가상화폐 기술 및 보안

지도교수 : 이 호
연 구 자 : 이진호

< 목 차 >

요 약

요즘 블록체인 기술을 기반으로 한 가상화폐(비트코인)에 대한 관심이 열풍이다. 코로나가 터지고 더한 열풍을 부는 것 같다. 하지만 이러한 가상화폐에도 보안이 있지만, 기술도 같이 발전함으로써 공격도 많아지고 있다. 그래서 가상화폐에 보안이 어떠한지 알아보고자 한다.

주요어 : 가상화폐, 비트코인, 블록체인, 코인

1. 서론

2008년 비트코인이라는 가상화폐의 개념이 발표된 이후, 비트코인의 기반이 되는 블록체인 기술은 향후 우리 사회를 변화시킬 수 있는 4차 산업혁명 시대의 중요한 플랫폼 기술로 주목받고 있다. 가상화폐의 기반이 되는 블록체인의 핵심 기술 영역은 검증된 암호기술을 기반으로 위조와 해킹이 어렵도록 일정 수준 이상의 보안성을 갖추고 있으나, 가상화폐를 사고파는 거래 서비스나 상품 대금으로 지급하는 결제 서비스의 구현에 있어서는 새로운 보안 취약점 등 보안 위험이 존재할 수 있기에 가상화폐 사용에 있어서 보안 위험에 대해서 살펴보고 대응 방안에 대해서 논하고자 한다.

2. 가상화폐

가상화폐는 지폐나 동전과 같은 실물이 없이 네트워크로 연결된 특정한 가상공간(virtual community)에서 전자적 형태로 사용되는 디지털 화폐 도는 전자화폐를 말한다. 주로 비트코인 등의 암호화폐를 일컫는 말로 사용하지만, 실제로는 암호화폐보다 폭넓은 개념이라고 한다. 비트코인은 블록체인 기술을 기반으로 하는 암호화폐이다. 암호화폐(코인)의 경우 2017년 기준 약, 700개 이상이 존재한다고 한다. 이 가운데 2017년 12월 기준 한국에서 거래가 가능한 코인은 12개 정도이다. 그 중, 가장 잘 알려진 암호화폐가 바로 비트코인이다. 블록체인 기술을 기반으로 만든 암호화폐로 익명의 개발자가 배포했다고 한다. 거래 내역을 중앙 서버에 저장하는 일반 금융기관과 달리 블록체인 기술을 바탕으로 사용자 모두의 컴퓨터에 거래 내역을 저장하는 것이 특징이다. 일반 화폐와 달리 발행 주체가 없고, 암호를 풀어내는 방식으로 누구나 비트코인을 '채굴(Mining)'할 수 있다.

[사진 1] '312만 명' 돌파한 가상화폐 앱 사용자 수 상승세 지속

가상화폐의 종류에는 다음과 같이 있다.

1) 지불형 코인 또는 결제형 코인

지불형 코인이란 이름에서도 알 수 있듯이 상품을 사는데 지불하거나 결제가 가능한 코인이다. 따라서 코인이 만들어진 목적 자체가 지불형 또는 결제형인 경우를 의미한다. 쉽게 말해 화폐의 대용으로 사용 가능하다고 할 수 있다. 우리가 아는 것 중 대표적인 지불형 코인은 비트코인이다. 물론 비트코인뿐만 아닌 여러 개가 존재한다. (라이트코인, 비트코인 캐시, 도지코인, 페이코인 등등)

2) 플랫폼형 코인

플랫폼이란 흔히 시스템에서 가장 기초가 되는 틀을 의미한다. 즉, 플랫폼 코인이란 어떠한 서비스를 제공하는 기초 틀에 사용되는 코인이다. 예를 들어 게임이라는 플랫폼에서 통용되는 코인이 있다면 그게 바로 플랫폼형 코인의 종류가 될 수 있다. 플랫폼형 코인의 대표적인 코인은 이더리움이다. 그 외(체인링크, 비체인, 스텔라루맨, 이더리움 클래식)

3) 스테이블 코인

스테이블 코인이란 이름에서 오듯 안정성을 가진 코인을 의미한다. 스테이블 코인은 변동성을 최소화하기 위해 1코인 = 1달러 가치를 갖도록 설계했다. 스테이블 코인의 장점으로는 더 적은 수수료로 빠른 거래를 할 수 있다. 대표적인 코인은 테더이다. 그 외(USD 코인, 바이낸스 USD, 다이)

4) 유틸리티 코인

유틸리티 코인이랑 블록체인 기술의 가치를 증명하기 위해 특정 플랫폼에서 발행한 코인이다. 따라서 해당 플랫폼에서 진행 중인 탈중앙화 앱 디앱(Dapp)에서 화폐의 대용으로 사용할 수 있는 것이 특징이다. 유틸리티 코인부터는 플랫폼 코인이거나 증권형 코인 등이 해당한다. (바이낸스코인, 스팀, 링크)

5) 프라이버시 코인

프라이버시 코인은 개인 정보를 중요시하는 익명성 기반의 코인이다. 최근 이슈가 되고 있는 '다크 코인'들이 이에 해당하며, 현재 세금 탈세나 불법 증여 등의 타겟이 되고 있다. (모네로, 제트캐쉬, 대쉬)

6) 디파이용 코인

디파이란 Decentralized Finance 즉 탈중앙화 금융이다. 코인이 디파이용으로 만들어졌다기보다는 탈중앙화 은행에 코인을 거치할 수 있다면 디파이용으로 불릴 수 있다. 한국에서는 카카오 코인 중 하나인 클레이스왑 이란 코인이다. (유니스왑, 체인링크, 랩 비트코인)

