가상 화폐의 보안 위협

지도교수 : 이 호
연 구 자 : 강윤지

< 목 차 >

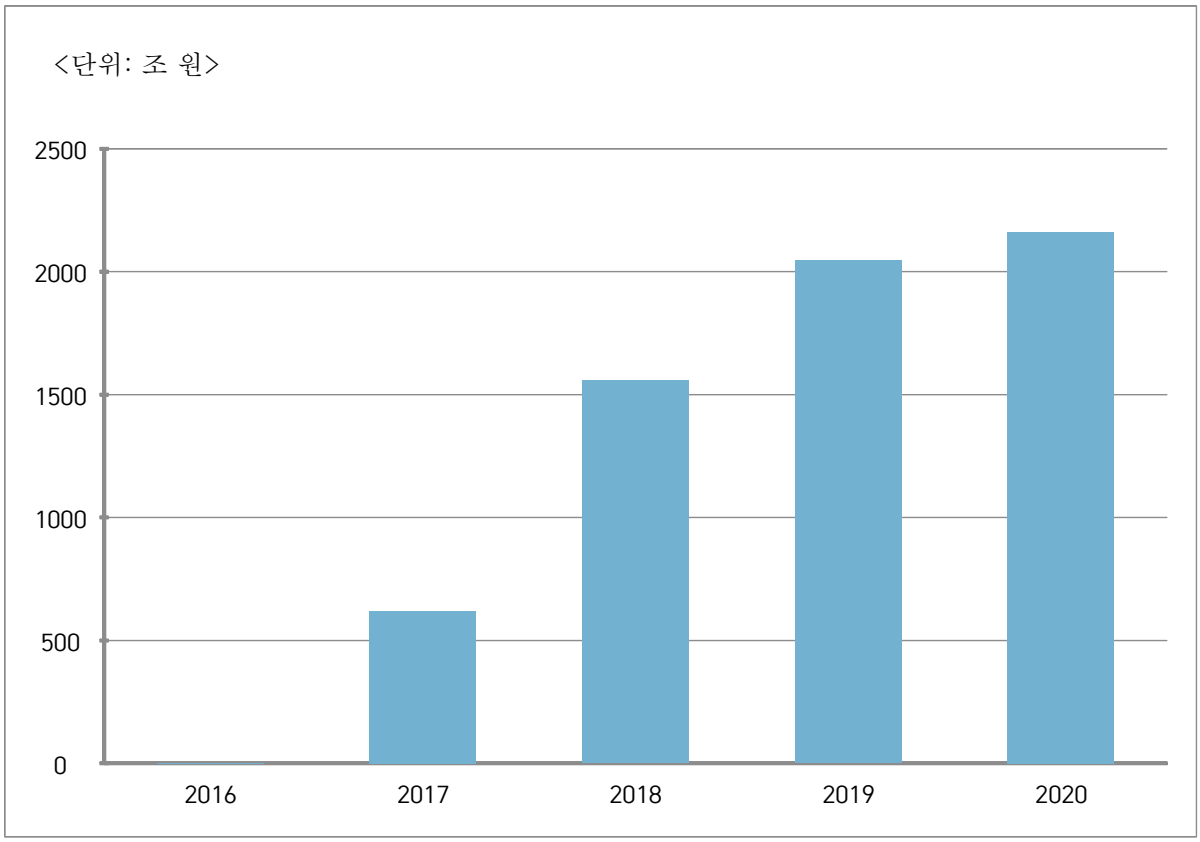
요 약

기술이 발전함에 따라 블록체인 기술을 기반으로 한 가상 자산에 대한 관심이 커지고 있다. 가상 자산인 가상 화폐가 미래의 화폐로서 통용될 것이라는 추측이 이어지고 있다. 이에 가상 화폐가 새로운 투자처로 각광 받고 있다. 금전이 오고 가는 거래라는 이유로 가상 화폐를 향한 공격도 날이 갈수록 많아지고 있는 가운데, 가상 화폐에 대한 보안 문제가 없는 것인지 알아보고자 한다.

주요어 : 가상 화폐, 블록 체인, 비트코인

1. 서론

고대에 필요한 물건을 교환하기 시작하면서 화폐의 역사는 기술이 발전함에 따라 실존하는 화폐가 아닌 가상의 화폐를 사용하는 현재로 이어진다. 가상 화폐는 2009년 블록체인 기술을 기반으로 한 가상 화폐가 등장한 이후 유명세가 커지고 있다. 가상 화폐라는 개념이 생소할 수 있다.



