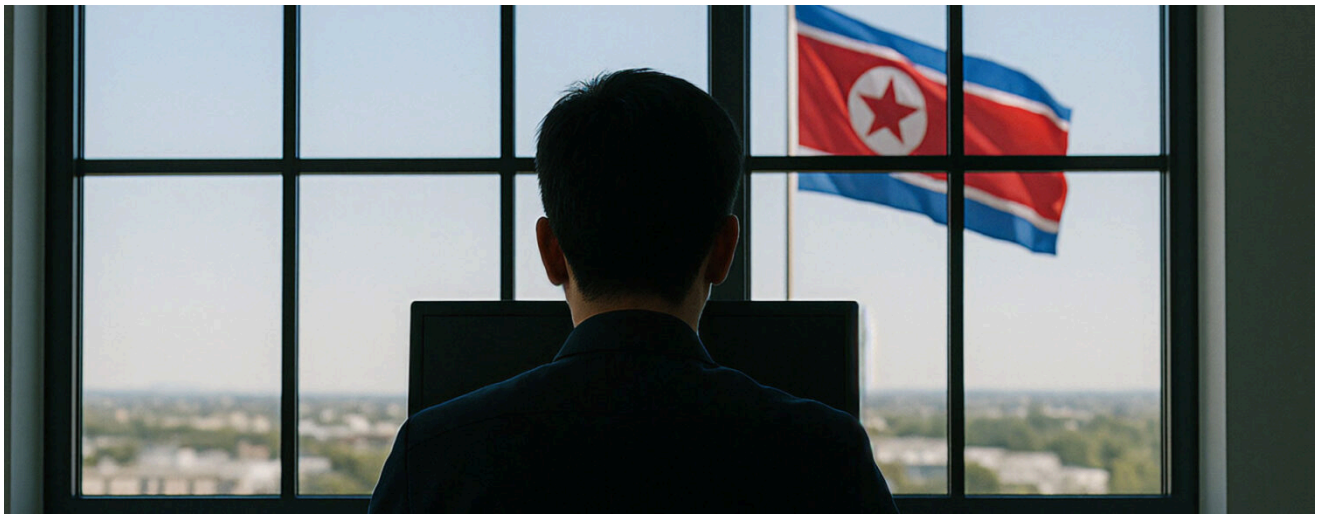
Chainalysis

제재

북한 IT 근로자의 암호화 자산 돈세탁 네트워크 내막

10월 1, 2025 | BY CHAINALYSIS TEAM



※이 기사는 자동 번역되어 있습니다.

북한(DPRK)의 IT 노동자들은 전세계 IT 기업에 잠입해 수익을 얻고 있습니다. 그 수익은 암호화 자산으로 받는 경우가 많으며, 북한의 대량 파괴 무기와 탄도 미사일의 제조 자금이 되고 있습니다. 지난 몇 년 동안 미국 재무부 외국 자산 관리국 (OFAC) 및 한국 외교부 (MOFA)와 같은 규제 당국은 이러한 계획을 가능하게하는 개인과 조직에 제재 조치를 취해 왔습니다. 제재 지정에는 암호화 자산의 주소가 식별자로 포함되는 경우가 많습니다.

Chainalysis는 북한 IT 노동자 체계를 위한 제재 지정에 암호 자산 주소를 추가하고 이 위협에 [illegible] 오픈 소스 정보를 면밀히 추적합니다. 당사는 북한이 암호자산을 활용하여 수익을 창출하고, 자[illegible]

(Chinyong, 일명 Jinyong IT Cooperation Company)에 대한 지급을 중개한 러시아 국적자를 대상으로 한 것입니다. Chinyong은 2023 년 5 월 OFAC 및 한국 외교부에 의해 해외에서 북한 IT 노동자를 고용했다고 제재를 받았습니다.

