JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 6, pp. 77-86, June 2022
https://doi.org/10.9708/jksci.2022.27.06.077

Overview of technologies: ensure anonymity of privacy coins

Hoon Kwon*, Eun-Young Kim*

*Professor, Dept. of Software Convergence Design, Jeju Campus of Korea Polytechnic University, Jeju, Korea
*Professor, Dept. of Software Convergence Design, Jeju Campus of Korea Polytechnic University, Jeju, Korea

[Abstract]

Recently, various cryptocurrencies (coins) based on block chains have appeared, and interest in privacy coins, which is an anonymity-based cryptocurrency that values personal information protection, is growing. In this paper, we look at coin abuse cases using privacy coins, and analyze the technology that guarantees the anonymity of 8 mainly traded privacy coins (Monero, Dash, Zcash, BEAM, Grin, Horizen, Verge, and Pirate Chain). We would like to analyze the applied technologies for We present the problems that can occur in these privacy coins, check the technology and each element applied to the privacy coin, and analyze the technical difficulty of the anonymity guarantee technology for the mainly traded coins through this, and Appropriate countermeasures and classification of privacy coins for technical difficulty were presented through the problem. Through this, the standard for re-evaluating the value of the coin according to the application of appropriate technology for the privacy coin can be presented.

▸ **Key words**: Privacy Coin, Cryptocurrency, Block chain, anonymization, ensuring anonymity technology

[요 약]

최근 블록체인 기반의 다양한 암호화폐(코인)들이 등장하고 있으며, 특히 개인정보보호를 중요시하는 익명성 기반의 암호화폐인 프라이버시 코인에 대한 관심이 높아지고 있다. 본 논문에서는 프라이버시 코인을 이용한 악용 사례에 대해 살펴보고, 이러한 악용 사례에 주로 거래되고 있는 프라이버시 코인 8개(Monero, Dash, Zcash, BEAM, Grin, Horizen, Verge, Pirate Chain)에 대한 익명성 모장을 위한 적용 기술들에 대해 분석하고자 한다. 이러한 프라이버시 코인에서 발생할 수 있는 문제점을 제시하고, 프라이버시 코인에 적용된 기술과 각 요소를 확인하고, 이를 통해 주로 거래되는 코인들에 대한 익명성 보장 기술에 대한 기술 난이도 등을 분석하고, 이러한 기술들에 대한 문제을 통해 적절한 대응 방안과, 기술 난이도에 대한 프라이버시 코인들에 대한 분류를 제시하였다. 이를 통해 프라이버시 코인에 대한 적절한 기술 적용에 따른 코인에 대한 가치를 재평가할 수 있는 기준이 제시될 수 있을 것이다.

▸ **주제어**: 프라이버시 코인, 암호화폐, 블록체인, 익명성, 익명성 보장 기술

• First Author: Hoon Kwon, Corresponding Author: Hoon Kwon
*Hoon Kwon (kwonhoons@gmail.com), Dept. of Software Convergence Design, Jeju Campus of Korea Polytechnic University
*Eun-Young Kim (key@kopo.ac.kr), Dept. of Software Convergence Design, Jeju Campus of Korea Polytechnic University
• Received: 2022. 04. 29, Revised: 2022. 06. 13, Accepted: 2022. 06. 13.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 블록체인 기반의 다양한 암호화폐들이 등장하고 있다. 이러한 임호화폐는 탈중앙화된 P2P(peer to peer) 방식의 블록체인 기술을 이용하여 중앙 기관 없이 개인 간 거래에 쉽게 이용될 수 있다는 특징을 지닌다. 또한, 익명성을 기반으로 하고 있으며, 이러한 익명성을 악용하여 다크웹에서 마약 거래, 무기거래 등 많은 불법 상거래에 사용되고 있다[1].

최초의 암호화폐인 비트코인[2]은 거래에 사용할 지갑생성을 위한 개인정보가 필요하지 않아, 익명성을 보장하고 있다. 범죄자들은 거래의 대상자들이 누구인지 식별이 어려운 점을 악용하여, 여러 지갑을 생성하고 거래 내역을 뒤섞는 방식으로 거래 내용에 대한 추적을 어렵게 한다. 다만 완전히 추적이 불가능하지는 않다. 이에 최근에는 불법적 거래를 위하여 더욱 추적이 힘든 프라이버시 코인을 사용하는 형태로 변화하고 있다.

프라이버시 코인[3]은 암호화폐 중에서도 개인정보보호를 중요시하는 암호화폐들을 의미하며, 대표적인 코인에는 모네로(Monero), 대시(Dash), 지캐시(ZCash), 코모도(Komodo), 버지(Verge) 등이 있다.

이러한 프라이버시 코인을 이용한 거래가 랜섬웨어와 같은 사이버 범죄에도 악용되고 있는 실정이며, 이러한 프라이버시 코인들을 대상으로 어떠한 악용 사례들이 존재하는지에 대해 알아보고자 한다.

Fig. 1.은 CoinLore[4]에 소개된 프라이버시 코인 중 하루 거래량을 기준으로 유통량이 많은 순을 나타낸 것이다[21/06/16 기준]. 본 논문에서는 이들 중 유통량이 많은 프라이버시 코인들을 대상으로 익명성 보장에 따른 기술들을 분석하고, 기술 자체의 문제점을 확인하여 프라이버시 코인이 완전한 익명성을 보장하는 데 필요한 요소들을 알아보고자 한다.

Privacy Coins

Coins which hides identity of the user, wallet balance or transfers.