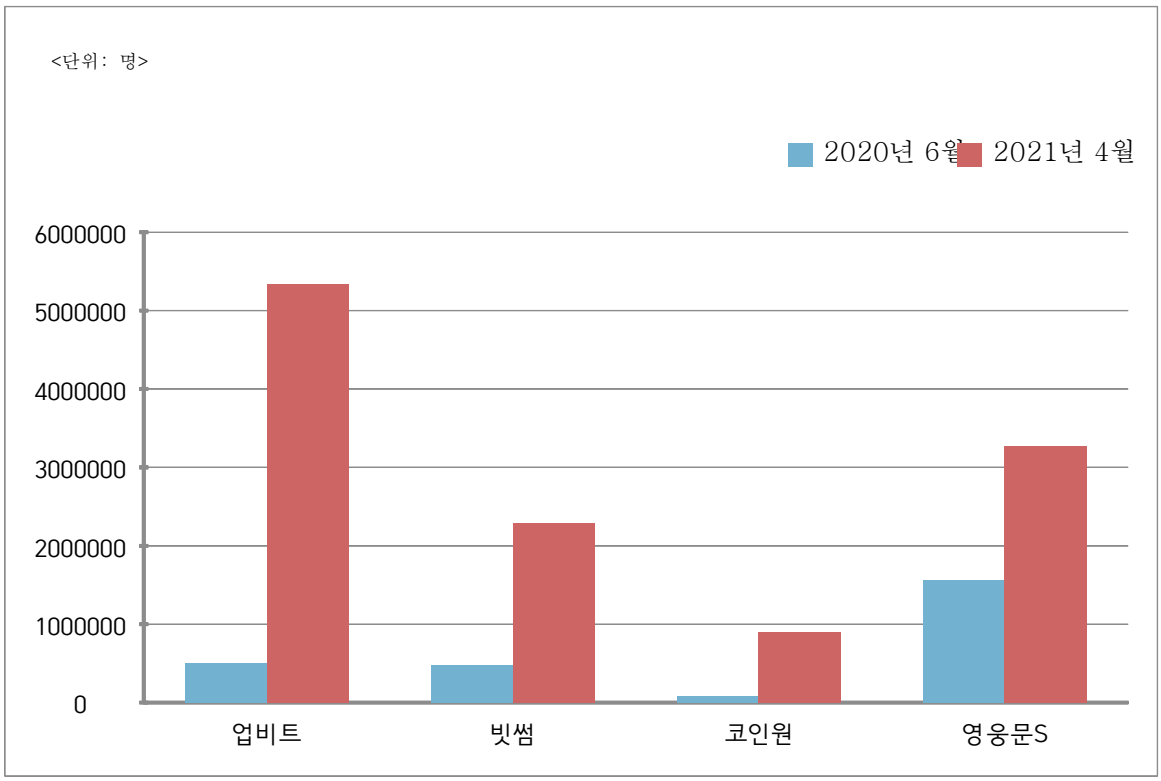
[사진 1] 가상 화폐 누적 거래 금액 (※2020년은 5월 말 기준)

2015년 이후부터 가상 화폐 거래소에서 거래되는 가상 화폐의 양이 매년 늘고 있다. 화폐와 기술의 발전으로 멀지 않은 미래에는 신용 화폐나 실물 화폐 대신 가상 화폐를 주로 이용하고 있는 모습을 볼 수 있을 것이라 예측하므로 가상 화폐에 관심을 가지고 익숙해질 필요가 있다.

화폐의 가치는 화폐의 양에 따라 변경된다. 화폐 위조가 쉬워지면 화폐의 양이 늘어 화폐의 가치는 떨어진다. 본 논문은 가상 화폐의 개념과 블록체인 기술을 소개하고 실물 화폐에 비해 위조의 가능성이 현저히 낮은 가상 화폐가 기존의 실물 화폐에서는 볼 수 없었던 보안 위험으로부터 안전할 수 있을 것인지 의문을 제기하고자 한다.

1.1 가상 화폐란?

가상 화폐는 실제 시장에서 사용되는 실물 화폐가 아니라 가상공간에서만 사용할 수 있는 화폐이다. 전자 상거래 업체나 온라인 콘텐츠 제공 업체가 이용자에게 마일리지 형태로 제공하기도 한다. 대표적인 예로는 '비트코인(Bitcoin)'이 있다. 비트코인은 2009년 '사토시 나카모토'라 소개한 익명의 개인 또는 다수의 개발자를 통해 알려지게 되었다. 기존의 가상 화폐들과는 달리 암호화 기술과 해시를 이용한 POW(작업증명) 방식을 이용하였다는 점에서 암호 화폐로 불리고 있다. 또한, 분산 네트워크 형 가상 화폐로 중앙 집중형 금융 시스템의 대안으로 주목 받고 있다. 가상 화폐는 주로 가상 화폐 거래소에서 거래된다. 가상 화폐에 대한 수요가 늘며 가상 화폐 거래소의 이용자 수도 증가하고 있다.



