Journal of the Korea Convergence Society
Vol. 9. No. 11, pp. 75-81, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.11.075

블록체인 환경에서 보안 기법들의 융합을 통한 프라이버시 및 익명성 강화 기법에 대한 연구

강용혁
극동대학교 글로벌경영학과 교수

A Study on An Enhancement Scheme of Privacy and Anonymity through Convergence of Security Mechanisms in Blockchain Environments

Yong-Hyeog Kang
Professor, Department of Global Business Administration, Far East University

요 약 블록체인 내의 모든 트랜잭션이 공개되기 때문에 익명성과 프라이버시 문제는 중요해지고 있다. 공개 블록체인은 사용자 대신 공개키 주소를 사용하여 익명성을 보장하는 것처럼 보이지만 트랜잭션 그래프를 기반으로 다양한 기법을 통해 추적함으로써 익명성을 약화시킬 수 있다. 본 논문에서는 블록체인 환경에서 익명성과 프라이버스를 보호하기 위하여 다양한 보안 기법을 융합하여 사용자의 추적을 어렵게 하는 기법을 제안한다. 제안 기법은 k-anonymity 기술, 믹싱 기술, 은닉서명, 다단계 기법, 램덤 선택기법, 영지식 증명 기법 등을 융합하여 인센티브 및 기여자의 참여를 통해 익명성과 프라이버시를 보호한다. 성능 분석을 통해 제안기법은 기여자의 수가 공모자의 수보다 많은 환경에서는 공모를 통한 프라이버시 및 익명성 훼손이 어렵다는 것을 보였다.

주제어 : 융합, 믹싱 기술, 은닉 서명, K-익명성, 영지식 증명

Abstract Anonymity and privacy issues are becoming important as all transactions in the blockchain are open to users. Public blockchains appear to guarantee anonymity by using public-key addresses on behalf of users, but they can weaken anonymity by tracking with various analytic techniques based on transaction graph. In this paper, we propose a scheme to protect anonymity and privacy by converging various security techniques such as k-anonymity, mixing, blind signature, multi-phase processing, random selection, and zero-knowledge proof techniques with incentive mechanism and contributor participation. Through performance analysis, our proposed scheme shows that it is difficult to invade privacy and anonymity through collusion attacks if the number of contributors is larger than that of conspirators.

Key Words : Convergence, Mixing scheme, Blind signature, K-anonymity, Zero-knowledge proof

1. 서론

블록체인은 암호화폐(cryptocurrency) 트랜잭션(transaction)에 대한 디지털화되고 비집중화되고 공개된 원장(ledger)이다[1]. 블록체인 내의 트랜잭션은 시간 순서적으로 문서화되며 참여자들에게 중앙 기록을 유지하

*This work was supported by the 2018Far East University Research Grant(FEU2018R03)
*Corresponding Author : Yong-Hyeog Kang (yhkang@kdu.ac.kr)
Received September 15, 2018 Revised November 2, 2018
Accepted November 20, 2018 Published November 28, 2018

지 않고 디지털 화폐를 추적할 수 있도록 도와준다. 이러한 트랜잭션은 공개키 암호 기법에 의해 디지털적으로 서명되지만, 공개키 기반 디지털 서명 기법은 사용자의 프라이버시(privacy)와 익명성(anonymity)을 침해하는 단점을 갖고 있으며, 부가적인 정보의 사용은 사용자의 프라이버시에 큰 위협이 될 수 있다[2].

기존 은행 시스템은 신뢰할 수 있는 제3자를 포함하여 다른 사용자에게 트랜잭션의 정보를 제한함으로서 프라이버시 레벨을 제공하고 있다. 비트코인(Bitcoin)과 같은 공개 블록체인 기술은 모든 트랜잭션의 정보를 네트워크에 연결된 사용자에게 노출시키고 있으나, 공개키를 익명으로 하여 프라이버시는 어느 정도 레벨까지는 유지하고 있다. 하지만, 여러 분석 기법을 통해 연결성은 노출되고 키의 소유자는 노출 될 수 있으며, 키의 소유자가 노출되면 동일한 사용자에게 속하는 다른 트랜잭션도 노출될 수 있다[3].