7) 증권형 코인

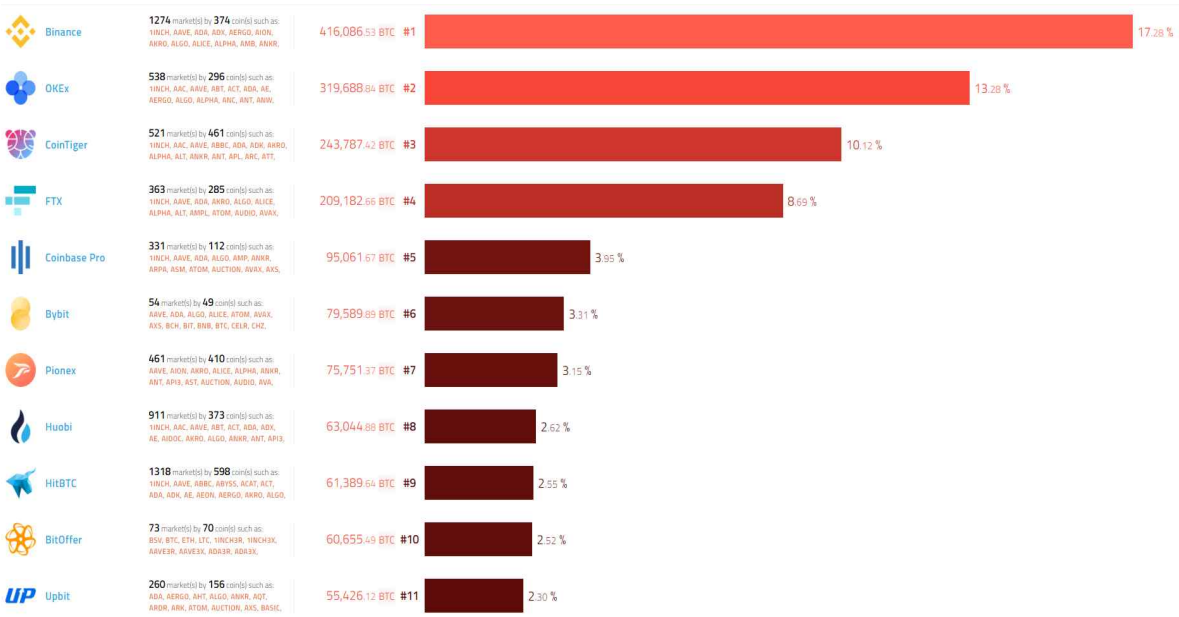
증권형 코인이란 주식, 채권, 부동산 등 실물 자산을 블록체인 기반의 코인에 고정한 것이다. 증권형 코인의 대표적인 것은 리플이다. 리플은 분류가 애매하긴 하지만 가상화

폐 세계에서 가장 이슈가 있었던 SEC 소송 건이 리플을 증권형 코인으로 보는 계기가 되었다. 소송은 아직도 현재 진행 중이다.

3. 가상화폐 거래의 시스템과 보안 및 대응 방안

3.1 가상화폐 거래소

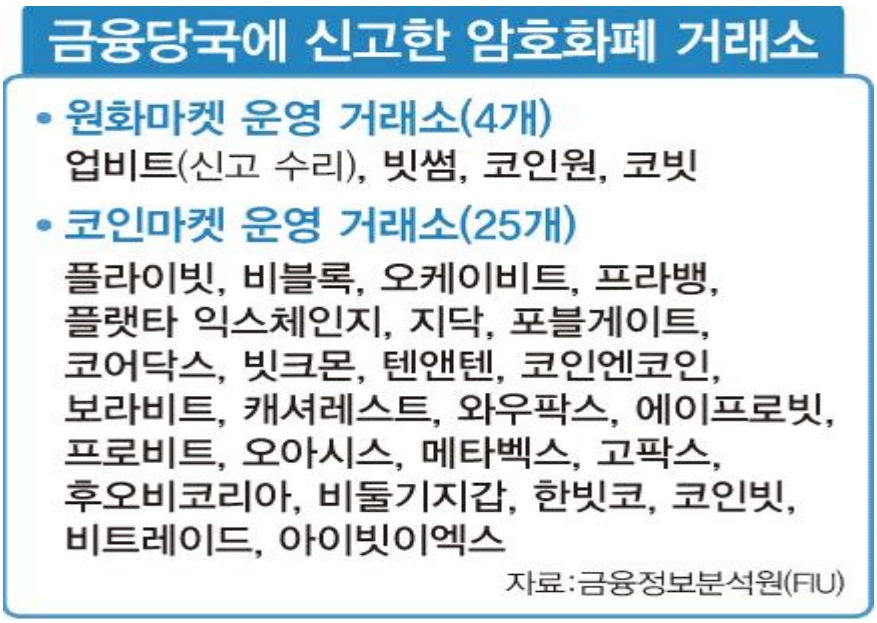
가상화폐 거래소는 암호화폐를 거래할 수 있는 시장을 말한다. 간단히 거래소라고 부른다. 암호자산거래 플랫폼이라고도 한다. 영어로는 익스체인지 대한민국 정부에서는 가상통화 취급 업소라는 용어를 사용한다. 중국에서는 교역소라고 한다. 암호화폐 거래소를 통해 비트코인, 이더리움 등의 암호화폐를 달러($), 유로(€), 파운드(£), 위안(¥), 엔(¥), 원(₩)화 등 실제 화폐로 교환할 수 있다. 암호화폐 거래소는 주식 거래소와 달리 개장 시간과 폐장 시간이 없이 1일 24시간, 1년 365일 항상 인터넷으로 암호화폐를 거래할 수 있다.



[사진 2] 전 세계 가상화폐 거래소 순위

저번 달인 9월에 특정금융정보법이 본격 시행된 가운데 가상자산 거래소들의 줄폐업이 현실화됐다. 4대 거래소(업비트·빗썸·코인원·코빗)를 제외한 정보보호 관리체계(ISMS) 인증 거래소들은 은행으로부터 실명계좌를 발급받지 못해 코인마켓만 신고했으며, ISMS 인증조차 받지 못한 거래소들은 폐업 수순을 밟게 됐다. 가상자산 거래업자는 ISMS 인증받은 거래소 29곳이 모두 신고접수를 완료했다. 기타 사업자의 경우 14개 사 가운데 13개 사가 신고접수를 마쳤다. 신고접수를 마친 거래소는 업비트, 빗썸, 코인원, 코빗, 플라이빗, 비블록, 오케이비트, 프라뱅, 플랫타이엑스, 지닥, 포블게이트, 코어닥스, 빗크몬, 텐앤텐, 코인엔코인, 보라비트, 캐셔레스트, 와우팍스익스체인지, 에이프로빗, 프로비트, 오아시스거래소, 메타벡스, 고팍스, 후오비코리아, 비둘기지갑, 한빗코, 코인빗, 비트레이드, 아이빗이엑스 등이다. 다만 은행으로부터 실명계좌를 발급받고 신고접수를 마친 곳은 업비트, 빗썸, 코인원, 코빗 네 곳에 불과하다. 업비트의 경우 지난 17일 신고 수리