#	이름	시가총액	가격	24시간 거래량	유통량	알고리즘	거래소	날짜	변동 (24시간)
3	Zcash	$1.5 B	$134.29	$869.9 M	11.4 M	Equihash	0	2016	-3.53%
2	Dash	$1.7 B	$170.00	$505.4 M	10 M	X11	0	2014	-2.64%
1	Monero	$4.7 B	$275.30	$256.9 M	17.2 M	CryptoNight	0	2014	-2.79%
4	Horizen	$592.7 M	$82.48	$29 M	7.2 M	Equihash	0	2017	-2.49%
14	BEAM	$21.3 M	$0.6438830	$16.2 M	33 M	Equihash	0	2019	-2.13%
6	Verge	$458.7 M	$0.0279050	$12.7 M	16.4 B	Multiple	0	2016	-2.63%
18	Grin	$7.4 M	$0.3881874	$5.3 M	19.1 M		0	—	-5.25%
10	Groestlcoin	$54.9 M	$0.7112165	$4 M	77.2 M		0	2014	-0.12%
8	PRCY Coin	$74.8 M	$1.24	$2 M	60.2 M		0	2021	12.72%
5	Pirate Chain	$465.1 M	$4.03	$1.3 M	115.5 M	Equihash	0	2019	-2.95%
13	NAVCoin	$26.5 M	$0.3716969	$656.2 K	71.3 M	X13	0	2014	-4.41%
7	Haven Protocol	$90.5 M	$11.54	$636.4 K	7.8 M		0	—	-1.57%
12	Dero	$34.3 M	$4.23	$550.6 K	8.1 M		0	—	3.65%

Fig. 1. Privacy Coin daily trading volume

1.1 Scenario

자금세탁을 위한 시나리오는 크게 5단계를 거쳐 이뤄진다. 첫 번째, Fig. 2에 나타난 것과 같이 법정화폐를 기본 코인으로 교환한다. 법정 화폐를 은행 계좌에 입금하여 전자화폐로 교환하며, 이 때의 기본 코인은 비트코인, 이더리움, 라이트 코인, 티더 등 시가 총액과 거래량이 높은 코인을 의미한다. 추적 방지를 위해 암호화된 이메일 서비스와 가명을 사용하여 지갑을 설정하고, VPN을 사용하여 거래를 진행한다.

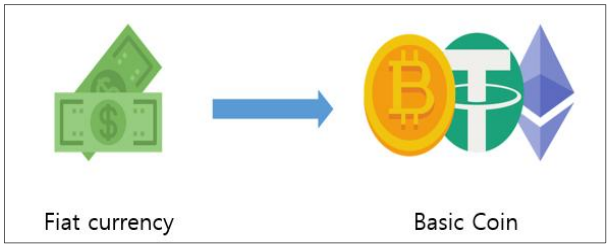

Fig. 2. Fiat currency and basic coin exchange

두 번째, 믹싱(Mixing)은 코인을 여러 임시 지갑으로 전송하여 추적을 난독화하는 기술이며, 이를 사용하여 Fig. 3.과 같이 기본 코인을 믹싱하고 거래소 지갑을 통해 프라이버시 코인을 구매한다. 믹싱된 기본 코인을 거래소 지갑에 전송하고 거래소 지갑에 있는 기본 코인을 여러 프라이버시 코인으로 교환한다.

II. Privacy Coin Abuse Cases

1. Money Laundering Case

범죄자들은 비트코인에서의 완전한 익명성 보장이 불가능한 이유로 자금 세탁을 위해 프라이버시 코인을 이용하기 시작했으며, 다음과 같은 시나리오에 의해 이뤄지게 된다.

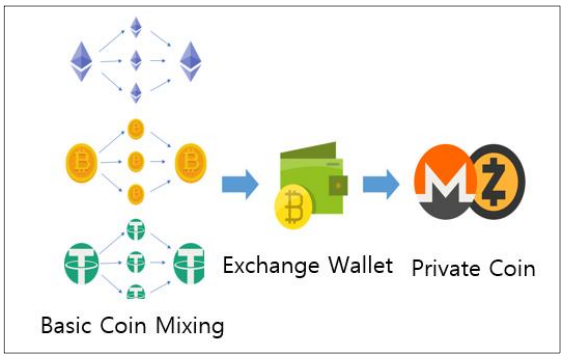

Fig. 3. Private coin exchange after basic coin mixing

세 번째 단계는 Fig 4.와 같이 프라이버시 코인을 계층화한 뒤 믹싱한다. 여러 프라이버시 코인을 한 번 더 믹싱한다. 프라이버시 코인은 익명성을 보장하는 기술을 제공하여 추적을 어렵게 만든다.

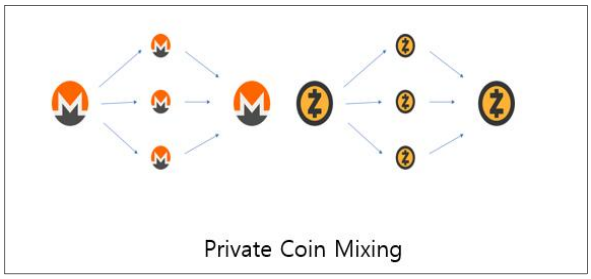

Fig. 4. Private coin mixing

네 번째, 프라이버시 코인을 거래소 지갑을 통해 기본 코인으로 교환한다. 거래소를 통해 믹싱한 프라이버시 코인을 기본 코인으로 교환한다.

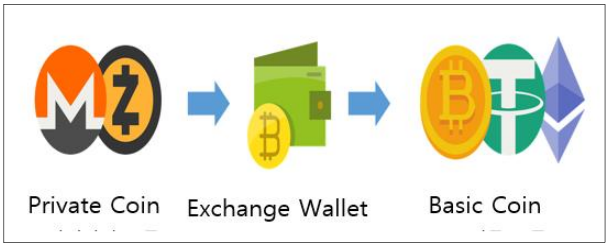

Fig. 5. After mixing privacy coin, exchange for basic coin

마지막으로, 기본 코인에서 법정화폐로 교환한다. 암호화폐 거래소에서 법정화폐를 기본 코인으로 교환한다. 첫 번째에서 사용했던 은행 계좌가 아닌 다른 은행 계좌로 거래를 진행한다. 은행 계좌에서 출금하여 전자화폐를 법정화폐로 교환한다.