2023년 초, OFAC은 한국광병 은행사(KKBC)의 대표인 심현 쏘(심)를 제재 대상으로 하고, 암호화 자산 주소도 지정했다. Sim은 북한 IT 노동자 수익의 일부를 포함하여 수천만 달러의 암호화 자산을 받고 있습니다. 또한 상대 거래업체인 Lu Huaying(Lu, UAE 거주 중국인)도 북한 정권을 위해 IT 노동자 자금의 세정에 관여했다고 제재 대상이 되고 있습니다.

이러한 활동은 암호화 자산에 크게 의존하고 수익을 얻고 청소하는 복잡한 네트워크를 돋보이게합니다. 그 때문에 법 집행기관에 의한 적발의 기회도 탄생하고 있습니다. 미국 사법부(DOJ)의 최신 압류 명령에서 알 수 있듯이 고급 블록체인 분석은 IT 근로자의 부정한 자금 세척 네트워크를 탐지 및 박멸하기 위한 독자적인 통찰력과 효과적인 수단을 제공합니다.

본 블로그에서는 북한 IT노동자가 수익을 얻고 세정하기 위한 네트워크, 구조, 운영방법에 대해 설명합니다. 이러한 네트워크를 이해함으로써 법 집행 기관, 규제 당국, 민간 기업은 온 체인에서의 IT 노동자 활동을 감지하고 대량 파괴 무기(WMD) 프로그램에 자금이 흐르는 것을 저지할 수 있습니다.

암호화 자산으로 수익 얻기

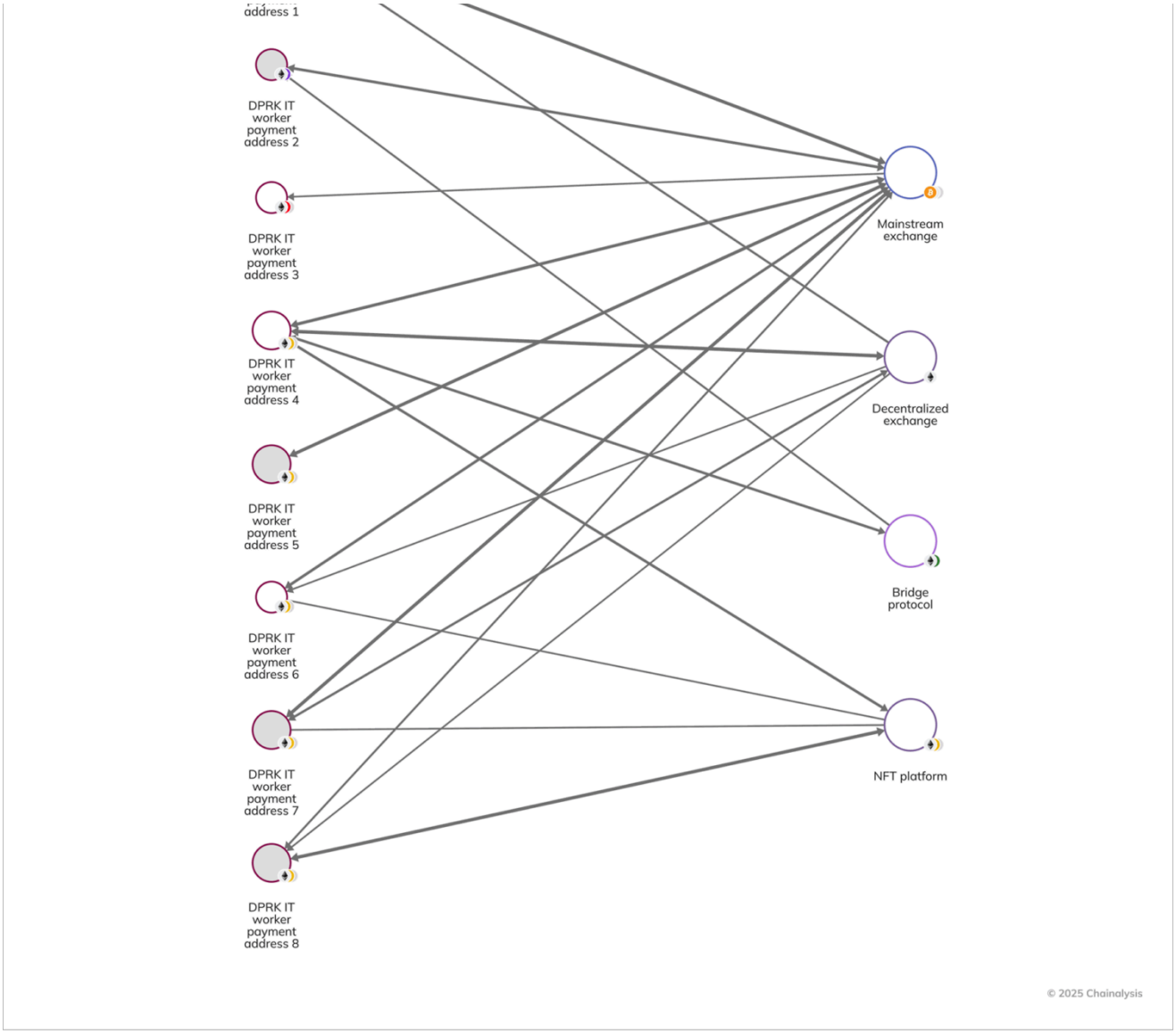
북한 IT노동자들은 보통 청용 등 중개업자를 통해 해외로 파견되어 전세계 IT기업에 응모합니다. 그들은 가상 사설망(VPN), 위조·도난 신분증, AI 음성·얼굴 인증 기술 등 다양한 오브스케이션(은폐) 기법을 구사하여 거주지와 신원을 숨깁니다.

