

북한의 가상자산 탈취 대응을 위한 국제안보 협력 방안 International Security Cooperation to Counter North Korea's Cryptocurrency Theft

윤지원 (고려대학교 정보보호대학원/사이버국방학과 교수)

<초록>

가상자산이 금융자산으로 인식되고 있는 상황에서 북한이 주도하는 가상자산 탈취 활동과 그로 인한 국제 안보 위협이 발생하고 있다. 최근 가상자산은 금융자산으로 자리 잡으며 투자 다양성을 제공하는 동시에, 그 익명성과 탈중앙화 특성으로 인해 범죄자들에게도 매력적인 수단이 되고 있다. 특히 북한은 정권 차원에서 조직화된 해커 그룹을 운영하며, 전 세계 가상자산 거래소를 대상으로 사이버 공격을 감행하고 있다. 대표적인 사례로는 2024년 일본의 DMM 비트코인 거래소 해킹 사건과 2025년 UAE 바이빗 해킹 사건이 있으며, 이들은 수억 달러 규모의 암호화폐 탈취로 이어졌다. 이러한 불법 행위는 북한의 핵·미사일 등 대량살상무기(WMD) 개발 자금으로 활용되며, 국제 제재를 회피하는 주요 수단이 되고 있다. 이에 따라 한국, 미국, 일본 등 주요국은 북한의 해킹 조직과 믹싱(mixing) 서비스에 대한 제재를 강화하고 블록체인 분석 및 민간 보안 기업들과의 협력을 통해 불법 자금 흐름을 차단하는 등 글로벌 차원에서의 공동 전략 수립이 시급하다.

<Abstract>

In a global environment where virtual assets are increasingly recognized as financial assets, this study analyzes the North Korean-led theft of virtual assets and its implications for international security. While virtual assets became established financial instruments offering diverse investment opportunities, their anonymity and decentralized nature also make them attractive tools for criminals. In particular, North Korea operates state-sponsored hacker groups that conduct cyberattacks targeting cryptocurrency exchanges worldwide. Notable cases include the 2024 hacking of Japan's DMM Bitcoin exchange and the 2025 breach of Bybit, both resulting in the theft of hundreds of millions of dollars worth of cryptocurrency. These illicit activities are used to finance North Korea's weapons of mass destruction (WMD) programs, including nuclear and missile development, and serve as a key method for circumventing international sanctions. In response, countries such as South Korea, the United States, and Japan have strengthened sanctions against North Korean hacking groups and mixing services. They are also collaborating with blockchain analytics and private security firms to trace and block illicit fund flows. North Korea's virtual asset-based cyberattacks must be viewed not merely as financial crimes but as state-sponsored strategic threats to global security, necessitating a coordinated international response.

본 글에 게재된 내용은 저자의 개인적 견해에 바탕을 둔 것으로, 경제기술안보연구원의 공식적 견해가 아님을 밝힙니다.

□ 양날의 칼 가상자산

2025년 5월 18일 비트코인 1개의 가격이 1억 4천만 원을 넘어섰다. 매일 전 세계적으로 수백에서 수천 가지의 새로운 암호화폐들이 생겨나고 있고, 각종 민간 주도의 거래소들은 새로운 코인들을 발굴하여 상장하고 있다. 또한 주식과 채권 매매처럼 암호화폐 매매도 일반인들이 손쉽게 진행할 수 있는 환경으로 바뀌고 있다. 이러한 상황에서 2024년 7월 19일에는 ‘가상자산 이용자 보호 등에 관련 법률’이 시행되면서, 암호화폐 등의 가상자산을 매매하는 이용자들을 보호하기 위한 법적 제도적 장치도 마련되어 가상자산이 하나의 금융자산으로 자리 잡혀가고 있다.

