Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.3, Jun. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.3.513

수정 가능한 블록체인 기반 권한 변경 및 접근 제어 시스템*

이 연 주,[1†] 최 재 현,[1] 노 건 태,[2] 정 익 래[3‡]
[1,3]고려대학교 (대학원생, 교수), [2]서울사이버대학교 (교수)

Redactable Blockchain Based Authority Alteration and Accessn Control System*

Yeon Joo Lee,[1†] Jae Hyun Choi,[1] Geontae Noh,[2] Ik Rae Jeong[3‡]
[1,3]Korea University (Graduate student, Professor), [2]Seoul Cyber University (Professor)

요 약

블록체인의 불변성은 블록체인의 보안을 담당하는 주요 요인으로 데이터 무결성을 보장한다. 그러나 블록체인에 한 번 기록된 데이터에 대한 수정이 불가하다는 특성은 특정 사용자에 의해 악용될 여지가 존재한다. 실제로 비트코인 상에는 유해 데이터, 사용자 개인 데이터와 같이 블록체인에 기록되기에 부적절한 콘텐츠들이 노출되어 있다. 블록체인에 존재하는 부적절한 콘텐츠를 관리하는 방안으로는 G. Ateniese 등에 의해 처음으로 제안된 카멜레온 해시 기반 수정 가능한 블록체인이 존재한다. 수정 가능한 블록체인은 데이터 수정·삭제가 가능하다는 특성으로 GDPR의 잊힐 권리(right to be forgotten)를 충족하며, 최근 개인 데이터 관리에 관한 연구가 활발히 진행되고 있다. 그중 Y. Jia 등의 연구에서는 수정 가능한 블록체인 상에서 사용자 개인 데이터 관리가 가능한 모델을 제안하였으나 블록체인 참여 노드인 준 신뢰하는 규제자(semi-trusted regulator)가 블록체인에서 모든 블록에 대한 수정 권한과 트랜잭션 권한 박탈 등의 과도한 권한을 가지고 있어 부작용의 소지가 존재한다. 따라서 본 논문에서는 Y. Jia 등의 연구에서 규제자의 권한을 약화하고자 권한 주체 변경 및 권한 공유 방법을 제시하고 적용 가능한 시나리오를 토대로 수정 가능한 블록체인 기반 권한 변경 및 접근 제어 시스템 모델을 제안한다.

ABSTRACT

The immutability of blockchain is core elements of security of blockchain and guarantee data integrity. However, the characteristic that the data recoreded once in the blockchain cannot be modified has place for abuse by a specific user. In fact improper contents that is inappropriate to be recorded on the blockchain, such as harmful data and user personal data, is exposed on Bitcoin. As a way to manage improper content existing in the blockchain, there is a redactable blockchain using chameleon hash proposed for the first time by Ateniese. The redactable blockchain meet the right to be forgotten of GDPR by allowing data modification and deletion. Recently, Research on personal data management is being conducted in a redactable blockchain. Research by Jia et al. proposed a model that enables users to manage their personal data in the redactable blockchain. However, semi trusted regulators, which are blockchain participation nodes, have powerful authority in the blockchain, such as modification rights and deprivation of transaction rights for all blocks, which may cause side effects. In this paper, to weaken the authority of regulators in Y. Jia et al., we propose a method of authority subject altering and authority sharing, and propose a redactable blockchain-based authority change and access control system model based on applicable scenarios.

Keywords: Redactable Blockchain, Authority Alteration, Personal Data Management, Access Control, GDPR

Received(04. 04. 2022), Modified(05. 18. 2022), Accepted(05. 19. 2022)
* 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1F1A1060543).
† 주저자, lyjoo17@korea.ac.kr
‡ 교신저자, irjeong@korea.ac.kr(Corresponding author)

I. 서 론

블록체인 기술은 S. Nakamoto[1]의 비트코인으로부터 처음 제기된 개념으로 기존 중앙화된 시스템의 거래 방식을 탈피하여 시스템에 참여한 각 노드들이 분산원장을 유지함으로써 탈중앙성, 데이터 무결성 및 불변성을 보장한다. 이는 시스템 구성원들 간 PoW(Proof-of-Work), PoS(Proof-of-Stake)라는 합의 알고리즘을 사용하여 분산원장에 데이터를 기록함으로써 블록체인에서 사용자들의 독단적인 데이터 기록 및 수정이 불가하다는 보안상 이점을 가진다.

블록체인의 불변성은 분산된 시스템에서 데이터 무결성을 보장하고 블록체인의 보안에 중요한 역할을 한다. 그러나 이러한 특성은 유럽연합의 개인정보보호 법령(General Data Protection Regulation, GDPR)의 잊힐 권리(right to be forgotten)를 충족하지 못하며, 사용자에 의해 악용될 여지가 존재한다. R. Matzutt 등[2]의 연구에 따르면 비트코인 상에는 유해 데이터(아동 포르노, 음란사이트 링크, 악성코드 등), 개인 데이터(주소, 전화번호, 은행 계좌, 사진 등)와 같이 블록체인에 부적절한 콘텐츠가 기록되어 있다. 블록체인에 저장된 부적절한 콘텐츠는 블록체인을 사용하는 정직한 사용자들의 시스템 사용을 저해할 수 있다. 따라서 블록체인에 존재하는 부적절한 콘텐츠를 수정·삭제할 방안이 필요하다.

2017년 G. Ateniese 등[3]은 카멜레온 해시를 사용하여 수정·삭제가 가능한 수정 가능한 블록체인(Redactable Blockchain)을 처음으로 제안하였다. 수정 가능한 블록체인은 블록체인에서 데이터 수정이 가능하다는 특성으로 현재 IoT[4], 의료 시스템[5], 헬스케어[6], 스마트시티[7], 모바일 네트워크[8] 등 다양한 분야에서 데이터 수정 및 관리에 관한 연구가 활발히 진행되고 있다.

Y. Jia 등[9]의 연구에서는 수정 가능한 블록체인에서 사용자 개인 데이터를 관리하고자 취소 가능한 서브키를 가지는 상태 카멜레온 해시(stateful Chameleon Hash with Revocable Subkey, sCHRS)를 처음으로 제안하였다. Y. Jia 등에서 제안한 수정 가능한 블록체인 시스템 내부에는 준 신뢰하는 규제자(semi-trusted regulator)와 사용자(user)가 노드로써 참여하고 있다. 그러나 규제자는 블록체인에서 모든 블록을 수정할 수 있고, 블록체인에 부적절한 콘텐츠를 기록하는 사용자의 트랜잭션 수정 권한을 박탈할 수 있으며, 사용자의 키 쌍을 생성할 수 있는 등 블록체인에서 막강한 권한을 소유하고 있어 부작용의 소지가 존재한다. 블록체인에서 준 신뢰하는 규제자의 막강한 권한은 향후 시스템의 탈중앙화 속성을 잃게 된다는 문제를 발생시킬 우려가 존재하므로 개선할 필요가 있다.

본 논문에서는 수정 가능한 블록체인에서 사용자 트랜잭션 수정 권한을 변경·공유하고자 sCHRS를 변형한 변경 가능한 서브키를 가지는 상태 카멜레온 해시(stateful Chameleon Hash with Alterable Subkey, sCHAS)를 제안한다. 또한, Y. Jia 등에서 준 신뢰하는 규제자의 막강한 권한을 약화하고자 두 가지 방안을 제안하고, 그에 대한 적용 가능한 시나리오를 제시한다.

다음은 본 논문의 공헌이다.