익명성과 프라이버시는 차이점이 있다. 익명성은 컨텍스트(context)의 소유를 숨기는 것이고, 프라이버시는 컨텍스트의 내용을 숨기는 것이다[4]. 익명성보다는 프라이버시가 더 많이 추구된다. 왜냐하면 e-mail 주소는 알려줘도 e-mail의 내용은 숨겨야하기 때문이다. 프라이버시는 대부분의 시스템과 응용에서 필요하지만, 익명성은 무기명 투표나 여론 조사 등에서는 필요하지만 주로 범죄자들이 추구하는 것이다[4]. 블록체인 내에서의 프라이버시는 식별자 정보의 누출없이 트랜잭션을 수행할 수 있음을 의미한다[1]. 이는 공개키 익명성으로 공개키는 공개하지만 트랜잭션의 소유자가 누구인지 모르게 하는 것으로 공개키의 소유자가 실제로 누구인지 모르게 하는 것이다. 본 논문에서는 프라이버시를 공개키 익명성으로 보고 익명성과 혼용하여 사용한다.

블록체인 기술은 암호화폐뿐만 아니라 저작권 보호 및 인증 등 다양한 응용에 적용될 수 있다[5-7]. 이러한 응용에는 사물인터넷이나 마켓 플랫폼에도 적용되고 있으며 프라이버시 관리나 생체정보를 이용한 인증 기법에도 적용되고 있다[8-11]. 응용 기술에 대한 블록체인 기술의 활용은 프라이버시와 익명성에 대한 요구사항을 증가시키며 사용자들에게 프라이버시와 익명성에 대한 만족할만한 수준의 서비스를 제공을 요구하고 있다[2]. 본 논문에서는 이러한 익명성과 프라이버시 문제를 다양한 보안 기법을 융합하여 해결하는 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서 관련연구를 설명하고 3장에서 제안기법을 설명하고 4장에서 성능을 분석하고 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 관련연구

비트코인에서 완전한 익명성은 복잡한 문제이다[2]. 트랜잭션의 익명성을 강화하기 위해서 다수의 비트코인 주소(address)들을 생성하는 것을 허용한다. 다수의 주소를 사용하면 공격자는 1대N 매핑을 구성해야 하지만, 공개 블록체인을 분석함으로써 프라이버시를 약화시킬 수 있다. 블록체인의 분석은 우선 다음과 같은 세 가지 그래프를 만든 후 수행된다. 트랜잭션 그래프는 전제 블록체인을 비순환(acyclic) 트랜잭션 그래프 G_t={T, E_t}로 본다. 여기서 T는 블록체인 내에 포함된 트랜잭션의 집합이며 E_t는 이러한 트랜잭션들 간의 무방향 선분들의 집합이다. 주소 그래프(는 트랜잭션 그래프를 탐색함으로써 다양한 입력과 출력 주소간의 관계를 쉽게 추론할 수 있으며 이를 통해 주소 그래프 G_p={P, E_p}을 생성한다. 여기서 P는 주소들의 집합이며, E_p은 이러한 주소들을 연결하는 선분이다. 사용자/엔터티(user/entity) 그래프는 주소 그래프를 분석하여 동일한 사용자에 속하는 것처럼 보이는 주소들을 묶음으로써 사용자/엔터티 그래프 G_u={U, E_u}를 작성한다. 여기서 U는 주소들의 집합이며, E_u은 이러한 주소들을 연결하는 선분이다[2].

블록체인의 분석은 두 가지의 휴리스틱 기법을 사용한다[12]. 첫 번째는 트랜잭션의 모든 입력은 동일한 사용자에 의해 생성된다는 가정이다. 왜냐하면 실제적으로 사용자는 다른 사용자의 트랜잭션에 거의 참여를 하지 않기 때문이다. 이 규칙은 또한 전이 클로저(transitive closure)를 적용할 수 있어서 트랜잭션 그래프에 적용하여 비트 코인 주소들에 대한 묶음을 생성할 수 있다. 두 번째는 입력 주소와 출력 주소를 연결할 수 있다. 왜냐하면 출력에 있는 주소가 완전히 새로운 주소이면 새로운 주소는 잔돈(change) 주소로 가정할 수 있기 때문이다[2]. 또한, 실세계 식별자를 이용하여 주소 클러스터를 연결 할 수 있다. 이러한 엔터티와 다수의 상호작용을 하는 온라인 지갑, 중개자, 다른 서비스 제공자를 이용하여 높은 정밀도를 가지고 클러스터들의 연결을 수행한다. 최근에는 사용자가 암호화폐를 이용하여 구매를 하게 되면 공격자는 구매에 대한 충분한 정보를 가진 제3자 트래커

