정 보 보 호 학 회 지
제28권 제3호, 2018. 6

비트코인 익명화 기술 연구 동향

홍 영 기*, 허 준 범**

요 약

세계적 열풍의 중심인 비트코인에는 많은 이슈가 발생하고 있다. 특히 비트코인의 익명성은 사회적으로 중요한 문제이다. 비트코인이 익명성을 보장하지 못할 경우 거래내역이 공개되어 프라이버시가 노출될 수 있다. 반대로 비트코인이 익명성을 보장할 경우 마약 거래, 자금 세탁, 랜섬웨어 공격 등의 각종 범죄가 발생할 수 있다. 이밖에도 다양한 상황에 적절한 대처를 하기 위해서는 비트코인 기술에 대한 정리와 이해가 필요하다. 본 논문에서는 비트코인의 익명성을 약화시키는 클러스터링 기술과, 비트코인의 익명성을 강화시키는 믹싱 프로토콜 기술에 대한 연구 흐름을 정리하였다.

Ⅰ. 서 론

비트코인은 2008년 사토시 나카모토의 논문에서 제안된 암호 화폐이다. 비트코인은 현재 암호화폐의 대명사로 사용되고 있으며, 시가 총액은 150조에 육박한다. 비트코인 트랜잭션은 누구나 생성이 가능하고, 발행된 트랜잭션은 P2P 네트워크를 통해 전파된다. 전파된 트랜잭션은 마이너들에 의해 검증되고, proof-of-work 시스템을 통해 합의되어 블록체인에 저장된다. 블록은 평균 10분에 한 개씩 생성되도록 난이도가 조정되며, 현재 524119 개의 블록이 블록체인에 저장되어 있다. (2018-05-24 기준)

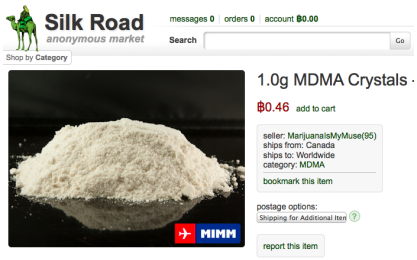
비트코인은 초창기에 익명성을 가진 암호화폐로 알려졌다. 비트코인은 분산된 네트워크 시스템이며, 중앙 통제 기관이 없기 때문이다. 즉, 은행에서 발급하는 통장의 경우 계좌번호와 연결된 주민번호 등의 개인정보가 저장되어 있는 반면, 비트코인 주소는 암호 알고리즘을 통해 무작위로 생성되며 주소 자체에 어떠한 정보도 저장되어 있지 않다. 또한 비트코인 주소는 1회용이기 때문에 새로운 주소가 매 거래마다 생성되며, 누구나 언제든지 제약 없이 새로운 주소를 생성할 수 있다. 따라서 비트코인 주소 자체로 사용자를 식별하기는 쉽지 않다.

하지만 비트코인은 주소를 가명으로 활용할 뿐 익명성을 보이지 않는다. 모든 거래내역이 공개되어 있어서 누구나 거래 흐름분석이 가능하며, 이는 블록체인에 클러스터링 기술을 적용할 경우 비익명화 공격의 성능을 비약적으로 증가시킬 수 있다. 또한 대부분 비트코인을 구매하기 위해 중개거래소를 이용하는데, 중개 거래소는 고객 파악 정책(KYC, Know Your Customer)을 가지고 있기 때문에 비트코인 구매를 위해 핸드폰 또는 계좌 인증이 필수적이다. 추가로 최근 정부에서 '가상통화 거래실명제'를 도입하여, 실명 인증이 더욱 강화되었다. 마지막으로 트랜잭션을 생성한 IP 주소를 이용하여 비익명화 공격을 시도한 연구들이 있다 [8-10].

결과적으로 비트코인은 완전한 익명성을 보장하지 못한다. 비트코인이 화폐의 기능을 수행할 때 익명성이 없을 경우 다음과 같은 문제들이 있다. 비트코인으로 월급을 나누어준다고 가정했을 때, 모두의 월급이 얼마인지 구체적으로 알 수 있게 될 것이다. 또한 비트코인을 이용한 익명의 기부도 불가능하다. 비트코인으로 사적으로 알려지고 싶지 않은 물건을 구매하지 못할 것이며, 부채 이자, 등의 내역도 투명하게 공개될 것이다.

