정 보 보 호 학 회 지
제 32 권 제3호, 2022. 6

랜섬웨어를 이용한 암호화폐 탈취 및 자금세탁 방법에 대한 대응방안 연구 동향 분석

조 욱*, 김 금 보*, 허 신 욱**, 김 호 원***

요 약

스마트컨트랙트를 사용하는 블록체인 2세대를 넘어오면서 블록체인 생태계는 지속적으로 성장하고 있으며, 블록체인 플랫폼 내에서 자체 발행되는 암호화폐는 다양한 수익 상품들(ICO, DeFi, NFT, Staking 등)을 등장시켰다. 암호화폐가 실물화폐를 대체할 새로운 대안이라고 여겨지고 있지만, 최근 암호화폐를 악용한 범죄가 증가하고 있다. 특히 시스템을 감염시켜 몸값을 요구하는 랜섬웨어의 경우 기존의 현금을 요구하기보다 자금 세탁에 용이한 암호화폐로 요구하는 빈도가 증가하고 있다. 암호화폐의 경우 손쉽게 믹싱 서비스를 받을 수 있으며, 블록체인의 특성상 모든 트랜잭션을 확인할 수 있음 제3의 신뢰기관이 존재하지 않으며 모든 네트워크는 계좌로 연결되기 때문에 익명성이 보장되어 범죄자들이 자금세탁에 이용하고 있다. 본 논문을 통해 랜섬웨어에 사용되는 암호화폐 자금세탁 사례를 살펴보고 자금 세탁 시 사용되는 믹싱 서비스에 대해서 분석했다. 또한 불법 자금세탁을 식별하기 위한 기술적 연구 동향에 대해서 분석하였다.

Ⅰ. 서 론

2009년 사토시 나카모토를 통해 처음 등장한 비트코인 등장 이후 스마트컨트랙트를 지원하는 이더리움을 시작으로 다양한 블록체인 플랫폼이 등장하며 블록체인 생태계를 확장시키고 있다[1]. 특히 블록체인 플랫폼 내에서 자체 발행되는 암호화폐는 금융시장에 ICO(Initial Coin Offering), 디파이(DeFi), NFT (Non Fingible Token), 그리고 스테이킹(Staking)과 같은 새로운 수익 상품들을 등장시켰다[2][3][4][5].

블록체인 플랫폼 내의 암호화폐는 자체 발행되며 플랫폼 내의 애플리케이션 이용 시 제3의 금융기관 없이도 결제가 가능하다는 이점[6] 때문에 암호화폐가 실물화폐를 대체할 새로운 대안이라고 인정받고 있다. 하지만 이와는 반대로 범죄자들은 블록체인 플랫폼의 익명성을 악용해 암호화폐를 범죄에 이용하고 있으며, 특히 시스템을 감염시켜 몸값을 요구하는 랜섬웨어의 경우 기존의 현금을 요구하는 것에서 암호화폐를 요구하는 빈도가 증가하고 있다[7].

암호화폐가 범죄에 악용되기 쉬운 것은 불법 수익을 은닉하고 합법한 방식으로 수익을 얻은 것으로 속이기 위한 자금 세탁이 암호화폐 믹싱 서비스를 이용하면 손쉽게 자금세탁이 가능하기 때문이다. 또한 블록체인 네트워크의 특성상 모든 거래 내역을 확인할 수 있는 제3의 신뢰기관이 존재하지 않으며, 모든 네트워크는 계좌로 이루어지기 때문에 참여자들에게 익명성이 보장되기 때문에 많은 범죄자가 암호화폐를 이용하고 있다.

본 논문은 이와 같이 범죄에 악용되는 암호화폐 동향 및 감지 기술을 분석해 보기 위해 2장에서는 블록체인과 암호화폐, 그리고 랜섬웨어에서 사용되는 암호화폐 사례를 살펴보고, 3장에서는 자금세탁의 개념과 자금세탁에 이용되는 암호화폐 사례 그리고 자금세탁이 가능하게 하는 암호화폐 믹싱 서비스에 대해서 분석하고자 한다. 4장에서는 불법 자금세탁에 이용되는 믹싱 서비스를 감지하기 위한 기술적 연구에 대해서 설명하고, 5장에서 결론으로 마무리한다.