를 이용하여 트랜잭션을 유일하게 식별할 수 있다. 이러한 구매 트랜잭션은 사용자 쿠키(cookies)와 연결될 수 있고 사용자의 실제 식별자와 구매 내역까지 노출될 수 있다. 네트워크 비익명화도 사용될 수 있다. 왜냐하면 트랜잭션의 내용이 모든 참여자에게 브로드캐스트되기 때문에 IP 주소와 P2P 네트워크 상의 사용자가 연결될 수 있기 때문이다[2].

프라이버시 취약점들이 나오게 되면서 비트코인의 기본적인 설계원리를 깨지 않고 프라이버시를 강화하고 익명성을 향상시키는 기법들이 제안되었다[2]. 현재 프라이버시를 강화하는 제안기법들을 분류하면 세 가지 유형으로 분류할 수 있다.

- P2P 믹싱(mixing) 프로토콜
- 분산(Distributed) 믹싱 네트워크
- 비트코인 확장 또는 Altcoin

믹싱 시스템은 익명성 서비스 제공자로서 트랜잭션의 추적을 어렵게 하는 믹싱 프로토콜을 사용한다. 믹싱 과정에서 클라이언트 자금은 작은 부분으로 램덤으로 나누어지며 다른 클라이언트 자금의 작은 부분과 램덤으로 섞이며 결과적으로 새로운 코인을 생성하게 된다. 이것은 사용자와 코인과의 연결을 깨뜨림으로써 익명성과 비연결성을 강화한다. P2P 믹싱 프로토콜[13,14]에서는 사용자 집합이 동시에 메시지를 브로드캐스트하여 신뢰있는 제3자 없이 일련의 트랜잭션을 만든다. 이 기법은 보내는 자의 익명을 차명자의 집합 속에 코인의 소유권을 혼합함으로써 익명성을 보장한다. 익명성의 차수(degree)는 익명성 집합의 사용자 수에 의존한다. CodeJoin 기법이 대표적이다[15]. 하지만, 믹싱 집합에 있는 참여자들이 서명을 관리할 필요에 의해서 제한적 확장성(scalability)과 프라이버시 내부 누출 문제, DoS 공격에 취약한 단점이 있으며 이러한 단점을 해결하기 위한 기법들이 많이 제안되었다[2].

분산 믹싱 네트워크는 익명 지불이 가능한 제 3자 믹싱 프로토콜을 사용한다[2]. 대표적으로 MixCoin기법은 평판(reputation) 기반 암호화 회계 책임(accountability) 기법으로 다른 사용자가 절도나 프로토콜을 혼란시키는 것을 방지한다[16]. MixCoin은 표준 크기의 트랜잭션을 이용하여 제 3자 믹싱 시스템을 통해 자금을 송수신한다. 이 기법의 단점은 믹싱 시스템이 사용자의 자금을 훔칠 수 있으며 사용자와 출력사이의 내부 매핑을 알 수 있기 때문에 익명성에 위협이 된다. 이러한 문제를 해결하기 위해 MixCoin을 확장한 BlindCoin 기법은 은닉 서명(blind signature)[17]을 통해 익명성을 강화한다[18].

비트코인은 사실상의 표준이지만 비트코인으로 파생되어 생성된 다른 코인도 있으며 알트코인(altcoin)이라고 한다. 대표적인 것은 ZeroCoin 기법이다[19]. 완전히 암호화된 트랜잭션을 수행하는 영지식(zero-knowledge) 기법을 이용하여 익명성을 제공하는 비트코인의 확장형이다. 사용자는 코인에 대한 추적 문제를 완전히 해결할 수 있다. 왜냐하면 전송되는 화폐의 양과 수혜자 주소 등의 트랜잭션의 추가적인 정보가 숨겨지기 때문이다. 대표적인 기법은 zk-SNARK 프로토콜을 사용하는 zeroCash이며 ZeroCoin 기법의 확장형이며 zCash로 알려져 있다[20]. 이 기법의 단점은 기존 암호화폐 시스템과의 호환성 문제이다.

