

**코인원,
모두에게 안전한 가상자산
취급업소로의 도약**

1. AML을 도입하는 이유
2. 코인원의 운영 현황
3. 코인원 AML 대응 방안

가상자산 취급업소가 AML을 도입하는 이유

가상자산과 거래소에 대한 불편한 시선

범죄

- 다크웹 사이트를 통해 마약, 총기 등의 불법 대금 지급
- 불법컨텐츠 결제 수단
- 유사 수신 및 사기

해킹

- 해킹, 가상자산 탈취 등을 통한 고객 자산 손실

자금세탁

- 가상자산의 익명성을 이용한 자금세탁
- 차명거래 등 실소유자 은닉
- 불법자금 은닉/세탁 통로로 이용

가상자산과 거래소의 대응



- 이상거래 판단시 거래 제한
- 블랙리스트 관리

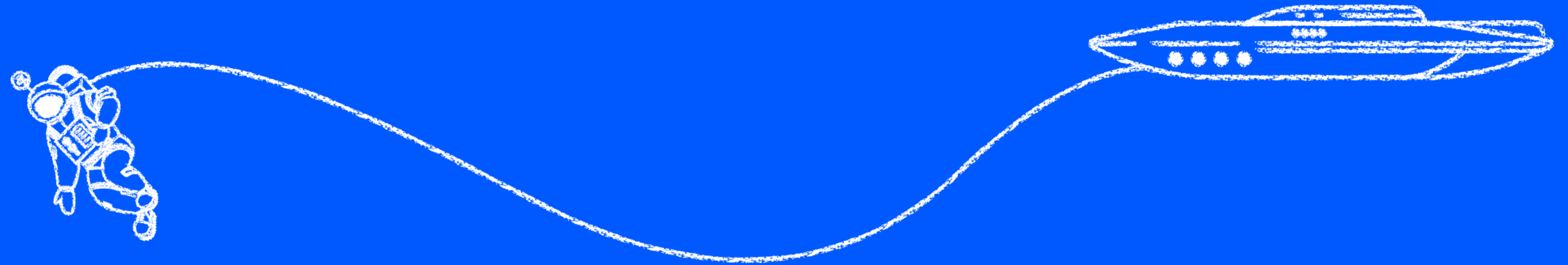


- 보안 강화를 통한 해킹 시도의 차단 및 리스크 최소화



- 자금세탁방지체계 수립
- 자금세탁방지 시스템 구축

코인원의 오늘



코인원, 모두에게 안전한
가상자산 취급업소로의 도약

2

코인원의 운영 현황

1. 정보 보안 체계

해킹으로 인한 암호화폐 유출 피해 규모

사건 발생일	피해 업소	피해 내용	경제적 피해 추정 규모 언론보도 추정
2017. 4	코000000	가상통화 유출	약 55억
2017. 6	비000000	1. 개인정보 약 3.6만건 유출 2. 해킹메일 열람 (직원 개인PC) 후 악성코드감염 3. 외부(개인PC)에서 개인정보 열람 4. 개인정보 유출	약 70억
2017. 9	코000000	가상통화 유출	약 21억
2017. 12	유000000	가상통화 유출	약 170억
2017. 6	코000000	가상통화 유출	약 500억
2018. 6	빗000000	가상통화 유출	약 350억
2018. 10	올000000	가상통화 유출	확인 불가
2019. 3	빗000000	가상통화 유출	약 100억~200억
합계			약 1,266억

출처: 신용현 의원실 (과학기술정보통신부, 한국인터넷진흥원 제출자료 재구성)

1. 정보 보안 체계

화이트해커 출신 창업자

- 차명훈 CEO의 수상 이력
 - 데프콘 CTF 수상 (09')
 - 코드게이트 수상 (09')

보안인증 획득

- 정보보호관리체계(ISMS) (18'~)
- 국제표준 정보보호 인증 (ISO27001) (19'~)

