논문 19-44-12-11 The Journal of Korean Institute of Communications and Information Sciences '19-12 Vol.44 No.12
https://doi.org/10.7840/kics.2019.44.12.2252

블록체인 프라이버시 보호 프로토콜 동향 및 분석

이 상 현◆, 김 용 수*, 김 호 원°

Trends and Analysis of Blockchain Privacy Protocols

Sanghyun Lee◆, Yongsu Kim*, Howon Kim°

요 약

최근 블록체인 기술의 발전에 따라 블록체인 내 데이터 및 트랜잭션의 프라이버시 보호에 대한 관심이 높아지고 있다. 2008년 최초의 블록체인 시스템 비트코인이 발표된 이후 블록체인의 데이터가 모두에게 공개된다는 특징은 많은 사람들의 주목을 받았지만 이는 오히려 블록체인의 활용도를 낮추고 있다. 이에 따라 다양한 형태의 블록체인 프라이버시 보호 프로토콜이 연구되고 있다. 이와 같은 프로토콜들은 대부분 영지식 증명을 기반으로 연구되고 있으며 블록체인 시스템에 영향을 줄이기위해 실행 시간을 최소화하는 방향으로 연구되고 있다. 블록체인 내에 프라이버시 보호 프로토콜이 적용되면 기존의 블록체인의 장점인 신뢰성, 투명성뿐만 아니라 익명성 또한 제공하여 블록체인의 활성화에 기여할 수 있다. 2019년 현재 다양한 프라이버시 보호 프로토콜들이 제시되었고, 상용화된 플랫폼에 활용되고 있다. 본 논문에서는 이러한 프로토콜들의 동향 및 성능에 대해 분석하고 향후 연구 방향에 대해 기술하고자 한다.

Key Words : Blockchain, Privacy, Zero-Knowledge Proof, Information security, zk-SNARKs

ABSTRACT

Recently, with the development of blockchain technology, there is a growing interest in preserving the privacy of data and transactions in the blockchain. Since the first blockchain system bitcoin was announced in 2008, the characteristic of blockchain data being public to all has drawn the attention of many people, but this is rather lowering the utilization of blockchain. Accordingly, various types of blockchain privacy-preserving protocols are being studied. Most of these protocols are being studied on the basis of zero-knowledge proof and in a way that minimizes execution time to reduce impact on blockchain systems. When privacy-preserving protocols are applied within blockchain, they can contribute to activating blockchain by providing anonymity as well as reliability and transparency which are advantages of blockchain. In 2019, a variety of privacy- preserving protocols have been presented and applied to the commercialized platform. In this paper, we will analyze the trends and performance of these protocols and describe their future research directions.

Ⅰ. 서 론

블록체인(blockchain)은 블록에 데이터를 담고 체인 형태로 연결한 탈중앙화된 분산형 데이터베이스이다. 2008년 사토시 나카모토가 발표한 "Bitcoin:A Peer-to-Peer Electronic Cash System"[1] 논문에서 처

※이 논문은 국토교통부의 스마트시티 혁신인재육성사업으로 지원되었습니다.
◆ First Author : Department of Computer Science Engineering, Pusan National Univ., jdsd2233@gmail.com, 학생회원
° Corresponding Author : Department of Computer Science Engineering, Pusan National Univ., howonkim@gmail.com, 종신회원
* Department of Computer Science Engineering, Pusan National Univ., dkgoggog0329@gmail.com
논문번호 : 201910-248-C-RU, Received October 23, 2019; Revised November 19, 2019; Accepted November 24, 2019

음으로 블록체인 개념이 등장하였으며, 블록체인이 적용된 최초의 시스템인 비트코인 이후에 수 많은 블록체인 적용 시스템이 등장하였다. 블록체인 초기에는 단순히 암호화폐의 전송만을 지원하는 시스템이 대부분이었지만, 블록체인 기술이 발전하며 단순한 시스템을 벗어나 튜링 완전(turing-complete)한 언어를 지원하는 플랫폼의 형태를 띄고 있다[2]. 이렇게 블록체인의 형태가 바뀌어 감에 따라 블록체인 내에서의 프라이버시 보호의 필요성 또한 높아지고 있다[3,4].

