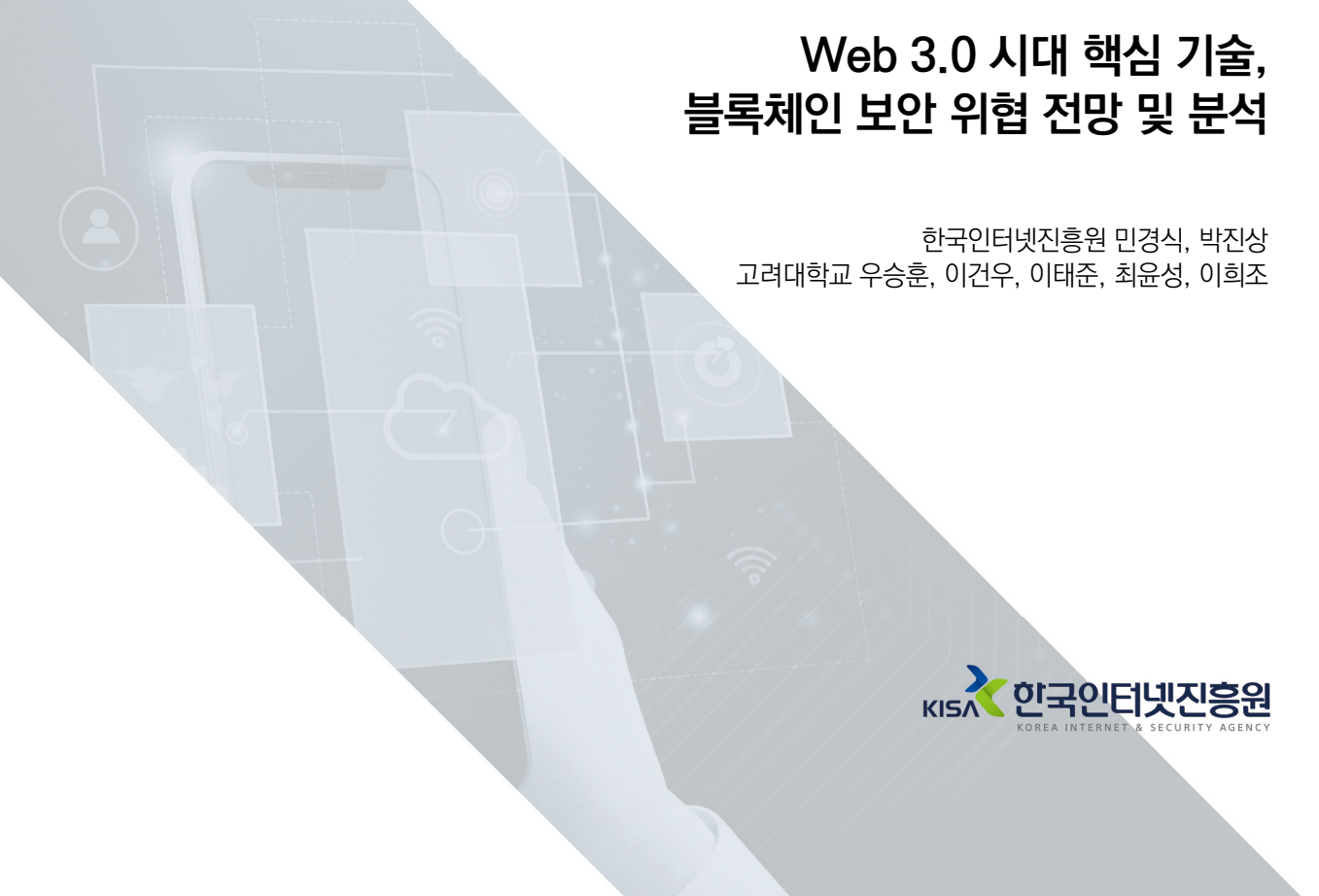
KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 2

Web 3.0 시대 핵심 기술, 블록체인 보안 위협 전망 및 분석

한국인터넷진흥원 민경식, 박진상
고려대학교 우승훈, 이건우, 이태준, 최윤성, 이희조



KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA INSIGHT
DIGITAL & SECURITY POLICY
2023 VOL. 2

Web 3.0 시대 핵심 기술, 블록체인 보안 위협 전망 및 분석

CONTENTS

[작성]

한국인터넷진흥원(KISA) 미래정책연구실 디지털정책팀

민경식 팀장	061-820-1454	kyoungsik@kisa.or.kr
박진상 선임연구원	061-820-1195	jinsang@kisa.or.kr

고려대학교

우승훈 연구교수	02-3290-3638	seunghoonwoo@korea.ac.kr
이건우 연구원		gnu@korea.ac.kr
이태준 연구원		tjlee@korea.ac.kr
최윤성 산학교수	02-3290-4816	yunseong@korea.ac.kr
이희조 교수	02-3290-3208	heejo@korea.ac.kr

요 약

Ⅰ 블록체인은 디지털 대전환과 디지털 경제를 견인할 핵심 기술이며, 웹 3.0 패러다임 전환의 주요 동인으로 작용

- 코로나 19 팬데믹을 경험하면서 디지털 기술의 혁신, 통신망 고도화, 모바일 기기 확산 등 경제·사회 전반에서 대전환이 촉발되었고, 빅테크 기업을 중심으로 관련 경제가 급성장
- 디지털 기술의 활용이 증대됨에 따라, 중앙 집중형 시스템의 문제점, 빅테크 기업에 대한 과도한 의존도, 대규모 개인정보 유출 등 다양한 문제가 발생하였고, 이에 따라 기술 역할에 대한 사회적 인식의 변화가 시작
- 기존 웹 2.0 환경의 문제점 극복에서 시작된 웹 3.0 패러다임 전환에 대한 논의가 전 세계적으로 진행 중이며, 차세대 웹의 진화 방향은 시맨틱 웹과 블록체인 기반의 웹 3을 중심으로 전개

Ⅰ 블록체인 기반 웹 3.0 전환의 주요 대안 기술인 웹 3 구현을 위한 주요 구성요소 검토 및 웹 아키텍처 구성(안) 제시

- 웹 3.0은 현재 주요 핵심 기술, 정의·범위 등이 정립되지 않은 초기 논의단계로 차세대 웹의 방향성을 논의할 주도 기술 선정은 시기상조이나, 여기에서는 웹 3.0 패러다임에 있어 논의되고 있는 기술 중 블록체인 기반의 웹 3을 중심으로 분석
- 웹 3.0 도래의 기대로 블록체인 기술의 새로운 가능성이 주목받고 있으나, 이러한 사회적 기대에 부응하기에는 아직 블록체인의 기술 성숙도는 부족하고 다양한 한계가 존재
- 블록체인 기반의 웹 3.0을 실현하기 위해서는 우선 기술의 태생적 문제점을 극복하고, 글로벌 사례 연구, 도전적인 시범사업, 법·제도 기반 마련 등 지속적인 노력이 필요하고, 특히 기술이 제공하는 가치와 활용에 대해 사회적 공감대를 형성하는 것도 중요
- 웹 3.0 아키텍처 구성(안)은 △이더리움 블록체인, △이더리움 가상머신(EVM), △스마트 계약, △프론트엔드로 구성되고, 이용자의 서비스 사용에 편리함을 주는 기타 요소(노드 관리, 서명, 저장, 쿼리, 확장 등)가 존재

요 약

Ⅰ 블록체인 보안위협은 지속 증가할 것으로 예상되며, 보안위협은 어플리케이션, 시스템, 네트워크를 중심으로 다양하게 발생

- 현재·미래의 블록체인 보안위협은 코드·스마트 계약 취약점 등 시스템 부문과 키 유출, 전자지갑 이슈 등 이용자를 대상으로 한 서비스 이용 부문의 위협이 가장 높음
- 다양한 블록체인 보안위협을 ① 어플리케이션, ② 시스템, ③ 네트워크로 재분류하여 각 계층별 발생하는 보안 위협을 분석하고 최신 침해사고 사례를 논의
- 또한, 계층별 보안위협 별로 위협을 체계적으로 완화할 수 있는 기술적 대응방안(보안 취약점 탐지, 시스템 오픈소스 구성요소 분석, 네트워크 보안 등) 제시

Ⅰ 웹 3.0 패러다임 전환을 위해 블록체인은 기술 한계 극복을 위한 지속적인 노력과 수용성 제고가 필요하며, 서비스 및 시스템의 보안성 향상 필요

- 웹 2.0의 다양한 문제점이 웹 3.0 전환의 동인이 되고 있으나 경제·사회 전반의 공감대 형성은 조금 더 시간이 걸릴 것으로 보임
- 또한, 블록체인 기반의 신뢰 사회 구현을 위해 소프트웨어 개발 업체의 보안 내재화를 촉진하는 연구·개발 및 정책적 지원이 필요하고, 시스템의 안전성 검증을 위한 암호기술 가이드라인 준수 요구

I

블록체인과 웹 3.0

블록체인은 디지털 대전환과 디지털 경제를 견인할 핵심 기술

디지털 대전환은 ICT 기술을 통한 사회 혁신뿐만 아니라, 기술의 역할에 대한 사회적 인식에도 새로운 변화를 유발

- 코로나 19 팬데믹을 경험하면서 디지털 기술의 혁신, 통신망 고도화, 모바일 기기 확산 등 경제·사회 전반에서 대전환이 촉발되었고, 빅테크 기업을 중심으로 관련 경제가 급성장
  - 사회적 거리두기 시행으로 원격근무, 온라인 쇼핑, OTT, 개인 방송 등 디지털화에 대한 요구는 혁신적인 ICT 기술들을 일상생활에 과감히 도입할 수 있는 계기가 됨
  - 블록체인, 인공지능 등 핵심 기술을 통해 경제, 사회, 일상 등 모든 영역이 디지털화 되는 현상이 전 세계적으로 유행[1]
  - 특히, 애플, 메타, 아마존 등 주요 빅테크 기업을 중심으로 ICT 신기술 활용 및 디지털 플랫폼 산업이 폭발적으로 성장하고 전 산업으로 확산되면서 경제 전반을 견인
- 디지털 대전환이 진행됨에 따라 기술의 편리함과 유용성을 넘어 다양한 측면에서 디지털 기술을 바라보게 되었으며, 이에 따라 탈중앙화, 데이터 주권, 개인정보보호 등 새로운 요구사항들이 등장
  - 디지털 기술의 활용이 증대됨에 따라, 중앙 집중형 시스템의 문제점, 빅테크 기업에 대한 과도한 의존도, 대규모 개인정보 유출 등 다양한 우려가 발생하였고, 개선을 위한 사회적 요구가 등장
  - 블록체인, 인공지능 등 ICT 新기술은 이러한 사회적 문제를 해결할 기술로 주목 받고 있음
- 이러한 사회적 변화에 맞춰 블록체인 기술 또한 새로운 변화를 맞이하는 중이며, 특히 웹 3.0 패러다임의 등장에 따라 사회적 요구를 준수할 수 있는 유력한 대안 기술로 촉망
  - 기존 블록체인 1.0 패러다임은 가상자산(비트코인 등)을 중심으로 한 활용이 스마트 계약, DeFi, NFT 등 이더리움 중심의 블록체인 2.0으로 패러다임이 변화하였고, 블록체인 3.0으로 진화 중에 있음

1 민경식·장한나(2021), “언택트에서 온택트 시대로”, KISA Insight 2021 vol.1, 2021.

- 또한, 분산 컴퓨팅 기반의 블록체인은 탈중앙화, P2P 거래 활성화, 데이터 주권 보장, 개인정보보호 강화 등 새로운 사회적 트렌드에 적합한 기술로 평가받는 중

참고1 블록체인 기술 개요

❖ 블록체인 정의 및 개념[2]

- 블록체인은 네트워크 참여자가 공유한 정보 및 가치를 제3의 신뢰기관 없이 분산형 네트워크를 통해 기록·검증·보관·실행하는 자율·신뢰 인프라, 시스템, 서비스 기술을 의미(IITP, 2020)
  - 모든 참여자(노드)가 거래내역이 기록된 원장 전체를 각각 보관하고, 공동으로 거래 정보를 검증하고 해시 기반으로 블록 처리하여 기록·보관·갱신
  - 일정 주기로 데이터가 담긴 블록을 생성한 후 이전 블록(block)들을 체인(chain)처럼 연결하는 구조로 이루어져 블록체인(Blockchain)으로 명명
- 블록체인은 ① 탈중앙성, ② 투명성, ③ 불변성, ④ 가용성 등 기술적 특성을 통해 데이터의 신뢰성을 확보
  - 데이터를 중앙 집중형으로 관리하던 기존 구조를 탈중앙화·분산화로 전환하여 업무 효율화 및 사회 혁신을 지향하며 가치의 인터넷(IoV) 실현 가능
- 1세대 분산장부 공유기술을 시작으로, 스마트 계약을 활용해 다양한 분야에 시도되는 2세대, 기술의 한계를 개선하기 위한 3세대로 발전 중

[표 1] 블록체인 기술의 발전단계 및 특징

발전단계	특징
1세대 (도입기)	– '09년 분산장부 공유기술(Distributed Ledger Technology) 기반의 비트코인 등장 후 디지털 자산(Digital Asset) 발행·유통이 주용도
2세대 (확산기)	– 스마트 계약이 추가되어 이더리움 등 응용플랫폼 성격이 강화된 활용 사례가 등장, 이를 기반으로 다양한 응용서비스로 확장
3세대 (자율형)	– 블록체인 데이터 전송 최적화 및 프라이버시 보장, IoT 등 다종 데이터 연동 처리, 블록체인 간 상호운용성, 산업 및 실생활 블록체인 적용 문제 해결