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2022-0-01201)
* 부산대학교 정보컴퓨터공학부 (대학원생, jouk@islab.re.kr, 대학원생, guembo@islab.re.kr)
** ㈜스마트엠투엠 IoT 보안팀 (팀장, shinwookheo@smartm2m.co.kr)
*** 부산대학교 정보컴퓨터공학부 (정교수, howonkim@pusan.ac.kr)

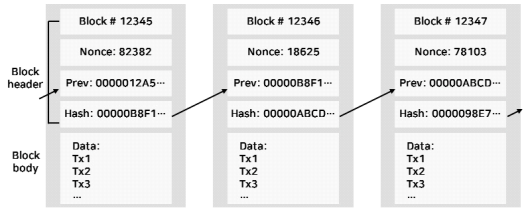
Ⅱ. 블록체인과 암호화폐

본 장에서는 블록체인과 암호화폐에 대해 설명하고 최근 랜섬웨어 공격에 암호화폐를 요구하는 사례들을 살펴보고자 한다.

2.1. 블록체인

블록체인 기술은 2009년 사토시 나카모토가 처음 발표한 비트코인[8]에 이어 스크립트 기반의 비트코인의 한계를 지적하며 스마트 컨트랙트를 지원하는 블록체인 2세대 이더리움, 이후 카르다노, IOTA 등 3세대 블록체인까지 많은 연구가 진행되고 있다[9][10][11]. 블록체인 기술은 P2P(Peer-to-Peer) 환경의 합의 알고리즘에 의해 생성되는 블록이 그림 1과 같이 이전 블록의 해시값을 저장하여 서로 연결된 구조를 가진다. 과거의 블록을 수정 시 이후 모든 블록이 보유한 과거 블록 해시값을 수정해야 하며 이러한 특성 때문에 블록체인은 데이터의 무결성을 보장한다. 초기 블록체인 모델인 비트코인과 이더리움은 작업증명(Proof of Work) 방식의 합의 알고리즘을 사용하여 블록 내 nonce 값을 추가한 해시의 특정 값을 찾는 방식으로 진행된다. 채굴자가 작업증명을 통해 블록을 생성하면 네트워크 참여자들은 블록의 nonce 값이 제대로 생성되었는지 검증한다. 블록체인은 P2P 환경에서 운영되기 때문에 여러 곳에서 동시에 블록이 생성될 수 있으며 보통 비트코인은 6개 이상의 블록 생성을 확인한다.

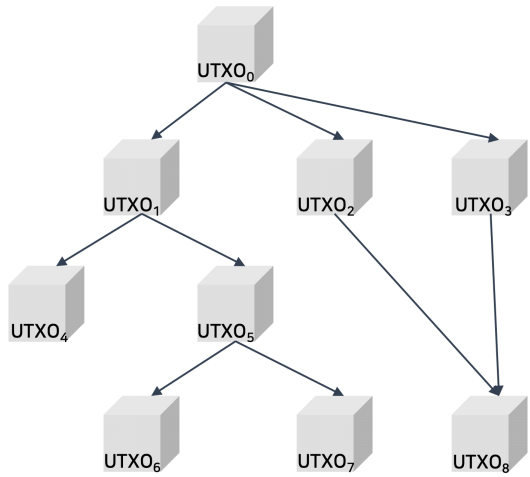
비트코인은 단순 결제만을 지원하는 모델이며 이를 극복하기 위해 비탈릭 부테린은 스마트 컨트랙트를 지원하는 이더리움을 구현하였다. 스마트 컨트랙트는 모든 계약을 제 3자 없이 개인과 개인의 계약을 지원하는 기술이다. 하지만 이더리움도 비트코인과 같이 확장성 문제를 해결하지 못했으며 이더리움 네트워크 참여자들이 수수료로 지불하는 가스비의 상승 등의 문제가 제기되었다. 이후 작업증명 방식의 합의 알고리즘이 아닌 지분증명(Proof of Stake), 위임 지분 증명(Delegated Proof of Stake) 등 다양한 합의 알고리즘을 사용하는 블록체인 기술과 블록체인의 낮은 TPS와 투명성으로 기업의 참여가 제한되자 검증된 참여자만 참여하는 프라이빗 블록체인 등 다양한 종류의 블록체인 기술이 연구되고 있다[12]. 또한 블록체인의 낮은 확장성을 극복하기 위해 플라즈마, 롤업, 페이먼트 채널과 같은 Layer 2 기술의 연구도 진행된다[13][14][15].