대부분의 블록체인 시스템은 트랜잭션이 모두 공개되는 구조를 갖추고 있다. 이는 누가, 언제, 어떠한 거래를 하였는지가 모두 공개된다는 의미이다[5,6]. 일반적으로 블록체인 시스템 내에서는 사용자에 대한 정보는 드러내지 않고 익명성을 유지하는 것으로 알려져 있다. 하지만 거래내역을 모두 드러내기 때문에 사용자가 어떠한 거래를 하였는지 알 수 있고, 사용자의 신원이 특정 되면 사용자의 블록체인 내 모든 정보가 노출된다[7]. 블록체인은 모두에게 정보를 공개해 투명성 및 신뢰성을 보장 하지만, 이러한 특성은 오히려 민감한 개인정보를 블록체인에 올릴 수 없게 만들었다. 또, 기업들은 기업 내부 정보가 공개되는 것을 원하지 않기 때문에 블록체인의 장점이 오히려 기업의 블록체인 활용에 걸림돌이 되고 있다.

블록체인의 장점인 투명성 및 신뢰성을 보장하고, 데이터에 대한 프라이버시 보호와 관련된 다양한 연구들이 진행되고 있다. 여러 가지 프라이버시 보호 프로토콜들이 공개되고 있는데, 이러한 프로토콜들은 블록체인 내에서 프라이버시 보호를 보장하지만, 블록체인의 트랜잭션 처리 속도를 저하시킨다. 이러한 단점을 보완하기 위해 블록체인 트랜잭션 처리 성능에 영향을 최소한으로 주면서 프라이버시 보호를 보장하는 프로토콜의 필요성이 제기되고 있다. 따라서 본 논문에서는 현재 공개된 프라이버시 보호 프로토콜의 동향에 대해 알아보고, 프로토콜들의 동작 방식, 특징, 개선점, 주요 알고리즘 실행 시간 등에 대해 기술한다.

Ⅱ. 프라이버시 보호 개요

블록체인 내에서 프라이버시 보호는 다양한 방식으로 적용된다. 대표적으로 트랜잭션에 나타나는 데이터, 참가자 인증에 사용하는 인증서[8], 스마트 컨트랙트에 사용되는 민감 데이터에 대한 프라이버시 보호가 있다[9].

2.1 트랜잭션 데이터 프라이버시

트랜잭션에 대한 프라이버시 보호는 암호화폐를 포함한 퍼블릭 블록체인에서 주로 활용한다. 퍼블릭 블록체인의 네트워크는 누구나 참여할 수 있으므로 거래내역에 대한 프라이버시 보호가 이루어지지 않으면 누구나 거래내역을 조회할 수 있게 된다. 가장 대표적인 암호화폐인 비트코인의 경우 블록 탐색기를 통해 모든 거래내역을 조회할 수 있다. 거래내역에는 비트코인을 보내는 사용자의 주소, 받는 사용자의 주소, 보내는 양 등이 포함되어 있다. 또 사용자의 주소에 얼마만큼의 비트코인이 들어있는지, 언제 어떤 거래를 했지는 모두 조회할 수 있어 특정인의 주소를 알게되면 그 사용자의 블록체인 내 활동을 모두 조회할 수 있게 된다.

따라서 트랜잭션에 대한 프라이버시 보호는 트랜잭션에 담긴 데이터를 감춤으로써 이루어진다. 트랜잭션에 담긴 사용자의 주소, 보내는 양 등 거래데이터를 암호화를 통해 감추는 대신 영지식 증명을 활용해 해당 거래가 유효함을 검증한다. 따라서 사용자가 어떤 거래를 하는지 드러나지 않는다. 트랜잭션에 대한 프라이버시 보호가 적용된 블록체인의 경우 블록체인 내의 사용자 활동이 드러나지 않아 사용자들은 자신의 프라이버시를 보호할 수 있다.