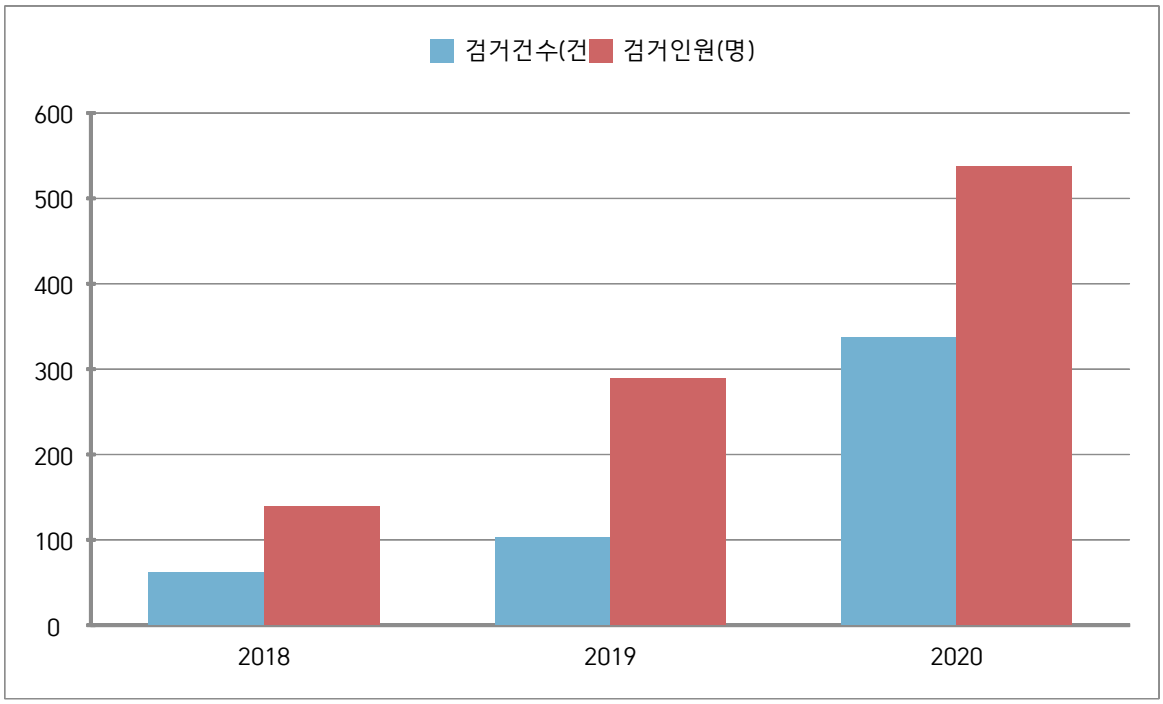
[사진 2] 가상 화폐 거래소 사용자

가상 화폐의 모든 거래 내역은 10분 단위로 기록된다. 거래 내역은 모두 암호화되어 있기 때문에 이 암호를 풀어 해독하여 기록하는 것을 작업 증명이라 한다. 이 암호를 해독하면 대가로 얻을 수 있는 것이 1개의 비트코인인 것이며 이 과정을 '비트코인을 채굴한다.'고 한다. 비트코인 채굴은 많은 연산을 하고 빠른 연산 능력을 요구하므로 개인이 채굴하는 것보다 전문 채굴업자가 유리한 구조이다. 비트코인 채굴 원리는 블록체인을 기반으로 하므로 비트코인을 위조하기 위해서는 블록의 해시 값을 통해서 연결되어 있는 모든 블록의 정보를 변경해야 한다. 10분 이내에 비트코인의 암호를 해독하고 이를 전파해야 하므로 위조와 변조가 불가능하다.

2. 가상 화폐의 보안

2.1 가상 화폐의 보안에 대하여

2017년 비트코인의 가격이 급증하며 가상 화폐에 대한 관심도 함께 늘었다. 가상에만 존재하는 화폐이지만 실물 화폐로 거래가 가능하여 화폐로서의 가치를 하는 가상 화폐는 다양한 연령대의 관심사가 되며 범죄자들의 표적이 되었다.



[사진 3] 최근 3년간 가상 자산 관련 경제 범죄 검거

2021년 4월 27일 경찰청 국가수사본부에 따르면 국가수사본부 경제범죄수사과가 담당하는 가상 자산 범죄로 지난해 337건이 경찰에 검거된 것으로 나타났다. 이는 2019년 103건보다 약 3.3배, 2018년 62건보다 약 5.4배 증가한 것이다. 검거 인원도 함께 증가하였다. 이는 가상 화폐의 보안은 어떻게 되고 있는 것인지 생각해 보는 계기가 된다.

2.1.1 블록체인(Block Chain)

대표적 가상 화폐인 비트코인의 배경인 블록체인이란 P2P(Peer to Peer, 개인 대 개인) 네트워크를 통해서 관리되는 분산 데이터베이스의 한 형태로, 거래 정보를 담은 장부를 중앙 서버 한 곳에서 저장하는 것이 아니라 블록체인 네트워크에 연결된 여러 컴퓨터에 저장 및 보관하는 기술로 다양한 분야에 활용이 가능한 기술이다. 분산원장 기술(DLT: Distributed Ledger Technology)이라고도 불리며, 이는 거래 정보를 기록한 원장 데이터를 중앙 서버가 아닌 참가자들이 공동으로 기록 및 관리하는 것을 의미한다. 블록체인은 분산 처리와 암호화 기술을 동시에 적용하여 높은 보안성을 확보하고 거래 과정의 신속성과 투명성을 특징으로 한다.

