Digital Asset eXchange Alliance

보도 자료(Press Release)

배포일시	2024년 9월 12일	보도일시	2024년 9월 12일(즉시)
사진	유 ■ 무 □	쪽수	6쪽(본문1, 별첨5)

DAXA, 가상자산 지갑 운영관리 모범사례 및 해설서 마련

디지털자산거래소 공동협의체(DAXA)는 지난달 시행된 「가상자산 이용자 보호 등에 관한 법률(이하 '이용자보호법')」 제7조에 따라 가상자산사업자(VASP)에게 부여된 가상자산 보관과 관련한 수범 의무를 지원하고자 「가상자산 지갑 운영관리 모범사례(이하 '모범사례') 및 해설서」'를 마련했다고 12일 밝혔다.

이용자보호법 제7조는 이용자자산의 보호를 위해 사업자의 고유자산 및 고객 자산 간 분리 보관, 동종 동량의 실질 보유, 인터넷과 분리 보관 등에 대해 규정하고 있다. 이에 DAXA는 가상자산사업자 및 관련 업무 종사자의 이해를 돕고자 자율규제의 일환으로 모범사례 및 해설서를 마련한 것이다.

이번 모범사례는 DAXA를 중심으로 감독당국의 지원 하에 총 23개 가상자산사업자가 공동으로 참여한 가운데 마련되었다. 특히 올 상반기 감독당국이 주관한 사업자 현장컨설팅 내용을 바탕으로 실제 사업자가 가상자산을 보관·관리하는 실정이 반영되었으며, 업계 역시 총 3차례에 걸친 의견수렴 과정을 거쳐 최종적으로 본 모범사례 및 해설서가 제정된 것이다.

모범사례의 구체적인 내용으로는 ▲인적·물리적 보안 절차, ▲지갑 생성·보유·관리방안 ▲콜드월렛 내 가상자산의 출금 절차 등의 내용을 담고 있으며, 해설서는 모범사례의 내용을 보다 구체화하여 자세한 예시와 함께 절차 등의 설명을 담고 있다.

한편, DAXA는 이용자보호법 시행 전후로 계속해서 가상자산사업자의 관계 법령 준수를 위한 여러 지원활동을 이어오고 있다. 지난 7월에는 이용자보호법 시행에 맞추어 「가상자산 거래지원 모범사례」를 발표한 바 있으며, '이상거래 상시감시 모범규정'과 '표준 광고 규정' 등을 제정 및 공개하는 등 가상자산업계의 자율규제 역량 강화를 위해 부단히 힘쓰고 있다. 끝.

GOPAX bithumb UPbit korbit coinone
BORABIT Beeblock BITCMON BTX OASIS Exchange GDAC
CORDAX crypto.com | KOREA FOBL pravang FLYBIT Flata EXCHANGE
O-HI Wallet INFINITE BLOCK KOREA DIGITAL ASSET CUSTODY KODA 한국 디지털 에셋 CUSTELLA PayProtocol

별첨#1 | **가상자산 지갑 운영관리 모범사례 및 해설서 주요 내용**

1 가상자산 지갑 정의

① **콜드월렛** : 가상자산에 접근 가능한 **개인키** 등의 정보를 **오프라인** 상태로 **보관** 및 **사용**하는 지갑으로 **정의**

* 이용자보호법(§7)상 콜드월렛을 "가상자산을 인터넷과 분리해 안전하게 보관"하는 것으로 규정

- **개인키**를 **인터넷**과 **분리**해 **보관**하더라도, 인터넷과 **분리되지 않은 상태**로 개인키를 **사용***하는 경우 콜드월렛으로 인정받기 곤란

* 콜드월렛에서 핫월렛으로의 가상자산 출금 및 여타 스테이킹 거래 등을 위한 전자서명 행위는 개인키의 사용에 해당

② **핫월렛** : 지갑의 **개인키**를 **온라인**에 **보관** 또는 **사용**하는 지갑

2 인적 · 물리적 보안 등

① **역할의 분리** : 가상자산 **지갑**에 **접근**이 **가능**한 **역할**과 **책임**을 정의하고, **3인 이상 담당자**에게 **분리·할당***해 **권한**의 **오남용 방지**

* ①월렛룸 접근, ②금고 개폐·지갑 사용, ③출금 내역 감시 및 잔고 일일대사 역할 분리

② **월렛룸** : **개인키 보관·사용** 등을 위한 업무공간을 일반 사무공간과 **분리**(통제구역 지정)하고, 가상자산 **지갑 보호 대책**을 마련·시행

- **출입·개방통제** : **CCTV, 방화벽** 및 **출입통제장치** 등을 **설치**해 **비인가자의 접근** 등을 **차단**하고, **출입관리대장**을 **기록·보존**

  - [출입]**월렛룸 접근 권한**과 [개방·사용]**내화금고*** **개폐**(지갑정보 접근) **권한**을 **엄격히 분리**하거나 **복수**의 **인력**이 **공동**으로 **수행**

* ❶콜드월렛 개인키가 저장된 장치(예: H/W월렛, 종이·철판월렛 등)와 ❷지갑 생성·이체 업무를 수행하기 위한 PC, 노트북 등 콜드월렛 업무지원 단말기를 내화금고에 보관