2.2 인증서 프라이버시

사용자에 대한 익명성은 허가형 블록체인에서 활용된다. 허가형 블록체인의 네트워크에 참가하기 위해서는 반드시 참가 허가를 받아야 한다. 이때 네트워크 참가자들은 블록체인 내에서 본인을 인증하기 위해 인증서를 사용 한다. 인증서에는 참가자의 정보가 담겨있게 되는데 이를 통해 참가자가 블록체인 내에서 어떤 활동을 하는지 추적할 수 있게 된다. 따라서, 네트워크 참가자의 익명성을 보장하는 블록체인은 사용자 정보가 드러나지 않는 인증을 사용하게 된다. 이러한 방식은 영지식 증명을 통해 구현한다[10]. 사용자는 인증서에 담긴 정보 중 드러내기를 원하는 정보만 드러내고 감추고 싶은 정보는 드러내지 않을 수 있다. 이러한 기술은 Controllable Privacy라고 하며 사용자는 본인의 정보가 노출되는 정도를 조절할 수 있다.

2.3 스마트 컨트랙트 데이터 프라이버시

블록체인 내에서 구현되는 스마트 컨트랙트는 민감한 데이터를 필요로 할 수 있다. 예를 들어, 의료 데이터의 경우 환자와 의료진 외에는 누구도 열람할 수 없어야 하지만 블록체인 내에서 데이터가 활용될 경우

모두에게 공개된다. 이를 방지하기 위해 데이터를 조작해 스마트 컨트랙트를 실행해도 다른 사용자들이 데이터를 조회할 수 없게 한다.

데이터를 조작하면 일반적인 블록체인 사용자들에게는 데이터가 노출되지 않지만, 스마트 컨트랙트를 실행하는 노드에게는 데이터가 노출된다. 따라서 단순한 데이터에 대한 조작뿐 아니라 조작된 데이터를 원본으로 복구하지 않아도 스마트 컨트랙트를 실행할 수 있는 기술 또한 필요하다. 스마트 컨트랙트에 활용되는 데이터에 대한 프라이버시 보호는 데이터의 조작 및 조작된 데이터를 통한 스마트 컨트랙트 실행 두 가지를 모두 수행해야 보장된다.

Ⅲ. 프라이버시 보호 프로토콜 동향 및 분석

3.1 zk-SNARKs

zk-SNARKs(zero-knowledge Succint Non-interactive Argument of Knowledge)는 동형암호의 특성과 타원곡선암호, 페어링, 다항식 등을 활용하여 증명 및 검증을 수행한다[11,12]. zk-SNARKs는 증명의 크기가 작아 간결하고 신속하게 검증을 할 수 있으며, 증명자와 검증자 사이의 상호작용이 필요하지 않다[13-16]. 하지만 이러한 특성을 가지기위해 신뢰 기관(trusted party)이 존재하게 되는데, 신뢰 기관은 증명자가 알고있다고 주장하는 비밀 값(witness)을 받아 이를 통해 증명을 생성한다. 이러한 구조에는 증명자의 비밀 값이 노출될 수 있는 가능성과 신뢰 기관에 의한 거짓 증명 생성의 가능성이 있다.

zk-SNARKs는 Trusted Setup, Prove, Verify 세 단계를 수행한다. Trusted Setup 단계에는 신뢰 기관이 증명과 검증에 사용할 증명 키(proving key)와 검증 키(verification key)를 생성한다. 이 과정에서 계산식을 R1CS, QAP 형태로 바꾸는 기법이 적용되는데, 그림 1과 같이 증명자의 비밀 값을 통해 계산식을 만들고 이를 산술 회로(arithmetic circuit)로 구성한다[17]. 이 회로는 곱셈과 덧셈으로 이루어지는데 이를 R1CS의 형태로 바꾸면 게이트의 입출력 유효성 검사를 할 수행할 수 있다. 하지만 R1CS 형태는 전체 게이트에 대한 유효성 검사를 수행해야 전체 수식의 유효성을 알 수 있으므로 이를 QAP 형태로 바꾸어 게이트 별 유효성 검사를 수행할 수 있게 한다[18]. QAP 형태로 바꾸고 난 이후에는 그림 2와 같이 다항식 형태로 활용할 수 있다. QAP가 구성된 이후에는 게이트에 해당하는 변수가 다항식의 해가 되는 목표 다항식(target polynomial)을 정의할 수 있다. 결과적으로 QAP가