3. 제안기법

본 논문에서 제안하는 기법은 믹싱 기법과 기여자들의 기여와 k-anonymity 기법[21]과 다중 단계(multi-phase) 처리 기법을 융합하여 사용한다. 본 논문에서 제안하는 기법의 설계 원리는 다음과 같다.

- 사용자가 보안 레벨을 설정할 수 있다.
- 기여자는 기여에 따른 인센티브를 받고 사용자는 보안 레벨에 따른 수수료를 낸다.
- 여러 단계에 걸쳐서 수행할 수 있다.
- 기존 기법과 호환가능하다.

첫 번째 원리는 사용자는 익명성의 보안 레벨을 k-anonymity와 n-phase로 설정할 수 있다는 것이다. k-anonymity는 믹싱 기법을 통해 공격자가 k개의 정보를 가지기 전까지 익명성을 보장하는 기법이다[22]. 또한 n-phase 기법은 입력과 출력을 다단계로 구성하여 추적성을 어렵게 한다. 두 번째 원리는 k-anonymity를 위해 불특정 다수의 기여자를 모집하고 기여자에게 인센티브를 줌으로써 익명성 보장하는 기법이다. 익명성을 위해 사용자에게는 수수료를 받고 기여자에게는 인센티브를 부여하는 방식으로 다수의 공격자가 공모하는 것을 방지하는 방식이다. 세 번째 원리는 단일 단계에서만 수행할 경우 입력과 출력 매핑이 용이하여 여러 단계를 수행함으로써 익명성을 높이는 기법이다. 네 번째 원리는 이러한 트랜잭션을 기존 블록체인 시스템으로 전환하여 수행함으로써 기존 기법 위에서 동작하는 방식이다.

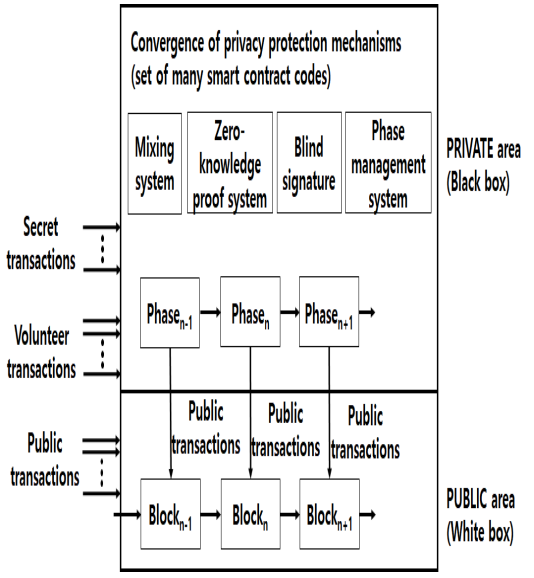

Fig. 1. Conceptual model of our proposed scheme

Fig. 1은 본 논문에서 제안하는 기법의 개념도이다. 비공개(private) 영역에서는 프라이버시를 보장하기 위한 영역이며 공개(public) 영역은 기존 블록체인의 영역이다. 블록체인 사용자들은 세 가지 유형의 트랜잭션을 블록체인 시스템에 생성시킬 수 있다.

- 일반 트랜잭션
- 비밀 트랜잭션
- 기여자 트랜잭션

일반 트랜잭션은 기존 블록체인 시스템에 포함되는 트랜잭션과 동일한 트랜잭션으로 제안 기법과 상관없이 동작하는 트랜잭션이며 비밀 트랜잭션은 익명성과 프라이버시가 필요한 트랜잭션으로 수수료를 지불하는 트랜잭션이며, 기여자 트랜잭션은 일반 트랜잭션 기능 외에 비밀 트랜잭션의 수수료를 얻을 수 있도록 비공개 영역에 참여하는 트랜잭션이다. 이 트랜잭션은 비공개 영역의 참여를 마치면 공개 영역의 트랜잭션으로 변환된다.

제안기법은 또한 추적을 어렵게 하기 위해 여러 단계를 거쳐 트랜잭션을 수행할 수 있도록 한다. 각 단계는 Fig. 2와 같이 구성된다. 입력 시스템이 있으며 출력 시스템도 있다. 믹싱을 처리하는 컴포넌트와 비호환(non-compatible) 트랜잭션으로 변환되는 작업을 하는 영지식 증명을 위한 컴포넌트도 있다. 입력은 임의의 단계에서 가능하지만 입력조건이 맞을 경우 시스템 안으로 들어가며 비밀 트랜잭션의 조건이 맞지 않거나 기여자의 조건이 맞지 않을 경우 해당 트랜잭션은 입력시스템에서 조건이 만족할 때까지 대기한다. 출력은 기여자의 기여를 만족하거나 보안레벨이 만족할 때는 공개 영역 트랜잭션으로 변환되어 공개 영역으로 출력되며 만족되지 않았을 때에는 다음 단계로 넘어간다.

