Journal of Korea Multimedia Society Vol. 23, No. 2, February 2020(pp. 262-273)
https://doi.org/10.9717/kmms.2020.23.2.262

마이데이터 개념을 활용한 탈중앙화 저작권 관리 모델

김혜빈[†], 신 원[††], 신상욱[†††]

A Decentralized Copyright Management Model using Mydata Concept

Hyebin Kim[†], Weon Shin[††], Sang Uk Shin[†††]

ABSTRACT

This paper analyzes the existing copyright management and copyright sharing model and discusses the limitations. It then proposes a consortium Blockchain-based copyright management model in which the service platform participates as a node, and discusses how to combine the My Data concept with Blockchain and smart contracts. Also, Blockchain-based CP-ABE is introduced and applied to the proposed model as a way for users to define access policies and store copyright data in encrypted form on the storage of the online service providers (OSP). Compared with the existing copyright management model, the proposed model allows the copyright holder to focus on copyright registration, license content design, and sharing, as the data subject. And it is expected to be able to transparently manage the usage records and the basis for the settlement of the copyrighted data that are shared and used on each platform.

Key words: MyData, Blockchain, Smart Contract, CP-ABE

1. 서 론

저작권(Copyright)은 창작물을 만든 이가 본인의 저작물에 대해 가지는 배타적인 법적 권리로써, 저작물을 보호하는 역할을 한다[1]. 최근 저작물을 서비스하는 플랫폼의 증가와 함께 다양한 종류의 수많은 창작물들이 저작권자와 소비자사이에서 거래 및 공유되어왔다. 그리고 분야를 막론하고 다양한 유형의 저작물들이 융합하여 새로운 저작물이 탄생하는 등 저작물 산업계가 복잡해졌고, 이에 따라 서비스 플랫폼과 저작권자, 소비자 간에는 복잡한 이용 및 권리 관계가 존재하게 되었다. 이를 명확하기 위하여 저작물의 저장 및 관리 그리고 저작물 이용 기록에 대한 신뢰성 보장의 중요성이 대두되었다.

기존의 저작권 및 저작물 공유 시스템은 저작권자가 서비스 플랫폼에 저작물 데이터를 등록하면, 플랫폼이 그것들을 관리하며 필요한 소비자에게 게시하거나 판매한다. 데이터 이용 기록을 근거로 하여 판매 수익을 정산하고, 수수료를 제한 후 저작권자에게 저작권료를 지급하는 형태이다. 다시 말해 서비스 플랫폼이 중앙의 데이터 공유 중개자 역할을 수행하는 셈이다.

※ Corresponding Author : Sang Uk Shin, Address: (48513) 45, Yongso-ro, Nam-Gu. Busan, Korea, TEL : +82-51-629-6249, FAX : +82-51-629-6230, E-mail : shinsu@pknu.ac.kr
Receipt date : Jan. 13, 2020, Approval date : Feb. 11, 2020
[†] Interdisciplinary Program of Information Security, Graduate School, Pukyong National University (E-mail : khbin1346@pukyong.ac.kr)
[††] Dept. of Information Security, Tongmyoung University (E-mail : shinweon@tu.ac.kr)
[†††] Dept. of IT Convergence and Application Eng., Pukyong National University
※ This work was supported by a Research Grant of Pukyong National University(2019).

문제는 이러한 시스템은 클라이언트-서버(Client-Server) 구조의 중앙 집중형 시스템의 단점을 상속한다. 저작권자는 자신의 데이터를 공유하는 데 있어 서비스 플랫폼의 관련 정책에 의존하며, 서비스 플랫폼이 제공하는 이용 기록을 신뢰할 수밖에 없다. 그러나 서비스 플랫폼의 부당한 이익 취득을 위한 이용 기록 위·변조 사건이 다수 발생해왔다[2]. 또한 소비자들의 저작물 무단 사용 및 재배포 문제도 끊임없이 문제점으로 제기되고 있다. 제기되는 문제점은 주로 저작물 취급 대상이 아님에도 불구하고 무단으로 사용하거나, 자신의 저작물인 것처럼 타 플랫폼에 업로드 하는 것들이다. 이러한 저작권 침해사고들은 저작권자로 하여금 창작의 의지를 위축시키고 이로 인해 이용할 수 있는 저작물이 줄어들게 되면 저작물 산업계가 원활하지 못하게 될 수 있다. 그 동안 저작권 침해사고를 해결하기 위한 대책방안으로 [3]과 같이 디지털 워터마킹(Digital Watermarking)에 대한 심화된 연구도 끊임없이 진행되어 왔다. 이는 가장 잘 알려진 기술로써 널리 사용되고 있지만, 원본 데이터에 변형을 가하여 워터마크를 훼손시키거나, 많은 계산량을 요구하는 등의 단점이 근본적으로 존재한다. 따라서 플랫폼에 걸쳐 전반적으로 저작권을 보호할 수 있는 기술이 요구된다.

최근 들어 4차 산업혁명 기술 중 하나인 블록체인(Blockchain)을 저작권 관리 모델에 적용함으로써 [4]에서와 같이 이용 기록의 신뢰성 및 투명성을 보장하여 저작권자 중심의 저작물 공유를 하는 시스템에 대한 많은 연구가 진행되어 왔다. 이는 블록체인이 P2P(Peer-to-Peer) 네트워크라는 특징을 통해 서비스 플랫폼과 같이 중개자가 존재하지 않는 C2C(Consumer to Consumer)모델을 구현해 낼 수 있을 것으로 기대되었다. 이는 저작물 생태계의 또 다른 패러다임을 불러 왔음은 분명하다. 하지만 개인이 온전히 저작권을 주장하거나, 서비스 플랫폼을 완전히 배제시키는 것은 실질적으로 불가능하다. 또한 소비자의 이용 기록 위반에 대해서 완전히 파악하지 못하는 점도 존재한다.

따라서 서비스 플랫폼들을 배제시키지 않은 현실적인 모델에서 중앙 정책에 의존하지 않고 저작권자 중심으로 저작물을 공유할 수 있는 시스템에 대한 연구가 필요하다. 본 논문에서는 우선 서비스 플랫폼을 호스팅하는 조직들로 구성된 블록체인을 구성한다. 그 후 GDPR(General Data Protection Regulation)에 의거한 개인 데이터 관리 정책인 마이데이터(MyData)[5]를 이용하여 사용자의 속성을 바탕으로 저작권자가 직접 저작물 이용조건을 설계하고 그 내용을 계정정보로 관리할 수 있는 플랫폼을 제안한다.

2. 관련연구

2.1 마이데이터(MyData)

마이데이터(MyData)는 정보의 주체가 되는 개인이 본인 정보를 적극적으로 제어하여 이를 이용한 신용관리, 자산관리, 건강관리 등 생활에 주도적으로 활용할 수 있는 일련의 과정들을 지칭한다[5]. 이는 분산된 본인의 데이터를 한 곳에 모아 관리 할 수 있도록 한다.

