The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 5, pp.33-38, Oct. 31, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.5.33
JIIBC 2019-5-5

GDPR에 기반한 블록체인 프라이버시 강화 방안

A GDPR based Approach to Enhancing Blockchain Privacy

한세진[*], 김순태[**], 박수용[***]

Sejin Han[*], Suntae Kim[**], Sooyoung Park[***]

요 약 본 논문에서는 유럽연합의 개인정보 보호 규제인 GDPR을 준수하는 새로운 블록체인 모델을 제안한다. 제안하는 모델은 블록체인 거래에 포함된 개인정보에 대한 접근을 권한에 따라 차등적으로 통제하여 불법적인 개인정보 처리를 방지하는 한편, 보유기간이 경과된 또는 임의의 합법적 삭제 요청을 받은 개인정보에 대하여 접근을 영구히 차단하여 잊혀질 권리을 보장한다. 제안 모델의 핵심 메카니즘은, 개인정보를 접근정책에 따라 속성기반암호화한 후 이를 조회자의 속성(소속, 직무 등)을 반영한 일회용 토큰으로 복호화하는 것이다. 주목할 점은, 기존 기술이 제3의 신뢰기관을 필요로 하였다면 제안 모델은 신뢰기관 없이 블록체인에서 선발된 다수의 노드들로 하여금 그 기능을 대체하도록 하여 신뢰기관 리스크를 개선하였고, 아울러 속성 갱신에 따른 키 관리 효율성을 극대화하고자 복호키를 일회용 토큰으로 생성하였다는 점이다. 우리는 제안 모델을 허가형 블록체인인 패브릭의 체인코드를 이용하여 시뮬레이션 하고, 보안성을 분석함으로써 타당성을 입증하였다.

Abstract In this paper, we propose a new blockchain technology that could comply with GDPR. The proposed model can prevent illegal access by controlling access to the personal information according to a access policy. For example, it can control access to the information on a role-basis and information validation period. The core mechanism of the proposed model is to encrypt the personal information with public key which is associated with users attributes policy, and then decrypt it with a private key and users attributes based on a Attribute-based Encryption scheme. It can reduce a trusted third-part risk by replacing it with a number of nodes selected from the blockchain. And also the private key is generated in the form of one-time token to improve key management efficiency. We proved the feasibility by simulating the proposed model using the chaincode of the Hyperledger Fabric and evaluate the security.

Key Words : Access Control, Attribute-Based Encryption, Access tree, Blockchain, GDPR, Hyperledger Fabric, Personal Information, Public Key, Private Key, Right to be forgotten, Token, X.509

[*]준회원, 서강대학교 컴퓨터공학과
[**]준회원, 전북대학교 컴퓨터공학과
[***]비회원, 서강대학교 컴퓨터공학과
접수일자 2019년 8월 9일, 수정완료 2019년 9월 9일
게재확정일자 2019년 10월 4일

Received: 9 August, 2019 / Revised: 9 September, 2019 / Accepted: 4 October, 2019
[**]Corresponding Author: stkim@jbnu.ac.kr
Department of Software Engineering, ChonBuk National University, Korea.

Ⅰ. 서 론

유럽연합(EU : European Union)은 회원국 거주민에 대한 개인정보의 보호를 위하여 2018년 5월 25일부터 일반 정보보호 규정(GDPR : General Data Protection Regulation)을 시행하고 있다. 반면, 최근 4차 산업 기술로 각광 받고 있는 블록체인은 고유의 특징인 탈중앙화 및 분산원장의 구조로 인하여 개인정보 보호 의무를 준수하여야 할 중앙기관에 기반한 현행의 GDPR 규범 체계와 대부분 상충되고 있다. 예를들어 권한 또는 보유기간에 따른 접근통제가 어렵고 잊혀질 권리 보장이 되지 않으므로 블록체인이 현재의 GDPR 체계와 정합될 것인지에는 많은 논란의 여지가 존재한다.