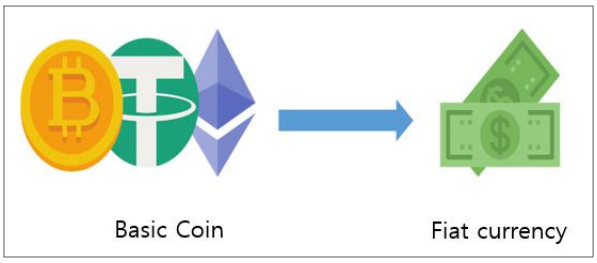

Fig. 6. Basic Coins and Fiat Exchanges

2. Drug Trading and Exchange Hacking

암호화폐의 보안성과 익명성을 이용하여 마약거래를 시도하는 단순한 거래만으로는 범죄행위에 대한 수사기법의 발달로 더욱 힘들어지고 있으며, 이를 피하기 위해 코인 믹싱 기술을 접목하여 마약 거래에 있어 프라이버시 코인이 사용되고 있다. 텔레그램과 같은 익명 메세징 서비스를 이용하여 여러 부계정을 만들어 코인 믹싱을 통한 마약 거래가 성행하고 있다. 추적 회피를 위한 사례로 마약 거래에 있어 다크웹을 통한 프라이버시 코인 거래가 이뤄졌으며, 일본 암호화폐 거래소인 코인체크에서 넴 코인이 해킹되어 추적을 회피하기 위해 모네로(Monero) 등과 같은 프라이버시 코인으로의 전환이 이뤄진 사례를 들 수 있다.

범죄자들은 비트코인에서의 완전한 익명성 보장이 불가능한 이유로 자금 세탁을 위해 프라이버시 코인을 이용하기 시작했으며, 다음과 같은 시나리오에 의해 이뤄지게 된다.

3. Illegal Mining

프라이버시 코인은 그 특성 때문에 불법 채굴도 많이 일어난다[5]. 불법 채굴은 해커들이 악성 프로그램을 이용해 타인의 컴퓨터를 감염시켜 암호화폐를 채굴하는 범죄다. 프라이버시 코인은 대체 가능성을 유지하므로 불법 채굴로 얻은 코인을 일반 코인처럼 사용할 수 있다. 특히 모네로는 전체 유통량 중 5%가 불법 채굴을 통해 생성되었다[6].

개인정보보호를 위하여 익명성을 강화할 목적으로 만들어진 프라이버시 코인이 예상과는 다르게 불법행위에 악용되고 있다. 이런 이유로 여러 법 집행 기구들은 프라이버시 코인의 사용을 우려하고 있다. 유로폴 보고서[7]는 프라이버시 코인을 최고 위협으로 선정하였고, 미국 법무부 보고서는 프라이버시 코인의 사용은 범죄 행위 가능성을 보여주는 것이라고 평가했다[8]. 프라이버시 코인은 코인의 익명화 기술이 불법행위에 악용될 수 있다는 가능성 때문에 여러 보고서에서 저평가되고 있다. 이런 형태의 평가는 프라이버시 코인 생태계에 악영향을 줄 것이며, 사용자와 암호화폐 서비스 업체들만 피해를 볼 것이다.

III. Privacy Coin Technical Overview

1. Monero

모네로(XMR)는 2014년에 바이트 코인을 포크 하여 탄생한 암호화폐다. 모네로는 링 시그니처와 스텔스 주소를 사용하여 철저히 개인정보를 보호한다. 모든 거래의 송신자, 금액 및 수신자 역시 숨길 수 있다. 링 시그니처는 트랜잭션에 서명한 이를 드러내지 않는 익명의 디지털 서명이다. 이는 송금자가 본인의 공개키를 여러 사람의 공개키와 함께 섞어 서명하는 방식이다. 스텔스 주소는 각 트랜잭션 중에 무작위로 생성되는 일회성 주소다. 송금자는 스텔스 주소를 사용해 토큰을 수신자의 주소로 보내고 거래가 완료되면 스텔스 주소가 사라져 추적이 어려워진다. 또한 모네로는 링 기밀 트랜잭션(RingCT)를 사용하여 트랜잭션의 금액 또한 알 수 없게 한다.

1.1 Stealth Address

스텔스 주소(Stealth address)는 전송자가 수신자를 대신하여 모든 거래에 대해 임의의 일회성 주소를 사용하는 것이다. 이 주소는 다른 거래와 연결할 수 없는 블록체인의 고유한 주소가 되고, 송신자와 수신자 주소를 연결하지 못하게 된다. 즉, 송신자가 스텔스 주소를 사용해 수신자의 주소로 보내게 되고, 거래가 완료되면 일회용 주소는 삭제된다. 이런 원리 때문에 거래에서 스텔스 주소를 사용할 경우 추적하기가 훨씬 어려워지고, 범죄에 악용되기 쉽다.

모네로에서의 스텔스 주소 기술은 DKSAP(Dual-Key Stealth Address Protocol)[9]이 사용되었고, 모네로 지갑 주소는 공개 읽기 키(Public scan key)와 공개 쓰기 키(Public spend key)를 포함한 95개의 문자로 구성되어 있다. 여기서 공개 읽기 키와 공개 쓰기 키는 각각 비밀 읽기 키 및 비밀 쓰기 키와 쌍을 이룬다. 앨리스와 밥이 스텔스 주소를 사용하여 거래할 경우 아래와 같은 과정으로 진행된다.

1. 앨리스가 밥에게 모네로를 보낼 때 앨리스의 지갑은 밥의 공개 읽기 키와 공개 쓰기 키 그리고 다른 랜덤한 데이터를 이용해 일회용 공개 키를 만든다.
2. 거래의 출력은 오직 밥만이 블록체인에서 자신의 비공개 키를 이용하여 찾을 수 있게 만들어진다.
3. 출력이 밥의 지갑에 의해 탐지되면 그의 지갑은 일회용 공개키에 맞는 일회용 비공개 키를 계산해내어 자신의 비공개 쓰기 키로 돈을 사용할 수 있게 된다.

이 모든 과정은 밥의 지갑 주소와 그 어떤 거래와의 공개적인 연결 없이 일어난다. 이처럼 스텔스 주소는 출력의 그 어떤 주소와의 연결도 방지한다. 이때 보내는 이의 프라이버시는 링 시그니처(ring signature)에 의해 보호된다.