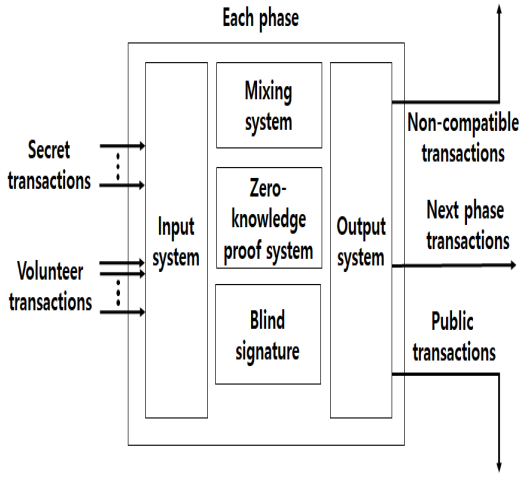

Fig. 2. Each phase of private area

믹싱 기법은 일반적으로 믹싱에 참여하는 트랜잭션들이 동일한 양의 금액을 수행하며 공개된 송신주소와 공개된 수신주소와의 매핑을 혼합시키는 방식이다. 동일한 금액을 쓰지 않으면 금액을 통해 송신과 수신주소의 매핑관계를 추적할 수 있다. 제안기법은 여러 출력 주소를 이용하여 여러 단계로 금액을 나눠서 전송하는 방식을 제안한다. 이렇게 함으로써 동일한 금액을 써야하는 믹싱 기법의 단점을 극복한다. 제안기법에서는 믹싱 기법에 은닉 서명 기법이나 공정한 교환(fair exchange) 기법을 사용하여 입력 주소와 출력주소와의 관계를 믹싱 시스템 내에서도 모르게 하는 숨겨진 주소 섞기(hidden address shuffling)[4] 기법도 사용한다.

공개 블록체인에 저장하는 방식은 믹싱시스템에 입력과 출력에 쓰이는 임의의 주소 $Addr_m$를 만들어서 다음과 같이 수행된다. 한 개의 트랜잭션은 송신자에서 이 믹싱 시스템의 주소로 전달하는 트랜잭션과 이 믹싱 시스템의 $Addr_m$에서 수신자에게 전달하는 트랜잭션으로 구성되어 공개 블록체인에 저장된다. 인센티브는 보안성을 높이는 기여자에게 기여도에 따라 부여한다. 기여자 트랜잭션이 송신자와 수신자 목록이 많으면 여러 단계로 동작할 수

있으므로 추적이 더 어려워지며, 기여자 트랜잭션의 송금액이 현재 거래되는 평균보다 너무 크거나 작지 않으면 추적을 어렵게 할 수 있다. 기여 정도에 따라 보안 트랜잭션들의 보안 수수료를 규칙없이 램덤하게 각 단계별로 배분함으로써 금액을 통한 추적을 어렵게 한다.

기여자 트랜잭션과 비밀 트랜잭션을 실행시킬 사용자는 트랜잭션을 생성할 때 비공개되는 정보를 부가적으로 가지고 있다. 비공개되는 부가적인 정보는 익명성과 프라이버시를 위한 것이며 암호화하여 트랜잭션 생성 시에 부가적으로 트랜잭션에 저장한다. 공통으로 비공개되는 정보는 다음과 같다.

- 수행 단계
- 송신자 목록
- 송금 금액
- 수신자 목록

수행단계는 여러 단계를 거쳐서 수행함으로써 추적성을 어렵게 하기 사용된다. 기여자의 단계는 장단점이 있다. 기여자의 단계를 길게 하면 악의적인 의도로 사용하여 익명성의 보안성을 떨어뜨릴 가능성이 높아지지만, 악의적인 의도가 아닌 경우 보안성을 높이는 데 더 많은 기여가 된다. 송신자의 목록과 수신자의 목록도 같은 특성을 갖는다. 일반적으로는 보안성을 높이는 역할을 하지만, 악의적인 의도로 사용될 경우에는 보안성을 떨어뜨리게 된다.