기존 연구들은 공개형 블록체인의 탈중앙화 및 분산원장의 특성은 개인정보 규범상의 의무를 준수하고 책임을 부담하는 데이터 컨트롤러에 기반한 현재의 개인정보규범 체계와 충돌한다고 지적한다[1]. 특히 블록정보의 비가역성 및 참여자간 블록의 공유와 같은 특성은 개인정보 보호 법제의 삭제와 제3자 제공과 상충된다고 지적하고 기술적 대안 및 법제의 개정이 필요하다고 주장한다[2].

우리는 이에 블록체인이 GDPR 법리와 상충되는 부분을 분석하고 상호간의 합리적 접점을 찾아 GDPR을 준수하는 새로운 블록체인 모델을 개발하고자 한다. 제안하는 방식은 블록체인 거래에 포함된 개인정보를 접근정책에 따라 공개키로 암호화하고 해당 접근정책을 충족하는 속성을 지닌 이용자의 개인키로 복호화하는 개념이다. 이와 같은 암호기술은 불법적인 정보처리를 방지하는 한편, 정보 보유기간 경과후 접근을 차단하여 개인의 잊혀질 권리를 보장할 수 있다.

이하 나머지 절에서는 관련 기술 및 기존 연구를 살펴보고, GDPR의 원칙을 준수하는 새로운 블록체인 모델을 제안함과 아울러, 제안한 알고리즘을 하이퍼래저 패브릭상에서 시뮬레이션한 후, 성능 및 보안성 평가를 통해 타당성을 입증하도록 하겠다.

Ⅱ. 배경지식 및 관련 연구

1. 블록체인 기술

블록체인은 암호화폐인 비트코인을 구현하는 기반 기술로서 2008년에 처음으로 소개되었다[3]. 블록체인은 별도의 중앙기관이 존재하지 않는 피어-투-피어(Peer-to-Peer) 구조에서 가명의 계정을 사용하여 거래를 주고 받을 수 있는 혁신적 기술로 평가된다. 중앙기관이 존재하지 않아도 거래가 정상적으로 수행될 수 있는 것은 모든 데이터 기록이 각 노드에 동일하게 복제된 분산원장을 사용하기 때문이다. 분산원장은 블록체인의 핵심적인 기술로서, 일정 시간동안 모아진 거래의 집합인 블록들을 시간 순으로 나열한 것이며, 각 블록은 전후 블록의 해쉬값을 참조하는 형식으로 서로가 연결된다. 따라서 임의의 블록을 위변조하기 어렵다.

블록은 노드중에서 선발된 하나의 노드에 의하여 승인되어 블록체인에 추가된다. 노드 선발 과정은 예를들어 작업증명(Proof of work, POW)이라는 과정을 거치는데 이는 일방향 해쉬값에 대한 입력값을 알아내는 단순한 계산을 의미한다. 작업증명은 많은 전력을 소모하는 일이나, 작업증명에 성공한 노드는 이에 대한 보상(Incentive)으로 암호화폐를 제공 받는다. 보상은 곧 블록체인을 유지하는 원동력이 된다.

블록체인은 데이터 불변성, 탈중앙화의 고유의 특징으로 인하여 행정, 납세 등 각종 증명서를 발행하는 다양한 응용분야에 활용될 수 있고[4], 의료나 금융 분야처럼 정보의 무결성이 중요한 분야에서도 효과적으로 활용될 수 있다[5].