스텔스 주소를 사용할 경우, 수신자는 거래의 출력을 찾기 위해 자신의 비공개 키를 이용하여 네트워크를 수시로 탐색해야 한다. 더 많은 사람이 스텔스 주소를 사용할수록 익명성은 높아지지만, 잔액을 찾는데 드는 비용도 비싸진다. 이러한 문제를 밸런스 디스커버리(balance discovery)라고 한다.

1.2 Ring Signature

스텔스 주소는 수신자의 프라이버시를 보호한다면, 링 서명(Ring Signature)은 전송자의 프라이버시를 보호한다. 링 서명은 여러 사람의 공개키를 섞어 전송자를 특정지을 수 없게 만드는 서명 기술이다. 실 서명인과 가짜 서명인들이 함께 링을 이루어 만들어진다.

모네로에서는 사용자가 입력을 발생시키면 블록체인에서 제3자의 입력을 무작위로 불러오고 실제로 발생한 것 같이 보이게 한다. 이 기능은 모든 입력이 분간이 안 되게 만들어 거래의 출처를 숨긴다. 여기서 제 3자가 어떤 출력이 실제로 사용되는 것인지 검증할 수가 없다면 이중 지불문제(double spending)이 일어날 수 있다. 하지만 모네로에서는 키 이미지(key image)의 사용으로 문제를 해결한다.

키 이미지는 사용되는 출력에서 파생되며 모든 링 시그니쳐 거래의 일부로 사용되는 암호화된 키이다. 블록체인의 모든 출력에는 단 하나의 키 이미지만이 존재할 수 있다. 하지만 암호화된 성질 때문에 어떤 출력이 어떤 키 이미지를 생성해냈는지 알아내는 것은 불가능하다. 이중 지불(double spending) 문제는 이미 사용된 모든 키 이미지들을 블록체인에 저장하여 해결한다. 이를 앨리스와 밥의 거래로 나타내면 아래와 같다.

1. 앨리스가 링 사이즈를 5로 설정한 후 밥에게 모네로를 보내려고 한다.
2. 거래의 다섯 가지 입력 중의 하나는 앨리스에게서 오게 된다.
3. 다른 네 개의 입력들은 블록체인에서 무작위로 선정되어 앨리스의 추적을 방해한다.
4. 제3자와 밥은 어떤 입력이 실제 앨리스의 입력인지 알 수 없지만, 밥에게 전송되는 모네로의 사용 여부는 키 이미지를 통해 네트워크가 안전하게 확인해줄 수 있다.

이처럼 링 서명은 입력의 출처를 모호하게 만들어 전송자의 프라이버시를 지켜줌으로써 모든 모네로 거래의 출발지를 추적 불가능하게 만든다.

링 서명은 링 크기만큼 공개키를 섞기 때문에 크기가 클수록 서명 값도 이에 비례하여 길어진다는 단점을 가지고 있다. 또한, 모네로에서의 링 서명은 다수의 사용자가 링 크기를 0으로 설정하면 가짜로 만들어진 출력의 진실 여부가 판단되어 모든 사용자의 프라이버시를 위협한다. 이를 해결하기 위해 모네로는 2016년 3월 22일에 하드포크를 진행하여 최소 링 크기를 3 이상으로 설정하게 제한했다.

1.3 RingCT(Ring Confidential Transaction)

기밀 거래(Confidential Transaction)는 비트코인 코어 개발자인 Greg Maxwell이 Confidential Transaction에서 발표한 알고리즘이다. 링 기밀거래(Ring CT)는 기밀거래 알고리즘을 링 서명에 맞게 수정한 기술이다. 링 서명과 스텔스 주소는 특정 트랜잭션의 출처나 주소를 식별할 수 없게 만들었지만, 거래 금액은 숨길 수 없었다. 모네로는 이 문제를 해결하기 위해 링 기밀거래를 설계했고, 모네로 연구소에서 처음 발표했다.[10]

링 기밀거래는 거래량을 블록체인에 숨겨 개인정보 유출을 방지한다. 채굴로 새로 생성된 Monero는 공개적으로 출력에 나타나고, 이 Monero가 처음 전송되면 금액이 숨겨진 RingCT 출력이 생성된다. 이를 앨리스와 밥의 거래로 나타내면 아래와 같다.

1. 앨리스의 출력은 12.56이고, 밥에게 2.5 Monero를 보내려고 한다.
2. 출력은 두 번 발행 할 수 없으므로 앨리스는 전체 출력을 소비하고 나머지 금액을 다시 받아야 한다.
3. 따라서 앨리스의 트랜잭션은 12.56 Monero의 입력을 갖고, 두 개의 출력을 갖는다.
4. 밥에게 보내는 2.5 Monero와 자신에게 돌아올 10.06 Monero의 출력이다.
5. 10.06 Monero는 거래에 대한 "변경"으로 지갑에 반환된다.
6. 거래에서 사기로 생성된 Monero가 없음을 증명하기 위해 거래의 입력 합계는 출력 합계와 일치해야 한다.
7. RingCT의 암호화 속성으로 인해 앨리스는 자신의 출력량을 커밋한다.
8. 따라서 거래를 확인하기 위해 네트워크에 충분한 정보만 공개하고 지출 금액을 공개적으로 공개하지는 않는다.
9. 금액은 난수처럼 보이지만 채굴자는 밥에게 전송된 금액이 Monero로 이동하는지 확인할 수 있다. 즉, 사용 가능한 자금에 해당한다.
10. 또한, RingCT 트랜잭션은 범위 증명을 통해 전송자가 음수 값을 커밋하지 못하도록 방지한다.
11. 범위 증명은 거래에 사용된 금액을 암호화 방식으로 증명한다. 금액은 0보다 크고 어떤 숫자보다 작다.
12. 외부 관찰자는 거래 결과에서 실제 금액을 볼 수 없지만, 거래가 합법적인지 확인할 수 있다.