높은 보안 관리체계 운영

- 소스코드 레벨의 취약점 점검 및 조치
- 이상 행위 상시 모니터링
- 가상자산의 85% 이상을 물리적으로 분리하여 관리

2014년 출시 이래 보안사고 0건

2. 실명확인 입출금 계정 사용



NH농협은행 실명확인
입출금계정 서비스 이용 중



은행과 커뮤니케이션 통해 협업
자금세탁방지 업무 준수 현황 실사,
암호화폐 AML 이슈 협의 등

3. FDS / 사고방지

FDS/사고방지 룰 수립

- FDS/사고방지 룰을 수립하고, 지속적 모니터링 체계 구축

데이터를 기반으로, 지속적인 업데이트

- 실제 사기 사례 등 다양한 데이터를 기반으로, 룰의 지속적 업데이트

출금제한정책 적용

- 출금제한정책 등을 적용하여 사고율 대폭 감소

2019년 8월 이후, 사고 발생 0건

4. 상장 및 상장폐지 기준

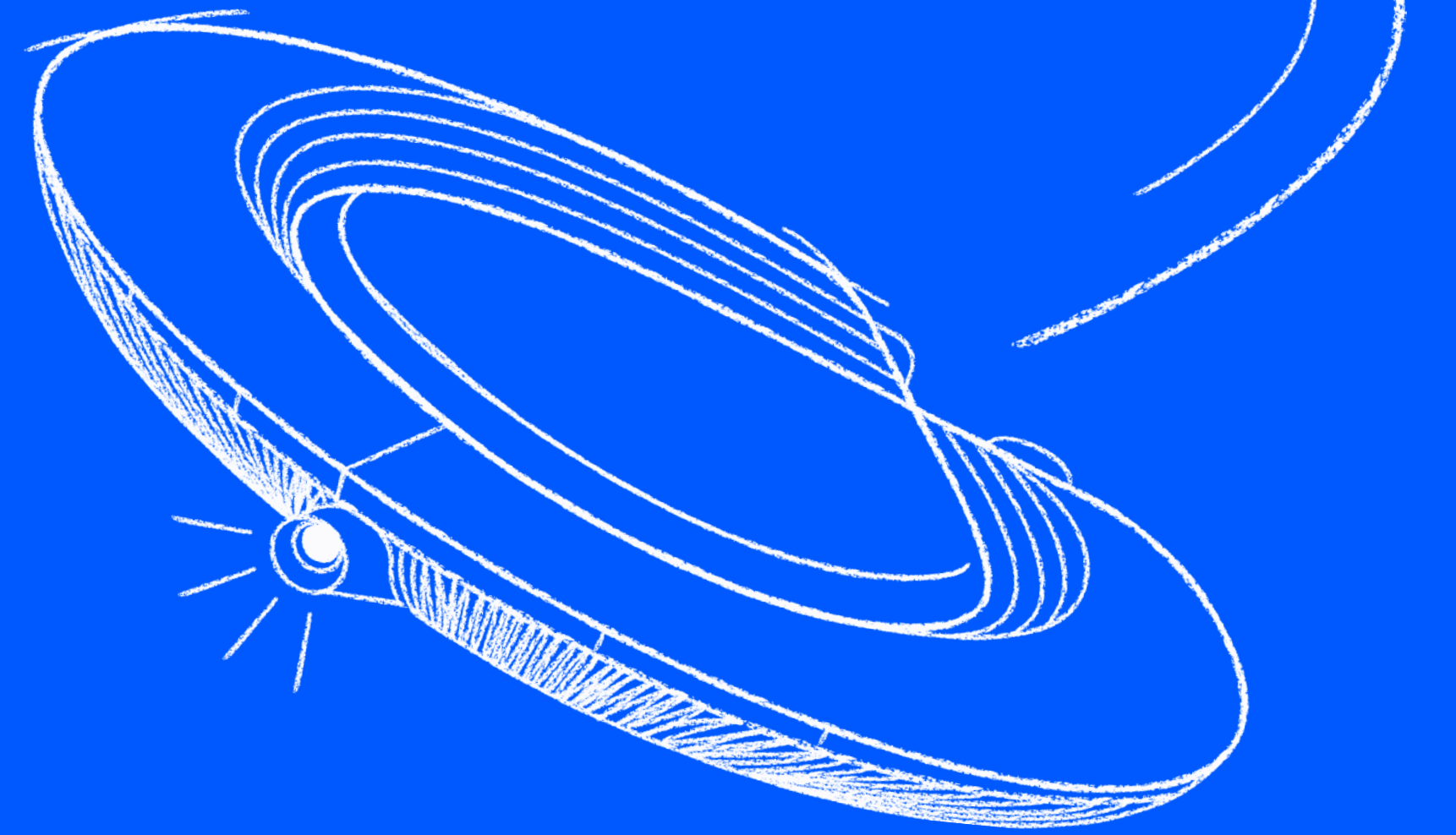
보수적 상장

- 거래소 자체의 명확하고 보수적 상장 기준 수립
- 코인원 심사 기준에 부합하는 프로젝트는 전체에서 5%미만
- 다크코인 상장 경험 없음

신중한 폐지

- 상장된 프로젝트에 대해서 지속적 검토 진행
- 자금세탁위험이 있는 프로젝트의 경우 상장폐지 대상으로 고려, 유의종목 지정 및 폐지 예정

코인원의 내일



코인원, 모두에게 안전한
가상자산 취급업소로의 도약

3

코인원 AML 대응 방안

1. 선제적인 AML 체계 수립

금융회사 수준 자금세탁방지체계 수립

- FATF 권고안, 특정금융정보법 및 동법시행령, 업무규정 요구 사항 충족
- 자금세탁방지 전문 컨설팅 업체와 함께 내부통제, 거래 모니터링 및 고객확인 의무 체계 수립, 운영 솔루션 구축 중

KYC

회원 에 대한 고객확인절차 체계 수립

TMS

효과적인 의심거래 탐지를 위한 상시 거래 모니터링 시스템 운영

RA

신규 및 기존고객의 자금세탁 위험 식별 및 평가를 위한 고객위험평가

STR

의심거래패턴 분석을 통한 거래모니터링 및 보고 체계 구축

2. AML Governance 체계 강화

Governance 체계

- 최고위 경영진인 EVP(부대표)가 AML 총괄 책임
- AML 내부통제 위원회 운영 – 대표이사 참석

전사 차원의 AML책임 관리

