프라이버시 코인이란? 그것에 대해 알아야할 것

원문:
https://www.btcc.com/ko-KR/academy/crypto-basics/what-is-privacy-coin

최근 프라이버시 코인, 일명 다크 코인에 대한 논란이 뜨겁습니다. 지난 8월 미국 재무부는 이더리움 기반 코인 믹싱 플랫폼인 토네이도캐시의 사용을 금지한 바 있습니다. 업비트, 빗썸 등 국내 거래소도 올해 6월 '익명 전송 기능'을 이유로 라이트코인(LTC)을 상장 폐지했습니다. 또 암호화폐 거래소 후오비가 ZEC(지캐시), XMR(모네로) 등 7개의 프라이버시(익명) 코인을 상장폐지한다고 12일 밝혔습니다.

자금세탁(ML)과 테러자금 지원(TF)을 촉진하는 능력 때문에 글로벌 자금세탁방지(AML) 규제기관들의 십자선에 프라이버시 코인 점점 더 많이 등장하고 있으며 그결과 많은 거래소에 의해 상장폐지되었다고 보아야 합니다.

오늘은 프라이버시 코인에 대해 알아보겠습니다.

프라이버시 코인이란?

프라이버시 코인은 발신자와 목적지를 흐려 개인 및 익명 블록체인 거래에 힘을 실어주는 일종 암호화폐입니다. 사용되는 기술 중에는 사용자의 실제 지갑 잔고와 주소를 숨기고 여러 트래잭션을 서로 혼합하여 체인 분석을 회피하는 것도 있습니다.

그래서 다크 코인이라고 부르기도 합니다.

이유야 어찌됐든 프라이버시 코인은 높은 수준의 프라이버시와 익명성을 유지하기 위해 블록체인 상에 트랜잭션을 숨기거나 암호화합니다.

참고로 대부분의 코인은 블록체인에 트랜잭션이 공공원장(public ledger)으로 기록돼 누구나 볼 수 있게 공개됩니다. 이런 시스템은 여러 가지 장점이 있지만, 사용자에게 완전한 개인 정보 보호와 익명성을 제공하지 못합니다.

프라이버시 코인은 익명성과 추적 불가능성의 두 가지 다른 측면을 처리합니다. 익명성은 거래 뒤에 정체성을 숨기고 추적 불가능성은 블록체인 분석과 같은 서비스를 이용한 거래의 추적을 제3자가 사실상 불가능하게 만듭니다.

프라이버시 코인에 활용되는 기술

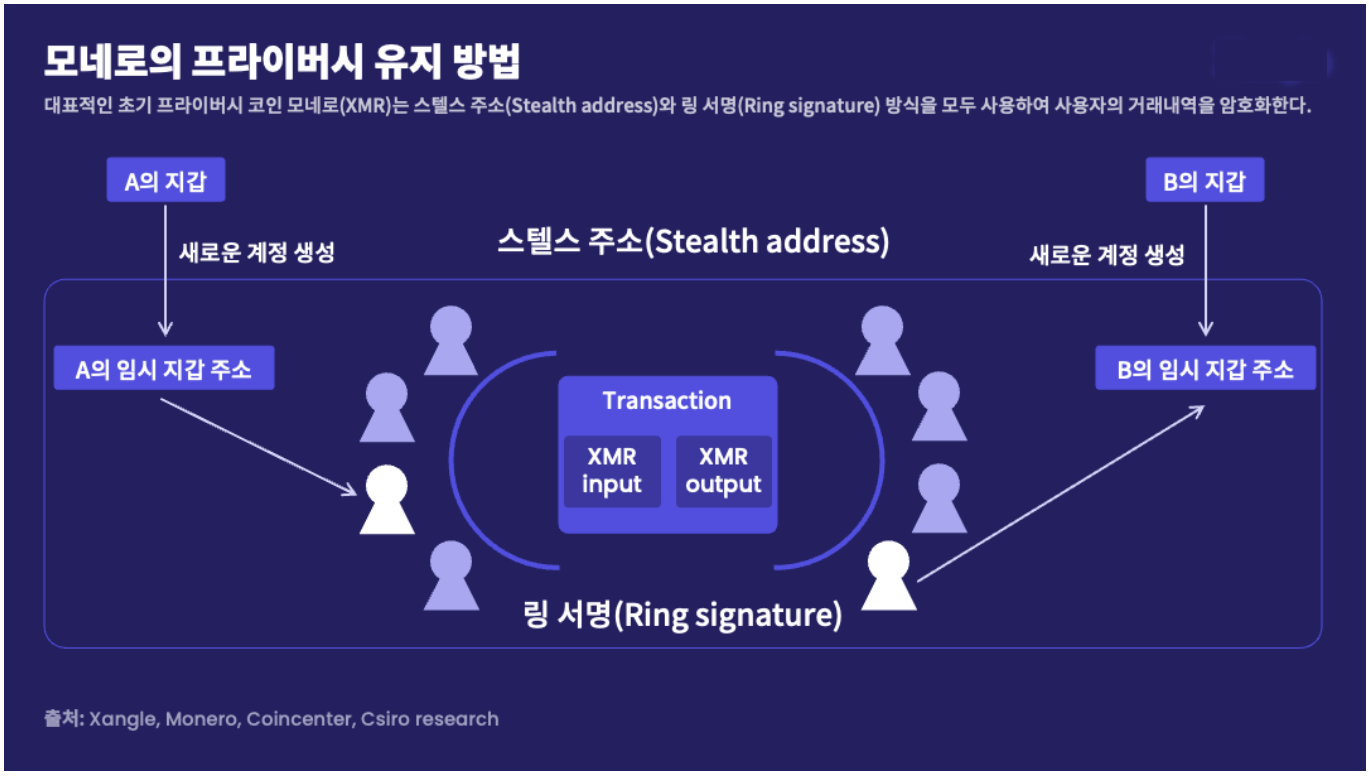
1) 스텔스 주소(Stealth Address)