링 기밀거래는 1.0부터 현재 3.0까지 개발되었으며, 입력 크기를 줄이고 거래 속도를 향상해 거래 수수료를 낮췄다. 모네로는 스텔스 주소와 링 서명 그리고 링 기밀거래의 조합으로 강한 익명성을 보장하여 트랜잭션 추적 가능성을 현저히 낮췄다. 또한, 현재 모든 국내 거래소에서 모네로 거래를 지원하지 않는다.[11]

2. Dash

대시(Dash)는 2014년에 엑스코인(Coin) 이라는 이름으로 출시된 암호화폐이다. 이후, 익명성이 강하다는 특징을 드러내기 위해 다크코인(Darkcoin)으로 이름이 바뀌었지만, 불법 사이트와 연관이 있다는 루머로 인해 다시 대시(Dash)로 이름을 바꿨다. 대시는 프라이빗 송금(PrivateSend)과 인스턴트 송금(InstantSend)을 선택할 수 있다. 대시는 이 프라이빗 송금이라는 방식을 사용해 익명성을 보장하고 있다. 프라이빗 송금은 코인조인(coinjoin)[12]의 개선된 버전으로 거래내역을 믹싱하여 추적을 어렵게 한다.

2.1 PrivateSend

대시는 네트워크의 중요한 기능과 향상된 서비스를 지원하기 위해 마스터 노드를 사용한다. 마스터 노드는 블록체인의 완전한 복사본이 있는 서버로, 프라이빗 송금(PrivateSend)과 인스턴트 송금(InstantSend)을 지원하며, 블록 유효성 검사와 관련된 특정 작업을 수행한다. 프라이빗 송금은 대시 프로토콜의 분산형 코인 믹서 기능으로, 대시에서만 사용이 가능하다.

프라이빗송금은 네트워크에서 트랜잭션의 출처를 난독화하여 대시 코인의 대체 가능성을 유지한다. 대체 가능성은 모든 통화를 자유롭게 교환할 수 있는 특성으로 프라이버시 코인이 가져야 할 핵심 특성이다. 이는 일부 사용자가 불법 활동과 관련된 거래와 관련 있는 코인을 받아들이기 거부할 수 있다. 즉, 네트워크의 잠재적 위협이 되기 때문에 대체 가능성은 유지되어야 한다.

지갑에서 프라이빗송금을 할 때, 관련 금액(0.1, 1, 10)으로 분할된다. 거래의 이러한 액면가는 마스터 노드에 의해 처리되며, 다른 프라이빗 송금을 사용하는 트랜잭션과 일치시킨다. 마스터 노드가 분할된 여러 액면가를 일치시킨 후 믹싱 프로세스가 시작된다. 믹싱이 이루어지는 턴마다

마스터 노드는 입력을 믹싱하고 일치된 트랜잭션의 지갑 모두에게 믹싱된 입력을 다시 지불시키도록 요청한다. 마스터 노드는 위 과정을 반복하여 출처를 모호하게 만든다.

대쉬에서의 프라이빗 송금은 전송 및 수신자 주소와 금액을 공개하기 때문에 트랜잭션 분석을 통해 확률적으로 출처의 식별이 가능하다. 또한, 프라이빗 송금의 사용은 선택 사항이며, 실제 자금 이체를 구성하는 거래 비율은 0.7% 미만이다.[13] 즉, 프라이버시 보호 목적으로 대시를 사용하는 것은 위험하다.

3. Zcash

지캐시(ZEC)는 2016년에 출시된 암호화폐로 영지식 암호 기술(zero-knowledge)이 사용되었다. 이 기술은 차폐주소(shielded address)를 보호하는 데 사용되며, 차폐주소는 블록체인에 저장된 거래 및 주소 데이터를 암호화시킨다. 지캐시는 사용자에게 익명 수준을 선택할 수 있도록 두 가지 유형의 주소, 즉 투명주소(transparent address)와 차폐주소(shielded address)를 제공한다. 이는 선택적 송금으로 익명 수준을 선택할 수 있는 대시와 비슷하다. 지캐시는 비공개 거래를 할 경우, 거래 메타데이터를 암호화하고 영지식 스나크(zk-SNARK)라는 영지식 증명구조를 사용하여 부정행위 및 도용 행위가 없음을 증명하는 방식으로 익명성을 보장하고 있다.

3.1 zk-SNARK

영지식 스나크(zk-SNARK)는 영지식 증명을 좀 더 간결하고 비상호적인 환경에서 적용할 수 있도록 변형한 기술이다. 지캐시에 의해 개발되었으며, 익명성을 제공하는 기술이다. 여기서 영지식 증명은 진술 자체의 타당성을 벗어난 정보를 공개하지 않고 진술이 진실이라는 것을 한 당사자가 다른 당사자에게 증명할 수 있도록 하는 것이다. 예를 들면, 주어진 임의의 숫자의 해시에 대해, 영지식 증명을 사용하여 증명자는 검증자에게 그 숫자를 밝히지 않고 그 숫자가 실제로 존재한다는 것을 납득시킬 수 있다.

지캐시는 영지식 스나크에 네트워크의 합의 규칙 중 일부를 인코딩하여 영지식 프라이버시를 구현하였다. 이를 통해 트랜잭션에 포함된 주소와 값에 대한 중요 정보를 공개하지 않고 트랜잭션이 유효한지 검사할 수 있다.[14] 사용자들은 차폐주소와 투명주소를 사용하여 거래를 진행할 수 있다. 차폐주소와 투명주소는 지갑을 통해서 만들어지지만, 거래 시 차폐주소는 블록체인에서 주소를 숨기고 투명주소는 주소를 공개한다. 또한, 지캐시는 두 주소 체계의 공존을 허용하여 차폐주소와 투명주소 간의 거래가 가능하다.

- 차폐주소 → 차폐주소 (Private)
- 차폐주소 → 공개주소 (Deshielding)
- 공개주소 → 차폐주소 (Shielding)
- 공개주소 → 공개주소 (Public)

지캐시에서의 익명성 보장 기술 사용은 대시와 마찬가지로 선택이다. 이는 익명성을 낮추는 원인이 되며 높은 확률로 추적이 가능하다. 지캐시는 높은 수준의 암호화 기능을 제공했지만, 완전한 익명성을 보장하지 못한다. 또한, 영지식 스나크는 타원곡선암호 기법으로 암호화를 하기 때문에 양자컴퓨터 공격에 매우 취약하다.