이러한 부족한 익명성을 개선하고자 트랜잭션을 섞어 거래 흐름 추적을 어렵게 하는 믹싱 서비스가 등장했다. 먼저 믹싱 서비스란, 제 3의 엔티티가 여러 사용자들로부터 비트코인을 받은 뒤 트랜잭션을 혼합하여 돌려준다. 결과적으로 입력과 출력의 상관관계를 낮춤

이 논문은 2018년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00269, 개인정보를 안전하고 편리하게 빅데이터 처리할 수 있는 방법)
* 고려대학교 컴퓨터학과 정보시스템보안연구실 (gee308@korea.ac.kr)
** 교신저자, 고려대학교 컴퓨터학과 정보시스템보안연구실 (jbhur@korea.ac.kr)



〔그림 1〕 비트코인 마약 거래

으로서 믹싱 기능을 수행한다. 하지만 믹싱 서비스가 돈을 절도할 가능성이 있으며, 믹싱 서비스는 누가 누구에게 비트코인을 보냈는지 알고 있다는 단점이 있다. 이는 법 집행기관을 통해 수사를 진행할 경우 노출이 될 가능성이 있다. 이러한 단점을 개선하고자 비트코인을 익명 암호화폐로 만들어주는 믹싱 프로토콜 [11-17] 연구가 있다.

하지만 비트코인의 익명성은 양날의 검과 같다. 비트코인이 익명성을 보장할 경우 마약 거래, 자금 세탁, 탈세 등 각종 범죄에 비트코인이 이용될 수 있다. 실제로 과거에 실크 로드 등의 다크웹 사이트에서 비트코인을 지불 수단으로 마약 거래가 활발하게 이루어졌다. 또한 최근 랜섬웨어 공격들은 사용자의 컴퓨터를 암호화한 뒤, 복호화를 원할 경우 비트코인 송금을 요구했다. 이처럼 비트코인의 익명성에 관련된 문제는 세계적으로 발생하고 있기 때문에 분석하여 정리할 필요가 있다. 하지만 비트코인 연구는 빠르게 발전하며 새로운 정보가 계속해서 생성되고 있어 정리하는데 어려움이 있다.

본 연구는 비트코인 익명성 관련 연구에 대해 살펴본다. 본 논문 2장에서는 먼저 어떤 주소와 관련된 주소 목록을 그룹화 하는 클러스터링 연구에 대해 정리한다. 3장에서는 비트코인을 섞어 주소간 연결성을 약화시키는 믹싱 프로토콜에 대해 항목별로 분류하여 연구 흐름을 정리한다.

Ⅱ. 클러스터링

비트코인은 주소를 이용하여 사용자들끼리 비트코인을 주고받는다. 앞서 설명한 바와 같이 비트코인 주소는 한 번만 사용하는 것이 권장되기 때문에 각 트랜잭션에 마다 새로운 비트코인 주소가 생성되며, 사용자들은 원할 때 언제든지 새로운 주소를 생성할 수 있다. 따라서 사용자는 지갑이라는 단위 안에 여러 개의 비트코인 주소를 관리한다. Harrigan의 논문 [7] 그림 4를 참조하면, 하나의 지갑에 몇 개의 주소가 구성되어 있는지 대략적인 그래프를 확인할 수 있다.

블록체인 트랜잭션 데이터는 모두 공개되어 있기 때문에, 어떤 주소가 주어졌을 때 클러스터링 기술을 적용해 어떤 주소와 같은 사용자가 관리하는 것으로 판단되는 여러 주소들을 그룹화 할 수 있다. 이때 그룹화된 주소중 하나라도 비익명화가 가능할 경우, 해당 지갑에 포함된 모든 주소들을 비익명화 할 수 있으므로 비트코인 비익명화 공격을 극대화 시킬 수 있다.

클러스터링 기술은 사토시 나카모토가 작성한 논문에서 이미 언급되었다 [1]. 논문에서는, 그림 2와 같이 하나의 트랜잭션에 여러 개의 입력주소가 있을 경우, 해당 입력들은 같은 소유자가 관리하는 것으로 밝혀진다고 설명한다. 그 이유는, 현재 비트코인 시스템에서는 여러 명의 사용자가 하나의 트랜잭션을 생성하는 기능이 없기 때문이다.

