이용과 관련하여 회사와 회원과의 권리, 의무 및 책임사항, 기타 필요한 사항을 규정함을 목적으로 합니다. 제 2 조 (정의) 이 약관에서 사용하는 용어의 정의는 다음과 같습니다. ①"서비스"라 함은 구현되는 단말기(PC, TV, 휴대형단말기 등의 각종 유무선 장치를 포함)와 상관없이 "회원"이 이용할 수 있는 *** 및 *** 관련 제반 서비스를 의미합니다. ②"회원"이라 함은 회사의 "서비스"에 접속하여 이 약관에 따라 "회사"와 이용계약을 체결하고 "회사"가 제공하는 "서비스"를 이용하는 고객을 말합니다. ③"아이디(ID)"라 함은 "회원"의 식별과 "서비스" 이용을 위하여 "회원"이 정하고 "회사"가 승인하는 문자와 숫자의 조합을 의미합니다. ④"비밀번호"라 함은 "회원"이 부여 받은 "아이디와 일치되는 "회원"임을 확인하고 비밀보호를 위해 "회원" 자신이 정한 문자 또는 숫자의 조합을 의미합니다. ⑤"유료서비스"라 함은 "회사"가 유료로 제공하는 각종 온라인디지털콘텐츠(각종 정보콘텐츠, VOD, 아이템 기타 유료콘텐츠를 포함) 및 제반 서비스를 의미합니다. ⑥"포인트"라 함은 서비스의 효율적 이용을 위해 회사가 임의로 책정 또는 지급, 조정할 수 있는 재산적 가치가 없는 "서비스" 상의 가상 데이터를 의미합니다. ⑦"게시물"이라 함은 "회원"이 "서비스"를 이용함에 있어 "서비스상"에 게시한 부호・문자・음성・음향・화상・동영상 등의 정보 형태의 글, 사진, 동영상 및 각종 파일과 링크 등을 의미합니다.
Agreement2	정보통신망법 규정에 따라 ***에 회원가입 신청하시는 분께 수집하는 개인정보의 항목, 개인정보의 수집 및 이용목적, 개인정보의 보유 및 이용기간을 안내 드리오니 자세히 읽은 후 동의하여 주시기 바랍니다. 1. 수집하는 개인정보 이용자는 회원가입을 하지 않아도 정보 검색, 뉴스 보기 등 대부분의 *** 서비스를 회원과 동일하게 이용할 수 있습니다. 이용자가 메일, 캘린더, 카페, 블로그 등과 같이 개인화 혹은 회원제 서비스를 이용하기 위해 회원가입을 할 경우, ***는 서비스 이용을 위해 필요한 최소한의 개인정보를 수집합니다.
Agreement3	No Agreement
Agreement Time	Mon May 18 2020 10:47:43 GMT+0900(KST)

그림 9. 사용자 입장 약관에 동의한 내용 조회
Fig. 9. Check the details of which the user agreed to the terms and conditions

제안된 블록체인 기반 약관 동의 증명 시스템을 통해 사용자가 회원가입 시 동의했던 내용을 확인할 수 있다. 또한 PC 관점에서는 TP를 통해 사용자의 개인정보 데이터 활용에 따른 동의 내용을 위/증명 자료로 활용함으로써 GDPR의 '동의 조건'을 만족 시 킬 수 있다.

Ⅴ. 기존의 서비스 사업자 정보 저장 방식과 구현된 블록체인 시스템 비교 분석

서비스 사업자들이 약관 동의 내용을 저장하기 위해 사용한 기존의 데이터베이스 방식과 블록체인 기반의 약관 동의 내용 증명 시스템을 표 6에서 비교 분석하고 제안하는 시스템의 효율성을 검증하였다.