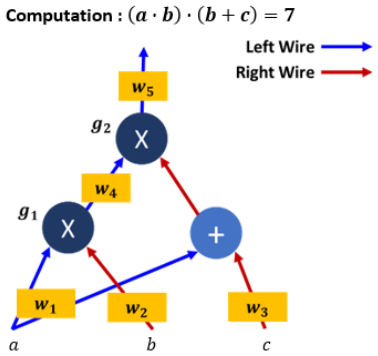


그림 1. 계산식의 산술 회로 구성
Fig. 1. Arithmetic circuit configuration of computation

구성된 형태인 그림2의 목표 다항식은 $(x-1)(x-2)(x-3)$이 되며, 이 다항식을 통해 증명 키와 검증 키를 생성한다[19-21].

Prove 단계에서는 증명자가 신뢰 기관으로부터 받은 증명 키와 비밀 값을 통해 proof를 생성한다. Proof가 생성된 이후에는 이를 통해 비밀 값을 유추할 수 없고 proof를 생성하는데 걸리는 시간은 비밀 값의 크기와 비례한다. Prove 단계에서 생성되는 proof는 검증자에게 보내지고, proof의 길이는 다른 프로토콜에 비해 짧은 편이므로 이를 통해 간결함(succint)을 얻을 수 있다. Prove 단계에서 생성된 proof의 크기는 80bits of security에서 230bytes, 128bits of security에서 288bytes이다.

Verify 단계에서는 검증자가 신뢰 기관으로부터 받은 검증 키를 활용해 증명자로부터 받은 proof의 유효성을 검증한다. zk-SNARKs는 검증에 걸리는 시간이 다른 프로토콜에 비해 짧은데 이 또한 간결함을 얻게 하는 요소이다. Verify 단계는 약 5ms가 소요된다.

표 1은 vnTinyRam[22]에서 측정한 프로토콜의 수행 시간을 나타낸다. Security level에 따라 키생성 시간, 증명 시간, proof의 크기가 증가하지만 검증 시간은 비슷함을 알 수 있다.

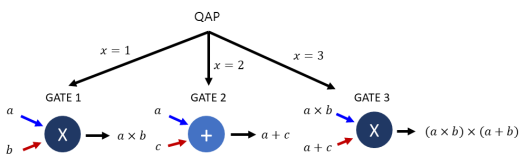


그림 2. 산술 회로 게이트의 QAP 구성
Fig. 2. QAP Configuration of Arithmetic Circuit Gates

표 1. vnTinyRam에서 측정한 zk-SNARKs 실행 시간 및 proof 크기
Table 1. zk-SNARKs execution time and proof size measured by vnTinyRam

	80 bits of security	128 bits of security
키 생성	97s	117s
증명	115s	147s
검증	4.9ms	5.1ms
Proof 크기	230B	288B

3.2 zk-STARKs

zk-STARKs는 zk-SNARKs의 문제점을 보완하여 나온 프라이버시 보호 프로토콜이다. zk-SNARKs의 가장 주요한 문제점은 Trusted Setup 단계가 존재한다는 것인데 zk-STARKs는 Trusted Setup 단계가 필요하지 않다. zk-STARKs는 zk-SNARKs에서 사용하던 타원곡선암호, 페어링 등을 대신해 hash와 information theory를 사용한다. hash를 통해 Trusted Setup 단계에 만들어지는 데이터들을 랜덤하게 생성되도록 설계하였기 때문에 신뢰 기관이 거짓 증명을 생성할 수 있는 zk-SNARKs에 비해 보안적으로 개선되었다[23].

zk-STARKs는 보안적으로 개선 되었고, Prove 단계의 시간은 zk-SNARKs에 비해 크게 감소하였다. 하지 만 proof의 크기와 Verify단계의 시간이 증가하였는데 그럼에도 확장성면에서 크게 개선되었다[23]. 이는 산술 회로를 생성할 때의 복잡도가 감소하였기 때문이다. zk-STARKs는 늘어난 proof의 크기를 줄이는 방향으로 연구가 진행 중이다.