비밀 트랜잭션은 추가적으로 다음과 같은 정보도 트랜잭션의 부가정보로 저장한다.

- 보안 레벨
- 각 단계마다 지불하는 보안 수수료

보안 레벨은 k-anonymity와 관련된 레벨로 시스템에 보안 레벨의 수만큼의 비밀 트랜잭션과 기여자 트랜잭션이 참여해야 한다는 요구조건이다. 각 단계마다 지불하는 보안 수수료는 한 단계를 거칠 때마다 제공하는 보안 수수료이다. 단계마다 수수료를 지불하는 이유는 수수료를 분석하여 트랜잭션을 추적하는 것을 방지하기 위함이다.

A 사용자가 B 사용자에게 임의의 크기의 금액 m을 보내는 비밀 트랜잭션을 실행하고자 하는 경우, A는 이 내용을 보안 레벨과 수수료 등을 설정하여 블랙박스에 스마트 계약(smart contract)[23] 형식으로 삽입한다. 스마트 계약 형식으로 삽입하는 이유는 조건이 맞을 경우 실행되게 한다는 의미이다. A도 여러 개의 주소를 이용하여 전송 가능하며 B도 여러 개의 주소를 사용하여 수신 가능하다. 기여자 C가 D 사용자는 임의의 크기의 금액 n을 D 사용자에게 보내는 기여자 트랜잭션의 경우도 마찬가지이다. C는 이러한 내용을 설정하여 스마트계약 형식으로 블랙박스에 삽입한다. 이 경우에도 여러 개의 송신자 및 수신자가 사용될 수 있다.

믹싱시스템에서는 이러한 비밀 트랜잭션과 기여자 트랜잭션 등이 스마트계약 형식으로 들어왔기 때문에 해당 조건이 맞을 경우 실행하게 된다. 블랙박스 안에서 트랜잭션 등이 믹싱될 때 보안 트랜잭션이 제공하는 수수료는 기여자 트랜잭션들에게 보안도 기여에 따라 분배된다. 분배방식도 균등하게 하는 것이 아니라 램덤하게 하여 추적을 어렵게 한다. 블랙박스에서는 인센티브를 이용하여 기여자들의 참여를 유도하여 보안도를 높인다.

보안 트랜잭션 및 기여자 트랜잭션이 여러 단계를 가질 경우 해당 단계가 끝나면 출력할 때 단계값을 1씩 감소시키고 다음 단계로 넘어간다. 이런 방식으로 각 단계마다 재진입하고 출력하는 과정을 반복한다. 단계값이 0이 되면 출력한다.

4. 제안기법의 성능 분석

본 논문에서 제안한 기법의 보안 성능을 분석한다. 제안기법은 k-anonymity 기법을 사용하였으므로 k개의 공모자가 있기 전까지는 추적되지 않는다. 본 논문에서는 보안도 측정방법을 송신자와 수신자의 연결성을 찾을 확률로 평가한다. 기여자가 $l(l>k)$명 믹싱 시스템에 같이 참여할 경우 공모자의 수에 따른 추적의 성공 확률을 구해보면 Table 1과 같다.

Table 1. Probability of traceability according to number of conspirators

Conspirators \ Phases	1	2	…	p
0	$1/l$	$1/(2\times l)$	…	$1/(p\times l)$
1	$1/(l-1)$	$1/(2\times(l-1))$	…	$1/(p\times(l-1)$
2	$1/(l-2)$	$1/(2\times(l-2))$	…	$1/(p\times(l-2)$
…	…	…	…	…
$l/2$	$2/l$	$1/l$	…	$2/(p\times l)$

공모자가 없는 경우에는 $1/l$이 되며 단계가 p인 경우

추적의 성공확률은 더욱 낮아져서 $1/(l*p)$이 된다. 이 값은 단계가 한 개인 경우보다 여러 단계를 두는 것이 추적 확률이 p배 작아지게 되어 추적의 어려움은 기존 기법보다 제안기법이 p배 높은 성능을 가짐을 알 수 있다.

