J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

블록체인을 위한 믹스 기반 분산화된 익명 거래☆

Mix-based Decentralized Anonymous Transaction for Blockchain

이 윤 호1*
Yun-ho Lee

요 약

기존 화폐가 은행과 같은 신뢰할 수 있는 중앙기관에 의존하는 것과 달리 비트코인을 비롯한 암호화폐는 탈중앙화, 분산화 및 P2P의 특성을 갖는다. 암호화폐에서 거래는 모든 참여자가 확인할 수 있도록 투명하게 분산 저장되며 공개되지만, 이미 저장된 거래 내역의 위변조는 사실상 불가능한 특징이 있다. 흔히 암호화폐도 기존 화폐와 같이 익명성을 갖는 것으로 생각하지만, 암호화폐는 익명성이 아닌 가명성을 제공한다. 이런 이유로 익명성을 보장하기 위한 다양한 연구가 진행되고 있으며, 믹스를 기반으로 한 익명성 보장도 그중 하나이다. 본 논문에서는 믹스를 기반으로 한 기존 익명성 보장 기법을 살펴보고 효율성을 개선한 하이브리드 믹스 기법을 제안한다.

☞ 주제어 : 암호화폐, 비트코인, 익명성, 믹스

ABSTRACT

Cryptocurrencies, including Bitcoin, has decentralization, distribution and P2P properties unlike traditional currencies relies on trusted central party such as banks. All transactions are stored transparently and distributively, hence all participants can check the details of those transactions. Due to the properties of cryptographic hash function, deletion or modification of the stored transations is computationally not possible. However, cryptocurrencies only provide pseudonymity, not anonymity, which is provided by traditional currencies. Therefore many researches were conducted to provide anonymity to cryptocurrencies such as mix-based methods. In this paper, I will propose more efficient hybrid mix-based method for anonymity than previous mix-based one.

☞ keyword : Cryptocurrency, Bitcoin, Anonymity, Mix

1. 서론

기존 (전자)화폐가 신뢰할 수 있는 기관(은행 등)을 기반으로 한다면, 비트코인으로 대표되는 암호화폐(cryptocurrency)는 탈중앙화(분산화)의 특징을 갖고 있다[1]. 즉 사용자간 거래 내역을 중앙 기관에 기록하지 않고 전체 사용자가 분산 보관하게 된다. 거내 내역의 유지를 중앙 기관에 의존하지 않기 때문에 위변조의 우려가 있지만 암호학적인 기법을 통해 이미 실행된 거래 내역을 바꾸지 못하도록 하고 있다. 비트코인의 경우 블록체인을 통해 이러한 안전성을 제공하는데, 블록체인은 작업증명(PoW, proof of work)이라는 연산에 기반하며, 기존 거래 내역을 바꾸기 위해서는 블록체인 네트워크에 참여하는 전체 사용자의 연산능력의 과반을 확보해야 하기 때문에 거래 내역의 위변조는 현실적으로 불가능하다.

암호화폐는 거래시 개인의 신원을 특정할 수 있는 정보를 사용하지 않고 임의의 공개키를 주소로 활용하기 때문에 흔히 익명성을 보장한다고 생각할 수 있지만, 엄밀히 말하면 암호화폐는 가명성(pseudonymity)은 제공하지만 익명성(anonymity)은 제공하지 않는다[2,3]. 가명성이란 특정 주소(공개키 주소)를 소유자와 연결할 수는 없지만, 해당 주소의 입출금 내역을 지우거나 감출 수 없기 때문에 나타나는 특성을 말하며, 익명성이란 특정 주소를 소유자와 연결한 수 없음은 물론이고 입출금 내역과 특정 주소도 연결할 수 없는 특성을 말한다.

이러한 이유로 비트코인에서는 다수의 지갑을 활용하거나, 매 거래마다 서로 다른 공개키를 이용할 것을 권장하고 있다[4].

비트코인의 익명성에 대한 분석 결과는 여러 논문을 통해 제시되었는데[5,6,7], 특히 2013년 R. Fergal과 M.