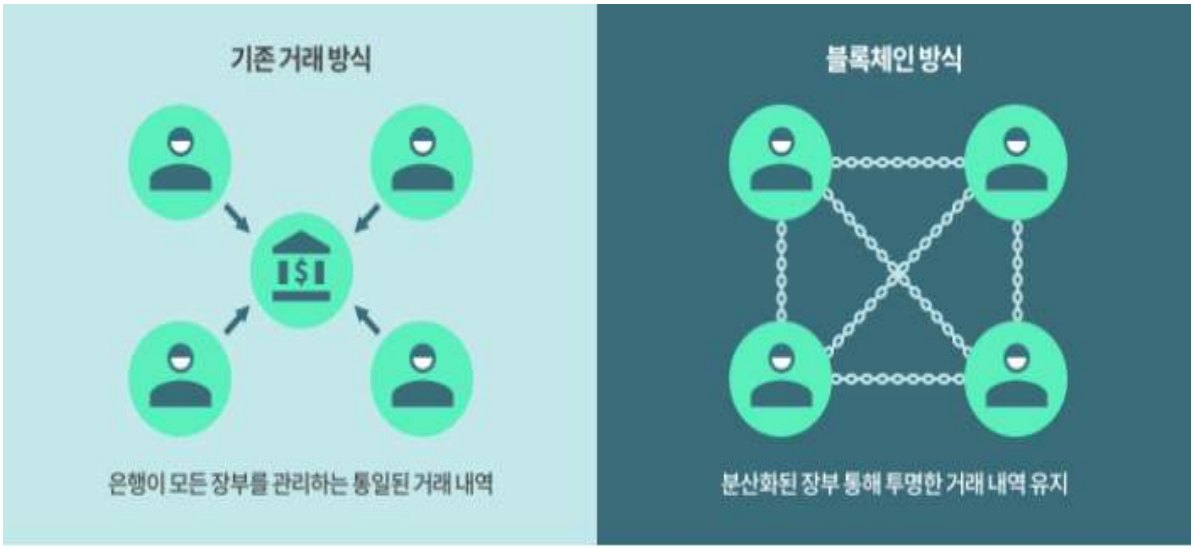
가 완료되면서 1호 정식 가상자산 거래소가 됐다. 나머지 거래소들은 실명 확인 계좌를 발급받지 못해 우선 코인마켓만 열겠다고 신청한 상태다.



[사진 3] 금융당국에 신고한 암호화폐 거래소

3.2 블록체인

블록체인은 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다. 이는 근본적으로 분산 데이터 저장 기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 블록체인 기술은 비트코인을 비롯한 대부분의 암호화폐 거래에 사용된다. 암호화폐의 거래 과정은 탈중앙화된 전자 장부에 쓰이기 때문에 블록체인 소프트웨어를 실행하는 많은 사용자의 각 컴퓨터에서 서버가 운영되어, 중앙에 존재하는 은행 없이 개인 간의 자유로운 거래가 가능하다.