고용 후 안정적인 가치를 가지고 OTC 업체에게 인기있는 스테이블 코인으로 지불을 요구합니다. 북한 IT 근로자의 지불 주소와 관련된 온체인 활동을 조사하면 이러한 월렛은 거의 매달 5000달러 정도의 정기 지불을 확인하고 급여 지불임을 시사합니다.

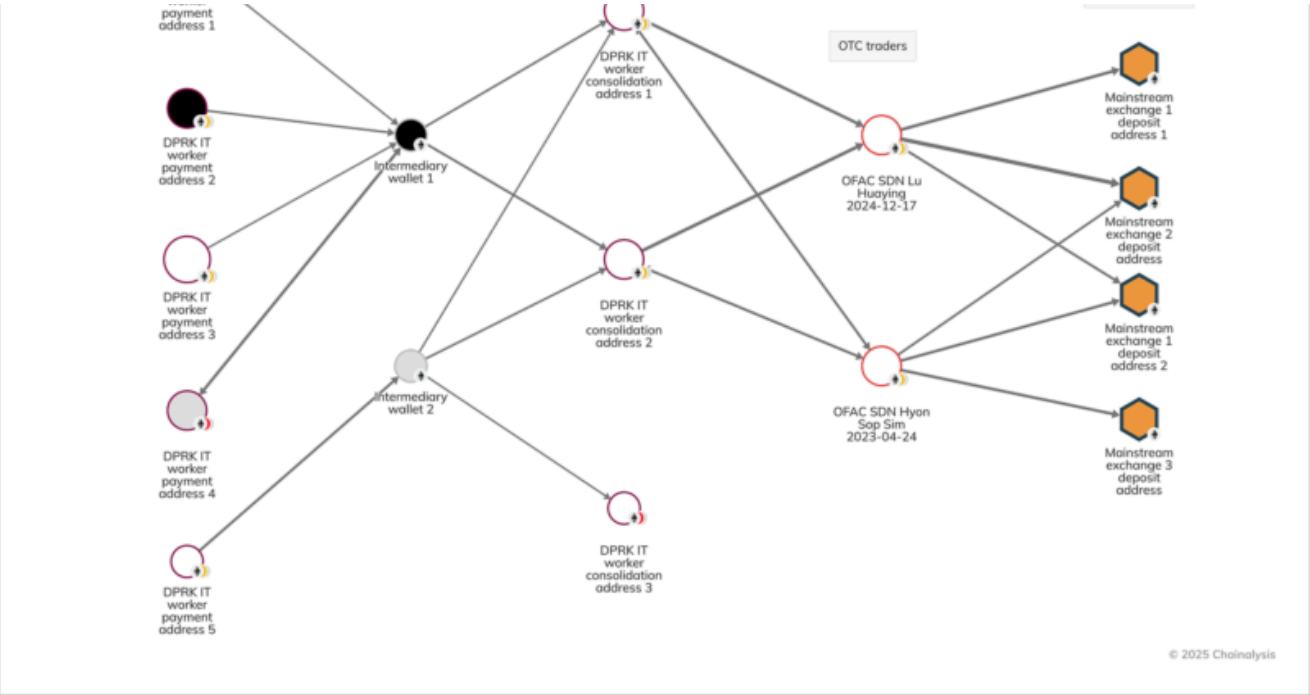
블록체인 기술로 수익 은폐

급여 결제 후 북한 IT 근로자는 여러 자금 세정 방법을 사용하여 암호화 자산을 이동합니다. IT 노동자와 자금 세탁자가 온 체인에서 자금의 기점과 종점을 절단하는 방법 중 하나는 체인 호핑과 토큰 스왑입니다. 분산 형 거래소 (DEX) 및 브리지 프로토콜과 같은 스마트 계약을 활용하여 자금 추적을 어렵게 만듭니다.

아래의 Chainalysis Reactor 그래프에서는 분산형 프로토콜이나 브릿지, 일반적인 거래소가 자금 흐름의 은폐에 활용되고 있는 모습을 알 수 있습니다.



북한 IT노동자는 자금세정 프로세스를 원활하게 진행하고 최종적으로 북한으로 송금하기 위해 중개자도 활용합니다. DOJ의 자금 압류 명령에 따르면 IT 노동자의 지불 자금은 다른 범죄 수익이나 북한 IT 노동자의 자금과 혼합(계층), 가짜 신분증으로 메인스트림 거래소에 계정을 개설한 정권 관계자에게 송금됩니다.