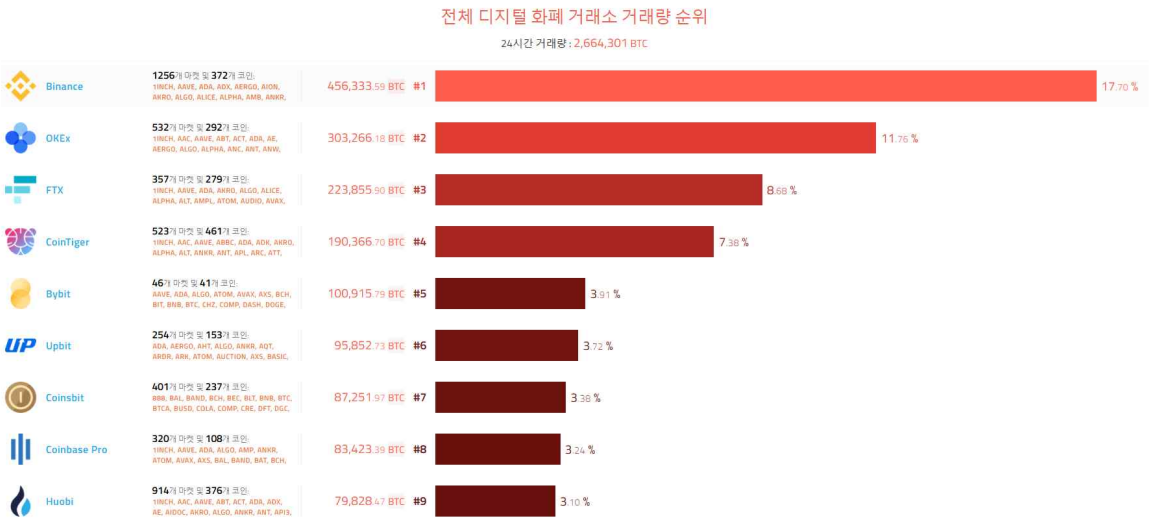
블록체인 기술은 P2P 거래를 지향하는 탈중앙화를 핵심 개념으로 하는 기술이다. 송금을 원하는 자가 거래 요청을 하면 해당 거래 정보가 담긴 블록이 생성되고 이 블록이 네트워크상의 모든 참여자에게 전송된다. 참여자들은 거래 정보의 유효성을 상호 검증하며 참여자 과반수의 데이터와 일치하는 거래 내역은 정상 장부로 확인하는 방식으로 검증을 진행한다. 검증이 완료되면 블록은 이전 블록에 연결되고, 그 사본이 만들어져 각 사용자의 컴퓨터에 분산 저장되며 블록체인 거래 과정이 끝이 난다. 이렇게 거래할 때마다 거래 정보가 담긴 블록이 생성되어 계속 연결되며 모든 참여자의 컴퓨터에 분한 저장되는데, 이를 해킹하여 임의로 수정하거나 위조 또는 변조하려면 전체 참여자의 과반수, 즉 약 51% 이상의 거래 정보를 동시에 수정해야 하므로 위조와 변조는 불가능하다. 블록체인은 크게 3종류로 나눌 수 있으며 각 블록체인마다 특징이 있다.

구분	Public Blockchain	Consortium Blockchain	Private Blockchain
관리자	모든 거래 참여자	컨소시엄에 소속된 참여자	한 중앙 기관이 모든 권한 보유
거버넌스	한 번 정해진 법칙을 바꾸기 매우 어려움	컨소시엄 참여자들의 합의에 따라 법칙을 바꿀 수 있음	중앙 기관의 의사 결정에 따라 용이하게 법칙을 바꿀 수 있음
거래 속도	네트워크 확장이 어렵고 속도가 느림	네트워크 확장이 쉽고 거래 속도가 빠름	네트워크 확장이 매우 쉽고 거래 속도가 빠름
데이터 접근	누구나 접근 가능	허가 받은 사용자만 접근 가능	허가 받은 사용자만 접근 가능
식별성	익명성	식별 가능	식별 가능

[표 1] 블록 체인 종류와 특징

2.1.2 가상 화폐 거래소

가상 화폐 거래소는 가상 화폐를 화폐로 거래할 수 있는 곳이다. 가상 화폐는 새로운 화폐로 세계적으로 각광 받고 있다. 가상 화폐 거래소 이용자는 가상 화폐를 손쉽게 화폐로 거래할 수 있는 가상 화폐 거래소를 애용하고 있다. 그만큼 가상 화폐 거래소의 수도 많다.



[사진 4] 전세계 가상 화폐 거래소 거래량 순위

국내 가상 화폐 거래소는 100여 개가 넘는다. 그중 '빗썸', '업비트', '코인원', '코빗'은 4대 거래소라 불린다. 빗썸은 전세계 가상 화폐 거래소 거래량 순위에서 33위를 달리고 있다.

가상 화폐의 보안을 위해 정부는 가상 화폐 거래소에 2021년 9월 25일부터 정보보호관리체계(ISMS) 인증을 필수로 지정하였다. ISMS는 특정 조직에 적합한 정보 보호 정책을 짜고, 위험에 상시 대응하는 등 여러 보안 대책을 유기적으로 통합해 관리하는 것이 목적이다. 기술적 · 물리적 보호 조치를 포함한 종합 관리 체계가 방송통신위원회가 고시한 기준에 적합한지 한국인터넷진흥원(KISA)이 인증해 준다. ISMS 인증 외에도 실명 계좌를 확보해야 거래소가 현금으로 가상 화폐를 사고 팔 수 있다. 실명 계좌를 확보하지 못하면 비트코인 등 가상 화폐로 다른 가상 화폐를 교환하는 '코인 마켓'만 가능하다.

국내 가상 화폐 거래소 원화마켓 현황 (2021년 9월 23일 기준)	
원화마켓 운영(4곳)	업비트, 빗썸, 코인원, 코빗
원화마켓 중단(25곳)	고팍스, 메타벡스, 보라비트, 비둘기지갑, 비블록, 비트레이드, 빗크몬, 아이빗이엑스, 에이프로빗, 오아시스, 오케이비트, 와우팍스, 지닥, 캐셔레스트, 코어닥스, 코인빗, 코인엔코인, 텐앤텐, 포블게이트, 프라뱅, 프로비트, 플라이빗, 플랫타익스체인지, 한빗코, 후오비코리아

[표 2] ISMS 인증과 실명 계좌 발급을 받은 국내 가상 화폐 거래소

2021년 9월 23일까지 실명 계좌를 발급 받은 거래소는 업비트, 빗썸, 코빗 등 4곳, ISMS 인증을 받은 거래소는 실명 계좌를 발급 받은 4곳을 포함해 총 29곳이다.