기존의 다른 금융자산들과 달리 암호화폐가 짧은 시간 안에 활성화가 된 이유는 암호화폐들이 갖고 있는 상징적이고 기술적인 특징에 기인한다. 예를 들어, 암호화폐 중 가장 대표적인 비트코인은 기존의 중앙화된 신뢰 시스템에서 벗어나 탈중앙화된 가치 저장 수단으로 전 세계에 이목을 집중시키고 있다. 또한 블록체인을 채택하여 만들어짐으로써 정보독점과 이중지불(Double Spending) 문제를 해결하였고, 무엇보다도 누구나 화폐의 발행에 참여할 수 있는 가능성을 제시함으로써 기존 금융 시스템의 한계를 뛰어넘게 되었다.

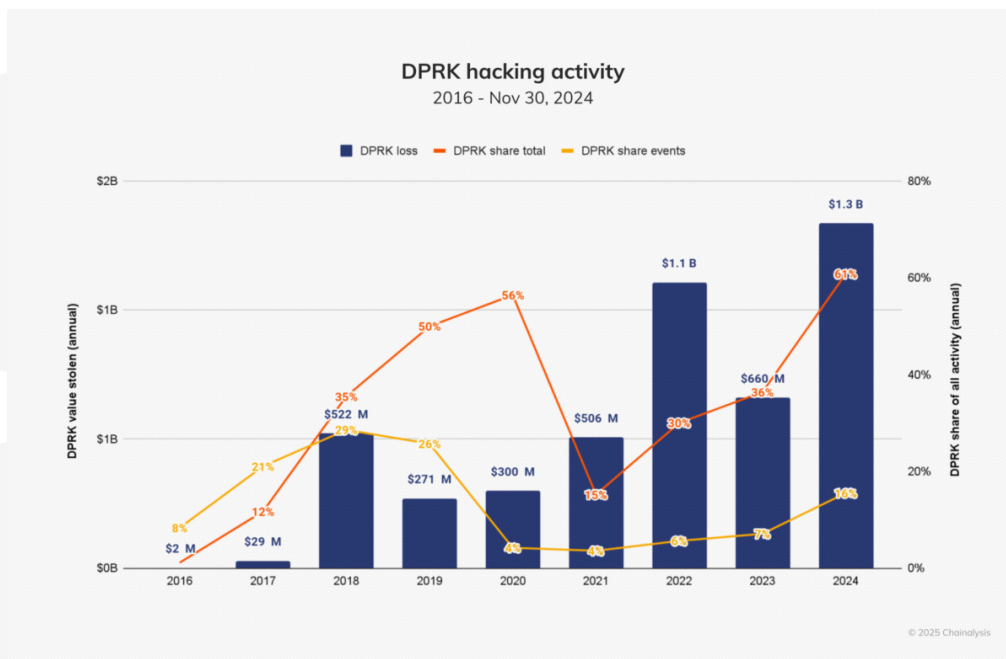
이로써 비트코인을 포함하는 다양한 암호화폐(가상자산)들이 주식 거래나 채권 거래만큼 활성화되었고, 일반인들에게 투자의 다양성 제공이라는 밝은 면을 제공하고 있다. 하지만, 양날의 칼처럼 탈중앙화 및 투자의 다양성 제공이라는 장점이 일반적인 투자자들뿐만 아니라, 범죄자들에게도 충분히 매력적이기에 여러 가지 사회문제를 발생시키고 있다. 예를 들어, 암호화폐의 지갑 주소는 익명성을 기반하고 있으며 또한 프라이버시를 보호한다는 이유로 모네로(Monero) 같은 추적이 불가능한 암호화폐까지로도 확장되고 있다. 또한, 암호화폐 거래패턴을 감추기 위한 믹서(Mixer) 등의 기술들이 개발되는 등 신분을 숨기면서 자금을 거래하고자 하는 범죄자들의 암호화폐 이용이 나날이 증가하고 있다.

더욱 큰 문제로 커지고 있는 사항은 단순 소규모 범죄자들에 의한 것이 아닌, 국가 차원에서의 암호화폐 관련 범죄가 일어나고 있다는 점이다. 비트코인 1개의 가격이 1억 4천만 원이 넘어가는 상황에서 북한 등 국가의 지원으로 다양한 해킹그룹이 가상자산 거래소들을 해킹하여 이용자들의 자산을 탈취하는 사건 사고가 매년 발생하고 있기에

국내뿐 아니라, 전 세계적인 이슈가 되고 있다. 그러므로 특히 국가 주도의 전략적 범죄로서 북한의 지원 하에 이뤄지고 있는 해킹 및 랜섬웨어 등의 사이버공격에 의한 가상자산 탈취는 국제안보 관점에서 살펴볼 필요가 있다.