2. 블록체인 데이터 프라이버시 보호 기술

가. 속성기반암호화

속성기반암호화(ABE:Attribute-Based Encryption)는 데이터에 접근정책을 부여하고 이를 암호화 한 다음, 데이터 이용자가 동 접근정책을 충족하는 속성을 지닐 경우에 복호화를 허용하는 암호기술이다. ABE는 Sahai와 Waters에 의하여 2005년에 최초로 소개되었다[6]. 이들이 제안한 ABE는 암호화된 문서가 가지는 속성값들과 이용자가 가지는 속성이 임계치 k개 이상 일치하면 복호화가 가능한 특징을 가진다. 그러나 이 방식은 속성값들의 단순 갯수 비교라는 한계가 있기 때문에 다양한 접근정책의 표현이 어렵다는 문제가 있다. Goyal, Bethencourt 등은 이 점을 보완하여 속성들간의 관계를 논리연산(AND, OR)으로 표현한 접근트리를 제안한다[6][7]. 나아가 Bethencourt 등은 속성에 유효기간을 부여하여 기간이 만료된 속성을 철회하는 방안을 제시하였다. 한편, Chase 등은 ABE가 단일 신뢰기관에 의존하기 때문에 오라클이 될 수 있는 문제점을 해결하고자 다중 신뢰기관 모델을 제안한다. 이용자 속성을 다수의 신뢰기관이 나누어 관리하기 때문에 신뢰기관이 오라클이 되는

문제점을 해결한다[8]. 한편 Jamel 등은 신뢰기관 대신 블록체인을 활용한 모델을 제안하였다[9].

나. 오프체인

Aurelie 등은 오프체인을 이용하여 블록체인에서 잊혀질 권리를 보장하는 기법을 제안하였다[10]. 주요내용은, 민감한 개인정보를 블록체인 밖의 오프체인에 별도로 저장하여 이들을 삭제할 수 있도록 하는 것이나, 보안문제, 시스템 부하 집중문제가 존재한다.

다. 정보은닉

Goldwasser 등은 블록체인에 저장한 개인정보의 노출을 방지하기 위하여 영지식증명(ZKP:Zero-Knowledge Proof)을 활용하여 개인정보를 공개하지 않고도 업무를 처리할 수 있도록 하였다[11]. ZCash는 영지식증명을 이용한 대표적인 블록체인 송금기술으로서, 구매자의 계좌 잔액을 영지식증명하여 물건을 구매할 수 있다[12]. 한편, Cecchetti 등이 제안한 Solidus는 공개형 블록체인에서 트랜젝션의 계정 정보와 내역을 영지식증명하여 송금자를 은닉한 상태로 거래한다[13]. Van Wirdum은 동형암호(HE:Homomorphic Encryption) 기술과 영지식증명을 결합하여 Blockstream confidential asset을 제안하였다[14]. 동형암호는 어떤 값 a,b 를 동형함수를 통해 암호화 하면 두 대수 구조 사이의 연산이 암호문에서도 보존되는 특징을 갖는 암호기술로서, 정보를 노출하지 않고도 정보분석, 통계산출 등의 업무가 가능하다. Zyskind 등은 블록체인의 민감한 정보를 별도의 오프체인에서 안전한 다자간계산 프로토콜(SMC:Secure Multi-Party Computation)을 통해 처리하고 그 결과를 다시 블록체인에 기록하는 ENIGMA 프로토콜을 제안하였다[15][16]. Fabrice 등은 하이퍼래져 패브릭에서 다자간계산 프로토콜을 체인코드와 연동하여 처리하는 방식을 제안하였다[17].

Ⅲ. 블록체인과 GDPR의 정합성 분석

1. GDPR의 개인정보 처리 원칙

GDPR은 유럽 시민들의 개인정보 보호를 강화하기 위해 만든 통합 규정으로 적용 대상은 EU 시민의 데이터를 활용하는 일정 규모 이상의 개인정보 처리자이며 이들은 개인정보의 수집에서부터 처리까지 정보주체의 프라이버시를 보장하기 위한 원칙을 준수하여야 한다. 개인정보 처리원칙은 적법성, 공정성, 투명성, 목적 및 보유기간 제한, 최소처리, 정확성, 무결성, 기밀성, 책임성으로 구성된다.