1 Department of Cyber Security & Police, Gwangju University, 277 Hyodeok-Ro, Nan-Gu, Gwangju, 61743, Korea.
* Corresponding author (leeyh@gwangju.ac.kr)
[Received 7 July 2020, Reviewed 4 August 2020(R2 5 Ocotober 2020), Accepted 28 October 2020]
☆ 이 연구는 2020년도 광주대학교 대학 연구비의 지원을 받아 수행되었음

Harrigan은 비트코인을 대상으로 '거래 네트워크'와 '사용자 네트워크'를 도입하여 익명성을 분석하면서, 개인이 다수의 공개키를 사용하더라도 익명성을 충분히 보장하기는 어렵다고 밝힌 바 있다. 특히, IP 주소 등의 Off-network 정보를 추가 결합할 경우 익명성을 침해할 가능성은 더욱 높아진다[5].

암호화폐에서 익명성이란 특정 거래의 송신자(지불인)와 수신자(수취인)를 확인할 수 없다는 것으로, 만약 익명성이 보장되지 않는다면 사용자(상인)의 프라이버시를 심각하게 침해하는 등의 문제가 발생할 수 있다[8].

암호화폐의 익명성을 보장하기 위해 널리 사용되는 방법중 하나는 믹스를 이용하는 것인데[9,10,11], 믹스는 D. L. Chaum이 1981년 제안한 방식으로 입/출력값(송/수신자)을 연결할 수 없도록 익명성을 부여하는 기법으로 흔히 믹스넷이라고 부른다[12]. 암호화폐의 익명성을 보장하기 위한 믹스기반 방식은 크게 중앙집중화 믹스(centralized mix)와 탈중앙화 믹스(decentralized mix)로 구분되는데, 중앙집중화 믹스는 전통적인 믹스넷을 활용한 방법으로 믹스 서버는 신뢰할 수 있다고 가정한다. 현재 제공되고 있는 다양한 상용 믹스 서비스가 이에 해당하지만, 이 방식은 탈중앙화 또는 분산화된 암호화폐의 환경과는 맞지 않는 문제가 있다.

이에 비해 탈중앙화 믹스는 신뢰해야 하는 믹스 서버를 사용하지 않는 방식으로 믹스를 담당하는 전용 서버 또는 네트워크 대신 사용자간 통신을 통해 믹스를 진행한다. 이는 암호화폐의 특성과도 일치하고 익명성을 높이는 장점이 있지만 사용자간 통신 및 연산 과정때문에 중앙집중화 믹스에 비해 효율성이 떨어지는 문제가 있다.

T. Ruffing 등은 2014년 비트코인의 거래 익명성을 보장하기 위한 탈중앙화 믹스 기법인 CoinShuffle을 제안하였다[10]. 이 방식은 중첩 암/복호화를 기반으로 하며, 전통적인 암호화 믹스 또는 복호화 믹스와 유사하게 동작한다. 이들은 2017년 CoinShuffle++ 방식을 제안하는데[11], 이는 CoinShuffle보다 연산 효율성은 낮지만 익명성을 높인 방식이다[8].

본 논문에서는 중앙집중화 믹스와 탈중앙화 믹스를 혼합한 하이브리드 믹스 방식을 제안한다. 제안한 방식은 연산효율성은 높이면서 믹스 서버에 대한 신뢰도는 낮춘 장점이 있다. 본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용할 표기법과 기존 중앙집중화 믹스 및 탈중앙화 믹스에 대해 설명한다. 3장에서 하이브리드 믹스 기법을 제안하고 4장에서 기존 방식과 비교 분석한 후, 5장에서 결론을 맺는다.

2. 관련 연구

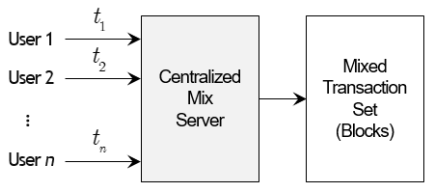
2.1 표기법

본 논문에서 사용할 표기법은 다음과 같다.