2 IITP, "ICT R&D 기술로드맵 2025 차세대보안·블록체인", 2020.

블록체인은 웹 3.0 패러다임 전환의 주요 동인으로 작용

웹 3.0 패러다임 전환으로 인해 블록체인 기술의 활용 및 새로운 기회 재조명

- 기존 웹 2.0 환경의 문제점 극복에서 시작된 웹 3.0 패러다임 전환에 대한 논의가 전 세계적으로 진행 중
  - 정보 전달을 주목적으로 하는 정적인 웹 1.0과 달리 웹 2.0은 구글, 메타, 아마존 등 주요 기업을 필두로 모바일 인터넷 및 소셜 네트워크 발전과 함께 경제·사회·문화 등 다양한 분야에서 혁신과 성장을 동인
  - 하지만 웹 2.0에서 감시자본주의 도래, 빅테크 기업의 출현과 독과점 이슈, 대규모 개인정보 유출 등 기업들의 과도한 영향력과 사회적 문제가 발생함에 따라, 이를 극복하고자 새로운 웹 패러다임 전환에 대한 필요성이 지속적으로 제기됨
- 웹 3.0의 개념은 월드와이드웹(www)을 고안한 팀 버너스 리(Tim Berners Lee)가 제안한 시맨틱 웹(Semantic Web)에 있으며, W3C에서 표준화 논의가 진행되었음
  - 시맨틱 웹: '의미론적 웹'을 뜻하며, 컴퓨터가 사람을 대신하여 정보를 읽고, 이해하고 가공하여 새로운 정보를 만드는 차세대 지능형 웹을 의미
  - 하지만 시맨틱 웹은 AI 기술의 한계와 알고리즘 기반으로 동작하는 웹 2.0과 명확한 구분이 어렵다는 비판이 존재하여, 최근 팀 버너스 리는 새로운 대안으로 솔리드(Solid) 프로젝트를 추진 중
- 현재는 이더리움 공동 창시자인 개빈 우드(Gavin Wood)가 2014년에 제안한 블록체인 기반의 탈중앙화 된 차세대 인터넷 웹 3(Web 3)을 중심으로 웹 3.0 패러다임 논의가 진행
  - 웹 3: 개빈 우드는 CNBC 팟캐스트 '비욘드 더 밸리(Beyond the Valley)' 인터뷰에서 "특정 기업이나 조직이 아닌 블록체인 기술의 신뢰에 기반한 이상적인 웹으로, 현재 인터넷 보다 분산되고 더욱 민주적인 버전의 인터넷"이며, "일반 이용자들이 인터넷의 일부를 소유하는 형태"라고 언급('22. 4.)
  - 탈중앙화(De-centralization) 및 소유권(Ownership)을 핵심 키워드로 하며[3], 중앙 집중형 시스템이 아니라 이용자가 자신의 데이터를 직접 통제하고, 디지털 자산과 콘텐츠를 중심으로 토큰·크리에이터 경제가 활성화될 것으로 예상
  - 허나, 웹 3은 트랜잭션 처리 속도, '탈중앙화'라는 지향점과 현실 간의 괴리, 블록체인 생태계의 미성숙함 등 다양한 기술적 한계가 존재함에 따라, 웹 3.0의 주요 대안이 될 수 있는가는 면밀한 검토 필요
- 웹 3.0은 아직 개념적 정의·범위가 명확하지 않은 초기 단계로, 블록체인 등 특정 기술에 초점을 두는 것이 아니라, 차세대 웹 진화 방향에 대한 포괄적인 관점의 논의가 필요
  - 시맨틱 웹, 웹 3, 솔리드(Solid), DWeb 등 다양한 웹 대안 기술과 함께 차세대 웹의 지향점, 극복해야 할 기술·사회 문제점 등 다양한 이슈에 대한 심층적인 고려 요구

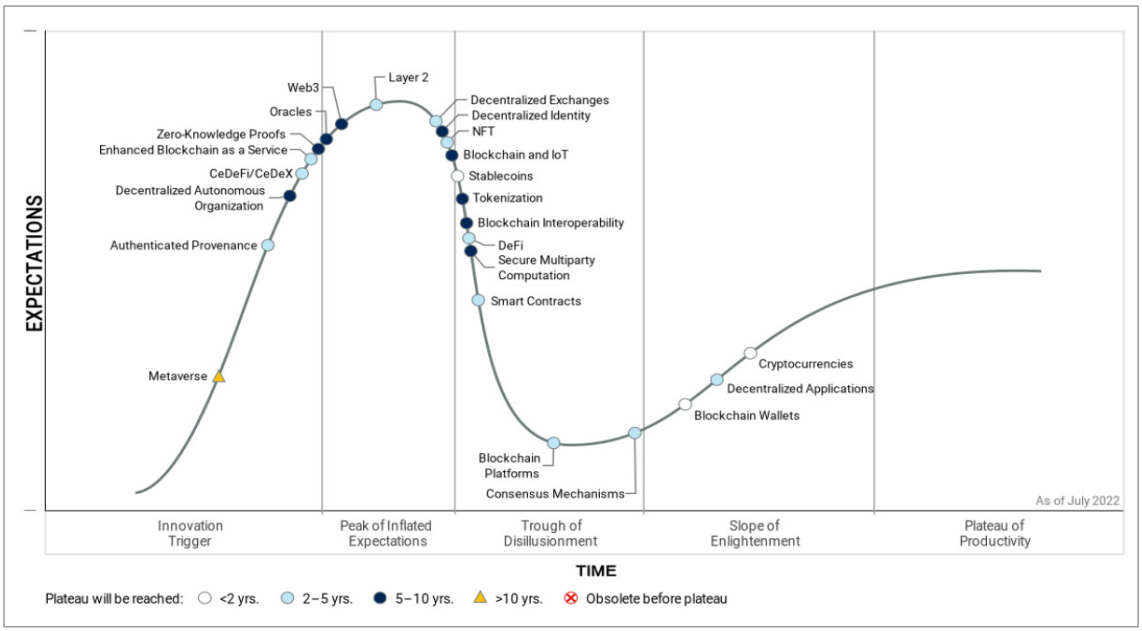
3 NIA, "Web 3.0, 디지털 공간 속 공정함과 새로움을 논하다", Digital Insight 2022, 2022. 4.

- VC(Venture Capital) 중심의 새로운 독과점의 한 형태이거나 단순히 마케팅 용어라는 부정적 여론도 있으나, 새로운 패러다임 전환에 긍·부정 평가가 동반되는 것은 일반적인 현상으로, 변화의 원인과 방향을 주시하고, 이를 기회로 바꾸는 지속적인 관심과 준비 필요

세계경제포럼과 마켓앤마켓, IDC 등 시장 조사기관들은 글로벌 블록체인 시장의 성장, 높은 가치 창출, 솔루션 수요의 지속적인 증가를 전망

- 세계경제포럼(WEF)은 2025년 전 세계 GDP의 10%가 블록체인 기술에서 창출될 것으로 전망[4]
- 마켓앤마켓(Markets and Markets)은 전 세계 블록체인 시장 규모가 연평균 67.3% 성장하여 2020년 3조 5,000억 원에서 2025년 46조 5,200억 원에 이를 것으로 예측[5]
- IDC는 전 세계 블록체인 솔루션 지출이 2024년까지 약 24조 8,140억 원에 이를 것으로 예측[6]
- 가트너(Gartner)에 의하면, DApp, 스마트 계약, DeFi, NFT 등과 같은 기술들이 앞으로 2년~5년 내로, DAO, 영지식 증명, 오라클, Web 3, DID 등 기술은 5년~10년 내에 상용화 예상[7]

[그림 1] 블록체인 기술 하이프사이클



출처) Gartner, “Hype Cycle for Blockchain and Web3 2022”, 2022. 7.

4 World Economic Forum, “Building Block(chain)s for a Better Planet”, 2018. 9.
5 Markets and Markets, “Blockchain Market by Component, Provider, Type, Organization Size, Application Area and Region – Global Forecast to 2025”, 2020. 5.
6 IDC, “Worldwide Blockchain Spending Guide”, 2021. 4.
7 Gartner, “Hype Cycle for Blockchain and Web3 2022”, 2022. 7.

| 주요국은 웹 3.0 시대에서 디지털 패권 경쟁의 우위를 확보하기 위해 활성화 전략 및 정책을 발표하고 기술 개발, 법제 개선 등 블록체인 역량을 강화 중

[표 2] 주요국의 웹 3.0 및 블록체인 전략·정책 동향

국가	주요 특징
 한국	- 관계부처 합동으로 새로운 웹 3 시대에서 블록체인 산업 육성을 통한 디지털 신뢰 생태계 조성을 목표로 하는 '블록체인 산업 진흥 전략' 발표(2022. 11.) - 데이터, 네트워크, 인공지능 기반의 'DNA+BIG3: 도미노 확산 전략(2022)'을 수립하여 5년간 10.9조 원 규모의 재정투자 및 D.N.A 생태계 조성을 위한 전략 및 정책 수립 - 과학기술정보통신부는 초연결·비대면 신뢰 사회를 위한 블록체인 확산전략(2020) 발표
 미국	- 바이든 대통령은 '디지털 자산의 책임 있는 발전을 보장하기 위한 행정명령(2022)'을 통해 가상자산의 안전성 보장, 금융시장과의 조화 등을 추진 - 통화주도권을 디지털 금융체제에서도 유지하기 위해 '디지털 자산 개발 전략에 관한 행정명령(2022. 3.)'을 통한 디지털 자산 정책 발굴, CBDC 연구 등 추진 - 연방 차원에서 블록체인 경쟁력 확보를 위한 '블록체인혁신법(2021. 6.)', 캘리포니아주 '디지털 금융자산법(2022. 6.)', 뉴욕주 '스테이블코인 사업자 지침(2022. 6.)' 등 발표 - '혁신 및 경쟁법(2021)', '미국경쟁법(2022)'을 추진하여 AI 등 ICT 신기술에 집중 지원 및 사이버 대응 지원 강화 등의 내용을 포함하여 경쟁력 강화를 목표로 함
 일본	- '디지털 사회 실현을 위한 중점 계획(2022)'을 기본 전략으로 국가 차원에서 웹 3.0을 추진 중 - 총무성 '기술 활용 연구회(2022. 8.)', 디지털청 '웹 3.0 연구회(2022. 10.)' 등을 운영하며 웹 3.0 사회를 위한 법제 정비, DAO 사례 검토, DID 실증 사업 등 다양한 현황 조사 및 과제 추진 중 - 각 부처에 분산되어 있는 웹 3.0 관련 담당 부서와 업무를 총괄하여 일관성 있는 정책 추진을 위해 경제산업성에 '웹 3.0 정책 추진실' 발족(2022. 7.) - 금융청(FSA)은 기존 자금결제법의 규정 하에 있던 가상통화 관련 법안을 금융상품거래법과 연계 적용하는 방안에 대한 검토 시작(2018)
 중국	- 국가 주도의 글로벌 블록체인 인프라(BSN)를 기반으로 공공-민간 연계 확장성 확보를 위한 전 세계 119개 노드 확보(2022. 7.) 후 40여개의 공공서비스 적용 - 부동산 등기, 농산물 이력 추적, 조달입찰, 저작권 보호, 전자계약, 의료·건강 등 사회 전반으로 블록체인 활용 분야를 확대 중(2022. 7.) - 코로나19로부터의 경제적 회복과 경쟁력 강화를 위해 '14차 5개년 계획'(2021)을 발표하여 7대 ICT 기술로 블록체인을 지정하는 등 디지털 중국의 건설 방향을 제시
 EU	- 유럽 디지털 신원 지갑 제도를 신설한 '전자신원확인체계(eIDAS 2.0, 2021. 6.)'와 '디지털 자산에 대한 규제 프레임워크(MICA, 2022. 6.)' 발표 - 국경 간 문서 공증, 졸업증명서 인증, 신원인증, 데이터 공유 등 공공 중심으로 블록체인 활용 도입 및 확산 중(2022. 5.) - 범 유럽 디지털 인프라 핵심 표준 확보 및 블록체인 기반 공공서비스 제공을 위한 '공공주도 유럽 블록체인 인프라(EBSI) 확보 및 유럽 전역에 38개 노드 구축 및 운영(2021. 12.)

Ⅱ

블록체인 기반의 웹 3.0

블록체인 기반 웹 3.0 전환의 주요 대안 기술인 웹 3

웹 3.0은 현재 주요 핵심 기술, 정의·범위 등이 정립되지 않은 초기 논의단계

- 시맨틱 웹, 솔리드, 웹 3 등 웹 3.0의 주요 대안 기술이 제시되고 있으나, 각 기술의 현실적인 한계, 기타 고려해야 할 사항에 대한 많은 검토가 필요한 상황으로, 차세대 웹의 방향성을 논의할 주도 기술 선정은 시기상조
  - 빅테크 기업의 과도한 영향력, 대규모 개인정보 유출 등 기존 웹 2.0의 다양한 문제점을 대안 기술을 통해 어떻게 극복할 수 있는가와 차세대 웹의 주요 철학(read-write-own)인 '데이터 주권(Data Ownership)'을 일반 이용자들에게 얼마만큼 실현 가능할 것인가 하는 문제도 과제임
  - 또한, AI, 블록체인 등 대안 기술이 가지는 사회 혁신성이 기존 제도나 경제·사회 일반에 수용될 것인가에 대해서도 신중한 접근 필요
- 웹 3.0 시대의 기술 확보 필요성이 제기되는 가운데, 국내에서도 차세대 웹 관련하여 산·학·연·관 등 전문가들이 모여 기술 활용에 대한 논의가 다양하게 진행되기 시작
  - 최근 블록체인 학회 등 ICT 학회가 주도하는 "웹 3.0" 포럼이 발족되고 기술 연구회가 만들어지고 있음
- 본 장에서는 웹 3.0 패러다임에 있어 논의되고 있는 기술 중 블록체인 기반의 웹 3(Web 3)을 중심으로 차세대 웹이 제공할 가치와 이를 구현하기 위한 구성요소를 분석

웹 3은 웹 3.0 패러다임 전환을 주도하기에 아직 기술 성숙도가 부족

- 웹 3.0 도래의 기대로 블록체인 기술의 새로운 가능성이 주목받고 있으나, 이러한 사회적 기대에 부응하기에 아직 다양한 한계가 존재
  - 금융, 유통, 게임 분야를 대표로 타 산업과 융합되어 주로 활용되고 있으며, DeFi, DID, NFT 등 블록체인 서비스도 웹 2.0 환경의 활용에 머무르는 수준