- **Authority Alteration**: 사용자는 다른 사용자에게 자신의 트랜잭션 수정 권한을 변경·공유할 수 있으며, 준 신뢰하는 규제자는 블록체인에 부적절한 콘텐츠를 기록하는 악의적인 사용자의 트랜잭션 수정 권한을 회수하여 정직한 사용자에게 트랜잭션에 대한 수정 권한을 부여할 수 있다.
- **Hierarchical Structure of Blockchain**: 본 논문에서 제안하는 블록체인은 사용자의 해시값을 규제자가 다시 해시하는 이중 해시 구조를 취하고 있어 규제자와 사용자 간의 계층 구조를 가진다.
- **Management of Personal Data**: 사용자는 자신의 트랜잭션을 수정·삭제함으로써 자신의 개인 데이터를 직접 관리하고 개인 데이터에 대한 접근을 제어할 수 있다.
- **Protection of Blockchain Security**: 블록체인 거래에서 주소(in/output address), 거래 금액(amount) 등과 같이 변경되지 말아야 할 정보가 저장된 Standard Part(SP)와 사용자의 개인 데이터를 저장할 수 있는 Arbitrary Part(AP)를 서로 다른 해시함수를 이용하여 블록에 저장함으로써 블록체인을 보호할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 수정 가능한 블록체인의 관련 연구와 수정 가능한 블록체인의 주요 프리미티브인 카멜레온 해시함수와 수정 가능한 블록체인의 배경지식에 관하여 서술한다. 3장에서는 변경 가능한 서브키를 가지는 상태 카멜레온 해시를 소개하고, 4장에서는 규제자의 권한을 약

화한 두 가지 방안과 선행연구와의 비교 및 분석을 수행한다. 5장에서는 적용 가능한 시나리오에 대하여 제시하고 마지막 6장에서는 결론에 대해 논한다.

II. 배경지식

2.1 관련 연구

블록체인에서 데이터를 수정·삭제할 수 있는 방안으로는 G. Ateniese 등[3]의 연구에서 처음으로 제안한 카멜레온 해시 기반 수정 가능한 블록체인이 존재한다. [3]에서는 블록의 수정, 압축, 삽입이 가능한 블록체인 구조와 기존 카멜레온 해시의 키 노출 문제를 해결하고자 강화된 카멜레온 해시를 제안하였다. K. Huang 등[10]의 연구에서는 블록체인에 존재하는 부적절한 콘텐츠를 자동으로 삭제하고 트랩도어의 부정 사용을 방지하고자 단기 트랩도어 기반 셀프 수정 가능한 블록체인을 제안하였다. 단기 트랩도어를 받은 사용자는 블록체인에 존재하는 부적절한 콘텐츠를 수정·삭제함으로써 블록체인에 존재하는 부적절한 콘텐츠를 제거할 수 있다. 이외 IoT, 모바일 네트워크 등의 개인 데이터를 활용하는 다양한 분야에서 수정 가능한 블록체인을 사용한 연구는 활발히 수행되고 있다[4, 8].

H. Precht와 J. Marx Gómez 등[11]의 연구, 정성수 등[12]의 연구, 임준호 등[13]의 연구에서는 블록체인에서 카멜레온 해시를 사용하여 GDPR 준수 가능한 블록체인을 제안하였다. H. Precht와 J. Marx Gómez 등[11]의 연구에서는 국제 무역에서 사용되는 선하 증권의 디지털화를 목표로 블록체인에서 GDPR과 같은 법적 쟁점들을 만족하는 모델을 제안하였다. 정성수 등[12]의 연구에서는 최근 GDPR과 같은 개인 데이터를 관리하는 법령이 제정되어 있지만, 데이터의 개인 정보 처리 요청 기록에 관한 신뢰성과 무결성을 보장할 수 있는 방법은 존재하지 않아 실제로 블록체인에 적용하기엔 한계가 존재한다고 지적하였다. 이에 정성수 등의 연구에서는 개인 데이터 처리 요청에 관한 신뢰성을 보장하고자 블록체인에 저장된 개인 데이터를 다른 사용자에게 위임하여 처리할 수 있는 공증 프레임워크를 제안하였다. 임준호 등[13]의 연구에서는 카멜레온 해시와 속성기반 암호화를 활용하여 정보 주체의 권리를 보장할 수 있는 GDPR 준수 가능한 다중 블록체인 기반 접근 제어 시스템을 제안하였다. 사용자는 TA(Trusted Authority)와 컨트롤러에 의해 속성 기반 암호 키 쌍을 부여받아 블록체인에 개인 데이터를 기록할 수 있다. 사용자 개인 데이터 암호문과 암호화키는 서로 다른 체인에 저장하여 다른 사용자에게 암호화키가 저장된 블록을 알려줌으로써 개인 데이터에 대한 접근 제어를 수행할 수 있다.

2.2 카멜레온 해시(Chameleon Hash)

카멜레온 해시는 트랩도어의 유무에 따라 일반적인 암호학적 해시처럼 동작하거나, 인가된 사용자에 한해 해시값을 유지하면서 메시지를 변경할 수 있다. 이는 암호학적 해시함수 특징인 충돌 저항성(Collision Resistance)을 만족하며, 트랩도어를 가진 사용자는 카멜레온 해시의 충돌쌍을 쉽게 찾을 수 있다. 기존 카멜레온 해시 정의는 다음 5개의 알고리즘으로 구성되어 있다.

$CH = (ParGen_{CH}, KeyGen_{CH}, Hash_{CH}, HCol_{CH}, HCheck_{CH})$:

- $pp_{CH} \xleftarrow{\$} ParGen_{CH}(1^{\lambda})$: 파라미터 생성 알고리즘으로 보안 파라미터 λ를 입력받아 파라미터 pp_{CH}를 출력한다.
- $(sk_{CH}, pk_{CH}) \xleftarrow{\$} KeyGen_{CH}(pp_{CH})$: 키 생성 알고리즘으로 파라미터 pp_{CH}를 입력받아 개인키와 공개키 쌍 (sk_{CH}, pk_{CH})를 출력한다.
- $(h,r) \xleftarrow{\$} Hash_{CH}(pk_{CH}, m)$: 해시 알고리즘으로 공개키 pk_{CH}와 메시지 m $(m \in M)$를 입력받아 해시값 h와 난수 r를 출력한다.
- $r' \xleftarrow{\$} HCol_{CH}(sk_{CH}, (h,r,m), m')$: 충돌쌍을 찾는 알고리즘으로 개인키 sk_{CH}와 이전 해시 h와 난수 r, 이전 메시지 m과 새로운 메시지 m'을 입력받아 새로운 난수 r'를 출력한다.
- $\{0,1\} \leftarrow HCheck(pk_{CH}, (h,r,m))$: 검증 알고리즘으로 공개키 pk_{CH}와 해시값 h, 난수 r, 메시지 m을 입력받는다. 만약 (h,r)이 m에 대한 정당한 해시와 난수 쌍을 가질 경우, 1을 출력하고 아닌 경우 0을 출력한다.

2.3 수정 가능한 블록체인(Redactable Blockchain)

2017년, G. Ateneise 등[3]의 연구에서는 카멜레온 해시의 트랩도어를 다른 사용자에게 양도할 수 없다는 속성으로 인한 트랩도어 키 노출 문제[14]를 해결하기 위하여 다중 트랩도어의 강화된 카멜레온 해시를 제안하였다. Fig. 1.은 [3]에서 처음으로 제안한 카멜레온 해시 기반 수정 가능한 블록체인의 기본 구조로 각 블록은 블록의 헤더 해시값 s'과 이전 블록의 헤더 해시값 s, 트랜잭션 해시값 x, 넌스 ctr, 카멜레온 해시가 사용하는 난수 r로 구성되어 있다.

Fig. 1.의 구조처럼 트랩도어를 소유한 권한 있는 사용자는 카멜레온 해시를 사용하여 블록 B의 해시값 $Head(B) := < s,x,ctr >$을 유지한 가운데 난수 r을 조정함으로써 데이터를 수정할 수 있다. 따라서 수정 가능한 블록체인은 블록체인의 블록 간 연결성을 유지한 채 블록의 데이터를 수정할 수 있다.