마이데이터의 핵심은 데이터 소유주 중심으로 데이터 관리 및 제어를 수행한다는 점이다. 현재 데이터 관리 및 사용 동의 결정 수행은 데이터를 가지고 있는 조직을 중심으로 이루어진다. 반면 마이데이터 모델을 적용하게 되면 데이터를 사용하고자 하는 사용자가 데이터를 소유하고 있는 플랫폼에 데이터 사용 및 제공 요청을 할 때 해당 데이터를 소유 및 서비스하는 플랫폼 사업자가 소유자의 이용 동의를 요청한다. 소유자의 동의가 이루어지고 나면 데이터 공유가 가능하다. 이러한 방식을 통하여 정보 주체는 자신이 동의한 수준에 따라 데이터를 이동하거나 처리할 수 있다. 가장 대표적으로 알려져 있는 모델로는 핀란드 교통 통신부가 내놓은 MyData 모델로써 마이데이터 계정 정보를 기반으로 정보 제공의 동의서를 관리한다. 해당 계정정보는 마이데이터 운영자(Operator)가 관리한다.

2.2 블록체인과 스마트 계약

블록체인은 P2P 네트워크를 기반으로 하는 탈중앙화 분산 원장기술(Decentralized Distributed Ledger Technology)이다[6]. 2008년 사토시 나카모토(Satoshi Nakamoto)가 제안한 비트코인 거래를 위한 기반 기술로써 처음 등장하였다. 블록체인의 핵심은 P2P 네트워크에 있는 노드가 작업 증명(Proof Of Work, PoW)과 같은 합의 메커니즘(Consensus Mechanism)으로 분산 장부를 동일하게 유지 및 관리한다는 것이다[7]. 이는 기존의 클라이언트-서버

구조에서는 서버가 TTP(Trusted Third Party)로써 저장된 데이터의 신뢰성을 보장한 것과는 다르다. 블록체인 네트워크는 TTP가 존재하지 않는 탈중앙화 모델이기 때문에 다른 방법으로 저장된 데이터의 신뢰성을 보장해야했으며 이를 위해 노드 간 합의를 수행함으로써 전체 네트워크를 관리할 수 있다.

블록체인의 데이터를 네트워크에 있는 노드 누구나 열람할 수 있도록 투명하게 공개하면 데이터를 임의적으로 위·변조하지 못한다[8].

그리고 스마트 계약(Smart Contracts)은 2013년 Vitalik Buterin이 블록체인과 결합한 확장된 개념으로 소개함으로써 널리 알려지게 되었다. 스마트 계약은 기타 거래 내역들과 마찬가지로 블록체인 내에 트랜잭션 형태로 포함이 됨으로써, 조건이 충족되면 누구도 부인할 수 없는 자동화 된 작업을 수행할 수 있다.

또한 스마트 계약은 블록체인 내에 코드가 포함이 되어 조건이 충족되면 해당 코드를 실행할 수 있다. 이를 이용해 블록체인 현재 상태, 즉 블록체인에 등록되어있는 데이터 및 자산의 상태를 나타내고 변경하는 역할을 한다[9]. 이더리움에서의 스마트 계약 등장 이후 단순 화폐 거래 이외에 다양하고 복잡한 계약을 코드화하여 블록체인 상에서 수행할 수 있게 되었다.

2.3 분산 CP-ABE

다중 권한 CP-ABE[11]라고도 하는 분산 CP-ABE 기법은 기존의 CP-ABE[10]의 AA(Attribute Authority)를 여러 개를 두어 관리하는 것을 의미한다. 이는 기존 CP-ABE의 문제점 중 하나였던 속성 관리에서의 과부하를 줄여 대규모 시스템에 적용할 수 있다. 분산 CP-ABE 기법의 프로세스는 다음과 같다[11].

1) $globalsetup(1^{\lambda}) \rightarrow PP$

비밀 매개변수 1^{λ}을 입력 값으로 하여 공개 파라미터 PP(Public Parameter) 값을 먼저 계산한다. g, y는 순환군 G의 독립된 두 개의 생성자(generator) 값이다. G, G_T는 같은 위수 p를 가지는 두 개의 곱셈 순환군이며, e는 $G \times G = G_T$ 를 계산하는 겹선형 사상이다. 이 때 각각의 AA 집합을 $\{A_1, A_2, \ldots, A_{n_a}\}$로 표현할 수 있다. 그리고 임의의 A_i가 관리하는 속성의 집합을 $\widetilde{A}_i = \{a_1, a_2, \ldots, a_{N_i}\}$ 라고 한다. 계산된 PP는 다음과 같다.

$$PP = (g, y, e, p, G, G_T) \tag{1}$$

2) $AuthoritySetup(\widetilde{A}_i, S_{i,j}) \rightarrow MSK_i, PK_i$

AA가 수행하여 마스터 키 및 공개키 MSK_i, PK_i를 생성하며 그 값은 다음과 같다.

$$MSK_i = \{\alpha_i, \beta_i, \gamma_i, z_{i_j,k} | 1 \le j \le N_i, 1 \le k \le n_{i_j}\} \tag{2}$$

$$PK_i = \{A_i, B_i, Q_i, Z_{i_j,k}, T_{i_j,k} | 1 \le j \le N_i, 1 \le k \le n_{i_j}\} \tag{3}$$

3) $KeyGen(MSK, Attrs) \rightarrow SK$

이는 사용자의 속성 비밀키를 생성하는 단계로써, 입력 값은 사용자의 GID 값인 u와 사용자의 속성 리스트 $Attrs$, 즉 $\widetilde{U} = L_1, L_2, \ldots, L_d$이다. 각 A_i는 랜덤하게 $t_{U,i}, d_{U,i} \in_R Z_P$를 선택한다. 이렇게 계산되는 속성 비밀키 SK_U^i는 다음과 같다.

$$SK = \{ G_{i_j,k} = g^{\alpha_i} g^{Z_{i_j,k} d_{U,i}} y^{\frac{\beta+u}{t_{U,i}}}, L_{i_j,k} = g^{Z_{i_j,k} d_{U,i}}, R_i = g^{\frac{1}{t_{U,i}}}, R'_i = g^{\frac{\beta_i}{t_{U,i}}} \} \tag{4}$$

4) $Encrypt(M, \mathbb{W}) \rightarrow CT$

데이터 소유주는 자신이 암호화하고자 하는 메시지 $M \in G_T$ 에 접근 구조 $\mathbb{W}$를 적용하여 암호화한다. 생성되는 암호문 CT는 다음과 같다.