3.3 Bulletproof

Bulletproof는 스탠포드 대학에서 제시한 상호작용이 없는 영지식 증명 프로토콜로 이산 로그 가정(discrete logarithm assumption)을 기반해 Trusted setup 과정이 필요하지 않다. Bulletproof는 Multi-Party Computation을 도입하여 비밀 값의 공개 없이 다수의 참가자들이 하나의 proof를 생성할 수 있다. Bulletproof는 Jonathan Bottle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, Christophe Petit가 제시한 zero-knowledge argument를 사용하는데, 이를 통해 산술 회로 크기에 대한 proof의 크기가 대수적으로 증가하게 하여 proof의 크기를 기존 영지식 프로토콜에 비해 작게 만든다. 또, 다수의 검증에 대해 일괄 처리 방식을 도입해 검증 시간 또한 감소하였는데, ECDSA의 검증 시간과 유사한 검증 시간을 나타낸다[24].

표 2. Bulletproof 실행 시간 및 proof 크기
Table 2. Bulletproof execution time and proof size

Problem 크기	proof 크기 (bytes)	시간(ms)		
		증명	검증	batch
8bit	482	3.7	0.9	0.28
16bit	546	7.2	1.4	0.33
32bit	610	15	2.4	0.38
64bit	675	29	3.9	0.45

표 2는 Problem 크기에 따른 proof 크기와 각 단계의 실행 시간을 나타낸다. 표 3에서는 위의 세 프라이버시 보호 프로토콜들을 비교한다.

3.4 Identity Mixer

Identity Mixer는 IBM의 허가형 블록체인 플랫폼 하이퍼레저 패브릭(hyperledger fabric)에서 사용되는 프라이버시 보호 프로토콜이다. Jan Camenisch와 Anna Lysyanskaya가 제시한 페어링 기반 서명 기법 CL signature를 활용해 영지식 증명 기반의 인증서를 도입하였다[25,26,27]. 이 인증서는 기존에 사용하던 X.509 인증서를 대체하는데, 사용자의 정보를 선택적으로 드러내는 기능을 제공한다. 또, 하나의 인증서를 통해 여러 번 인증하더라도 같은 인증서로 인증하였는지 알 수 없는 불연계성(unlinkability) 특성을 가지고 있다[28].

표 3. 프라이버시 보호 프로토콜 비교
Table 3. Privacy-preserving protocol comparision

	zk-SNARKs	zk-STARKs	Bulletproofs
알고리즘 복잡도 : 증명	$O(N\times\log(N))$	$O(N\times poly-\log(N))$	$O(N\times\log(N))$
알고리즘 복잡도 : 검증	$O(1)$	$O(poly-\log(N))$	$O(N)$
Trusted Setup 단계 유무	있음	없음	없음
양자컴퓨터 저항성	없음	있음	없음
암호 가정	Knowledge of Exponent Assumption	Collision resistant hashes	Discrete log

Identity Mixer에서 사용하는 인증서는 Credential이라고 명칭한다. 이 인증서는 하나의 인증서에 대해 여러 개의 공개 키를 생성할 수 있어 동일한 인증서로 인증이 필요할 때마다 서로 다른 공개 키를 사용해 같은 사용자라는 것을 숨길 수 있다. 결과적으로 사용자는 블록체인 내에서 어떤 활동을 하는지 드러내지 않을 수 있다[29].

그림 3은 Identity Mixer를 사용하는 블록체인 구조를 보여준다.