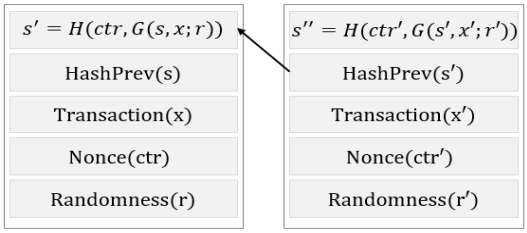

Fig. 1. The formal structure of redactable blockchain

III. 변경 가능한 서브키를 가지는 상태 카멜레온 해시

본 논문에서는 수정 가능한 블록체인에서 트랜잭션에 대한 접근 제어를 수행할 수 있는 사용자와 사용자의 요청에 따라 트랜잭션 권한을 다른 사용자로 변경하거나 블록체인에 악의적인 사용자가 존재할 시 악의적인 사용자의 권한을 회수하는 준 신뢰하는 규제자가 블록체인에 노드로써 공존함을 목표로 한다. 사용자와 규제자는 변경 가능한 상태 카멜레온 해시(stateful Chameleon Hash with Alterable Subkey, sCHAS)의 $HCol_{sCHAS}$을 사용하여 트랜잭션의 충돌쌍을 쉽게 찾을 수 있으며, 준 신뢰하는 규제자는 $HAlter_{sCHAS}$을 사용함으로써 트랜잭션 권한 주체를 변경·공유할 수 있다.

3.1 Notation

이번 장에서는 Table 1.을 통해 논문에서 사용하는 표기를 정리한다.

Table 1. Notation

Notation	
m	Message
pp	Public parameter
rsk_{sCHAS} / rpk_{sCHAS}	Semi-trusted regulator's private/ public key pair used in blockchain
usk_i / upk_i	i'th user's private/public key pair used in blockchain
r	Randomness
st_j	Stateful of transaction
id	Transaction number
σ_i	Original signature of transaction in the auxiliary set
σ_i^*	Signature of user/regulator on the alteration transaction
σ_i^{**}	Signature of regulator on the withdraw transaction
CH	Chameleon hash function
$sCHAS$	stateful Chameleon Hash with Alterable Subkey function
AP	Arbitrary part of transaction
SP	Standard part of transaction

3.2 sCHAS 구조

변경 가능한 서브키를 가지는 상태 카멜레온 해시는 다음 7개의 알고리즘으로 구성되어 있다.

$sCHAS = (ParGen_{sCHAS}, RKGen_{sCHAS}, UKGen_{sCHAS}, Hash_{sCHAS}, HCol_{sCHAS}, HAlter_{sCHAS}, HCheck_{sCHAS})$:

- $pp_{sCHAS} \xleftarrow{\$} ParGen_{sCHAS}(1^\lambda)$: 파라미터 생성 알고리즘으로 보안 파라미터 λ를 입력받아 파라미터 pp_{sCHAS}를 출력한다.

- $(rsk_{sCHAS}, rpk_{sCHAS}) \xleftarrow{\$} RKGen_{sCHAS}(pp_{sCHAS})$: 규제자의 키 생성 알고리즘으로 파라미터 pp_{sCHAS}를 입력받아 규제자의 개인키와 공개키 쌍인 $(rsk_{sCHAS}, rpk_{sCHAS})$를 출력한다.
- $(usk_i, upk_i) \xleftarrow{\$} UKGen_{sCHAS}(pp_{sCHAS})$: 사용자의 키 생성 알고리즘으로 파라미터 pp_{sCHAS}를 입력받아 사용자의 개인키와 공개키 쌍인 (usk_i, upk_i)를 출력한다.
- $(h, r, st_j) \xleftarrow{\$} Hash_{sCHAS}(rpk_{sCHAS}, upk_i, m)$: 해시 알고리즘으로 규제자와 사용자의 공개키 rpk_{sCHAS}, upk_i와 메시지 m $(m \in M)$를 입력받아 해시값 h와 해시에 대한 난수 r, 해당 블록을 생성한 사용자의 공개키를 저장하는 상태 st_j를 출력한다.
- $r' \xleftarrow{\$} HCol_{sCHAS}(sk, (h, r, m, upk_i), m')$: 충돌쌍을 찾는 알고리즘으로 규제자 또는 사용자의 개인키 $sk(rsk_{sCHAS}$ or $usk_i)$와 이전 해시 h, 난수 r, 이전 메시지 m, 해당 블록을 생성한 사용자의 공개키 upk_i와 새로운 메시지 m' $(m' \neq m)$을 입력받아 새로운 난수 r'를 출력한다.
- $(r', st_{j+1}) \xleftarrow{\$} HAlter_{sCHAS}(rsk_{sCHAS}, (h, r, m, upk_i), st_j, m')$: 사용자의 트랜잭션 권한을 변경·공유하는 알고리즘으로 규제자가 수행한다. 규제자의 개인키 rsk_{sCHAS}와 해당 블록의 해시 h, 난수 r, 메시지 m, 해당 트랜잭션 소유자의 공개키 upk_i와 블록의 상태 st_j와 새로운 메시지 m'를 입력받아 새로운 난수 r'와 업데이트된 상태 st_{j+1}를 출력한다.
- $b \leftarrow HCheck_{sCHAS}(rpk_{sCHAS}, h, st, (upk_i', r', m'))$: 검증 알고리즘으로 규제자의 공개키 rpk_{sCHAS}와 해시값 h, 해당 블록의 상태 st와 새로운 사용자의 공개키 upk_i', 난수 r', 메시지 m'을 입력받는다. 만약 (h, r', m')이 (usk_i', upk_i')에 대한 정당한 값일 경우 1을 출력하고 아닌 경우 0을 출력한다.

$(\mathbf{h}, \mathbf{r}, \mathbf{st_0}) \xleftarrow{\$} \mathbf{Hash_{sCHAS}(rpk_{sCHAS}, upk_i, m)}$:

$(h_2, r_2) \leftarrow \mathrm{Hash}_{CH_2}(\mathrm{upk_i}, \mathrm{m})$;
$\mathrm{st_0} = \mathrm{upk_i}$;
$(\mathrm{h_1}, \mathrm{r_1}) \leftarrow \mathrm{Hash}_{CH_1}(\mathrm{rpk_{sCHAS}}, \mathrm{h_2}||\mathrm{st_0})$;
return $(\mathrm{h}, \mathrm{r}, \mathrm{st_0}) = (\mathrm{h_1}, (\mathrm{r_1}, \mathrm{r_2}, \mathrm{h_2}), \mathrm{upk_i})$.

$\mathbf{r'} \xleftarrow{\$} \boldsymbol{HCol_{sCHAS}(sk, (h, r, m, upk_i), m')}$:

parse $\mathrm{h} = \mathrm{h_1}, \mathrm{r} = (\mathrm{r_1}, \mathrm{r_2}, \mathrm{h_2})$;
if $\mathrm{sk} = \mathrm{usk_i}$,
$\mathrm{r_2'} \leftarrow \mathrm{HCol}_{CH_2}(\mathrm{usk_i}, (\mathrm{h_2}, \mathrm{r_2}, \mathrm{m}), \mathrm{m'})$;
return $\mathrm{r'} = (\mathrm{r_1}, \mathrm{r_2'}, \mathrm{h_2})$.
if $\mathrm{sk} = \mathrm{rsk_{sCHAS}}$,
$(\mathrm{h_2'}, \mathrm{r_2'}) \leftarrow \mathrm{Hash}_{CH_2}(\mathrm{upk_i}, \mathrm{m'})$;
$\mathrm{r_1'} \leftarrow \mathrm{HCol}_{CH_1}(\mathrm{rsk_{sCHAS}}, (\mathrm{h_1}, \mathrm{r_1}, \mathrm{h_2}||\mathrm{upk_i}), \mathrm{h_2'}||\mathrm{upk_i})$;
return $\mathrm{r'} = (\mathrm{r_1'}, \mathrm{r_2'}, \mathrm{h_2'})$.