- e_i : 참가자 i
- e : 참가자 그룹 $(e_1,...,e_n)$
- M : 믹스 서버
- sk_i : e_i의 개인키
- pk_i : e_i의 공개키
- sk : M의 개인키
- pk : M의 공개키
- A_i : e_i가 송금하려는 주소
- ek_i : e_i의 임시 공개키
- dk_i : e_i의 임시 개인키
- $c = E_k(m)$: 메시지 m을 공개키 k로 암호화
- $M = D_k(c)$: 암호문 c를 개인키 k로 복호화
- $\sigma = Sign_k(m)$: 개인키 k로 메시지 m의 서명생성
- $Verify_k(\sigma,m)$: 공개키 k로 메시지 m의 서명검증
- $V=(v_1,...,v_n)$: 암호문 $v_1,...,v_n$으로 구성된 벡터
- V^{sort} : 벡터 V의 원소를 정렬한 형태

2.2 중앙집중화 믹스

전자화폐에서 익명성을 제공하는 손쉬운 방법은 신뢰할 수 있는 믹스 서버를 이용하는 것이다. 이 방법은 비트코인과 같은 분산화 특성이 없기 때문에 중앙집중화 믹스 방식이라고 하며, Bitcoin Laundry[2], Bitcoin tumblers[3], MixCoin[9] 등이 이에 해당된다. 동작 과정은 간단하다. 익명 처리를 원하는 사용자는 믹스서버에 트랜잭션 내용을 전송하고, 믹스 서버는 여러 사용자의 트랜잭션 요청을 받아 믹스된 블록을 출력한다(그림 1 참조).

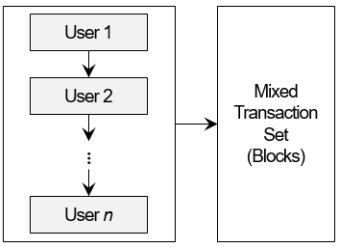


(그림 1) 중앙집중화 믹스
(Figure 1) Centralized Mix

이 방식의 단점은 이용자가 믹스 서버를 신뢰해야 하고, 보통 수수료를 지불해야 한다는 점이다.

2.3 탈중앙화 믹스

탈중앙화 믹스란 말 그대로 신뢰해야 하는 제3자(믹스 서버)를 가정하지 않는 방식이다. 일반적으로 익명 처리를 원하는 사용자들간 통신을 통해 믹스된 트랜잭션을 생성하게 된다(그림 2 참조).



(그림 2) 탈중앙화 믹스
(Figure 2) Decentralized Mix

CoinShuffle은 대표적인 탈중앙화 믹스 방식으로 2014년 Ruffing 등이 제안하였다[10]. 본 절에서는 CoinShuffle의 동작 과정에 대해 간단히 살펴본다.

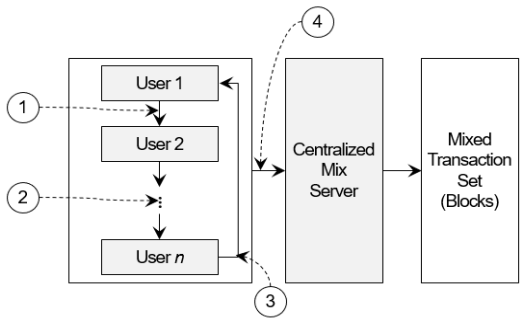
CoinShuffle은 중첩 암호화를 기반으로 하는데, 예를 들어 메시지 m에 대해, n개의 키 $k_1,...,k_n$을 이용한 중첩 암호화는 $E_{k_1}(E_{k_2}(...E_{k_n}(m)...))$이며, 간단하게 $E_{k_1,k_2,...,k_n}(m)$으로 표기하기로 한다. 또한, 믹스에 참여할 참가자 $e_i(i=1,...,n)$는 자신의 공개키-개인키 쌍 (pk_i,sk_i)를 가지고 있으며, $e_i(i=2,...,n)$는 임의의 공개키-개인키 쌍 (ek_i,dk_i) 및 자신의 개인키 sk_i를 이용한 서명 $\sigma_i = Sign_{sk_i}(ek_i)$를 생성한 후, (ek_i,σ_i)를 전체 참가자 그룹 e에게 브로드캐스트한다. 그리고 다른 참가자 $e_j(j=1,..,i-1,i+1,...,n)$가 브로드캐스트한 (ek_j,σ_j) 및 pk_j를 이용하여 $Verify_{sk_j}(\sigma_j,ek_j)$를 실행하여 서명 σ_j를 검증한다. 만약, 검증에 실패하면 프로토콜 진행을 중지한다.