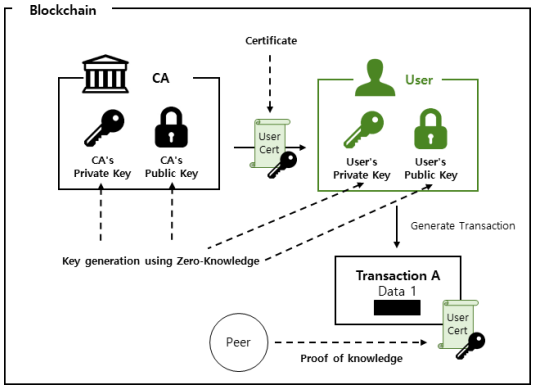


그림 3. Identity Mixer를 사용하는 블록체인 구조
Fig. 3. Blockchain Structure Using Identity Mixer

3.5 Enigma

Enigma는 MIT 대학에서 개발한 블록체인 프로토콜로 기존 블록체인에 존재하는 privacy에 대한 문제의 해결책을 제시하였다. Enigma는 초기에 기존 블록체인의 오프체인 형태로 연결되어 프로토콜을 수행하게 설계되었는데 후에 독자적인 블록체인 플랫폼으로 개발되었다.

Enigma는 sMPC(secure Multi-Party Computation)를 사용해 스마트 컨트랙트의 데이터에 대한 프라이버시를 보호한다. Enigma에서는 이러한 형태의 스마트 컨트랙트를 시크릿 컨트랙트(secret contract)라고 한다. 시크릿 컨트랙트에서는 서로 다른 노드들이 데이터 조각을 나누어 가지게 되며, 데이터가 시크릿 컨트랙트 실행에 필요한 경우 조각들을 합쳐서 연산하게 된다. 이 과정에서 각 노드는 다른 노드가 가지고 있는 데이터를 알 수 없으며, 따라서 전체 데이터는 어떠한 노드도 알 수 없다. 마찬가지로 블록체인에도 전체 데이터가 저장되지 않는다. Enigma에는 DHT(Distributed Hash-Table)가 존재하고 여기에 데이터에 대한 참조(reference)를 저장한다. 블록체인에는 시크릿 컨트랙트 실행에 대한 proof를 저장하게 되

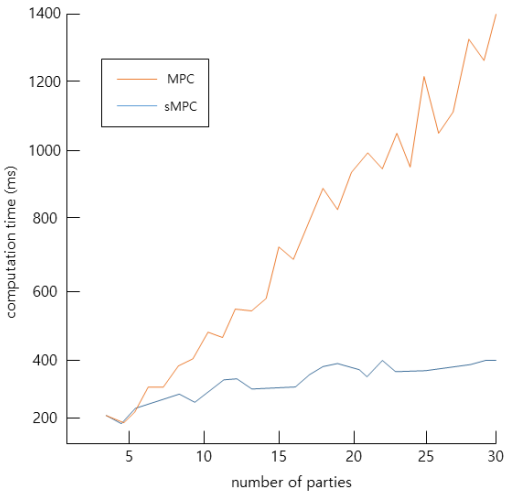


그림 4. MPC와 sMPC 실행 시간 비교
Fig. 4. MPC and sMPC execution time

는데, 이는 시크릿 컨트랙트 실행이 제대로 이루어졌음을 검증하는데 사용할 수 있다[30].

그림 4에서 나타나듯이 Enigma의 sMPC는 최적화를 통해 일반적인 MPC에 비해 연산 성능이 향상되었는데, 연산 참가자의 수가 많을수록 비교적 더 빠른 연산 속도를 나타내고 있다[31].

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 최신 블록체인 프라이버시 보호 프로토콜 5종에 대하여 알아보았다. 현재 블록체인에 대한 연구는 분야를 가리지 않고 활발하게 진행되고 있다. 프라이버시 보호 프로토콜에 대한 연구도 활발하게 진행되고 있어 프라이버시 보호 프로토콜의 수 또한 증가하는 추세이다. 그 중 인증서, 스마트 컨트랙트 데이터에 대한 프라이버시 프로토콜 연구는 트랜잭션 데이터에 비해 활발하지 않으며, 특정 블록체인 플랫폼에서 추가적인 기능으로 제공하는 경우가 대부분이다. 특히, 인증서의 경우 허가형 블록체인의 경우에만 인증서가 필요해 퍼블릭 블록체인이 더 많은 관심을 받던 기존에는 활발한 연구가 이루어지지 않았다. 그에 비해, 트랜잭션 데이터에 대한 프라이버시 보호 프로토콜 연구는 활발하게 이루어지고 있는 편이며 기존 연구에 대한 개선 또한 활발하게 이루어지고 있다. 본 논문에서 분석한 zk-STARKs, Bulletproof의 경우에도 zk-SNARKs에서 파생된 프로토콜들이다. 해당 프로토콜들은 zk-SNARKs에서 Trusted Setup 단계를 없앰으로써 보안적 개선을 이루