□ 북한의 사이버 위협: 국가주도의 전략적 범죄

북한은 정권 차원에서 사이버 작전을 수행하는 정예 해커 조직을 운영하며, 이들은 전 세계 가상자산 거래소와 금융 플랫폼을 대상으로 공격을 감행하고 있다. 암호화폐 범죄 추적 및 자금 흐름 분석 전문업체인 체인어널리시스(Chainalysis)에 따르면 [그림1]에서 보듯이 2016년부터 해킹 관련으로 피해액이 보고되기 시작하여 2024년엔 10억~20억 달러에 이르는 자금이 북한 지원 해킹그룹에 의해 탈취당하고 있다.



[그림 1] 북한의 가상자산 해킹관련 연도별 피해액 (출처: Chainalysis)

2017년도부터 급격히 가상자산 탈취 사례와 금액이 증가하는 상황에서 북한 관련 가상자산 탈취 사건들이 다양하게 발생하였다. 예를 들어, Five Eyes에 의해 처음 보고된 후 대한민국 국가정보원에서는 2017년에 북한이 수십억 원 상당의 가상자산을 탈취했다고 발표했다. 또한, 체인어널리시스에 따르면 북한이 2022년에는 약 17억 달러의 암호화폐를 탈취한 것으로 보고하였다. 이 중에는 Axie Infinity Ronin Bridge 해킹 사건이 있었으며 이 사건은 라자루스 그룹(Lazarus Group)이라 불리는 북한의 해킹그룹이 인기 비디오게임인 액시 인피니티(Axie Infinity)를 지원하는 게임 중심의

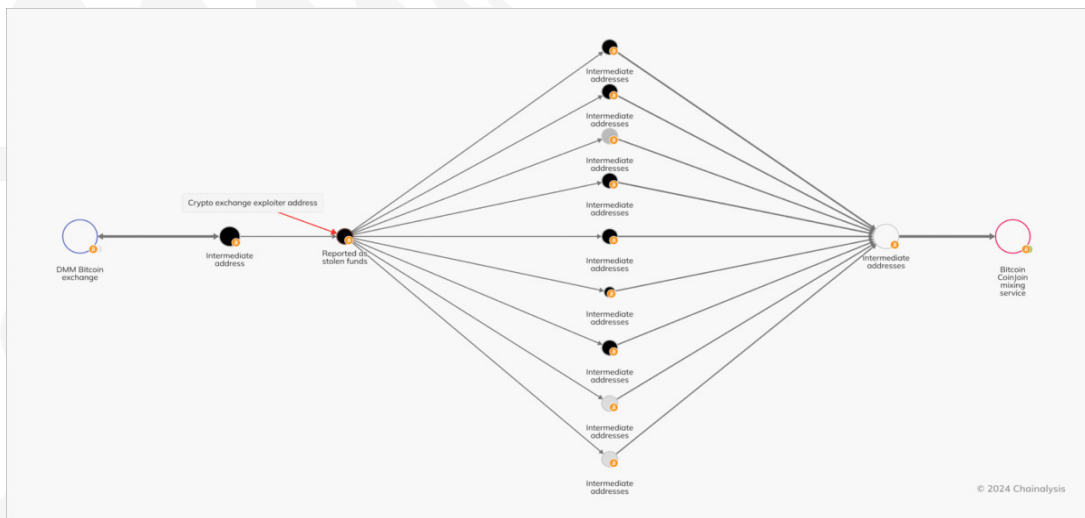
블록체인 네트워크를 표적으로 삼은 해킹 사건이었다. 이를 통해 약 6억 2,500만 달러 상당의 이더리움과 USDC 두 가지 암호화폐를 훔쳐 달아났으며, 이는 역사상 가장 큰 암호화폐 해킹 중 하나였다. 같은 해에, Harmony Horizon Bridge 해킹 관련 사건도 보고되었으며, 이 사건은 라자루스 그룹과 APT38로 명명된 북한의 해킹 그룹이 약 1억 달러 상당의 암호화폐를 탈취한 사건이다. 미국 연방수사국(FBI)은 미국회사인 Harmony 회사로부터 1억 달러 상당의 암호화폐를 훔친 혐의로 북한 정부와 관련이 있으리라 보이는 해커 그룹 2명을 기소했다고 발표하였는데, Harmony는 암호화폐 사용자들이 임의의 블록체인에서 다른 블록체인으로 암호화폐를 전송할 수 있도록 하는 Horizon Bridge를 만든 회사이다. 또한, 가장 최근 사례로 2025년 2월에는 두바이에 본사를 둔 가상자산 거래소 바이빗(Bybit)에서 약 15억 달러 상당의 이더리움을 탈취한 사건이 있었다. 이 공격은 북한의 라자루스 그룹(Lazarus Group) 산하의 트레이더트레이터(TraderTraitor) 조직에 의해 수행된 것으로 알려졌다.