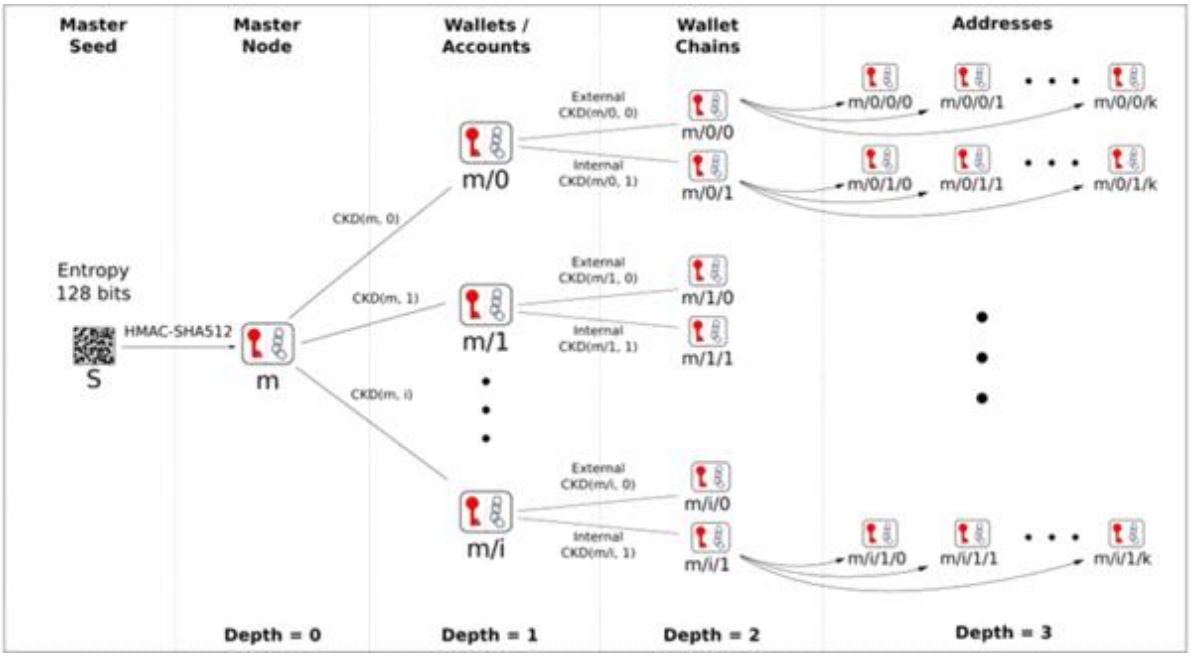


[사진 4] 기존거래와 블록체인의 차이점

3.3 암호화폐 지갑과 기술의 발전

일상에서 '지갑'은 화폐, 신용카드, 신분증 등을 넣고 휴대하는 물건이다. 그래서 '암호화폐 지갑'이라 하면 흔히 암호화폐를 보관하는 진짜 지갑 같은 물건을 떠올린다. 비트코인이나 이더리움 등 암호화폐가 지갑 안에 들어 있을 것 같다. 그러나 암호화폐 지갑 안에는 암호화폐가 없다. 암호화폐 지갑은 블록체인 분산원장에 기록되는 거래 트랜잭션 데이터를 생성하고 서명하는 일에 사용되는 비공개 키를 보관하고 관리하기 위한 도구일 뿐이다. 그럼 암호화폐는 어디에 있는 걸까? 참여자 모두가 공유하는 블록체인 안에 있다. 내 자산, 비트코인이라면 내 키와 연결된 주소의 UTXO 합, 이더리움이라면 내 키와 연결된 계좌의 잔고 등 내 자산은 블록체인에 들어 있다. 암호화폐 지갑이란 바로 그 키 관리하기 위한 도구다. 지갑에서 관리하는 개인 키를 잃어버리면 암호화폐가 사라지는 것이 아니라 내 자산의 소유권을 증명할 수 없게 된다. 그렇기 때문에 암호화폐 자산 관리에서 가장 중요한 일은 키 관리다. 인류 문명의 발전사는 결국 온갖 도구의 편리한 이용을 향한 연구개발의 역사 아닌가 싶다. 암호화폐 지갑도 날이 갈수록 점점 더 편리해졌는데, 그 변화는 암호화폐 지갑 기술에 대한 아주 중요한 의미를 담고 있으니 간략하게나마 살펴보자. 앞서 암호화폐 거래는 개인 키와 공개키 쌍에 대한 검증을 통해 증명된다 했다. 그렇다면 개인 키와 공개키 각각 1개씩만 갖고 있으면 거래를 막 해도 되는 걸까. 그렇진 않다. 거래 트랜잭션에는 거래자 명의와 주소 그리고 공개키 정보가 기록된다. 그리고 모든 트랜잭션은 누구나 간단히 조회할 수 있어서, 같은 키와 주소를 계속 사용하면 내 자산 규모나 거래 내역 등이 모두 다 노출된다. 이는 개인의 프라이버시 침해 문제라 이를 피하고 사용자 편의를 향상하는 방법이 지속해서 개선됐고, 그 변화가 암호화폐 지갑 기술의 발전사라 할 수 있다. 최초의 암호화폐 지갑은 주소와 키 재사용을 피하고자 기본 100개 이상의 개인 키를 무작위로 생성하고 코인별 그리고 용도별로 다른 개인 키와 공개키를 사용했다. 이로써 프라이버시 노출 문제는 피할 수 있었지만, 모든 거래에 대해 사용된 키를 저장하고 관리해야 하는 불편함이 컸다. 키를 무작위로 생성하기 때문에 이를 '랜덤 지갑(Random Wallets)'이라 한다. 아래 결정성 지갑과 대비해 '비결정성 지갑(Nondeterministic Wallets)'이라고도 부른다. 랜덤 지갑의 불편함을

해소하기 위해 개발된 것이 '결정성 지갑(Deterministic Wallets)'이다. 결정성 지갑은 다수의 난수표로부터 하나를 골라 난수를 생성하는 랜덤 시드 값을 이용하기 때문에 '시드 지갑(Seeded Wallets)'이라고도 부른다. 결정성 지갑은 날것의 무작위 키를 생성하지 않고 하나의 시드 값으로 순차적으로 키를 생성한다. 따라서 시드를 안전하게 보관하기만 하면 언제든 시드로부터 개인 키를 순차적으로 재생성할 수 있기 때문에 거래에 사용된 모든 키를 백업하고 관리하는 불편함 문제를 해소한 지갑이다. 하지만 완전히 편리해진 건 아니다. 암호화폐 종류는 다양하고 한 사용자가 여러 주소를 가질 수도 있는데 결정성 지갑만으로는 그 복잡다단한 환경 전체를 모두 다 관리할 수가 없다. 그래서 '계층 구조 결정성 지갑(Hierarchical Deterministic Wallets)' 개념이 제안되었다. 줄여서 'HD 지갑'이라고도 부르는 계층 구조 결정성 지갑은 마스터 시드로부터 개인 키를 계층적으로 생성하고 관리함으로써 하나의 지갑으로 여러 화폐 그리고 주소를 관리할 수 있게 되었다. HD 지갑 기술은 'BIP-0032'란 이름의 형식으로 사실상 표준화되었고, BIP-0032 이후 BIP-0043 그리고 BIP-0044 등을 통해 계층 구조를 보다 정교화하는 등 기술을 보강해 왔다.



[사진 5] BIP-0032 구조

4. 가상화폐 기술 및 보안 위협

가상화폐 기술 및 보안 위협은 생각보다 많고 다양하게 이뤄지고 있다. 실제로 화폐가 있는 게 아니다 보니 거래를 하는 이용자들도 안일하게 보안에 취약하게 행동을 한다. 무엇들이 위협을 하는지 알아보자.

4.1 가상화폐 거래소 시스템 위협

북한이 배후세력으로 추정되는 다양한 해킹그룹에 의한 사이버 위협이 위험수위에 달하고 있다는 지적이 이어지고 있다. 특히 코로나 19 방역을 위한 국경 봉쇄, 대북 제재