첫 번째 참가자 e_1은 $v_1 = E_{ek_2,...,ek_n}(A_1)$을 계산하고, $V_1=(v_1)$과 $\sigma_1 = Sign_{sk_1}(V_1)$을 다음 참가자에게 전송한다. 참가자 e_i는 $Verify_{pk_{i-1}}(\sigma_{i-1},V_{i-1})$을 통한 서명 검증 및 V_{i-1}의 정렬 여부를 검증하고, 검증에 실패하였을 경우 프로토콜 진행을 중지한다. 이후 $V=D_{dk_i}(V_{i-1})$과 $v_i = E_{ek_{i+1},...,ek_n}(A_i)$ 및 $V_i = V \cup v_i$를 계산한다. 그리고, V_i^{sort}와 $\sigma_i = Sign_{sk_i}(V_i^{sort})$를 e_{i+1}에게 전송한다. 마지막 참가자 e_n은 $Verify_{pk_{n-1}}(\sigma_{n-1},V_{n-1})$을 통한 서명 검증 및 V_{n-1}의 정렬 여부를 검증하고, 검증에 실패하였을 경우 프로토콜 진행을 중지한다. 이후 $V=D_{dk_n}(V_{n-1})$과 $V_n = V \cup A_n$을 계산하고, V_n^{sort}를 공개한다.

모든 $e_i(i=1,...,n)$는 V_n^{sort}에 자신의 수신 주소 A_i가 있는지 검증하고 없을 경우 프로토콜 진행을 중지한다. 검증을 완료하면 자신의 개인키 sk_i를 이용하여 트랜잭션에 서명한다.

3. 제안 방식

본 장에서는 거래의 익명성을 보장하기 위해, 탈중앙화 믹스 기법과 중앙집중화 믹스 기법을 이용한 하이브리드 믹스 기법을 제안한다(그림 3 참조).



(그림 3) 제안한 믹스
(Figure 3) Proposed Mix

제안한 방식은 준비, 참가자 믹스, 검증 및 서버 믹스 단계로 구성되며 자세한 단계별 진행 과정은 다음과 같다.

3.1 1단계(준비)

믹스에 참여할 참가자 $e_i(i=1,...,n)$는 자신의 공개키-개인키 쌍 (pk_i,sk_i)를 가지고 있으며, 임의의 공개키-개인키 쌍 (ek_i,dk_i) 및 자신의 개인키 sk_i를 이용한 서명 $\sigma_i = Sign_{sk_i}(ek_i)$를 생성한 후, (ek_i,σ_i)를 전체 참

가자 그룹 e에게 브로드캐스트한다. 그리고 다른 참가자 $e_j(j=1,..,i-1,i+1,...,n)$가 브로드캐스트한 (ek_j,σ_j) 및 pk_j를 이용하여 $Verify_{pk_j}(\sigma_j,ek_j)$를 실행하여 서명 σ_j를 검증한다. 만약, 검증에 실패하면 프로토콜 진행을 중지한다.

3.2 2단계(참가자 믹스)

참가자 e_1은 $c_1=E_{pk}(A_1)$ 및 $v_1=E_{pk_1}(c_1)$을 계산하고, $V_1=(v_1)$과 $\sigma_1=Sign_{sk_1}(V_1)$을 생성한다. 그리고 $E_{ek_2}(V_1)$과 σ_1을 e_2에게 전송한다(그림 3-① 참조).

e_i는 자신의 개인키 dk_i를 이용하여 V_{i-1}을 획득하고 V_{i-1}의 정렬 여부 검증 및 $Verify_{pk_{i-1}}(\sigma_{i-1},V_{i-1})$을 계산하여 서명을 검증한다. 검증에 성공하면 $c_i=E_{pk}(A_i)$ 및 $v_i=E_{pk_1}(c_i)$를 계산하고, $V_i=V_{i-1}\cup v_i$와 $\sigma_i=Sign_{sk_i}(V_i)$를 생성한다. 그리고 $E_{ek_{i+1}}(V_i^{sort})$와 σ_i를 e_{i+1}에게 전송한다(그림 3-② 참조).