2.1.3 암호 화폐 지갑

암호 화폐 지갑은 분산 원장을 위해 디지털 서명하는 데 사용되는 비밀 키와 개인 키들의 집합이자 소프트웨어이다. 비밀 키는 디지털 자산의 소유권을 증명하고 자산을 양도하거나 변경하는 거래를 실행하는 유일한 수단이므로 암호 화폐 분야에서 핵심적인 요소이다. 암호 화폐 지갑이 없으면 가상 자산의 소유권을 입증할 방법도 없다. 거래에 사용되는 암호화 키를 추적할 뿐만 아니라 특정 자산이 위치하는 블록체인의 주소도 저장한다. 리눅스 재단의 하이퍼레저 프로젝트에서 보안 전문가로 활동하는 데이비드 휴즈비에 따르면 소유자는 이 주소를 분실할 시 자신의 가상 화폐에 대한 통제력을 잃게 된다고 경고했다. 암호 화폐 지갑은 크게 하드웨어 지갑과 소프트웨어 지갑 두 가지 유형으로 나눈다. 각각 콜드 스토리지 지갑, 핫 스토리지 지갑이라고 한다.

소프트웨어 지갑은 온라인 지갑을 제공하는 세계적인 가상 화폐 거래소인 “코인베이스(Coinbase)”와 같은 인터넷 서비스를 통해 액세스할 수 있으며, 사용자의 컴퓨터 또는 모바일 디바이스에서 관리되는 클라이언트 측 지갑과 온라인 지갑으로 세분화할 수 있다. 인쇄하거나 QR 코드로 렌더링할 수 있는 키를 생성하는 종이 지갑 생성기도 존재한다.

하드웨어 지갑은 USB 드라이브 또는 스마트폰과 같은 하드웨어에 오프라인 상태로 존재한다. 이는 소프트웨어가 이미 설치된 상태의 디바이스 형태로도 구할 수 있다. 하드웨어 지갑은 인터넷에 연결되지 않는다는 면에서 소프트웨어 지갑보다 더 안전하다.

2.2 가상 화폐의 보안 위협

가상 화폐는 실물 화폐와 달리 도난과 파손, 위조의 위험에서 자유롭다. 실물 화폐를 사용하며 발생하는 불편함이 사라질 것이라는 기대감에 가상 화폐는 각광 받고 있다. 하지만 가상 화폐가 디지털 정보로 이루어진 디지털 화폐인 만큼 해킹 등 정보 보안 문제에 대한 우려의 목소리도 큰 상황이다. 가상 화폐의 보안에는 어떠한 문제점이 있을지 알아보자.

2.2.1 블록체인의 보안 위협

호주의 첫 공공 블록체인인 Hcash(H캐시) 아담 게리 부사장과 앤드류 와슬비치 매니저는 IT조선이 5일 서울 여의도 전경련회관 그랜드볼룸에서 개최한 '블록체인·암호 화폐 콘퍼런스 2017' 강연에서 '암호 화폐 성공 사례 및 블록체인의 미래'를 주제로 "슈퍼컴퓨터를 능가하는 양자 컴퓨터의 등장으로 블록체인 시스템이 무너질 수 있다. 블록체인 설계 초기부터 양자 컴퓨터의 공격에 버틸 수 있는 최상의 보안 체계가 필요하다."고 발표했다. 앤드류 와슬비치 비즈니스 디벨롭먼트 매니저는 향후 양자 컴퓨터가 상용화되면 블록체인 시스템 보안이 위험해질 수 있다고 경고했다. 양자 컴퓨터는 양자 역학의 원리에 따라 작동되는 미래형 첨단 컴퓨터다. 앤드류 매니저는 "양자 컴퓨터는 슈퍼컴퓨터와는 비교할 수 없는 양산 능력을 가지고 있어 한 명의 해커만으로 블록체인 시스템이 무너질 수 있다"고 말했다. 외에도 블록체인의 보안 위협은 블록체인에 대한 신뢰도와 함께 증가하고 있다.

분류	보안 위협	설명
키 관리	도난 및 분실	키를 도난당하거나 분실된 키 악용될 경우 가상 자산 위험
	취약한 키	취약한 키 생성 알고리즘으로 키 재생성 공격이 가능할 경우 가상 자산 도난 위험
거래 검증 및 합의	합의 가로채기	참여자 중 과반수 또는 운영체제를 장악하여 블록 체인 합의 과정 조작
	사이드 체인 내 비정상 거래 발생	메인 체인에서 유효하지 않은 자산이 사이드 체인에서 거래 가능
참여자 권한 관리	개인정보 침해	개인정보에 대한 참여자의 접근 권한 관리 부족 시 개인정보 침해 가능
블록 체인 S/W 보안	블록 체인 S/W 취약점	블록 체인 S/W에 보안 취약점이 존재할 경우 키 도난, 합의 조작, DDoS 공격 등에 악용 가능
서비스 보안	비정상 거래 탐지 불가	비정상 거래에 대한 탐지 및 차단 기술이 부족하여 사기 거래, 자금 세탁, 이중지불 등의 거래 발생 가능