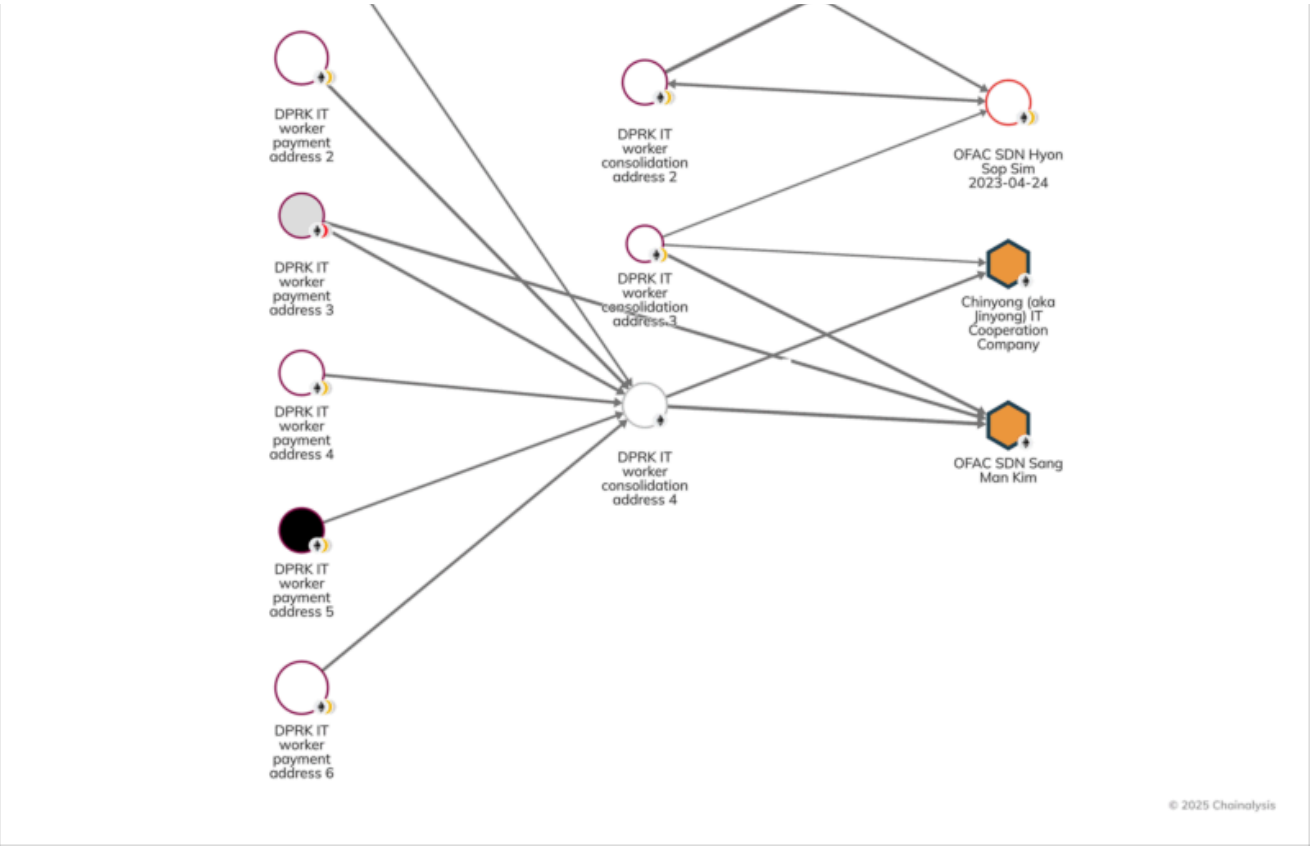


북한의 자금세탁자는 위신분증으로 거래소 계정을 개설하고 있습니다만, 타국에서 활동하는 사람은 본명으로 개설하는 경우도 볼 수 있습니다. DOJ의 명령에 따르면 Sim은 가짜 러시아 신분증을 사용했으며 Lu는 자신의 이름과 UAE 거주 카드로 FTX (현재 폐쇄됨) 계정을 개설했습니다.

A copy of the Russian identification documents utilized by Kim to open accounts, as per the DOJ civil forfeiture.