어내었다. 또, 실행 시간을 줄여 실제 블록체인 시스템에 적용되었을 때 트랜잭션 처리 성능 저하를 줄일 수 있게 되었다. 이외에도 zk-SNARKs를 통한 Verfiable Computation에 대한 연구 또한 이루어지고 있는데[32] 이와 더불어 스마트 컨트랙트 데이터에 대한 프라이버시 보호 역시 함께 연구되고 있다.

현재 퍼블릭 블록체인 플랫폼 중 가장 널리 알려진 이더리움 또한 zk-SNARKs를 적용하려는 연구를 진행중에 있는데, 향후에는 프라이버시 보호 프로토콜 자체의 실행 시간을 줄이는 것과 더불어 실제 시스템에 적용했을 때 영향을 줄이는 방향으로 연구가 진행될 것으로 예측된다. 또한, 허가형 블록체인에 대한 관심이 높아짐에 따라 인증서에 대한 프라이버시 보호 프로토콜에 대한 연구도 사용자의 영지식 증명 기반의 사용자 익명성을 강화하는 방향으로 연구가 활발해질 것으로 예측된다.

References

[1] N. Satoshi, "*Bitcoin: A Peer-to-Peer Electronic Cash System*(2008)," Retrieved Oct. 3, 2019, from http://bitcoin.org/bitcoin

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," *2017 IEEE Int. Congress on Big Data (BigData Congress)*, pp. 557-564, 2017.

[3] G. Zyskind, O. Nathan, and A. 'Sandy' Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *2015 IEEE Secur. and Privacy WorkShops*, pp. 180-184, 2015.

[4] P. Zhong, Q. Zhong, H. Mi, S. Zhang, and Y. Xiang, "Privacy-protected blockchain system," *2019 20th IEEE MDM*, pp. 457-461, 2019.

[5] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," *2017 IEEE EuroS&PW*, pp. 1-3, 2017.

[6] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "To blockchain or not to blockchain: That is the question," *IEEE IT Professional*, vol. 20, no. 2, pp. 62-74, 2018.

[7] J. Barcelo, "*User privacy in the public bitcoin blockchain*(2014)," Retrieved Sep. 26, 2019, from https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf

[8] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. and Comput. Appl.*, pp. 45-58, 2019.

[9] A. Unterweger, F. Knirsch, C. Leixnering, and D. Engel, "Lessons learned from implementing a privacy-preserving smart contract in ethereum," *2018 9th IFIP Int. Conf. New Technol., Mobility and Secur. (NTMS)*, pp. 1-5, 2018.

[10] J. Kilian, "A note on efficient zero-knowledge proofs and arguments," in *Proc. Twenty-fourth Annu. ACM Symp. Theory of Computing*, pp. 723-732, 1992.

[11] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," *23rd USENIX Secur. Symp.*, pp. 781-796, 2014.

[12] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," *2013 IEEE Symp. Secur. and Privacy*, pp. 232-237, 2013.

[13] G. Jens, "On the size of pairing-based non-interactive arguments," *Annu. Int. Conf. Theory and Appl. Cryptographic Techniques*, pp. 305-326, 2016.

[14] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, *From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again*, Retrieved Oct. 3, 2019, from https://eprint.iacr.org/2011/443, 2011

[15] C. Reitwiessner, "*zkSNARKs in a nutshell* (2016)," Retrieved Sep. 28, 2019, from https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/

[16] J. Lee, J. Y. Hwang, H. Oh, and J. Kim, "Personal information management system with blockchain using zk-SNARK," *J. The Korea Inst. Inf. Secur. & Cryptology*, vol. 29, no. 2, pp. 299-308, 2019.