현재의 다수 서비스 사업자들은 사용자의 약관 동의 저장을 위해 서버-클라이언트 방식의 데이터베이스를 직접적으로 관리한다.[30] 약관 동의 내용을 데이터베이스에 저장하는 방식은 서비스 사업자가 임의로 사용자의 동의 내용을 변경, 추가, 삭제할 가능성이 있어 기록에 대한 이해관계자들간의 투명성 및 신뢰성 보장의 한계가 있다. 또한 기존의 방식은 사용자들이 약관 동의 내용이 변경되었음을 인지하기 어렵게 만드는 구조적인 문제를 가지고 있다. 이로 인해 서비스 사업자는 사용자 동의 시점에서의 약관 정보 수집에 대한 신뢰할 수 있는 근거를 입증하는 것에 한계가 존재한다.

본 논문에서 제안하는 약관 동의 증명 시스템에서는 네트워크 내에 모든 거래가 기록되고 공유되는 허가형 공유 원장 블록체인 기술 적용하였다. 이를 통해 사용자 동의 증명에 있어 각 이해관계자들간의 신뢰할 수 있는 시스템을 제공하였다.[31] 제안한 방식은 블록체인을 이용함으로써 기존에 사용자가 동의했던 내용에 시스템적인 투명성을 보장하고, 해당 정보들이 암호화된 상태로 피어 노드들에게 분산 저장됨으로써 동의 기록에 대한 증명 이슈 발생 시 이를 상호 신뢰할 수 있는 장점을 가진다. 이러한 특징을 바탕으로 표1에서와 같이 GDPR에서 규정하고 있는 동의 조항을 만족시킬 수 있었다.

표 6. 약관 동의 내용 저장을 위한 데이터베이스 방식과 블록체인 방식의 비교
Table 6. Comparison of database method and blockchain method for storing the contents

Properties	Blockchain	DB/Cloud
Operations	Only Insert Operations	Perform CRUD (create, read, update, delete) Operations
Control	Decentralized	Centralized
Architecture	Public peer-to-peer	Server-Client
Responsibility	Transparency	Non-Transparency
Data persistence	Immutability	Non-Persistence

Ⅵ. 결 론

본 논문에서는 온라인 서비스 사업자 및 사용자가 상호 신뢰할 수 있는 약관 동의 증명 시스템을 하이퍼레저패브릭을 이용해 설계 및 구현하였다. 이를 통해 온라인 서비스를 활용하는 사용자가 서비스 약관 동의 시 개인정보에 대한 이용 권한을 명시적으로 기록, 관리, 확인이 가능하도록 하고, 온라인 서비스 사업자 입장에서 사용자 가입 시점에서 동의 정보 및 해당 시점에서의 서비스 약관 정보 등에 대한 근거를 입증하는 것으로 목적을 달성할 수 있었다.

제안된 본 시스템은 사용자 약관 동의와 관련된 내용을 서비스 사업자 측에 저장하는 기존의 방식과 달리 신뢰할 수 있는 블록체인 상에 함께 저장함으로써 사용자가 인지하고 동의했던 내용의 변경 및 삭제를 막고 사용자의 개인정보 활용 권한 및 인식을 강화 시킬 수 있었다. 또한 사용자 및 온라인 서비스사업자가 동의 내역과 관련된 위/증명이 필요한 경우 증거 자료로 활용함으로써 '정보처리자(온라인 서비스 사업자)는 정보주체(온라인 서비스 사용자)가 개인정보 활용에 동의함을 입증해야 한다.'는 EU의 GDPR 규정을 만족 시 킬 수 있다.

향후 연구에서는 사용자 개인이 Key 파일을 보관하는 형식이 아닌 CA 기관이 인증서 보관을 하도록 함으로써 보안성 및 접근성을 높이고, 사용자가 편리하게 시스템에 접근할 수 있는 인터페이스 개발을 통해 '블록체인 기반 약관 동의 증명 시스템' 플랫폼의 사용성을 높이고자 한다. 더 나아가 온체인(on-chain) 환경에서 벗어나 오프체인(off-chain) 또는 수정이 가능한 블록체인 등 다른 방식의 장점을 수용한 약관 동의 증명 시스템의 연구를 진행할 예정이다.