- 또한 '18년부터 국가 주도의 다양한 실증·시범사업이 추진되었지만 기술적용 한계 등의 이유로 아직 실물경제에 적극 도입되고 있지 않음

참고2 DeFi, NFT 기술 개요

❖ 디파이(DeFi), 탈중앙화 된 금융 플랫폼

- DeFi는 비트코인, 이더리움과 같은 개방형 블록체인 네트워크를 통해 구축된 금융 서비스를 의미[8]
  - 기존의 금융기관이 제공하던 대출, 거래, 결제, 보험 등의 금융 서비스에 대한 탈중앙화 시도
  - 블록체인 네트워크를 사용하여 기존 기술보다 빠르고 효율적으로 금융 서비스를 제공하고자 함
- 기존 금융 서비스에 비해 DeFi를 사용함으로써 이용자가 얻을 수 있는 이점은 다음과 같음[9]
  - 금융 서비스 접근성 향상: 가상자산 지갑을 소유하고 있으며, 인터넷에 접근할 수 있는 모든 이용자가 금융 서비스를 제공받을 수 있음
  - 시간·공간적 제약 해소: 블록체인 네트워크 전체가 마비되지 않는 한, 언제 어디서나 이용자가 금융 서비스를 제공받음
  - 거래의 투명성 보장: 블록체인 네트워크를 통해 신뢰 보장 가능(전체 이용자가 거래 기록 검증에 참여)
  - 서비스의 다양성 보장: 오픈소스를 기반으로 한 DeFi 프로토콜의 경우 개발자가 자유롭게 어플리케이션을 제작하여 서비스를 추가할 수 있으며, 이에 따라 이용자가 다양한 서비스를 활용
- DeFi 서비스는 미래 기술이 아니라, 현재 사용할 수 있는 기술 수준에 이름[10]
  - 스마트 계약 기반의 대출 프로토콜(예: 메이커다오, 컴파운드)
  - 탈중앙화 된 가상자산 거래소(예: 유니스왑, 클레이스왑)
  - 가상자산 손실에 대한 보험 프로토콜(예: 넥서스 뮤추얼 등)
- 기존 금융기관이 가상자산 서비스를 제공하기 시작하여 DeFi 시장 규모는 지속적으로 증가 중이며, '22년 2월 기준으로 지난해의 12배인 약 2,030억 달러가 시장에 예치됨

❖ 대체불가능 토큰(NFT), 가상자산의 소유권 증명서

- NFT는 블록체인 기술을 활용한 디지털 토큰으로 가상자산에 대한 소유권을 증명[11]
  - 디지털 토큰에 소유권에 관한 정보를 저장하여 블록체인 시스템에 저장함으로써 소유권 검증 가능

- 희소성 있는 가상자산에 대해 NFT를 발급하고 경매하여 가상자산의 소유권에 대한 거래 진행
- 미술작품, 디지털 캐릭터, 온라인 게시물 등의 디지털 정보에 대한 NFT 거래가 다수 진행

• 국내 기업 역시 NFT를 활용한 사업모델을 지속해서 개발 중[12] [13]

- 온라인게임: 캐릭터 및 아이템에 NFT를 이용하여 실 소유권 부여
- 엔터테인먼트: 소속 연예인들의 음악, 화보 등의 저작물에 대한 NFT 발행 사업을 진행
- 카드사: 공연에 대한 NFT 티켓을 발매하여 기존 티켓보다 더 많은 혜택 제공

• "디지털 등기 권리증" NFT는 다른 블록체인 기술에 자연스럽게 융화

- 메타버스, 웹 3.0 등의 블록체인 기술에서 NFT를 통하여 이용자가 제작한 콘텐츠의 소유권 증명 및 수익 창출, 유통 등 진행

[표 3] NFT로 거래된 가상자산 예시

분류	이름	거래 가격	비고
디지털 예술작품	The merge	1,300억원	Pak의 예술작품, 3만여 명의 투자자들이 분산구매 진행
	The First 5000 Days	986억원	5,000개의 NFT 작품을 콜라주(Collage)한 NFT 작품
디지털 캐릭터	크립토펑크 #7523	167억원	희귀한 확률로 생성되는 크립토펑크 NFT 캐릭터
영상 기록물	MBC 무한도전 '무야호' 영상	950만원	8초 분량의 영상 클립
온라인 게시물	잭 도시의 첫 번째 트위터 트윗	35억원	트위터 창업자의 첫 번째 트윗 내용

출처) YTN, "MBC 무한도전 '무야호~' NFT, 950만 원에 낙찰", 2021. 11.
B2C Korean, "역대 비싸게 팔린 NFT 가격 순위 top 10", 2022. 10.

8 김협, 권혁준, "디파이(DeFi) 기술의 이해와 활용 -금융 서비스를 중심으로-". 지급결제학회지, 12(2), 1-14. 2020.
9 Vistra, "Decentralized finance: Understanding the benefits, risks and challenges of DeFi". 2022. 11.
10 업비트, "DeFi 기반 금융 서비스 사례". 2022. 1.
11 서정민, 오유진, "[한국 미술시장 1조 시대] 등록·구매 제한 없는 NFT 아트, 10년간 100배 이상 커진다", 중앙일보. 2022. 3.
12 서울경제, "NFT, 어디서 쓰이고 있나...국내 NFT 활용사례 살펴보기". 2021, 7.
13 Samsung SDS, "기업의 NFT 그 활용 방안과 개발 방법". Samsung SDS 인사이트, 2022. 7.

- 블록체인 기술이 본격적으로 도입되어 약 6년 정도의 시간이 경과하였으나, 우리가 실감할 수 있을 정도로 실생활에서 활용되거나, 주요 산업으로 자리매김 하지 못하고 있음[14]
  - 주요 원인: ① 기술의 태생적 문제점 극복과 신뢰성 확보의 한계, ② 가상자산의 높은 변동성으로 인한 안정적인 시장형성 저해, ③ 블록체인의 실물경제와의 상생을 위한 노력 부족
- 블록체인 기반의 웹 3.0을 실현하기 위해서는 우선 기술의 태생적 문제점을 극복하고, 글로벌 사례 연구, 도전적인 시범사업, 법·제도 기반 마련 등 지속적인 노력 필요
  - 웹 3.0 시대에서 모든 데이터를 블록체인이 처리하고 보관하기 위해서는 트랜잭션 처리속도 개선, 비용 발생 이슈 해결, 스마트 계약의 고도화, 정보보호 및 개인정보보호 이슈 해결 등 다양한 문제점 극복 필요
- 기술이 제공하는 가치와 활용에 대해 정부, 기업, 이용자 등 모든 이해관계자 간 사회적 공감대를 형성하는 것도 중요할 것으로 보임

블록체인 기반의 웹 3.0 구현을 위한 주요 구성요소 검토

코드에 대한 신뢰를 기반으로 이용자의 데이터 주권을 보장하고 토큰 이코노미의 성장과 자율적인 조직(DAO) 운영을 중심으로 하는 웹 3.0 설계

- 기존 플랫폼 기업의 중앙 집중형 데이터 관리를 벗어나 탈중앙화 된 방식으로 이용자도 참여하여 개인정보를 관리하는 구조로 구상되고 있음
  - 웹 1.0: 일방향 데이터 이용 및 집중관리(Transferring Information)
  - 웹 2.0: 양방향 데이터 이용 및 집중관리(Interaction Between Users to Exchange Information)
  - 웹 3.0: 양방향 데이터 이용 및 분산관리(Transferring Ownership)
- 또한, 정부·빅테크 기업 등 제 3자 조직에 대한 신뢰를 기반으로 데이터가 이용·관리되는 방식이 웹 3.0에서는 블록체인 코드(Code)에 대한 신뢰를 바탕으로 데이터 이용·관리가 이루어짐
  - 웹 1.0: 국가·정부 신뢰 / 정보 전달
  - 웹 2.0: 빅테크 기업 신뢰 / 데이터 관리
  - 웹 3.0: 코드 신뢰 / 블록체인의 데이터 검증·관리

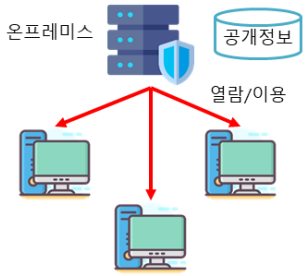
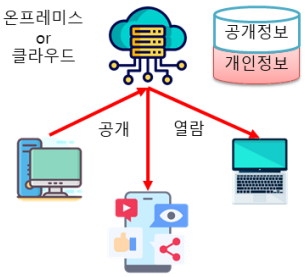
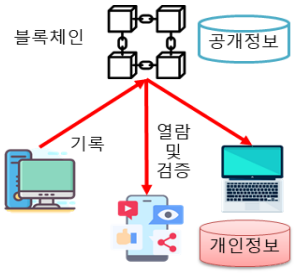
14 한국인터넷진흥원, “블록체인 기술의 실물경제 도입을 위한 정책 제언 연구”, 2022. 11.

[표 4] 웹 세대별 특징 비교

구분	웹 1.0	웹 2.0	웹 3.0(웹 3)
특징	웹 기반 마련	콘텐츠 생성 촉진, 정보 공유	인터넷 탈중앙화 가치 공유
네트워크	비교적 탈중앙화	중앙화	탈중앙화
거버넌스	웹페이지 보유자	플랫폼 기업 간 통합 권력	탈중앙화 조직(DAO)
콘텐츠	거의 생성하지 못함	플랫폼 기업 소유	이용자 소유
비즈니스	-	이용자 정보로 수익 창출	이용자 참여로 수익 배분
이용자 참여	소비자	소비자-생산자 중개기관에 금전 지급	소비자-생산자-소유자 생산자에 직접 코인 지급
인터페이스	PC 웹	웹, 소셜 네트워크, 모바일 웹	DApp, AR/VR
인증	ID, 비밀번호	ID, 비밀번호, 기타 인증	가상자산 지갑과 개인키
마이데이터	API 모델	플랫폼 모델	MyData 모델
기술	www 및 쿠키 생성	빅데이터, AI, 클라우드	블록체인, NFT, DAO, 메타버스

출처) 가트너 등 각종 자료 참고

[그림 2] 웹 세대별 구성(예시)

웹 1.0	웹 2.0	웹 3.0(웹 3)
일방향 데이터 이용 및 집중관리	양방향 데이터 이용 및 집중관리	양방향 데이터 이용 및 분산관리
		
발신자와 수신자 고정(일방 제공)	누구나 정보 발신·수신	이용자가 개별정보 발신 토큰을 이용한 서비스 자율제어

출처) 일본총합연구소(2022); "Web 3.0 트렌드 분석", p3. 각색

- 웹 3.0에서 데이터를 소유·관리하는 주체는 기업이나 조직뿐만 아니라 이용자도 포함되며 현재 웹 3.0은 여명기에 해당하고 분산형 앱(DApp)이 이용되기 시작한 단계
  - DApp: 스마트 계약을 이용해 블록체인에 데이터를 저장하는 웹 어플리케이션
  - DApp은 전자지갑(가상자산 보관)에 사용되는 암호키를 사용해 통신(서명)하고 블록체인에 데이터를 저장

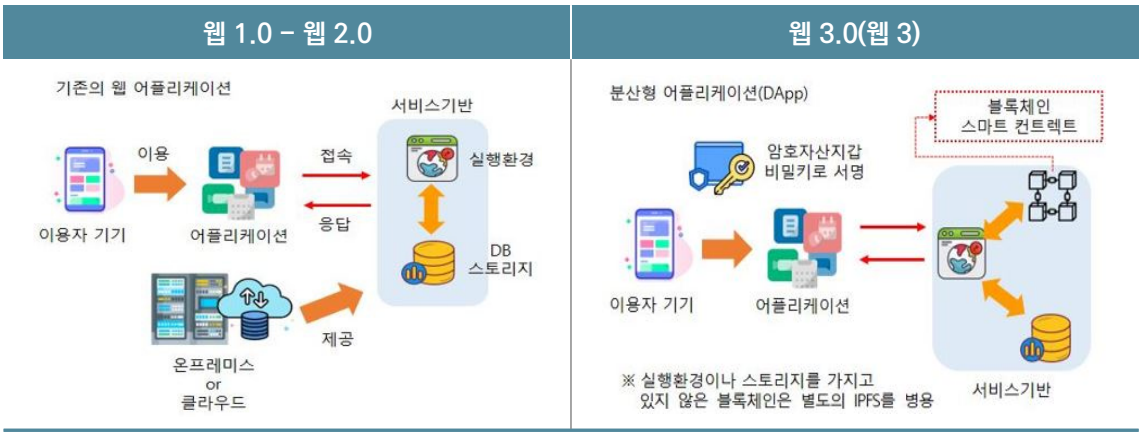
• 또한 DApp을 중심으로 DeFi, NFT 거래 등 토큰 이코노미가 더욱 활성화 될 것이며, 블록체인의 스마트 계약을 기반으로 자율적으로 운영되는 분산형 자율조직(DAO) 또한 증가할 것으로 보임

- 토큰 이코노미: 경제활동에 수반되는 모든 가치 유통을 블록체인에서 토큰을 발행하여 수행하는 경제권을 의미

  * Native Token(비트코인, 이더리움), Fungible Token(스마트 계약이 발행한 토큰), Non-Fungible Token(소유권 관리 토큰)