[17] V. Buterin, "Quadratic arithmetic programs: from zero to hero(2016)," Retrieved Sep. 28, 2019, from https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero

-f6d558cea649

[18] R. Gennaro, C. Gentry, B. Parno, and M. Raykova, "Quadratic span programs and succinct NIZKs without PCPs," *32nd Annu. Int. Conf. Theory and Appl. Cryptographic Techniques*, pp. 626-645, 2013.

[19] ZCash-What are zk-SNARKs, Retrieved Oct. 11, 2019, from https://z.cash/technology/zksnarks/

[20] M. Petkus, "Why and how zk-SNARK works," Retrieved Sep. 28, 2019, from https://arxiv.org/abs/1906.07221

[21] V. Buterin, "zk-SNARKs: Under the hood (2017)," Retrieved Sep. 28, 2019, from https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6

[22] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "TinyRAM architecture specification v0.991(2013)," Retrieved Oct. 10, 2019, from http://www.scipr-lab.org/specs

[23] E. Ben-Saason, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," 2018.

[24] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," *2018 IEEE Symp. Secur. and Privacy (SP)*, pp. 315-334, 2018.

[25] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," *Annu. Int. Cryptology Conf. Advanced in Cryptology-CRYPTO 2004, LNCS*, vol. 3152, pp. 56-72, 2004.

[26] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," *Secur. and Cryptography for Netw., LNCS*, vol. 4116, pp. 111-125, 2006.

[27] J. Camenisch, M. Drijvers, and A. Lehmann, "Anonymous attestation using the strong diffie hellman assumption revisited," *Trust and Trustworthy Computing, LNCS*, vol. 9824, pp. 1-20, 2016.

[28] Hyperledger Fabric – *Read the Docs*(2019), Retrieved Oct. 11, 2019, from https://hyperledger-fabric.readthedocs.io/en/release-1.4/idemix

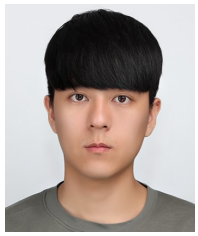
[29] J. Camenisch, M. Dubovitskaya, A. Lehmann, G. Neven, C. Paquin, and F.-S. Preiss, "Concepts and languages for privacy-preserving attribute-based authentication," *Policies and Research in Identity Management, IFIPAICT*, vol. 396, pp. 34-52, 2013.

[30] G. zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *Cryptography and Secur.*, Jun. 2015.

[31] I. Damgard, M. Keller, E. Larraia, V. Pastro, P. Scholl, and N. P. Smart, "Practical covertly secure MPC for dishonest majority - or: breaking the SPDZ limits," *Computer Secur. ESORICS*, pp. 1-18, 2013.

[32] B. Prano, C. Gentry, J. Howell, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," *2013 IEEE Symp. Secur. and Privacy*, pp. 238-252, 2013.

이 상 현 (Sanghyun Lee)



2019년 2월 : 부산대학교 전기컴퓨터공학부 졸업

2019년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석사과정

<관심분야> 블록체인, 정보보호, 인공지능

[ORCID:0000-0002-1188-6551]

김 용 수 (Yongsu Kim)

2019년 2월 : 부산대학교 전기컴퓨터공학부 졸업

2019년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석사과정

<관심분야> 지능형IoT, 딥러닝, 인공지능

[ORCID:0000-0001-6169-5537]

김 호 원 (Howon Kim)

1993년 2월 : 경북대학교 공학사
1995년 2월 : 포항공과대학교 공학석사
1999년 2월 : 포항공과대학교 공학박사
2004년 : Ruhr University Bochum, Post Doctorial
1998년~2008년 : 한국전자통신연구원 팀장
2008년~현재 : 부산대학교 전기컴퓨터공학부 교수
<관심분야> 정보보호, 지능형IoT, FPGA/ASIC, 인공지능
[ORCID:0000-0001-8475-7294]