〔그림 1〕 Blockchain Structure

2.2. 암호화폐

암호화폐는 암호 기술을 사용해 만든 디지털 화폐이며 블록체인 기술의 발전으로 대부분의 암호화폐는 블록체인 네트워크에서 사용된다. 대표적인 암호화폐인 비트코인은 작업증명과정에서 채굴에 성공한 채굴자에게 보상으로 지급되며 총 2100만 개의 발행량을 가진다. 비트코인은 UTXO(Unspend Transaction Output)로 관리되며 자신의 비밀키를 사용해 UTXO Locking을 해제할 수 있다. 이더리움은 비트코인과는 다르게 계좌(Account) 모델을 기반으로 이더를 관리한다[16]. UTXO 모델이 그림 2와 같이 자산의 이동을 주소 간의 DAG(방향성 비순환 그래프)로 기록하여 관리하는 것에 반해 계좌 모델은 네트워크 내에 데이터베이스로 관리한다. 계좌 모델은 사용자 잔액을 모든 네트워크에 데이터베이스를 업데이트하여 관리하고 UTXO 모델은 거래 영수증(receipt)만을 블록에 기록



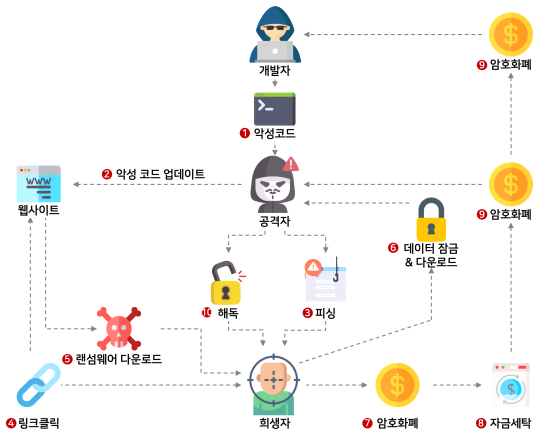
〔그림 2〕 UTXO DAG 모델

한 후 클라이언트에서 잔액을 계산하여 알려준다. 자금세탁을 위한 믹싱 서비스는 UTXO 모델과 계좌 모델에 따라서 다르게 개발되고 사용되고 있다.

2.3. 암호화폐와 랜섬웨어

랜섬웨어는 시스템을 감염시켜 접근을 제한하며 공격자에게 몸값을 강요받는 악성 소프트웨어이다[17]. 그림 3은 랜섬웨어 공격 중 하나인 RaaS(Ransomware as a Service)로 랜섬웨어 공격 활동을 개발자, 공격자, 자금세탁원으로 분업화하여 진행한다[18]. RaaS는 랜섬웨어 악성코드를 만들 수 없는 공격자들도 개발자들의 도움을 받아 랜섬웨어 공격을 할 수 있다. 개발자는 먼저 공격자에게 악성코드를 만들어 전달한다. 공격자는 이를 웹사이트에 업데이트하고, 피싱 공격을 통해 희생자를 유인한다. 희생자가 링크를 클릭하여 랜섬웨어를 다운로드 받으면 희생자의 데이터를 암호화해서 잠그거나 다운로드하여 탈취한다. 이후 희생자는 자금세탁 주소로 암호화폐를 전달하고 전달된 암호화폐는 자금세탁이 되어 공격자와 개발자에게 전달된다. 이후 공격자는 희생자의 데이터를 해독 프로그램을 전달한다.

랜섬웨어 피해액은 해마다 증가하여 2021년 말 글로벌 피해액 23조 6천억 원이 예측되며 단순 암호화를 통한 협상이 아닌 탈취한 데이터의 다크웹 유출을 통한 기업의 이미지, 정부 기관의 벌금 등을 위협하여 높은 몸값을 요구한다[19]. 또한 코로나19로 인한 재택근무의 증가로 취약해진 사이버 보안을 노려 랜섬웨어 감염률은 2배 이상 급증하였다[20]. 또한 몸값을 지불하여 복호화 키를 받아도 완벽한 복구가 보장되지 않



〔그림 3〕 RaaS(Ransomware as a Service)

으며 실제 2017년 나야나 업체는 랜섬웨어 몸값으로 암호화폐 13억 원치를 지불했지만 완벽한 복구에 실패했다[21].