해킹이나 랜섬웨어 공격 등 다양한 사이버범죄를 통해 획득하고 탈취한 가상자산은 다양한 경로로 북한의 핵 및 미사일 개발 자금으로 활용되며, 국제 제재를 무력화하는 수단으로 사용되고 있다. 외교부의 공동 보도자료에 따르면 이러한 불법 외화벌이로 인해 북한이 2024년 전 세계 암호화폐 탈취 금액의 61%이자 역대 최대 금액인 약 13억 불을 탈취하였다고 평가되고 있다. 또한 2024년 유엔 북한 제재위원회 전문가 패널 연례 보고서에는 북한이 사이버 탈취로 핵무기, 생물학적 무기, 화학전 무기 등을 뜻하는 대량 살상 무기 (Weapons of Mass Destruction, WMD) 개발 비용의 약 40%를 충당한다고 보고하였다.

□ 거래소 해킹을 통한 북한의 가상자산 탈취 사례: DMM 비트코인

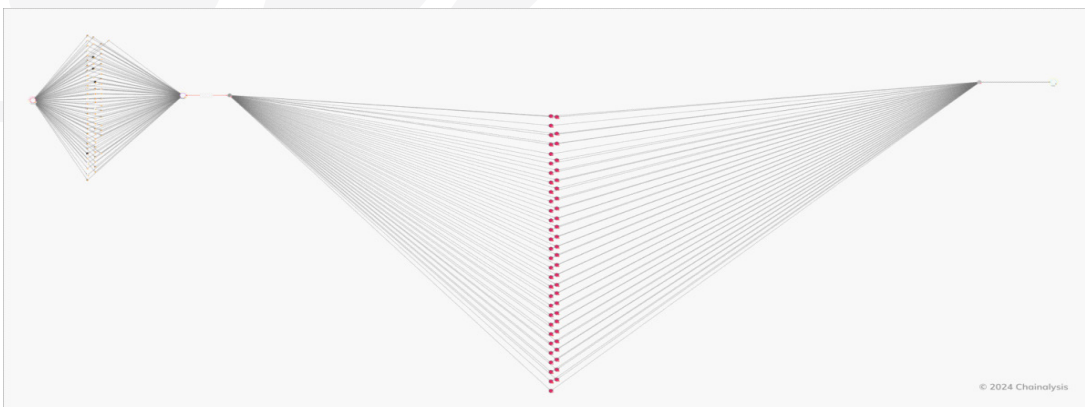
다음은, 북한의 가상자산 탈취 사건과 관련해서 자금세탁이 어떻게 이루어지는지의 사례들을 살펴볼 필요가 있다. 북한이 관련된 가장 주목할 만한 탈취 사건 중 하나로는, 2024년에 일본 암호화폐 거래소인 DMM이 해킹된 사건이 있었다. 이 사건으로 약 4,502.9 비트코인 (당시 약 3억 500만 달러 상당)이 유출되었으며, 해커는 DMM의 인프라 취약점을 노려 무단 인출을 감행했다. 이후 블록체인상의 자금 흐름을 분석한 결과, 공격자는 먼저 거액의 암호화폐를 여러 중간 지갑으로 옮긴 후, 최종적으로 비트코인 믹싱 서비스를 통해 자금을 세탁하였다.