가. 개인정보의 적법성, 공정성, 투명성, 최소처리(제6조제1항)

적법성은 개인정보 처리를 위해 동의서를 징구하거나 법적으로 처리가 필요한 경우인지 등을 확인하는 것을 의미한다. 투명성은 처리 과정이 명확하고 간결해야 함을 뜻하며 공정성은 불공평한 정보제공으로 인하여 정보주체의 거래에 불리함이 없어야 함을 뜻한다. 마지막으로 개인정보는 필요한 범위로 수집을 최소화하여야 하고 목적 외 수집을 해서는 안된다.

나. 개인정보의 무결성과 기밀성 보장(제20조제1~2항)

개인정보는 적절한 기술적·관리적 조치를 통하여 권한 없는 처리, 불법적 처리 등에 대비한 적절한 보안을 보장하여야 한다.

다. 개인정보의 정확성과 보유기간의 제한(제6조제1항)

정확성은 처리 목적상 부정확한 정보는 즉각 삭제되거나 정정되어야 함을 일컫는다. 보유기간의 제한은 필요한 경우에 한하여 보유하고 보유기간이 경과하면 삭제되어야 함을 의미한다. 참고로 GDPR의 삭제는 절대적 삭제가 아니고(GDPR전문 제65~66항) 정보의 링크를 삭제하는 것을 포괄하는 개념이다.

2. 블록체인의 GDPR 규제 정합성

블록체인에 포함된 모든 개인정보는 GDPR의 원칙에 따라 처리되어야 한다. 그러나 탈중앙화의 특징을 갖는 블록체인이 중앙화 구조를 전제로 하는 GDPR과 정합될 것인지에 대해서는 많은 논란이 존재한다. 비록 블록체인이 공정한 정보 접근성과 투명한 정보처리를 제공하나 다음과 같은 상충점이 존재한다.

가. 개인정보의 무결성과 기밀성 보장

블록체인은 근본적으로 모든 이용자가 투명하고 공정하게 정보에 접근할 수 있는 사상으로 설계되었기 때문에 특히 공개형 블록체인에서는 권한에 따른 세부적인 정보 처리 제한을 할 수 없다. 허가형 블록체인이라 하더라도 참여 노드의 권한 정도에 따라 정보를 차등적으로 접근할 수 있는 메커니즘은 설계에 반영되어 있지 않다.

나. 정확성과 보유기간의 제한

블록체인은 과거 블록의 내용을 조작할 수 없는 구조로 설계되었으므로 부정확한 정보가 발견되거나 보유기간이 지난 정보가 있더라도 이를 삭제 또는 정정할 수 없다.

Ⅲ. 설계 및 구현

1. 제안하는 블록체인 프레임워크

GDPR에 따른 블록체인 프라이버시를 강화하기 위하여 분산원장 기반의 개인정보 접근통제시스템(DPIACS : Distributed personal information access control system)을 제안한다. DPIACS는 개인정보를 접근권한 및 보유기간 정책과 연계하여 암호화하고 이용자의 속성(소속, 직급, 접근일자 등)에 따라 복호화하는 개념이다. 그림 1은 DPIACS가 블록체인의 거래 생성시 개인정보를 암호화하고 블록 조회시 이를 복호화하는 동작 절차를 나타낸다.

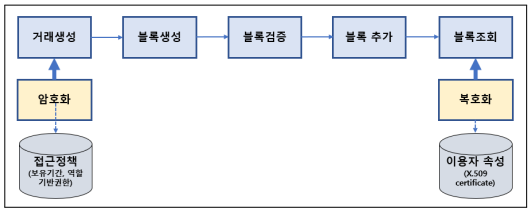

그림 1. DPIACS 동작 개요
Fig. 1. PDPIACS Flow

DPIACS는 다음과 같은 기능으로 구성된다.

(1) Blockchain Module : 거래를 생성하고 유효성을 검증한 후 블록에 추가하여 조회한다.