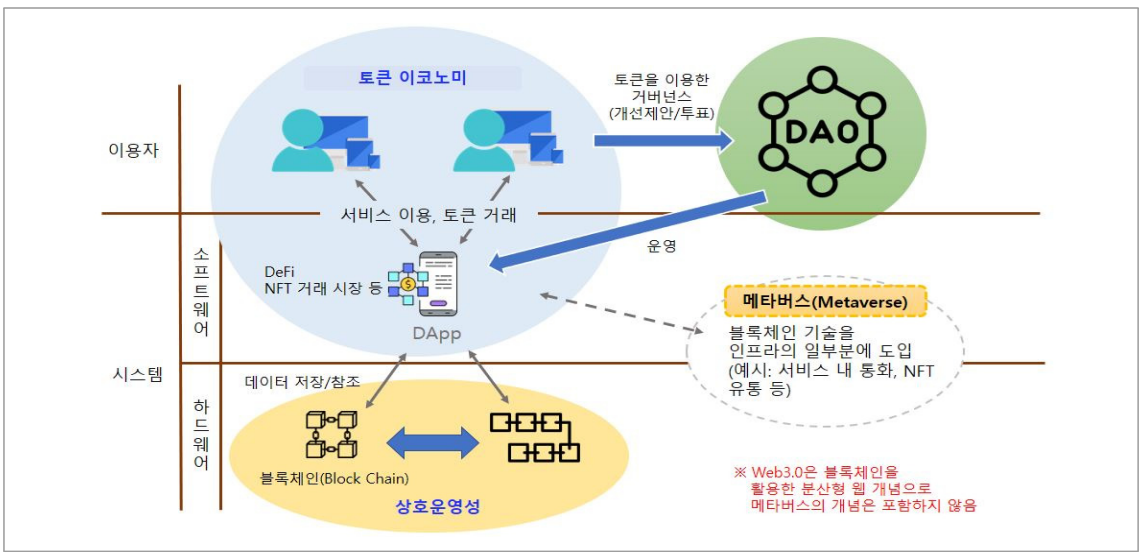
- 분산형 자율조직(DAO): 블록체인의 스마트 계약 기능을 활용하여 프로그램에 기록된 룰에 따라 운영되는 조직을 의미하며, 특정 관리자가 없어도 블록체인이 가동하는 한 자율적으로 운영 가능

[그림 3] 블록체인 기반의 웹 3.0에서의 DApp 활용



출처) 일본총합연구소(2022); "Web 3.0 트렌드 분석", p4. 각색

[그림 4] 블록체인 기반의 웹 3.0 구현 이미지

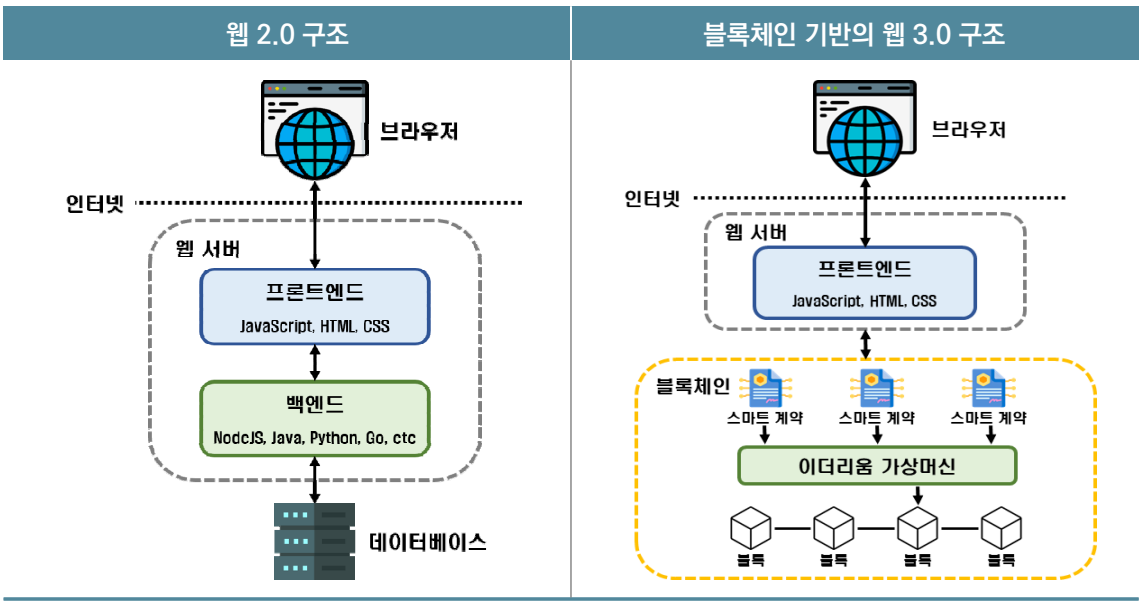


출처) 일본총합연구소(2022); "Web 3.0 트렌드 분석", p5. 각색

블록체인 기반의 웹 3.0 구현을 위한 웹 아키텍처 구성(안)[15]

- **(주요변화)** 웹 2.0과 비교하여 블록체인 기반의 웹 3.0(Web 3)은 이용자 입장에서 브라우저와 프론트엔드는 비슷하나, 기존 중앙 집중형 데이터베이스 및 백엔드 역할을 블록체인이 대체
  - 웹 2.0은 일반적으로 △데이터베이스(정보 저장), △백엔드(비즈니스 로직 정의), △프론트엔드(이용자 인터페이스 로직 정의)로 구성
  - 웹 3.0에서는 블록체인에 정보가 저장되고, 개별 노드로 운영되는 탈중앙화 된 상태머신(State machine) 內 스마트 계약이 비즈니스 로직을 정의

[그림 5] 웹 2.0 및 블록체인 기반의 웹 3.0 구조



출처) Preethi Kasireddy, "The Architecture of a Web 3.0 Application", 2021. 9.

- **(웹 3.0 아키텍처)** 블록체인 기반의 웹 3.0은 △이더리움 블록체인, △이더리움 가상머신(EVM), △스마트 계약, △프론트엔드로 구성
  - 이더리움 블록체인: 전 세계 어디서든 접근 가능하고, 노드간 합의와 P2P 네트워크를 통한 결정론적 상태머신*으로 동작

    * Deterministic state machine: 예측한대로 동작하는 알고리즘을 가지는 상태기계
  - 이더리움 가상머신: 스마트 계약 실행 및 블록체인 상태를 변경하는 상태 머신이며, 프로그래밍 언어를 해석할 수 없기 때문에 바이트 코드(Bytecode)로 컴파일 필요

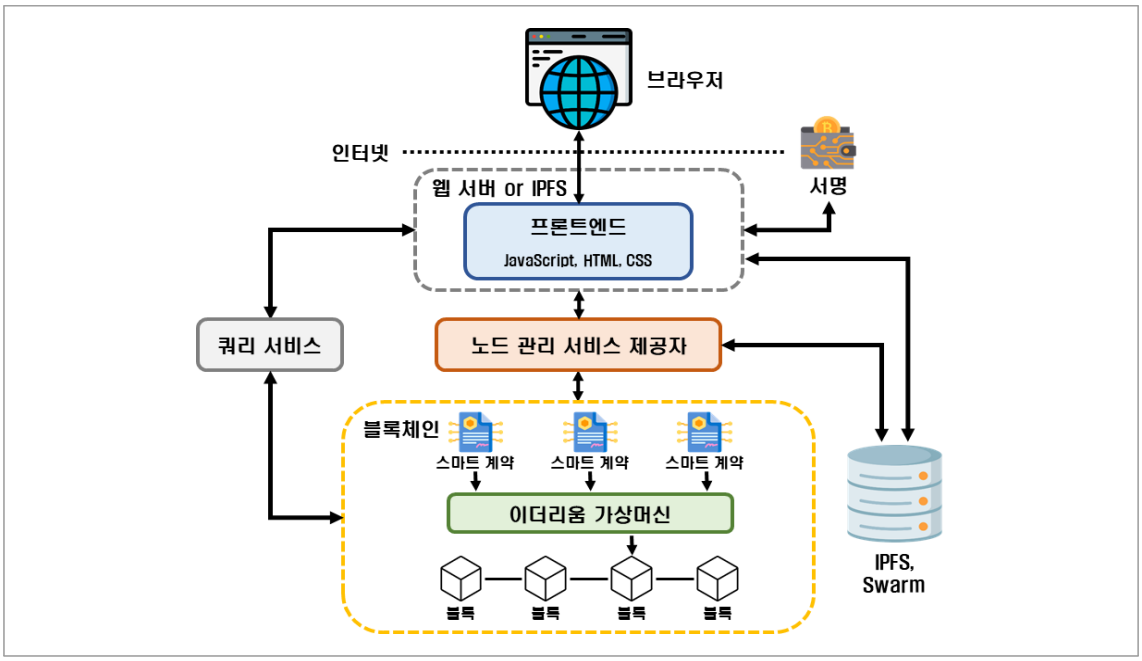
15 Preethi Kasireddy, "The Architecture of a Web 3.0 Application", 2021. 9.

- 스마트 계약: 이더리움 블록체인 상의 프로그램으로, 상태를 변경하는 비즈니스 로직을 정의하고 프로그래밍 언어(Solidity, Vyper)로 기술
- 프론트엔드: 이용자 인터페이스(User Interface) 로직을 정의하고 스마트 계약과 통신 가능

• **(웹 3.0 기타요소)** 웹 3.0 아키텍처의 주요 구성요소 외에도, 이용자의 서비스 사용에 편리함을 주는 기타 요소 또한 존재

- 실제 이용자가 웹 3.0에서 활동하기 위해 △노드 관리, △서명, △저장, △쿼리, △확장 등 관련한 대행 서비스 제공자 및 솔루션의 역할 필요

[그림 6] 블록체인 기반의 웹 3.0 전체 아키텍처



출처) Preethi Kasireddy, "The Architecture of a Web 3.0 Application", 2021. 9.

① (노드 관리) 이용자는 정보에 '접근'하기 위해 프론트엔드와 스마트 계약 간 통신이 이루어지도록 노드 관리를 대행하는 서비스 제공자(Infura, Alchemy, Quicknode)를 활용

* 이용자가 직접 노드를 운영할 수 있지만, 비용·저장공간 이슈로 인해 대행 서비스를 활용(다만, 중앙 집중형 서비스 의존이라는 우려 존재)

- 모든 서비스 제공자는 프론트엔드 어플리케이션이 블록체인과 상호작용 하도록 표준화 된 JSON-RPC* 규약을 구현

  * TCP에서 동작하는 데이터 교환 형식 포맷(JavaScript Object Notation)인 원격 프로시저 호출(Remote Procedure Call) 규약으로 데이터 구조와 처리방법을 정의

② (서명) 이용자는 정보를 '쓰기' 위해 새로운 트랜잭션을 블록체인에 전송하기 전 개인키로 서명하고 키 관리를 하는 지갑(Metamask)을 활용

- 지갑은 이용자의 개인키를 브라우저에 저장하고, 트랜잭션에 서명이 필요할 때 프론트엔드가 지갑을 호출
- 블록체인 기반의 웹 3.0에서 지갑은 이용자의 데이터 주권을 실현하는 주요 도구로 활용

  * 지갑의 역할이 중요함에 따라, EU는 '디지털 신원 지갑 프레임워크(The European Digital Identity Wallet Architecture and Reference Framework, '23. 2.)'를 발표하였고, 이더리움도 지갑의 UI/UX 개선을 위한 ERC-4337 표준을 발표('23. 3.)

③ (저장 공간) 이용자는 정보를 '저장'할 때 높은 비용의 발생을 막기 위해 탈중앙화 된 오프체인 저장 공간 솔루션(IPFS, Swarm)을 활용

- IPFS(Inter Planetary File System)은 분산 파일 시스템으로 정보를 P2P 네트워크 상의 노드에 분산 저장하는 기능을 제공(Infura, Pinata)

  * 파일코인(Filecoin)을 통해 전 세계 노드들에게 보상을 제공하고 저장 공간 확보
- 스웜(Swarm) 또한 IPFS와 같이 탈중앙화 된 저장 공간 네트워크이며, 차이점으로는 보상체계(SWM 코인)가 별도의 시스템이 아니라 내장됨

④ (쿼리) 이용자는 정보를 '읽기' 위해 블록체인 상의 스마트 계약에 정보를 요청하는 오프체인 인덱싱 솔루션(The Graph)을 활용

* 이용자가 직접 Web3.js 라이브러리를 통해 개별 스마트 계약의 이벤트를 확인할 수 있지만, UI 로직이 복잡해지기 때문에 오프체인 솔루션을 활용

- 더그래프는 쿼리 언어(GraphQL)를 통해 블록체인 內 정보를 인덱싱 하여 이용자가 쉽고 빠르게 온체인 정보를 요청하도록 함

⑤ (확장) 이용자는 'DApp을 이용'할 때 속도·비용 이슈를 해결하기 위해 확장 솔루션(Polygon)을 통한 사이드체인* 활용

* Sidechain: 정보를 분산 처리하고, 트랜젝션 처리속도를 향상시키기 위해 메인 블록체인에 연결된 체인

- 솔루션은 트랜잭션을 오프체인에서 처리하고, 주기적으로 트랜젝션 정보만 온체인에 저장하기 위해 사이드체인을 메인 체인에 연결

다음에서는 웹 3.0 시대의 핵심 기반 기술인 블록체인의 대표적인 보안위협을 도출하고, 대응 기술의 개발 현황을 소개

- 블록체인 기술의 보안위협을 어플리케이션, 시스템, 네트워크로 분류하고, 각 계층별 발생하는 위협의 세부내용 및 최신 침해사고 사례 분석
- 또한, 보안이 시급한 코드·스마트 계약 취약점 등 시스템 부문과 전자지갑 등 이용자를 대상으로 한 서비스 이용 부문의 보안위협에 대한 기술 개발 현황을 살펴봄

Ⅲ 블록체인 보안 이슈

블록체인 보안위협은 지속적으로 증가할 것으로 예상되고 대응준비 필요

현재·미래의 블록체인 보안위협은 코드·스마트 계약 취약점 등 시스템 부문과 키 유출, 전자지갑 이슈 등 이용자를 대상으로 한 서비스 이용 부문의 위협이 가장 높음[16]

[표 5] 블록체인 기술의 보안 위협 분류

ICT 기술명	보안 위협		
	대분류	중분류	세분류
블록체인	공급자	시스템	- 코드 취약점(시스템 측면) - 스마트 계약 취약점 - 전자지갑(Hot Wallet) 대상 보안 위협(악성코드, 랜섬웨어, 가상자산 탈취 등) - APT 공격 취약 등
		기기·인프라	- (퍼블릭 블록체인) 분산 노드 해킹 위험 - 블록체인 생성 노드 또는 가상자산 채굴 등 시스템에 대한 악성코드/랜섬웨어 유포 등
		데이터	- (개인키, 공개키) 권한 탈취 - 51% 합의를 장악(하이재킹) 등
		네트워크	- DDoS 공격 - 합의 시간차 공격(플래시론 공격) - DNS, BGP Hijacking 등
	이용자	서비스 이용 보안 이슈	- 개인키 유출 - 전자지갑 보안 이슈 - 개인정보 유출 및 쉬운 암호화 해제 문제 등

16 민경식, 김관영, 장한나, “2030 미래사회 변화 및 ICT 8대 유망기술의 사이버 위협 전망”, KISA Insight, Vol.1, 2022.