여러 기여자가 공모하여 추적하는 위협도 있을 수 있다. 공모자가 많아질수록 추적가능성은 그만큼 높아지지만 제안기법에서는 기여자를 랜덤으로 선택하기 때문에 기여자의 수가 공모자의 수보다 많은 경우에는 공모자의 수를 기여자의 1/2 이상으로 올리기는 어렵다. 공모자가 기여자의 1/2인 경우에 추적가능성을 평가하면 $1/(l/2)$이 되며 이 값은 $2/l$이므로 추적 확률은 공모자가 없는 경우의 2배 만큼만 늘어나게 된다. 즉, 기여자가 공모자보다 많고 l값이 충분히 클 경우 공모자가 많더라도 추적 확률이 크게 높아지지 않음을 알 수 있다.

금액을 이용하여 추적하는 경우를 고려하면 다음과 같다. 레벨이 l이고 단계가 p인 경우 출력되는 수신 값들은 약 $p\times l$ 개의 숫자들 중에서 매칭을 구하는 문제로 귀결된다. 왜냐하면 단계가 1개인 경우는 현재 단계의 레벨 값인 l_c개의 값에서 구하며 단계가 2인 경우에는 이전 단계의 레벨의 수인 l_{c-1}개의 값들이 다음 단계에 포함되게 되어 약 $l_{c-1}+l_c$개의 값에서 매칭을 구하여야 한다. 이 값을 단순하게 $2\times l$로 가정하면 단계가 p인 경우 $p\times l$ 개의 숫자에서 매칭을 구하는 것이 된다. Table 2는 금액을 이용한 추적 확률을 구하기 위해 단계의 수와 인센티브의 숫자에 따른 추적의 성공 확률을 구하였다.

Table 2. Probability of traceability by using quantities of money according to number of incentives

Phases / Incentives	1	2	…	p
0	l/l	$l/(2\times l)$	…	$1/(p\times l)$
1	$(l-1)/l$	$(l-2\times1)/(2\times l)$	…	$(l-p\times1)/(p\times l)$
2	$(l-2)/l$	$(l-2\times2)/(2\times l)$	…	$(l-p\times2)/(p\times l)$
…	…	…	…	…
l/p	$(1-l/p)/l$	…	…	0
…	…	…	…	0
$l/2$	1/2	0	0	0
…	…	0	0	0
$l-1$	$1/l$	0	0	0
l	0	0	0	0

단계가 1이고 인센티브가 0인 경우 입력 l개의 값이 출력 l개의 값이 되며 l개 모두 서로 다른 값인 경우 추적 확률은 l/l이 되어 모두 찾을 수 있는 1이 된다. 인센티브의 개수가 1개인 경우 1개의 값이 변경되어 $l-1$개의 값은 찾을 수 있어서 추적 확률은 $(l-1)/l$이 된다. 단계가 2인 경우에는 $2\times l$개에서 찾아야 하며 입력된 l개의 서로 다른 값을 가지고 숫자 분할 연산 수식 결과를 최대한 분석하여 변경된 l개의 값을 구분할 수 있다고 가정하면 추적 확률은 $l/(2\times l)$이 된다. 인센티브의 개수가 1개인 경우 이 값은 2단계에 걸쳐서 영향을 주기 때문에 구분할 수 있는 숫자의 개수는 전체 개수에서 l에서 2를 뺀 $l-2\times1$이 된다. 결과에서 보듯이 서로 다른 금액에 적용되는 인센티브의 개수가 많을수록 그리고 단계가 많을수록 추적 확률은 작아지게 된다. 특히 단계가 p인 경우 인센티브의 개수가 l/p인 경우 추적 확률은 0이 된다.

5. 결론 및 향후 연구과제

공개 블록체인의 내부에 있는 모든 트랜잭션이 공개되기 때문에 프라이버시 문제와 익명성 문제가 중요해지고 있다. 본 논문에서는 믹싱 기법과 기여자들의 기여와 k-anonymity 기법과 다중 단계(multi-phase) 처리 기법 등 다양한 보안 기법을 융합하여 블록체인 환경에서 사용자의 프라이버시 및 익명성을 강화하는 기법을 제안하였다. 성능 분석을 통해 기여자가 공모자보다 많을 때에는 프라이버시 침해가 어렵다는 것을 보였다. 또한, 제약조건이 있지만 금액을 이용하여 추적할 수 있는 가능성도 평가하였다. 기여자의 수가 많고 단계가 많을 경우 추적 확률은 작아짐을 보였다.