과거의 해커는 대포통장을 사용해 몸값을 요구하였지만 암호화폐의 등장으로 암호화폐를 요구하는 사례가 증가하고 있다. 2018년 사탄(Satan)은 RaaS의 한 종류로 감염되면 약 220만 원 상당의 비트코인을 요구했다[22]. 국내 이랜드 그룹은 2021년 클롭(CL0P)에 의해 신용카드 정보 200만 건을 탈취했으며 비트코인 4,000만 달러(약 442억원)을 요구했다.[23] 2021년 미국 최대 송유관 기업인 콜로니얼 파이프라인을 공격한 해커는 랜섬웨어의 몸값으로 57억원에 해당하는 비트코인을 요구하였으며 JBS사도 랜섬웨어 공격으로 1100만 달러의 비트코인을 해커 집단에 지불하였다. [24]은 2021년 불법거래에 쓰인 암호화폐 금액은 140억 달러 이상으로 2020년에 비해 79% 증가하였다. 블리핑컴퓨터에 따르면 한 포럼 회원들이 불법 와레즈 사이트에서 윈도우 10 업데이트 파일을 설치한 후 매그니베르(Magniber) 랜섬웨어에 감염되어 파일 복구에 따른 몸값으로 약 2,600달러(약 329만 원)에 해당하는 비트코인을 전송 요구를 했다고 보고했다[25].

Ⅲ. 자금세탁

자금세탁(money laundering)은 불법 활동을 통해 얻은 수익을 합법적인 활동으로 얻은 수익으로 전환하거나 자금 출처를 숨기는 것을 말한다[26]. 자금 세탁은 미국 관세청에 의해 제안된 3단계 모델이론으로 예치, 은폐, 통합의 세 단계를 거쳐 이루어진다[27]. 예치단계에서는 대량의 불법 수익을 가치물(valuables)로 전환하기 위해 우선적으로 국내 또는 국외 은행에 예치하거나 국외로 송금하는 과정을 말한다. 은폐단계는 불법 자금을 작은 단위로 분할하여 은행, 개인, 기업 간에 반복적으로 이체시키거나 현금으로 인출하여 다른 은행으로 예치하는 등의 행위로 출처를 감추려는 시도를 말한다. 통합 단계는 합법적인 활동으로 둔갑하기 위해 합법적인 사업에 투자하는 등의 합법적 자금 출처를 창조하는 단계를 말한다.

3.1. 암호화폐와 자금세탁

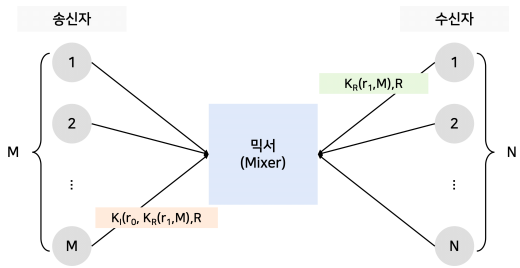
랜섬웨어와 같은 불법적인 활동으로 얻은 암호화폐

의 경우 자금세탁을 통해 합법적인 수익으로 둔갑시킨다. 현금 수익을 암호화폐로 자금 세탁을 하는 경우 현금을 암호화폐로 전환한 뒤 거래소를 통해 환전하는 방법을 이용했으나 최근에는 암호화폐로 직접 수익을 얻음으로써 믹싱 서비스를 이용하여 자금세탁을 진행한다. 믹싱 서비스는 이용 자체가 불법이 아니며 불법적인 목적과 결합하였을 때 불법이 되기 때문에 이를 구분하기가 어려워졌으며 범죄자들은 자금세탁이 더욱 용이해졌다.

2022년 북한이 탈취한 암호화폐의 자금세탁을 도운 블렌더(Blender)가 미국에서 제재당했다. 미국 재무부는 북한과 연계된 해킹 조직인 라자루스가 2022년 3월 엑시 인피니티에서 암호화폐를 7천 880억 원을 탈취했으며 이 중 260억 원이 북한의 불법적인 수익을 처리하는데 블렌더가 이용됐다고 밝혔다[28]. 여성 성착취 동영상으로 범죄 수익을 얻었던 n번방 사건에서도 암호화폐로 결제를 받고 이를 믹싱 서비스를 통해 자금 세탁을 시도한 사례가 있다[29].