[표 3] 블록 체인의 보안 위협

2.2.2 가상 화폐 거래소의 보안 위협

가상 화폐 거래소는 비트코인의 치솟는 인기에 비례하여 수많은 공격자들의 공격을 받았다. 가상 화폐 거래소는 가상 화폐 자체가 아닌 사이트이기 때문에 해킹, DDoS, 악성 코드, 무한 환불 공격 등의 공격을 빈번하게 받고 있다. 거래소를 통해 가상 화폐의 현금화가 쉬워져 해커들은 가상 화폐 거래소를 주요 공격 대상으로 삼고 있다. 또한, 가상 화폐 거래소에서 거래되는 가상 화폐 거래 내역은 블록체인에 기록되지 않고 거래소 내부의 거래로 취급되기 때문에 내부자가 시세를 조작해 차액을 남기거나 외부로 유출되는 사례가 발생하고 있다.

2.2.3 암호 화폐 지갑의 보안 위협

가상 화폐 거래에 주로 사용하는 암호 화폐 지갑은 '핫 월렛(Hot Wallet)'이라 불리는 소프트웨어 지갑이다. USB 등으로 이루어진 오프라인에서 이용 가능한 '콜드 월렛(Cold Wallet)'이라 불리는 하드웨어 지갑과 달리 핫 월렛은 입출금 및 송금이 바로 가능해 매우 편리하지만, 해킹의 위협으로부터 자유롭지 못하다. 핫 월렛 속에 보관되고 있는 가상 화폐 자체를 해킹하는 것은 어려울지라도 이용자가 사용하는 공개 키와 개인 키를 해킹하는 것은 어려운 일이 아니기 때문이다. 가상 화폐는 위조나 복제 등의 위협에서는 비교적 안전하지만 그를 보관하는 지갑 자체를 도난당하면 자산을 잃는 것이나 다름없다.

3. 보안 위협 사례

3.1 블록체인 해킹 사례

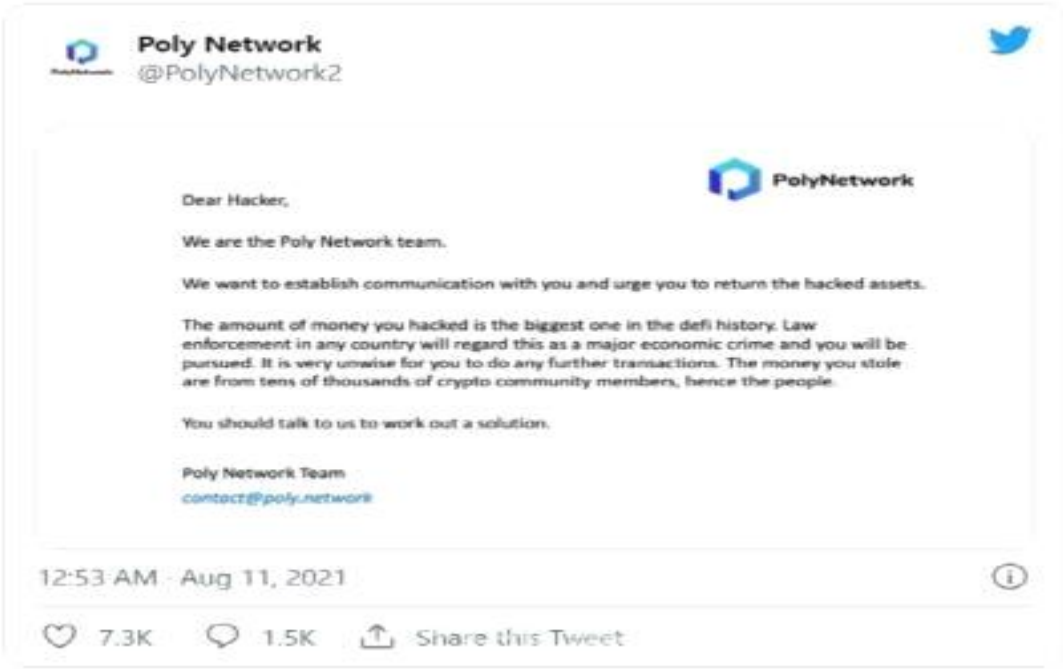
블록체인 해킹 공격의 유형은 다양하다. 블록체인의 해킹 사례를 보며 블록체인의 보안 문제점을 알아보자.

유형	구분	위협
블록 체인 인프라 공격	DDoS 공격	스팸 거래 생성 네트워크 부하 발생
블록 체인 코드 공격	스마트 컨트랙트 취약점	코드 버그로 인한 거래 오류
블록 체인 노드 공격	합의 가로채기	51% 공격을 통한 유효성 검사 조작

[표 4] 블록체인 해킹 공격 유형 별 정리

⑴ 폴리네트워크 해킹 사건

폴리네트워크(Poly Network)는 탈중앙화 금융 네트워크를 표방하는 중국 기업이다. 2021년 8월 해커들은 폴리네트워크를 공격해 사상 최대 규모의 암호 화폐 해킹을 단행했다. 이들은 폴리네트워크에서 6억 달러(한화 약 6950억 원)을 훔쳤다. 폴리네트워크는 이날 SNS를 통해 해킹 사실을 공개하며 해커들에게 가상 화폐 반환을 촉구했다.