$$CT = \{ g^s, M(\prod_{i \in I} e(g,g)^{\alpha_i})^S, y^S, \prod_{i \in I} g^{Z_{i_j,k}(S_i)}, \prod_{i \in I} e(g^{Z_{i_j,k}}, g^{S_i})^S \} \tag{5}$$

5) $Decrypt(SK_U^i, CT) \rightarrow M$

CT는 접근 정책 내에 인가된 속성을 가지고 있는 주체들만이 복호화 할 수 있다. 속성에 따라 생성된 비밀키 SK를 가지고 복호화한다. 식은 다음과 같다.

$$\begin{aligned} & \frac{C_2 \cdot C^{2_{i_j,k}} \cdot e(\prod_{i \in 1} L_{i_j,k}, C_1) \cdot e(\prod_{i \in 1} R_i, C_3)^u}{e(C^1_{i_j,k}, C_1) \cdot e(\prod_{i \in 1} G_{i_j,k}, C_1)} \\ = & \frac{M(\prod_{i \in 1} e(g,g)^{\alpha_i})^S \cdot \prod_{i \in 1} e(g^{Z_{i_j,k}}, g^{S_i})^S \cdot e(\prod_{i \in 1} g^{Z_{i_j,k} d_{U,i}}, g^s)}{e(\prod_{i \in 1} g^{Z_{i_j,k} k^{\tilde{S}}}, g^S) \cdot e(\prod_{i \in 1} g^{\alpha_i} g^{Z_{i_j,k} d_{U,i}} y^{\frac{\beta_i+u}{t_{U,i}}}, g^S)} \\ & \cdot e\left(\prod_{i \in I} g^{\frac{\beta_i}{t_{U,i}}}, y^s\right) \cdot e\left(\prod_{i \in I} g^{\frac{1}{t_{U,i}}}, y^s\right)^u \\ = & M \end{aligned} \tag{6}$$

CP-ABE를 이용하여 저작물을 암호화하면 다음과 같은 장점이 있다. 우선 일대다 복호화를 지원하기 때문에, 한 쌍의 공개키 및 개인키를 생성할 필요가 없다. 또한 제안하고자 하는 모델에서의 이용 허락 동의는 시스템 사용자의 속성을 기반으로 제어할 수 있다. 이때 가장 많이 사용할 수 있는 속성으로써 사용자가 속한 플랫폼 ID, 연령층, 성별 등이 될 수 있는데 CP-ABE는 이러한 속성들을 이용하여 정밀한 접근 제어를 제공할 수 있다. 이를 제안 모델에 적용한 방법은 다음 장에서 다시 논의한다.

3. 제안 모델

본 장에서는 앞서 기술한 관련 연구 내용을 기반으로 마이데이터를 이용한 블록체인 저작권 관리 플랫폼에 대하여 논의한다. 제안 모델의 목적은 플랫폼을 통해 저작권 관리와 저작물 공유를 같이 수행할 수 있는 것으로 한다. 또한 저작권자는 1인 창작자들로 고려하였으며 이들이 보다 쉬운 방법으로 저작물 공유에 대한 제어를 할 수 있도록 한다. 크게 저작권 관리와 저작물 공유로 나누어 논한다.

3.1 저작권 관리

제안 모델의 참여 구성요소는 다음과 같이 크게 3가지로 나눌 수 있다.

1) 블록체인 기반 온라인 서비스 사업자(Blockchain based Online Service Provider, BOSP) : 저작물 데이터를 서비스하는 플랫폼 사업자 조직들로 마이데이터 모델에서 서비스를 제공하거나 받는 플랫폼들이 모두 해당된다[12]. 기존 플랫폼과는 달리 유통 이력 및 저작권 이용 동의와 같은 내용이 블록체인에 등록되어 네트워크에 참여하는 모든 노드들에게 공유가 되므로 위·변조와 같은 악의적인 행위를 할 수 없다. 이들은 저작권자의 데이터를 서비스할 때 반드시 저작권자의 동의(consent)가 이루어진 이후에 서로 데이터를 사용할 수 있다. 또한 이들은 저작권 이용 허락 여부를 판단하기 위한 사용자들의 속성(attribute)을 관리하고 저작물을 암호화 또는 복호화 할 수 있는 속성 비밀키를 발급할 수 있다.

2) 저작권자(Copyright Holder) : 저작권자는 창작에 대한 권리를 보호 받아야하는 데이터 주체이다. 저작권자들은 스마트 계약을 통해 자신들의 이용허락 조건, 즉 이용허락 동의를 블록체인에 등록함으로써 저작물과 저작권 데이터 및 데이터 이용 동의 허락 정보 및 동의 상태를 게시한다. 데이터를 직접 소유하고 있지 않아도 데이터에 대한 소유권과 정산 관련 권리를 주장 할 수 있다.

3) 소비자 (Data Consumer, End User) : 플랫폼이 제공하는 서비스를 통해 저작물을 공유하고 소비하고자 하는 여러 플랫폼에 분산된 다양한 사용자들이다. 이들은 거래하고자 하는 데이터를 플랫폼에서 검색한 다음, 해당 데이터를 서비스해주는 플랫폼의 피어에게 앞에서 논한 스마트 계약을 통하여 공유 요청을 한다. 해당 플랫폼에서 소비자가 저작물 이용 기록은 블록체인에 저장된다.

다음은 스마트 계약으로 변경할 수 있는 데이터 필드(field) 3가지에 대해 논의한다. 각 데이터 필드 중에서도 사용자의 계정 정보 데이터 필드가 핵심으로써 이용된다.

1) 사용자 계정 정보 : 블록체인 네트워크에서 사용자의 모든 신원은 마이데이터 계정을 기반으로 식별한다. 이 계정은 처음 사용자가 플랫폼에 가입할 때, 계정 *ID*(*Account ID*)를 부여받는데, 이는 고유한 값이다. 제안 모델에서 사용되는 CP-ABE에서 데이터를 암호화 하는데 필요한 속성 값을 계산하는데 신원 정보(Global ID)로써 활용된다.

2) 저작물 정보: 저작권자는 자신의 이름으로 여러 개의 저작물을 생성하고 배포할 수 있다. 저작물은 배포되기 전에 부여 받은 고유한 식별 번호 *License ID*와 실제 저작물의 위치 *location*, 해당 데이터의 메타데이터(*metadata*) 값이 포함되어 있다. 메타데이터 값을 포함시키는 이유는 사용자로 하여금 복호화 한 데이터와 블록체인 상에 게시된 데이터가 일치하는지 확인하기 위한 작업에 사용된다. 이용허락 받은 서비스 플랫폼 참여자 및 최종 사용자는 스마트 계약을 이용하여 해당 값을 요청할 수 있다.