3.2. 암호화폐 자금세탁에 이용되는 믹싱 서비스

블록체인 네트워크의 특성상 모든 블록 데이터는 공개되며, 블록 내에 기록되어있는 트랜잭션을 분석하면 수신자와 송신자 간의 연결성을 확인할 수 있다. 범죄자들은 이런 연결성을 완화하기 위해 믹서(텀블러) 등을 통해 트랜잭션을 난독화하는 믹싱 서비스를 진행한다. [30]에 처음 제안된 그림 4 믹싱 서비스는 수신자가 송신자에게 메시지를 전달할 때, 수신자는 중개자인 믹서에 전달하고 믹서가 송신자에게 메시지를 전달하게 함으로써 메시지의 수가 많아질수록 송신자와 수신자의 연결성을 완화할 수 있다. 여기서 K_R은 수신자의 공개키, K_I는 믹서의 공개키, r_0와 r_1은 랜덤 값, M은 메시지, R은 송신자의 주소를 나타낸다. 연

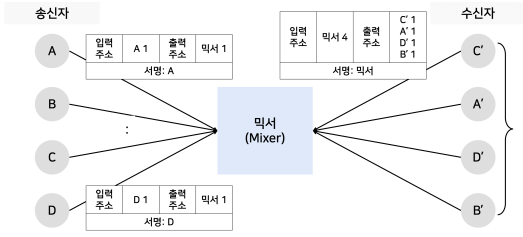


〔그림 4〕 기본 믹싱 서비스

결성을 더욱 낮추기 위해 여러 개의 믹서를 사용할 수도 있다.

3.2.1. 중앙집중식 믹싱 서비스

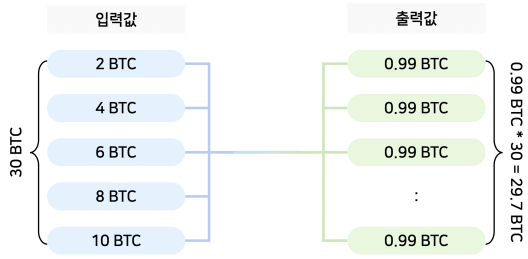
중앙집중식 믹싱서비스는 믹서를 신뢰한다고 가정하고, 참가자들이 믹서에 암호화폐를 전달하고, 믹서는 수신자를 임의로 선정하여 트랜잭션을 출력한다. 중앙집중식 믹싱서비스는 믹서를 전적으로 신뢰하기 때문에 발생될 수 있는 문제들을 해결함으로써 발전해 왔다. 중앙화된 믹서의 암호화폐 절도를 막기 위해 Mixcoin[31], CoinSwap[32]이 제안되었으며, 출력주소를 감추기 위해 은닉서명을 사용하는 Blindcoin이 제안되었다. TumbleBit[33]은 2PC(Two Party Computaion)과 영지식 증명을 활용해 믹서가 입력주소와 출력주소를 연결할 수 없도록 하였으며, 참여자는 믹서를 신뢰하지 않아도 믹싱을 수행할 수 있도록 하였다. 그림 5는 중앙집중식 믹싱 서비스를 보여준다.



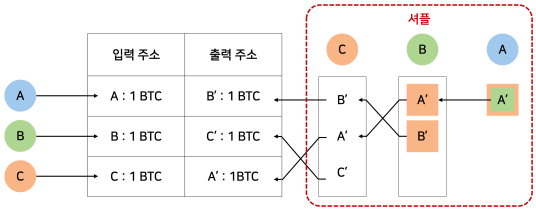
〔그림 5〕 중앙집중식 믹싱 서비스

3.2.2. 탈중앙화 믹싱 서비스

탈중앙화 믹싱 서비스는 중앙화된 믹서 대신 다수의 참여자가 P2P 방식으로 믹싱 서비스를 구현하는 서비스를 말한다. 최초의 P2P 믹싱 서비스는 CoinJoin으로 비트코인 개발자 그레고리 맥스웰(Gregory Maxwell)이 2013년에 최초로 제시했다[34]. 수많은 사용자들의 UTXO 입력들을 결합하고 동일한 수의 UTXO을 여러 개 출력 반환하는 방식이다. 예를 들어 5명의 사용자가 각각 2 BTC, 4 BTC, 6 BTC, 8 BTC, 10 BTC를 입력하면 수수료 0.3을 제외한 0.99 BTC에 해당하는 30개의 개별 출력을 생성한다. 생성된 30개의 개별출력을 출력 계좌가 받아야 하는 금액에 따라 나누어 거래 영수증을 블록에 저장한다. 그림 6은 코인 조인의 입력과 출력의 상태를 보여준다.



〔그림 6〕 CoinJoin



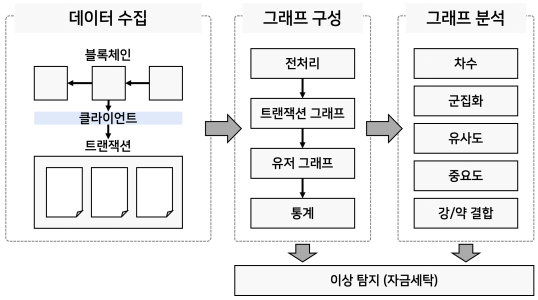
〔그림 7〕 코인 셔플

이후 2014년 Saarland University의 연구원에 의해 제안된 CoinShuffle은 코인조인에서 영감을 받아 더욱 발전된 형태로 제안한 믹싱 서비스로, 코인조인 서비스가 서비스를 이용하는 참여자들이 다른 참여자의 입력주소와 출력 주소를 연결할 수 있다는 단점을 Mix-net을 통해 극복했다[35]. 그림 7에서 보듯이 A는 B, C의 공개키를 알고 있는 상태에서 자신이 원하는 출력 주소를 암호화해서 B로 전달하고, B는 자신이 원하는 출력주소를 C의 공개키로 암호화하는 동시에 A로부터 받은 암호화된 출력주소를 복호화하여 두 개의 주소를 C로 보내게 되는데, 이때 C는 두 개의 주소가 누구에게 속하는지 추측할 수 없다.

이후 CoinShuffle의 수행시간이 긴 단점을 극복한 CoinShuffle++[36]이 제안되었지만, 여전히 참여자 모두가 동일한 금액을 보내야 하는 단점이 존재했으며, 해당 단점을 극복하기 위해 영지식 범위 증명을 활용한 ValueShuffle[37] 방법이 제안되었다.

Ⅳ. 자금세탁 대응방법에 대한 연구 동향

최근 암호화폐의 이상 거래를 탐지하기 위해서 그림 8과 같이 3단계 분석을 진행한다. 먼저, 네트워크에 클라이언트 노드를 구성해 블록을 다운받고 블록 안에 있는 트랜잭션을 수집하는 데이터 수집 단계이다. 두 번째 단계에서 트랜잭션을 전처리한 후에 트랜잭션의 그래프를 구성하고 이를 통해 유저 그래프를 구성한



〔그림 8〕 암호화폐 이상거래 분석 3단계

후에 통계를 분석하여 연관성을 파악한다. 마지막으로 그래프의 차수, 군집화, 유사도, 중요도, 강/약 결합등의 지수들을 확인한다. 추가적으로 웹 크롤링을 진행해 얻은 웹 정보들을(불법계좌, 게시글, 랜섬웨어 이메일 등) 바탕으로 블록체인 플랫폼 계좌에 레이블을 지정하여 사용한다.

[38]은 모티브라는 개념을 도입하여 자금 세탁에 2개의 특정 모티브가 있는 것으로 간주하고 유향 하이퍼 그래프(directed hypergraphs)에 모티브 개념을 도입했다. 비트코인의 입력과 출력을 통해 거래소 주소의 통계적 특성을 확인했으며, 이를 이용하여 서브 그래프 특정 패턴을 정의한 후, 분석한 그래프가 특정 패턴 중 하나만 해당되는 경우 모티브를 “pure”라 식별하고, 특정 패턴이 두 개 이상일 경우 “mixed”로 식별하여 잠재적 이상 패턴으로 분류한다. 해당 주소가 자금 세탁을 하고 있는지를 80% 이상의 정확도로 검출 가능함을 확인했다.

[39]는 3개의 믹싱 서비스 Blockchain.info, Bitcoin Fog, BitLaundry의 운영 모델을 조사하고 자금 세탁을 위한 익명 트랜잭션을 추적하려고 했다. 해당 논문에서는 실제로 믹싱 서비스에 참가해서 입력 트랜잭션에 소량의 비트를 지불하고, 인출할 비트코인의 양, 하나 이상의 인출 주소, 출력 트랜잭션 수 및 트랜잭션 확산 시간 등을 매개변수에 직접 입력하여 실험을 진행하였다. 트랜잭션 입력에 따라 트랜잭션 그래프를 재구성하여 오픈 소스 Gephi4를 사용하여 시각화했다.