- 보안위협의 대분류를 공급자·이용자로 하고 중분류로 공급자는 시스템, 기기·인프라, 데이터, 네트워크로 구분하고, 이용자는 서비스 이용에서의 보안 이슈를 도출
  - 중분류별 보안위협을 세분화하여 전문가(60명) 대상으로 설문을 진행하여 해당 보안위협의 현재·미래 위협수준 및 대응 준비도를 5점 척도로 평가
- 시스템과 서비스 이용 부문의 현재·미래 위험도가 상대적으로 높게 평가되었으며, 특히 시스템의 대응준비도가 2.86점으로 가장 취약한 것으로 나타남
  - (현재 위험도) 서비스 이용에 관한 현재 위험도가 3.64점으로 가장 높게 평가되었으며, 시스템 위협이 3.61점, 네트워크가 3.22점으로 그 뒤를 이음
  - (미래 위험도) 시스템이 3.82점, 서비스 이용이 3.75점으로 높게 평가되었음
  - (대응준비도) 미래 위험도가 가장 높게 평가된 시스템의 대응 준비도는 2.86점으로 보통(3점) 수준에 못 미치는 것으로 나타남
- 현재·미래 위험도가 높고, 대응준비도가 부족한 코드 취약점, 스마트 계약 취약점, 전자지갑 보안 위협 등 시스템 및 블록체인 서비스 이용 부문에서 발생 가능한 보안위협에 대한 보안이 요구됨

[표 6] 블록체인의 현재, 미래위험도와 대응준비도 평가 결과

	현재위험도	미래위험도	준비도
시스템	3.61	3.82	2.86
기기·인프라	3.15	3.38	3.01
데이터	3.16	3.37	2.99
네트워크	3.22	3.36	2.92
서비스 이용	3.64	3.75	3.06

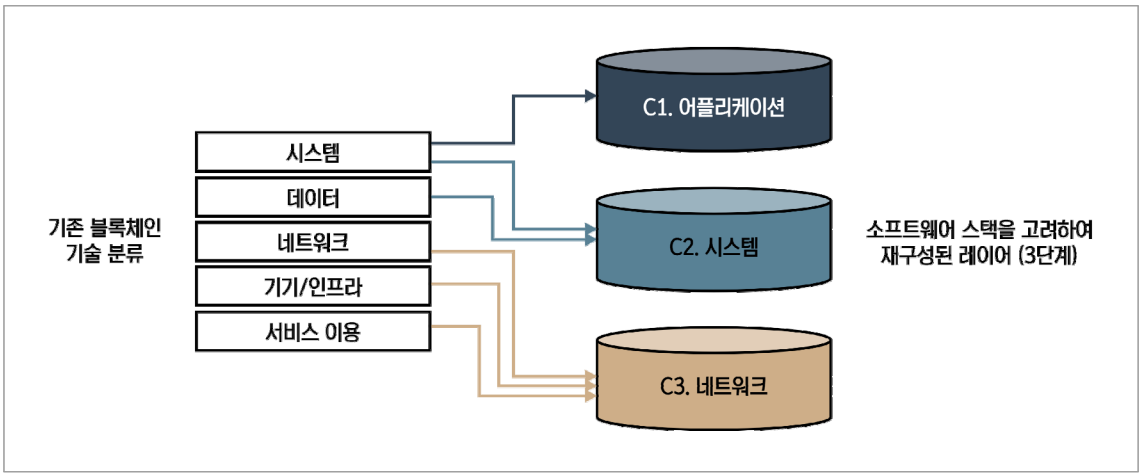
다양한 블록체인 보안위협을 ① 어플리케이션, ② 시스템, ③ 네트워크로 재분류하고, 각 계층별 발생하는 보안 위협을 분석

- 기존 5 계층(시스템, 기기·인프라, 데이터, 네트워크, 서비스 이용)으로 분류되었던 보안위협을 소프트웨어 스택을 고려하여 어플리케이션, 시스템, 네트워크 3 계층으로 재분류
  - 더 세부적인 분류 및 대응이 필요한 기존의 시스템, 데이터 계층을 어플리케이션 및 시스템으로 구별하고, 기기·인프라, 네트워크, 서비스 이용의 계층을 네트워크 계층으로 통합
  - 특정 계층에서 발생한 보안 위협은 다른 계층의 안전성에도 영향을 미치기 때문에, 각 계층의 보안성 확보 필요

• 블록체인 어플리케이션(시스템), 시스템(일반 시스템, 데이터), 네트워크(기기·인프라, 네트워크, 서비스 이용) 각각에 대한 보안위협 고려 필요

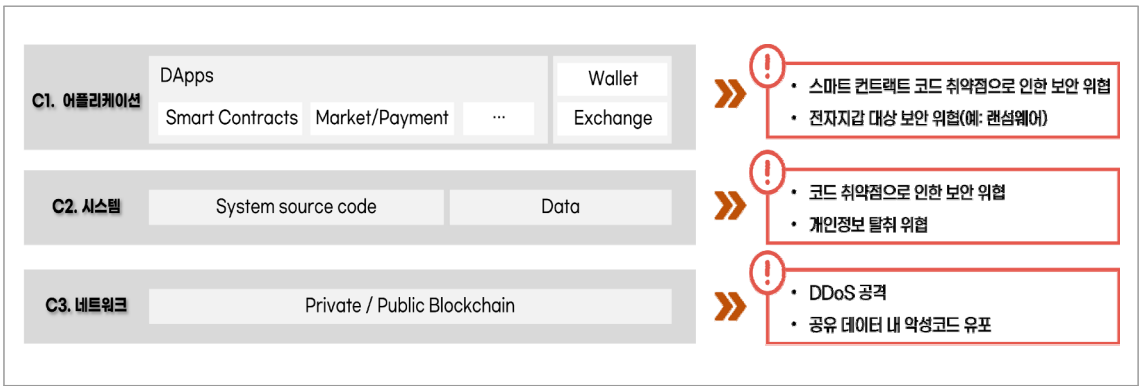
- (C1) 어플리케이션: DApp 및 스마트 계약과 같은 블록체인 어플리케이션에 존재하는 취약점으로 인해 보안위협 발생
- (C2) 시스템: 블록체인 시스템 코드의 취약점으로 인한 보안위협 발생
- (C3) 네트워크: 블록체인 네트워크에 대한 DDoS 공격을 비롯하여, BGP 하이재킹, 네트워크 내에서 공유되는 데이터 내 악성코드 유포 등 보안위협 발생

[그림 7] 소프트웨어 스택을 고려한 블록체인 기술의 3단계 분류



출처) 고려대학교 컴퓨터보안연구실

[그림 8] 블록체인 기술의 보안 위협(어플리케이션·시스템·네트워크)



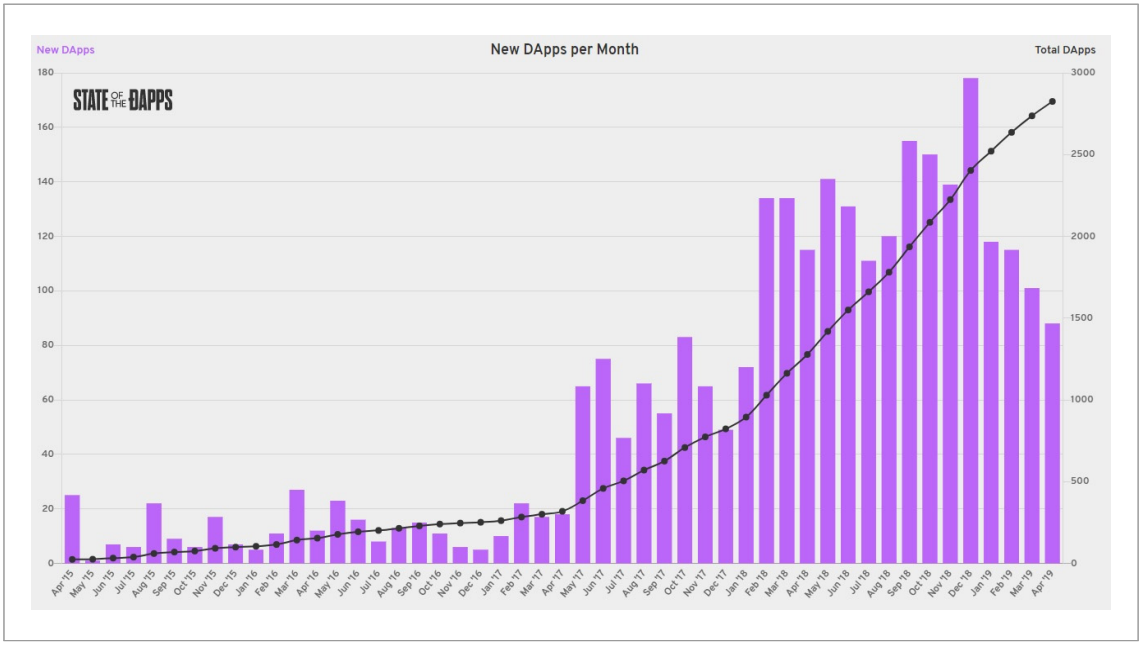
출처) 고려대학교 컴퓨터보안연구실

블록체인 보안위협은 어플리케이션, 시스템, 네트워크를 중심으로 다양하게 발생

[C1] 어플리케이션 보안위협

- 블록체인 어플리케이션 현황
  - 블록체인 서비스를 위한 DApp의 수는 꾸준히 증가 중(그림 9 참고)
  - 2022년에 발생한 블록체인 보안사고 중, 스마트 계약을 겨냥한 공격이 가장 큰 비중을 차지[17]
  - 가상자산 및 대체불가토큰(NFT) 활성화 등의 영향으로, 개인이 지갑을 직접 관리하는 추세

[그림 9] 월간 DApp 수 변화 추이



출처) State of the DApps, “New DApps per Month”, 2019. 5.

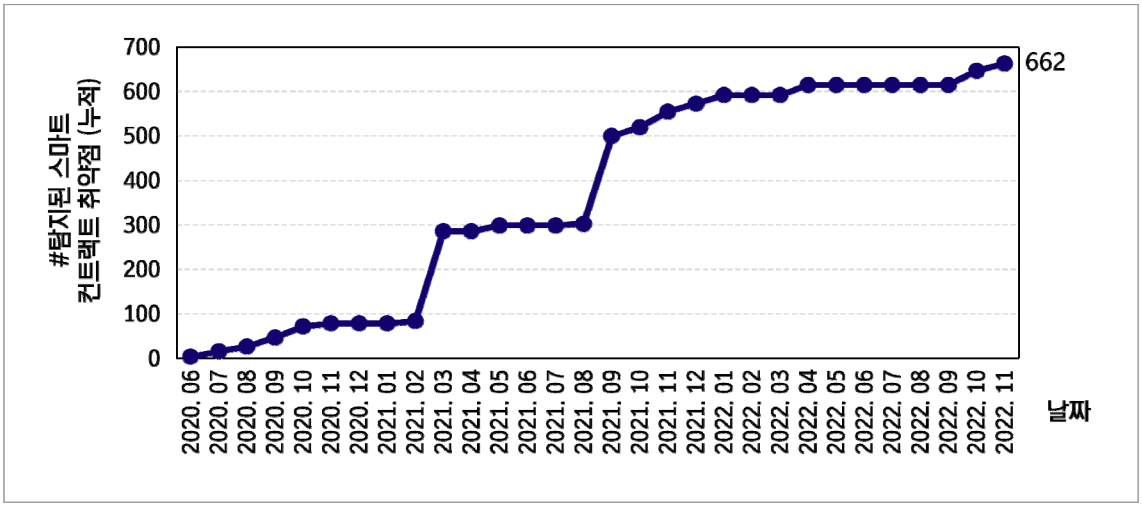
- (어플리케이션 취약점 악용) DApp 및 스마트 계약과 같이 블록체인 어플리케이션에 존재하는 취약점을 악용하여 금전적인 이득을 취하는 공격
  - 조사 결과에 따르면, 스마트 계약의 취약점은 매년 증가 중(그림 10 참고)
  - 배포된 이더리움 스마트 계약의 수집 가능한 소스코드 표본을 기준으로 취약점 분석을 진행한 결과, 전체

17 CoinDesk, “올해 블록체인 보안사고, 스마트 콘트랙트 공격이 최다”, 2022. 11.

표본의 95%가 하나 이상의 취약점을 가지고 있다는 연구 결과 존재[18]

- 스마트 계약 취약점은 단 한 줄의 코드에 의해 발생할 수 있으며, 이는 보유한 화폐 잔고 보다 훨씬 높은 금액을 전송할 수 있는 등 막대한 금전적인 손실로 이어질 수 있음
- 또한 코드 재사용이 활발한 블록체인 스마트 계약의 개발 환경 특성으로 인해, 하나의 계약에서 발견된 취약점은 다른 계약으로 전파될 가능성이 높음

[그림 10] VERISMART 기술을 통해 분석한 스마트 계약 취약점 증가 추세(누적)



출처) 고려대학교 컴퓨터보안연구실

- (개인키·정보 탈취) 해커가 블록체인 지갑(Wallet)의 개인키를 빼돌려 가상자산에 대한 권한을 획득한 후, 가상자산을 훔치는 공격
  - 공격자들은 지갑을 해킹하여 블록체인 서비스 이용자의 개인키 및 개인정보를 빼돌려 가상자산을 탈취하거나 서비스 가용성을 해치는 등의 공격 수행
  - 특히 온라인상에 저장되는 핫 월렛(Hot Wallet)은, 하드웨어에 저장되는 콜드 월렛(Cold Wallet)에 비해 해킹 공격에 더욱 취약함