(2) Access Control Policy Module : GDPR에 따른 개인정보 접근정책(보유기간, 접근권한)을 정의한다.

(3) Cryptography Module : 개인정보를 암호화 하고, 정보이용자의 속성에 따라 복호화 한다.

2. DPIACS 알고리즘

DPIACS 알고리즘은 II.2절에서 설명한 Chase의 다중 신뢰기관 기반의 CP-ABE를 블록체인에 효과적으로 결합한 것으로서 Chase와 차별점은 (1)신뢰기관 대신 블록체인 다수 노드를 활용한다는 점, (2) 기존 기술이 공개키·개인키를 동시에 생성하는데 반해 공개키를 생성하고 이후 조회 요청시 개인키가 생성된다는 점이다. 한편, 개인키는 이용자 속성과 요청시각을 반영하여 생성되고 이용 후에는 폐기되는 일회용 토큰으로 발행되므로 키관리 부담이 감소한다. 다음은 DPIACS 알고리즘의 각 단계를 나타낸다.

표 1. 파라메터 정의
Table 1. parameters definition

파라메터	설명
p	매우 큰 소수
Z_p^*	법 p를 모듈로로 하는 승법군
g	Z_p^*의 생성자
e(g,g)	겹선형 함수
A_n	이용자 속성에 대한 전체 집합
T	접근트리
T_k	속성노드 k의 부분 접근트리
$q_{(k,x)}$	속성노드 K에 속한 부분트리 노드 x에 대한 다항식
s	임의의 $s \in Z_p^*$에 대하여 $s = q_{root(0)}$
i	$1 \le i \le n$, n은 전체 이용자 속성의 갯수
R_k, R_{ki}	임의의 R_k, $R_{ki} \in Z_p^*$
k	$1 \le k \le K$, K는 속성노드 갯수
att(x)	접근트리의 노드 x가 표현하는 이용자 속성
H	해쉬함수
α, β	중앙노드가 생성하는 마스터 비밀키

(1) 초기화

허가형 블록체인은 노드 중에서 1개의 중앙노드와 K개의 속성노드를 선정한다. 이 노드들은 신뢰기관 역할을 하며 Cryptography module과 관계된다.

(2) 키생성

중앙노드가 실행하는 알고리즘으로서, 시스템공개키1개와 속성노드 공개키 K개를 생성하고, 접근정책을 생성한 후, 각 속성노드에 접근정책을 분할하여 할당한다. 접근정책은 Access Control Policy Module의 핵심부분으로서, 속성과 논리연산자를 결합한 트리구조로 표현된다. 각 속성노드는 이 트리의 부분트리를 관리한다.

- 시스템 공개키 : $e(g,g)^{\alpha}, h = g^{\beta}$
- 속성노드 비밀키 : v_k

(3) 접근정책 암호문 생성

속성노드가 실행하는 알고리즘으로서, Cryptography Module에 해당한다. 속성노드 공개키를 이용하여 접근정책에 대한 암호문을 생성한다.

- 속성노드 공개키 : g^{v_k}

$$C_{k,i} = g^{v_k \cdot q_{k,i}(0)}, C'_{k,i} = H(att(k,i))^{q_{k,i}(0)}$$

(4) 개인정보 암호화

정보주체가 실행하는 알고리즘으로서, Cryptography Module에 해당한다. 시스템 공개키와 마스터 비밀키 등을 이용하여 개인정보 암호문을 생성한다.