[40]에서는 비트코인 내의 트랜잭션 그래프를 통한 유저 그래프를 구성하고 토폴로지 특성을 통해 비상적인 패턴을 분석했다. 유저 그래프의 짧은 거리 (short distance)의 평균을 구해 작은 세계(small world)로 특정 짓고, 직경도 함께 계산한 후, 특정 몇몇 이상치의 존재를 비정상적인 트랜잭션, ps(pseudo spam) 트랜잭

션으로 간주했다.

[41]은 2020년 Alarabetal.이 제안한 방식으로 비트코인 트랜잭션 그래프를 구성하고 악의적 트랜잭션을 예측하기 위한 다층 퍼셉트론과 함께 그래프 컨볼루션 신경망(GCN, Graph Convolution Network)을 이용하는 새로운 방식을 제안했다. 해당 방법은 elliptic 데이터 세트를 사용하였다. 트랜잭션 유향 그래프의 노드들은 지불 흐름을 나타낸다. 해당 모델의 정확도는 0.974이다. 비교된 이전 GCN와 skip-GCN의 정확도는 모두 0.961이다.

[42]는 SVM, LR(Liner Regression), MLP(Multi Layer Perceptro)을 이용하여 의심스러운 행동과 자금세탁으로 분류할 수 있는 다중 분류 방법을 제안했다. 먼저 ReLU와 함께 SVM, LR, MLP를 활용하여 트랜잭션과 프로파일 데이터를 통해 의심 행동을 검출한다. 또한 사기 트랜잭션과 의심 행동 트랜잭션을 입력으로 범죄 행동을 분류한다.

Ⅴ. 결 론

본 논문에서는 블록체인과 암호화폐에 대해 분석하고 최근 랜섬웨어 공격이 암호화폐를 요구하는 방법과 사례에 대해서 조사했다. 랜섬웨어 공격에 있어 암호화폐를 요구하는 이유는 암호화폐를 믹싱 서비스를 통해 자금 세탁이 가능하기 때문이다. 암호화폐의 믹싱 서비스는 모든 트랜잭션을 모아서 처리하는 믹서를 이용하는 중앙 집중형 믹싱서비스와 참여자간의 P2P 믹싱 서비스를 진행하는 탈중앙 믹싱서비스로 나뉘며 각각 믹싱 방식에 대한 다양한 제안 방식에 대해서 분석하였다. 마지막으로는 블록체인 네트워크 내의 악의적 행동 중 자금 세탁 행동을 탐지할 방법들에 대해 연구가 활발이 되고 있음을 확인 할 수 있었다. 향후 암호화폐 네트워크의 생태계 확장과 발전을 위해 지속적인 불법적 행동 탐지 방법에 대한 지속적인 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] Cusumano, M. A. (2014). The bitcoin ecosystem. Communications of the ACM, 57(10), 22-24.

[2] Hahn, C., & Wons, A. (2018). Initial Coin Offering (ICO): Unternehmensfinanzierung auf Basis der Blockchain-Technologie. Springer-Verlag.

[3] Chohan, U. W. (2021). Decentralized finance (DeFi): an emergent alternative financial architecture. Critical Blockchain Research Initiative (CBRI) Working Papers.

[4] Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447.

[5] Price, T. (2017). Predictive Cryptocurrency Mining and Staking.

[6] WEB2 VS WEB3, “https://ethereum.org/en/developers/docs/web2-vs-web3/”

[7] Kshetri, N., & Voas, J. (2017). Do crypto-currencies fuel ransomware?. IT professional, 19(5), 11-15.

[8] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[9] Dannen, Chris. Introducing Ethereum and solidity. Vol. 1. Berkeley: Apress, 2017.

[10] Silvano, Wellington Fernandes, and Roderval Marcelino. "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data." Future generation computer systems 112 (2020): 307-319.

[11] Charles, “why we are building cardano.”

[12] Bach, Leo Maxim, Branko Mihaljevic, and Mario Zagar. "Comparative analysis of blockchain consensus algorithms." 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Ieee, 2018.

[13] POON, Joseph; BUTERIN, Vitalik. Plasma: Scalable autonomous smart contracts. White paper, 2017, 1-47.

[14] ethereum optimistic-rollup, “https://ethereum.org/ko/developers/docs/scaling/optimistic-rollups/”

[15] POON, Joseph; DRYJA, Thaddeus. The bitcoin lightning network: Scalable off-chain instant

payments. 2016.

[16] UTXO VS. ACCOUNT MODEL “https://academy.horizen.io/technology/expert/utxo-vs-account-model/”

[17] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.

[18] Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, 101762.