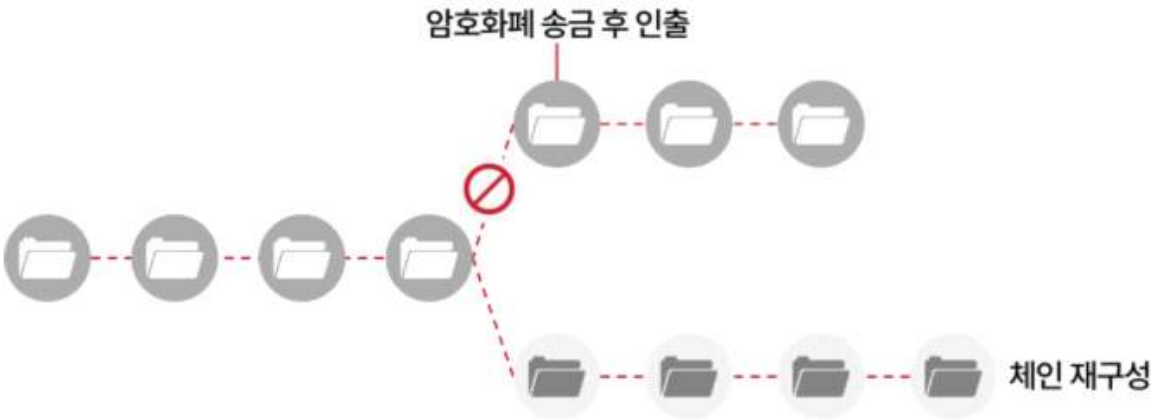
로 인한 밀수출 루트 차단 등으로 경제난에 허덕이는 북한 당국이 불법적으로 수익을 올릴 수 있는 사실상의 유일한 방법이 해킹 같은 사이버 공작뿐인 만큼 국내 금융기관이나 가상화폐거래소 등의 각별한 보안 대책이 요구되고 있는 실정이다. 10일 국내 사이버 안보 관계자 등에 따르면 국내에서 금전적 이득을 노리는 북한 배후 추정의 사이버 공작은 2010년대부터 본격화하기 시작했다. 초반에는 국내 업자들과 손잡고 악성코드가 설치된 사행성 불법도박프로그램을 유포하는 방식이었다. 지난 2014년 검찰은 불법 온라인 도박으로 돈을 벌려고 북한 해커와 손잡고 해킹 프로그램을 들여와 국내에 유포시킨 일당 세 명을 적발했다. 이들은 지난 2011년 4월 해킹 프로그램 제작자를 찾던 중 북한 정찰총국 산하로 추정되는 '조선백설무역회사 심양대표부' 소속 해커와 접촉해 1,400만 원을 주고 원격감시 프로그램을 사들인 것으로 전해졌다. 유동열 자유민주연구원장은 북한이 이런 방식으로 국내 업자에게 불법도박프로그램을 판매하고 수익을 분해해 약 1,000억 원대의 수익을 올린 것으로 추산했다. 이후 북한 배후 추정 해킹그룹의 사이버 공작은 더욱 대담해졌다. 직접적으로 국내 사이트를 해킹하거나 금융기관 해킹에 나선 것이다. 지난 2016년 5월 해킹 피해를 본 인터파크는 대규모 고객 정보 유출 피해를 봤다. 수사에 착수한 경찰과 정보 합동조사팀은 해킹에 사용된 IP와 악성코드가 북한이 과거 사이버테러에 동원한 것과 유사하다는 점 등을 바탕으로 '북한 정찰총국 소행'으로 판단했다. 당시 해킹 조직은 인터파크 측에 30억 원 상당의 비트코인을 요구한 것으로 알려졌다. 비트코인 같은 가상화폐가 대중화되고 그 가치가 상승하자 북한의 사이버 위협은 직접적으로 가상화폐를 노리기 시작했다. 피해가 외부로 알려진 사건만 2017년 이후 최소 8건에 달한다. 북한이 배후로 추정되는 해킹그룹은 2017년 4월 A 가상화폐거래소를 해킹해 21억 원 상당의 가상화폐를 탈취한 것으로 전해졌다. 또 같은 해 2월과 7월에는 B 가상화폐거래소를 해킹해 고객 관련 개인 정보 3만여 건을 유출하고, 700만 달러(약 84억 원) 상당의 가상화폐도 탈취한 것으로 알려졌다. 이후에도 가상화폐거래소는 북한 배후 추정 해킹그룹의 주된 먹잇감이 됐다. C 가상화폐거래소는 같은 해 4월과 7월 두 차례 해킹 피해를 보아 총 270억 원 상당의 가상화폐를 탈취당한 것으로 알려졌다. 2017년 두 차례 피해를 본 B 가상화폐거래소는 2018년과 2019년에도 한 차례씩 해킹 피해를 본 것으로 전해졌다. 이들 사건으로 2018년 6월에는 3,100만 달러(약 370억 원) 상당, 2019년 3월에는 2,000만 달러(약 240억 원) 상당의 가상화폐를 각각 탈취당한 것으로 파악되고 있다. 북한 배후 추정 해킹그룹은 2018년 6월 D 가상화폐거래소를 해킹해 500억 원 상당의 가상화폐를 탈취했으며, 2019년 11월에는 F 가상화폐거래소를 해킹해 580억 원 상당의 가상화폐를 탈취하는 등 점점 가상화폐 탈취 규모도 확대하고 있다. 그 밖에도 북한 배후 추정 해킹그룹은 은행권의 ATM을 해킹해 직접 현금을 탈취하거나 민간 기업에 랜섬웨어(탈취한 데이터에 대한 몸값을 요구하는 악성코드) 공격을 가해 대가를 요구하는 방식의 사이버 공격도 가하고 있는 것으로 알려졌다. 그러나 민간 분야에 대한 북한의 사이버 공격은 피해업체 측이 관련 기관에 신고하거나 조사를 요청하지 않으면 구체적으로 피해 규모를 파악하기 어려운 실정이다. 유 원장은 "북한의 과거 사이버 공격은 국가기관 사이트 해킹 같은 사회적 혼란을 초래하는 방식이었지만, 최근에는 대북 제재로 인한 경제난 때문에 금전적 이득을 노리는 사이버 공격을 가하고 있는 것으로 보인다"라고 지적했다.

4.2 블록체인 보안 위협 및 대응 방안

블록체인을 공격하는 것은 분산 데이터베이스에 대해 위변조하기 위해서이다. 일반적으로 데이터를 위변조하여 암호화폐를 탈취하거나 증식시키고, 블록체인을 이용한 인증 서비스에서는 신원을 위장할 수도 있다. 블록체인에는 어떤 종류의 위협이 있는지 알아보자.

4.2.1 51% 공격

51% 공격이란 탈중앙화에 기반한 많은 블록체인에서 일어날 수 있는 공통적인 보안 위협이다. 전체 네트워크의 지분, 해시파워 등의 자원을 51% 이상 독식하였을 경우 블록체인에 대한 조작된 체인 재구성을 일으키는 공격이다. 이는 비가역성과 무결성을 원칙으로 하는 블록체인에게 가장 큰 위협이다. 체인의 재구성은 암호화폐 거래소에서 입금 내역에 대한 블록을 입금하지 않은 상태로 재구성하여 입금 후 환전, 입금 내역 무효화 방식의 이중 지불을 통해 이득을 취할 수 있다.



[사진 6] 51% 공격을 통한 체인 재구성

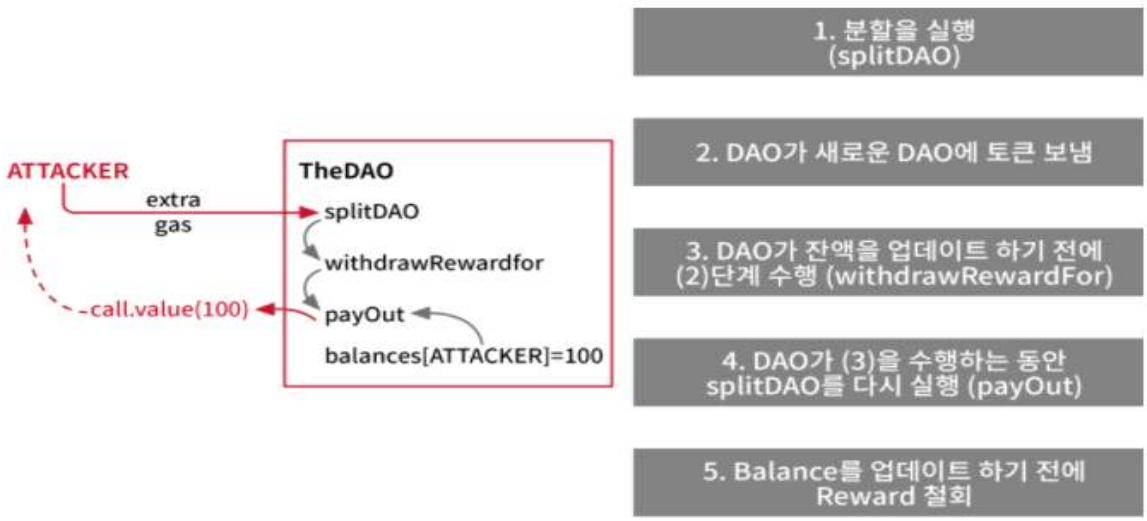
이러한 공격을 막기 위해 암호화폐 거래소들의 경우, 입금에 대한 컴펌수를 증가시켜 이중 지불 여부를 확인할 때까지 거래 확정을 늦추도록 조치한다. 이 방안은 컴펌을 기다리는 시간이 길어져서 기존 입금 소요 시간보다 더 긴 시간이 소요되지만, 51% 공격을 저비용 고효율로 막을 수 있는 좋은 대응 방안이다. 51% 공격은 블록체인의 근본적인 취약점이라 할 수 있지만, 탈중앙화를 제한하거나 자원 독식에 대한 리스크를 증가시키는 등의 방법으로 합의 알고리즘을 개선하여 대응할 수도 있다.