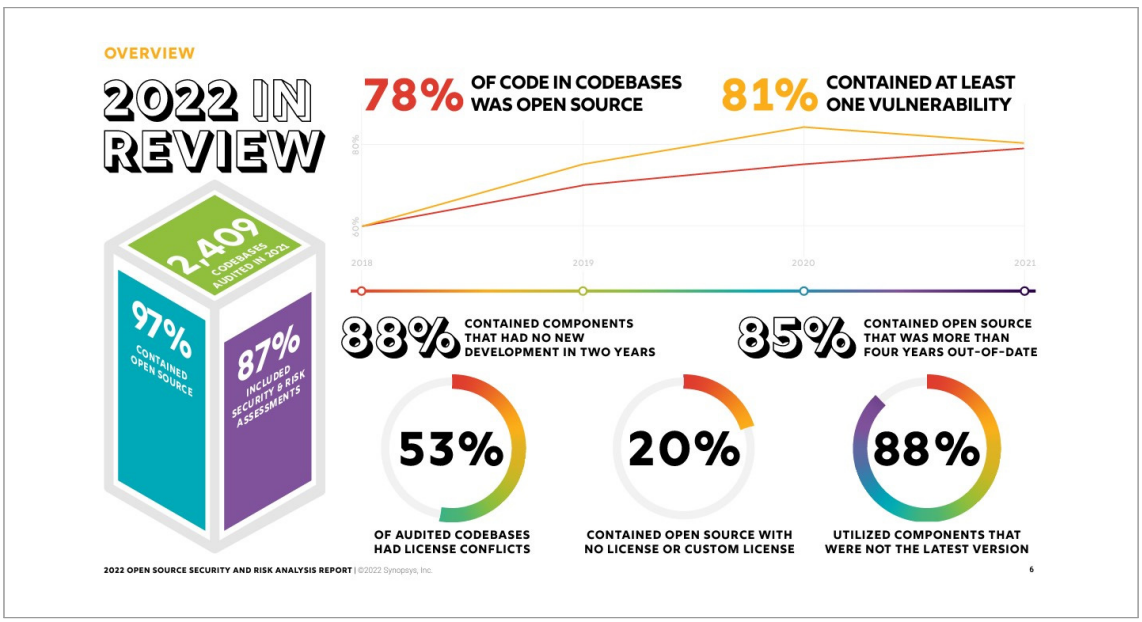
[C2] 시스템 보안위협

- (취약한 오픈소스 구성요소 악용) 블록체인 시스템에 존재하는 취약한 오픈소스 소프트웨어 구성요소를 악용하여 악의적인 이득을 취하는 공격

18 Sukrit Kalra, Seep Goel, Mohan Dhawan, Subodh Sharma, "ZEUS: Analyzing Safety of Smart Contracts, Network and Distributed Systems Security Symposium", 2018. 2.

- 블록체인은 기본적으로 암호화 해시체인, 분산 네트워크 및 전자 서명 등의 기술을 활용함으로써 보안에 안전하다고 알려졌지만, 블록체인 서비스를 구현한 ICT 시스템은 기존 사이버 위협에 동일하게 노출
- 블록체인 시스템은 기존 소프트웨어와 동일하게, 개발 과정에서 효율성을 높이고 혁신적인 소프트웨어 개발을 위해 다양한 오픈소스 소프트웨어를 재사용
- 조사 결과에 따르면, 비트코인을 포함한 가상자산 블록체인 소프트웨어에는 평균 10개 이상의 오픈소스 소프트웨어가 재사용되는 중[19]
- Synopsys에 따르면, 조사 대상 소프트웨어의 97%는 하나 이상의 오픈소스 구성요소를 포함하고 있으며, 특히 소프트웨어 중 81%는 하나 이상의 취약점을 포함[20] (그림 11 참고)
- 꾸준히 관리되지 않은 오픈소스 소프트웨어 구성요소에는 취약점이 존재할 수 있으며, 취약한 오픈소스 소프트웨어 구성요소를 겨냥한 가상자산 탈취, 블록체인 서비스 가용성 저해 등 다양한 공격이 가능

[그림 11] 오픈소스 소프트웨어 재사용 현황 및 취약 소프트웨어 비율



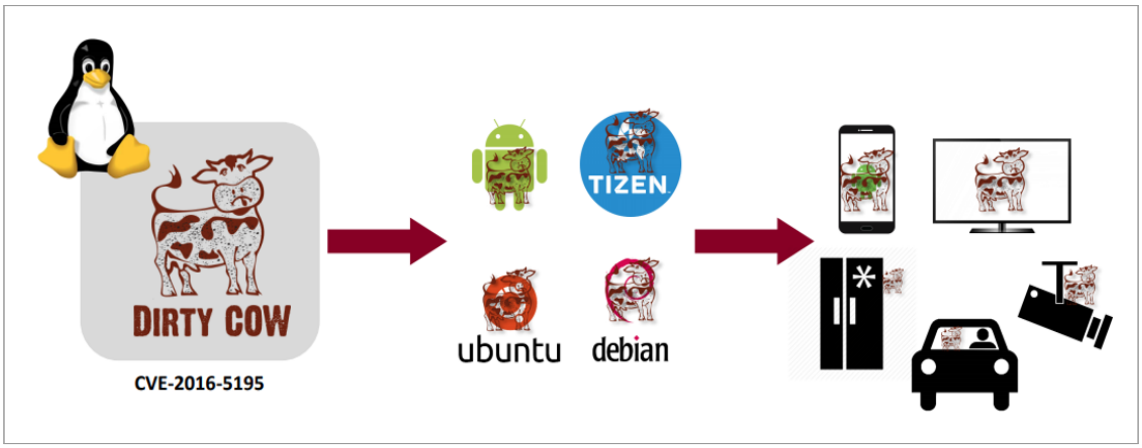
출처) Synopsys, “Open Source Security and Risk Analysis Report”, 2022. 4.

- (전파된 취약코드 악용) 코드 재사용으로 인해 전파된 취약점을 악용하여 이득을 취하는 공격
  - 비트코인의 합의 알고리즘 코드가 다른 가상자산에서 널리 활용되듯이, 블록체인 코드 역시 다른 블록체인 시스템에서 자주 재사용됨

19 고려대학교, “블록체인 플랫폼 보안 취약점 자동분석 기술 개발 과제”, 2022.
20 Synopsys, “Open Source Security and Risk Analysis Report”, 2022. 4.

- 코드 재사용은 혁신적인 소프트웨어를 개발하기 위한 효율적인 프로세스지만, 취약한 코드가 전파되어 전체 소프트웨어 시스템의 보안성을 위협(그림 12 참고)
- 또한 블록체인 시스템에 존재하는 보안 취약점은 코드 재사용 프로세스로 인해 다양한 블록체인 시스템으로 전파될 수 있으며, 전체 블록체인 시스템의 보안성을 위협

[그림 12] Dirty COW(CVE-2016-5195) 취약점 전파 과정

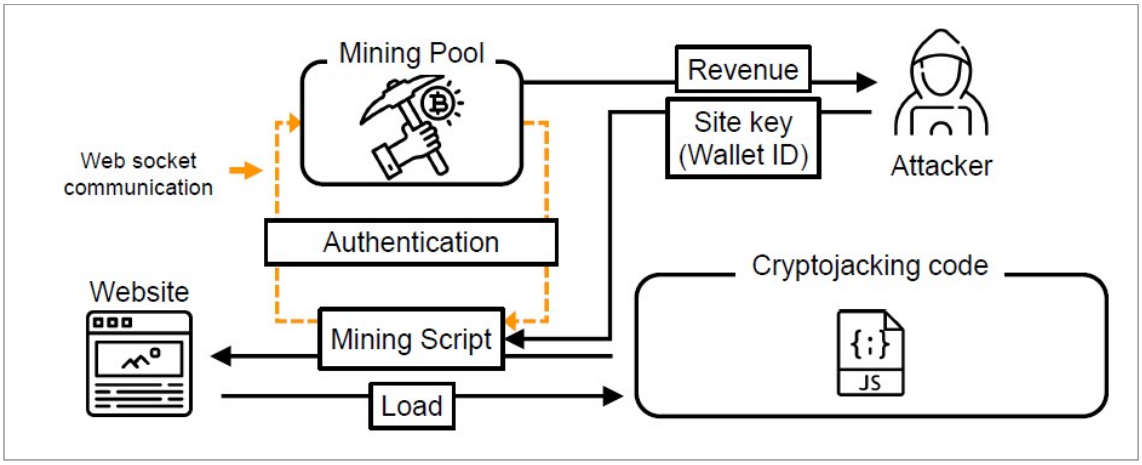


출처) 고려대학교 컴퓨터보안연구실

[C3] 네트워크 보안위협

- (BGP 하이재킹) 인터넷 인프라의 구조적 취약점을 겨냥하여 데이터를 탈취하거나, 전체 네트워크 마비 등을 일으키는 공격
  - 네트워크 자율시스템(NAS) 간 라우팅 테이블을 공유할 때 사용되는 경계 경로 프로토콜(BGP)의 구조적인 취약점을 공격
  - 라우팅 테이블을 조작하여 악성코드를 배포하거나, 특정 서버로 전송되는 요청을 가로챔으로써 데이터 및 가상자산 탈취
- (크립토재킹) 타겟 피해자의 컴퓨팅 자원을 악용하여 금전적인 이득을 취하는 공격
  - 해커들은 PC, 서버 등에 크립토재킹 악성코드를 설치하여 타겟 피해자의 컴퓨팅 자원을 악용하고, 가상자산을 채굴함으로써 금전적인 이득을 취함(그림 13 참고)
  - 악성코드로 인한 증상이 미비하여(CPU 사용량 증가 등) 피해자들이 공격을 판단하기가 어려움
  - Javascript 언어의 패키지 관리자인 Node Package Manager(NPM)와 Python 언어의 패키지 관리자인 PyPI에서 크립토재킹을 수행하는 악성 패키지가 다수 발견

[그림 13] 크립토재킹 공격 발생 과정



출처) 고려대학교 컴퓨터보안연구실

- (블록체인 브릿지 해킹) 2개의 다른 블록체인 네트워크를 연결해 자산을 옮길 수 있도록 도와주는 블록체인 브릿지 기술을 해킹하여 악의적인 이득을 취하는 공격
  - 블록체인 브릿지는 특정 블록체인 상에서 가상자산을 담보로 예치한 후, 브릿지 노드들의 승인을 거쳐 다른 블록체인에서 자금을 인출하는 방식으로 구동
  - 이러한 블록체인 브릿지를 활용한 거래 승인 과정에서 취약점이 발생하면 해킹에 노출될 수 있음

전 세계적으로 블록체인 어플리케이션, 시스템, 네트워크의 취약점을 악용한 침해사고가 다수 발생

[표 7] 블록체인 침해사고 사례

구분	침해사고 사례
어플리케이션	• 이더리움의 스마트 계약 프로젝트 중 하나인 DAO에 존재하던 재귀호출 버그로 인해 투자금을 이더리움으로 반환하는 기능이 무한이 실행되는 취약점 발생('16. 7.) – 해커는 해당 취약점을 악용하여 243만 개에 달하는 이더리움을 탈취 • 가상자산 거래소 빗썸에 핫 월렛 해킹 사고 발생('18. 6.) – 빗썸 핫 월렛에 보관되었던 350억 원 규모의 가상자산이 탈취 • 트론(TRX)의 DApp 해킹을 통한 가상자산 탈취('19. 4.) – 트론의 DApp인 트론뱅크와 트론와우가 해킹되어 공격자에게 가상자산이 탈취 • 카이카스 전자지갑 內 개인키 탈취('21. 11.) – 전자지갑 서비스 "카이카스" 이용자들의 개인키가 탈취되는 해킹 피해 발생

구분	침해사고 사례
시스템	• 비트코인 코어에서 이중지불 취약점 발견('18. 9.) – 비트코인에서 이중지불 취약점(CVE-2018-17144)이 발견됨 – 비트코인 코드를 재사용하던 일부 가상자산에서 금전적인 손실 발생(예: 피존 코인) • 액시 인피니티(Axie Infinity) 취약점 해킹('22. 3.) – 게임을 하며 수익을 창출하는 플레이투언(P2E) 게임의 선두주자인 액시 인피니티에서 해킹 발생 – 해커들은 액시 인피니티 내 사이드체인인 로닌(Ronin)의 취약점을 악용하여 한화 7,000억 원 이상의 금전적인 이득을 취함 • 스테이블 코인 빈스톡(Beanstalk) 해킹('22. 4.) – 해커들이 빈스톡에 존재했던 플래시론 취약점을 악용하여 1억 8,200만 달러의 이득을 취함
네트워크	• 유럽 국가들의 슈퍼컴퓨터를 대상으로 한 크립토재킹 공격('20. 5.) – 해커들이 영국, 독일, 스위스 등 유럽 국가들의 슈퍼컴퓨터를 악용하여 크립토재킹 수행 – 슈퍼컴퓨터의 자원을 해킹하여 가상자산을 채굴함으로써 금전적인 이득을 취함 • 클레이스왑(KLAYswap) BGP 하이재킹('22. 2.) – BGP 하이재킹 공격을 통해 국내 최대 규모 DeFi 서비스 클레이스왑(KLAYswap)에서 22억 규모의 가상자산 해킹 사건이 발생 – 해킹 사고로 인해 가상자산 탈취뿐 아니라 카카오가 운영하는 QR 체크인, 카카오맵 등 일부 서비스에서 1시간가량 오류가 발생하여 국민 일상생활에도 지장을 줌 • 솔라나(Solana) 크로스 체인 브릿지 서비스 웜홀 해킹 사건('22. 2.) – 솔라나와 이더리움을 연결하는 크로스체인 프로토콜 웜홀이 해킹되어 3억 2,400만 달러가 탈취 • 노마드(Nomad) 크로스 체인 브릿지 해킹 사건('22. 8.) – 미국 크로스 체인 기업 '노마드'가 해킹당해 1억 9천만 달러 이상의 가상자산이 탈취