[사진 5] 폴리네트워크의 SNS

해커들은 후에 자산을 반환하며 블록체인을 통해 입장을 발표했다. 그들은 폴리네트워크가 보안 결함이 있음에도 이를 감출 것을 우려해 해킹을 한 것이라 밝혔다. “돈에는 관심이 없기 때문에 반환하기로 결정했다.”며 폴리네트워크 보안의 허점을 지적했다.

⑵ DAO(Decentralized Autonomous Organization, 탈중앙화된 자율 조직) 해킹

DAO는 2016년 ICO를 통해 생겨난 이더리움 스마트 컨트랙트 프로젝트이다. 코드만으로 돌아가는 무형의 조직으로 주인 없는 공동 출자 회사였다. 실제 주소, 경영진이 없고 업무가 코드로 수행되어 누구나 깃허브(Github)에서 코드를 통해 업무 진행 내용을 볼 수 있다. DAO는 DAO 토큰으로 경영하고 토큰 보유자들이 보유한 토큰에 따라 투표권을 행사하고, 배당금을 분배하며, 계약자의 제안서가 20% 이상 표를 받으면 해당 프로젝트가 승인되는 구조이다.

2016년 6월 17일, DAO는 재귀 호출 버그(Rexursive Call Vulnerability)를 이용한 해커의 무한 환불 공격에 한화 510억 원을 해킹당했다.

[사진 6] DAO 무한 환불 공격

간단하게 DAO 토큰을 환불받고도 DAO 토큰이 남아 있어 무한정으로 인출할 수 있는 것이다. DAO 프로젝트의 책임 개발자는 소프트 포크(Sofr Fork)와 하드 포크(Hard Fork)로 크게 두 가지 해결책을 제시했다. 소프트 포크를 이용한 방법은 DAO와 해당 공격자의 DAO 지갑 사용을 정지하는 형태이다. 하드 포크는 DAO 토큰 보유자들이 이더리움을 돌려받도록 하는 형태이다. 결과적으로 이더리움 재단이 관계자들과 협의하여 소프트 포크를 이용한 방법을 적용하도록 진행되었다.

3.2 가상 화폐 거래소 피해 사례

발생 시기		거래소 명	피해 규모	피해 원인	결과	발생 국가
2018	9월	자이프	667억 원	해킹	매각	일본
	6월	빗썸	350억 원	이메일 악성 코드 추정	피해 보상	한국
	6월	코인레일	450억 원	이메일 악성 코드 추정	피해 보상	한국
	2월	비트그레일	1,921억 원	해킹	파산	이탈리아
	1월	코인체크	5,700억 원	해킹	매각	일본
2019	4월	빗썸	약 200억 원	해킹		한국
2020	9월	쿠코인	1,760억 원	암호 화폐 지갑 유출	피해 보상	싱가포르

[표 5] 가상 화폐 거래소 해킹 사례

⑴ 코인체크 사건

2018년 1월 26일에 발생한 해킹 사례는 최악의 거래소 해킹 사례로 언급된다. 일본의 가상 화폐 거래소인 코인체크가 해킹 공격으로 인해 580억 엔(약 5,700억 원) 상당의 가상 화폐를 도난당한 것이다. 피해자가 26만 명에 달하며 최초로 유출되기 시작한 지 19분 만에 피해액의 99%가 탈취당한 것으로 나타났다.

1. 해커가 코인체커 직원으로 위장
2. 코인체크 고객 계좌에서 10Xem(약 1,100억 엔) 가상 화폐 뉴이코노미무브먼트(NEM)가 외부 소재 익명의 가상 통화 계좌로 옮겨짐
3. 576억 엔(약 5,600억 원) 가치 가상 화폐를 외부 계좌로 유출, 19분 만에 99% 탈취
4. 2차로 훔친 가상 화폐를 8개 계좌에 분산
5. 추가로 3회에 걸쳐 1억~3억 엔 가치의 남은 NEM 전량 탈취

[표 6] 코인체크 사건 가상 화폐 유출 과정

⑵ 쿠코인 사건

2020년 싱가포르의 가상 화폐 거래소 쿠코인에서 2억 8,100만 달러(약 3,130억 원)가 유출됐다. 해당 사건에 대해 북한과 연관성이 강하다는 말이 나오고 있다. 해당 해킹 공격은 자동화된 거래를 용이하게 스마트 컨트랙트 등의 일부 기술을 악용한 defi 프로토콜을 사용하는 방식으로 알려졌다.

3.3 암호 화폐 지갑 관련 피해 사례

⑴ 마운트곡스 사건

핫 월렛 기반 암호 화폐 지갑을 해커들이 해킹한 사건이다. 2013년 비트코인이 황금기를 맞이했을 때, 마운트곡스는 세계 비트코인 거래량의 절반을 차지할 정도로 가상 화폐 시장에서 영향력이 큰 거래소였다. 당시 마운트곡스는 이 사건으로 인해 85만 개에 달하는 비트코인과 한화 약 5,660억 원에 달하는 금액을 도난당하고 파산했다. 마운트곡스는 2011년 상반기에 암호 화폐 지갑 안 비밀 키를 도난당하고 85만 개에 해당하는 비트코인을 해킹 당했다. 마운트곡스의 CEO 마크 카펠리스는 이 도난 사건이 마운트곡스 거래소의 내부적인 시스템 결함이 아닌 비트코인의 기반인 블록체인 기술의 결함이라고 주장하여 비트코인의 가격이 폭락하였다. 이후 사건의 전말이 밝혀져 블록체인 기술의 문제가 아닌 마운트곡스 거래소에서 암호 화폐 지갑의 보안을 소홀히 하여 해커가 데이터 파일을 복사할 수 있게 되어 피해를 입은 것이라 알려졌다.