마지막 참가자 e_n은 자신의 개인키 dk_n을 이용하여 V_{n-1}을 획득하고 V_{n-1}의 정렬 여부 검증 및 $Verify_{pk_{n-1}}(\sigma_{n-1},V_{n-1})$을 계산하여 서명을 검증한다. 검증에 성공하면 $c_n=E_{pk}(A_n)$ 및 $v_n=E_{pk_1}(c_n)$을 계산하고 $V_n=V_{n-1}\cup v_n$과 $\sigma_n=Sign_{sk_n}(V_n)$을 생성한다. 그리고 $E_{ek_1}(V_n^{sort})$ 및 σ_n을 e_1에게 전송한다(그림 3-③ 참조).

첫 번째 참가자 e_1은 자신의 개인키 dk_1을 이용하여 V_n을 획득하고 V_n의 정렬 여부 검증 및 $Verify_{pk_n}(\sigma_n,V_n)$을 계산하여 서명을 검증한다. 검증에 성공하면 $i=1,...,n$에 대해 $c_i=D_{sk_1}(v_i)$를 계산하여 새로운 벡터 $c=(c_1,...,c_n)$를 구성하고 c^{sort}를 e에게 브로드캐스트한다.

3.3 3단계(검증)

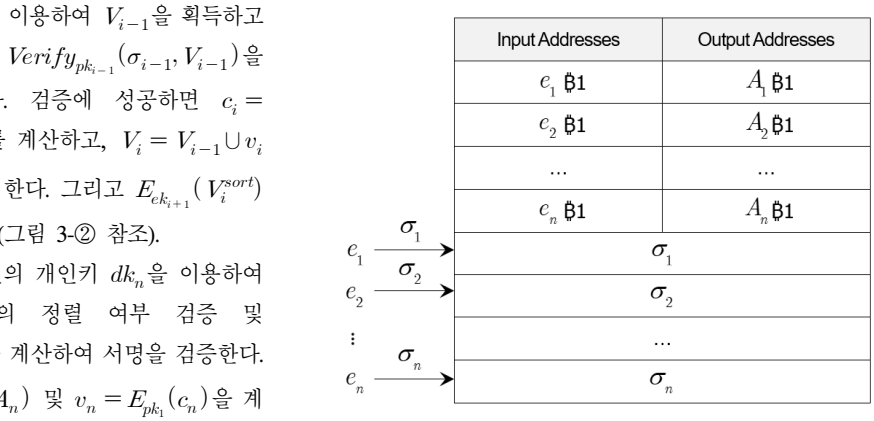
각 참가자 $e_i(i=2,...,n)$는 c^{sort}의 정렬 여부를 검증하고, 자신의 암호문 c_i가 포함되었는지 확인한다. 만약 검증에 실패하거나 자신의 암호문이 없다면 프로토콜 진행을 중지한다.

e_1은 c^{sort}를 믹스 서버 M에게 전송한다(그림 3-④ 참조).

3.4 4단계(서버 믹스)

믹스 서버 M은 $i=1,...,n$에 대해 $A_i=D_{sk}(c_i)$를 획득하고, A^{sort}를 계산하여 e에 브로드캐스트한다. 참가자 $e_i(i=1,...,n)$는 A^{sort}의 정렬 여부 및 자신이 지정한 수신자 주소 A_i가 있는지 검증하고, 검증에 실패할 경우 프로토콜 진행을 중지한다.

검증이 완료되면, 트랜잭션을 구성하고 각 참가자는 자신의 서명을 추가한다(그림 4 참조).