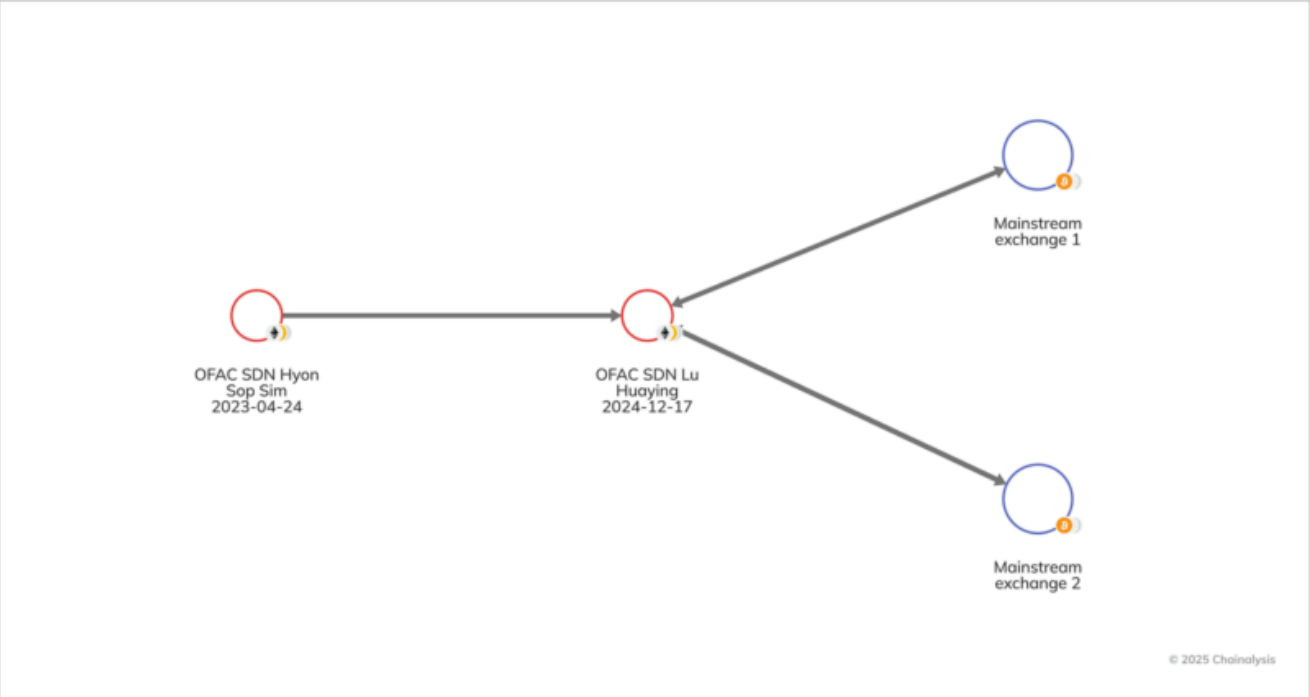
자금 압류 명령은 북한 IT 노동자의 자금이 치영의 대표인 김상만(KIM), KKBC 소속인 심현소프(SIM), 그리고 2024년 12월 UAE의 프론트 기업을 사용해 평양으로의 부정자금송금으로 제재된 OTC 업체 Lu로 송금됐다.

아래의 Reactor 그래프는 북한 IT노동자의 자금이 KIM의 거래소 계정이나 SIM·Lu가 운영하는 언호스테드 월렛에 송금된 흐름을 나타내고 있습니다.



수익을 법정 통화로 현금화

북한 IT 노동자가 블록체인에서 수익을 씻고 북한 정부 대리인에게 송금한 후 이 자금은 법정 통화로 교환됩니다. 대부분의 경우 메인스트림 거래소의 가상 계정과 OTC 업체를 통해 현금화됩니다. 아래 그래프는 SIM이 Lu에 강하게 의존하고 북한 정권을 위한 자금세정을 하고 있던 모습을 보여줍니다.



앞으로도 법 집행 기관의 주요 목표가 될 것입니다.

영국 재무부 OFSI와 미국 FBI의 인터넷 범죄 불만 센터가 발행하는 권고는 민간 기업이 감시 및 식별해야 할 위험의 징후 (레드 플래그)를 보여줍니다. 주요 주의점은 신원·장소·증명서의 불일치, 익명화 인프라의 이용, 불규칙한 지불 흐름, 은폐를 나타내는 행동 등입니다. 온체인 및 오프체인 지표를 검토함으로써 IT 업계 관계자는 이러한 자금 파이프라인 차단에 크게 기여할 수 있습니다.

기업이 북한 IT노동자의 활동을 파악하기 위해서는 다음과 같은 구체적인 점검이 필요하다. IP소재지와 신고소재지가 일치하지 않는, 신분증이 조작되고 있는, 화상 통화를 거부한다 · AI 생성 프로파일을 이용하는, 스테이블 코인으로의 지불 희망, 복수 지갑에의 분할 지불 요구, 복잡한 제3자 지불을 요구하는, 기술력이 높은 것에 비해 보상이 시세보다 낮은 등입니다. 이러한 점검을 컴플라이언스 체제에 통합하고 계약자와의 상호 작용을 상세하게 기록함으로써 기업은 모르게 북한의 제재 회피를 조장 할 위험을 피할 수 있습니다.

사이버 범죄 | 머니 론더링 | 돈세탁 | 마네론 | 북한

북한 IT노동자 | 암호화 자산 범죄 | 조선민주주의인민공화국 | 도난 자금

자금 세척