4.2.2 블록체인 코드 오류

블록체인은 하나의 소프트웨어 구현체이므로 소스 코드상의 오류가 존재할 수 있다. 대표적인 예시로 이더리움 DAO 공격과 취약점 CVE-2018-17144와 관련된 이중 지불 버그를 들 수 있다.

1) DAO 해킹

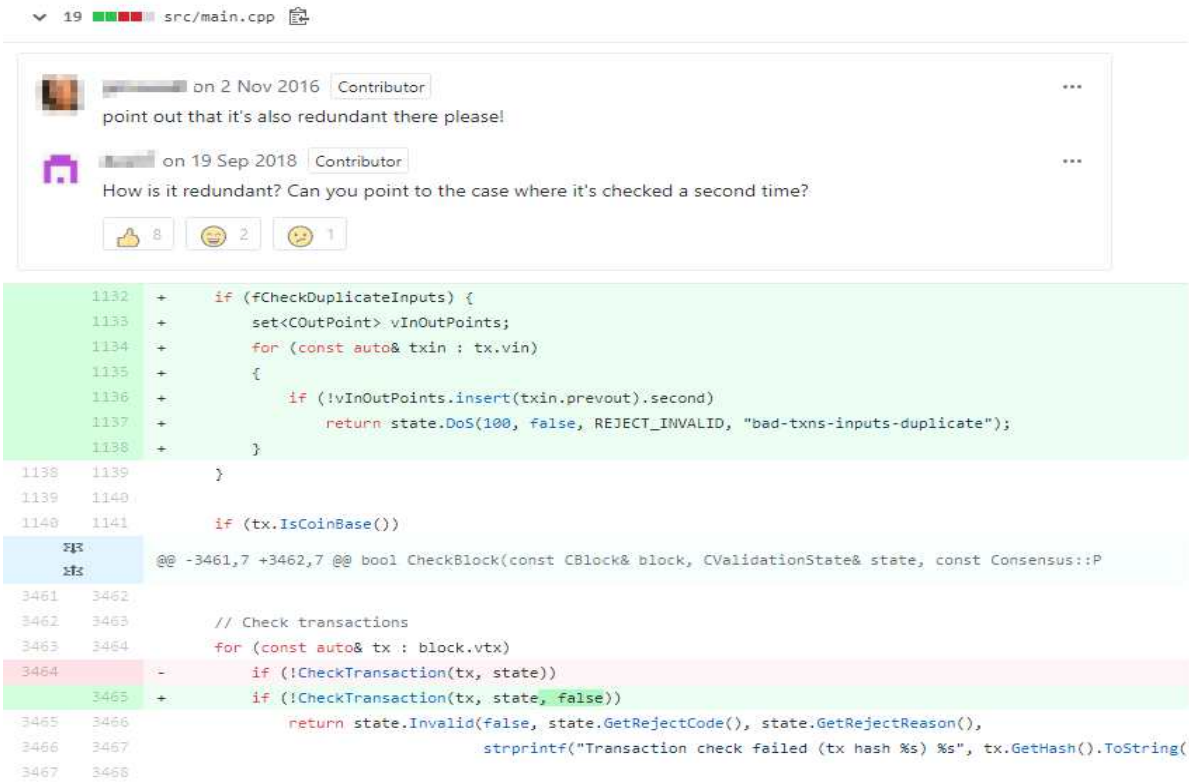
DAO는 2016년 5월에 등장한 이더리움을 이용한 스마트 컨트랙트 프로젝트이다. DAO는 코드로만 돌아가는 주인 없는 공동출자 회사로써 DAO 토큰 보유자들의 투표에 의하여 투자 계약이 성립되고 배당금을 분배받는다. 그런데 지난 2016년 6월, DAO는 프로그램상의 재귀호출 버그로 인해 투자금을 이더리움으로 반환하는 기능이 무한이 실행되었고, 243만 개에 달하는 이더리움을 탈취당하였다. 당시 이더리움은 하드포크를 통해 탈취된 이더리움을 복구시켰다. 블록체인 자체가 이 사건의 직접적인 원인이 되지는 않았지만, 블록체인을 기반으로 한 damp의 취약점이 블록체인 네트워크에 큰 영향을 미칠 수 있다는 것은 시사했다.



[사진 7] DAO를 이용한 재귀호출 공격 과정

2) CVE-2018-17144

CVE-2018-17144 취약점은 비트코인 코어 상의 버그로 이중지불을 발생시킬 수 있다. 비트코인 네트워크에 참여할 수 있는 비트코인 코어는 오픈소스 프로젝트로 많은 사람들의 참여가 가능하다. 오픈소스 프로젝트의 특성상 코드 반영이 신중히 결정되지 않으면 많은 버그가 발생할 수 있는데, 2016년 12월에 반영된 코드로 인해 단일블록에 대한 이중지불 체크를 불필요한 것으로 간주하였다. 그리고 약간의 속도 향상을 얻고자 이 기능을 제거하게 되었고, 동일한 입력(UTXO)을 두 번 사용한 트랜잭션이 포함된 블록을 생성할 수 있게 되었다.



[사진 8] 문제의 코드 반영 내역

해당 버그는 2018년 9월에 발견되어 뒤늦게 업데이트되었으나 공격을 시도하려면 높은 해시파워로 직접 블록을 생성해야 했다. 공격 대비 기회비용이 낮은 이유 때문인지 직접 공격을 시도한 블록은 다행히 체인에 존재하지 않았다.

3) 외부 시스템

블록체인은 분산 데이터베이스 시스템의 기능을 수행하며 많은 외부 시스템이 존재한다. 외부 시스템은 블록체인 네트워크상에서는 통제가 불가하며 의도하지 않은 많은 보안 취약점이 존재한다. 대표적인 외부 시스템으로 암호화폐 거래소가 존재한다. 암호화폐 거래소는 블록체인을 이용한 가장 기본적인 응용 기술인 암호화폐를 거래하는 시스템으로 마치 주식 거래처럼 암호화폐를 거래한다. 이러한 거래소의 경우 기본 자본이 항시 준비되어 있어야 하는데, 이것을 보관하는 곳이 핫 월렛과 콜드 월렛이다. 핫 월렛은 인터넷에 연결된 온라인 저장소이며, 콜드 월렛은 하드웨어적으로 완전히 분리된 오프라인 저장소이다. 핫 월렛의 경우 소유자임을 증명하는 개인 키를 알고 있다면 네트워크를 통해 접근이 가능하다. 자산을 핫 월렛에서 운용하게 되면 개인 키 유출 시 막대한 금전적 손실과 더불어 탈취된 암호화폐 블록체인 네트워크에 큰 영향을 미칠 수 있다. 그렇기 때문에 대부분의 자산은 오프라인 저장소인 콜드 월렛에 보관하고 다중 서명을 통해 인출 가능하도록 조치하여야 한다.

[사진 9] 안전한 자산 운용을 위한 가상화폐 안전장치 사례

4) 개인 키 탈취

블록체인에는 블록에 대한 무결성과 부인방지 등을 위해 전자서명과 같은 암호화 기술이 사용된다. 전자서명에 사용되는 공개키는 곧 자산의 식별 주소가 되고, 개인 키는 자산에 접근할 수 있는 열쇠가 된다. 그러므로 우리는 블록체인을 이용함에 있어서 가장 먼저 키에 대한 안전한 관리가 필요하다. 흔히 자신의 계정 정보를 탈취당하지 않도록 안전하게 보관하며 조심하듯이 블록체인에서도 키에 대한 관리적 보안이 최우선이 되어야 한다.

4.3 암호화폐 지갑 보안 위협

4.3.1 암호화폐 계정 키 보호가 관건

암호화폐 해킹사고의 대부분은 암호화폐 지갑 정보를 탈취해 발생한다. 암호화폐 지갑에는 암호화폐가 보관된 것이 아니라 계정에 접근할 수 있는 키가 보관돼 있다. 암호화폐 거래가 일어났을 때 이를 증명하기 위해 키로 트랜잭션을 만들고 서명한 후 브로드캐스트하면 거래 참여자들이 승인하고 블록이 공유되고 거래가 완료된다. 암호화폐는 익명성이 보장되기 때문에 키를 잃어버리거나 도난당했을 때 되찾을 방법이 없다. 트랜잭션이 투명하게 공개돼 있기 때문에 도난당한 암호화폐를 추적할 수는 있지만, 공격자들은 암호화폐를 탈취한 후 수백 개의 계좌로 분산시켜 여러 차례 거래를 반복하기 때문에 추적이 어렵다. 암호화폐 사용자 키는 무단으로 탈취하기 쉽다. 키는 복잡한 문자 조합으로 이뤄져 있으며, 대부분의 경우 단말이나 앱에 저장해두고 거래가 필요할 때 호출해서 사용할 수 있다. 사회공학적 기법을 이용하면 쉽게 키를 가져갈 수 있다. 보안에 투자하지 않은 거래소는 키를 직원의 단말이나 서버에 무방비로 보관하고 있었으며, 이를 도난당해 해킹 피해를 입었다.

4.3.2 키 분산저장으로 계정 보호

키를 안전하게 보호하는 가장 확실한 방법은 분산저장이다. 개인이 소지한 단말이나 앱, 거래소, 클라우드 혹은 제3의 저장소 등에 분산 저장한 후, 거래가 필요하면 각각의 키를 호출해 사용할 수 있다. 하나의 키를 도난당한다 해도 다른 2개의 키가 없으면 공

격자가 마음대로 거래를 할 수 없다. 이상준 지란지교시큐리티 연구소장은 “지갑 ID 하나에 쌍이 되는 개인 키가 여러 개 있으며, 이 키가 모두 조합돼야 트랜잭션이 완료되는 것으로 설계한다면 지금보다는 더 암호화폐 거래가가 이뤄질 수 있을 것이다. 서명을 하드닝하거나 서명 값을 분산 저장하거나 복수의 키를 합쳐서 새로운 키를 만들어야 거래가 되는 등의 아이디어를 생각할 수 있다”라며 “이렇게 되면 거래 과정이 복잡해지고 승인 시간이 오래 걸린다는 단점이 있지만, 자산을 탈취당할 우려는 줄어들 것”이라고 말했다. 분산저장도 완벽하다고 할 수 없다. 분할된 키가 같은 저장소에 있다면 키 하나만 사용하는 것과 다르지 않다. 키를 개인과 거래소가 분할 보관한다면 보다 안전하게 자산을 보호할 수 있으며, ‘멀티시그(Multisig)’가 그 대안으로 제안된다. 거래소와 개인 회원이 키를 분산 저장하고 각각의 키를 동시에 호출해 서명해야 트랜잭션이 발생하게 된다. 해커가 개인 회원 키를 탈취했다 해도 거래소에 보관된 키를 훔치지 못하면 암호화폐를 훔칠 수 없다. 거래소는 고객의 키를 안전하게 보호해야 할 의무가 생긴다.