4. Beam

빔(BEAM)은 2019년에 출시된 Mimblewimble[15] 및 Lelantus MW[16] 프로토콜 기반 암호화폐이다. Mimblewimble 프로토콜이 익명성 블록체인 프로토콜이기 때문에 익명성을 보장한다는 것을 제외하고는 독자적인 익명성 보장 기술은 존재하지 않는다.

4.1 Mimblewinble

밈블윔블(Mimblewimble)은 블록체인 프로토콜 중 하나이며, 비트코인과 달리 트랜잭션에 주소가 없다. 즉, 모든 트랜잭션이 제3자에게 임의이 데이터처럼 보인다. 또한, 기밀거래와 같이 트랜잭션 데이터는 각 참여자만 볼 수 있다. 밈블윔블 블록은 검증과 확인을 할 수 있지만, 각 트랜잭션에 대한 세부내용이 제공되지 않기 때문에 개별적인 입력값과 각 출력값은 연결할 방법이 없다. 이에 코인의 이동을 위해서는 전송자와 수신자가 반드시 검증 정보를 교환해야 한다. 밈블윔블은 커트 쓰루(cut-through) 기능을 제공하여 불필요한 트랜잭션 정보를 제거하고 블록 데이터를 간소화한다. 이를 앨리스와 밥의 거래로 나타내면 아래와 같다.

1. 앨리스는 어머니에게 5 밈블윔블 코인, 아버지에게 5 밈블윔블 코인을 받는다.
2. 앨리스는 밥에게 10개의 코인을 보낸다.
3. 밥은 앨리스가 자신에게 코인을 보냈다는 정보 외에 어떤 정보도 알 수 없다.
4. 블록이 생성될 때 이 거래는 밈블윔블의 커트 쓰루에 의해 하나의 입력-출력값 쌍(앨리스의 부모님으로부터 밥에게)으로 기록된다.

밈블윔블은 대시와 마찬가지로 코인조인(coinjoin)[12]을 사용한다. 네트워크의 여러 트랜잭션이 하나의 트랜잭

션으로 믹싱되어 특정 트랜잭션의 전송자와 수신자를 식별할 수 없게 한다.

밈블윔블은 커트 쓰루와 코인조인을 통해 익명성을 보장한다. 커트 쓰루는 트랜잭션이 지속적으로 블록 내에 누적되고 이루어지며 코인 조인이 되어 추적하기 힘들게 한다. 여기서 트랜잭션은 누적되면서 브로드 캐스팅이 되기 때문에 마지막 커트 쓰루 집계가 완료되기 전, 모든 트랜잭션을 선택하는 스니퍼 노드를 실행하면 코인조인을 해제할 수 있다. 이를 통해 전송자와 수신자의 96%를 알아낼 수 있다.[17]

5. Grin

그린코인(GRIN)은 2019년에 출시된 Mimblewimble 프로토콜 기반 암호화폐이다. 빔(BEAM)과 같은 Mimblewimble 프로토콜 기반 암호화폐이지만 통화정책, 커뮤니티, 채광, 기술적 방향에 차이가 있다.[18] 그린 또한, 프로토콜이 익명성 블록체인 프로토콜이기 때문에 익명성을 보장한다는 것을 제외하고는 독자적인 익명성 보장 기술은 존재하지 않는다.

6. Horizen

호라이즌(ZEN)은 2017년에 ZenCash로 출시되고, 2018년에 Horizen으로 리브랜딩된 암호화폐이다. 익명성을 보장하기 위해 zk-SNARK, TLS 통합, 도메인 프론팅, 클라이언트-노드 암호화 및 엔드-투-엔드 암호화를 제공한다. 이 중 송신자와 수신자의 거래내역 및 개인정보를 보호하는 기술은 zk-SNARK이며 Zcash와 동일하게 선택적으로 개인정보보호 기능을 사용할 수 있다.

7. Verge

버지(XVG)는 2014년에 도지코인(Dogecoin)을 기반으로 도지코인다크(DogecoinDark)라는 이름으로 개발 된 후, 2016년에 리브랜딩하여 출시된 암호화폐이다. 이중 키 스텔스 주소(Dual-Key Stealth Addressing)를 사용하여 송신자와 수신자의 상호 작용 없이 거래할 수 있다는 것이 특징이다. 또한, 물리적 위치와 같은 특정 트랜잭션의 IP를 숨기기 위해 TOR 및 I2P의 조합을 제공한다.

7.1 TOR Integration

The Onion Router의 약어에서 파생된 Tor는 계층화된 회로 기반 네트워크에서 익명 통신을 가능하게 하는 IP 난독화 서비스이다. 버지는 Tor를 모든 지갑에 통합하여 소스와 목적지를 알고 있는 네트워크 감시를 통해 통신 피어를 결정할 수 있는 단일 지점을 제거한다.[19]

7.2 I2P Integration

Invisible Internet Project의 약어에서 파생된 I2P는 네트워크를 통해 전송되는 모든 버지 데이터를 익명화하는 IPv6를 사용하는 터널링 서비스이다. 버지의 클라리언트에는 i2P "라우터"가 있으며 여러 개의 인바운드 및 아웃바운드 터널 속 데이터를 순서(클라이언트에서 보내고받는)대로 전달한다. 클라이언트가 다른 클라이언트의 버지 데이터를 보내려고하면 다른 클라이언트의 인바운드 터널 중 하나를 대상으로하는 아웃 바운드 터널 중 하나를 골라 메시지를 전달한다.[19]

8. Pirate Chain

피레이트 체인(ARRR)은 2018년에 코모도(Komodo)를 기반으로 만들어진 암호화폐이다. 여기서 코모도(Komodo)는 지캐시(Zcash) 기반이기 때문에 피레이트 체인도 zk-SNARK를 통해 익명성을 보장한다. 하지만, 지캐시와 달리 개인 전송 거래만 가능하여 차폐 주소(shielded address)만 사용할 수 있다. 즉 피레이트 체인은 100% 비공개 전송 블록 체인이다.

