잊혀질 권리와 블록체인의 상관관계 및 개선방안 연구

허재욱*, 김성수**, 강정호***, 전문석*
*숭실대학교 컴퓨터학과
**한국정보화진흥원
***배화여자대학교 정보보호과
e-mail:*g13621@soongsil.ac.kr **cryptoauth@nia.or.kr
***kangsamm@baewha.ac.kr *mjun@ssu.ac.kr

Study on Improvement and Correlation of Blockchain and Right to be Forgotten

Jae-Wook Heo*, Sung-Soo Kim**, Jeong-Ho Kang***, Moon-Seog Jun*
*Dept. of Computer Science, SoongSil University
**National Information Society Agency
***Dept. of Information Protection, BaeWha Women's University

요 약

4차 산업혁명을 주도하는 신기술인 블록체인은 블록체인 네트워크에 속한 모두가 신뢰성을 가질 수 있는 새로운 형태의 탈중앙화 P2P 플랫폼이다. 2018년 기존 개인정보 보호 지침을 대체하는 GDPR이 발효되어 다양한 부분의 개인정보 보호에 법적인 영향을 미치게 되었다. 블록체인 또한 GDPR의 법적 규제를 피할 수 없게 되었고, 블록체인에서 잊혀질 권리를 충족시키기 위해 정보주체의 요청 시 민감한 개인정보를 삭제할 수 있어야 하는 필요성이 요구되었다. 본 연구에서는 기존 블록체인 시스템에서 잊혀질 권리를 준수할 개선방안을 제안한다.

1. 서론

GDPR(General Data Protection Regulation)의 개인정보 보호에 관한 다양한 조항 중 잊혀질 권리(Right to be Forgotten, 법 제17조)는 정보주체는 본인에 대한 개인정보를 삭제하도록 요구할 수 있고, 요청에 따라서 정당한 이유가 없는 한 삭제하게 할 수 있는 권리를 말한다. GDPR이 발효됨에 따라 민감한 개인정보를 다루는 대다수의 블록체인(Blockchain) 역시 GDPR의 법적인 규제를 벗어날 수 없게 되었고, 잊혀질 권리를 준수하기 위해서 블록체인 시스템에서 정보주체의 요청 시 개인정보를 삭제할 수 있어야 한다. 그러나 블록체인은 정부나 은행과 같은 중앙기관이 통제 및 관리를 하는 구조에서 벗어나 블록체인 네트워크를 이용해 분산 형태로 저장 및 전파하여 관리하는 탈중앙화된 특성을 가지고, 블록체인의 구조는 블록들이 체인과 같이 이어져 있어서 악의를 가진 공격자가 쉽게 블록의 내용을 위·변조할 수가 없는 고유한 구조를 가진다. 즉, 블록체인의 위·변조 불가능 고유 특징 때문에 삭제나 수정이 일반적으로 불가능한 형태이다. 잊혀질 권리를 준수하기 위해서는 정보주체의 요청 시에 민감한 개인정보를 바로 삭제할 수 있도록 하는 새로운 블록체인 시스템이 요구된다. 본 연구에서는 2장에서 GDPR과 적용 범위, 잊혀질 권리에 대해서 다루고, 3장에서 블록체인에 대해 다룬다. 4장에선 잊혀질 권리와 블록체인의 상관관계 분석을, 5장에서 잊혀질 권리를 준수할 개선방안에 대해 제안하며, 6장 결론으로 끝을 맺는다.

2. GDPR

개인정보 보호 지침은 개인정보 보호라는 공통적인 목적을 가졌으나 시대가 지남에 따라 다양하고 새로운 신기술들의 도입과 국가별로 다른 제도기반과 법적 환경 등에 따라서 오히려 유럽연합 회원국 간에 자유로운 정보의 교류를 제한하게 되고 유럽연합이 최종적 목표로 하는 단일 시장의 발전을 저해하는 요인으로 작용하였다[1]. 이러한 이유로 인해 2012년 초안 발표와 지속적인 수정을 통해 최종적으로 2016년 기존의 개인정보 보호 지침을 대체하는 새로운 개인정보 보호법인 일반 개인정보 보호법 GDPR이 제정되고 2018년 발효되었다. 만약 GDPR을 위반할 경우에는 강력한 제재가 가해진다. GDPR 규정을 심각하게 위반할 때는 직전 연도의 세계 매출액의 4%나 최대 2천만 유로(약 250억 원) 중 더 큰 금액이 과징금으로 부과될 수가 있다. 일반적 위반의 경우에도 직전 연도의 세계 매출액의 2%나 1천만 유로(약 125억 원) 중 더 큰 금액으로 과징금이 부과될 수 있다[2]. 이는 매우 강력한 제재로써 기업의 입장에서 쉽게 위반하기 어려운 구속력을 가진다.

