Quantum Guard 퀀텀가드

Chainalysis

특별 세션 : 가상자산 인사이트

인공지능 기반의 블록체인 인텔리전스와 사이버 보안의 미래

부제: 미군의 실례로 본 블록체인 인텔리전스

블록체인 인텔리전스

군사 안보의 새로운 지평

(사)국방정보통신협회 국방AI융합세미나

Chainalysis

세미나 세션 : 특별세션

인공지능 기반의 블록체인 인텔리전스와 사이버보안의 미래

한국군의 블록체인 인텔리전스 역량은 선택이 아닌 국가 안보의 필수 요소

“전쟁에는 세 가지가 필요합니다. 돈과 돈, 그리고 또 돈입니다.”

(..Pour faire la guerre, il faut trois choses: de l’argent, de l’argent et encore de l’argent.)

— 잔 자코모 트리불치오(Gian Giacomo Trivulzio, 1448–1518)가 프랑스 루이 12세에게 한 답변

Chainalysis

목 차

서론: 디지털 전장에서의 새로운 정보 우위

블록체인 인텔리전스의 등장 배경

더 이상 단순한 금융 기술 분석의 영역에 머물러 있지 않고, 군사 커뮤니티가 적성국의 비대칭적 위협에 대응하기 위한 핵심 국가 안보 정보 자산으로 자리매김

지정학적 분쟁과 사이버 위협의 확대

암호화폐의 등장은 지정학적 분쟁과 안보 위협의 새로운 전장(戰場)을 형성하고, 국가 급 행위자들이 달러 중심 국제 금융 시스템 우회와 불법 자금 조달에 활용

FBI 사이버범죄 피해 통계

2023년 기준

총 사이버 범죄 피해액

$ 125억 달러 초과

투자 사기 피해액

$ 45억 7천만 달러

기업 이메일 침해(BEC) 피해

$ 29억 달러

실증적 가치 입증 필요성

본 보고서는 블록체인 인텔리전스가 어떻게 위협의 실체를 파악하고, 적성국의 제재 회피 네트워크를 추적하고 와해시키는 데 기여하는지 실제 사례를 통해 입증

국가안보 위협 요소

암호화폐를 통한 제재 회피, 자금세탁, 랜섬웨어 공격이 핵심 국가안보 위협으로 부상

블록체인 인텔리전스는 이제 군사 안보의 필수 정보 역량으로 자리매김

핵심 용어 정의: 군사 · 국가 안보적 관점

블록체인 인텔리전스
(Blockchain Intelligence)

공개된 블록체인상의 거래 데이터(On-chain data)를 분석하여 익명의 지갑 주소와 자금 흐름을 추적하고, 이를 통해 적성국의 불법 활동, 위협 금융 네트워크, 제재 회피 시도를 식별 및 무력화하는 정보 활동.

위협 금융
(Threat Finance)

테러 조직, 범죄 단체, 제재 대상 국가 등 국가 안보에 위협이 되는 행위자들이 무기 개발, 작전 수행, 영향력 확대 등의 목적으로 자금을 조달, 이동, 저장, 사용하는 모든 금융 활동과 관련 네트워크를 지칭.

가상자산서비스제공자
(VASP: Virtual Asset Service Provider)

암호화폐 거래소, 지갑 제공업체, 커스터디 서비스 등 가상자산 관련 서비스를 제공하는 업체. 자금세탁방지 규정(AML)에 따라 고객 신원확인(KYC)과 의심거래 보고 의무가 있으나, 규제 관할권에 따라 다른 준수 수준을 보임.

믹서
(Mixer)

다수의 사용자로부터 암호화폐를 수집하여 혼합한 뒤 출처를 알 수 없게 만들어 다른 지갑으로 송금하는 서비스. 거래 추적 방해와 자금 출처 은폐에 활용되며, 미 재무부는 Tornado Cash 등 주요 믹서를 제재 대상으로 지정.

