# 블록체인 진짜 안전해요?

광주MBC칼럼
이흥노 교수
6월 12일

가상화폐 거래소 코인레일 해킹… 40분간 400억 털렸다.
Monacoin, Bitcoin Gold, Zencash, Verge, Litecoin cash...
등 변종 코인들도 수 백억원대 해킹을 당했다는 소식이 들려온다.
지난 몇일 간 전세계를 강타한 암울한 뉴스들이다.
코인레일은 즉각 거래중단 조치를 단행했다.
그러나 해당 거래소 사용자들이 피해액을 온전히 돌려받을 수 있을 지는 의문이다.
보험을 들었는지, 보험금액은 충분한지 모르기 때문이다.

한 편에서는 블록체인은 4차 산업혁명의 핵심기술이다, 디지털 미래를 개척한다,
라고 띄우며 기업 투자, 교육, 연구를 독려하는 판인데,
다른 편에서는 동일 기술 관련 금융보안사고가 계속해서 나고 있다.
이런 상황에서 어떻게 이 기술의 미래를 믿을 수 있을까?
블록체인은 해킹이 불가능하다고하지 않았던가?

분석을 해 보니 가장 큰 문제는 역시 거래소였다.
다음은 소규모 신규 암호화폐 들이다.

첫 째. 거래소는 천문학적인 암호화폐를 보관하고 있기 때문에 해커들의 목표가 된다.
이런 상황에서 수준 낮은 보안 시스템을 유지하는 거래소들이 큰 문제가 되고있다.
이런 거래소에서는 블록체인과는 아무 상관없는 해킹사고가 난다.
거래소에 있는 컴퓨터서버는 다른 컴퓨터서버들과 다를 바 없다.
인터넷을 타고 들어가 서버에 침투해서 지갑에 저장된 고객의 주소를 털어가면 속수무책이다.
수준 높은 보안을 유지하는 규모가 큰 거래소로 옮기는 것을 추천한다.

둘 째. 소규모 암호화폐들을 조심해야 한다.
해킹 사고가 난 코인들은 모두 신종 코인들이다.
신종암호화폐의 블록체인은 해킹에 취약할 수 밖에 없다.
Bitcoin이나 Ethereum은 전세계로부터 수 많은 채굴자들이 참여하므로,
블록체인 무결성이 유지된다.
블록체인을 해킹하기 위해서는 정상채굴자들이 확보한 채굴기보다
더 많은 수의 채굴기를 확보해야 가능한데,
당연히 정상 채굴자를 수없이 많이 확보한 코인은 공격하기 어렵게 된다.
반대로 정상 채굴자를 충분히 확보하지 못 한 소규모 코인은 공격에 매우 취약해진다.

그러면 암호화폐 투자자 및 거래소 사용자들은 어떻게 해야 할까?

개인 월렛을 다운로드 받아서 사용하고 개인월렛에 자금을 보관하는 게 좋다.
개인 월렛 사용이 어렵다면 최소한 서버를 잘 관리하고
충분한 금액의 보험을 들고 있는 대형 거래소로 옮기는게 좋다.
거래소는 환전할 때만 사용하라.
최소한 거래소 지갑에 장기간 자금을 보관하는 것은 피해야 한다.

전 세계 채굴시장 환경의 변화가 매우 빠르다.
이제는 채굴기 대여시장도 생겨났다.
공격자들은 이를 악용하고 있다.
즉, 1시간 동안의 공격을 위해서 채굴기를 대여만 해도 되는 것이다.
거래소를 터는데 필요한 시간은 몇 십분이면 된다.

51Crypto 라는 웹 사이트는 매우 충격적인 내용을 공개해 놓았다.
특정 코인을 한 시간 동안 공격하는데 들어가는 총 비용을 계산해 놓은 것이다.
가령 Bitcoin은 48만 불, Ethereum은 37만 불이 든다.
그러나 8억구천만 불의 Market Cap을 보유한 Bytecoin을 공격하는데에는
겨우 6백 불 밖에 안든다.

사용자는 개인지갑을 적극 활용하고 거래소는 환전할 때만 이용하는 지혜가 필요하다.
개발자는 Bitcoin과 Ethereum을 뛰어 넘을 만한 새로운 혁신아이디어 개발이 필요하다.
혁신 없는 블록체인은 그저 사라지고 말 뿐이다.

끝