Ron[2]는 사토시 나카모토가 언급한 클러스터링 기술을 적용하여 비트코인 트랜잭션에 대한 분석 연구를 진행하였다. 추가로 m-to-n 트랜잭션을 n개의 m-to-1 트랜잭션으로 분할하여, 트랜잭션 그래프를 엔티티 그래프로 표현하는 방법을 제안하였다. 클러스터링 기술을 적용하여, 엔티티당 주소 개수, 받은 비트코인 값, 현재 보유한 비트코인 값, 주소가 보유한 최대 비트코인 값, 발생 트랜잭션 수, 트랜잭션 당 비트코인 크기, 가장 활동적인 엔티티 등을 분석하여 표로 정리했다.

Androulaki[3]은 사토시 나카모토가 언급한 클러스터링 기술을 휴리스틱 1이라고 명명하고, 휴리스틱 2를 제안하였다. 휴리스틱 2는 비트코인 사용자들이 하나의 트랜잭션으로 두 명 이상의 사용자에게 코인을 전송하는 경우가 적다는 경험적 사실에 기반을 둔다. 그림 3과 같이 1개의 입력주소와 2개의 출력주소가 있을 때, 2개

〔그림 2〕 다중-입력 휴리스틱

〔그림 3〕 그림자 주소 휴리스틱

의 출력 주소중 하나가 이전 거래 기록이 없다면 입력 주소와 같은 소유자로 그룹화 한다. 이유는 비트코인 시스템에서는 가지고 있는 모든 비트코인을 트랜잭션에 투입하고 잔액을 새로운 주소로 전송해야하기 때문에, 일반적으로 어떤 사용자가 다른 사용자에게 돈을 보낼 때 1개의 입력주소와 2개의 출력주소가 나타난다. 따라서 2개의 주소중 하나가 이전 거래 기록이 없을 경우, 높을 확률로 같은 사용자가 관리하는 주소라고 판단할 수 있다. 새로 생성되어 잔액을 전송하는 주소를 그림자 주소라고 부르기 때문에, 휴리스틱 2를 그림자 주소 휴리스틱으로 명명하였다.

Meiklejohn[4]는 휴리스틱 2에 대한 false positive를 크게 줄였다. 휴리스틱 1은 비트코인의 시스템 특징을 이용한데에 반해, 휴리스틱 2는 시스템 특징이 아닌 경험적 사실에 기반을 두기 때문에 false positive가 존재한다. Meiklejohn은 false positive를 분석해본 결과, false positive의 대부분이 사토시 다이스(비트코인을 이용한 도박 사이트)와 관련된 트랜잭션에서 발생하는 것을 발견하였다. 사토시 다이스와 관련된 트랜잭션에는 휴리스틱 2를 적용하지 않은 결과, false positive 가 1%대로 크게 감소하였다.

Spagnuolo[5]는 2013년까지의 비트코인 시스템의 구현 취약점을 이용하여, 휴리스틱 2의 성공 확률을 비약적으로 증가시켰다. 취약점은 그림자 주소의 위치를 결정하는 코드에서 발생하였다. 그림자 주소의 위치를 결정하는 함수에 수취인의 수를 파라미터로 받는데, 휴리스틱 2의 상황에서는 항상 수취인의 수가 1명이고, 수취인의 수가 1명일 때 함수는 항상 0을 반환한다. 결과적으로 그림자 주소의 위치가 첫 번째 출력주소로 고정되는 취약점이 발생하였다. 휴리스틱을 구현하여 클러스터링 기술을 적용한 결과, 휴리스틱 1만 적용할 경우 평균 4.31개의 주소를 하나의 지갑으로 클러스터링 하였고, 휴리스틱 1과 2를 모두 적용한 결과 평균 7.32개의 주소를 하나의 지갑으로 클러스터링 하였다. 또한 Spagnuolo은 'BitIodine' 툴을 개발하여 거래 흐름을 시각적으로 분석 하였다.