3) 저작권자 동의 허락 정보: 저작권자는 자신이 가지고 있는 저작물 정보 내에 이용허락 정보를 매핑할 수 있다. 동의 버전(Version)과 동의 기록(Consent Record ID)및 원래의 저작권자가 배포한 저작물 ID가 포함된다[13]. 제안 모델에서는 간단히 동의

허락 사항을 사용 가능(Active), 불가능(Disabled), 철회(Withdraw)로 분류한다.

3.2 저작물 공유

실제 저작물을 저장할 때에는, 저작물 데이터에 대한 BOSP의 내부 변조를 방지하기 위하여 암호화를 먼저 수행한다. 이를 위해 블록체인을 기반으로 하는 분산 CP-ABE 기법을 사용할 수 있다.

실제 데이터는 AES와 같은 대칭 키 암호화 기법의 비밀키로 암호화되어있고 해당 비밀키, 즉 데이터 복호화 키를 CP-ABE를 이용하여 암호화한다. 이렇게 암호화된 데이터 복호화 키는 접근 정책을 만족하는 속성 집합을 가진 사용자만이 복호화 할 수 있다. 저작권자는 사용자의 속성에 기반하여 각 저작물 데이터에 대해 나이, 성별과 같은 정보들을 이용하여 접근 정책을 정의할 수 있다.

본 논문에서 사용하는 CP-ABE 기법은 AND와 OR 게이트를 지원하는 계층적인 트리 형태의 접근 구조를 적용할 수 있으며, 본 논문에서는 제안 모델의 타당성을 보여주기 위한 프로토타입(Prototype)의 구현을 단순화하기 위해 가장 간단한 형태의 접근 구조를 적용하여 보여준다. 접근 구조는 다음과 같다.

접근 구조를 위해 사용되는 속성은 사용자의 신원정보인 마이데이터 계정인 Account ID 값을 이용한다. AA는 해당 마이데이터 계정 ID 값을 $string$ 값으로 입력 받아, Z_p의 원소로 랜덤하게 매핑하는 해시 함수를 이용하여 속성 값을 만들어낸다. 사용되는 충돌 저항 해시 함수 H는 다음과 같이 나타낼 수 있다.

$$H: \{0,1\}^* \rightarrow Z_p \tag{7}$$

따라서 속성 값은 사용자의 마이데이터 계정 값 GID를 해시 함수로 처리한 $ID = H(GID)$를 이용한다.

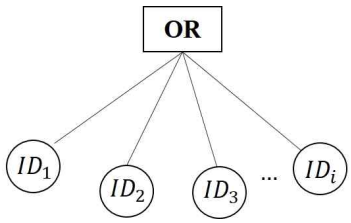

Fig. 1. An access structure tree used in proposed model.

일반적인 CP-ABE와는 다르게 블록체인을 기반으로 하는 다중 AA가 참여한다. 별도의 CA(Central Authority)를 두지 않고, 바로 블록체인 네트워크를 구성하는 각 플랫폼들이 AAs(Attribute Authorities) 역할을 수행한다. 다시 말해 전체 네트워크를 구성하는 플랫폼의 개수가 i 개일 때, i 개의 AA가 존재하는 것이다. 블록체인을 기반으로 한 CP-ABE 수행 단계는 다음과 같다. 각 단계를 수행하는 데 필요한 계산은 앞서 논한 식 (1)~(6)을 이용한다. 제안 모델에서는 [11]의 분산 CP-ABE 기법을 블록체인 기반의 모델로 개선하여 적용하며, 암호화와 복호화의 정확성과 안전성은 [11]과 동일하다.

1) $globalsetup(1^{\lambda}) \rightarrow PP = (g, y, e, p, G, G_T)$

이는 2.3절의 식(1)과 같은 과정을 따라 PP를 생성한다. 이때 생성된 PP는 블록체인 상에 공개한다.

2) $AuthoritySetup(\widetilde{A}_i, S_i) \rightarrow MSK, PK$

2.3절에서 $\widetilde{A}_i$는 i 번째 AA가 관리하는 속성 집합이라 명시하였다. 접근 구조에 필요한 속성을 ID 한 가지로 정의했기 때문에 $\widetilde{A}_i = \{ID\}$이다. 그리고 S_i는 각 플랫폼에 소속되어있는 사용자의 ID가 해당된다. 이를 이용하여 MSK, PK를 생성한다. 앞서 생성된 PP를 통해 이를 검증할 수 있다.

3) $KeyGen(MSK, Attrs) \rightarrow SK$

저작권자와 소비자는 자신이 소속된 플랫폼 사업자 즉 A_i에게 속성 비밀키의 생성을 요청한다. 이 비밀키는 블록체인의 스마트 계약으로 생성하기에는 무리가 있으므로 안전한 채널로 전달받을 필요가 있다. 속성 비밀키의 생성은 식 (4)와 같다. 각 AA는 하나의 집합, 사용자의 ID만을 속성 집합으로 가지고 있기 때문에 플랫폼 1번, 즉 AA_1이 관리하는 플랫폼의 사용자 속성키는 다음과 같다.

$$SK_U^1 = \{G_{1_j,k} = g^{\alpha_1} g^{Z_{1_j,k} d_{UA1}} y^{\frac{\beta_1 + u}{t_{UA1}}}, L_{1_j,k} = g^{Z_{1_j,k} d_{UA1}}, R_1 = g^{\frac{1}{t_{UA1}}}, R'_1 = g^{\frac{\beta_1}{t_{UA1}}}\} \tag{8}$$

(j : AA_1이 관리하는 ID집합, 위 상황에서는 1의 값을 가짐)

4) $Encrypt(PK, M, Access\ Policy)$, $CT = Encrypt(K, \ )$

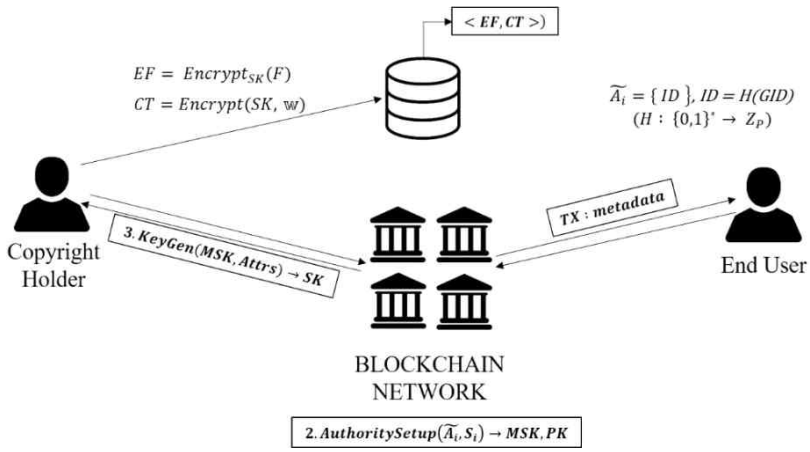

Fig. 2. Copyright data sharing with blockchain-based CP-ABE.

저작권자는 대칭키 K를 이용하여 데이터 F를 암호화한다. 암호화된 파일을 EF라고 할 때 $EF = Enc_K(F)$ 로 나타낼 수 있다. 그리고 데이터를 암호화는 데 사용한 대칭키 K를 접근정책 $\mathbb{W}$에 따라 CP-ABE로 암호화한다. 우선 저작권자는 랜덤한 값 S를 선택하여 K를 암호화하는데 사용한다.

$$CT = \{ C_1 = g^s, C_2 = K(\prod_{i\in I} e(g,g)^{\alpha_i})^S, C_3 = y^S, C_4 = \prod_{i\in I} g^{Z_{i,k}(S_i)}, C_5 = \prod_{i\in I} e(g^{Z_{i,k}}, g^{S_i})^S \} \quad (9)$$

그 후 암호화된 데이터 EF는 CT 값과 함께 외부 저장소에 저장한다. 후에 데이터 소비자들의 데이터 검증을 위하여 데이터의 메타데이터를 저장한다.

5) $Decrypt(CT,SK) \rightarrow K$

저작권자에게 이용 허락이 된 집합 U내의 사용자들만이 앞선 단계에서 생성된 속성 비밀키 SK_U^i 를 이용하여 복호화 할 수 있다. 복호화 식은 다음과 같다.

$$\begin{aligned} &\frac{C_2 \cdot C^{2_{i,k}} \cdot e(\prod_{i\in 1} L_{i,j,k}, C_1) \cdot e(\prod_{i\in 1} R_i, C_3)^u}{e(C^1_{i,j,k}, C_1) \cdot e(\prod_{i\in 1} G_{i,j,k}, C_1)} \\ &= \frac{K(\prod_{i\in 1} e(g,g)^{\alpha_i})^S \cdot \prod_{i\in 1} e(g^{Z_{i,k}}, g^{S_i})^S \cdot e(\prod_{i\in 1} g^{Z_{i,k} d_{U_i}}, g^s)}{e(\prod_{i\in 1} g^{Z_{p} k^{\hat{S}}}, g^S) \cdot e(\prod_{i\in 1} g^{\alpha_i} g^{Z_{i,k} d_{U_i}} y^{\frac{\beta_i + u}{t_{U_i}}}, g^S)} \\ &\cdot e\left(\prod_{i\in I} g^{\frac{\beta_i}{t_{U_i}}}, y^s\right) \cdot e\left(\prod_{i\in I} g^{\frac{1}{t_{U_i}}}, y^s\right)^u \quad (10) \\ &= K \end{aligned}$$

6) $Dec(K,EF) \rightarrow F$

해당 속성을 가진 사용자가 CT를 복호화하고 나면 데이터를 복호화할 수 있는 대칭키 K를 얻을 수 있다. K를 이용하여 EF를 복호화하면 원본 파일 F를 얻게 되는데, 이 F가 올바른 데이터인지에 대한 검증은 블록체인에 등록된 메타데이터를 검증함으로써 확인할 수 있다.

3.3 전체적인 프로세스

다음은 제안 플랫폼에서 수행되는 작업을 저작권 등록과 데이터 사용 요청으로 분류하여 논한다.

3.3.1 저작권자의 저작권 등록

1) 네트워크를 구성하는 피어는 BOSP이며, 이들은 서비스하는 플랫폼 사용자들에게는 AA(Attribute Authority)로서의 역할을 수행한다. 해당 플랫폼에 속한 클라이언트들의 GID(Global Id)를 바탕으로 속성 비밀키를 생성하여 사용자들에게 부여한다.

2) 저작권자는 저작권 정보, 이용허락 정보, 즉 저작물을 사용하기 위한 사용자의 속성 정보를 플랫폼의 프론트앤드(front-end)에 작성한다. 이 값은 트랜잭션으로 배포한다.

3) 또한 저작권자는 AES와 같은 대칭 키 암호화 알고리즘을 통하여 암호화된 저작물을 자신이 속한 BOSP의 데이터베이스에 저장한다.

4) BOSP는 사전에 정의된 저작물 이용허락 범위 내에서, 이용허락 동의가 된 다른 BOSP의 플랫폼으로의 데이터 공유가 가능하다.

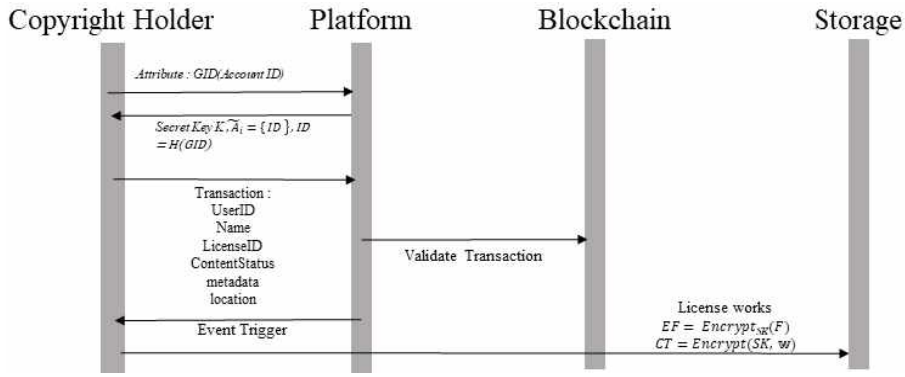

Fig. 3. Register copyright information in blockchain.

5) 저작물을 사용하는 데 있어서 자신이 가지고 있는 속성 비밀키로 저작물을 복호화 할 수 있는 사용자, 즉 접근 권한이 있는 사용자들은 이용허락 범위 내에서 2차 가공 또는 재배포할 수 있다.

6) 하나의 저작물이 공유되면, 해당 저작물에 대한 권리를 갖고 있는 저작권자 계정에 포함된다. 이로써 한 계정 정보에는 조직이 관리하는 블록체인 네트워크에 분산된 본인의 창작물 데이터 이용 기록이 저장될 수 있다.

3.3.2 소비자 또는 다른 저작권자의 저작물 데이터 사용 요청

1) 타 플랫폼에 소속된 사용자는 플랫폼에 접속하여 자신이 사용하고자 하는 저작물을 검색한다.

2) 저작물을 검색하고 사용하기 위해 자신의 User ID와 License ID를 입력하여 트랜잭션으로 배포한다.

3) 배포된 값은 블록체인에 등록되기 전 해당 ID가 검색된 저작물을 사용하기에 적합한지를 스마트 계약으로 검토한다. 입력받은 ID의 플랫폼 ID, 나이, 성별 등을 이용하여 사용하기에 적합하다고 판단이 된다면 저작권자에게 이용 이벤트를 알림(trigger)해준다. 또한 저작권자는 AES와 같은 대칭 키 암호화 알고리즘을 통하여 암호화된 저작물을 자신이 속한 BOSP의 데이터베이스에 저장한다.