- **작업통제** : 월렛룸에서 **지갑 생성**, **가상자산 출금** 등 **최소한**의 **업무**를 **수행**하고, **독립적 지위에 있는 자***가 **작업과정**을 **감독·기록**

* 가상자산 지갑의 접근·출금 업무에 관여하지 않는 자

  - 가상자산 **지갑** 및 콜드월렛 업무지원 **단말기** 등의 **외부 반출**을 **제한**하고, 작업에 필요한 **최소한**의 **비품**(예: 책상, 의자)만 **비치**

3 지갑 생성 · 보유 · 관리 등

① **생성** : 가상자산사업자는 **사전검토** 및 **승인 절차** 등을 거쳐 안전한 암호화 알고리즘을 활용해 **가상자산 지갑**을 **직접 생성**

- **지갑 관련 최고 책임자**가 **복구 코드**의 **기록·보관** 단계 전반을 수행하고 **제3자**의 **정보 접근**을 **제한***

  * 복구코드로 지갑을 복원해 부당거래에 서명 후 가상자산을 탈취할 가능성을 차단

- **백업용 개인키** 및 **복구코드** 등은 월렛룸과 물리적으로 떨어진 안전한 장소에 별도 **소산**

② **보유** : 가상자산사업자는 이용자 가상자산의 **동종동량 보유 여부**를 **확인**하기 위해 매일 **일일대사**를 **수행***

  * 분산원장과 내부원장 상 잔고의 일치 여부를 확인하고, 불일치 발생 시 차이 내역을 관리

- **외부 지갑 서비스** 사용 시에도 사업자가 해당 지갑의 **독립적 통제권**을 확보*함으로써 가상자산의 **실질 보유 의무**를 **준수**

  * [통제권 확보 기준] ❶직접 지갑생성, ❷자사 서버, 단말기에 개인키 보관·관리, ❸자사 서버, 단말기에서 전자서명, ❹독립적인 전자서명 이행 수단 확보

- 만약, 지갑의 독립적 통제권을 확보하지 못하고 외부 위탁에 해당할 경우 **수탁기관**이 **보안기준***을 **충족**하는지 **여부**를 **평가**

  * 연 1회 이상 보안취약점 분석·평가 실시, 수탁 가상자산을 콜드월렛에 100% 보관 등

③ **관리** : 가상자산 출금 거래 승인 및 접근통제 절차를 운영하고, 개인키의 유출·도난·분실 등 사고예방을 위한 보안대책 등 수립

- **멀티시그**(다중서명), **MPC*** 등 전자서명 방식을 활용해 **콜드월렛**의 **보안수준**을 **강화**하고, **업무지속계획(BCP)** 등을 수립

  * MPC(Multi-party Computation, 다자간연산) : 여러 소유자가 공동으로 각자의 키 조각을 입력하면 개인키 조합 없이 함수 연산을 통해 전자서명이 이루어짐

- **지갑**과 **노드**(Node) **서버**를 **분리**하고, **노드서버 이중화** 및 노드 **외부위탁 운영 기준 마련** 등을 통해 **입출금 거래**의 **안정성 확보**

④ **분리 보관** : **고유·고객 자산 지갑**을 **별도 생성**하고 동일 지갑 내 자산 **혼장여부**를 점검해 **고유·고객 가상자산 분리**

4 콜드월렛 가상자산 출금 절차

① **콜드월렛 운영** : **콜드월렛 개인키**를 월렛룸 內 **오프라인** 환경에서 **생성, 유지·보관** 및 **사용**(전자서명)해야 함

- ㅇ 가상자산 보유 규모, 거래 빈도 등을 고려해 콜드월렛을 복수의 저장매체 또는 금고에 분리 보관해 집중 리스크를 최소화

- ㅇ 업무용 단말기를 ❶**개인키 전자서명**에 사용하는 **업무지원 단말기**(오프라인)와 ❷거래정보의 **브로드캐스트 단말기**(온라인)로 **분리**

② **출금거래 통제** : 콜드월렛의 **출금 한도**, **화이트리스트*** 정책, **사전 승인 절차** 등을 마련해 **출금 거래**를 **통제**

* 사전에 등록한 지갑 주소로만 가상자산을 이체

- ㅇ **이체**할 가상자산의 **종류**, **수량**, **송수신 지갑 주소**, **사유** 등의 내용을 포함해 **작업계획서**를 작성해 책임자 **승인·보고**

③ **출금 절차** : 단말기에서 **거래정보**(Unsigned transaction)를 **생성***하고, **작업 감독자**는 입력된 **수신주소** 등이 **화이트리스트 주소** 및 **작업계획서**와 **일치하는지 여부를 2차 확인****

* 그룹웨어 상 작업계획서 승인 내역, 지갑 주소 QR코드 등의 인쇄물을 활용하고, 불가피한 경우를 제외하고 인터넷, USB 등 외부 연결을 차단

** 최근 발생한 日 'DMM 비트코인' 해킹사고 등에 악용된 것으로 추정되는 지갑 주소 오염 공격(Address Poisoning Attack) 등에 대응

- ㅇ **개인키**가 **인터넷** 환경 등에 **노출되지 않도록 오프라인** 단말기에서 **전자서명**을 수행