스텔스 주소는 매 트랜잭션마다 사용할 새로운 주소를 생성하는 방식입니다. 이 방식은 각 트랜잭션마다 새로운 주소를 사용해 거래를 하기 때문에 트랜잭션을 통해 거래주소를 추적하기 매우 어렵게 만듭니다.

2) 링 서명(Ring Signature)

링 서명은 최종적으로 서명한 주소를 밝히지 않고 익명으로 트랜잭션에 서명하기 위해 여러 사용자 주소를 함께 연결하는 방식을 말합니다. 한 주소가 트랜잭션을 위해 자신의 서명을 발송하면 다른 주소들의 서명이 링의 고리처럼 모여있어 외부 관찰자들은 무엇이 진짜 트랜잭션 주소인지 알 수 없습니다.

2012년 나온 바이트코인(ByteCoin)은 이러한 링 서명 방식을 사용해서 사용자의 거래내역을 추적하기 어렵게 만들었습니다. 2014년 바이트코인을 포크하여 만든 모네로(Monero, XMR)는 스텔스 주소와 링 서명 방식을 모두 사용했습니다. 모네로는 스텔스 주소로 새로운 주소를 만들고 이를 링 서명으로 거래를 하는 이중 보안 장치를 통해 외부인이 거래 내역을 추적하는 것을 불가능하게 만들었습니다.



이렇게 초기 단계의 프라이버시 코인들은 스텔스 주소와 링 서명 방식을 통해 지갑 주소를 새로 생성하거나 다른 후보군을 만드는 방식으로 추적 불가능하게 만들었습니다. 이렇게 추적 불가능한 코인들(특히 모네로)은 범죄에도 사용되었습니다.

2020년과 2021년 암호화폐가 점차 주목받고 제도권화의 움직임을 보이자 다수의 주요 거래소에서 상장폐지의 운명을 맞이했습니다.

(3) 코인조인(CoinJoin)

암호학자 그레그 맥스웰이 2013년 처음 고안한 거래 방식으로, 여러 건의 거래를 모아 하나의 묶음으로 섞은 다음 재분배해 거래의 익명성을 강화하는 기술입니다.

코인 믹서(coin mixer)처럼 각각 다른 트랜잭션을 단일 트랜잭션으로 병합합니다.

코인조인은 다양한 개인들의 거래를 하나의 거래로 병합한 다음 새로운 주소를 사용하여 각각의 사용자에게 배포합니다. 각 수식인은 추적성을 줄이기 위해 새 주소에서 코인을 받게 됩니다.

(4) 영지식 스나크(Zk-SNARKs)

영지식 스나크는 발신인, 수신인, 금액 등의 세부 정보를 공유하지 않고 트랜잭션이 유효함을 증명할 수 있는 기술입니다.특정 개인정보를 드러내지 않고 정보를 공유하고 있다는 사실만을 증명하는 암호학 증명 구조입니다.

대표적인 프라이버시 코인

1.모네로 (XMR)

모네로(XMR)는 암호화폐 시장에서 최초의 프라이버시 코인 프로젝트 중 하나입니다. 포괄적인 익명성을 촉진하기 위해 링CT, 스텔스 주소, 링 서명등 강력한 프라이버시 기능을 사용하므로 많은 사람들이 사장에서 최고의 익명 암호화폐로 꼽고 있습니다.

모네로에서 트랜잭션이 시작되면 프로토콜은 스텔스 주소라고 하는 트랜잭션에 대해 임의의 일회용 대상 주소를 생성합니다. 스텔스 주소는 개인 정보를 보호하기 위해 수신자에게 다시 연결할 수 없습니다. 보낸 사람의 익명성을 보호하기 위해 모네로는 링 서명을 사용하여 거래에 서명합니다. 링 서명은 보낸 사람의 공개 키와 기타 여러 공개 키로 구성됩니다. 이렇게 하면 실제 보낸 사람의 신원을 모호하게 만드는 데 도움이 됩니다.