4) 저작권자는 이를 판단하고 저작물을 암호화하는 데 사용하였던 비밀키 K를 사용자 속성, 즉 앞의 식 (7)에 의하여 계산된 ID를 포함하여 재암호화한다. 플랫폼은 작업이 완료되고 나면 사용자의 이용 동의가 완전히 이루어졌다고 판단하여, 앞서 사용자가 배포한 트랜잭션의 검증을 완료한 후 블록체인에 등록한다.

5) 사용자는 트랜잭션의 반환 값으로 데이터 저장 위치, 메타데이터, 암호화하는데 사용하는 키 K가 암호화된 CT 값을 얻는다. 자신의 속성 비밀키로 CT

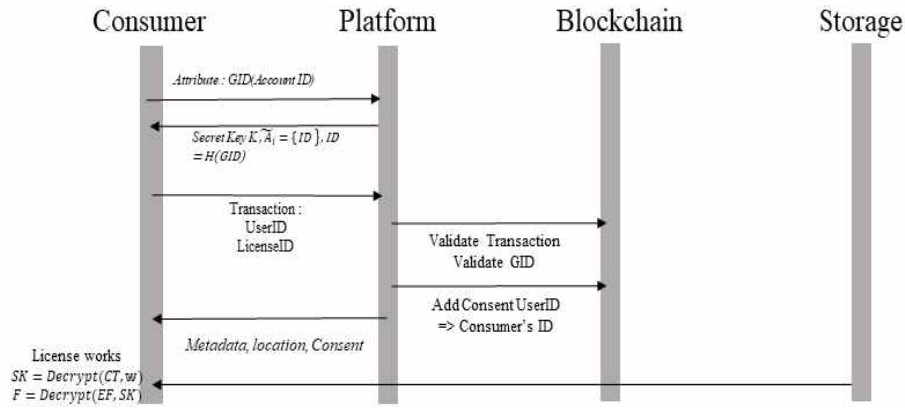

Fig. 4. Search for and request the use of the work.

를 복호화한 후 얻은 K로 저장 위치에서 파일을 읽어들일 수 있다. 그 후 메타데이터 값으로 자신이 얻은 데이터가 원본 데이터가 맞는지 확인할 수 있다.

6) 또한 저작물을 사용할 때에는 Active, Disabled, Withdraw와 같은 명시된 조건을 준수해야 한다. 저작물을 사용하기로 한 이후로 원 저작권자의 계정 정보 및 저작물 정보에 사용자의 ID와 저작물 이용 기록이 남아있기 때문에, 이를 위반할 시 추적이 가능하다.

4. 분석 및 평가

4.1 블록체인의 형태

본 모델은 저작물의 유통 플랫폼을 호스팅하는 온라인 서비스 사업자(OSP)가 블록체인의 피어(peer)가 되어 네트워크를 유지하고 관리한다. 사용자들은 플랫폼을 통해 조직의 피어에 접속함으로써 서비스를 이용할 수 있다.

네트워크에 클라이언트들로부터 생성된 트랜잭션이 발생하면 피어(Peer)들이 그에 대해 검증을 한다. 올바른 트랜잭션을 합의를 통해 채택하고 나면 블록에 포함되며 그 결과는 네트워크 내에 있는 노드 모두가 열람할 수 있다. OSP는 이미 상위 인증기관에 의해 인증된 참여자들이며, 이들의 신원은 이미 네트워크에 알려져 있으므로 신뢰관계 확보를 위한 채굴, 즉 작업 증명(PoW, Proof of Work)에서 사용하는 컴퓨팅 파워를 필요로 하지 않는다. 그리고 저작권 정보는 등록 시간 즉 타임스탬프 값(Timestamp)을 중요시한다. 또한 저작권 정보가 블록체인에 한번 잘못 등록되면 수정이 어렵기 때문에 브로드캐스트 전 시뮬레이션 과정이 필요하다. 브로드캐스트 후 분기가 발생할 것에 대해서도 고려를 해야 한다. 따라서 트랜잭션을 블록에 등록하기 전, 검증하는 과정이 필요하다. 따라서 최종성(finality)을 중요시하는 비잔틴 장애 허용 (Practical Byzantine Fault Tolerance, PBFT)과 같은 알고리즘을 이용하여 합의를 수행하는 것이 적합하다. PBFT는 네트워크 노드 1/3이하의 노드가 장애를 일으키더라도 전체 시스템의 합의를 이끌어낼 수 있는 알고리즘이다[14].

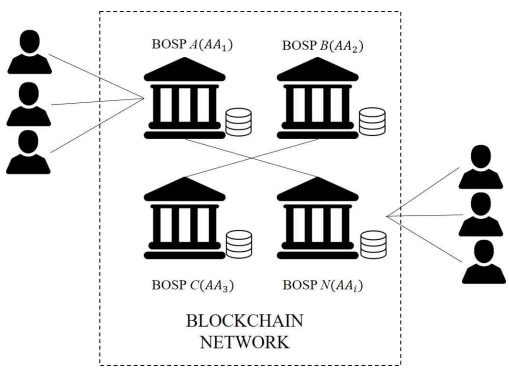

Fig. 5. Consoritum Blockchain.

따라서 [15]의 분류에 따라 본 모델을 구성하는 블록체인의 형태는 컨소시엄-허가형(Consoritum-Permissioned) 블록체인이다.

4.2 저작권 관리 시스템 비교 및 분석

1) 기존 중앙 집중형 구조 저작권 관리 모델과의 비교 분석

기존의 저작권 관리 모델은 OSP의 서버 및 데이터베이스에 저작물 이용 기록과 저작권 관련 정보를 저장해두고 이용하는 방식을 채택해왔다. 저작권자는 이들에게 위탁함으로써 자신의 저작물을 플랫폼 사용자들에게 쉽게 알림으로써 배포할 수 있었고, 사용자는 OSP가 제공하는 플랫폼에서 원하는 저작물을 검색하고 이용할 수 있었다. 앞서 논한 것과 같이 조직 중심의 클라이언트-서버 구조는 서버가 단일 실패 지점이 될 위험성이 높다. 또한 조직 내부의 악의적인 관리자가 자신들의 이익을 위하여 데이터 이용 로그를 위·변조할 수 있다는 단점이 존재하였다. 이를 보완하기 위한 방안으로써 제안된 블록체인 기반 저작권 관리 모델의 특성은 다음과 같다.