2.1 GDPR의 적용 범위

GDPR의 적용 범위는 크게 물적 적용 범위, 지역적 적용 범위, 인적 적용 범위 세 가지로 나눌 수 있다. 첫 번째로 물적 적용 범위는 개인정보가 자동화된 수단에 의해 처리될 경우 GDPR이 적용된다. 단 자동화된 수단 이외에도 파일링시스템의 일부를 구성하거나 목적으로 하는 개인정보의 처리에는 GDPR이 적용될 수 있다. 예외로 익명의 정보는 개인정보에 해당하지 않기 때문에 GDPR이 적용되지 않는다. 또 특정한 기준에 따라서 구성되지 않은 물리적 파일이나 파일의 집합물에는 적용되지 않는다. 두 번째는 지역적 적용 범위의 경우이다. 유럽연합의 데이터 컨트롤러와 프로세스의 사무소나 거점이 수행하는 활동에는 GDPR이 적용된다. 여기서 언급된 사무소나 거점이란 개인정보 보호의 관점에서 특정 조직이 어느 유럽연합 회원국의 사법관할권 영향에 놓이게 되는지를 결정하는 개념으로, 법률적 형태에 구속되지 않는 넓은 표현이라고 할 수 있다. 유럽연합 외의 국가에서도 유럽연합 정보주체에게 언어, 통화 등의 정보를 제공하는 경우에 GDPR이 적용된다. 제공한다고 판단되는 요소는 다음과 같다.

<표 1> 정보 제공으로 판단되는 요소

요소	내용
언어	소재 또는 거주 국가의 고객과 관련 없는 유럽연합 회원국의 언어를 사용
통화	소재 또는 거주 국가에서 일반적으로 사용하지 않는 유럽연합 회원국의 통화를 사용
도메인 이름	웹사이트의 도메인 이름이 유럽연합 회원국의 최상위 도메인 명칭을 사용함
회원국 시민 언급	재화나 서비스를 홍보하기 위해 유럽연합 회원국 시민을 언급함
소비자 기반	유럽연합 내에 높은 비율의 소비자를 보유하고 있음
광고 타게팅	유럽연합 회원국의 정보주체를 목표로 광고를 제공함

세 번째로 인적 적용 범위가 있다. 법인의 정보나 사망한 사람의 개인정보를 처리하는 경우에는 GDPR이 적용되지 않는다. 또한 GDPR이 적용되는지 여부를 고려할 때 정보주체인 자연인의 국적이나 거주지가 반드시 유럽연합 회원국일 필요는 없다는 것이 있다[3].

2.2 잊혀질 권리

정보사회가 발달함에 따라 정보주체의 권리가 강화되어 유럽연합 지침에 잊혀질 권리가 새롭게 도입되어 정보주체의 권리가 강화되었다. 잊혀질 권리는 “정보주체는 본인에 대한 개인정보를 삭제하도록 요구할 수 있는 권리를 가진다. 컨트롤러는 요청에 따라서 정당한 이유가 없는 한 삭제해야 한다.”로 GDPR 제17조에 명시되어 있다. 잊혀질 권리에 따라 다음과 같은 경우에는 바로 개인정보가 삭제되어야 한다.

1. 개인정보가 수집 및 처리 목적과 관련하여 더 이상 필요하지 않은 경우
2. 정보주체가 개인정보 처리에 대한 동의를 철회하였으며, 해당 개인정보를 처리할 법적 근거가 없는 경우
3. 정보주체가 법 제21조(반대권) 제1항에 따라 개인정보의 처리에 반대하고, 관련 개인정보처리에 우선하는 정당한 사유가 없는 경우 또는 법 제21조 제2항에 의한 직접 마케팅(Direct marketing)에 정보주체가 반대하는 경우
4. 개인정보가 불법적으로 처리된 경우
5. 유럽연합 또는 유럽연합 회원국 법령의 준수를 위해서 개인정보의 삭제가 필요한 경우
6. 아동을 대상으로 한 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우

다만 예외적 상황도 존재하는데 다음의 경우에는 삭제 요구를 거부할 수 있다.