- $C = h^s$, $C = M \cdot e(g,g)^{\alpha \cdot s}$
- Final Ciphertext : $E_{k,i} = (T, C, \tilde{C}, C_{k,i}, C'_{k,i})$

(5) 토큰생성 및 복호화

속성노드가 실행하는 알고리즘으로서, Cryptography Module을 이용하여 정보이용자(조회자)의 일회용 토큰을 생성한다.

$$D_k = g^{(\alpha + r_k)/\beta}, D_{k,i} = g^{r_k} \cdot H(k,i)^{r_{k,i}}, \; D'_{k,i} = g^{r_{k,i}}$$

정보이용자(조회자)는 암호문과 일회용 토큰을 이용하여 암호문을 복호화 한다.

$$Decrypt(E_{k,i}, D_{k,i}) = M$$

Ⅳ. 실험 및 평가

1. 제안모델 실험

DPIACS를 다음과 같이 의료산업을 예시로 패브릭 기반에서 시뮬레이션 하고자 한다.

(1) 접근정책 생성

개인정보 M은 감염내과 소속 간호사 이거나 또는 감염내과 소속 의사인 경우에 접근될 수 있으며 보유기간은 2019년 12월 31일까지이다. 이 경우 접근정책은 다음과 같이 표현된다.

((간호사 ∧ 감염내과) ∨ (의사 ∧ 감염내과)) ∧ 2019-12-31

(2) 개인정보 암호화

환자 개인정보를 (1)의 접근정책과 함께 DPIACS로 암호화 한다. 암호화된 개인정보를 변수 PersonalData에 저장한다.

(3) 체인코드 인스턴스 생성

노드에 체인코드를 설치하고 PersonalData를 이용하여 체인코드 인스턴스를 생성한다.

#chaincode instaniate -o orderer0:7050 -C ch1 -n example -v 1.0 -c '\{"Args": ["Init","PersonalData", "CT"]\}'\; -P "OR ('Org0MSP.member', 'Org1MSP.mmember')"}

(4) 조회 체인코드 생성

#chaincode instaniate -o orderer0:7050 -C ch1 -n\; example-v 1.0 -c '\{"Args": ["Init","Pe\#chaincode query -C ch1 -n -testnetCC -c '{"Args":["query", "PersonalData"]}' }

(5) 개인정보 복호화

DPIACS는 조회자의 속성(직책 : 의사, 소속 : 감염내과, 접근시각 : 2019년 1월 1일)을 반영하여 일회용 토큰을 발급한다. 발급된 토큰이 접근정책을 만족하므로 PersonalData의 값이 응용프로그램의 화면에 출력된다. 접근정책을 만족하지 않는다면 정보 조회가 차단된다.

2. 제안모델 평가

표 2는 DPIACS가 GDPR의 권한별 접근통제, 부정확한 정보의 삭제 그리고 보유기간 경과 후 삭제 등 요건을 충족하며, 유사 연구에 비해 많은 장점이 있음을 보여준다.

표 2. GDPR 요구사항 만족도 평가
Table 2. GDPR Compliance evaluation

	ours	ZKP	MPC	HP	Stealth Address
권한통제	O	O	O	O	X
정확성(삭제)	O	X	X	X	X
보유기간 통제	O	X	X	X	X

표 3은 DPIACS가 AES보다 키관리 효율성과 보안성이 높음을 보여준다.

표 3. 효율성 및 보안성 평가
Table 3. Efficiency and Security evaluation

	ours	Bethencourt	Jemel	Chase	S&W
속성변경유연성	O	X	O	X	X
오라클방지	O	X	X	O	X
키분실위험관리	O	X	O	X	X
계산량	C^n	C^n	C^n	C^n	C^n

Ⅴ. 결 론

본 논문에서 우리는 블록체인의 GDPR 준수 가능성을 알아보았다. 제안한 DPIACS는 개인정보를 접근정책으로 암호화하고 해당 접근정책을 충족하는 이용자만 복호화 할 수 있도록 하여 블록체인의 개인정보 보호를 실현한다. 신뢰기관 대신 블록체인 노드를 활용하여 비용, 보안 문제를 경감시켰고 복호키 대신 일회용 토큰을 사용하여 키관리 부담을 감소시킨 것은 기존 대비 차별점이라 할 수 있다. 향후 본 연구결과를 기반으로 블록체인 표준 개인정보 보호 프레임워크를 수립한다면 보다 많은 프로젝트가 이를 활용할 수 있을 것으로 기대한다.

References

[1] Dae-Hee Lee, “Personal Data Issues in Applying Blockchain Technologies”, Journal of Korea Information law, Vol.22 No.3, pp.244-272, 2018.

[2] Choi Yong Hyuk, “A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information”, The Korea Institute Of Information Security and Cryptography, 2018.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[4] https://proofofexistence.com

[5] https://www.ibm.com/blockchain/financial-services

[6] V.Goyal, O.Pandey, A.Sahai, and B.Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", ACM Conference on Computer and Communications Security, 2006. DOI: https://doi.org/10.1145/1180405.1180418

[7] J.Bethencourt, A.Sahai, B.Waters, “Cipher text-Policy Attribute-Based Encryption”, IEEE Symposium on Security and Privacy, 2007. DOI: https://doi.org/10.1109/SP.2007.11

[8] Melissa Chase, "Multi-authority attribute based encryption", Theory of Cryptography Conference, 2007. DOI: https://doi.org/10.1007/978-3-540-70936-7_28

[9] Mayssa Jemel, Ahmed Serhrouchni, “Decentralized access control mechanism with temporal dimension based on blockchain”, IEEE 14th International Conference on e-Business Engineering, 2017. DOI: https://doi.org/10.1109/ICEBE.2017.35

[10] Aurelie Bayle, Mirko Koscina, David Manset, Octavio Perez-Kempner, "When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry",2018 IEEE/WIC/ACM International Conference on Web Intelligence(WI), 2019. DOI: https://doi.org/10.1109/WI.2018.00133

[11] Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems", SIAM Journal on Computing, 1989. DOI: https://doi.org/10.1137/0218012

[12] https://z.cash/. Accessed August 2019.

[13] E. Cecchetti, F. Zhang, Y. Ji, A. E. Kosba, A. Juels, and E. Shi, “Solidus:Confidential distributed ledger transactions via PVORM", Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp.701-717. ACM, 2017. DOI: https://doi.org/10.1145/3133956.3134010

[14] A. van Wirdum, “confidential assets brings privacy to all blockchain assets: Blockstream", Bitcoin Magazine, 2017.

[15] AC Yao, "Protocols for secure computations", 23rd Annual symposium on foundations of computer science, 1982.

[16] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentralized computation platform with guaranteed privacy", arXiv preprint arXiv, 2015.

[17] Fabrice Benhamouda, Shai Halevi, Tzipora Halevi, "Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation", 2018 IEEE International Conference on Cloud Engineering, 2018. DOI: https://doi.org/10.1147/JRD.2019.2913621

[18] Soonduck Yoo, Kiheung Kim, “A Study on Improvement for Service Proliferation Based on Blockchain”, The Institute of Internet, Broadcasting and Communication, 2018. DOI: https://doi.org/10./JIIBC.2018.18.1.185

저 자 소 개

한 세 진(준회원)

- 서강대학교 컴퓨터공학과 학사('98), 석사('01), 박사수료('18)
- KT 책임연구원('01~'11)
- 금융감독원 선임조사역('11~現)
- 관심분야 : 핀테크, 블록체인

김 순 태(준회원)

- 중앙대학교 컴퓨터공학과 학사('03), 서강대학교 컴퓨터공학과 석사('07), 박사('10)
- 전북대학교 소프트웨어공학과 교수('14~現)
- 관심분야 : 소프트웨어공학, 블록체인, 인공지능

박 수 용(비회원)

- 서강대학교 컴퓨터공학과 학사('86), Florida State University 컴퓨터 및 정보과학 석사('88), George Mason University 정보기술학 박사('95)
- 서강대학교 컴퓨터공학과 교수('98~現)
- 관심분야 : 블록체인, 요구공학

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음(IITP-2019-2017-0-01628*)