기업 이메일 침해
(BEC: Business Email Compromise)

공격자가 CEO, CFO 등 기업 고위 임원이나 신뢰할 수 있는 거래처로 위장해 이메일을 보내 자금 이체를 유도하는 사회공학적 공격 수법. FBI 집계 기준 2023년 29억 달러의 피해가 발생했으며, 탈취한 자금은 주로 암호화폐로 전환되어 추적을 회피함.

이러한 용어와 개념의 이해는 현대 군사 및 국가안보 영역에서 블록체인 인텔리전스 역량 구축의 기본이 됩니다.

전략적 당위성: 암호화폐의 위협 요인

암호화폐와 국제 제재 우회

기존 국제금융체계 우회

암호화폐가 SWIFT 등 전통적 금융감시망을 우회하며 제재 무력화의 핵심 수단으로 부상

자금세탁 기법 고도화

믹서 서비스: 거래 추적 불가능화 체인호핑: 여러 블록체인 간 이동 P2P 거래: KYC 절차 우회

세계 경제 안보 위협

불법 자금 조달 흐름을 세계 경제 안보에 대한 실존적 위협으로 인식하는 미국 안보 커뮤니티의 패러다임 전환

적성국 활용 사례

북한

라자루스 그룹 - 사이버 금융 해킹으로 연 10억 달러 획득

2023년 WMD 개발 자금으로 암호화폐 해킹액 즉각 전환

사이버 기술과 핵무기 간 자금 순환고리 형성

이란

2022년 공식 암호화폐 수입 주문 승인

CSIS 확인 - 1,000만 달러 규모 국가 주도 거래

석유 등 제재 품목의 결제 수단으로 활용

* 국제전략문제연구소(CSIS)

FBI·CSIS 통계 데이터 (2023)

FBI 인터넷범죄신고센터(IC3) 집계

$ 투자 사기 피해액45억 7천만 달러

사이버 범죄 유형별 비중

랜섬웨어 공격	32%
기업 이메일 침해(BEC)	24%
암호화폐 직접 탈취	21%

위협 금융의 장기 영향

대규모 자금이 적대적 국가 행위자에게 유입되며 안보 불균형 심화 및 비대칭 위협 증가

블록체인 인텔리전스는 위협 금융 추적·차단의 핵심 수단

사이버 기반 위협 금융 네트워크 I

사이버 위협 금융의 구조

전략적 중요성: 범죄수익 추적을 넘어 적의 금융 인프라 자체를 타격할 수 있는 역량

1. **자금 탈취 및 생성**
   랜섬웨어, 기업 이메일 침해(BEC), 투자 사기를 통한 자금 탈취와 생성
2. **자금 세탁**
   암호화폐 플랫폼으로 자금 이동 후 믹서, 익명화 서비스 활용, 추적 방해
3. **통합 및 활용**
   세탁된 자금을 합법적 경로를 통해 통합, 불법 활동 자금화 및 자산 구매

블록체인 인텔리전스의 활용

- 온체인 추적을 통한 자금 흐름 파악
- 위협 행위자 식별 및 네트워크 분석
- 자산 동결 및 회수 작전 지원

주목할 위협 요소

사이버 공격과 암호화폐 결합의 시너지 효과

국가 지원 해킹 그룹의 금융 인프라 침투

비대칭 위협에 블록체인 추적 역량 필수

대표적 해킹 사례

FBI 보고서 기준

기업 이메일 침해 (BEC)