⑵ 악성 코드

암호 화폐 지갑의 주소는 영문과 숫자의 조합이다. 가상 자산 사용자들은 대부분 별도로 이 주소를 저장해 놓고 ‘붙여넣기’를 해서 사용한다. 이 악성 코드는 사용자의 가상 자산 지갑 주소를 공격자의 지갑 주소로 바꿔치기 하도록 프로그래밍 되어 있다. 공격자는 먼저 보안이 취약한 일부 웹사이트를 침해한 이후, 악성 코드 유포 도구인 '익스플로잇 킷'을 이용해 악성 코드를 유포한다. 만약 사용자가 운영체제(OS)나 웹 브라우저 등에 최신 버전의 보안 패치가 적용되지 않은 PC로 해당 웹사이트에 접속하면, 익스플로잇 킷이 접속한 PC 내 취약점을 분석한 이후 악성 코드가 설치된다.

PC 감염 이후 악성 코드는 사용자의 PC를 모니터링 하며 사용자가 비트코인, 이더리움, 라이트코인, 지캐시, 비트코인 캐시 등의 가상 자산 지갑 주소를 복사하는 시점을 파악한다. 가상 자산 전송 시점을 파악하는 것이다. 이후 사용자가 가상 자산을 거래하기 위해 지갑 주소를 붙여넣기 할 때, 사용자가 입력한 원래 지갑 주소를 공격자의 가상 자산 지갑 주소로 바꿔치기한다. 만약 사용자가 지갑 주소를 다시 확인하지 않고 가상 자산을 전송하면 이는 공격자의 지갑으로 전송된다.

4. 결론

2010년도 비트코인의 가격이 급상승해 비트코인 초기에 투자를 한 투자자들이 많은 수익을 낸 후로 비트코인이 각광 받고 있다. 비트코인을 선두로 다른 가상 화폐들 또한 많은 관심을 받는 중이다. 가상 화폐 중 가장 많은 관심을 받고 있는 비트코인은 블록체인 기술을 기반으로 하고 있어 보안 위협으로부터 안전하다 생각하는 경향이 있다. 하지만 블록체인 기술에도 보안적 결함이 있고 가상 화폐를 거래할 때 사용되는 가상 화폐 거래소와 암호 화폐 지갑 같은 가상 화폐가 거래되는 과정에서 발생하는 보안 위협은 앞으로도 꾸준히 발생할 것이고 현재도 발생하고 있다. 가상 화폐와 이와 관련된 기술은 꾸준히 늘어나고 발전하여 화폐로서의 영향력이 커질 것이다. 가상 화폐는 주로 사용될 화폐가 될 가능성이 있으므로 보안에 항상 신경을 쓰고 보안에 생긴 문제점을 보완하도록 기술을 발전시켜야 한다. 블록체인 기술의 결함과 가상 화폐 거래소에 가해지는 보안 위협, 암호 화폐 지갑의 취약점 등 가상 화폐 보안의 문제점에 항상 경각심을 갖고 기술을 발전시킨다면 가상 화폐의 발전에 기여할 것으로 기대된다.

참고문헌

1) 박종서, “가상 화폐 ‘살아있네’… 하루 7600억씩 거래”, 한경 경제, 2020. 07. 09.

2) 피넥터 연구팀(백종찬, 한승환, 안상욱, 김영진, Chris Hong), 블록 체인 기술의 발전 과정과 이해.

3) 나건웅, 박진욱, “코인 거래소 ‘빅5’, 비슷한 듯 다 다르네… ‘거래량’ 업비트 ‘탄탄한 고객’ 빗썸”, 매일경제, 2021. 05. 25.

4) 비트코인, https://bitcoin.org/ko/

5)
https://www.kiri.or.kr/pdf/%EC%97%B0%EA%B5%AC%EC%9E%90%EB%A3%8C/%EC%97%B0%EA%B5%AC%EB%B3%B4%EA%B3%A0%EC%84%9C/nre2018-24_02.pdf, 2018

6) 이광영, “[암호 화폐 2017] H캐시, 양자 컴퓨터 상용화 시 블록 체인 보안 위험 경고”, 2017. 12. 05.

7) 이승환, “'암호 화폐 광풍'에 가상 자산 범죄 2년만에 5배”,
머니투데이, 2021. 04. 27.

8) Lucas Mearian, https://www.itworld.co.kr/news/121412, 2019. 04. 19.

9) 전체 디지털 화폐 거래소 거래량 순위,
https://www.coinhills.com/ko/market/exchange/

10) 금융보안원 보안기술연구팀, “블록 체인 기술과 보안 고려사항”, 2017. 08. 17.

11) “잇따른 대규모 암호 화폐 해킹… 피해자는 누구?”,
BBC 뉴스 코리아, 2021. 08. 29

12) 김다솔, “암호 화폐 해커들이 3000억원 돌려준 이유는?”, 이데일리, 2021. 08. 12.