

디지털 지갑

우리 지갑은 점점 얇아지고 있다

권오현 계간 스켑틱 편집자

우리 지갑은 점점 얇아지고 있다. 경제가 어려워 소득이 줄어들었다는 말이 아니라 사람들이 현금과 카드를 들고 다니지 않게 되면서 정말 물리적으로 지갑이 비고 있다는 뜻이다. 모든 것을 흡수하는 스마트폰은 이제 지갑 역할도 대신하고 있다. 바로 디지털 지갑이다.

전통적 금융기업의 디지털 지갑 전쟁

은행권의 디지털 지갑은 온라인 뱅킹, 모바일 앱 뱅킹을 비롯한 금융 거래 및 전자 결제 수준을 뛰어넘어 소비자에게 진정으로 지갑을 대신하는 전방위적 서비스를 제공하는 것을 목표로 한다. 전자 신원 증명, NFT, 코인 등 가상 자산 거래, 전자 증명서 및 문서 보관 등 활용처는 무궁무진하다.

예를 들어 국내 1위 은행인 국민은행의 디지털 지갑 서비스 ‘KB월렛’은 공공문서 간편발급과 쿠폰 관리, 전자증명서 서비스, 국민비서, 전자문서 서비스를 제공한다. 인천공항 내 소요 시간 확인, 자동차 검사 예약, 국립자연휴양림 예약도 할 수 있다. 하나은행의 디지털 지갑 ‘하나원큐’는 국민비서 꾸뻬, 행안부 연계 인증서 발급 서비스를 제공한다. 은행, 증권, 카드, 보험까지 한 번에 통합 조회할 수 있으며, 디지털 보안을 위해 보이스피싱 애플리케이션 탐지 기능도 포함돼 있다. 신한은행의 ‘쏠지갑’은 토큰뱅크와 연계해 디지털 자산을 보관할 수 있는 NFT월렛이라는 서비스를 차별 포인트로 내세웠다. 4대 은행 중 가장 늦게 전자 지갑 서비스 ‘원더월렛’을 개시한 우리은행은 금융기관 디지털 지갑의 거의 모든 서비스를 종합하고자 한다. 원더월렛은 공공정보 알림부터 전자증명서 발급과 제출, 자격증명서 발급과 더불어 NFT지갑 서비스를 제공한다.

은행의 변신과 발맞추어 행정안전부도 디지털 지



갑 서비스에 나선다. 행정안전부는 디지털지갑 구축 업무 프로세스 재설계(BPR), 정보전략계획(ISP) 수립을 마치고 2024년 2월부터 디지털 지갑 본사업을 시작한다. 모바일 신분증, 전자증명서, 마이데이터 등을 통합한 공공서비스를 제공한다. 가령, 실직하여 건강보험공단의 자격정보가 변경되었을 경우 디지털 지갑에서 실업급여 신청, 구직사이트 연계, 자기개발 프로그램 신청 등 맞춤 서비스가 추천된다.

디지털 지갑의 보안을 위하여, 하드웨어 지갑 vs 소프트웨어 지갑

디지털 지갑으로 각종 정보가 통합되면서 사이버 보안 문제도 매우 중요해지고 있다. 물리적 지갑과 달리 디지털 지갑에는 전자서명용 개인 키가 있기 마련이라 해킹당했을 경우 피해 범위가 커진다. 게다가 컴퓨터 바이러스나 랜섬웨어가 침투할 위험도 상존한다.

보안과 관련해서는 디지털 지갑에 있는 정보의 저장 유형을 구분할 필요가 있다. 디지털 지갑은 크게 ‘핫월릿 또는 소프트웨어 지갑’과 ‘콜드월릿 또는 하드웨어 지갑’으로 나눌 수 있다. 핫월릿은 항상 인터넷에 연결되어 있는 온라인 저장 지갑을 말한다. 우리에게 익숙한 데스크톱, 스마트폰, 클라우드가 바로 핫월릿에 속한다. 핫월릿은 즉시 자금 이체가 가능하고 실시간으로 이체 내역을 확인할 수 있어 사용 편의성과 접근성이 뛰어나다.

핫월릿에 접근할 때도 당연히 접근 암호나 펀코드, 생체인증처럼 사용자가 설정한 보안 절차를 거쳐야 한다. 항상 인터넷에 연결되어 있다는 점은 보안의 위험 요소다. 해커들은 주로 핫월릿에 저장된 개인 키를 노리며 만일 내 디지털 지갑이 단일 키로만 보안이 되어 있다면 자산이 모두 출금되기까지는 단 몇 분밖에 걸리지 않는다. 수많은 암호화폐 거래소 해킹

사건이나 데스크톱에서 이뤄지는 랜섬웨어 해킹은 늘 인터넷에 연결되어 있다는 취약성에서 비롯했다. 특히 데스크톱보다는 스마트폰이 더 취약하다.

핫월릿의 이러한 약점을 보완하는 것이 콜드월릿이다. 이는 물리적 지갑과 마찬가지로 보안을 위한 스토리지, 즉 하드디스크 같은 물리적 저장장치에 보관하고 각종 보안 장치를 프로그램해 두는 것이다. 그래서 하드웨어 지갑이라는 이름으로 불리기도 한다.

콜드월릿은 인터넷에 연결되어 있지 않은 오프라인 장치이기 때문에 바로 출금이 불가능하며 여러 단계를 거쳐야 한다. 다소 편의성을 희생하더라도 콜드월릿은 해킹이나 바이러스로부터 상대적으로 안전하다는 장점이 있다. 전용 하드웨어 스토리지는 더 많은 보안 메커니즘을 제공하며, 컴퓨터에 연결하는 것 외에는 외부와의 연결이 없기 때문에 해커가 장치에 쉽게 접근할 수 없다. 물론 하드웨어 특성상 물리적 장애가 발생하면 복구가 불가능할 수도 있으므로 백업은 필수다.

트레저(Trezor), 레저(Ledger), 킵키(Keepkey)처럼 자산을 안전하기 보호하기 위한 전용 스토리지가 있지만, 오픈 소스 프로그램을 활용하여 내 USB나 하드디스크를 하드웨어 지갑으로 만들 수도 있다. 예를 들어 트루크립트(TrueCrypt) 같은 암호화 소프트웨어는 파일 형태의 암호화된 저장소를 만들어는데, 물리 하드 디스크 드라이브를 통째로 암호화해 준다. 이 프로그램은 FBI, CIA 같은 정보기관이 암호화 해제에 실패한 사례로 알려져 유명하다.

IT 강국인 우리나라는 이제 현금 없는 대중교통이 상징하듯이 디지털 지갑이 보편화된 사회로 가고 있으며 각종 신분증과 자격증도 디지털화되었다. 이렇게 막을 수 없는 변화의 흐름 앞에서 가장 중요한 건 과거에 대한 향수가 아니라 변화에 대한 안전한 적응 일 것이다. 