Nick[6]은 웹 지갑 서비스인 BitcoinJ에 대한 실제 지갑 데이터를 수집하여, 휴리스틱에 대한 신뢰도 높은 정확도를 측정하였다. 그 결과 휴리스틱 1을 적용할 경우 전체 주소중 68.59%를 그룹화 하였으며, 휴리스틱 1과 2 두개를 적용할 경우 전체 주소중 69.16%를 그룹화 하였다. 실험 결과 휴리스틱 2를 적용하여도 클러스터링 정확도를 0.57% 밖에 증가시키지 못했다. 이는 휴리스틱 2가 false positive를 보이는 것을 고려하면, 휴리스틱 2에 대한 타당성을 다시 검증할 필요가 있다고 보여진다. 또한 Nick은 새로운 휴리스틱 3, 4를 제안하였다. 하지만 휴리스틱 1,2,3,4를 모두 적용한 결과, 전체 주소 중 69.34%를 그룹화 하여 성능 향상을 거의 보이지 않았다.

Wallet Korbit.co.kr (link to service, show transactions)

Page 1 / 36 Next... Last (total addresses: 3,543)

address	balance	incoming txs	last used in block
16jce8CbnyF2dYkBzrXKEdeG2wGMwShkPq	14.8	59	495941
1B19K2yX6wKi9YEs5gFzseavk67BMjWqaY	0.357	199	495114
1EXWmfyG22LhiMhtxzWFjZpbAZvdxQqHuR	0.245	2	491906
1Giz3BA3tQFikwyj8qpmzQ9wt4XKAbAij9	0.08	7	486940
1GrCCd4m5vxLqKFzs8Pbny9qBqL65LFKJp	0.05544744	41	499556
135tMf9zBrXq3H9gPjSbRW3aPfTY6nb5e9	0.03988182	19	509414
1HMGCgUB5VN5ASGH7srBTzWbWr4amw9MVK	0.00817669	24	523320
1BNS5SwGATcVHAdmSXviYYoeHnps9PhGL	0.00418235	292	498689
16qaBxqomiNWFon94Ymd8NJ5zFGGFVGncZ	0.001	7	470125
1BsFwcxmUKpSNF3o4Zw5RPF4h3ZZs8vefB	0.00089532	270	463892
1AC7edgc7WiRPcvYUQahURRqBi4H6FLaCn	0.00023786	41	490076
1MoBHvENfHihW22P1hGXpdTF9Ty1YTsw2z	0.00003951	14	479784
1CsTzA5jqs8f63pzcw5f9LJoi2i1HLwKjd	0.00000004	739	478351
1AvGPjBB3PcdhLYwy7twKFrPwpwJ1iv9pF	0.00000002	558	475099
1Nh6sF7Bgxbeh6cEt8R8hRR4vuLWdcmeoB	0.00000002	71	461183

〔그림 4〕 WalletExplorer

Harrigan[7]은 다중 입력 휴리스틱의 효율성에 대한 분석을 하였다. 다중 입력 휴리스틱은 식별된 주소를 재사용하는 경우가 많기 때문에 효과가 크다고 분석했다. 또한 Harrigan은 1000개 이상의 주소가 하나의 엔티티로 클러스터링될 경우 슈퍼클러스터라고 명명하였으며, 슈퍼클러스터(예, 중개거래소, 도박 사이트, 다크 넷 시장)가 점진적으로 증가하기 때문에 클러스터링이 효과적이라고 결론지었다.

지금까지 클러스터링 연구 동향을 살펴보았다. 다음은 클러스터링 결과를 제공하는 몇 개의 서비스를 소개한다. WalletExplorer는 클러스터링 결과를 제공하는 무료 사이트 이다. 그림 4를 보면, 총 3,543개의 주소가 지갑 'Kobit'으로 클러스터링 되었다. WalletExplorer와 달리 라이센스를 판매하는 상용 툴로는 Chainalysis, Numisight, Blocksseer, Bitfury, Elliptic 등이 있다. 특히 Chainalysis는 WalletExplorer 개발자들의 후속 제품이며, 다음과 같은 장점을 가진다. 거래 흐름을 지갑 단위로 시각화여 보여주고, 더 많은 주소를 하나의 지갑으로 클러스터링 한다. 또한 식별된 주소 정보를 더 많이 보유하고 있으며, 더 편리한 사용자 인터페이스를 제공한다. 마지막으로 비트코인 주소에 대해 추가적인 정보를 웹에서 수집하는 기능을 제공한다.