References

[1] IAB, *Half-Year IAB Internet Ad Revenue Report*(2019), Retrieved May 20, 2020 from

https://www.iab.com/insights/internet-advertising-revenue-2019-half-year/

[2] S. An, "Self regulation of online behavioral advertising : An empirical examination of online behavioral advertising notices," *J. Broadcasting and Telecommun. Res.*, no. 81, pp. 156-181, Jan. 2013

[3] H. Park, J. Jung, and J. Yang, "A study on active user consent to obtaining and processing personal data - based on the types and conditions of consent in EU GDPR," *J. KICS*, vol. 44, no. 12, pp. 2352-2361, Dec. 2019.

[4] S.-Y. Lee, "Analysis of user's recognition for personal information agreement and new policy," *Korean Inst. Info. Technol.*, vol. 12, no. 8, pp. 85-92, Aug. 2014.

[5] Korea Ministry of Government Legislation, *Korea Personal Information Protection Act*(2017), Retrieved May 20, 2020, from http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EB%B2%95

[6] KISA, "*GDPR guidelines for consent*," KISA, 2017.

[7] D.-C. Kang, "Legal issue on consent for providing personal information to a third person - focus on cases of personal information dispute medication," *KIISE*, vol. 27, no. 12, pp. 34-41, Dec. 2009.

[8] Y. J. Kwon, *A study on the rights of personal information self-determination and consent system*, NAVER Privacy White Paper, pp. 120-127, 2015.

[9] R. Layton and S. Elaluf-Calderwood, "A social economic analysis of the impact of GDPR on security and privacy practices," *2019 12th CMI IEEE*, pp. 1-6, Copenhagen, Denmark, Nov. 2019.

[10] B. Choi, S. Chai, M. Kim, and Y. Kang, "A study of development plan regarding personal information management system and international standardization: GDPR perspective," *J. KICS*, vol. 43, no. 2, pp. 416-426, Feb. 2018.

[11] KISA, *Regulations of the European Parliament and the Council of Europe on the protection of individuals in relation to the processing of personal information and the free movement of personal information*, KISA, pp. 1-116, 2016.

[12] EU Blockchain Observatory and Forum, *Thematic reports*(2018), Retrieved May 15, 2020, from https://www.eublockchainforum.eu/reports

[13] Policy Wiki, *Data 3 Act*(2020), Retrieved May 17, 2020, from http://www.korea.kr/special/policyCurationView.do?newsId=148867915

[14] H. Kim, *Blockchain that is drawing more attention with the passage of the Data 3 Act*(2020), Retrieved May 17, 2020 from https://www.edaily.co.kr/news/read?newsId=04300086625704304&mediaCodeNo=257

[15] KISA, *GDPR Key terms*, Retrieved May 17, 2020 from https://gdpr.kisa.or.kr/gdpr/static/mainWord.do

[16] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-Compliant personal data management: A blockchain-based solution," *IEEE Trans. Info. Forensics and Secur.*, vol. 15, pp. 1746-1761, Oct. 2019.

[17] W. L. Sim, H. N. Chua, and M. Tahir, "Blockchain for identity management: The implications to personal data protection," *IEEE AINS*, pp. 30-35, Pulau Pinang, Malaysia, Nov. 2019.

[18] F. Zemler and M. Westner, "Blockchain and GDPR: Application scenarios and compliance requirements," *PICMET*, pp. 1-8, Portland, OR, USA, Aug. 2019.

[19] H. Yeom, "Blockchain security and privacy," *TTA J.*, vol. 177, pp. 55-64, May 2018.

[20] IBM-IBM Blockchain, *IBM Food Trust*(2019), Retrieved May 18, 2020, from https://www.ibm.com/kr-ko/blockchain/solutions/food-trust

[21] Infinite, *Block Chain Platform Chak*(2019), Retrieved May 18, 2020. from http://infinite.co.kr/portfolio/chak/

[22] J. Bernal Bernabe, J. L. Canovas, J. L.

Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, “Privacy-preserving solutions for blockchain: Review and challenges,” *IEEE Access*, vol. 7, pp. 164908-164940, Oct. 2019.

[23] B. Podgorelec, M. Heričko, and M. Turkanović, “State channel as a service based on a distributed and decentralized web,” *IEEE Access*, vol. 8, pp. 64678-64691, Mar. 2020.

[24] Asadal, *On-Chain*(2019), Retrieved May 13, 2020, from http://wiki.hash.kr/index.php/On-Chain

[25] T. Mitani and A. Otsuka, “Traceability in permissioned blockchain,” *2019 IEEE Int. Conf. Blockchain*, pp. 286-293, Atlanta, GA, USA, Jul. 2019.

[26] C. Li, B. Palanisamy, and R. Xu, “Scalable and privacy-preserving design of on/off-chain smart contracts,” *2019 IEEE 35th ICDEW*, pp. 7-12, Macao, Macao, Apr. 2019.

[27] J. Eberhardt and S. Tai, “ZoKrates - scalable privacy-preserving off-chain computations,” *2018 IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData*, pp. 1084-1091, Halifax, NS, Canada, Jul. 2018.

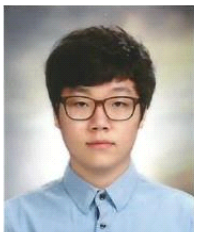
[28] Upbeat, *On-chain vs off-chain What’s the difference?*(2018), Retrieved May 13, 2020, from https://1boon.kakao.com/upbit/5becb287ed94d20001b0fa58

[29] N. Lee, J. Yang, M. M. H. Onik, and C. Kim, “Modifiable public blockchains using truncated hashing and sidechains,” *IEEE Access*, vol. 7, pp. 173571-173582, Nov. 2019.

[30] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain versus database: A critical analysis,” *2018 17th IEEE Int. Conf. Trust, Secur. and Privacy in Comput. and Commun./ 12th IEEE TrustCom/BigDataSE*, pp. 1348-1353, New York, NY, Aug. 2018.

[31] IBM, *what is hyperledger*(2018), Retrieved Jun. 15, 2020, from https://www.ibm.com/kr-ko/blockchain/hyperledger

이 정 현 (Jeong-Hyeon Lee)



2020년 2월 : 인제대학교 컴퓨터공학과 졸업

2019년 9월~현재 : 인제대학교 컴퓨터공학과 석사 재학 중

<관심분야> 개인정보보호, 블록체인, GDPR

[ORCID:0000-0001-8348-2049]

김 지 원 (Ji-Won Kim)

2018년 2월 : 인제대학교 컴퓨터공학과 졸업

2019년 9월~현재 : 인제대학교 컴퓨터공학과 석사 재학 중

<관심분야> 개인정보보호, 블록체인, GDPR

[ORCID:0000-0002-0764-3012]

김 철 수 (Chul-Soo Kim)

2003년 2월 : 부산대학교 컴퓨터공학 박사

1985년~2000년 : 한국전자통신연구원(ETRI) TDX 개발 운용SW 과제 책임자

2008년~2010년 : 지식경제부 네트워크 PD

2001년 9월~현재 : 인제대학교 컴퓨터공학과 교수

<관심분야> 네트워크 프로토콜, 트래픽 관리, 개인정보보호, GDPR, 블록체인

[ORCID:0000-0002-5522-1287]

양 진 홍 (Jinhong Yang)

2019년 2월 : KAIST 정보통신공학 박사
2017년 2월~2018년 1월 : HECAS 최고기술책임(CTO)
2018년 3월~현재 : 인제대학교 헬스케어IT 학과 조교수
<관심분야> CPS, IoT 시스템, 프라이버시

[ORCID:0000-0002-7756-0263]