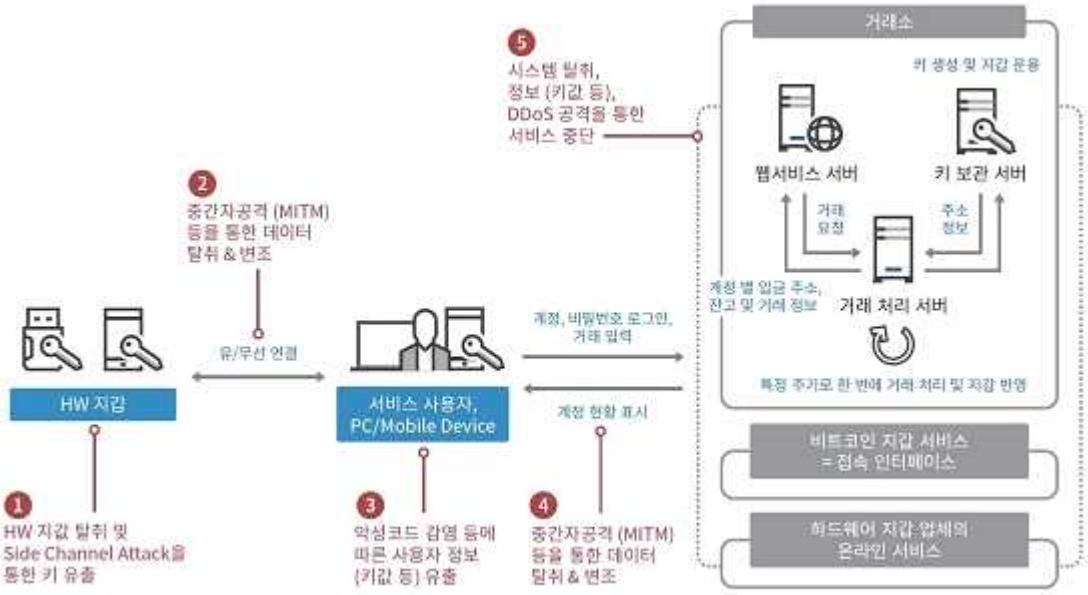
4.3.3 멀티시그로 암호화폐 지갑 보호

멀티시그를 암호화폐 지갑에 적용한 사례가 등장했다. 암호화폐 보안 지갑 ‘베리드 월렛(Berith Wallet)’은 사용자와 베리드가 키를 함께 보관하는 방식을 사용하고 있으며, 키는 사용자 계정 인증, 개인 키 인증, 결제전송 승인 비밀번호 등 삼중 인증으로 암호화폐를 보호한다. 김택균 베리드코리아 CTO는 “베리드 월렛은 고객의 키를 고객과 베리드가 나눠 갖는 방식으로, 고객이 보유한 키, 베리드의 키가 조합돼야 거래가 일어날 수 있도록 설계했다. 또한, 베리드 월렛에서 직접 거래를 할 수 있도록 설계해 거래소를 이용하지 않아도 자산을 관리할 수 있도록 했다. 사용자가 거래소에 종속되지 않아 선택의 폭이 넓어지게 된다”고 말했다. 베리드는 하나 멤버십, 신한판클럽, 시제이원, 엠포인트 등 금융·유통업계 대표적인 멤버십 시스템을 구축·관리하는 전문 기업인 아이비즈소프트웨어에서 런칭한 블록체인 전문 기업으로, 암호화폐 보안 지갑 ‘베리드 월렛’과 ‘베리드페이’, 블록체인 서비스(BaaS) 사업을 전개한다. 베리드월렛은 4월 정식 출시했으며, 베리드페이와 BaaS도 연내 공개할 계획이다. 베리드는 자체 코인을 발행해 이를 멤버십 포인트 혹은 가상통화 성격의 결제수단으로 사용할 수 있도록 한다. 소상공인, 중소 프랜차이즈 등을 가맹점으로 모집해 베리드 코인으로 포인트를 적립하고, 포인트는 가맹점 내에서 사용할 수 있도록 할 계획이다. 기존 암호화폐로도 거래할 수 있어 사용자 선택의 폭을 넓힐 수 있다.

4.3.4 암호화폐 금고로 개인 자산 보호

개인 사용자를 위한 암호화폐 지갑 중 가장 강력한 보안을 제공하는 솔루션은 ‘렛저’이다. 렛저는 ‘암호화폐 금고’라고 불리기도 하며, 해킹이 불가능한 전용 단말에 암호화폐 계정을 보관한다. 렛저는 각각의 단말에 복잡한 문자 조합으로 이뤄진 고유의 키를 부여하며, 해당 키를 이용해 렛저에 저장된 자신의 계좌에 접근할 수 있다. 이 키를 분실하면 계좌 접근 정보도 사라지기 때문에 키는 분실되지 않도록 잘 보관해야 한다. 거액의 암호화폐를 보관하는 사람은 은행의 금고에 보관하며, 렛저에서 키를 동판에 새겨 기념품으로 제공해주는 서비스도 제공한다. 렛저 국내 유통사인 SDF인터내셔널의 유승복 대표는 “렛저는 강력한 보안성을 제공하는 대신, 사용하기에 불편하다. 그러나 온라인에 있는 모든 자산은 해킹당할 수 있다는 사실을 감안하면, 다소의 불편함이 있다고

해도 자산을 안전하게 보호할 수 있는 방법을 택하는 것이 맞다"고 말했다. 유 대표는 이어 "렛저는 올해 사용 편의성을 보강해 스마트폰에서 사용할 수 있는 신제품과 거래소 및 채굴장에서 사용할 수 있는 엔터프라이즈용 제품을 출시하고 암호화폐 보안을 한 차원 강화할 것"이라고 덧붙였다.



[사진 10] 암호화폐 지갑 보호 방법

5. 결론

최근에 일부 국가에서 비트코인을 공식 화폐로 사용하고 있다. 현재 전 세계적으로 뜨거운 가상화폐와 블록체인에 대한 관심이 많다. 가상화폐와 블록체인 기술이 이제 누구나 다 알 수 있을 만큼 우리 주변에서 익숙해지고 있다. 이제 가상화폐가 자리를 잡아가면서 우리 생활 속으로 조금씩 다가오고 있고, 보안사고로 인해서 가상화폐에 대한 관심과 열기가 식지 않기를 바라면서 가상화폐 보안 대책을 통해서 조금 더 안전하고 신뢰할 수 있는 가상화폐 서비스 환경이 구축되고 블록체인 기반의 다양한 서비스가 활성화되기를 바라고 있다.

참고문헌

1) 김덕권, “가상화폐란 무엇인가?”, 2018.01.15.,
http://www.seniorsinmun.com/news/articleView.html?idxno=17615
2) 김문선, ‘312만 명’ 돌파한 가상화폐 앱 사용자 수 상승세 지속, 2021.03.25.,
https://platum.kr/archives/160058
3) 글 쓰는 핀테크, “블록체인 개념 완벽 정리”, 2019.03.20.,
https://www.banksalad.com/
4) 루레렁, “가상화폐 종류 한눈에 정리하기!”, 2021.06.19., https://lulluryu.tistory.com/
5) 김국배 기자, “코인 거래소 대표는 고객에 사과 편지, 시민단체는 금융위 비판”,
2021.09.26.,
https://www.edaily.co.kr/news/read?newsId=01735126629184056&mediaCodeNo=257
6) 펜타시큐리티, “안전한 암호화폐 지갑이란?” (feat. 비트베리 해킹), 2020.07.20.,
http://www.coindeskkorea.com/news/articleView.html?idxno=71258
7) 허민 기자, “北 해킹 먹잇감 된 가상화폐거래소…6곳서 최소 2000억 원 탈취”,
2021.08.10.,
http://www.munhwa.com/news/view.html?no=2021081001030442000001
8) 인포섹, “블록체인에서 발생 가능한 보안 위협”, 2019.11.19.,
https://blog.naver.com/skinfosec2000/221708719671
9) 김선애 기자, “지란지교시큐리티, 암호화폐 콜드월렛 ‘디센트’ 출시 예정”,
2018.05.29.,
http://www.datanet.co.kr/news/articleView.html?idxno=123154