- 무결성(Integrity): 저작권 데이터의 등록 당시의 시간 값(Timestamp)와 저작권자 그리고 저작물 메타데이터(metadata) 값이 블록체인 상에 등록되면, 이 값은 블록체인의 특성으로 인하여 변경할 수 없다. 또한 저작물 데이터는 암호화된 상태로 외부 데이터베이스에 저장이 되기 때문에, 악의적인 위·변조를 방지할 수 있다.

- 불변성(Immutability): 블록체인을 구성하는 블록과 그에 포함된 트랜잭션들은 변경할 수 없다. 따라서 한번 저작권 데이터가 등록되면, 해당 데이터의 상태(state)가 변경될 수는 있어도, 그에 대한 기록(history)가 삭제되지는 않는다. 다시 말해, 저작권의 이용 동의 상태가 변경되어도 저작권이 존재 여부에

대한 과거 기록이 변경 또는 삭제되지는 않는다.

- 투명성(Transparency): 블록체인을 구성하는 노드들, 즉 읽기 권한이 있는 노드들은 네트워크에 배포되거나 등록된 트랜잭션들을 열람할 수 있다. 이들 모두가 트랜잭션을 실시간으로 열람할 수 있게 됨으로써, 악의적인 노드들이 임의로 트랜잭션 내부 입력(input) 또는 출력(output) 값을 변경하지 못하게 된다.

- 책임 추적성(Accountability): 블록체인 내에는 계정을 기반으로 자신의 모든 이용 및 데이터 요청 기록이 포함되어 있다. 이를 이용하여 이용자의 이용 위반 행위 추적이 가능하다.

위와 같이 저작권 관리 모델을 블록체인을 적용함으로써 얻는 이득은 다양하다. 특히 지금까지 연구된 블록체인 기반 저작권 및 저작물 공유시스템은 주로 중개자 없는 C2C 모델을 채택하였으며 관련 플랫폼이 많이 등장하였으나 기존 플랫폼과 호환이 되지 않거나 서비스를 하는 데 어려움을 겪는 등의 문제가 다수 존재했다.

2) 기존 블록체인 기반 저작권 관리 모델과의 비교 분석

이론적으로 C2C 모델은 가장 이상적인 저작권자와 소비자 간의 저작물 공유 시스템을 이룰 수 있다. 그러나 실제 저작권 관리 시스템은 신탁관리단체와 서비스 사업자와 같은 다양한 중개자들이 참여하며 이들을 완전히 배제하는 것은 현실적으로 불가능하다. 따라서 개개인의 사용자가 하나의 노드가 되는 것이 아닌, 조직이 노드가 되어 클라이언트 역할을 하는 사용자에게 블록체인 기반 서비스를 제공하는 모델도 연구되었다. 개인의 노드가 아닌 조직 중심의 네트워크를 이루는 관계로 모델의 현실성이나 확장성은 충족되었으나, 기록의 투명성은 다시 낮아지게 되었다.

또한 조직 중심의 블록체인 모델은 저작권자 개인이 스마트 계약을 적극적으로 설계하여 배포하는 점보다는 이미 배포된 저작권 정보에 대한 투명성 보장을 중요시하였다. 다시 말해 본래 서비스 플랫폼이 가지고 있던 데이터 이용 기록을 탈중앙화시켜 단일 실패 지점 위협을 낮추고, 단일 플랫폼 내에서의 위조를 방지하여 기록에 대한 부인 방지가 가능하다는 점을 중점으로 한다. 제안 모델은 투명성 제공을 포함하여 저작권자 개인이 조직들 간의 블록체인 네트워크에서 분산되어 있는 자신의 저작물 정보 기록을 모아 보다 적극적으로 관리할 수 있도록 마이데이터 개념을 적용하였다. 이렇게 함으로써 일부 탈중앙화 모델임에도 불구하고, 저작권자 중심의 저작권 관리 및 저작물 공유에 대한 이용 동의 허락 계약 관리를 수행할 수 있다[16].

Table 1은 기존의 중앙 집중형 구조의 저작권 관

Table 1. Comparison and analysis between the existing copyright management model and the blockchain-based copyright management model and the proposed model

	The existing copyright management	The blockchain-based copyright management model	The proposed model
Network Type	Client-Server	Blockchain-based P2P network	Blockchain-based P2P network
Treats	Server (Single Point of Failure)	Internal node or Concensus node	Consensus Node
Read (Assurance of transparency)	△ → Completely trust the information provided by the server	○ (Copyright Holder)	○ (Copyright Holder)
Write	△ → Difficult to change the recorded content directly	△ → Only Read(B2C)	○ → The copyright holder can create the conditions for use
Assurance of Integrity	×	○	○
Difficulty In Using Platform to User	Easy	Difficult(C2C) Easy(B2C)	Easy

Table 2. An analysis with Multi-Authority CP-ABE and Blockchain based CP-ABE

	Multi-Authority CP-ABE	Blockchain-based CP-ABE
Authority	CA[17] / distributed authority	decentralized authority
Key Issuer	CA	Consensus with AAs
Internal Threats	CA	AA(max : 1/3 of AAs in PBFT)

리 모델과 블록체인 저작권 관리 모델 그리고 제안 모델의 특징을 비교 분석한 결과를 나타낸다.

4.3 블록체인 기반 CP-ABE 분석

제안 모델은 블록체인 기반의 CP-ABE를 이용하여 암호화 된 키를 저작물 복호화 할 때 사용한다. 이는 기존의 분산된 다중 권한 기반 CP-ABE를 블록체인 형태에 맞게 사용한 것이다. 속성 권한을 나누어 관리하기 때문에 두 기법 모두 단일 실패 지점에 대한 위협이 낮다. 그리고 시스템에 존재하는 권한에 대하여 속성 비밀키 계산을 분산하여 수행하기 때문에, 과부하의 문제도 해결할 수 있다.

일반적인 분산 CP-ABE와의 다른 점에 대해서 논하자면 다음과 같다. 공개 파라미터 값 *PP*에 대하여 PBFT와 같은 합의 과정을 거친 후 결정하기 때문에, 분산된 권한 노드 중 일부의 악의적인 행위를 방지할 수 있다. 또한 블록체인에 속성키를 사용할 때 생성한 *PP* 값을 공개하기 때문에 사용자들로 하여금 마스터키 및 공개키에 대한 검증을 할 수 있도록 하게 한다. 각 속성 권한이 어떠한 속성을 관리하는 지에 대해서는 블록체인을 통해 투명하게 공개한다. Table 2는 CP-ABE 기법에 대해 비교 분석한 것이다.

제안 모델에서 CP-ABE가 가지는 의미는 다음과 같다. 우선 OSP 조직이 권한을 CP-ABE의 분산된 권한의 역할을 수행한다. 이들은 관리하고 있는 각 사용자의 계정에 대한 관리함과 동시에 이를 이용하여 속성 비밀키를 발급한다. 따라서 내부의 암호화를 위한 시스템만 구축하면 되기 때문에, 별도의 속성 권한을 구축하지 않아도 된다.

5. 결 론

본 논문에서는 마이데이터를 이용한 블록체인 기반 저작권 관리 모델을 제안하였다. 제안 모델을 통해 각 온라인 서비스 플랫폼에 분산되어 유통되고 있는 자신의 저작물을 마이데이터 계정과 이용 허락 동의를 기반으로 저작권 및 저작물 공유에 관한 모든 프로세스를 관리할 수 있을 것 이다. 이는 우선 기존의 중앙 집중형 구조의 저작권 관리 모델과는 다르게 블록체인 기술을 이용하여 데이터 관리 주체를 탈중앙화시킴으로써 저작권 관리에 대한 투명성을 재고한다. 또한 지금까지 연구 및 개발되었던 블록체인 기반의 저작권 관리 모델이 제안하였던 블록체인 기반 단일 플랫폼과도 차별화 되어있다.

본 논문에서 제안한 마이데이터 개념을 이용한 저작권 관리 모델이 시사하는 바는 다음과 같다. 창작자들이 생산해내는 저작물 데이터의 양은 굉장히 많아지고 그것을 다루는 온라인 서비스 플랫폼들이 많아지는데, 저작권자는 그러한 플랫폼들에 분산되어 있는 자신들의 데이터 관리를 일일이 할 수 없으며 그런 점을 악용한 저작권 침해사고가 발생하였다. 제안 모델은 플랫폼들 간의 블록체인 네트워크 형성 후 그를 기반으로 하는 마이데이터 계정을 이용하여 저작권자가 직접 데이터 사용 및 이용 동의 내용을 직접 설계함으로써 네트워크 내에 배포된 자신의 데이터를 관리할 수 있다. 그리고 사용자들에게 플랫폼을 대여하는 온라인 서비스 사업자들은 이들로 하여금 창작물을 재생, 게시 및 사용하도록 해준다. 이러한 플랫폼을 사용하게 함으로써 저작권자들의 권리를 보호하고 창작을 도모하여 저작물 산업계의 더 큰 가치를 창출하고 이들이 생성하는 창작물을 서비스하기 위해 더 개선된 플랫폼을 연구하고 개발할 수 있을 것으로 기대된다.

향후 모든 데이터 사용 흐름은 점차적으로 기업 또는 조직 중심의 관리가 아닌, 개인 중심으로 수행될 것이다. 개인이 생성해내는 모든 데이터들 중 하나로써 저작권 데이터도 마이데이터를 이용한 관리 모델이 개발된다면 조직들 사이에서 저작권자 중심의 저작권 관리 모델을 충실히 수행할 수 있을 것으

로 기대된다.

REFERENCE

[1] Copyright, https://en.wikipedia.org/wiki/Copyright (accessed January 08, 2020).

[2] Research on New Copyright Services Using Blockchain Technology, http://www.copyright.or.kr/information-materials/publication/research-report/view.do?brdctsno=42013 (accessed January 01, 2020).

[3] S. Bae, "Improved CRT-based Image Watermaking in DCT Domain for Copyright Protection," *Journal of Korea Multimedia Society,* Vol. 16, No. 10, pp. 1163-1170, 2013.

[4] A. Savelyev, "Copyright in the Blockchain Era: Promises and Challenges," C*omputer Law and Security Review,* Vol. 34, No. 3 pp. 550-561, 2018.

[5] A. Poikola, K. Kuikkaniemi, and H. Honko, "Mydata a Nordic Model for Human-centered Personal Data Management and Processing," Finnish Ministry of Transport and Communications, http://urn.fi/URN:ISBN:978-952- 243-455-5 (accessed January 01, 2020).

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceeding of 2017 IEEE International Congress on Big Data*, pp. 557-564, 2017.

[7] L.S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications," *Proceeding of 4th International Conference on Advanced Computing and Communication Systems*, pp. 1-5, 2017.

[8] A.M. Antonopolous, *The Blockchain*, Mastering Bitcoin, 2ed, O'Reilly Media, Inc., Sebastopol, California, 2017.

[9] V. Buterin, *A Next-generation Smart Contract and Decentralized Application Platform*, Ethereum White Paper, 2014.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attribute-based Encryption," *Proceeding of IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[11] Y. Zhang, J. Li, and H. Yan, "Constant Size Ciphertext Distributed CP-ABE Scheme With Privacy Protection and Fully Hiding Access Structure," *IEEE Access*, Vol. 7, pp. 47982-47990, 2019.

[12] My Data Docs, https://github.com/HIIT/ mydata-service-linking.pdf (accessed January 01, 2020).

[13] My Data Authz Docs, https://github. com/HIIT/mydata-stack/raw/gh-pages/mydata-data-authz.pdf (accessed January 01, 2020).

[14] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *Proceeding of the Third Symposium on Operating Systems Design and Implementation*, pp. 173-186, 1999.

[15] D.L.K Chuen and R.H. Deng, *Blockchain - From Public to Private*, Handbook of Blockchain Digital Finance and Inclusion, Volume 2, pp. 145-177, Academic Press, Cambridge, Massachusetts, 2017.

[16] B. Faber, G.C. Michelet, N. Weidmann, R.R. Mukkamala, and R. Vatrapu, "BPDIMS: A Blockchain-based Personal Data and Identity Management System," *Proceeding of the 52nd Hawaii International Conference on System Sciences*, pp. 1-10, 2019.

[17] Z. Liu, Z.L. Jiang, X. Wang, and S.M. Yiu, "Practical Attribute-based Encryption: Outsourcing Decryption, Attribute Revocation and Policy Updating," *Journal of Network and Computer Applications,* Vol. 108, pp. 112-123, 2018.

김 혜 빈

2018년 2월 부경대학교 IT융합응용학과 졸업(학사)
2018년 3월～현재 부경대학교 정보보호학협동과정 재학
관심분야 : 블록체인, 탈중앙형 서비스 모델 연구, 분산 네트워크 보안

신 원

1996년 2월 부경대학교 전자계산학과(학사)
1998년 2월 부경대학교 전자계산학과(석사)
2001년 8월 부경대학교 전자계산학과(박사)

2002년 3월～2005년 1월 ㈜안랩(구, ㈜안철수연구소) 선임연구원
2005년 3월～현재 동명대학교 정보보호학과 교수
관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식

신 상 욱

1995년 2월 부경대학교 전자계산학과(학사)
1997년 2월 부경대학교 전자계산학과(석사)
2000년 2월 부경대학교 전자계산학과(박사)

2000년 4월～2003년 8월 한국전자통신연구원 선임연구원
2003년 9월～현재 부경대학교 IT융합응용공학과 교수
관심분야 : 암호 프로토콜, 블록체인, 디지털 포렌식, IT융합보안