출처) 각종 자료 참고

Ⅳ 블록체인 보안 및 대응 기술

블록체인 보안위협을 체계적으로 완화할 수 있는 기술 연구·개발 필요

블록체인 어플리케이션, 시스템, 네트워크 각 분야에서 보안성 검증에 활용할 수 있는 기술 필요

- 어플리케이션, 시스템, 네트워크 각 계층의 보안 위협은 전체 블록체인의 보안성까지 위협
- 각 계층별 고유한 특징 및 발생할 수 있는 보안위협 유형을 고려하여, 효과적인 보안 검증 기술 연구·개발 필요
- 블록체인 소프트웨어 개발 과정에서 연구·개발된 기술들을 활용함으로써 보안 내재화 가능
  - 시스템 개발 생명주기 및 단계별 공격 유형에 따라 자동화된 취약점 분석 도구, 라이브러리 등을 개발·보급
  - 어플리케이션 및 네트워크 보안성 검증 기술을 개발과정에 도입

[C1] 어플리케이션 보안 취약점 탐지 기술

- 스마트 계약 배포 이전에 계약 內 코드 등 취약점을 분석할 수 있는 기술 개발 필요
- 국내 연구진에 의해 스마트 계약에 존재하는 취약코드를 정확하게 탐지하는 VERISMART[21] 및 SMARTEST[22] 기술이 개발됨
  - VERISMART: 스마트 계약 안전성 검증에 유용한 트랜잭션 불변식(Invariant)을 자동으로 추론함으로써 계약 內 존재하는 취약점을 검출함과 동시에, 효율적인 불변식 생성을 통해 허위 경보율(False Positive)을 혁신적으로 낮춤(그림 14 참고)
  - 스마트 계약 취약점 탐지 시 검출률 100%, 탐지 정확도 99.5%를 보이며 기존 기술 대비 월등한 성능을

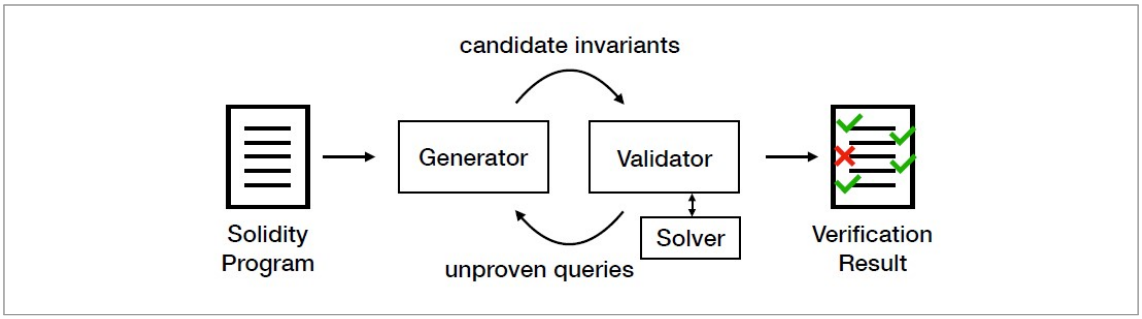
21 Sunbeom So, Myunho Lee, Jisu Park, Heejo Lee, Hakjoo Oh, “VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts”, IEEE Symposium on Security and Privacy, 2020. 5.

22 Sunbeom So, Seongjoon Hong, Hakjoo Oh, “SMARTEST: Effectively Hunting Vulnerable Transaction Sequences in Smart Contracts through Language Model-Guided Symbolic Execution”, USENIX Security, 2021. 8.

보임으로써, 블록체인 어플리케이션 보안으로 활용 가능[23]

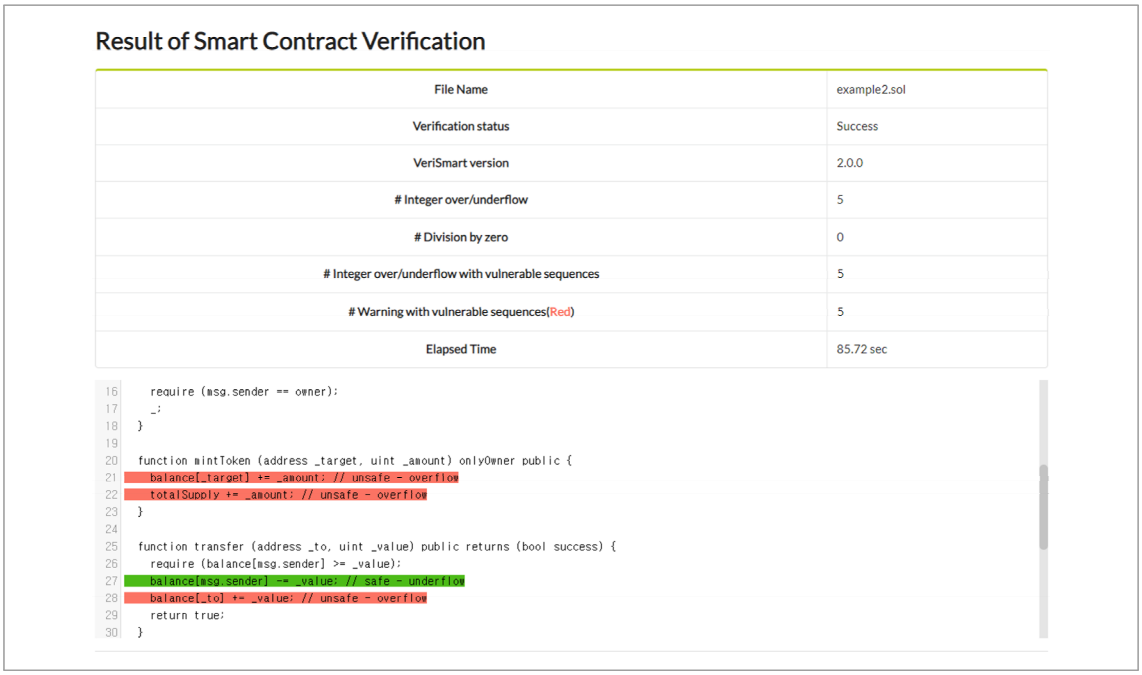
- SMARTEST: 스마트 계약의 취약한 트랜잭션 시퀀스(Transaction Sequence)를 식별해 냄으로써, 스마트 계약의 보안성 검증에 활용 가능
- VERISMART 및 SMARTEST는 누구나 사용할 수 있도록 오픈소스 플랫폼을 통해 제공[24] (그림 15 참고)

[그림 14] VERISMART 취약한 스마트 계약 탐지 알고리즘



출처) 소순범 외 4인, "VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts", 2020. 5.

[그림 15] VERISMART 스마트 계약 검증 결과(https://iotcube.net)



Result of Smart Contract Verification

File Name	example2.sol
Verification status	Success
VeriSmart version	2.0.0
# Integer over/underflow	5
# Division by zero	0
# Integer over/underflow with vulnerable sequences	5
# Warning with vulnerable sequences(Red)	5
Elapsed Time	85.72 sec

```
16    require (msg.sender == owner);
17    _;
18  }
19
20  function mintToken (address _target, uint _amount) onlyOwner public {
21    balance[_target] += _amount; // unsafe - overflow
22    totalSupply += _amount; // unsafe - overflow
23  }
24
25  function transfer (address _to, uint _value) public returns (bool success) {
26    require (balance[msg.sender] >= _value);
27    balance[msg.sender] -= _value; // safe - underflow
28    balance[_to] += _value; // unsafe - overflow
29    return true;
30  }
```

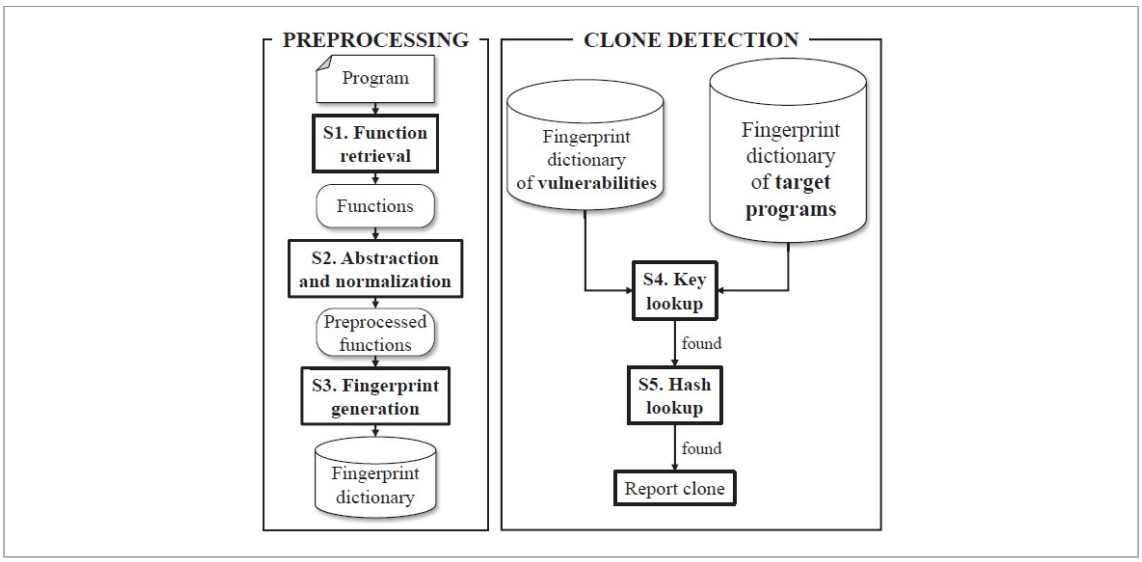
출처) 고려대학교 컴퓨터보안연구실

23 Metro, "고려대, '스마트 계약' 보안 취약점 잡아 오픈소스로 공개", 2020. 6.
24 IoTcube, "Security Experts are Always with You", 2022.

[C2] 시스템 보안 취약점 탐지 기술

- 코드 재사용으로 인해 전파된 취약점을 정확하게 탐지할 수 있는 기술 개발 필요
  - 블록체인 시스템에는 재사용한 코드 클론(복제된 코드)이 다수 존재하여, 하나의 시스템에서 발생한 취약점이 다른 시스템으로 전파될 가능성이 큼
  - 일부 취약점은 전파과정에서 코드의 형상이 수정되어, 현재까지 발견되지 않은 채 숨어있는 경우 다수 존재
- 전파된 취약한 코드 클론을 정확하게 탐지하는 VUDDY[25] 및 MOVERY[26] 기술이 개발됨
  - VUDDY: 전파된 취약점을 확장·탐지하기 위한 함수 기반 기술(오픈 플랫폼을 통해 제공, 그림 16 참고)
  - 취약 함수와 구문이 유사한 함수가 시스템에 존재 여부를 식별함으로써 취약 코드 클론을 탐지. 특히 확장성을 고려한 설계로 수천만 라인의 소프트웨어도 수 초 만에 전파된 취약점을 탐지[27] (그림 17 참고)
  - MOVERY: 코드 수정과 함께 전파된 취약 코드 클론을 정확하게 탐지하기 위한 기술(추후 공개 예정)
  - 기존 기술 대비 6배 이상 많은 취약점을 훨씬 높은 정확도(96% 정밀도 및 96% 재현율)로 탐지 가능하여, 시스템에서 전파된 취약점을 탐지하는데, 효율적으로 활용 가능[28]

[그림 16] VUDDY 취약점 탐지 알고리즘



출처) 김슬배 외 3인, "VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery", 2017. 5.

25 Seulbae Kim, Seunghoon Woo, Heejo Lee, Hakjoo Oh, "VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery", IEEE Symposium on Security and Privacy, 2017. 5.
26 Seunghoon Woo, Hyunji Hong, Eunjin Choi, Heejo Lee, "MOVERY: A Precise Approach for Modified Vulnerable Code Clone Discovery from Modified Open-Source Software Components", USENIX Security, 2022, 8.
27 VERITAS, "고려대, '재사용 코드'자동 탐지 기술 개발", 2017. 5.
28 전자신문, "이희조 고려대 교수팀, 취약 코드 탐지 MOVERY 기술 개발", 2022. 9.

[그림 17] VUDDY 취약 코드 재사용 탐지 결과(https://iotcube.net)

출처) 고려대학교 컴퓨터보안연구실

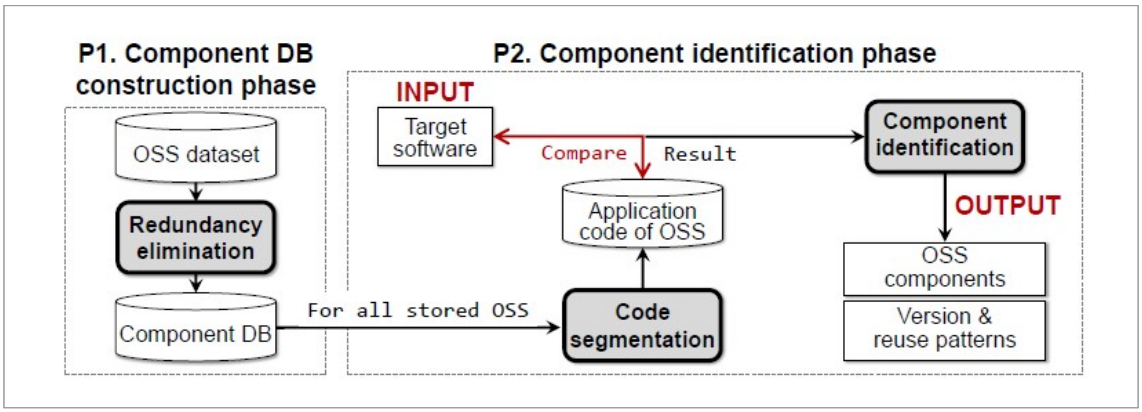
[C2] 시스템 오픈소스 구성요소 분석 기술

- 소프트웨어 개발 환경에서 오픈소스 소프트웨어를 활용하는 것은 투명성을 보장하며 혁신적인 개발을 위한 필수적인 요소
  - 오픈소스 소프트웨어 재사용은 개발 과정의 효율성을 높이고 개발 시간을 단축하지만, 꾸준한 관리가 수반되지 않은 오픈소스 소프트웨어 재사용은 보안 위협을 야기
  - 취약한 오픈소스 소프트웨어 구성요소로 인한 보안 위협을 완화하기 위한 소프트웨어 구성요소 분석 기술 연구·개발 및 이를 블록체인 도메인에 적용하는 방안 필요
- 오픈소스 구성요소를 정확하게 식별할 수 있는 기술인 CENTRIS[29]가 개발됨
  - 오픈소스 소프트웨어의 95%는 코드 및 구조 수정과 함께 재사용되기 때문에 정확하게 식별하기 어려움
  - CENTRIS: 각 오픈소스 소프트웨어의 고유한 코드만을 추출한 후, 이를 타겟 프로그램과 비교함으로써 정확하게 오픈소스 구성요소를 식별 가능(그림 18 참고)

29 Seunghoon Woo, Sunghan Park, Seulbae Kim, Heejo Lee, Hakjoo Oh, "CENTRIS: A Precise and Scalable Approach for Identifying Modified Open-Source Software Reuse", International Conference on Software Engineering, 2021. 5.