9. Privacy Coin Technical Analysis

프라이버시 코인에서 익명성을 보장하는 기술은 크게 트랜잭션 난독화와 네트워크 난독화로 나뉜다. 트랜잭션 난독화는 거래의 정보를 암호화시켜 제3자가 거래를 특정짓지 못하게 막는다.

네트워크 난독화는 노드의 ip를 숨기고 노드 간의 통신을 암호화시켜 사용자의 신원 노출을 막으며 제3자가 트래픽을 분석하기 어렵게 만들기 때문에 높은 추적 난이도를 가진다. 트랜잭션 난독화는 기술의 특성에 따라 추적 난이도가 낮아질 수 있으며 Table 1.을 통해 확인할 수 있다.

난독화 기술은 제작된 목적에 따라 다양한 난독 행위를 수행하며 기술의 특징에 따라 분류할 수 있다. 익명화 기술의 특징에 따라 분류하여 보면 Table 2.와 같다.

Table 1. Transaction obfuscation

Transaction Obfuscation	Network Obfuscation	Trace Level
Ring Signature		Low
PrivateSend		
Mimblewimble (coinjoin)		
Mimblewimble (cut-through)		Medium
Stealth Address		
Ring CT	TOR Integration	High
Zk-SNARK	I2P Integration	

Table 2. Classification of Anonymization Technology

Anonymization technology	Features
Ring Signature	Like coinjoin, it splits a transaction and mixes it with similar transactions.
PrivateSend	
Mimblewimble (coinjoin)	
Mimblewimble (cut-through)	By deleting the intermediate addresses, the contact point of the transaction is deleted.
Stealth Address	
Ring CT	After encrypting the main value of the transaction, it does not decrypt, but proves the transaction through the proof method.
Zk-SNARK	
TOR Integration	It obfuscates traffic to make it safe from man-in-the-middle attacks.
I2P Integration	

또한, 몇 기술들은 높은 익명성을 제공하지만, 기술적 문제점을 가진다. Table 3.은 각 기술의 문제점을 나타낸다.

Fig 7.은 프라이버시 코인과 코인에서 사용되는 기술들을 추적 난이도에 따라 분류한 것이다.

여기서 원의 색은 기술 사용의 선택 여부이며, 빨간색은 기술이 무조건적으로 사용되는 경우고, 파란색은 기술이 선택적으로 사용되는 경우다. 익명성 기술은 사용하는 사람이 적을 수록 위력이 약해지기 때문에 파란색 원을 가진 코인은 낮은 익명성을 보장한다. 반대로, 빨간 원을 가진 코인은 높은 익명성을 보장하며, 원의 개수가 많을수록 완전해진다.

프라이버시 코인들 중 익명성이 상대적으로 높은 코인은 Monero와 Pirate Chain이 있고, 상대적으로 낮은 코인은 Dash와 Zcash가 있다. Zcash 같은 경우, 추적 난이도가 높은 기술을 사용하고 있지만 기술이 선택적으로 사용되기 때문에 기술을 사용하지 않은 노드를 이용한 특정 트랜잭션의 추적이 가능하다. Verge 또한 트랜잭션 난독화 기술이 선택적으로 사용되고 있어 트랜잭션의 추적이 가능하다. Zcash와 다른 점은 추적 난이도가 높은 네트워크 난독화 기술을 사용하여 특정 노드의 신원을 보호한다는 것이다.

Table 3. Problems with Anonymization Technology

Anonymization technology	Problems
Ring Signature	Since the public key is mixed as much as the size of the ring, the larger the size, the longer the signature value.
PrivateSend	Since the sender and receiver addresses and amounts are opened, the source can be identified through transaction analysis.
Mimblewimble (coinjoin)	Because it is broadcast as transactions accumulate, coinjoin can be canceled by running a sniffer node that selects all transactions before the final cut-through aggregation is completed.
Mimblewimble (cut-through)	
Stealth Address	In the case of using a stealth address, the recipient must frequently search the network using his/her private key in order to obtain the output of the transaction. The more people use stealth addresses, the more anonymity you get, but at a cost.
Ring CT	
Zk-SNARK	Because it is encrypted with elliptic curve cryptography, it is very vulnerable to quantum computer attacks.
TOR Integration	
I2P Integration	