Ⅲ. 믹싱 프로토콜

비트코인의 트랜잭션은 블록체인에 누구나 볼 수 있게 공개되어 있다. 따라서 어떤 주소에서 어느 주소로 비트코인을 보냈는지 거래 흐름 연결이 가능하다. 이러한 연결성을 깨트리기 위해 많은 연구들이 믹싱 프로토콜을 제안했다. 믹싱 프로토콜은 참여자들의 비트코인을 섞어 주소 간 연결성을 약화시킨다. 믹싱 프로토콜은 크게 제 3의 엔티티인 믹서를 활용하는 Distributed 믹싱 프로토콜과, 제 3의 엔티티 없이 참여자들이 하나의 트랜잭션을 생성하여 비트코인을 섞어주는 Decentralized 믹싱 프로토콜로 나눌 수 있다.

3.1. Distributed mixing protocol

Mixcoin [11]은 사용자가 믹서에게 비트코인을 보내면 믹서는 다른 사용자들의 비트코인과 섞은 후 돌려준다. 비트코인과 호환 가능하며, 내가 믹싱에 참여했다는 사실을 부인할 수 있다. 믹서를 통한 믹싱을 하기 때문에 Dos 공격에 저항력이 있다. 절도를 할 경우 암호학적으로 절도한 사실을 증명할 수 있으며, 이를 명성 시스템을 통해 절도를 예방한다. 하지만 여전히 비트코인 절도가 가능하다는 단점이 있으며, 믹서는 입력과 출력 주소를 연결할 수 있다. 이는 법 집행기관을 통한 수사를 진행할 경우 강제적인 공개가 불가피할 수 있다. 마지막으로 모든 사용자가 동일한 비트코인을 믹싱 해야 하는 한계가 있다.

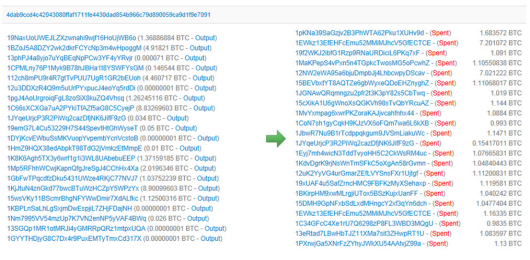
Blindcoin [12]는 Mixcoin의 한계를 극복하고자 제안됐다. Mixcoin에서는 믹서가 입력과 출력 주소를 연결할 수 있는 단점이 있었다. 이를 Blindcoin에서는 은닉서명을 이용하여 믹서가 출력주소를 알 수 없게 한다. 하지만 여전히 믹서는 비트코인을 절도할 수 있으며, 모든 사용자가 동일한 비트코인을 믹싱 해야 하는 한계가 있다. 추가적으로 은닉서명을 이용함으로써 익명성 레벨이 떨어지는 단점이 생겼다. Mixcoin과 Blindcoin 둘 다 여러 개의 믹서가 존재하는데, 은닉서명 기술을 적용하기 전에는 사용자가 어떤 믹서와 비트코인을 주고받았는지 구분이 불가능했다. 하지만 은닉서명 기술로 인해 믹서의 서명이 들어가면서 사용자가 어떤 믹서와 비트코인을 주고받았는지 구분이 가능해졌다. 이는 익명성 레벨이 참여자 수에 비례하는 믹싱 프로토콜에 치명적으로 작용한다.

Tumblebit [13]은 Mixcoin과 Blindcoin의 단점인 절도가 가능하다는 점을 개선했다. Tumblebit은 믹서를 신뢰하지 않아도 믹싱을 수행할 수 있는 최초의 프로토콜이다. 또한 800명의 사용자가 동시에 프로토콜에 참여할 수 있는 높은 확장성도 보였다. 믹서는 입력 주소와 출력 주소를 연결할 수 없으며, 익명성 레벨을 효과적으로 증가시켰다. Tumblebit은 전체 프로토콜 수행시간이 5초 이내로 짧은 소요시간을 보이며, 420bytes 이내의 낮은 대역폭을 보인다, 하지만 두 개의 연속적인 비트코인 트랜잭션이 요구되는 단점이 있다.