향후 연구과제로는 제안기법을 시뮬레이션을 통해 보다 일반적인 환경에서 성능 평가를 수행하는 것이며, 다양한 보안 취약성을 분석하는 것이다. 또한, 분석된 보안 취약성을 제거할 수 있도록 제안기법을 상세화하여 실제 스마트 계약이 동작하는 환경에서 실행 코드를 제작하여 동작하도록 구현하는 것이다.

REFERENCES

[1] A. P. Joshi, M. Han & Y. Wang. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing, 1(2),* 121-147.

[2] M. Conti, S. K. E, C. Lal & S. Ruj. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials.*

DOI : 10.1109/COMST.2018.2842460

[3] P. Frandco. (2015). *Understanding BitCoin: Cryptography, Engineering and Economics*. John Wiley & Sons.

[4] M. C. K. Khalilov & A. Levi. (2018). A survey on anonymity and privacy in Bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials. 20(3),* 2543-2585.

[5] E. M. Lee. (2018). A Research on Blockchain- based Copyright Protection for Computational Creativity. *Journal of the Korea Convergence Society,* 9(9), 23-29.

[6] S. T. Kim. (2018). Analysis on Consensus Algorithms of Blockchain and Attacks. *Journal of the Korea Convergence Society,* 9(9), 83-88.

[7] Y. J. Lee & S. H. Lee. (2018). Efficient RBAC based on Block Chain for Entities in Smart Factory. *Journal of the Korea Convergence Society,* 9(7), 69-75.

[8] I. G. Lee. (2018). A Study on Blockchain Networking for Internet of Things. *Journal of Digital Convergence*, 16(8), 201-210.

[9] K. N. Lee & G. H. Jeon. (2018). A Study on Improvement of Used-goods Market Platform Using Blockchain. *Journal of Digital Convergence*, 16(9), 133-145.

[10] Y. S. Jeong, Y. T. Kim, & G. C. Park. (2018). User Privacy management model using multiple group factor based on Block chain. *Journal of Convergence for Information Technology*, 8(5), 107-113.

[11] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology*, 8(3), 85-90.

[12] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, & S. Capkun. (2013). Evaluating user privacy in bitcoin. *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer Berlin Heidelberg.

[13] M. H. Ibrahim. (2017). Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem. *International Journal of Network Security,* 19(2), 295-312.

[14] T. Ruffing, P. Moreno-Sanchez, & A. Kate. (2014). Coinshuffle: Practical decentralized coin mixing for bitcoin. *19th European Symposium on Research in Computer Security* (pp. 345-364). Springer International Publishing.

[15] G. Maxwell. (2013). *CoinJoin: Bitcoin privacy for the real world.* Bitcoin Forum. https://bitcointalk.org/index.php?topic=279249.0.

[16] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, & E. W. Felten. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. *International Conference on Financial Cryptography and Data Security* (pp. 486 - 504). Springer Berlin Heidelberg.

[17] D. Chaum. (1983). Blind signatures for untraceable payments. *Advances in Cryptology: Proceedings of Crypto 82* (pp. 199 - 203). Springer.

[18] L. Valenta & B. Rowan. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. *International Conference on Financial Cryptography and Data Security.* (pp. 112-126). Springer Berlin Heidelberg.

[19] I. Miers, C. Garman, M. Green, & A. D. Rubin. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *IEEE Symposium on Security and Privacy.* (pp. 397-411). IEEE Computer Society.

[20] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, & M. Virza. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE Computer Society.

[21] L. Sweeney. (2002). k-Anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5),* 557-570.

[22] G. Zyskind, O. Nathan, & A. Pentland. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Symposium on Security and Privacy Workshops* (pp. 180 - 184). IEEE Computer Society.

[23] E. Heilman, F. Baldimtsi, & S. Goldberg. (2016). Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN'16* (pp. 43-60). Springer Berlin Heidelberg.

강 용 혁(Kang, Yong-Hyeog) [정회원]

- 1998년 2월 : 성균관대학교 정보공학과(공학석사)
- 2003년 8월 : 성균관대학교 전기전자및컴퓨터공학과(공학박사)
- 2003년 3월 ~ 현재 : 극동대학교 글로벌경영학과 교수

- 관심분야 : 분산컴퓨팅, 사물인터넷, 보안컴퓨팅
- E-Mail : yhkang@kdu.ac.kr