(그림 4) 트랜잭션 구성
(Figure 4) Construction of a Transaction

여기서 주의할 것은 트랜잭션 구성상 e_1이 A_1에게 1을 송금한 것처럼 보이지만, 실제로는 $A_1,...,A_n$ 가운데 하나이고, 이는 e_1만 확인할 수 있다는 점이다.

4. 비교 분석

제안한 방식은 탈중앙화 믹스와 중앙집중화 믹스를 함께 적용함으로써 연산효율 향상 및 익명성을 보장하고 있으며, 믹스서버에 대한 신뢰 가정을 제거하고 있다. 일반적으로 중앙집중화 믹스를 이용할 경우 믹스 서버를 신뢰해야 하지만 제안한 방식에서는 참가자가 직접 믹스 서버로 입력값을 전달하지 않기 때문에 믹스 서버를 신뢰할 필요는 없다. 다만, 기존 중앙집중화 믹스 방식처럼 수수료를 지불해야 할 수도 있다.

본 장에서는 기존 CoinShuffle과 제안한 방식을 안전성

과 효율성 측면에서 비교 분석한다.

4.1 안전성 분석

믹스에서 안전성이란 익명성 보장을 의미하는데, CoinShuffle 방식과 제안한 방식은 동작 과정이 상이하기 때문에 직접적인 비교는 쉽지 않은 측면이 있다.

먼저 CoinShuffle 방식은 최소 2명의 정직한 사용자가 믹스 과정을 수행한다면 익명성을 보장할 수 있다[10]. 즉, 전체 n명의 사용자 가운데 $t(2 \le t \le n)$명이 정직하다면 특정 사용자의 거래를 확인할 확률 $p = 1/t$이 된다.

반면 제안한 방식은 몇가지 경우의 수를 고려해야 하는데, 전체 n명의 사용자 가운데 $t(2 \le t \le n)$명이 정직하다고 가정했을 때, (1) 첫 번째 사용자의 정직성 여부와 (2) 믹스 서버의 정직성 여부가 그것이다.

첫 번째 사용자가 정직하거나 믹스 서버가 정직하다면 특정 사용자의 거래를 확인할 확률 $p = 1/t$이다. 하지만, 첫 번째 사용자와 믹스 서버가 모두 악의적이라면 악의적인 사용자와 정직한 사용자의 배치에 따라 특정 사용자의 거래를 확인할 확률 p는 $1/t \le p \le 1$이 된다. 즉, n명의 사용자중 정직한 사용자가 분산되어 있을수록 확률 p는 커지고, 밀집해 있을수록 작아진다(표 1 참조).

(표 1) 안전성 비교
(Table 1) Comparison Results of Security

	CoinShuffle	제안 방식
정직한 최소 사용자 수 t	$2 \le t$	
거래 확인 확률 p	$p = 1/t$	$p = 1/t^{*}$
		$1/t \le p \le 1^{**}$

* 첫 번째 사용자 또는 믹스 서버가 정직한 경우
** 첫 번째 사용자와 믹스 서버가 모두 악의적인 경우

4.2 효율성 분석

CoinShuffle 방식은 n명의 사용자가 참여할 경우, $n-1$회의 통신이 필요하며, 각 사용자마다 n회의 암/복호화가 필요하다. 따라서, 전체 암/복호화 횟수는 $n^2 - n$이다.

반면 제안한 방식은 n명의 사용자가 참여할 경우, 믹스 서버로의 전송까지 포함하여 모두 $n+1$회의 통신이 필요하며, 각 사용자마다 1회의 암호화 연산 및 첫 번째 사용자의 n회 복호화, 그리고 믹스 서버의 n회 복호화가 필요하다. 따라서, 전체 암/복호화 횟수는 $3n$으로, CoinShuffle 방식보다 우수하다(표 2 참조).