익명성에 중점을 두었기 때문에 거래 추적이 거의 불가능합니다. 그렇기 때문에 주로 모네로는 마약 거래 등 사이버 범죄자들 사이에서도 많이 활용됩니다. 또 자금 세탁 용도로 사용된다고 알려졌습니다.

2.대시

대시(Dash)는 2014년 비트코인의 포크로 시작된 익명 암호화폐입니다. 최초의 프라이버시 코인은 X코인이라고 블렸으며 다크코인으로 바뀌었습니다. 마지막에는 대시로 바뀌었습니다.

대시는 높은 익명성 · 즉시 결제 기능 제공 · 마스터노드가 대시를 지지 등 특징을 가지고 있습니다. 프라이버시를 보호하면서도 빠른 송금과 결제가 가능합니다.이러한 기능들이 구현되는 것은 마스터 노드가 있기 때문입니다.

대시는 PrivateSend 트랜잭션을 실행하기 위해 하이브리드 방식(코인조인이라고 함)을 사용합니다. 코인조인을 사용하면 각 PrivateSend 거래가 많은 소액으로 분할되고 지갑 주소가 다른 PrivateSend 사용자의 주소와 스크램블됩니다. 그런 다음 대시는 모든 트랜잭션을 병합하고 단일 통합 트랜잭션으로 게시합니다. 이 접근 방식은 거래를 해석하고 어떤 금액이 누구에게 속하는지 결정하는 것을 불가능하게 만듭니다.

관련페이지:

대시(DASH)란? 초보자 위한 간략한 소개 - BTCC

3.지캐시

2016년 출시된 지캐시는 비트코인의 포크인 대시와 같은 루트를 공유하는 또 다른 최고 프라이버시 코인입니다. 일렉트릭 코인 컴퍼니가 이끄는 이 암호화폐는 에너지 집약적인 작업증명(PoW) 메커니즘을 사용하여 거래를 확인합니다.

지캐시는 또한 실드 트랜잭션 및 영지식 스나크라고 하는 익명성 및 추적 불가능 메커니즘을 통해 트랜잭션을 숨길 수 있는 선택권을 제공합니다.

프라이버시 코인은 합법입니까?

프라이버시 코인의 합법성은 개별 관할 구역(individual jurisdiction)에 따라 다릅니다.

한국은 정부가 자금세탁 방지를 위해 국내 코인 거래소에서 프라이버시 코인을 거래하는 것을 금지했습니다.

하지만 프라이버시 코인 자체를 금지한 것이 아니기 때문에, 프라이버시 코인의 합법성 여부는 회색 지대에 속해있다고 볼 수 있습니다.

국제 자금세탁방지기구(FATF) 등 글로벌 규제 기관이 프라이버시 코인에 어떤 조치와 규제를 적용할지 지켜보는 것이 중요합니다.

프라이버시 코인은 트래블(자금이동규칙)을 시행하고있는 국가나 거래소들을 통해 제재를 받고 있습니다.

호주와 한국은 코인 거래소에서 프라이버시 코인 거래를 금지했고, 일본은 프라이버시 코인 자체를 국가에서 금지하고 있습니다.

일부 거래소에서 프라이버시 코인 상장폐지 이유

거래 당사자 등을 알 수 없어 자금세탁에 활용될 위험이 높다는 판단되기 때문입니다.

규제 기관은 프라이버시 코인을 상장한 중앙화거래소(CEX)를 감시합니다.

지난 몇 개월 동안 프라이버시 코인은 규제 기관의 엄격한 감시를 받아왔고, 그래서 일부 거래소들은 프라이버시 코인을 상장 폐지해야 했습니다.

프라이버시 코인의 위험성

프라이버시 코인의 위험은 모든 거래를 난독화할 수 있다는 핵심 매력에서 직접적으로 기인합니다. 이는 사생활 보호 코인이 악의적인 행위자에 의해 불법 행위 및 금융 거래에 사용될 가능성을 높이고, 법 집행 기관에서 자금의 흔적을 식별하기 어려울 것입니다.

대부분의 정부에서 프라이버시 코인을 승인하지 않기 때문에 많은 암호화폐 거래소도 프라이버시 코인을 상장할 때 일반적으로 신중합니다. 이것은 일반 암호 화폐 사용자에게 개인 정보 코인의 매력을 크게 줄입니다.

관련페이지:

라이트코인 자금세탁 방지 어렵다…업비트·빗썸, 유의종목 지정 (btcc.com)

라이트코인, 한국 5대 가상자산 거래소 일제히 상장폐지 - BTCC

후오비, 모네로■지캐시 등 '프라이버시 코인' 7종 상장폐지 - BTCC

'믹서' 토네이도캐시, 미 제재대상에 올라…미국내 자산 동결 - BTCC

이오스(EOS)란 무엇입니까? | 코인 소개 - BTCC

암호화폐 선물 거래란? BTCC 4가지 선물계약 유형 소개! - BTCC