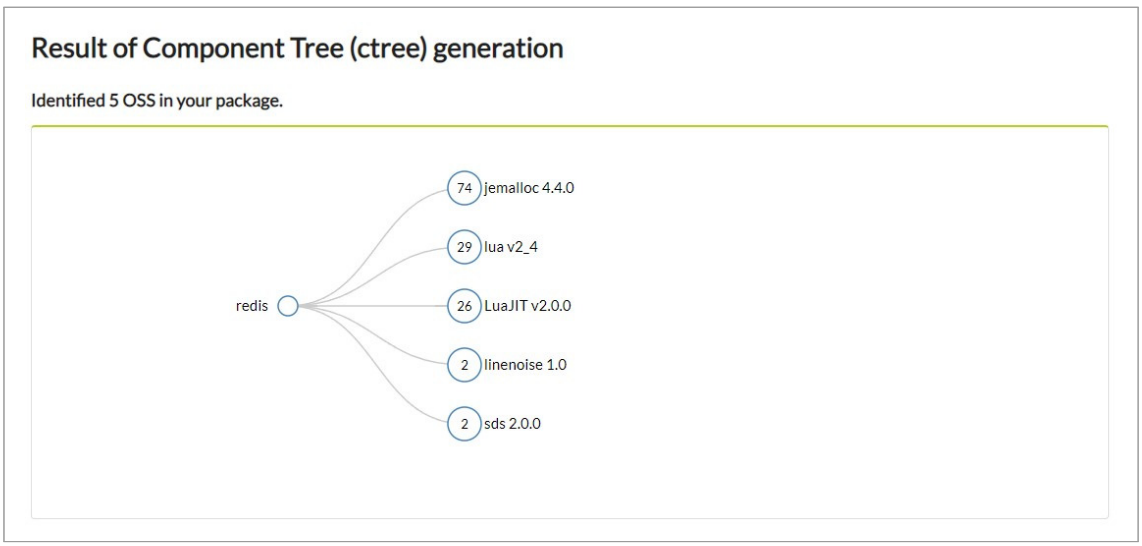
- CENTRIS 분석을 통해, 비트코인 등 가상자산들이 평균 10개 이상의 오픈소스 구성요소를 재사용하고 있으며, 업데이트가 10년 이상 안 된 구성요소들도 최신 버전의 블록체인 소프트웨어에서 사용됨을 확인
- 특히 수정된 오픈소스 구성요소까지도 높은 정확도(91% 정밀도 및 94% 재현율)로 식별이 가능하여, 오픈소스 재사용으로 인해 발생하는 보안위협(예: 공급망 공격)을 완화하는데 활용 가능[30]
- CENTRIS는 오픈소스 플랫폼을 통해 제공(그림 19 참고)

[그림 18] CENTRIS 오픈소스 구성요소 식별 알고리즘



출처) 고려대학교 컴퓨터보안연구실

[그림 19] CENTRIS 오픈소스 구성요소 식별 결과(https://iotcube.net)



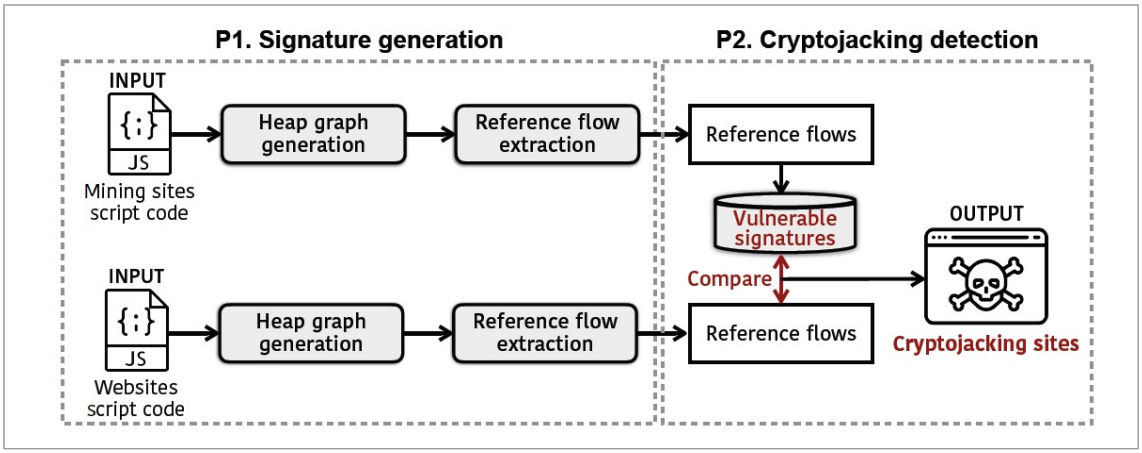
출처) 고려대학교 컴퓨터보안연구실

30 보안뉴스, "오픈소스 커뮤니티 노리는 공급망 공격, 국내 연구팀 기술로 차단한다", 2021. 3.

[C3] 차세대 네트워크 보안 기술

- 블록체인 네트워크의 보안위협(예: BGP 하이재킹) 완화 필요
  - 기존 인터넷 인프라를 대체할 수 있는 새로운 기술이 네트워크 보안의 해결책이 될 수 있음
- 기존 네트워크의 문제를 해결하고 신뢰성·가용성을 보장하는 차세대 네트워크를 연구·개발하는 시도가 전 세계적으로 진행 중
  - 스위스 연방공대(ETH) Adrian Perrig 교수 연구팀에서 개발한 SCION(Scalability, Control, and Isolation On Next-Generation Networks)은 멀티패스 라우팅을 통해 높은 가용성을 보장하고 효율적인 통신을 할 수 있는 차세대 네트워크 기술임[31]
  - 소프트웨어 정의 네트워킹(SDN) 기술은 네트워크의 제어 평면과 데이터 평면을 분리하여 이용자가 직접 프로그래밍 가능한 인프라를 만들 수 있는 기술로, 기존 네트워크 인프라를 개선 가능
- 크립토재킹을 탐지하기 위한 기술인 CIRCUIT이 개발됨[32]
  - CIRCUIT: 자바스크립트 메모리 힙(Heap) 그래프를 기반으로, 자바스크립트 코드가 난독화 되어있는 상황에서도 정확하게 크립토재킹을 탐지하는 기술(그림 20 참고)
  - 크립토재킹 된 웹사이트의 자바스크립트 메모리 힙 그래프로부터 크립토재킹의 시그니처(Signature)를 생성하고, 해당 시그니처가 포함되어있는 웹 사이트를 식별함으로써, 크립토재킹을 탐지
  - CIRCUIT을 통해 현재 운용되고 있는 30만 개의 웹 사이트에서 1,813개의 크립토재킹 웹 사이트를 탐지

[그림 20] CIRCUIT의 크립토재킹 탐지 알고리즘



출처) 고려대학교 컴퓨터보안연구실

31 Xin Zhang, Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, David G Andersen, "SCION: Scalability, control, and isolation on next-generation networks", IEEE Symposium on Security and Privacy, 2011. 5.

32 Hyunji Hong, Seunghoon Woo, Sunghan Park, Jeongwook Lee, Heejo Lee, "Circuit: A JavaScript Memory Heap-Based Approach for Precisely Detecting Cryptojacking Websites", IEEE ACCESS, 2022. 9.

V

시사점 및 정책 제언

웹 3.0 패러다임 전환의 핵심기술 블록체인은 기술 한계 극복을 위한 지속적인 노력과 수용성 제고 필요

웹 2.0의 다양한 문제점이 웹 3.0 전환의 동인이 되고 있으나 경제·사회 전반의 공감대 형성은 조금 더 시간이 걸릴 것으로 보임

- 현재 진행되고 있는 웹 3.0 패러다임 논의는 대부분 블록체인 산업계가 주도하고 있는 상황으로 전환에 대한 공감대 형성이 매우 제한적이라고 볼 수 있음
  - 특히, 웹 패러다임 변화는 단순히 보다 더 진화된 기술의 적용이 아닌 네트워크, 디바이스, 서비스 등을 비롯한 전후방 파급효과가 큰 만큼 이해관계가 복잡한 상황
  - 따라서, 블록체인 기술이 웹 패러다임을 주도할 수 있는 수준으로 고도화 되고 AI, 메타버스 등 다른 기술을 포용해야 할 것으로 보임
- 또한, 패러다임 전환의 동인이 데이터 주권확보, 개인정보보호 등으로 이용자 측면이 강한 만큼 블록체인의 기술적 우위는 있으나 대안기술이 없는 것은 아님
  - 그동안 블록체인 기술은 가상자산, DeFi, NFT 등 디지털 경제적 이미지가 강하였으나, 사회 전반적으로 통용되는 일반화 과정을 거쳐야 미래사회의 주도 기술로 자리 잡을 수 있을 것으로 전망

블록체인 기반의 신뢰 사회 구현을 위해 서비스에 대한 안전성 검증 및 다양한 보안위협 대비 필요

신뢰성, 보안성, 투명성, 탈중앙성의 장점으로 인해 블록체인은 다양한 산업 분야에 기반 기술로 널리 활용될 것으로 보이나, 보안위협에 대한 대비는 여전히 부족

- 블록체인은 금융기관, 의료기관, 물류 유통 등 여러 분야에서 분산화 된 방식으로 정보를 검증·

저장·실행함으로써 중개자 없이도 신뢰를 보장할 수 있기 때문에 향후 활용이 더욱 확산될 것으로 예상

- 다양하고 새로운 블록체인 서비스가 출시될 것으로 예상됨에 따라 안전성 검증의 중요도는 앞으로 더욱 커질 것으로 예측됨

• 하지만, 블록체인 시스템의 안전성은 단순히 연결된 암호화 해시체인(Hash Chain)이나 전자서명(PKI), 혹은 콜드 월렛(Cold Wallet)과 같은 몇 가지 단편적인 기술만으로 보장할 수 없음

- 블록체인 공급자 관점에서 시스템, 기기·인프라, 데이터, 네트워크에 대한 안전성 검증이 필요하며, 이용자 관점에서 서비스 사용 시 발생할 수 있는 보안 이슈에 대한 대비 필요

• 블록체인 시스템의 안전성을 검증하고 평가하기 위한 정책적 지원 필요

- 보안 내재화: 시스템 요구사항 분석 및 설계 단계에서부터 블록체인 기술의 실제 운영 단계까지 전체적으로 블록체인 안전성 검증 필요
- 정책적 지원: 보안 내재화를 위한 전문 컨설팅 지원, 블록체인 암호기술 가이드라인을 통한 안전성 검증 등 블록체인 기반 신뢰 사회 구현을 위한 정책적인 지원 필요

블록체인 서비스의 보안 내재화 및 암호기술 가이드라인 준수를 통한 보안성 향상

블록체인 소프트웨어 개발 업체의 보안 내재화 활성화를 위한 취약점 분석 기술 연구·개발 및 정책적 지원 요구

• 블록체인 보안 취약점 자동분석 기술을 지속 연구·개발하고 이를 활용하여 소프트웨어 개발 업체의 보안 내재화 활성화 필요

- 시스템 개발의 생명주기 및 단계별 공격 유형에 따라 블록체인 서비스 보안성 향상을 위한 취약점 분석 도구와 개발 지원 라이브러리 등을 제공함으로써, 개발 전 단계에서 블록체인 시스템 안전성 강화
- DevSecOps 및 S-SDLC 등 개발 생명주기 관리를 통해 소프트웨어 개발 단계에서부터 보안 고려
- SW 재료명세서(Software Bill of Materials, SBOM)를 통해 제3자 구성요소를 관리할 수 있음

• 보안 컨설팅, 검증 기술·도구 확산 등 보안 내재화 활성화를 위한 추가적인 정책 지원 필요

블록체인 시스템의 안전성 검증을 위한 암호기술 가이드라인 준수 요구

• 블록체인 시스템·서비스 관련 이해관계자들이 '블록체인 암호기술 가이드라인(국가정보원, '20. 12.)'을 준수하도록 촉진 필요

- 국가 공공기관의 블록체인 기술 도입을 위한 암호 안전성 기준 제시(관계부처 합동, '블록체인 기술 확산 전략'('20. 6.)에 포함)
- 주요내용: 암호 알고리즘, 계정 관리, 데이터 전송 보안 등 17개 항목에 대한 안전성 기준 및 준수 방안 제시
- 범위: 암호와 관련이 있는 안전성 중심 및 허가형 블록체인 기준으로 작성, 성숙도가 미비한 최신 기술 배제
- 블록체인의 안전한 활용을 위해 기본적으로 '블록체인 암호기술 가이드라인'의 준용 여부의 시험 필요 (한국정보통신기술협회에서 가이드라인의 평가방법론을 개발하여, 시험 서비스를 운영 중)

KISA INSIGHT

DIGITAL & SECURITY POLICY

2023 VOL. 2

Web 3.0 시대 핵심 기술, 블록체인 보안 위협 전망 및 분석

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY