Chainalysis

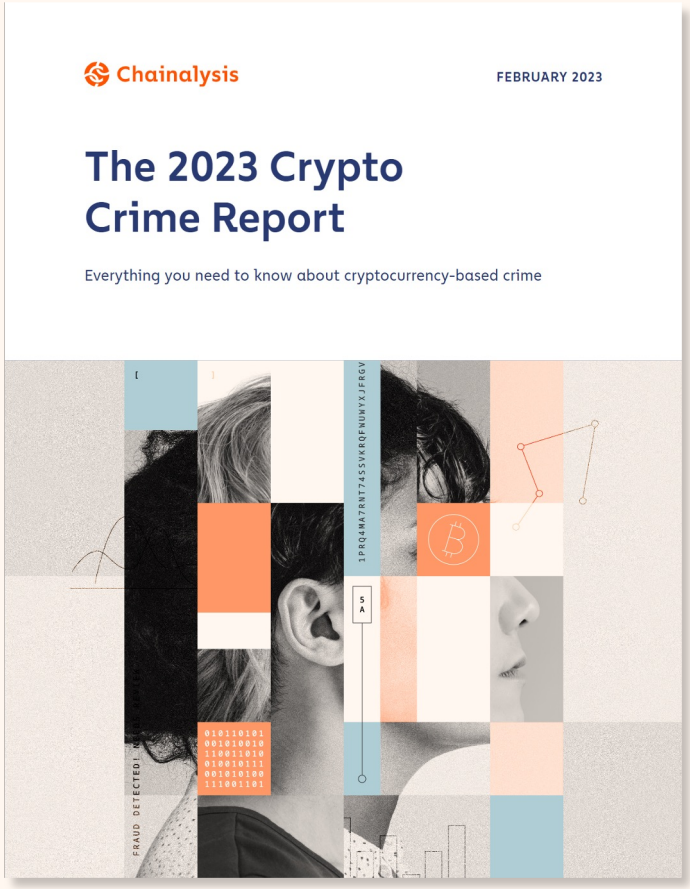
가상자산 해킹 기술 동향 및 피해 사례에 대하여

체이널리시스 코리아
송용일 차장

G-PRIVACY 2023
2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

Agenda

- 2023 가상자산 범죄 보고서
- 블록체인 분석의 주요 요소
- 가상자산 해킹 기술 동향 및 피해 사례 연구:
  - Liquid / Axie Infinity & Ronin Bridge / Harmony / Qubit
  - NFT 와 범죄
- 2022 글로벌 가상자산 지수

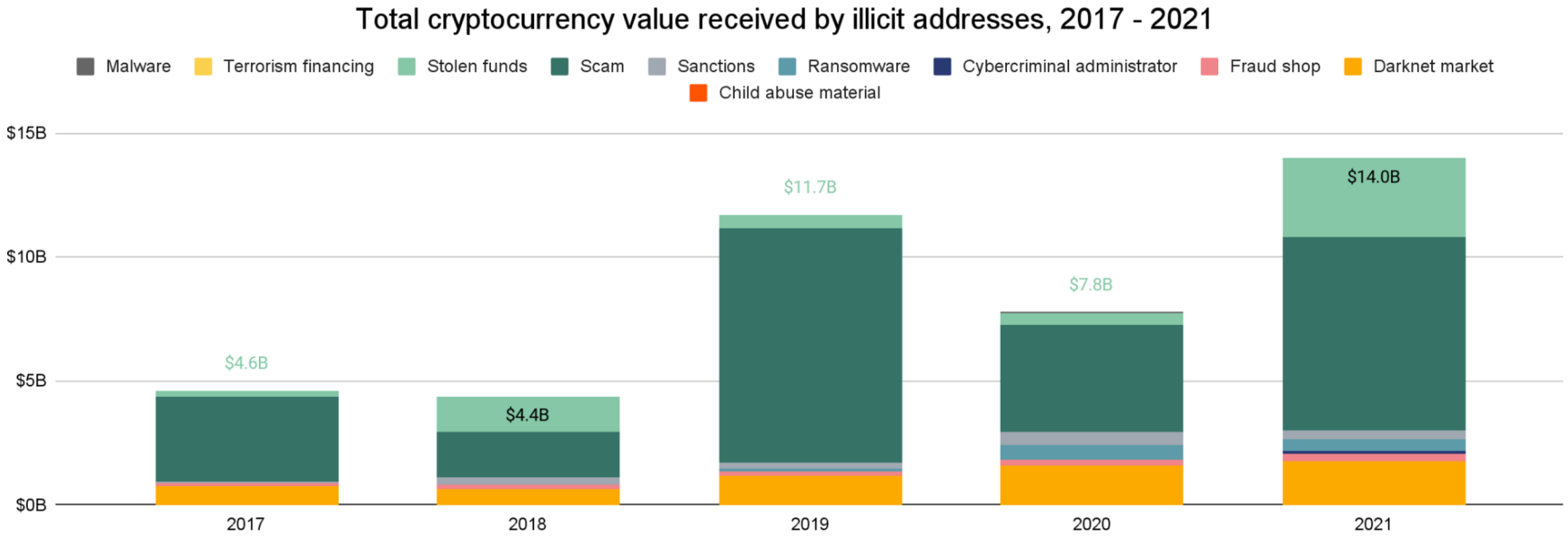


2023 가상자산 범죄 보고서 - 체이널리시스 웹사이트에서 다운로드 받으세요

chainalysis.com

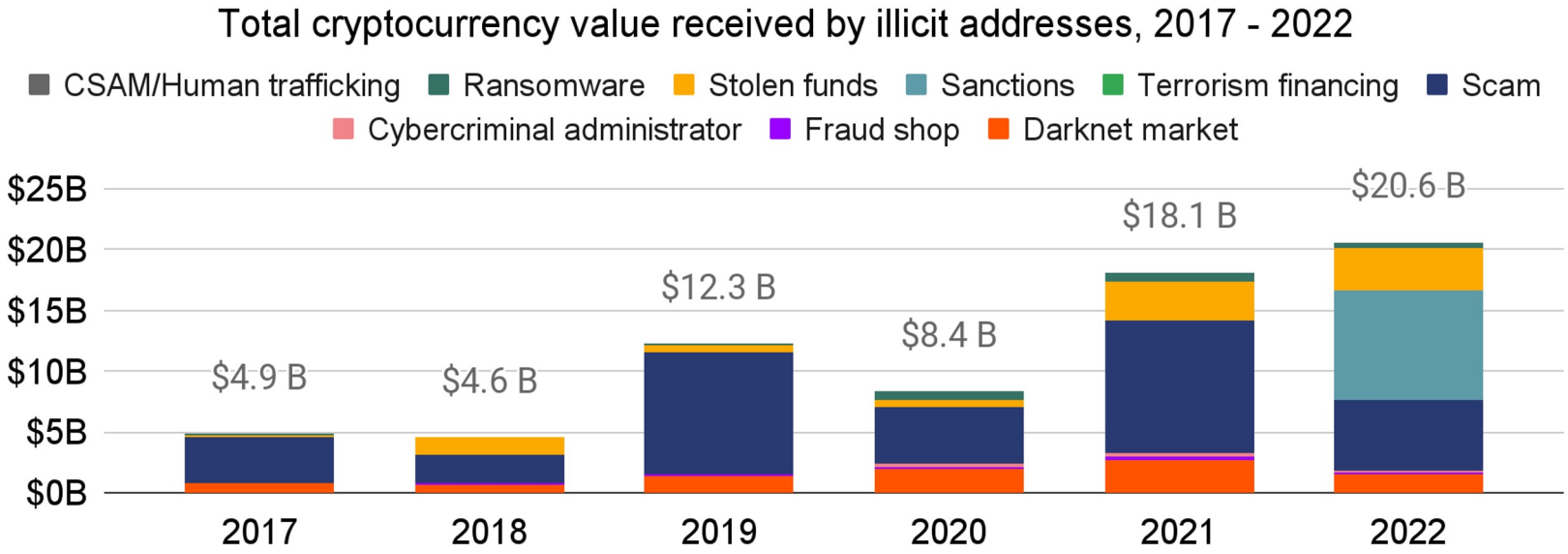
The 2022 Crypto Crime Report

2021년에 가상자산 내 불법 거래 활동이 사상 최고치를 기록

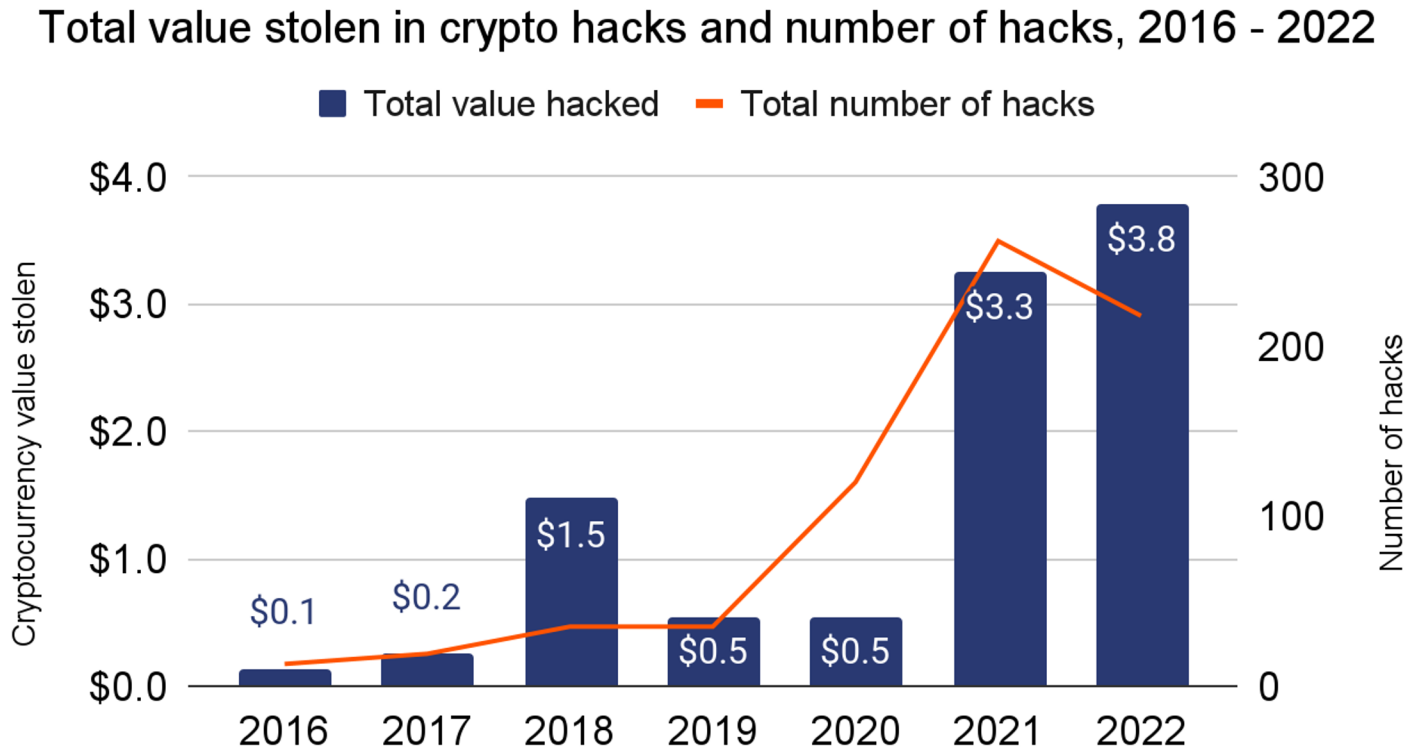


The 2023 Crypto Crime Report

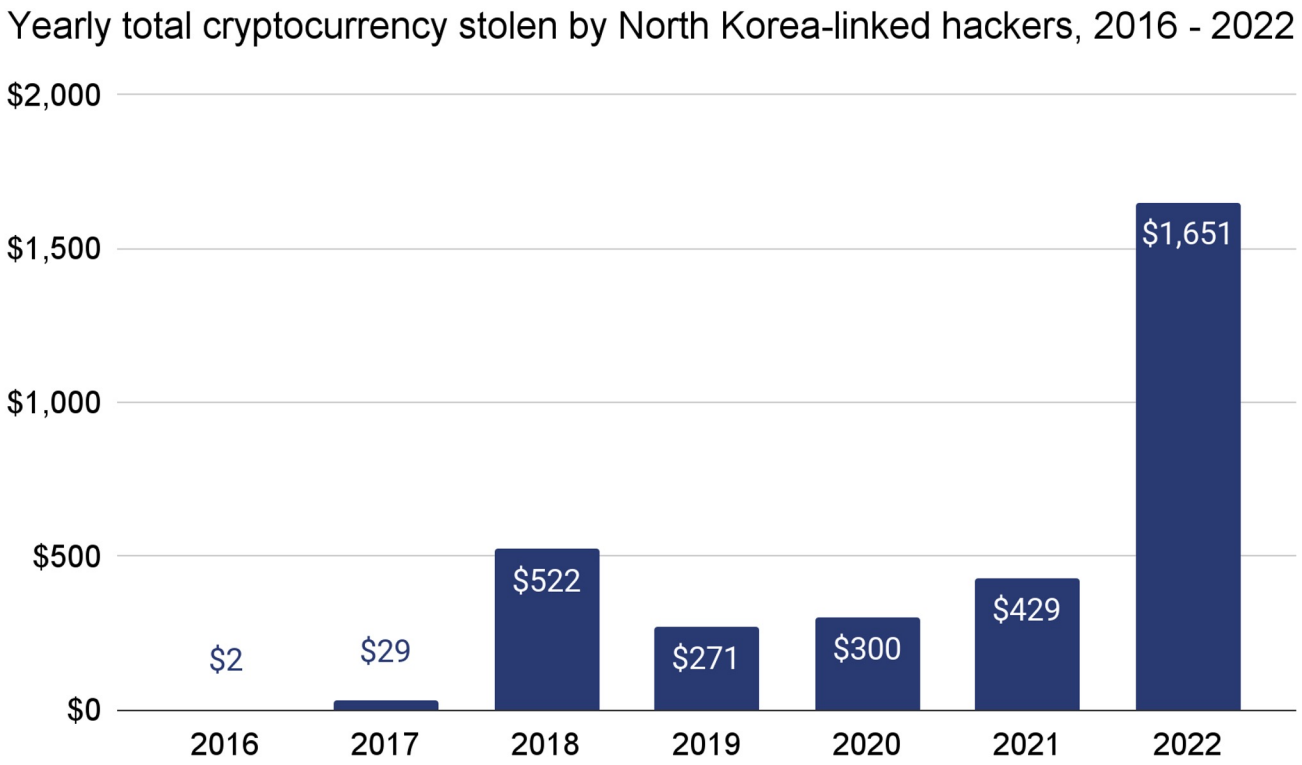
2022년에 가상자산 내 불법 거래 활동이 사상 최고치를 기록



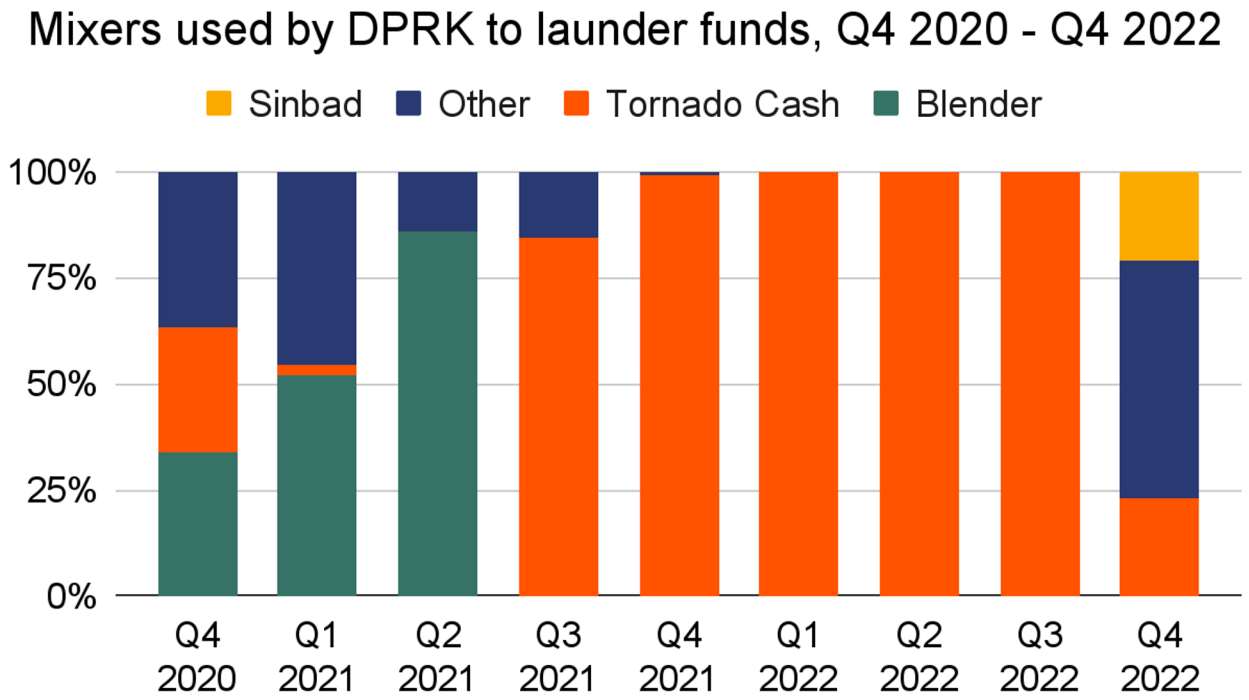
Hacking hits all time highs after record 2021



북한은 2022년 가상자산 해킹 급증의 주범



북한이 자금 세탁에 사용하는 믹서



2023 가상자산 범죄 보고서 요약

2022년에 식별된 불법 가상자산 거래액: $20.2B (한화 26조 2,600억원, 환율 1,300원 기준)

해킹된 가상자산 총액: $3.8B (한화 4조 9,400억원)

Pig-Butchering, NFT & Crypto 사기에 연루된 금액: $5.9B (한화 7조 6,700억원)

랜섬웨어로 송금된 금액: $0.45B (한화 5,850억원)

믹서로 세탁된 금액: $7.8B (한화 10조 140억원)

다크넷 마켓플레이스로 유통된 금액: $1.5B (한화 1조 9,500억원)

Chainalysis

블록체인 분석의 주요 요소

가상자산 산업에서의 주요 이슈

가상자산이 주류가 되었지만 불법적인 활동에 오용되기도 합니다. 이는 산업의 신뢰성을 훼손하고 번영을 저해합니다.

200억 달러 상당의 거래가 불법 활동과 관련되어 있습니다.

- 스캠
- 아동 성착취물
- 거래소 해킹
- 다크넷 마켓
- 테러리스트 자금 조달
- 랜섬웨어

Concerns

거래소	규정 준수 실패로 인한 거래소 폐쇄
금융 기관	평판 위험
법 집행 기관	사이버 범죄 및 자금 세탁

가상자산을 보다 투명하게 만들어 불법 행위에 대해 조치를 취해야 합니다.

가상자산은 왜 오용되는가?

가상자산이 불법적인 활동에 사용되는 이유는 크게 세 가지입니다.

가상자산이 오용되는 이유

편의성	결제 기관, 은행 등 중개기관 없이 인터넷으로 간편하게 거래
유동성	금전적 가치와 유동성이 있다
(유사)익명성	**소유자를 쉽게 식별할 수 없다.**

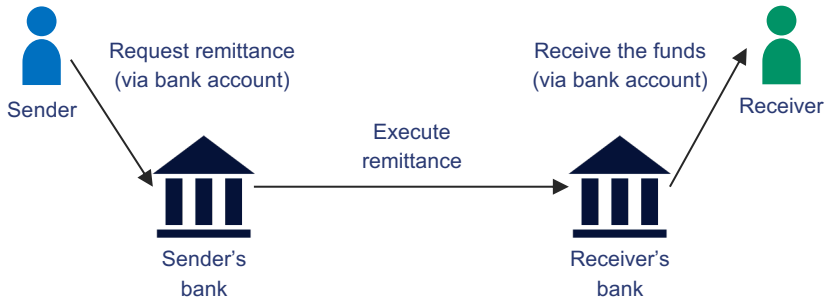
가상자산 거래에 관련된 사람들을 식별하기 어려운 이유는 무엇입니까?
기존 금융 시스템과 크게 다른 점은 무엇입니까?

가상자산 거래의 특성

은행이나 결제 서비스 등 중개자가 개입하는 기존 금융 시스템과 달리 암호화폐는 중개자 없이 P2P 방식으로 교환할 수 있습니다.

기존 화폐 거래

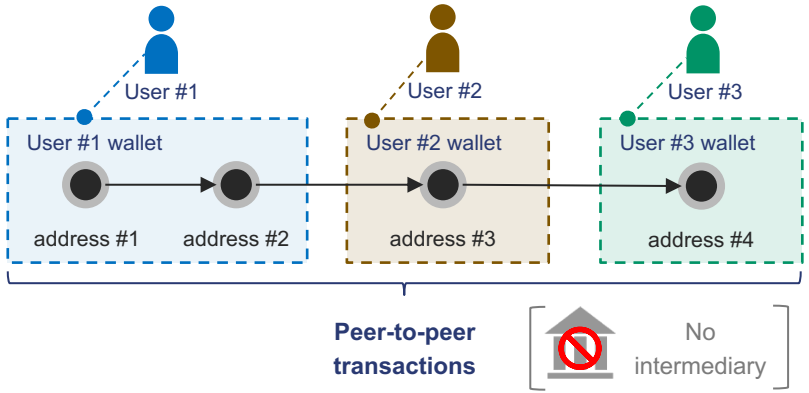
모든 거래는 항상 송금인과 수취인의 정보가 있는 금융 기관을 통해 전달됩니다.



각 금융기관에서 거래에 관여한 사람을 식별할 수 있습니다.

가상자산 거래

모든 거래는 P2P 방식으로 이루어지며 중개 서비스를 거치지 않아도 됩니다.



VASP 주소와 연결되어 있지 않으면 거래에 관련된 사람을 식별할 수 없습니다.

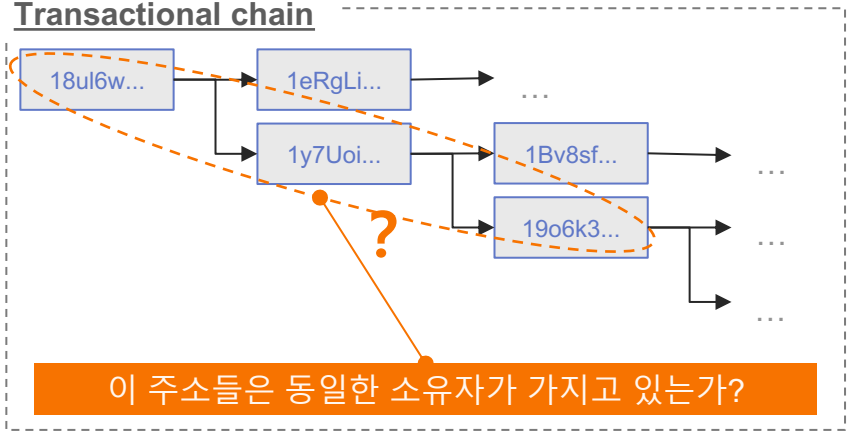
블록체인 데이터에서 가상자산의 자금을 추적할 수 없습니까?

가상자산에서 특정 자금 추적의 어려움

가상자산의 거래 데이터는 공개되어 누구나 접근할 수 있지만, **누가** 자금을 송금/수신했는지 식별하는 데 어려움이 있습니다(가명성).

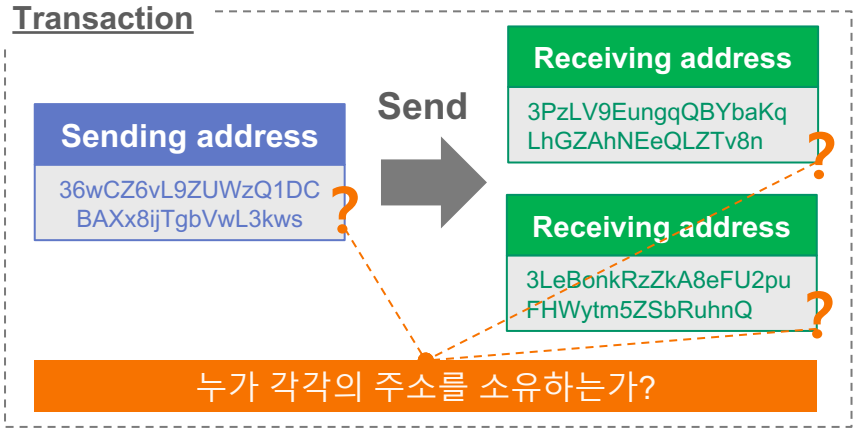
주소는 제한 없이 생성됩니다.

주소를 무제한 생성할 수 있기 때문에 누가 자금을 보유하고 있는지 파악하기 어렵습니다.



주소는 누군지 알려주지 않습니다

주소는 영문과 숫자로 이루어진 문자열일 뿐입니다.
추가 조사 없이는 누가 그것을 소유하고 있는지 알 수 없습니다.



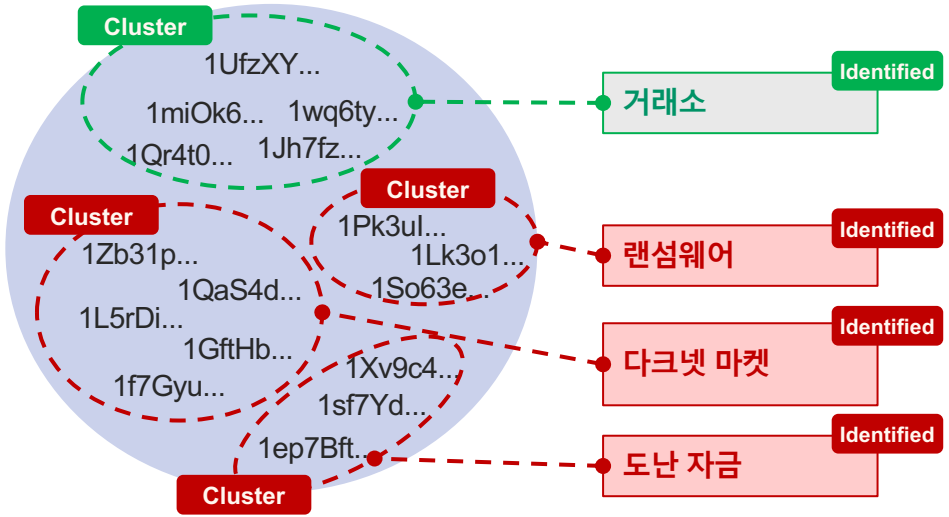
그러나 분석 능력으로 이러한 "가명성"을 극복할 수 있습니다.

클러스터링과 식별

유사 익명성을 극복하기 위해 단일 엔티티가 소유한 여러 주소를 그룹화(클러스터링)하여 클러스터를 제어하는 엔티티(식별)를 결정해야 합니다.

클러스터링	트랜잭션 패턴을 분석하여 여러 주소를 그룹화하고 단일 엔터티에 연결
식별	웹 크롤링 및 지상 조사와 같은 방법으로 클러스터된 주소를 누가 제어하는지 정확히 식별

시각적 표현



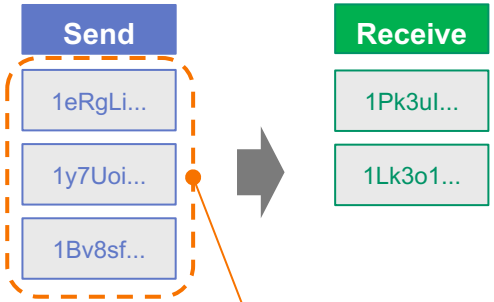
클러스터링 및 식별을 통해 자금 흐름을 쉽게 추적하고
해당 주소에 어떤 서비스가 연결되어 있는지 확인할 수 있습니다.
체이널리시스는 클러스터링 및 식별을 위한 데이터 연구를 전문으로 합니다.

클러스터링 기술

여러 주소를 동일한 엔터티가 소유한 클러스터로 그룹화하는 몇 가지 기술이 있습니다.

Co-spend Analysis

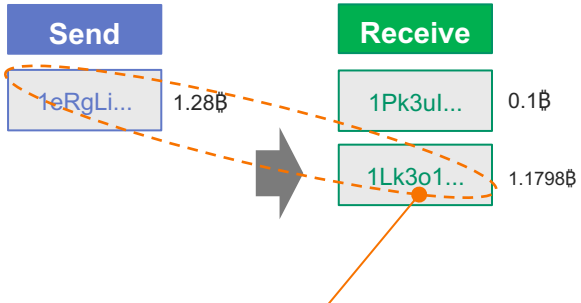
모든 송금 주소가 동일한 지갑(소유자)의 소유라고 생각하고 함께 병합합니다.



단일 클러스터로 병합

Change Analysis

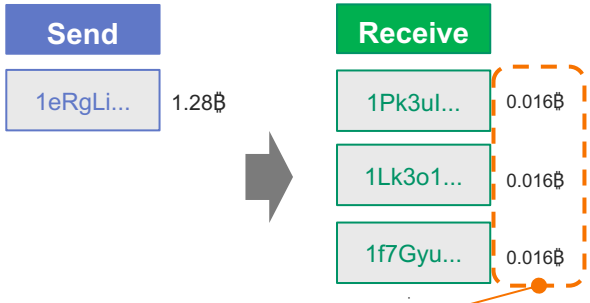
수신 주소 중 하나를 잔액(Change) 주소로 간주하고 송금 주소와 병합합니다.



잔액 주소는 송금 주소와 병합

Behavioral Analysis

서비스 또는 지갑의 특정 거래 패턴을 분석하고 그것이 무엇인지 식별합니다.



서비스에 특화된 거래 패턴으로 분석

Co-spend 분석은 가장 안정적인 방법이며 체이널리시스는 Co-spend 주소 클러스터링을 자동화합니다.

식별

블록체인 데이터만으로는 해당 주소의 소유자가 누구인지 알려주지 않기 때문에 Chainalysis는 아래와 같은 여러 방법으로 클러스터 소유자를 식별합니다.

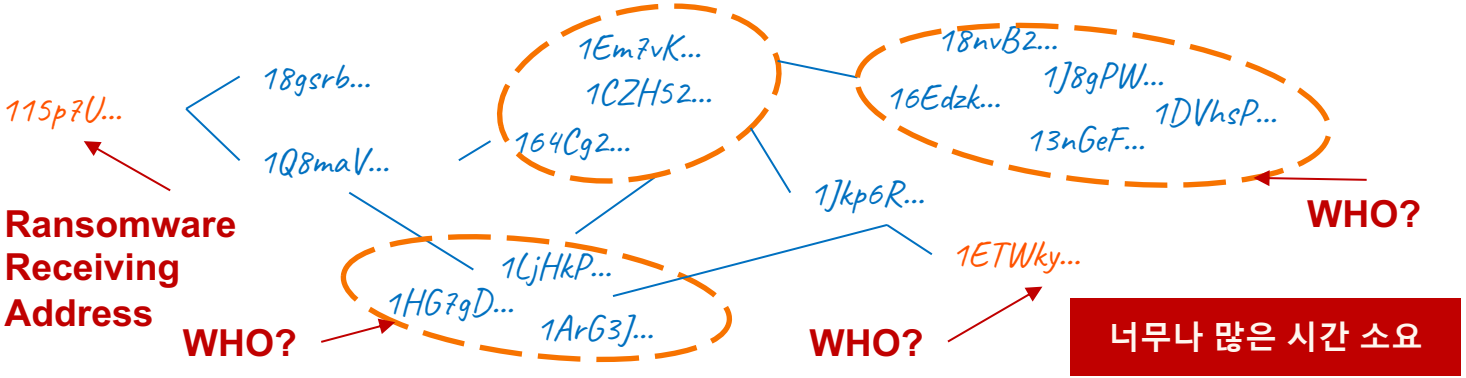
OSINT	웹사이트, 포럼 및 소셜 미디어를 확인하여 특정 엔터티 또는 서비스에 대한 암호화폐 주소 및 관련 정보를 찾습니다.
Making transactions	해당 서비스에 입금 및/또는 출금하고 암호화폐 주소와 매핑합니다.
Information sharing	Chainalysis 사용자 및 법 집행 기관으로부터 정보를 수신합니다.

위의 방법으로 Chainalysis는 서비스 수준의 식별을 수행합니다(개인 수준의 식별은 아님).

블록체인 분석 도구의 중요성

블록체인 분석 도구는 트랜잭션 흐름의 클러스터링/식별 및 시각화를 위한 광범위한 수동 작업을 크게 줄입니다.

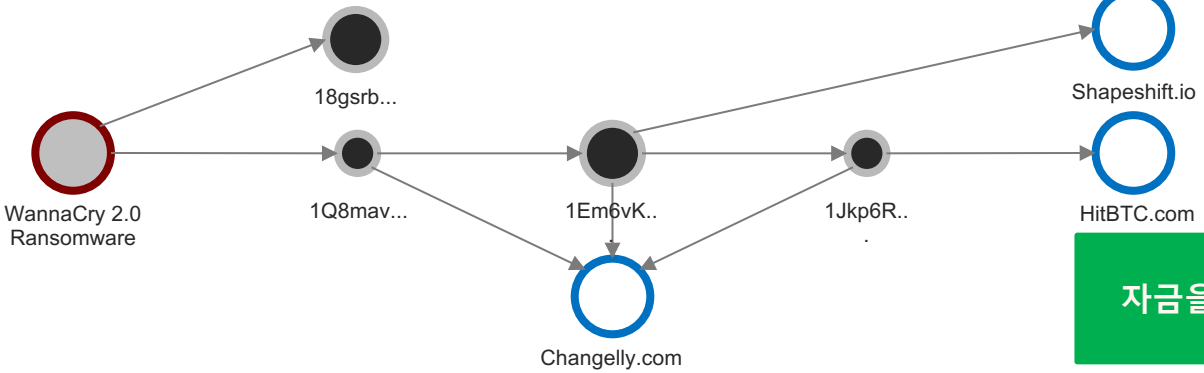
블록체인 분석도구 없이 수동 작업



너무나 많은 시간 소요

블록체인 분석도구 이용

(Chainalysis Reactor)



자금을 추적하기 쉬움

체이널리시스 리액터: Investigation tool

리액터를 사용하면 클러스터에 어떤 종류의 엔터티가 노출되어 있는지 확인하고 자금 흐름을 시각화하여 자금을 어디서 받고 보냈는지 명확히 할 수 있습니다.

Key features

1 Make a graph

- 클러스터 간의 트랜잭션 링크 시각화

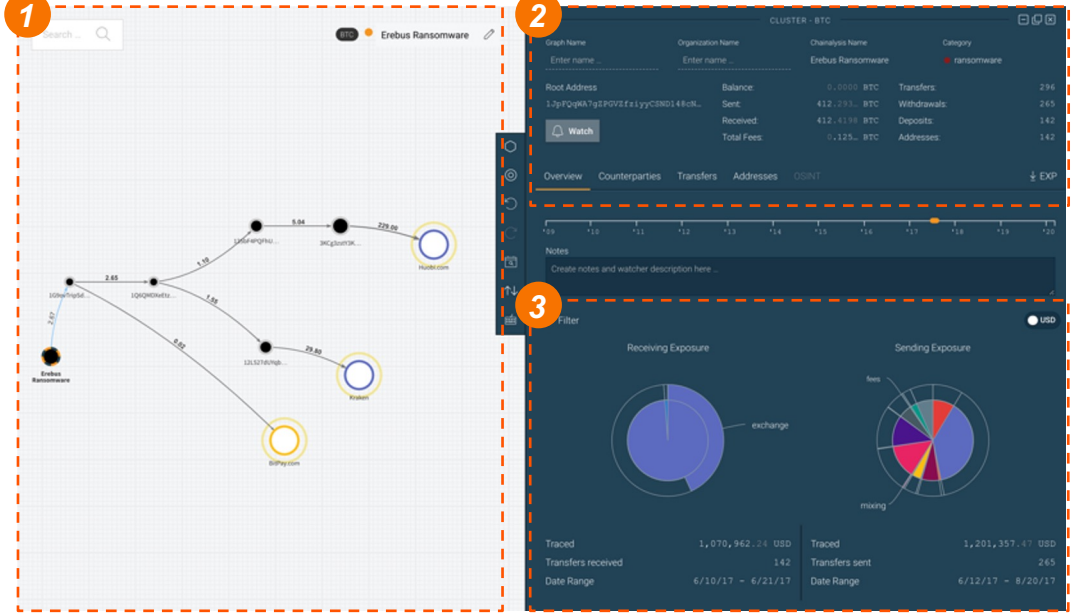
2 Check cluster information

- 주소
- 잔고 및 거래금액
- 클러스터 범주
- 거래상대방

3 Check exposure

- 클러스터에 어떤 종류의 엔터티가 노출되었는지 확인

Screenshot



Workflow in blockchain analysis

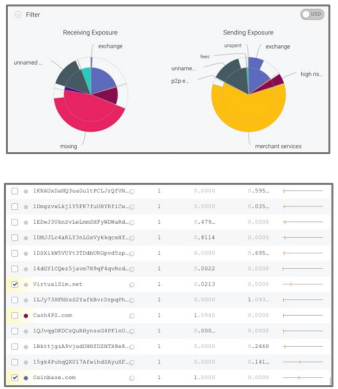
의심스러운 주소를 알게 되면, 블록체인의 자금을 따라가서 관련 클러스터와 서비스 간의 연결을 찾아 실제 개체의 정보를 찾습니다.

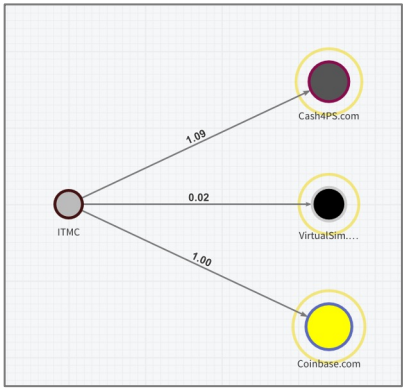
Search address → **Check counterparties** ⇄ **Trace funds forward/back** → **Inquire at service**

여러가지 방법으로 의심스러운 주소 검색:

- OSINT
- Making transactions
- Case investigation

1MMaU5nTrFdPZotfwdbv1wWnFjLCTFbpPY





Cash4PS
(High risk exchange)

VirtualSim.net
(Service offering a phone number for SMS without KYC)

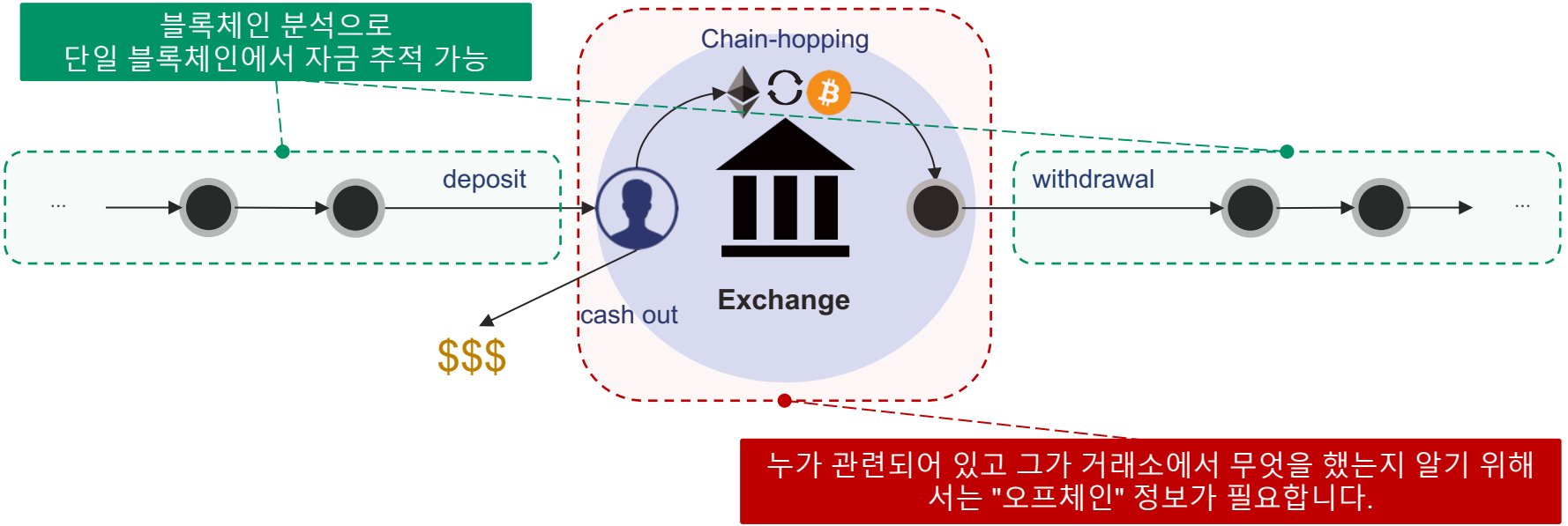
Coinbase
(Compliant exchange)

Candidate for subpoena

KYC를 수행하는 서비스에 자금이 들어가는 것을 발견하면 자금을 받은 사람에 대해 소환

거래소 - 수사를 위한 중요한 포인트

거래소는 가상자산 교환 및 현금 인출 서비스를 제공하고 KYC 정보를 가지고 있기 때문에 가상자산의 자금을 추적하는 매우 중요한 포인트입니다.



블록체인 분석에서 다룰 수 없는 정보를 얻기 위해서는
거래소에 대한 소환장 요청 등 다른 방법이 필요합니다.

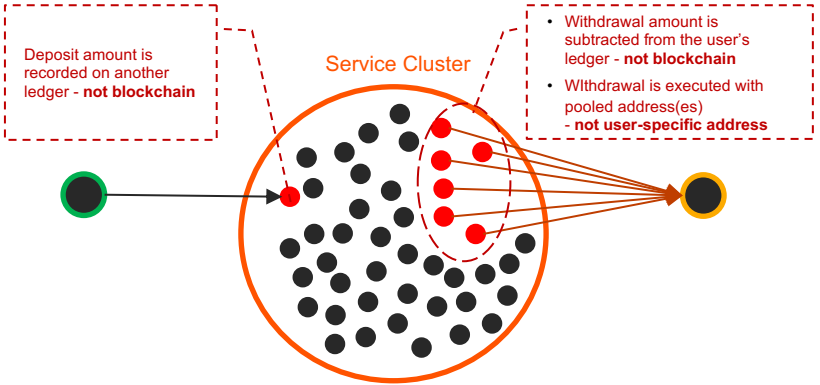
주의: 서비스를 통한 자금 추적의 한계

서비스에 속한 주소는 사용자가 소유하지 않기 때문에 블록체인 분석으로 서비스에 한 번 입금된 자금을 추적할 수 없습니다. 서비스가 소유한 풀링된 주소 중 하나일 뿐입니다.

https://blog.chainalysis.com/reports/blockchain-analysis-trace-through-service-exchange

서비스가 잔액 및 주소를 관리하는 방법

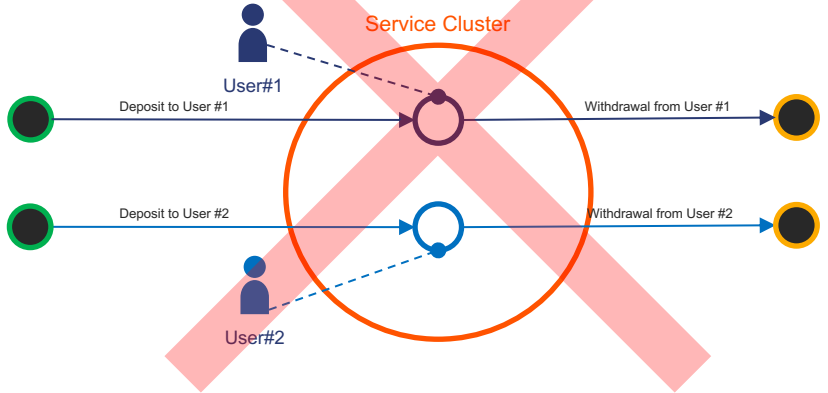
- 서비스 계정의 잔액은 블록체인 외부의 원장에 기록됩니다.
- 입금 주소는 특정 사용자의 자금을 받기 위해 사용되지만 입금 후 자금의 이동은 서비스에 의해 제어되며 사용자와 관련이 없습니다.



서비스가 제어하는 주소는
특정 사용자와 연결되어 있지 않습니다.

일반적인 오해

- 서비스 계정의 잔액은 사용자별 암호화폐 주소에 기록됩니다.
- 블록체인 분석은 거래소 사용자의 자금 이동을 추적할 수 있습니다.



서비스 사용자의 잔액은 서비스 주소와 연결되지 않습니다.

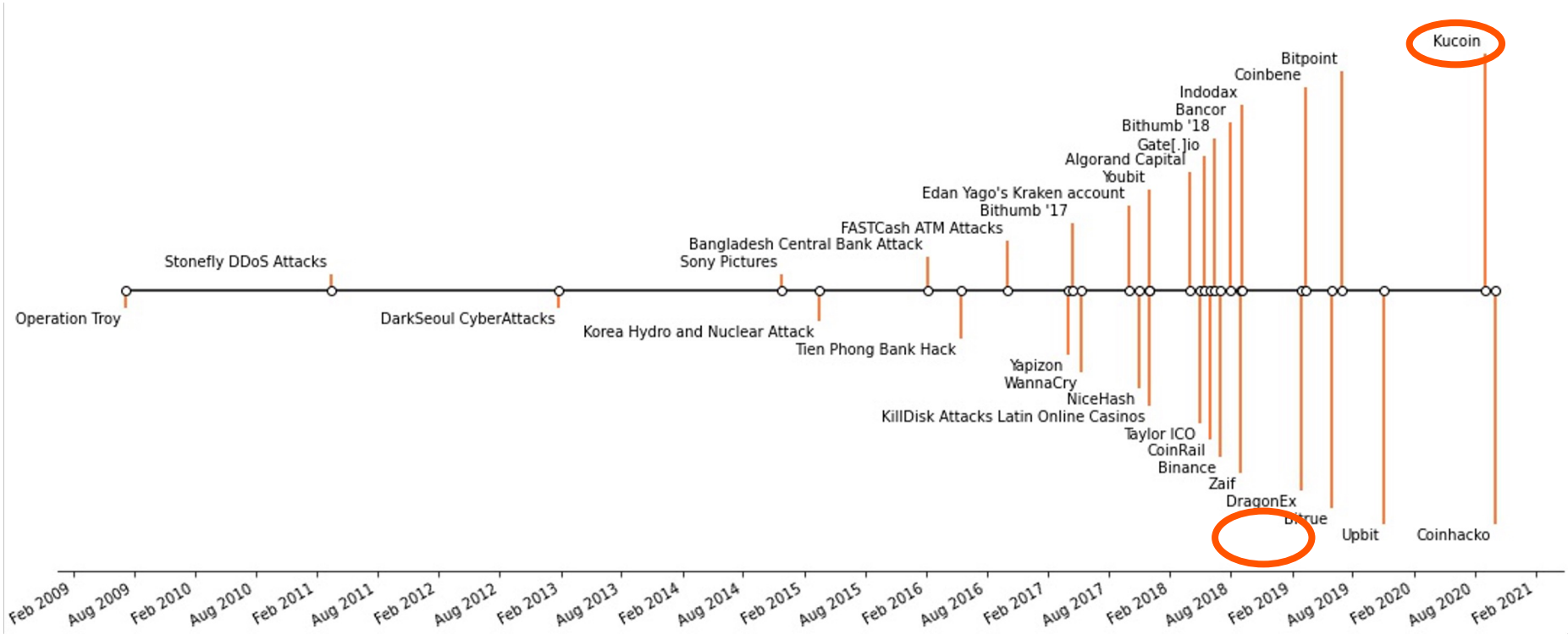
가상자산 해킹에 대한 DPRK의 특징 분석

가상자산 대상 해킹 및 DPRK 분석

체이널리시스는 2014년 마운트곡스 거래소 해킹사건을 시작으로 전세계적인 가상자산 대상 범죄 수사에 참여해오고 있습니다. 이를 통해 수십건의 가상자산 대상 DPRK의 해킹 사건을 분석해왔으며, 축적해온 정보를 기반으로 아래와 같은 최근 해킹 사건 또한 국내외 수사기관과 협업하여 분석중입니다.

- Liquid.com Hack
- Axie Infinity Ronin Bridge Hack
- KuCoin
- DragonEx
- Harmony Horizon Bridge Hack
- Nomad Chain Bridge Hack

가상자산 중심의 해킹 활동을 도입한 이후, 북한의 사이버 공격 빈도가 증가하고 있는 것으로 보입니다.



DPRK Crypto 해킹의 특징

- 최초 도난 이후, 아래 흔적들을 찾을 수 있습니다
  - 사회 공학 기법 사용
  - 체인 호핑(Chain hopping)
  - 시험 입금 후 입금 금액 증가
  - 필 체인(Peel chains)
  - 믹싱 또는 코인조인 서비스 이용
  - 통합(consolidation) 또는 중개(intermediary) 지갑 사용

- 그 후, 도난 자금은 아래와 같이 이동합니다.
  - 믹싱 서비스로 전송
  - 믹싱 서비스, 거래소를 거쳐 현금화 시도
  - 믹싱 서비스를 거쳐 개인 지갑으로 이동 후 유휴 상태로 변경
  - 장외 거래(OTC)를 통해 청산

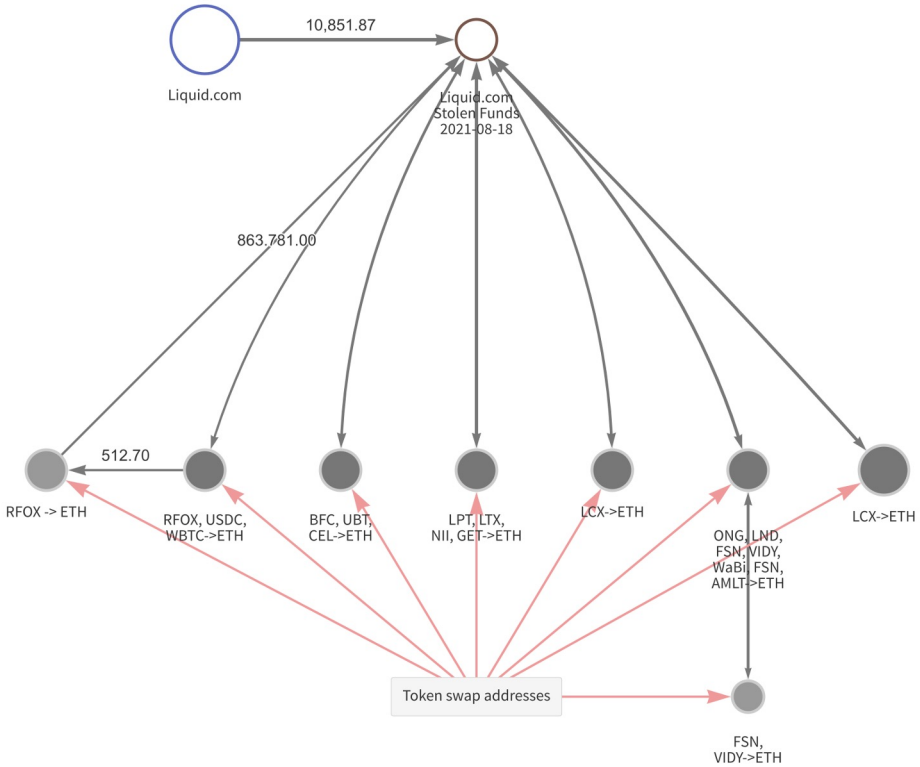
DPRK 불법자금 분석 기술
- Liquid.com

Liquid.com 해킹

- 2021년 8월 19일, 가상자산 거래소 Liquid.com 은 한 비인가 사용자가 Liquid 에서 관리하는 일부 가상자산 지갑에 접근했다고 발표.
- 전날 밤 **67**가지의 **ERC-20** 토큰이 상당한 양의 이더리움 및 비트코인과 함께 해당 지갑들에서 북한을 위해 활동하는 단체가 통제하는 지갑으로 이동.
- 이 공격자는 이후 탈중앙화 프로토콜을 이용해 각종 ERC-20 토큰을 이더리움으로 스왑.
- 그리고 이더리움을 한 데 모아 비트코인으로 바꾸고 모든 비트코인을 합쳐 새로운 지갑으로 통합한 다음, 아시아 소재 가상자산-법정통화 거래소로 자금을 입금.
- 결과적으로 약 9,135만 달러 정도의 가상자산이 세탁되었습니다.

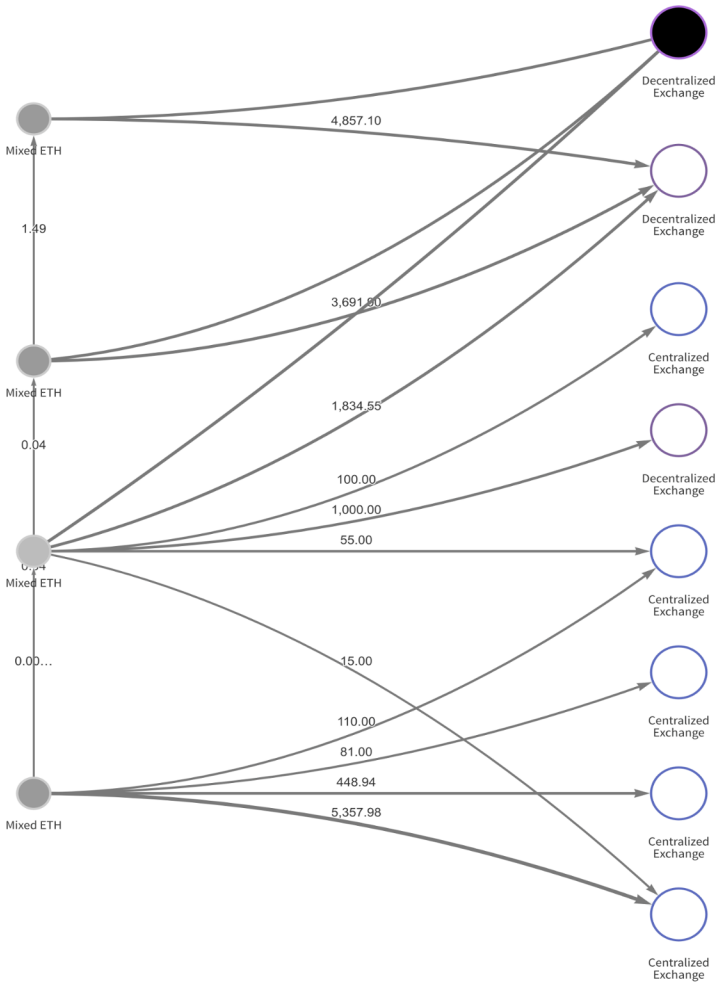
자금세탁 - 1단계

도난 ERC-20 토큰을 DEX 에서 이더리움으로 스왑



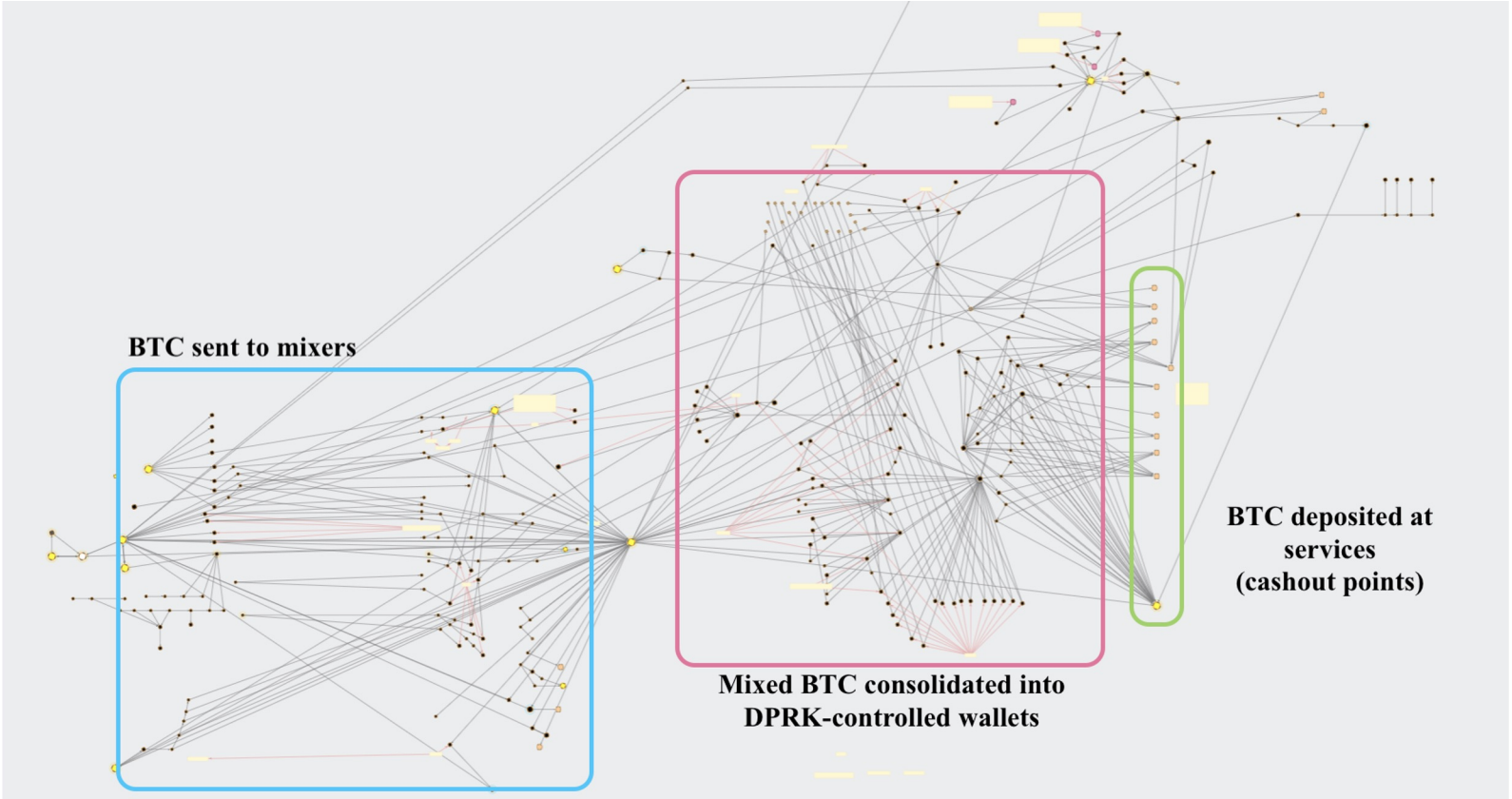
자금세탁 - 2단계

합친 이더리움을 DEX 와 CEX 에 입금해 비트코인으로 스왑



자금세탁 - 3단계

BTC 로 스왑한 도난 자금 이동



DPRK 불법자금 분석 기술
- Axie Infinity / Ronin Bridge Hack

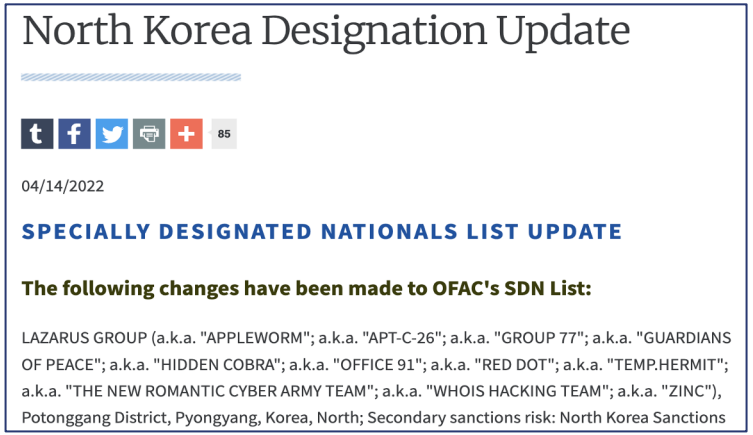
액시 인피니티 해킹

- **사건 개요**
  - 2022년 3월 23일, 액시 인피니티 자체 체인 **로닌 브리지**에서 대규모 해킹 발생
  - 17만 3600개의 이더리움(약 7150억원)과 2550만달러(약309억원) 상당의 USDC 도난
  - 사고 당시 가격으로 6억 2천만달러의 자금 탈취
- **해킹 방법**
  - 로닌 체인은 9개의 검증자(밸리데이터) 노드로 구성
  - 액시 인피니티 게임의 속도를 개선하기 위해 추가한 보조 블록체인 네트워크
  - 코인 입출금을 하기 위해서는 9개의 검증인 중 최소 5명의 검증자 승인이 필요
  - 해커는 스카이 마비스가 운영하는 4개의 로닌 검증자 노드키와 액시 다오(DAO)가 운영하는 검증자 노드키 획득
  - 획득한 5개의 노드키로 자금 도난 및 이동

액시 인피니티 해킹

- **수사 진행**
  - 해킹을 인지한 후, 로닌(Ronin)은 **체이널리시스**에 사건 분석 의뢰 (2022-03-29)
  - 체이널리시스는 미국 수사 기관과 함께 해킹 사건 분석
  - **지금까지의 DPRK 해킹 특징들과 비교했을 때, 이번 사건도 DPRK에 의한 해킹이라고 결론 (관련된 자세한 사항은 추후 공개 예정)**

- **진행 상황 (2022년 4월 18일)**
  - 미국 재무부 산하 해외 자산 통제국 (OFAC)은 2022년 4월 14일, 액시 인피니티 해킹으로 인한 도난 자금이 이동한 이더리움 주소에 대해 Lazarus 그룹에 속한 주소로 정의하고 제재 리스트에 포함시킨다고 발표
  - https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220414



North Korea Designation Update

85

04/14/2022

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following changes have been made to OFAC's SDN List:

LAZARUS GROUP (a.k.a. "APPLEWORM"; a.k.a. "APT-C-26"; a.k.a. "GROUP 77"; a.k.a. "GUARDIANS OF PEACE"; a.k.a. "HIDDEN COBRA"; a.k.a. "OFFICE 91"; a.k.a. "RED DOT"; a.k.a. "TEMP.HERMIT"; a.k.a. "THE NEW ROMANTIC CYBER ARMY TEAM"; a.k.a. "WHOIS HACKING TEAM"; a.k.a. "ZINC"), Potonggang District, Pyongyang, Korea, North; Secondary sanctions risk: North Korea Sanctions

해킹 분석

- SimpleSwap[.]io/Cryptomixer에서 1.06 ETH(가스 수수료) 펀딩
- 1inch에서 2,550만 USDC를 ETH로 교환
- FTX/Huobi를 사용하여 ETH를 BTC로 변환
  - ~87 BTC의 경우 각 입금 주소에 ~1,250 ETH
- Tornado Cash를 사용하여 ETH 혼합
  - 4월 18일 기준 ~31,000 ETH 입금
- Blender[.]io 및 Wasabi를 사용하여 혼합
- ERC20s/ETH를 BTC로 스왑

북한의 해킹 특성

- 스피어피싱 및 RAT 악성코드 사용
- ERC-20 토큰을 ETH로 전환
- 믹서 사용
- 도난자금 대부분 보유
- 거래소에 도난자금 중 소액을 입금해서 현금화를 시도 후, 입금액을 점점 증가시킴

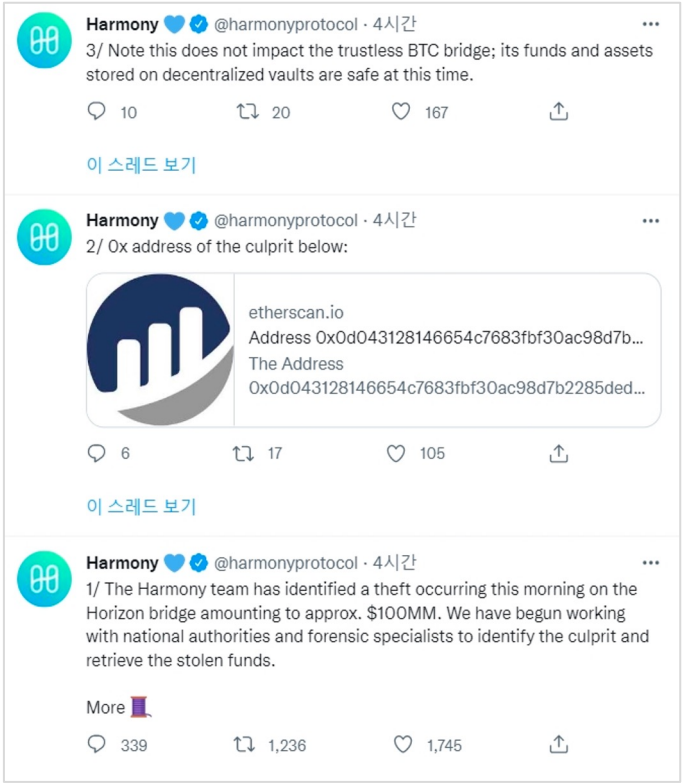
액시 인피니티 해킹과 DPRK의 관련성

- **DPRK와의 관련성**
  - 접근 벡터는 기존 북한 관련 해킹과 동일
  - Ronin 해킹에 사용된 악성코드 = 2021년 8월 9,100만 달러 Liquid 해킹의 동일한 악성코드
  - 2021년 6월 11일부터 27일까지 Sky Mavis의 내부 로그인 페이지를 호스팅하는 IP 주소와 알려진 Lazarus 악성코드의 C2 IP가 연결되어 있음
  - 자금 이동(지금까지)은 이전 북한 해킹과 동일한 패턴

DPRK 불법자금 분석 기술
- Harmony Horizon Bridge Hack

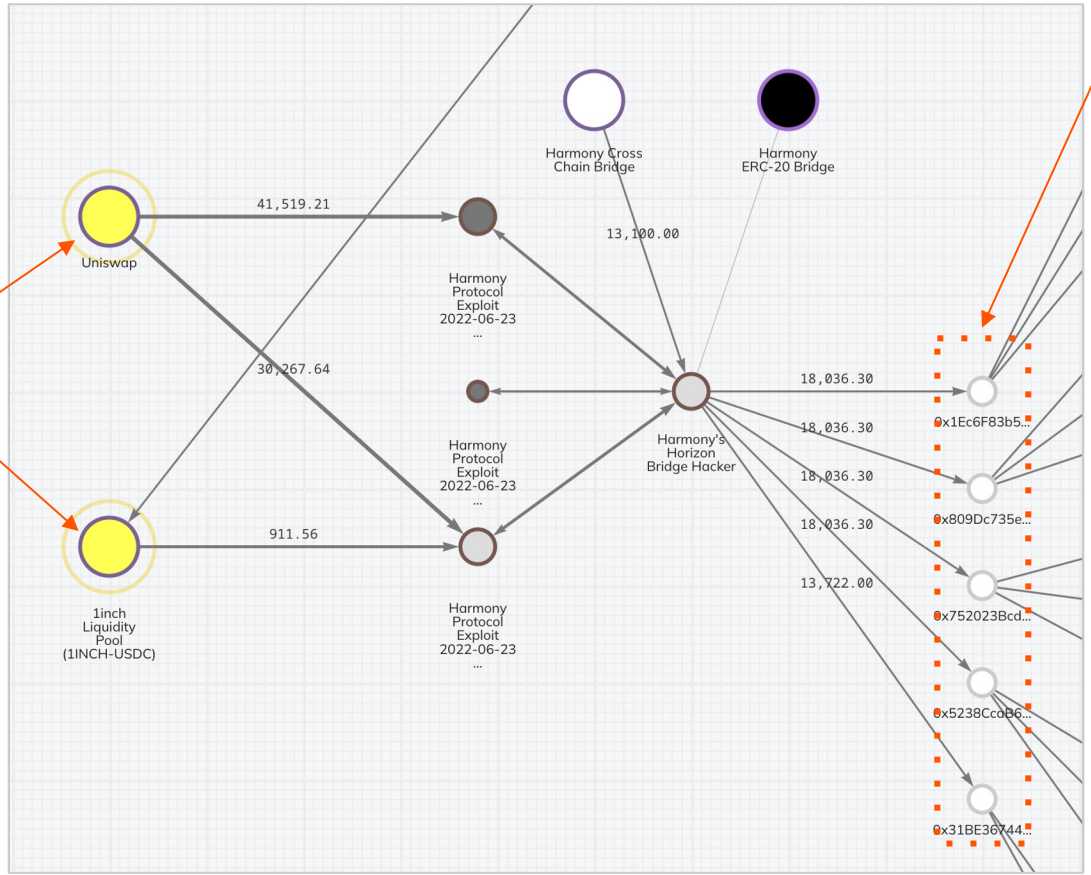
Harmony - Horizon Bridge Hack

- 하모니 블록체인의 크로스체인 브리지 호라이즌에서 약 1억달러 규모의 자금 탈취 (2022년 6월 23일)
- 다중 서명(Multi-Sig) 보안 취약점을 악용한 것으로 판단
- 2/5 유효성 검증에서 2개의 개인키가 도용 (현재는 4명의 승인 필요)
- ETH, USDC, WBTC, USDT, DAI, BUSD, AAG, FXS, SUSHI, AAVE, WETH 및 FRAX 등의 자산 탈취
- 토네이도 캐쉬를 통해서 세탁



Harmony - Horizon Bridge Hack

Uniswap, 1inch 네트워크를 통해 탈취한 ERC-20토큰을 ETH로 변환

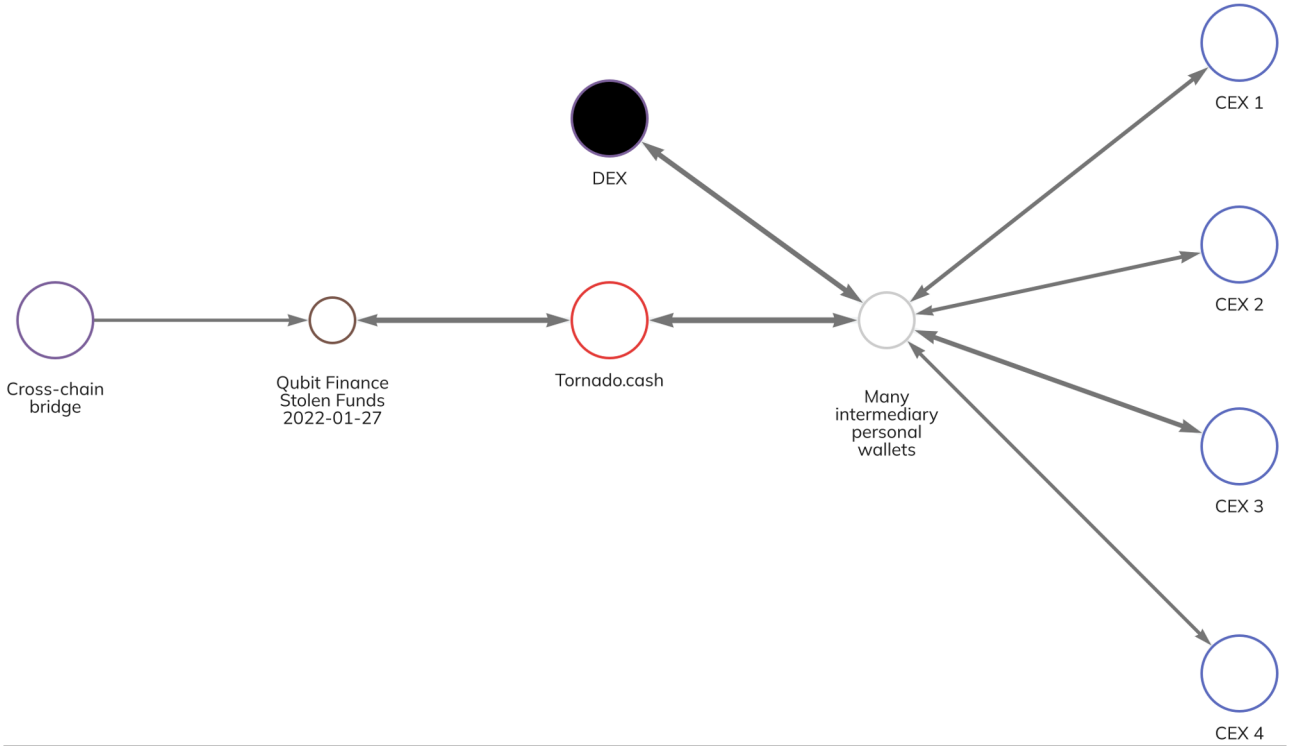


탈취 자금을 여러 개의 중간 지갑을 거쳐 토네이도 캐시로 이동 (믹싱 작업 수행)

큐빗 해킹 사례

- 큐빗(Qubit)은 BNB 체인을 기반으로 구축된 **대한민국의 디파이 대출 프로토콜**
- 큐브리지의 보유 자산 중 약 **8000만 달러(약 1000억 원) 상당의 자금이 유출**돼 2022년 한국 최대의 가상자산 탈취가 이뤄짐
- 큐빗 해커들은 이더리움 블록체인에서 브리징 된 이더리움을 나타내는 자산 'qXETH'를 큐브리지에서 무제한으로 발행
- 해커들은 도난 당시 프로토콜이 보유한 약 8000만 달러 상당의 자산(대부분 BNB 코인과 몇 개의 BEP-20 토큰)을 빌리기 위해 무제한 발행한 qXETH를 담보로 사용한 후 그 자금들을 **이더리움 블록체인에 연결 후 토네이도 캐시 믹서(Tornado Cash)로 전송**
- 이 활동은 **체이널리시스 블록체인 분석 툴인 리액터(Reactor), 스토리라인(Storyline)**을 통해 확인
- 큐빗 해킹은 전형적인 북한 해킹 전략. **디파이 프로토콜에서 자금을 탈취해 자금 동결이 불가능한 블록체인에 연결하고 믹싱한 후 중앙화 거래소로 이동**

큐빗 해킹 사례


DEX
CEX 1
CEX 2
Cross-chain bridge
Qubit Finance Stolen Funds 2022-01-27
Tornado.cash
Many intermediary personal wallets
CEX 3
CEX 4

DPRK Crypto 해킹의 특징

- 최초 도난 이후, 아래 흔적들을 찾을 수 있습니다
  - 사회 공학 기법 사용
  - 체인 호핑(Chain hopping)
  - 시험 입금 후 입금 금액 증가
  - 필 체인(Peel chains)
  - 믹싱 또는 코인조인 서비스 이용
  - 통합(consolidation) 또는 중개(intermediary) 지갑 사용

- 그 후, 도난 자금은 아래와 같이 이동합니다.
  - 믹싱 서비스로 전송
  - 믹싱 서비스, 거래소를 거쳐 현금화 시도
  - 믹싱 서비스를 거쳐 개인 지갑으로 이동 후 유휴 상태로 변경
  - 장외 거래(OTC)를 통해 청산