코네티컷주 사기 사례

$ 피해액: 670만 달러

위장된 송금 지시로 자금이 해외 암호화폐 계좌로 이체

랜섬웨어 공격

주요 인프라 표적 사례

$ 평균 요구액: 570만 달러

2023년 대비 114% 증가, 암호화폐로 지불 요구

투자 사기

가짜 암호화폐 투자 플랫폼

$ 총 피해액: 45억 달러 초과

2023년 사이버 범죄 피해 중 최대 규모

사이버 위협 금융 생태계 이해는 효과적인 대응 역량의 기반

사이버 기반 위협 금융 네트워크 II: 생태계 3단계와 대응 전략

위협 금융 생태계 3단계 구조

1 자금 탈취 및 생성

적대적 행위자가 사이버 범죄를 통해 자금을 획득하는 단계

- 랜섬웨어 공격
- 기업 이메일 침해(BEC)
- 해킹/데이터 유출
- 투자 사기

↓

2 자금 세탁

탈취한 자금의 출처를 은닉하고 추적을 방해하는 단계

- 암호화폐 믹서 이용
- 체인 호핑(Chain Hopping)
- P2P 거래 활용
- 중간자 계정 활용

↓

3 통합 및 활용

세탁된 자금을 합법적 금융 시스템으로 통합하고 실제 목적에 활용

- 법정화폐 교환
- 실물자산 구매
- 합법적 사업 투자
- 위협활동 자금화

블록체인 인텔리전스 단계별 대응 전략

1 온체인 추적(On-Chain Tracking)

블록체인에 기록된 거래 데이터를 실시간으로 분석하여 의심 지갑을 식별

실증 사례

- Harmony, CoinEx 해킹 공격자의 지갑 주소 72시간 내 식별

2 위협 행위자 식별(Threat Actor Identification)

거래 패턴 분석, 행동 프로필링, 믹서 서비스 이용 추적으로 행위자 특정

실증 사례

- 라자루스 그룹의 특징적 거래 패턴 식별 및 Kimsuky 연계 활동 확인

3 자산 동결 및 회수(Asset Freezing & Recovery)

국제 협력과 거래소 공조로 불법 자금 동결 및 환수 조치 실행

실증 사례

- OFAC의 Tornado Cash 제재로 북한 자금세탁 경로 차단

대응 전략 효율성 분석

- 순환적 분석 체계: 각 단계의 정보가 다른 단계의 효과를 강화하는 선순환 구조
- 실시간 대응: 블록체인 데이터의 불변성과 투명성을 활용한 신속한 위협 식별

선제적 대응과 자산 회수율은 블록체인 인텔리전스의 핵심 성과 지표

국제 제재 회피 및 불법 거래 네트워크

이란의 암호화폐 공식 수입 사례

CSIS(전략국제문제연구소) 보고에 따르면, 이란 정부는 공식적으로 1,000만 달러 규모의 암호화폐를 활용한 수입 주문을 승인하며 국제 제재를 우회하는 새로운 선례를 제시

제재 회피 주요 메커니즘

비수탁형 지갑(Non-custodial Wallet)을 통해 거래소 없이 직접 자산 보유, P2P 거래로 중앙 기관 우회, 온체인 흔적 최소화 기법 활용

제재 회피 거래의 특성

복잡한 다중 지갑 구조, 중간 거래소를 통한 자금 세탁, 여러 블록체인 간 자금 이동(체인호핑), 믹서 서비스 활용 등 다단계 거래 패턴으로 익명성 확보

제재 회피 거래 탐지 지표

의심 거래 패턴

- 비정상적 다중 전송 구조

위험 국가 연결성

- 제재 대상국 IP 접속 패턴

알려진 위험 지갑

- 제재 대상 지갑과의 연결성

블록체인 인텔리전스 대응 전략

네트워크 분석 | 패턴 식별 | 표적 지정 | 제재 적용

블록체인 인텔리전스는 지갑 간 반복 거래 패턴, 자금 세탁 믹서, 거래소 입출금 기록 등을 종합 분석하여 숨겨진 연결고리 파악

블록체인 인텔리전스를 통해 제재 회피 네트워크의 효과적 탐지와 대응 가능

미군 실증 유즈케이스 I: 제재 집행과 믹서 차단

미국 재무부(OFAC)의 믹서 제재 사례

OFAC은 북한 라자루스 그룹이 사용한 Tornado Cash 등 익명화 도구를 공식 제재 대상으로 지정하고, 모든 미국인의 해당 서비스 이용을 금지

사례: Tornado Cash 제재 (2022)

- 제재 이유: 북한의 7억 달러 이상 해킹 자금 세탁 연관성
- 대상: 특정 이더리움 스마트 계약 주소 및 관련 지갑 계정들
- 영향: 관련 USDC 자산 동결, 앱 개발자 체포, 전체 이더리움 생태계에 영향