$\mathbf{(r', st_{j+1})} \xleftarrow{\$} \boldsymbol{HAlter_{sCHAS}(rsk_{sCHAS}, (h, r, m, upk_i), st_j, m')}$:

parse $\mathrm{h} = \mathrm{h_1}, \mathrm{r} = (\mathrm{r_1}, \mathrm{r_2}, \mathrm{h_2})$;
$(\mathrm{h_2'}, \mathrm{r_2'}) \leftarrow \mathrm{Hash}_{CH_2}(\mathrm{upk_k}, \mathrm{m'})$;
$\mathrm{st_{j+1}} = \mathrm{upk_k}$;
$\mathrm{r_1'} \leftarrow \mathrm{HCol}_{sCHAS}(\mathrm{rsk_{sCHAS}}, (\mathrm{h_1}, \mathrm{r_1}, \mathrm{h_2}||\mathrm{st_j}), \mathrm{h_2'}||\mathrm{st_{j+1}})$;
return $(\mathrm{r'}, \mathrm{st_{j+1}}) = ((\mathrm{r_1'}, \mathrm{r_2'}, \mathrm{h_2'}), upk_k)$.

$\boldsymbol{b \leftarrow HCheck_{sCHAS}(rpk_{sCHAS}, h, st, (upk_k, r', m'))}$:

if $\mathrm{st} \neq upk_k$, return 0;
else, parse $h = h_1$, $r' = (r_1', r_2', h_2')$;
$b_2 = HCheck_{CH_2}(upk_k, (h_2', r_2', m'))$;
$b_1 = HCheck_{CH_1}(rpk_{sCHAS}, (h_1, r_1', h_2'||st))$;
return $b_1 \wedge b_2$.

Fig. 2. The Black-Box construction of sCHAS

3.3 Black-Box 구조

Y. Jia 등의 연구에서 처음으로 제안한 취소 가능한 서브키를 가지는 상태 카멜레온 해시(stateful Chameleon Hash with Rovocable Subkey, sCHRS)는 블록체인에 부적절한 콘텐츠를 기록하는 악의적인 사용자의 트랜잭션 권한을 박탈하는 $Revoke_{sCHRS}$ 과정이 존재한다. 준 신뢰하는 규제자는 악의적인 사용자의 권한을 박탈함과 동시에 $UKGen_{sCHRS}$ 과정을 수행함으로써 사용자의 새로운 키 쌍을 생성할 수 있다. 규제자는 생성한 사용자의 키 쌍을 사용하여 박탈한 트랜잭션을 직접 관리하며 트랜잭션 권한이 박탈된 악의적인 사용자는 더이상 해당 트랜잭션의 충돌쌍을 계산할 수 없다. 블록체인에서 규제자의 $Revoke_{sCHRS}$ 과정이 증가함에 따라 블록체인에 규제자가 관리하는 트랜잭션의 개수는 증가한다. 이는 향후 시스템의 탈중앙화 속성을 잃게 된다는 문제를 발생시킬 우려가 존재한다.

따라서 본 논문에서는 Y. Jia 등의 연구에서 제안한 모델의 $Revoke_{sCHRS}$ 과정에서 발생하는 규제자의 권한 집중화 문제를 해결하고, 블록체인에서 준 신뢰하는 규제자의 권한을 약화한 프리미티브인

sCHAS를 제안한다. Fig. 2.는 sCHAS의 black-box 구조로 sCHAS 프리미티브의 세부단계를 정밀하게 나타낸 그림이다.

$ParGen_{sCHAS}$, $RKGen_{sCHAS}$, $UKGen_{sCHAS}$는 Y. Jia 등의 sCHRS와 동일한 구조를 따른다.

- $Hash_{sCHAS}$는 해시 알고리즘으로 규제자와 사용자의 공개키만을 필요로 한다. sCHAS는 규제자와 사용자의 이중 해시 구조를 가진다. 사용자는 h_2를 계산하기 위하여 CH_2를 규제자는 h_1을 계산하기 위하여 CH_1을 사용한다. 사용자가 해시한 (h_2,r_2)를 규제자가 다시 해시하여 (h_1,r_1)를 출력함으로써 규제자는 사용자를 관리할 수 있다.
- $HCol_{sCHAS}$은 해시의 충돌쌍을 찾는 알고리즘으로 규제자와 트랜잭션 소유자는 sCHAS를 사용하여 트랜잭션 해시의 충돌쌍을 쉽게 찾을 수 있다. 규제자의 경우 sCHAS의 이중 해시 구조를 따르기 위하여 st_j에 저장된 트랜잭션 소유자의 공개키로 변경된 메시지에 대한 (h_2',r_2')를 계산한 후 해시 충돌쌍을 찾을 수 있다.
- $HAlter_{sCHAS}$는 트랜잭션 권한 주체를 변경하는 알고리즘으로 트랜잭션 권한 주체 변경·공유과 권한회수 과정에 사용된다. 규제자는 사용자의 권한 변경·공유 요청을 통하여 (usk_k,upk_k) 키 쌍을 가지는 사용자로 트랜잭션 권한을 변경하며, 악의적인 사용자의 권한 회수 시 규제자의 키로 권한을 변경한다. 이때 st_{j+1}는 변경된 사용자의 공개키인 upk_k 또는 규제자의 공개키 rpk_{sCHAS}가 저장된다.
- $HCheck_{sCHRS}$는 검증 알고리즘으로 새로운 사용자 $User^*$에게 트랜잭션 권한 변경이 유효한지 확인한다. 만약 변경된 트랜잭션의 검증이 정상적일 경우 b는 1을, 아닐 경우 0을 출력한다.

IV. 권한 변경 및 접근 제어 시스템 구조

이번 장에서는 Y. Jia 등의 연구에서 준 신뢰하는 규제자의 막강한 권한을 약화하는 두 가지 방안을 제안한다.

4.1에서는 수정 가능한 블록체인 기반 블록체인 권한 변경 및 접근 제어 시스템의 구조를 보임으로써 트랜잭션 저장 형태와 블록 구조에 대하여 제시한다. 4.2에서는 트랜잭션의 수정·접근 권한을 소유하고 있는 사용자를 변경하는 트랜잭션 권한 주체 변경 방안에 관하여 제안하고, 4.3에서는 트랜잭션의 수정·접근 권한을 다른 사용자와 공유한 트랜잭션 권한 공유 방안에 관하여 제안한다. 마지막 4.4에서는 선행연구와 제안한 모델과의 비교 및 분석한다.

4.1 수정 가능한 블록체인 구조

블록체인의 불변성은 블록체인의 보안을 담당하는 주요 요인으로 한번 기록된 데이터에 대해 수정·삭제가 불가하다. 블록체인에서 기타 정보를 저장할 수 있는 부분으로는 "OP_RETURN"과 "coinbase"가 존재한다. "OP_RETURN"은 스크립트 조작코드로 공개키 스크립트 상에 기타 데이터를 저장할 수 있다. 이는 데이터베이스 상에 저장되지 않아 비트코인 거래 시 디지털 자산의 소유권 증명에 사용된다. "Coinbase"는 코인베이스 트랜잭션 상에서 마이너들이 적을 수 있는 부가 저장소이다. 본 논문에서는 블록체인에서 기타 데이터를 저장할 수 있는 부분을 Arbitrary Part(AP), 나머지 부분을 Standard Part(SP)로 칭한다.