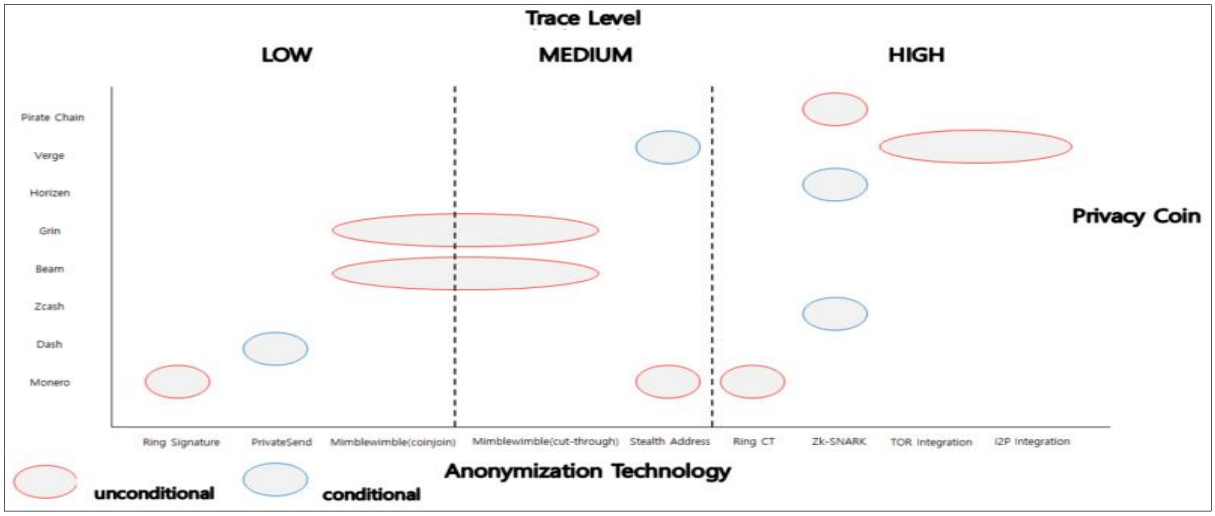

Fig. 7. Classification of Privacy Coins by Type of Technology

IV. Conclusions

추적이 어려운 프라이버시 코인은 개인정보를 중시하는 사람들과 범죄자들로부터 많은 관심을 끌어모았다. 그 결과, 추구하는 정보 보호 수준에 따라 다양한 방식의 코인들이 생겨났고, 여러 기술들이 개발되었다. 대부분의 기술은 트랜잭션 난독화와 네트워크 난독화이며, 블록체인에서 사용자와 거래를 숨겨 제3자가 추적하지 못하게 한다. 프라이버시 코인은 트랜잭션 난독화와 네트워크 난독화가 동시에 이루어질수록 좋고, 기술이 무조건적으로 사용될수록 높은 익명성을 보장한다. 또한, 다양한 난독화 기술이 사용될수록 안전하다. 그런 면에서 추적 난이도가 높은 기술 하나를 사용하는 Pirate Chain보다 Monero가 더 완전한 익명성을 보장한다.

프라이버시 코인이 갖고 있는 문제점은 익명성이 높을수록 비용이 증가하고, 익명성이 낮을수록 트랜잭션의 추적이 쉬워진다는 것이다. 증명방식 암호기술도 트랜잭션의 추적은 어렵게 만들지만, 언제든지 이중 지불 문제와 같은 문제가 발생할 수 있다. 이런 문제점을 해결하면 누구나 쉽게 프라이버시 코인에 접근할 수 있을 것이고, 이에 대한 긍정적인 평가도 기대할 수 있을 것이다. 또한, 익명성을 중시하는 사람들을 위해 만들어진 코인을 단순히 범죄에 악용될 수 있다는 이유로 저평가되는 것은 부당하므로 프라이버시 코인이 추구하는 가치에 대해 재평가가 필요할 것으로 보인다.

향후, 본 분석을 바탕으로 프라이버시 코인 기술이 갖고 있는 문제점을 보완하고, 기술에 맞는 채굴 알고리즘과 합의 알고리즘을 구축하여 높은 익명성은 제공하지만 범죄에 악용되기 어려운 코인이 제작되어야 할 것이다.

REFERENCES

[1] DOMINIK STROUKAL, BARBORA NEDVĚDOVÁ, "Bitcoin and other cryptocurrency as an instrument of crime in cyberspace", Proceedings of Business and Management Conferences 4407036, International Institute of Social and Economic Sciences, pp. 222-224, 2016-10-12

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", pp. 1~8, 2008-10-31

[3] Shapeshift, "What Are Privacy Coins?".Medium(Blog), https://link.medium.com/hCokKIcSibb?fbclid=IwAR0bgxFhhuies9Nyrtv_a2si4DV_xGPHSVdI-lKPORCGB4lagZn09spky7I

[4] Cryptocurrency Prices | Coin Market Overview | CoinLore, https://www.coinlore.com/ko/privacy-coins

[5] Sergio Pastrana, Guillermo Suarez-Tangil, "A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth" IMC '19: Proceedings of the Internet Measurement Conference, pp. 73~86, 2019-09-25, DOI:https://doi.org/10.1145/3355369.3355576

[6] Josh Grunzweig, The Rise of the Cryptocurrency Miners, https://unit42.paloaltonetworks.com/unit42-rise-cryptocurrency-miners/

[7] IOCTA, INTERNET ORGANISED CRIME THREAT ASSESS MENT, pp.57~58, 2020-10-05

[8] U.S. Department of Justice, "Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework", pp.41, 2020-10-08

[9] The Shadow Project. "Dual-key Stealth Addresses", in part of Shadow Documentation, https://doc.shadowproject.io/#dual-key-stealth-addresses

[10] S. Noether, A. Mackenzie, and the M. Research Lab, "Ring Confidential Transactions", ledger, vol. 1, pp. 1-18, 2016-12-21. DOI: https://doi.org/10.5195/ledger.2016.34

[11] Cryptocurrency 'Monero' with a market cap of $1 billion is virtually removed from Korea, https://m.etnews.com/20200416000179

[12] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, "A fistful of Bitcoins: characterizing payments among men with no names" Commun. ACM 59, 4 , pp. 86–93, 2016-03, DOI:https://doi.org/10.1145/2504730.2504747

[13] Chainalysis Team, https://blog.chainalysis.com/reports/introducing-chainalysis-investigation-compliance-support-dash-zcash

[14] What are zk-SNARKs?. https://z.cash/ko_KR/technology/zksnarks/

[15] Andrew Poelstra, "Mimblewimble", 2016-10-06

[16] Lelantus MW, https://github.com/BeamMW/beam/wiki/Lelantus-MW

[17] Ivan Bogatyy, "Breaking Mimblewimble's Privacy Model", https://medium.com/dragonfly-research/breaking-mimblewimble-privacy-model-84bcd67bfe52

[18] BRIAN CURRAN, "What is the BEAM Coin? Mimblewimble & Grin vs Beam", https://blockonomi.com/beam-coin-guide/

[19] CryptoRekt, "Blackpaper Verge Currency 5th edition", pp. 01-30, 2019-01,

Authors

Hoon Kwon received the M.S. and Ph.D. degrees in Computer Engineering from Jeju National University, Korea, in 2005 and 2011, respectively. Dr. Kwon joined the Part-time lecture of the Department of Computer Science at Jeju National University, Jeju, Korea, in 2005. He joined Jeju National University as an academic research professor since 2014. He is currently a Visiting Professor in the Department of Software Convergence Design, Jeju Campus, Korea Polytechnic University. He is interested in Internet Of Things, Blockchain and Physical Computing.

Eun-Young Kim received the B.S., M.S. degrees in Computer Engineering 1989, 2004, respectively and completed doctoral course from Jeju National University in 2008. Prof. Eun-Young Kim has been working in the Department of Software Convergence Design, Jeju Campus, Korea Polytechnic University, from 1993 to the present, and has been teaching computer graphics, video editing, animation, and vector graphic design and chromatics.