3.2. Decentralized mixing protocol

Coinjoin [14]는 비트코인 개발자가 포럼에 제안한 최초의 peer-to-peer 방식의 프로토콜이다. 다수의 사용자가 동시에 트랜잭션을 생성하여 어떤 입력주소가 어떤 출력주소에 대응되는지 연결을 어렵게 한다 (그림 5 참조). Decentralized 믹싱 프로토콜은 믹서가 없기 때문에 비트코인을 도난당할 위험이 없다. 하지만 Coinjoin은 Dos 공격에 취약한 단점이 있다. Dos 공격이란, 한명의 악의적인 사용자가 다수의 트랜잭션에 참여한 뒤 트랜잭션 생성 직전에 서명하지 않을 경우 다수의 트랜잭션 생성이 중단되는 공격을 말한다. 이는 소수의 악의적인 참여자가 전체 시스템에 영향을 줄 수 있다. 또한 참여자들은 다른 참여자의 입력과 출력주소를 연결할 수 있다는 단점이 있으며, 이러한 접근법 역시 모든 사용자가 동일한 비트코인을 믹싱 해야 하는 한계가 있다.

CoinShuffle [15]는 Coinjoin의 참여자들이 다른 참여자의 입력 주소와 출력 주소를 연결할 수 있는 단점을 극복하기 위해 제안된 프로토콜이다. CoinShuffle은



〔그림 5〕 Coinjoin 트랜잭션

Coinjoin에 익명 네트워크인 Mix-net을 적용하였다. 비트코인 주소를 참여자 수만큼 암/복호화 하여 전송하며, 결과적으로 내부 참여자들도 다른 참여자의 입출력 주소를 연결할 수 없다. Coinshuffle은 n명의 정직한 참여자와 c명의 악의적인 참여자가 있을 경우, n-c 수준의 익명성 레벨을 보인다. 또한 Dos 공격에 대한 대응으로 수수료를 이용한 방안을 제시했다. 트랜잭션에 참여를 결정한 순간 수수료를 지불하며, 이는 트랜잭션이 생성되지 않아도 돌려받지 못한다. 결과적으로 한 번에 많은 트랜잭션에 참여하려면 많은 비트코인이 필요하기 때문에 Dos 공격에 저항력을 갖지만, 정직한 참여자들조차 추가적인 수수료를 지불해야하는 단점이 있다.

CoinShuffle++ [16]은 CoinShuffle의 부족한 확장성을 개선하였다. Mix-net은 대역폭이 높은 장점이 있지만, 수행시간이 긴 단점이 있다. 하지만 비트코인 트랜잭션은 높은 대역폭이 필요하지 않으며, 짧은 수행시간을 요구한다. 따라서 CoinShuffle++는 대역폭이 낮지만 수행시간이 짧은 DC-net 기반으로 프로토콜을 설계하였다. n명의 참여자가 있을 때 n*f번의 라운드가 필요한 Mix-net과 달리, DC-net은 4+2f번의 라운드만 필요하다. (f: 악의적인 참가자) 또한 Ruffing은 CoinShuffle에 대한 deanonymization 공격을 제안하였다. CoinShuffle++는 내가 믹싱에 참여했다는 사실을 부인할 수 없으며, 여전히 참여자들이 모두 동일한 금액만 믹싱 할 수 있다는 단점이 있다.

ValueShuffle [17]은 Coinjoin, CoinShuffle, CoinShuffle++가 참여자들이 모두 동일한 금액만 믹싱해야 하는 단점을 개선하였다. ValueShuffle은 CoinShuffle++ 프로토콜에 기밀 트랜잭션 기술[18]을 적용하였다. 기존 트랜잭션의 경우 블록체인에 저장된 비트코인 값이 공개되지만, 기밀 트랜잭션의 경우 암호화 하여 비트코인 값을 은닉한다. 기밀 트랜잭션 기술은 비트코인 트랜잭션이 입력 값과 출력 값이 항상 같아야 한다는 특징을 이용하여 구현되었다. 입력 값과 출력 값을 동형암호 기술로 암호화 하여 채굴자들이 입력 값과 출력 값을 모르고도 입력 값과 출력 값이 같은지 검증한다. 추가적으로 영 지식 범위 증명을 위해 링 서명 기술을 이용하였다. 결과적으로 서로 다른 비트코인 값을 믹싱 가능하게 하였다. 또한 Stealth address 기술[19]를 적용하여, 수취인도 1회성 주소를 발급받아 다른 부가적인 공격을 방지한다.