- 업무 부서별 자금세탁방지업무 담당자 지정
- 현업 부서의 AML 관련 R&R 명확화 – KYC, 거래모니터링, 내부 보고체계, 독립적 감사 등

독립적 감사 체계

- 독립적 감사체계 마련을 위한 감사 조직 신설

3 Line Defense 체계

- 1차 : 현업 (Operating)
- 2차 : 전담조직 (Compliance)
- 3차 : 독립적 감사 (Internal Audit)

3. 전사 ML/TF 위험관리 체계(RBA) 구축

전사 ML/TF 위험 식별/분석 모델

- 자금세탁/테러자금조달 위험
평가모델 구축

지속적인 모니터링 및 평가

- 고객 및 거래 데이터 기반 위험값 산출
- 자금세탁 통제 활동에 대한 주기적인
평가 체계 수립

고위험 특별 관리

- 고위험 영역에 대해서는 원인파악,
추가점검, 교육수행 등의
후속조치 수행

* FATF RBA 기준 및 특정금융정보법 요구에 근거해 RBA 체계 구축

** 금융회사는 금융거래 등에 내재된 자금세탁행위와 공중협박자금조달행위의 위험을 식별, 분석, 평가하여 위험도에 따라 관리 수준을 차등화하는 업무체계를 구축 및 운영하여야 함

4. 고위험 집중 KYC 및 STR 모니터링 체계 운영



5. Travel Rule 관련 대응



- 입금 시 송금인 정보가 입수되는 경우 거래 거절 대상 여부 모니터링
- 이상 입금에 대한 자산 동결 처리 및 후속 조치 진행

- 수취인 정보 축적 관리
- 수취인에 대한 거래 거절 대상 여부 모니터링 및 출금 제한(AML 솔루션 업체와 논의 중)

6. 검사감독기관 및 금융회사와의 협업 강화

KoFIU/금감원 감독 검사 대응

- 특정금융정보법 개정(안) 충족
- FATF 권고안 준수
- KoFIU 운영위험지표를 기준으로 회사의 내부통제 수준을 은행 등 선진 금융회사 수준으로 향상

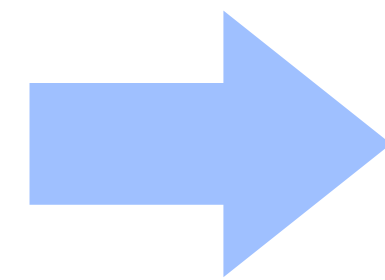
금융회사와 협업

- 의심거래 모니터링 완전성을 위해, 금융회사와 적극적으로 정보 공유
- 실명확인 입출금계정 서비스 이용 금융회사와 협업을 통한 사고 예방

끝내며,



거래소의 안전성
거래소의 투명성



투자자 불안 해소

블록체인 기술 발전의 양성화, 가상자산 산업의 활성화

감사합니다.