[19] Chainalysis, “https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-criminal-balances-criminal-whales/”

[20] 2020년 위협 결과 보고서, 트렌드마이크로

[21] Lee, S. H., Jun, H. J., & Kim, T. S. (2017). Risk Management Requirements for Cyber Insurance. Journal of the Korea Institute of Information Security & Cryptology, 27(5), 1233-1245.

[22] 220만원 상당 비트코인 요구하는 RaaS ‘사탄’ 국내 유포 “http://www.itdaily.kr/news/articleView.html?idxno=88407”

[23] 김기범. (2021). 랜섬웨어 피해현황 및 대응방안. KISO 저널, (44), 26-29.

[24] [하이테크 리포트] 암호화폐 범죄 140억 달러 규모, 거래량 늘면서 피해액도 증가 “https://www.ajunews.com/view/20220214110945494”

[25] 업데이트 설치하니 비트코인 요구" 윈도우 10 업데이트 파일로 가장한 랜섬웨어 주의 “https://www.itworld.co.kr/news/234969#csidxc30caac0c02310483d191f7cb71d640“

[26] Levi, M., & Reuter, P. (2006). Money laundering. Crime and justice, 34(1), 289-375.

[27] Force, F. A. T. (2014). Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors.

[28] 미, 북 가상자산 자금세탁 도운 '블렌더' 제재 나섰다 “https://www.edaily.co.kr/news/read?newsId=01095526632326624&mediaCodeNo=257”

[29] 정제용. (2021). 암호화폐 범죄 관련 범정부적 및 입법적 통제에 대한 연구 - 특정금융정보법 개정안을 중심으로. 경찰학연구, 21(1), 61-89.

[30] Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84-90.

[31] 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.

[32] Maxwell, G. CoinSwap: Transaction graph disjoint trustless trading. “bitcointalk.org”, Oct. 2013

[33] Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., & Goldberg, S. (2016). Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. Cryptology ePrint Archive.

[34] Maxwell, G. CoinJoin: Bitcoin privacy for the real world. “bitcointalk.org”, Aug. 2013.

[35] 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.

[36] Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2016). P2P mixing and unlinkable bitcoin transactions. Cryptology ePrint Archive.

[37] 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.

[38] Ranshous, S., Joslyn, C. A., Kreyling, S., Nowak, K., Samatova, N. F., West, C. L., & Winters, S. (2017, April). Exchange pattern mining in the bitcoin transaction directed hypergraph. In International conference on financial cryptography and data security (pp. 248-263). Springer, Cham.

[39] Zhao, C., & Guan, Y. (2015, January). A graph-based investigation of bitcoin transactions.

In IFIP International Conference on Digital Forensics (pp. 79-95). Springer, Cham.

[40] Francesco Maesa, D. D., Marino, A., & Ricci, L. (2016, November). An analysis of the Bitcoin users graph: inferring unusual behaviours. In International Workshop on Complex Networks and their Applications (pp. 749-760). Springer, Cham.

[41] Alarab, I., Prakoonwit, S., & Nacer, M. I. (2020, June). Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies (pp. 23-27).

[42] Feng, Y., Li, C., Wang, Y., Wang, J., Zhang, G., Xing, C., ... & Lian, Z. (2019, September). Anti-money laundering (AML) research: a system for identification and multi-classification. In International Conference on Web Information Systems and Applications (pp. 169-175). Springer, Cham.

〈저 자 소 개〉

조 욱 (Uk Jo)

학생회원

2012년 2월 : 광운대학교 전자공학 학사 졸업
2016년 2월 : 광운대학교 전자공학 석사 졸업
2020년 3월~현재 : 부산대학교 정보융합공학과 박사과정
<관심분야> 블록체인, 보안

김 금 보 (GuemBo Kim)

학생회원

2021년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2021년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
<관심분야> 블록체인, 보안

허 신 욱 (ShinWook Heo)

정회원

2015년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2018년 2월 : 부산대학교 전기전자컴퓨터공학과 박사과정 수료
2018년 2월~2021년 9월 : 부산대학교 전기전컴퓨터공학과 수료후 연구생
2021년 9월~현재 : (주)스마트엠투엠 책임연구원
<관심분야> 암호구현, 정보보호

김 호 원 (Howon Kim)

종신회원

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
2020년~현재 : 블록체인 플랫폼연구센터 센터장
2020년~현재 : 부산대 지능형 융합보안대학원 책임교수
<관심분야> 블록체인, AI, 보안, 사물인터넷