[그림 2]와 [그림 3]은 해커들에 의해 자금이 세탁되는 전체 자금 전송 흐름도를 두 개의 파트로 나눠서 보여주고 있다. [그림 2]는 해커가 DMM거래소로부터 탈취하여 중간 피의자 지갑으로 자금을 나누어서 송신하는 것을 보여주고 있다. 또한 이렇게 나누어진 자금이 자금세탁을 위해서 사용되는 믹서(Mixer)로 모여짐으로써 추적을 어렵게 하였다.



[그림 2] DMM 거래소 해킹 사건후 Mixer로 자금 세탁하는 과정 (출처: Chainalysis)

[그림 3]은 [그림 2]에서 믹서(mixer)를 통한 믹싱과정이 끝난 이후를 나타내고 있다. 즉, 탈취 자금을 비트코인 코인 믹싱 서비스를 통해 1차적으로 세탁한 뒤, 해커들은 그중 일부를 여러 브리징 서비스를 거쳐 최종적으로 캄보디아 후이원 그룹(Huione Guarantee)으로 이체했다. 이곳은 캄보디아 대기업인 Huione Group과 연관된 온라인 마켓플레이스로, 과거에도 사이버 범죄를 조장하는 주요 플랫폼으로 지목되었고, 2025년 5월 1일 미 재무부 금융범죄단속네트워크(FinCEN)가 캄보디아 후이원그룹을 ‘주요 자금세탁 우려 기업’으로 지정하였다.



[그림 3] DMM 거래소 해킹 사건 후 탈취자금이 후이원그룹 계좌로 이체되는 과정

결국 대규모 해킹 피해로 인해 이용자들의 피해뿐만 아니라, 운영상의 어려움으로 인해 DMM은 2024년 12월 거래소를 폐쇄하기에 이르렀다. 또한 이러한 자금 획득을 통해 해커 그룹과 국가 단위의 범죄 집단은 무기 구매나 개발 자금으로 운용함으로써 안보 위협으로까지 발전하게 되었다.

□ 국제 사회의 대응과 전략적 접근 방향

가상자산의 탈취에 대응하기 위한 국제사회의 노력으로, 먼저 한국, 미국, 일본은 암호화폐를 포함하는 가상자산 및 거래소에 대한 북한의 사이버 공격에 대하여 공동 경고를 발령하고, 가상자산 산업 전반에 걸쳐 보안 강화를 추진해야 한다. 이는 북한의 해커 조직이 가상자산 거래소, 디지털 자산 수탁 기관, 개인 사용자 등을 대상으로 지속적인 공격을 하고 있고, 이러한 행위가 국제 금융시스템의 안정성과 세계 금융안보에 위협이 되고 있기 때문이다. 실제, 미국 재무부는 북한의 해커 조직과 연계된 가상자산 믹싱 서비스들을 제재 대상에 포함하는 등, 지속적으로 북한의 불법 자금 세탁 경로를 차단하기 위한 조치를 취하고 있다.

두 번째로는 공공과 민간의 협력을 강화해야 한다. 가상자산 탈취 및 자금 세탁 이슈와 관련해서 국제사회는 공공 부문과 민간 부문 간의 협력을 통해 북한의 사이버 위협에 대응하고 있다. 블록체인 분석 기업, 규제 기관, 가상자산 서비스 제공업체, 법 집행 기관 등이 협력하여 도난당한 자금을 추적하고, 자산을 동결하며, 불법적인 자금 흐름을 차단하는 데 주력하고 있다. 현재에도 국내에서는 미국 정부 기관과 한국 과학기술정보통신부가 공동으로 기술 연구비를 마련하여 여러 기관들이 연구를 진행하고 있다. 이 연구과제에서는 가상자산 기반 자금세탁을 추적하는 시스템 개발연구를 진행하는 등 다각도로 공공 및 민간을 넘어 대학까지 참여하여 이 문제를 해결하고자 노력하고 있다.