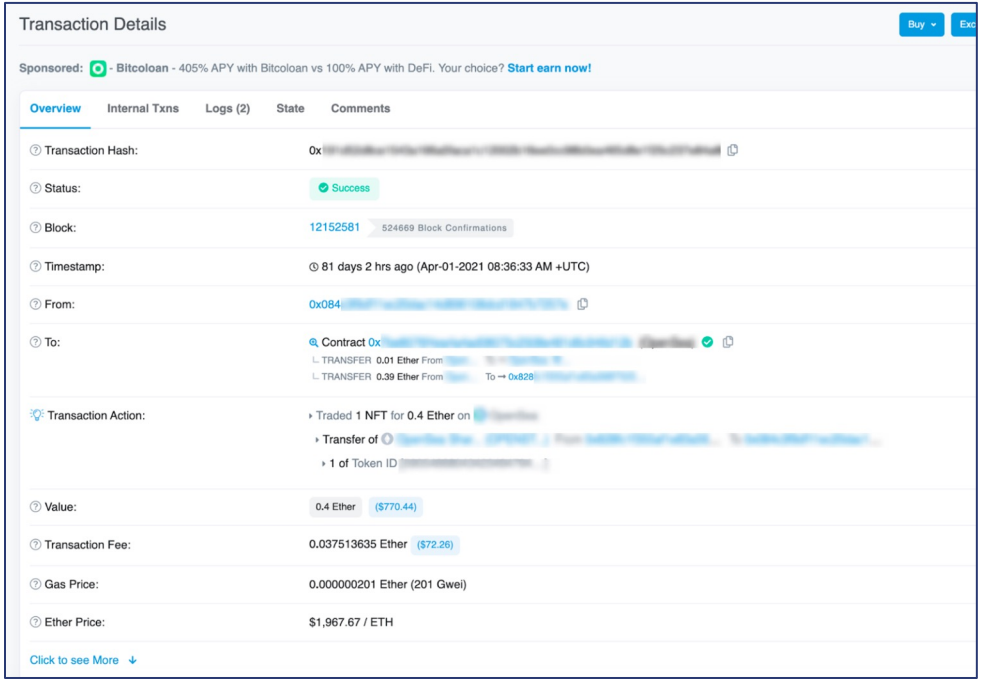
Chainalysis

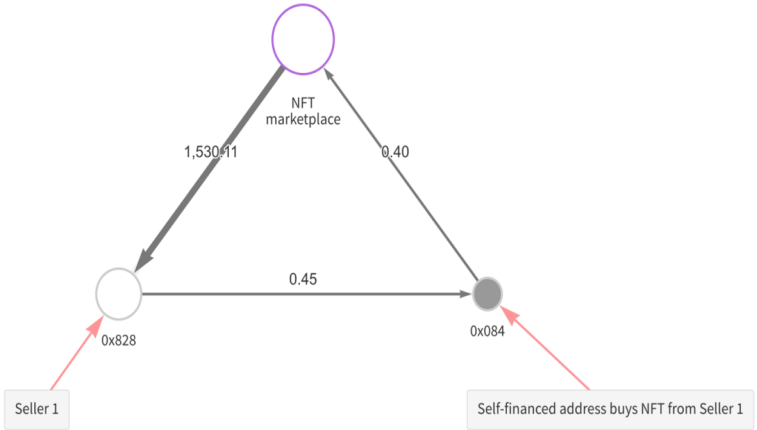
사례 연구 : NFT와 범죄

NFT와 범죄

NFT 자전 거래 (Wash Trading) 추적

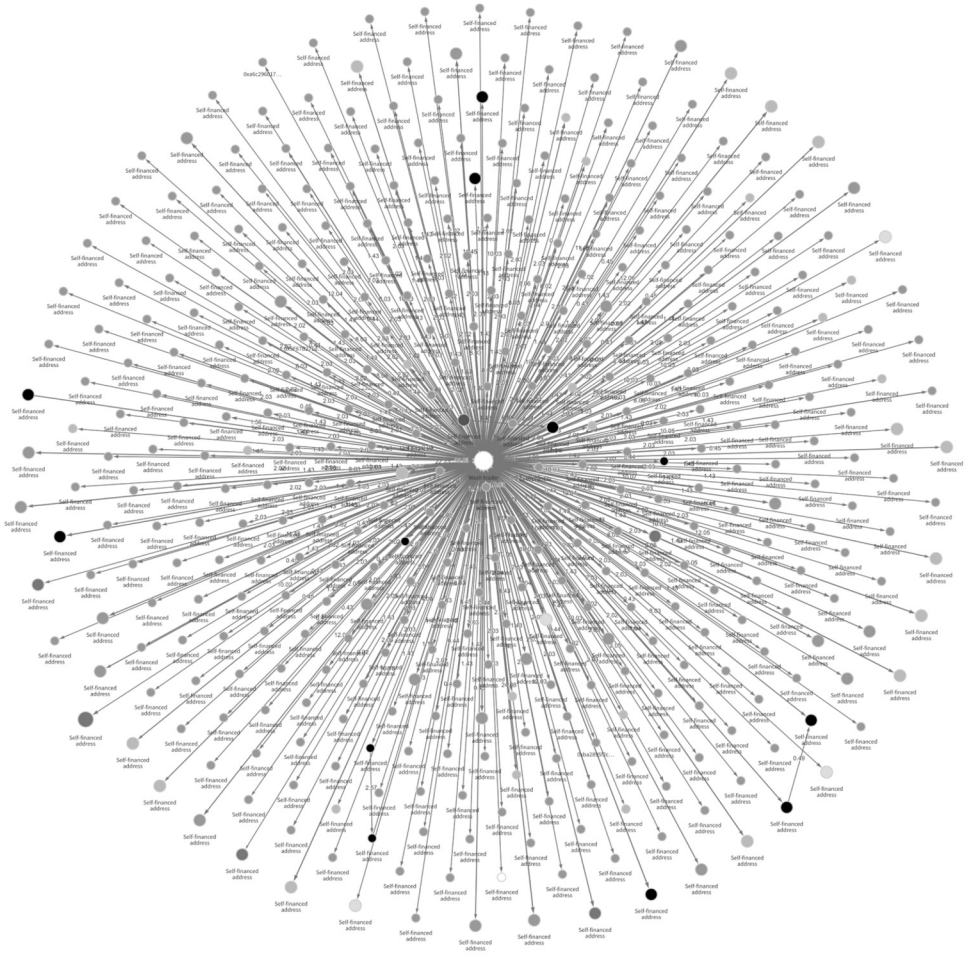
- Reactor 그래프는 판매 직전에 주소 0x828이 해당 주소 0x084로 0.45 이더리움을 보냈음을 보여줍니다





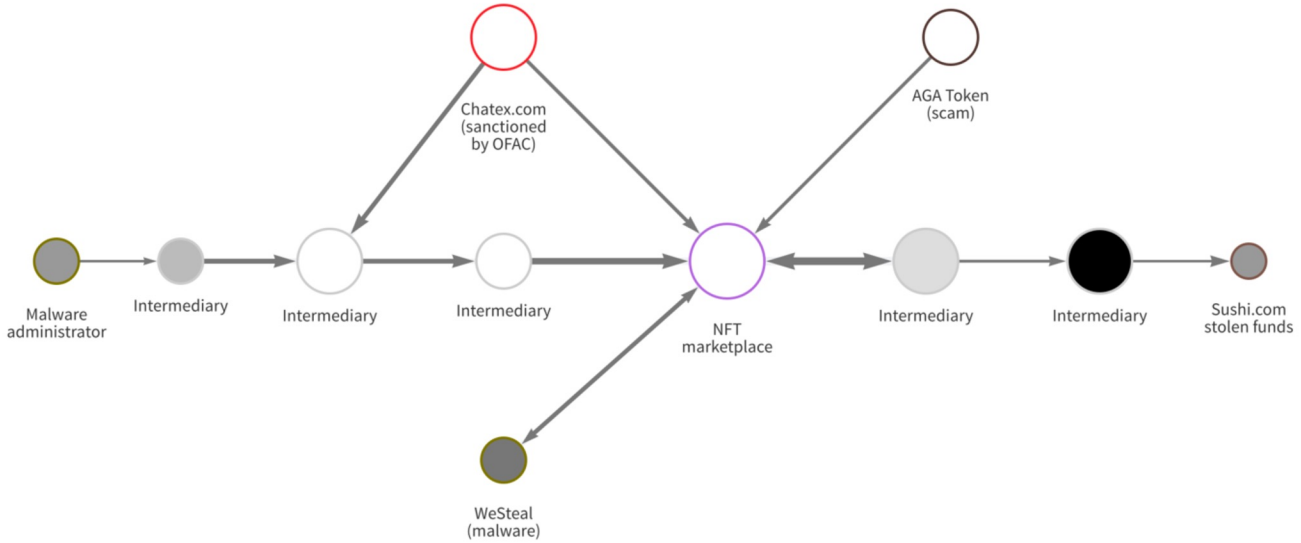
NFT와 범죄

NFT 자전 거래 (Wash Trading) 추적



NFT와 범죄

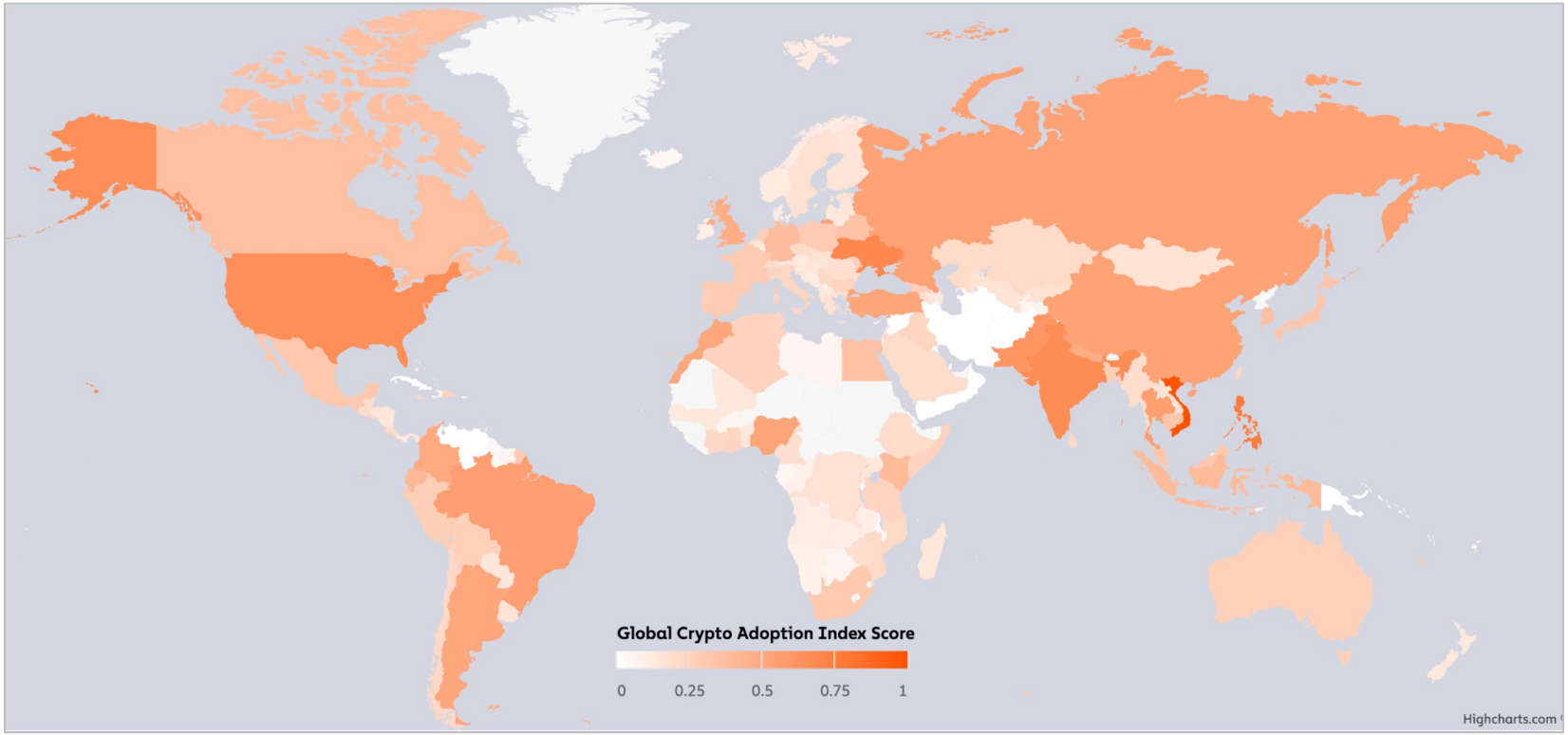
자금 세탁을 위한 NFT 거래 추적



Chainalysis

2022 글로벌 가상자산 지수

2022 글로벌 가상자산 지수



https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

2022 글로벌 가상자산 지수

Country	Overall index ranking	Overall index score	Centralized service value received ranking	Retail centralized service value received ranking	P2P exchange trade volume ranking	DeFi value received ranking	Retail DeFi value received ranking
Vietnam	1	1.000	5	5	2	7	6
Philippines	2	0.753	4	4	66	13	5
Ukraine	3	0.694	6	6	39	10	14
India	4	0.663	1	1	82	1	1
United States	5	0.653	3	3	111	3	2
Pakistan	6	0.609	10	10	50	22	16
Brazil	7	0.562	7	7	113	8	7
Thailand	8	0.560	12	12	61	5	3
Russia	9	0.541	8	8	109	11	12
China	10	0.535	2	2	144	6	4

Chainalysis

감사합니다

체이널리시스 코리아
송용일 차장
yong.il.song@chainalysis.com