(표 2) 효율성 비교
(Table 2) Comparison Result of Efficiency

	CoinShuffle	제안 방식
통신 횟수	$n-1$	$n+1$
암/복호화 횟수	$n^2 - n$	$3n$

익명성 보장을 위한 믹스의 경우 추가로 고려해야 할 사항으로 참여자 수인데, 일반적으로 참여자의 수에 제한이 없다고 할 수 있지만, 암호화폐 시스템을 고려할 경우 참여자 수가 많아지면 한꺼번에 많은 블록을 처리해야 하는 문제가 있다. 이를 해결하기 위해서는 참여자 수가 일정 기준에 도달하면 믹스를 실행하도록 해야 한다. 적정 참여자 수를 결정하는 것은 추가 연구가 필요하다.

5. 결 론

블록체인에서 거래의 익명성을 보장하기 위한 방법으로 믹스를 많이 이용하고 있다. 믹스는 중앙집중화 믹스와 탈중앙화 믹스로 구분되는데, 중앙집중화 믹스는 연산 효율성은 높지만 믹스 서버를 신뢰해야 하는 문제가 있고, 탈중앙화 믹스는 사용자간 통신 및 연산으로 인한 비효율성이라는 문제가 있다. 본 논문에서는 중앙집중화 믹스 및 탈중앙화 믹스의 장점을 갖는 하이브리드 믹스 방식을 제안하였다. 제안한 방식은 믹스 서버에 대한 신뢰도는 낮추면서 연산 효율성을 높은 특징이 있다. 추후에는 최소한 기존 CoinShuffle과 동등한 안전성(익명성)을 갖도록 개선할 필요가 있다.

참고문헌(Reference)

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash”, https://bitcoin.org/bitcoin.pdf, 2008.
[2] Bitcoin Laundry, “Bitcoin Laundry”, https://bitcoin-laundry.com/, accessed Jun. 24, 2020.
[3] BitMix.biz, “Anonymous Bitcoin Mixer”, https://bitmix.biz/en, accessed Jun. 24, 2020.
[4] Bitcoin.org, “Protect your privacy”, https://bitcoin.org/en/protect-your-privacy, accessed Jul. 3, 2020.
[5] R. Fergal, and M. Harrigan. “An analysis of anonymity in the bitcoin system”, Security and Privacy in Social Networks, pp. 197-223, 2013.

https://doi.org/10.1007/978-1-4614-4139-7_10
[6] M. Möser, “Anonymity of Bitcoin Transactions”, Munster Bitcoin Conference 2013, pp.17-26, 2013. https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf
[7] M. Ober, S. Katzenbeisser and K. Hamacher, “Structure and anonymity of the bitcoin transaction graph”, Future Internet, Vol. 5, No. 2, pp. 237-250, 2013. https://doi.org/10.3390/fi5020237
[8] N. Amarasinghe, X. Boyen, and M. McKague, “A Survey of Anonymity of Cryptocurrencies”, ACSW ’19, pp. 1-10, 2019. https://doi.org/10.1145/3290688.3290693
[9] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for Bitcoin with accountable mixes” International Conference on Financial Cryptography and Data Security, pp. 486-504, 2014. https://doi.org/10.1007/978-3-662-45472-5_31
[10] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin”, ESORICS 2014, LNCS 8713, pp. 345-364, 2014. https://doi.org/10.1007/978-3-319-11212-1_20
[11] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “P2P Mixing and Unlinkable Bitcoin Transactions”, IACR Cryptology ePrint Archive, https://eprint.iacr.org/2016/824.pdf, 2016.
[12] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, Vol. 24, No. 2, 1981. https://doi.org/10.1145/358549.358563

◐ 저 자 소 개 ◑

이 윤 호(Yunho Lee)
1991년 성균관대학교 정보공학과 졸업(학사)
1993년 성균관대학교 정보공학과 졸업(석사)
2008년 성균관대학교 컴퓨터공학과 졸업(박사)
1993년～2000년 한국통신(KT) 연구개발본부 전임연구원
2000년～2005년 KBS인터넷(주) 기술지원팀장
2004년～2005년 ㈜뱅크타운 책임연구원
2008년～2011년 성균관대학교 컴퓨터공학과 연구교수
2011년～현재 광주대학교 사이버보안경찰학과 교수
관심분야 : 전자투표, 컨텐츠보안, 시스템보안, 응용보안 등
E-mail : leeyh@gwangju.ac.kr