향후에도 북한의 사이버 공격은 점점 더 정교해질 것으로 예상되므로, 이에 대응하기 위해서는 보다 전략적인 접근이 필요하다. 먼저 정보 공유와 협력을 강화해야 하는데, 이는 국가간, 그리고 공공 부문과 민간 부문 간의 실시간 정보 공유를 통해 위협에 신속하게 대응할 수 있는 체계를 구축하는 것이다. 그리고 전략적 접근시 고려해야 할 것은 규제 체계의 정비분야이다. 이를 통해 가상자산 산업에 대한 명확한 규제 기준을 마련하고, 불법 행위에 대한 강력한 제재를 통해 북한의 자금 조달 경로를 차단해야 한다. 이와 더불어 기술적 대응 능력을 향상하는 것으로 인공지능(AI) 및 블록체인 분석 기술을 활용하여

Issues & Insights

on Economy, Technology, and Security

의심스러운 거래를 식별하고, 자금 세탁을 방지하는 기술적 역량을 강화해야 한다. 마지막으로 국제 협력 체계를 더욱 강화하여야 하는 바, 유엔 등 국제 기구와의 협력을 통해 글로벌 차원의 대응 전략을 수립하고, 북한의 사이버 위협에 대한 공동 대응 체계를 마련해야 한다.

저자 소개 / BIO



윤지원

- 現) 고려대학교 정보보호대학원 교수
- 現) 고려대학교 사이버국방학과 학과장
- 現) 한국우주안보학회 상임이사
- 現) 무역안보연구회 기술안보 분과 위원
- 現) 국립전파연구원 전파보안 자문위원
- 영국 캠브리지대학 공학(통계신호처리) 박사

Email: jiwon_yoon@korea.ac.kr

윤지원 교수는 고려대학교 정보보호대학원 교수로 재직 중이다. 전문 분야는 신호정보 해독 분야로써, 음성신호, 영상신호, 은닉신호 및 암호 신호 등의 다양한 신호를 분석하고 해독하여 고급 정보 (Advanced Intelligence) 추출하는 연구를 하고 있다. 특히, 현재 한국우주안보학회 상임이사로 우주 안보 관련 연구와 무역안보연구회에서 기술 안보 관련 활동을 하고 있다. 고려대로 부임하기 전에는 IBM Research와 University of Oxford에서 연구원으로 재직한 바 있다. 성균관대 정보공학 학사, 영국 University of Edinburgh에서 정보학(School of Informatics) 및 스코틀랜드 생물통계학 연구소(Scotland Biostatistics Institute)에서 인공지능 석사학위를 받고 이후 영국 캠브리지대학교 공과대학 통계 신호 및 통신연구실에서 2008년에 박사학위를 취득했다.

Jiwon YOON

- (Current) Professor, School of Cybersecurity, Korea University
- (Current) Chair, Cyber Defense Department, Korea University
- (Current) Member of Korean Academy of Space Security, Korea
- (Current) Member of the Technology Security Subcommittee, Trade Security Research Association, Korea
- (Current) Advisor in EM security, National Radio Research Agency, Korea
- Ph.D. in Statistical Signal Processing, University of Cambridge

Professor Jiwon Yoon is a faculty member at the school of Cybersecurity and the chair of the Department of Cyber Defense at Korea University. His area of expertise lies in signal intelligence analysis, where he conducts research on analyzing and decrypting various types of signals—including speech, video, covert, and encrypted signals—to extract advanced intelligence. He is currently serving as an executive director of the Korea Space Security Society, contributing to research in space security, and he is also active in technology security through the Trade Security Research Association.

Before joining Korea University, he worked for IBM Research and the University of Oxford. He earned B.Sc. degree in information engineering from Sungkyunkwan University, and a M.Sc. degree in artificial intelligence from the School of Informatics at the University of Edinburgh and the Scotland Biostatistics Institute. He received his Ph.D. in 2008 from the Signal Processing and Communications Research Group in the Department of Engineering at the University of Cambridge.