1. 표현(expression) 및 정보(information)의 자유에 관한 권리 행사를 위한 경우
2. 유럽연합 및 유럽연합 회원국의 법적 의무를 준수하거나, 공익상의 업무를 수행하기 위해 또는 컨트롤러에 부여된 공적 권한을 행사하기 위한 경우
3. 공익을 위한 보건 목적을 위한 경우
4. 공익적 기록보존(archiving purposes) 및 과학, 역사연구, 통계 목적을 위한 경우
5. 법적 청구권의 입증이나 행사 또는 방어를 위한 것인 경우

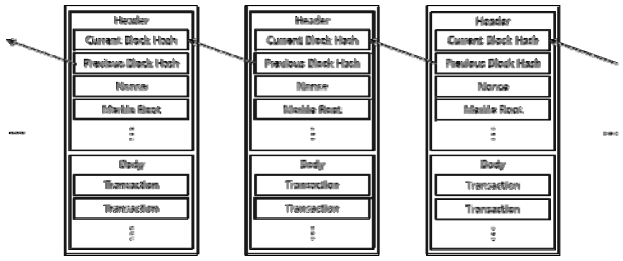
정보주체의 권리 강화를 위해 새롭게 도입된 잊혀질 권리의 경우에는 개인정보 처리의 근거와 목적을 확실히 파악해 개인정보의 삭제가 필요한 경우와 삭제를 거부할 수 있는 경우를 명확히 정의하여 구분해야 하고, 삭제 대상이 되는 모든 개인정보의 저장 위치, 형태, 담당 부서 등을 파악하여 복제본, 백업본, 사본 등도 빠짐없이 모두 삭제될 수 있게 조치해야 한다. 만약 개인정보를 수령인에게 제공 및 공개하였다면 해당 개인정보의 링크, 사본, 재현물이 삭제될 수 있도록 요청사항을 통지하는 등의 합리적인 조치를 취해야 한다[3].

3. 블록체인

4차 산업혁명을 주도하는 대표적인 플랫폼 기술이라고 할 수 있는 블록체인은 사토시 나카모토(Satoshi Nakamoto)의 논문으로부터 시작되어 비트코인(Bitcoin), 이더리움(Ethereum) 등 다양한 암호화폐를 탄생시켰다. 암호화폐를 시작으로 단순한 암호화폐의 기능을 넘어서 다방면의 산업에서 중요한 수단으로 블록체인이 활용될 수 있다. 블록체인의 핵심적 원리는 일정 시간 동안 발생한 트랜잭션(Transaction)을 수집하여 블록으로 생성하게 되고 이를 블록체인 네트워크의 모든 노드(node)에 전파한다. 전파된 블록의 유효성을 각 노드가 검증하게 되고 유효하다면 이를 체인 형태로 연결하게 된다.

3.1 블록체인 구조

블록체인의 구조에서 각 블록은 헤더(Header)와 바디(Body)로 구성된 형태를 가진다. 헤더에는 블록들의 해시값(Hash)과 넌스값(Nonce), 머클 트리값(Merkle Root) 등의 정보를 가진다. 바디에서는 일정시간 동안 발생한 트랜잭션을 가지게 된다.



(그림 1) 헤더와 바디로 구성된 체인 형태의 블록체인 구조

헤더에 존재하는 해시값들이 이전 블록의 해시값과 현재 블록의 해시값을 모두 가지는 구조로써 체인 형태로 블록들을 모두 검증하게 한다. 악의적인 공격자가 블록체인 네트워크에서 데이터를 위·변조하기 위해 블록을 수정하려면 모든 블록을 변경해야 하므로 실질적으로 데이터의 위·변조가 불가능한 구조를 가진다.

3.2 블록체인의 종류

블록체인 네트워크는 크게 세 종류인 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인(Consortium Blockchain)으로 나뉜다.

<표 2> 블록체인의 종류[4]

구분	개념 및 특징
퍼블릭 블록체인 (Public BlockChain)	- 모든 참여자에게 공유되는 완전한 분산형 구조 - 신뢰성 없이도 누구나 자유롭게 원장의 정보를 공유 - 거래 속도가 느리며 저장하는 내용이 한정적임
프라이빗 블록체인 (Private BlockChain)	- 승인된 관리주체가 관리하는 구조 - 관리주체가 검증자 역할을 수행하여 블록을 생성함 - 빠른 거래속도 등의 효율성이 높음 - 중앙화적 성격의 비판적 시각 존재
컨소시엄 블록체인 (Consortium BlockChain)	- 프라이빗 블록체인과 흡사하나 다수의 관리주체가 합의하에 운영하는 구조 - 검증자의 역할을 하는 관리주체가 분산되어 관리됨 - 시스템의 신뢰성 증대와 성능 향상이 가능함

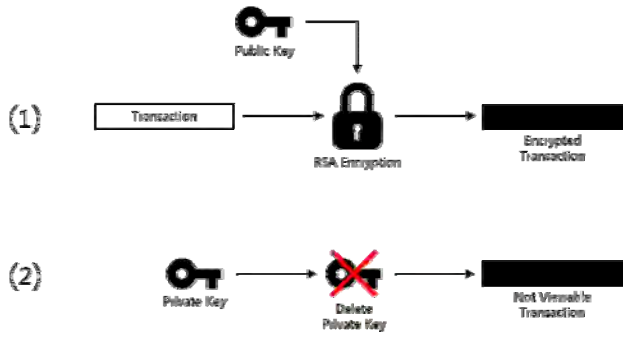
퍼블릭 블록체인은 비트코인과 같은 블록체인의 대표적 형태라고 할 수 있다. 완전히 분산된 구조를 가지며 모두에게 공개되어 누구나 장부를 열람할 수 있다. 프라이빗 블록체인의 경우, 개인형 및 중앙집권형 구조를 가져 중앙기관이 일정 수준의 통제권을 가진다. 컨소시엄 블록체인의 경우 반 중앙형 및 부분적 분산형 구조를 가진다. 컨소시엄에 포함된 N개의 기관이 연합하여 참여 주체들 간의 합의된 규칙을 통해 관리된다.

4. 잊혀질 권리와 블록체인의 상관관계

블록체인이 사용되는 가상화폐의 경우 가상화폐 거래자들의 거래 정보를 블록체인 블록에 기록한다. 이때 거래자의 이름과 거래내역, 재산보유상황 등 민감한 개인정보가 포함되는데 이는 GDPR 개인정보 보호 대상에 해당한다. 가상화폐뿐만 아니라 블록에 개인정보가 포함되는 다른 블록체인 시스템도 마찬가지로 법적 규제의 대상이 되고, 블록체인 시스템은 잊혀질 권리에 따라 정보주체가 요구할 시에 언제든지 블록에 기록된 개인정보를 삭제할 수 있어야 한다. 블록체인 구조는 헤더의 해시값으로 이전과 현재, 다음 블록이 모두 체인처럼 연결된다. 블록체인 특성상 하나의 블록을 수정하기 위해서는 모든 블록을 변경해야 하는 구조를 가지기에 블록이 생성되고 난 뒤에는 블록의 내용을 수정하기가 불가능하다. 이러한 점 때문에 현재의 블록체인 구조는 잊혀질 권리를 준수하기가 불가능하며 기존 블록체인 구조의 개선방안 필요성이 요구된다.

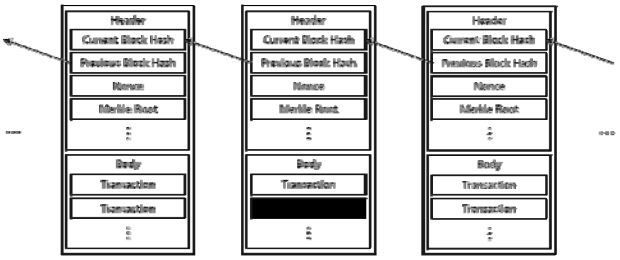
5. 잊혀질 권리를 준수하는 블록체인 개선방안

블록체인 구조가 가지는 특성은 잊혀질 권리를 준수할 수 없는 구조를 가짐에 따라 민감한 개인정보를 별도로 저장하는 방식 등의 새로운 방식들이 제안되었으나 별도의 복잡한 구조와 저장소가 필요한 단점과 같이 효율적인 방식이라 할 수 없다. 잊혀질 권리는 대표적으로 “정보주체는 본인에 대한 개인정보를 삭제하도록 요구할 수 있는 권리를 가진다. 컨트롤러는 요청에 따라서 정당한 이유가 없는 한 삭제해야 한다.”로 명시하고 있으나 잊혀질 권리의 정의에 다양한 해석에 따라서 “각종 조치를 통하여 타인이 자신과 관련된 정보를 포함하는 자료에 접근할 수 없도록 하는 권리[5]”로 해석될 수 있음을 이용해 새로운 방식의 개선방안을 제안한다. 프라이빗 블록체인을 기반으로 블록체인 네트워크에서 민감한 개인정보에 대해 정보주체가 잊혀질 권리로 삭제를 요청할 경우, 신뢰받는 관리주체는 개인정보가 포함된 해당 트랜잭션을 공개키 암호화 알고리즘인 RSA(Rivest Shamir Adleman) 암호화를 이용해 관리주체 자신의 RSA 키 쌍의 공개키로 암호화한다. 암호화된 트랜잭션은 개인키를 소유한 관리주체 자신 이외에 제삼자가 조회나 열람할 수 없게 된다. 이후 관리주체가 트랜잭션 복호화 시 필요한 개인키를 완전히 파기함으로써 암호화된 트랜잭션은 영구적으로 복호화가 불가능하고 관리주체를 포함한 아무도 조회하거나 열람할 수 없는 삭제와 같이 해석될 수 있는 상태가 된다.



(그림 2) RSA 암호화를 이용해 영구적으로 조회가 불가능한 트랜잭션

관리주체는 변경한 트랜잭션이 포함된 블록을 블록체인 네트워크 내에 재전파하여 기존의 블록을 교체함으로써 모든 노드에서 최종적으로 조회할 수 없게 만든다. 이러한 과정을 통해 해당 트랜잭션을 삭제와 같이 만들어 잊혀질 권리를 준수할 수 있으며, 대중적으로 사용되는 공개키 암호화를 이용함으로써 복잡한 구조적 변경 없이 쉽게 구현할 수 있다. 또한 해당 트랜잭션을 암호화하기 전 원본 해시값을 암호화하기 전에 별도 저장해 머클트리(Merkle Tree)에 따른 해시값과 기존 블록의 해시값의 유효성 검증에 문제가 없도록 하여 기존 블록체인의 구조적 특징은 변함없이 유지되어 블록체인의 장점은 그대로 유지할 수 있다.



(그림 3) 조회가 불가능한 트랜잭션을 가지는 블록체인 구조

6. 결론

민감한 개인정보를 포함하는 대다수의 블록체인 시스템은 GDPR의 개인정보 보호를 준수해야 함에 따라 잊혀질 권리에 의한 정보주체의 개인정보를 삭제할 필요성이 요구되었다. 본 연구에서는 신뢰받는 관리주체가 존재하는 프라이빗 블록체인을 이용해 기존 블록체인이 장점으로 가지는 위·변조가 불가능한 체인 구조는 그대로 유지 시키면서, 민감한 개인정보가 담긴 특정 트랜잭션을 삭제와 같이 조회할 수 없는 형태로 만들어 잊혀질 권리를 준수할 수 있게 하였다. 앞으로 블록체인이 지속해서 활발하게 적용되기 위해서는 법적인 규제를 준수해야 할 의무가 있다. 기존 퍼블릭 블록체인에서는 신뢰받는 관리주체가 존재하지 않기 때문에 잊혀질 권리를 준수하기에 많은 기술적 어려움이 따르는 것이 현실이다. 다양한 종류의 블록체인과 GDPR 개인정보 보호의 법적 관계에 대한 심층적인 연구를 통해 민감한 개인정보를 블록체인 시스템에서 효과적으로 준수할 수 있게 하는 지속적인 연구가 필요하다.

참고문헌

[1] 오태현, 강민지, (2018), "유럽연합 개인정보보호법(GDPR) 발효: 평가 및 대응방안", KIEP, Vol. 18 No. 19

[2] 김정곤, 윤재석, (2018), "EU의 일반개인정보보호법(GDPR) 발효와 대응과제", KOTRA, Global Strategy Report 18-002

[3] 한국인터넷진흥원, 행정안전부, (2017), "우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 1차 가이드라인"

[4] 남충현, (2018), "블록체인의 다변화: 채굴 없는 블록체인의 확산", KISDI, 18-01

[5] 구태언 (2014), “잊힐 권리의 국내법상 검토 및 발전방향”, 정보법학, 제18권 제3호