전례 없는 블록체인 기반 제재

분산화된 스마트 계약에 대한 세계 최초의 공식 제재로서, 암호화폐 업계와 국가안보 영역 사이 새로운 법적 선례 확립

FBI-민간 분석 기업 협업 구조

- 온체인 데이터 실시간 모니터링
- 자금 흐름 패턴 분석
- 실제신원 매핑 작업
- 법적 조치 및 자산 동결

추적 성공률 증가

2020년	47%
2023년	76%

민관군의 블록체인 분석 협력이 국가안보 위협에 대한 실질적 대응 수단으로 입증

미군 실증 유즈케이스 II: 북한 해킹 그룹 추적

라자루스 그룹 (Lazarus Group)

주요 공격 대상: 암호화폐 거래소, DeFi 프로토콜

공격 방식: 소셜 엔지니어링, 악성코드 침투

⚠ 2023년 주요 해킹: CoinEx, Poloniex, Atomic Wallet

FBI 공개 정보 : 라자루스 그룹은 북한 정찰총국(RGB) 소속으로 확인됨

김수키 (Kimsuky)

주요 공격 대상: 방산업체, 학술기관, 금융기관

공격 방식: 스피어피싱, 자격증명 탈취

⚠ 정보 수집 → 암호화폐 탈취 → 자금 세탁 패턴

주요 피해 규모

Harmony 브릿지 해킹 (2022)	1억 달러+
Ronin 브릿지 해킹 (2022)	6억 2천만 달러+
2023년 총 피해액	17억 달러+
피해자 수 (2023년)	700명+

블록체인 인텔리전스 분석 기업 역할 (탐지율/오탐률)

Chainalysis 글로벌 No.1 | 사법증거 | 법집행민간기관

공격자 지갑 식별 및 클러스터링 분석을 통해 북한 해킹 그룹과 연계된 2,000여 개 지갑 식별 **(탐지율 : 95%이상, 오탐률 5%미만)**

* 증거채택의 기준

Elliptic

혼합 패턴 분석을 통해 북한 해킹 그룹의 Tornado Cash 등 믹서 서비스 사용 패턴 발견 **(탐지율 : 50% 미만, 오탐률 50% 이상)**

TRM Labs

북한 라자루스와 연계된 체인호핑 활동 추적 및 포렌식 증거 제공 **(탐지율 : 50% 미만, 오탐률 50% 이상)**

블록체인 인텔리전스 작전 성과

- **FBI 자산 회수 성공 사례**
  - ✓ Axie Infinity 해킹: 3,000만 달러 회수 (2022)
  - ✓ Harmony 브릿지: 6천만 달러 동결 (2023)
- **블록체인 증거의 법적 활용**

  블록체인 분석 결과가 **법정 증거**로 인정되어 2022년부터 미군과 법 집행기관의 형사소송에 활용 ➡ 체이널리시스 Chainalysis

블록체인 인텔리전스를 통해 북한 해킹 조직의 금융 흐름 차단 및 자금 회수 실현

대한민국 국군 전략적 시사점

북한 사이버 금융범죄와 WMD 개발

북한의 사이버 금융범죄는 핵/미사일 개발의 핵심 생명선으로, 국제 제재 속에서도 지속적인 무기 개발 자금을 조달하는 주요 수단으로 작용

한반도 실존적 위협 요소

블록체인을 통한 제재 회피는 북한의 WMD 개발 가속화로 직결되며, 이는 한국 안보에 실존적 위협으로 작용. 기존의 군사적 위협에 사이버·금융 위협이 결합된 복합 안보위협 환경 조성