Fig. 3.는 사용자 권한 변경 및 개인 데이터에 대한 접근 제어를 수행할 수 있는 수정 가능한 블록체인 구조이다. 블록 헤더 부분에는 이전 블록의 해시 값(prehash), 난수(nonce), 데이터 무결성을 검증할 수 있는 머클루트(merkleroot)가 있다. 블록 바디 부분에는 블록의 모든 트랜잭션이 저장된 트랜잭션 리스트(transaction list), 블록에 저장된 트랜잭션 메타 데이터를 담고 있는 보조 집합(auxiliary set) 부분이 존재한다.

본 시스템의 트랜잭션은 규제자의 카멜레온 해시로 해시하는 SP와 규제자와 사용자가 사용하는 sCHAS로 해시하는 AP로 나뉘어 저장된다. SP는 블록체인 보안을 담당하는 부분으로 입출력 주소, 양(amount) 등과 같이 블록체인 거래에서 변경되지 말아야 할 정보를 담고 있다. AP에는 해당 블록 사용자의 개인 데이터가 담긴 부분으로 트랜잭션을 소유한 사용자는 AP 부분을 직접 관리할 수 있다. 이외 보조 집합에는 트랜잭션의 난수, 초기 상태, 사용자의 공개키와 해시와 전자서명이 저장된다.

4.2절에서 다룰 트랜잭션 주체 권한 변경과 4.3절에서 다룰 권한 공유 모델에서 사용자는 자신의 트랜잭션의 권한을 다른 사용자로 변경 및 공유하고자

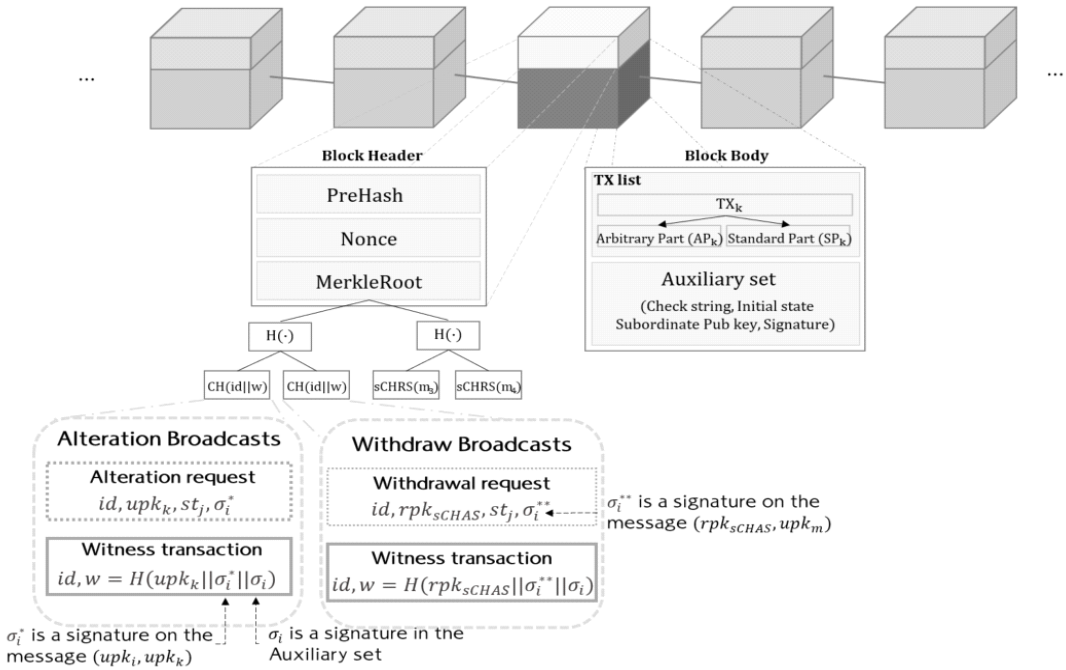

Fig. 3. The structure of redactable blockchain

트랜잭션 권한 변경·공유 트랜잭션을 생성해야 한다. 준 신뢰하는 규제자는 블록체인에 존재하는 악의적인 사용자의 트랜잭션 권한을 회수하고자 트랜잭션 권한 회수 트랜잭션을 생성해야 한다. 각 생성된 트랜잭션 내부에는 공개키와 서명이 저장된 Witness 정보 w가 포함되어 있으며, 마이너는 이후 트랜잭션 유효성 검증 과정을 수행함으로써 트랜잭션의 정당성을 판별한다.

트랜잭션 유효성 검증. 마이너들은 보조 집합에서 sCHAS의 해시값을 얻은 후 다음을 확인한다.

- 권한 변경·회수 요청에 포함된 $\sigma_i^*, \sigma_i^{**}$ 서명이 트랜잭션 제안자(사용자, 규제자)의 서명인지 확인한다.
- 트랜잭션 권한 주체 변경 시 사용자가 이전에 GDPR에 위반된 행위를 한 전과가 있는지 확인한다.
- w가 $upk_k \| \sigma_i^* \| \sigma_i$ 또는 $rpk_{sCHAS} \| \sigma_i^{**} \| \sigma_i$의 해시 값인지 확인한다.

트랜잭션 제안자(준 신뢰하는 규제자, 사용자)의 트랜잭션이 마이너의 트랜잭션 유효성 검증 항목을 모두 충족할 경우 마이너는 Witness 트랜잭션의 id와 w를 규제자만 수정할 수 있는 카멜레온 해시로 해시하여 머클루트에 상태가 변경되었음을 저장한다. 머클루트에 저장된 $CH(id \| w)$는 규제자만 수정할 수 있으며 변경된 상태 정보는 보조 집합에 업데이트 되어 저장된다.

4.2 권한 주체 변경

규제자의 권한을 약화한 첫 번째 방법인 트랜잭션 권한 주체 변경은 Fig. 4.와 같이 (a) 정직한 사용자 간의 트랜잭션 권한 변경 주체 방안과 (b) 블록체인에 부적절한 콘텐츠를 기록하는 악의적인 사용자의 권한회수 방안이 존재한다. 각 모델에는 준 신뢰하는 규제자, 트랜잭션을 관리하는 사용자, 트랜잭션 유효성을 검증하는 마이너(miner)가 존재한다.

(a)는 정직한 사용자 $User_1$이 $User_2$에게 자신의 트랜잭션에 대한 권한을 부여하는 과정으로 사용자 간의 트랜잭션 권한 주체 변경 과정을 나타낸다. 사용자는 변경·공유 요청(Alteration request)과 Witness 트랜잭션이 포함된 권한 변경·공유 요청 트랜잭션을 통해 규제자에게 권한 변경·공유를 요청할 수 있다. 변경·공유 요청은 트랜잭션의 일련번호

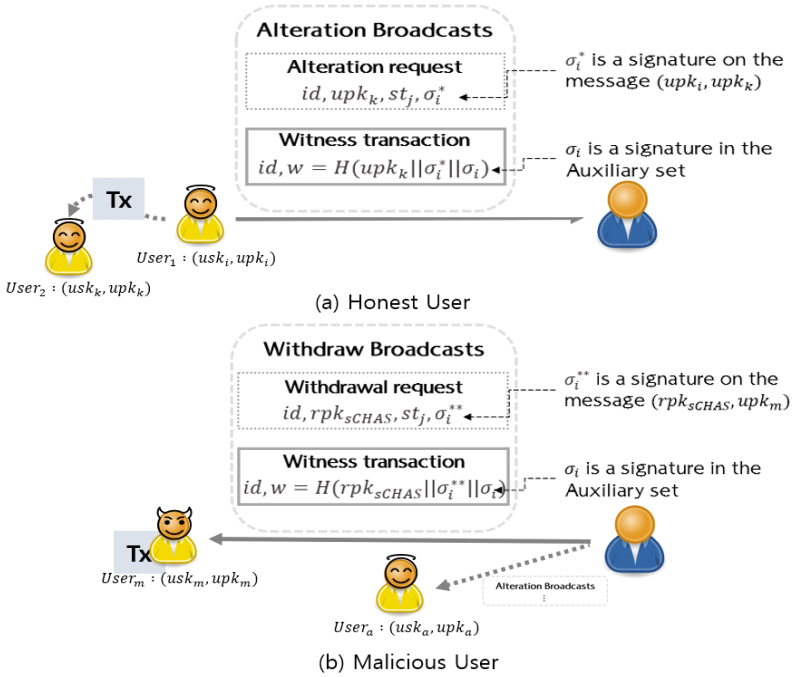

Fig. 4. Alter the subject of transaction authority

를 나타내는 id, $User_2$의 공개키 upk_k, 현재 트랜잭션 상태 st_j, $User_1$과 $User_2$의 공개키를 $User_1$의 서명키로 서명한 서명 σ_i^*이 포함되어 있다. σ_i^*는 향후 트랜잭션 유효성 검사 시 트랜잭션 권한 변경에 대한 $User_1$의 인증을 나타낸다. Witness 트랜잭션은 트랜잭션 id와 $User_2$의 공개키 upk_k, $User_1$의 트랜잭션 권한 변경 서명 σ_i^*, 트랜잭션의 본 서명인 σ_i을 해시한 Witness 정보 w가 포함되어 있다. 마이너는 $User_2$의 GDPR 범법행위로 인한 트랜잭션 권한회수 여부를 확인하고 정직한 사용자임이 증명될 시 트랜잭션 권한을 변경한다.

(b)는 블록체인에 부적절한 콘텐츠를 기록하는 악의적인 사용자의 권한을 회수하는 과정으로 준 신뢰하는 규제자가 수행한다. 규제자는 블록체인에 GDPR에 위반된 부적절한 콘텐츠를 기록하는 사용자 $User_m$의 트랜잭션 권한을 회수하고자 회수 요청(Withdrawal request)과 Witness 트랜잭션이 포함된 권한회수 요청 트랜잭션을 생성한다. 회수 요청은 트랜잭션 id, 규제자의 공개키 rpk_{sCHAS}, 현재 트랜잭션 상태 st_j, 규제자와 $User_m$의 공개키를 규제자의 서명키로 서명한 서명 σ_i^{**}이 포함되어 있다. σ_i^{**}는 향후 트랜잭션 유효성 검사 시 트랜잭션 권한 변경에 대한 $User_1$의 인증을 나타낸다. Witness 트랜잭션은 트랜잭션 id와 규제자의 공개키 rpk_{sCHAS}, 규제자의 트랜잭션 권한회수 서명 σ_i^{**}, 트랜잭션의 본 서명인 σ_i을 해시한 Witness 정보 w가 포함되어 있다. 규제자는 회수한 트랜잭션을 임시로 관리하며 트랜잭션을 소유하고 싶은 정직한 사용자 $User_a$가 존재할 경우 권한 변경·공유 요청 트랜잭션을 통해 트랜잭션 권한을 전달한다.

4.3 권한 공유

규제자의 권한을 약화한 두 번째 방법인 트랜잭션 권한 공유 모델은 시스템 환경에 따라 트랜잭션 권한을 공동으로 소유할 수 있는 사용자 수가 초기에 설정되어 있다. 본 논문에서는 두 명의 사용자가 트랜잭션을 관리할 수 있음을 보인다. Fig. 5.은 sCHAS의 트랜잭션 권한 공유 모델에 대한 black-box 구조로 두 명의 사용자가 트랜잭션을 관리할 수 있음을 보인다. 블록체인 참여 노드로는 준

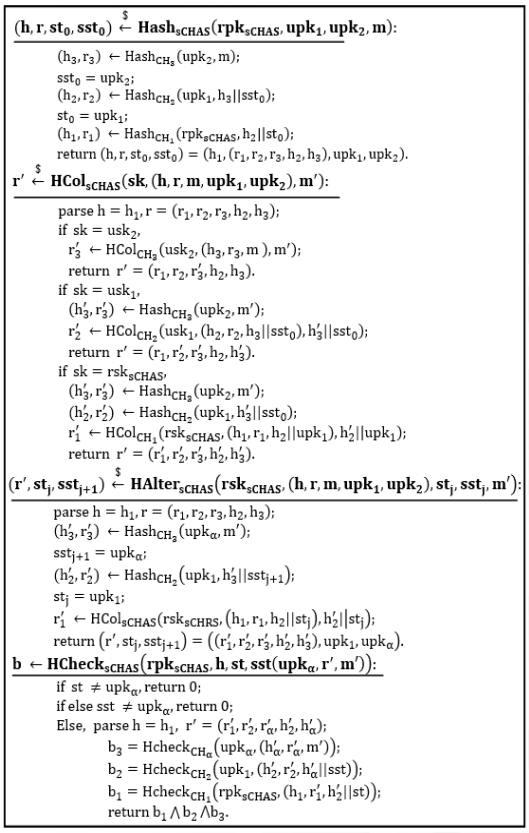

Fig. 5. The Black-Box construction of sCHAS (share the transaction authority)

신뢰하는 규제자, 트랜잭션을 관리하는 대표 소유자와 서브 소유자, 트랜잭션의 유효성을 검증하는 마이너가 존재한다.

- $Hash_{sCHAS}$는 해시 알고리즘으로 준 신뢰하는 규제자는 CH_1을 사용하여 (h_1,r_1)을 계산하고 트랜잭션 대표 소유자 $User_1$과 서브 소유자 $User_2$는 CH_2과 CH_3을 사용하여 (h_2,r_2), (h_3,r_3)을 계산한다. 해시 알고리즘의 출력값으로는 해시값 h와 해시에 대한 난수 r, 트랜잭션 대표 소유자와 서브 소유자의 공개키가 저장된 st_j와 sst_j가 존재한다.
- $HCol_{sCHAS}$은 해시의 충돌쌍을 찾는 알고리즘으로 트랜잭션 대표 소유자, 서브 소유자, 규제자는 sCHAS를 사용하여 충돌쌍을 찾을 수 있다.
- $HAlter_{sCHAS}$는 트랜잭션 권한 변경 알고리즘으로 트랜잭션 대표 소유자의 권한 주체 변경, 권한 공유 및 규제자의 권한회수에 사용된다. 이때, 트랜잭션 대표 소유자만이 서브 소유자를 변경할 수 있으며, 규제자는 악의적인 사용자의 권한회수 시 서브 소유자의 권한까지 모두 회수한다.

4.4 비교·분석

본 논문에서 제안하는 수정 가능한 블록체인 기반 권한 변경 및 개인 데이터 관리 모델은 기존 연구에서 준 신뢰하는 규제자 권한을 약화시킨 모델로 트랜잭션 권한 주체 변경과 권한 공유 방안이 존재한다. Table 2.은 권한 변경, 개인 데이터 관리, 접근 제어, 부인방지, 블록체인에서 제 3자(준 신뢰하는 규제자, 컨트롤러 등)가 소유한 권한 정도 및 GDPR 충족 조항들의 관점에 관하여 비교·분석한 표이다.

수정 가능한 블록체인은 3자의 존재 여부에 따라 두 가지 항목으로 분류된다. K. Huang 등[10]의 연구에서는 신뢰하는 3자가 없는 모델로 단기 트랩도어 기반 셀프 수정 가능한 블록체인을 제안하였다. 사용자는 자신의 트랜잭션을 임시로 수정할 수 있는 단기 트랩도어를 트랜잭션에 함께 저장함으로써 트랜잭션의 권한을 변경할 수 있으며 트랜잭션 변경 사항에 대한 서명을 통하여 악의적인 행동에 대한 부인방지 및 사용자의 인과성을 보장할 수 있다. 그러나 임준호 등[13]의 연구, Y. Jia 등[9]의 연구와 제안한 모델의 경우 블록체인에서 사용자의 속성기반 암호화(Attribute-based Encryption, ABE) 키를 부여하고 악의적인 사용자의 부적절한 콘텐츠를 탐지하는 등의 임무를 수행하는 (준)신뢰하는 3자가 존재한다.

임준호 등의 연구에서는 GDPR에 명시된 역할군으로 컨트롤러, 프로세서, TA(Trust Authority)가 참여하고 있다. 사용자의 개인 데이터는 역할군에 의해 블록체인에서 수집 및 관리되며 사용자는 자신의 개인 데이터를 열람할 수 있는 키값이 저장된 블록의 위치를 인가된 다른 사용자에게 전달함으로써 개인 데이터에 대한 접근을 통제 및 제어할 수 있다. 또한, 블록체인에 참여한 각 역할군은 수정된 데이터에 대한 계산값을 단계에 맞춰 전달함으로써 데이터의 기밀성과 무결성을 보장할 수 있으며 악의적인 사용자의 부적절한 콘텐츠 기록에 대한 부인을 방지할 수 있다.

본 논문에서 제안한 수정 가능한 블록체인 기반 권한 변경 및 접근 제어 시스템 모델은 개인 데이터

Table 2. Comparision between the proposed model and the existing studies

	Alteration of Rights	Management of Personal Data	Access Control	Non-repudiation	Third Party (Rights)	GDPR
[10]	△	×	×	○	No need	Art. 6, 16, 17
[13]	×	○	○	○	Trusted (High)	Art. 6, 16, 17, 18, 25
[9]	×	○	×	×	Semi-trusted (High)	Art. 6, 15, 16, 17
Ours	○	○	○	○	Semi-trusted (Middle)	Art. 6, 15, 16, 17, 18, 20

"△" : Rights can be temporarily altered.

관리가 가능한 블록체인 모델로 준 신뢰하는 규제자, 사용자, 마이너가 노드로써 참여하고 있다. 준 신뢰하는 규제자와 사용자는 sCHAS를 사용하여 트랜잭션을 관리할 수 있으며 권한 주체 변경 및 권한 공유 방법을 통하여 다른 사용자에게 권한을 변경·공유할 수 있다. Y. Jia 등의 연구와 다르게 제안한 모델은 사용자의 트랜잭션에 대한 통제권이 강화된 모델로 사용자는 다른 사용자들로부터 트랜잭션의 접근 제어 및 처리를 제한할 수 있으며 준 신뢰하는 규제자는 블록체인에 부적절한 콘텐츠를 기록하는 악의적인 사용자의 권한을 $HAlter_{sCHAS}$ 과정을 통하여 회수할 수 있다. $HAlter_{sCHAS}$ 과정은 블록에 저장된 공개키로부터 악의적인 규제자/사용자의 부적절한 행위를 부인방지할 수 있으며, Y. Jia 등의 $Revoke_{sCHRS}$ 과정으로부터 발생하는 문제를 해결한다.

K. Huang 등의 연구, 임준호 등의 연구, Y. Jia 등의 연구에서 제안한 모델은 수정 가능한 블록체인으로 블록체인에서 데이터 수정·삭제가 가능하다. 이는 GDPR 제6조 '처리의 적법성', 제16조 '정정권', 제17조 '삭제권'을 기본적으로 충족하며 제안한 모델에 따라 일부 다른 조항을 추가로 만족한다. 임준호 등의 연구에서 사용자는 컨트롤러에게 개인 데이터 이용 제한을 요청하고 컨트롤러는 사용자의 개인 데이터 보호 원칙을 이행하도록 기술 및 관리 조치를 요구한다. 이는 제18조 '처리제한권'과 제25조 '설계 및 기본설정에 의한 개인정보보호'를 추가로 충족한다. Y. Jia 등의 연구와 제안한 모델의 경우 사용자는 상태 카멜레온 해시를 사용하여 자신의 트랜잭션을 직접 관리함으로써 제15조 '개인 정보 주체의 열람권'을 충족한다. 제안한 모델은 트랜잭션 권한 주체 변경, 권한 공유 등 블록체인에서 사용자의 트랜잭션 통제권이 강화된 모델로 GDPR 제18조, 제20조 '개인 정보 이전권'을 추가로 충족한다.

V. 권한 변경 및 접근 제어 시스템과 응용

이번 장에서는 수정 가능한 블록체인 기반 권한 변경 및 접근 제어 시스템의 실제 적용 가능한 시나리오에 대하여 제시한다.

5.1 블록체인 기반 의료 데이터 관리 시스템

본 논문에서 제안한 트랜잭션 권한 주체 변경 모델은 병원에서 환자의 의료데이터를 관리하는 시스템에도 적용할 수 있다. 수정 가능한 블록체인 기반 의료데이터 관리 시스템의 참여 노드로는 준 신뢰하는 규제자인 병원과 블록체인 사용자인 의사, 환자가 존재한다. 의사는 자신이 담당하고 있는 환자의 의료데이터를 트랜잭션 형태로 관리한다. 트랜잭션은 블록체인 보안을 담당하는 부분, 환자의 기본 정보(이름, 나이, 성별, 주소 등)를 규제자인 병원만 수정할 수 있는 카멜레온 해시로 해시한 부분과, 환자 의료데이터 및 처방전 등을 규제자인 병원과 사용자인 의사 모두 수정할 수 있는 sCHAS로 해시한 부분으로 나누어 관리된다. 트랜잭션의 각 부분은 병원의 카멜레온 해시, sCHAS를 사용함으로써 데이터를 수정할 수 있는 주체가 분리되어 있다. 의사는 sCHAS를 사용하여 자신이 담당하는 환자의 의료데이터를 수정·삭제함으로써 관리할 수 있다.

수정 가능한 블록체인 기반 의료데이터 관리 시스템 상에서 의사가 소유한 환자 의료데이터 트랜잭션에 대한 권한이 변경되는 경우는 다음과 같다. 첫째, 주치의 휴진으로 인한 담당 환자의 응급 치료가 요구

될 경우, 병원은 응급환자에 대하여 일시적으로 다른 의사에게 트랜잭션 수정 및 접근 권한을 부여해 응급 치료를 이행한다. 이는 응급상황으로 인한 일시적인 권한 변경으로 환자의 응급 치료 완료 후 권한이 복구된다. 둘째, 의사의 소속 병원 이전으로 인한 환자 인수인계가 요구될 경우, 병원은 해당 의사가 담당하는 환자의 의료데이터 트랜잭션의 권한을 새로 들어온 의사로 변경한다. 새로 임명된 의사는 이전 주치의가 담당한 환자의 의료데이터 권한을 부여받아 진료를 이어갈 수 있다. 마지막, 환자의 요청으로 인한 주치의 변경이 요구될 경우, 병원은 다른 의사에게 환자의 의료데이터에 대한 수정 권한을 변경한다. 환자는 자신의 주치의를 선택·변경할 권리가 존재하여 병원으로부터 주치의 변경 요청을 제기할 수 있다.

이외 트랜잭션 권한 주체 변경 모델은 부동산 중개시스템 및 건물 위탁 관리 시스템, 사용자의 민감정보를 활용하는 IoT 시스템 등 다양한 분야에서 본 시스템을 적용할 수 있다.

5.2 블록체인 기반 OTT 계정 관리 시스템

본 논문에서 제안한 트랜잭션 권한 공유 모델은 OTT(Over-The-Top media service) 상에서 사용자 계정을 관리하는 시스템에도 적용할 수 있다. OTT는 인터넷을 통해 각종 미디어 콘텐츠를 제공하는 서비스로 현재 넷플릭스, 디지니 플러스, 애플티비 등 다양한 플랫폼이 구축되어 있다. OTT의 동시 접속 기기는 가족 구성원 또는 동거인에 한에서 한 계정당 2~6대로 제한을 두고 있으며, 일부 서비스는 프로필 잠금 기능을 제공한다.

수정 가능한 블록체인 기반 OTT 계정 관리 시스템의 참여 노드로는 준 신뢰하는 OTT와 서비스를 이용하는 사용자들이 존재한다. OTT는 시스템에 동시에 접속할 수 있는 인원수에 따라 각기 다른 블록체인 서비스를 운영하고 있으며, 사용자의 OTT 접속 권한 계정을 트랜잭션 형태로 관리한다. 사용자 계정 트랜잭션은 블록체인 보안을 담당하는 부분과 사용자 결제인증서를 OTT만 수정할 수 있는 카멜레온 해시로 해시한 부분과 결제인증서, 계정이 등록된 기기의 IP 주소를 OTT와 사용자 모두 수정할 수 있는 sCHAS로 해시한 부분으로 나누어 관리된다. 트랜잭션의 각 부분은 OTT의 카멜레온 해시와 sCHAS를 사용함으로써 데이터를 수정할 수 있는 주체가 분리되어 있다.

수정 가능한 블록체인 기반 OTT 계정 관리 시스템상에서 사용자는 자신의 OTT 이용 계정을 다른 사용자와 공유할 수 있다. 사용자는 공유된 트랜잭션의 데이터 필드에 접속기기의 IP를 등록함으로써 서비스를 사용할 수 있다. OTT는 부정적으로 서비스를 이용하는 사용자의 권한을 회수하여 서비스를 중지할 수 있다.

이외 트랜잭션 권한 공유 모델은 프로젝트 관리 시스템 및 계층 구조의 업무 시스템 등 다양한 분야에서 본 시스템 모델을 적용할 수 있다.

VI. 결 론

블록체인은 한 번 기록된 데이터에 대해 수정·삭제가 불가하여 데이터 무결성 및 불변성을 보장한다. 이러한 블록체인 성질은 잊힐 권리를 충족하지 못하며, 악의적인 사용자의 부적절한 콘텐츠 기록 현상으로 악이용될 여지가 존재한다. 블록체인에 기록된 부적절한 콘텐츠를 삭제할 방안으로는 수정 가능한 블록체인이 존재한다. 수정 가능한 블록체인은 블록체인에서 데이터 수정·삭제가 가능하다는 점에서 IoT, 의료 시스템 등 다양한 분야로 확대되어 연구되고 있다.

Y. Jia 등의 연구에서는 블록체인에서 사용자 개인 데이터 관리가 가능한 모델을 제안하였다. 그러나 준 신뢰하는 규제자는 블록체인에서 막강한 권한을 소유하고 있다는 문제가 존재하였고 이를 개선할 여지가 필요하다. 따라서 본 논문에서는 Y. Jia 등의 연구에서 규제자의 권한을 약화한 수정 가능한 블록체인 기반 권한 변경 및 접근 제어 시스템을 제안하였다. 제안된 트랜잭션 권한 주체 변경 및 권한 공유 방법은 기존 Y. Jia 등의 연구와 달리 규제자의 권한이 약화된 모델로 탈중앙화 속성이 증대되었으며 접근 제어 및 부인방지를 보장한다.

본 논문에서 제안한 두 가지 방법은 병원 의료데이터, OTT 등 다양한 분야로 확장되어 사용될 수 있다. 또한, 사용자는 변경 가능한 서브키를 가지는 상태 카멜레온 해시를 사용하여 개인 데이터 관리가 가능하다. 제안한 모델은 사용자의 트랜잭션 권한을 변경한다는 점에서 접근 제어와 부인방지를 보장하며 수정 가능한 블록체인의 기본 충족 요건인 GDPR의 '정정권', '삭제권' 이외에 '개인 정보 주체의 열람권', '처리제한권', '개인 정보 이전권' 등을 충족한다.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Decentralized Business Review, 2008.

[2] R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Müllmann, O. Hohlfeld and K. Wehrle, "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin," In International Conference on Financial Cryptography and Data Security, pp. 420-438, Feb. 2018.

[3] G. Ateniese, B. Magri, D. Venturi and E. Andrade, "Redactable blockchain -or- rewriting history in bitcoin and friends," 2017 IEEE European symposium on security and privacy (EuroS&P), pp. 111-126, April 2017.

[4] G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu and Y.J. Guo, "Enabling attribute revocation for fine-grained access control in blockchain -IoT systems," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1213-1230, Feb. 2020.

[5] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," In 2016 2nd international conference on open and big data (IEEE_OBD), pp. 25-30, August 2016.

[6] S. Angraal, H.M. Krumholz and W.L. Schulz, "Blockchain technology: applications in health care," Circulation: Cardiovascular quality and outcomes, vol. 10, no. 9, e003800, Sep. 2017.

[7] P.K. Sharma and J.H. Park, "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems, vol. 86, pp. 650-655, Sep. 2018.

[8] J. Xu, K. Xue, H. Tian, J. Hong, D.S. Wei and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," IEEE Transactions on Vehicular Technology vol. 69, no. 6, pp. 6688-6698, June 2020.

[9] Y. Jia, S.F. Sun, Y. Zhang, Z. Liu and D. Gu, "Redactable Blockchain Supporting Supervision and Self-Management," In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, pp. 844-858, May 2021.

[10] K. Huang, X. Zhang, Y. Mu, F. Rezaeibagha, X. Du and N. Guizani, "Achieving intelligent trust-layer for Internet-of-Things via self-redactable blockchain," IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2677-2686, April 2019.

[11] H. Precht and J.M. Gómez, "Redactable Blockchain-Leveraging Chameleon Hash Functions for a GDPR Compliant Blockchain," In Konferenzband zum Scientific Track der Blockchain Autumn School 2020, pp. 66-70, Dec. 2020.

[12] S.S. Jung, S.J. Lee and I.C. Euom, "Delegation-Based Personal Data Processing Request Notarization Framework for GDPR Based on Private Blockchain," Applied Sciences vol. 11, no. 22, pp. 10574, Nov. 2021.

[13] J.H. Lim, J.Y. Chun, G.T. Noh and I.R. Jeong, "GDPR Compliant Blockchain Based Access Control(GCBAC)," Journal of The Korea Institute of Information Security & Cryptology, 30(6), pp. 981-997, Dec. 2020.

[14] G. Ateniese and B. de Medeiros, "On the key exposure problem in chameleon hashes," In International Conference on Security in Communication Networks, pp. 165-179, Sep. 2004.

〈저자소개〉

이 연 주 (Yeon Joo Lee) 학생회원
2021년 2월: 백석대학교 ICT학부 정보보호학전공 졸업
2021년 3월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 블록체인, 프라이버시 향상 기술, 디지털포렌식

최 재 현 (Jae Hyun Choi) 학생회원
2019년 2월: 인천대학교 수학과 졸업
2021년 2월: 고려대학교 정보보호학과 석사
2021년 3월~현재: 고려대학교 정보보호학과 박사과정
〈관심분야〉 프라이버시 향상 기술, 블록체인

노 건 태 (Geontae Noh) 종신회원
2008년 2월: 고려대학교 산업시스템정보공학과 졸업
2010년 2월: 고려대학교 정보경영공학과 석사
2014년 8월: 고려대학교 정보보호학과 박사
2014년 9월~2017년 2월: 고려대학교 정보보호연구원 박사후 연구원, 연구교수
2017년 2월~현재: 서울사이버대학교 빅데이터·정보보호학과 조교수
2020년 3월~현재: 서울사이버대학교 빅데이터·AI센터 센터장
〈관심분야〉 암호 이론, 데이터 보안, 프라이버시 향상 기술

정 익 래 (Ik Rae Jeong) 종신회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 전산학과 석사
2004년 8월: 고려대학교 정보보호학과 박사
2006년 3월~2008년 2월: 한국전자통신연구원 암호기술연구팀 선임연구원
2008년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 이론, 프라이버시 향상 기술 (PET), 데이터베이스 보안, 생체인증