Ⅳ. 결 론

본 논문에서는 어떤 비트코인 주소와 관련된 주소목록을 그룹화 하여 비익명화 공격의 가능성을 크게 증가시키는 클러스터링 기술과, 여러 사용자의 비트코인을 섞어 주소 간 연결성을 깨트리는 믹싱 프로토콜 기술에 대해 살펴보았다.

많은 믹싱 프로토콜이 제안되고 있지만 아직 비트코인 시스템에 적용되지 않았으며, 믹싱 프로토콜을 도입하여도 시스템이 점점 커지는 상충관계가 있다. 또한 비트코인 시스템은 익명성을 목적으로 설계된 암호화폐가 아니기 때문에 완전한 익명성을 달성하기 어렵다. 따라서 높은 수준의 익명성이 요구될 경우 ZeroCoin과 같이 익명성을 핵심 속성으로 개발된 암호 화폐를 사용하는 것을 권장한다.

참 고 문 헌

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Ron, D., & Shamir, A. (2013, April). Quantitative analysis of the full bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security (pp. 6-24). Springer, Berlin, Heidelberg.

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

[4] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.

[5] Spagnuolo, M., Maggi, F., & Zanero, S. (2014, March). Bitiodine: Extracting intelligence from the bitcoin network. In International Conference on Financial Cryptography and Data Security (pp.

457-468). Springer, Berlin, Heidelberg.

[6] Nick, J. D. (2015). Data-Driven De-Anonymization in Bitcoin (Master's thesis, ETH-Zürich).

[7] Harrigan, M., & Fretter, C. (2016, July). The unreasonable effectiveness of address clustering. In Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences (pp. 368-373). IEEE.

[8] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 15-29). ACM.

[9] Koshy, P., Koshy, D., & McDaniel, P. (2014, March). An analysis of anonymity in bitcoin using p2p network traffic. In International Conference on Financial Cryptography and Data Security (pp. 469-485). Springer, Berlin, Heidelberg.

[10] Biryukov, A., & Pustogarov, I. (2015, May). Bitcoin over Tor isn't a good idea. In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 122-134). IEEE.

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

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

[13] Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., & Goldberg, S. (2017). Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. Proceedings of NDSS 2017.

[14] Maxwell, G.: CoinJoin: Bitcoin privacy for the real world. Post on Bitcoin Forum (August 2013), https://bitcointalk.org/index.php?topic=279249

[15] Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014, September). CoinShuffle: Practical decentralized coin mixing for Bitcoin. In European Symposium on Research in Computer Security (pp. 345-364). Springer, Cham.

[16] Ruffing, T., Moreno-Sanchez, P., Kate, A. (2017). P2P mixing and unlinkable Bitcoin transactions. In: NDSS 2017

[17] Ruffing, T., & Moreno-Sanchez, P. (2017, April). ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 133-154). Springer, Cham.

[18] Maxwell, G.: Confidential transactions (2015). https://people.xiph.org/~greg/confidential values.txt

[19] Todd, P.: Stealth addresses. Post on Bitcoin development mailing list. https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg03613.html

〈저 자 소 개〉

홍 영 기 (YoungGee Hong)
학생회원

2017년 2월 : 항공대학교 소프트웨어공학 학사
2017년 3월~현재 : 고려대학교 컴퓨터학과 석사과정
관심분야 : Cryptocurrency 등

허 준 범 (JunBeom Hur)
종신회원

2001년 2월 : 고려대학교 컴퓨터공학 졸업
2005년 8월 : 한국과학기술원 전산학 석사
2009년 8월 : 한국과학기술원 전산학 박사
2009년 9월~2011년 8월 : University of Illinois at Urbana-Champaign 박사후연구원
2011년 9월~2015년 2월 : 중앙대학교 컴퓨터공학부 조교수
2015년 3월~2016년 8월 : 고려대학교 컴퓨터학과 조교수
2016년 9월~현재 : 고려대학교 컴퓨터학과 부교수
관심분야 : 클라우드 보안, 빅데이터 보안, 네트워크 보안, 응용 암호학