안보 환경의 패러다임 변화

금융·사이버 영역에서의 우위가 전통적 군사 영역의 안보에 직접적 영향을 미치는 안보-금융-사이버의 연결성 강화

주요 표적 노출 현황

금융기관

은행·증권사·보험사 시스템 공격으로 금융 인프라 무력화 및 자금 탈취 시도 급증

방산업체

핵심 방위산업 기술 유출과 공급망 교란 목표, 북한 해킹그룹의 지속적 표적화

국가 주요 인프라

에너지·통신·교통·의료 등 핵심 인프라 운영 시스템 침투 시도 확인

가상자산 거래소

국내 주요 거래소 대상 지속적 공격, 라자루스 그룹의 주요 표적

북한 사이버 공격 증가율

전년 대비 **58%** 증가

한국군의 블록체인 인텔리전스 역량은 이제 선택이 아닌 국가 안보의 필수 요소

국군 대응 강화 방안: 전략적 역량 구축

북한의 블록체인 기반 불법 자금조달 및 제재회피 활동에 대응하기 위한 국군의 전략적 역량 강화가 필수적입니다. 다음 3가지 핵심 대응 방안을 제안합니다.

① 전문조직 · 인력 양성

- 사이버사령부 내 블록체인 인텔리전스 전담 부서 신설
- 암호화폐 추적 및 분석 전문 인력 양성 교육 프로그램 구축
- 정보부대 내 블록체인 데이터 분석팀 운영

2025년까지 100명 이상 전문인력 확보 목표

② 한미 정보공조 강화

- FBI, 미 재무부 OFAC와의 실시간 정보 공유 채널 구축
- 한미 합동 사이버 위협 인텔리전스 플랫폼 구축
- 북한 해킹 그룹(라자루스, 킴수키) 공동 추적 태스크포스 운영

분기별 합동 대응 훈련 및 역량 강화 연습

③ 민군협력 파트너십

- Chainalysis 등 글로벌 블록체인 분석 기업과 정보 협력
- 국내 주요 금융기관·가상자산거래소와 위협 정보 공유
- 블록체인 인텔리전스 민관 공동 연구 프로젝트 추진

주요 기반시설·방산기업 보호 협력체계 구축

통합적 대응체계 구축을 통한 북한의 가상자산 기반 불법활동 효과적 차단 및 국가 안보 강화

결론: 미래 안보를 위한 핵심 역량

블록체인 인텔리전스의 전략적 가치

블록체인 기술이 제공하는 익명성과 탈중앙성이 국가안보의 양날의 검으로 작용

적성국의 국제 제재 회피 수단

수십억 달러 규모 불법 자금 조달의 통로

북한의 WMD 개발 자금원으로 활용

전략적 대응 역량의 필요성

블록체인 인텔리전스는 이제 단순한 옵션이 아닌 현대 군사·안보 환경에서 필수적인 정보 역량으로 자리매김

실증적 성과 재확인

미 재무부와 FBI의 사례에서 입증된 위협 행위자 추적 및 자산 동결 성과

대한민국 국군 대응 전략 제언

전문 인력 양성 및 전담 조직 신설

사이버사령부 내 블록체인 인텔리전스 전담 부서 구축

한미 정보공조 강화

FBI, 미 재무부와의 실시간 정보 공유 채널 구축

민간 전문기업과 파트너십

Chainalysis 등 블록체인 분석 기업과 민군협력 강화

미래 안보 정책 방향

북한의 고도화되는 사이버 금융 위협에 대응하기 위해 블록체인 인텔리전스를 국가 안보 정책의 핵심 축으로 발전시켜야 함

한반도 특수 안보 환경에서 대한민국 국군의 선제적 역량 확보가 국가안보의 핵심 과제

> 블록체인 인텔리전스는 이제 미래 군사 안보의 필수 정보 역량이자 전략적 우위의 핵심 요소

BOSTECH

For Defense &
Public Applications

Chainalysis

「세계최고의 블록체인 데이터 및 분석 기관」-
미국 및 한국 정부 기관과 자금세탁
방지(AML)를 구현/집행하고 있으며,
디지털 자산과 관련된 테러 자금 조달(CFT)
수사 및 기타 공공 정책 목표에 대응하고
있습니다.

Chainalysis 공식 파트너 ㈜보스테크

㈜보스테크 | 서울특별시 영등포구 당산로 41길 11 SK V1 센터 W동 1511~1512호
TEL 02-3667-5803
FAX 02-3667-5804
E-MAIL koreasns@gmail.com
Mobile 010-3337-7373 (담당자 김정현 총괄/본부장)

블록체인DS사업부