

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

WEF, 중앙은행 디지털 화폐(CBDC)의 양자 컴퓨터 공격 취약성 경고

- 전 세계 중앙은행 98%가 CBDC 검토...CBDC, 데이터 이동 많아 양자컴퓨팅 사이버보안 위협에 취약
- WEF, '30년까지 5,000대 양자컴퓨터 상용화 전망...CBDC 핵심 인프라의 방어 대책 수립 필요성 강조

세계경제포럼(WEF)이 중앙은행 디지털화폐(CBDC)가 양자컴퓨팅을 활용한 사이버 공격에 취약할 수 있다고 경고하고, CBDC 시스템에 암호화 민첩성을 내장해 위협에 대비해야 한다고 권고

▶ 양자컴퓨팅, 공공 키 암호화 표준 무력화 우려 증대...암호화 민첩성 내장한 양자 내성 시스템 구축 필요

- WEF는 양자컴퓨팅(Quantum computing)*이 데이터 집약적 업무를 파괴적 수준으로 혁신할 잠재력을 가졌지만, 이동 데이터를 보호하는 암호화 기술을 깨뜨릴 수 있어 새로운 위협으로 작용한다고 지적
* 다차원 상태로 존재할 수 있는 양자비트(qubits)를 사용하여 금융 포트폴리오 최적화나 신약 발견과 같은 복잡한 문제를 기존 슈퍼컴퓨터보다 더 빠르게 해결할 수 있음
- WEF 금융서비스 기술·혁신 부문 드루 프로프슨(Drew Propson) 대표는 전 세계 금융 시스템이 점점 더 밀접하게 연결됨에 따라, 금융 시스템에 대한 신기술 위협은 매우 복잡하게 나타난다고 지적하고, 가짜 뉴스, 딥페이크, 사기 탐지 SW의 식별력 하락 등을 사례로 제시
- 전 세계 중앙은행이 CBDC 도입을 추진하면서 양자컴퓨팅, AI 등 신기술을 이용해 CBDC 인프라 시스템의 취약점을 노리는 악의적 공격자의 등장이 사이버 위협을 더욱 가중한다고 지적
- CBDC 인프라 시스템은 국가 간 결제 효율성을 개선하고 금융 시스템에 대한 접근성 확대를 목표로 여러 주체(Entity)에서 가져온 거래 데이터를 암호화 저장으로 구현되고 있어 다양한 이해 관계자의 참여가 필수
- 다양한 이해 관계자가 존재하는 만큼 악의적 공격자가 공격할 수 있는 접점도 늘어나는 보안 위협이 존재하며, 시스템 특성상 특정 참여 기관의 보안 취약점이 국가 결제 시스템과 글로벌 거래에 악영향을 미칠 수 있음
- 양자컴퓨팅 기술이 빠르게 발전하면서 공개 키 암호화 표준 기반의 현 암호화 기술이 무력화될 수 있다는 우려가 커지고 있으며, 언제 닥칠지 모르는 양자컴퓨팅 상용화에 대한 대비가 필요하다는 지적이 제기됨
- WEF는 CBDC 인프라를 노리는 양자컴퓨팅 사이버 공격에 대해 해당 CBDC 시스템에 암호화 민첩성(cryptographic agility)*을 내장해 양자컴퓨팅 내성(quantum-resistant) 시스템 구현을 권고
* 애플리케이션을 다시 작성하거나 새로운 하드웨어 시스템을 배포할 필요 없이 업계 표준에 따라 보안 하드웨어가 새로운 알고리즘으로 변경할 수 있는 기능

▶ 전 세계 중앙은행 98%가 CBDC 검토...CBDC, 데이터 이동 많아 양자컴퓨팅 사이버보안 위협에 취약

- **(CBDC 현황)** 전 세계 중앙은행의 98% 이상이 국경 간 결제 효율성 개선과 금융 포용성 강화를 목적으로 CBDC를 검토하고 있으며, 이를 통해 차세대 금융시장에서 중앙은행 화폐 역할 유지를 모색

- BIS는 '23년 7월 CBDC 및 암호화폐 관련 보고서*에서 대부분 중앙은행이 소매 CBDC와 빠른 국경 간 결제를 지원하는 도매 CBDC를 모두 보유하는 것이 잠재적 가치가 크다고 판단하며, '30년에는 15개의 소매 CBDC와 9개의 도매 CBDC가 등장할 것으로 예측

* BIS, Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto, 2023.07

[CBDC를 고려하는 글로벌 중앙은행 추이(2024년 3월 기준)]



출처 : Atlantic Council, CBDC tracker(<https://www.atlanticcouncil.org/cbdctracker/>)

- **(양자컴퓨팅 현황)** 양자컴퓨팅 시장은 2025년까지 1조 3,000억 달러 규모를 이룰 것으로 전망되며, IBM을 비롯한 주요 민간기업은 대규모로 작동할 수 있는 확장 가능한 양자컴퓨팅 구축을 추진하고 있음
 - 글로벌 컨설팅 기업 매켄지는 '24년 5월 양자컴퓨팅 보고서*를 발표하고, 금융, 화학, 생명 과학, 모빌리티 등 4개 산업이 양자컴퓨팅의 영향을 가장 크게 받고, '35년까지 최대 2조 달러 규모의 시장 형성을 전망
- * McKinsey, Quantum Technology Monitor, 2024.05

[매켄지의 양자컴퓨팅 시장 전망(2024년 5월)]



출처 : McKinsey, Quantum Technology Monitor, 2024.05

- **(양자컴퓨팅 보안 위협)** WEF는 악의적 공격자가 양자컴퓨팅 기술을 사용해 CBDC 핵심 시스템의 공개키 암호화 메커니즘을 깨뜨릴 수 있다고 평가
- 양자컴퓨팅은 금융 시스템에서 널리 사용하는 RSA* 및 타원곡선 암호화(ECC)**와 같은 이동 암호화 표준을 해독할 수 있어 새로운 보안 위협으로 간주함

- * Rivest-Shamir-Adleman(RSA) : 보안 데이터 전송에 널리 사용되는 공개키 암호화 시스템으로 공개 키를 통해 누구나 암호화할 수 있지만, 개인 키를 아는 사람만 해독할 수 있도록 구현
- ** Elliptic Curve Cryptography(ECC) : 타원 곡선의 수학적 속성을 사용한 공개 키 암호화 시스템으로 한 방향으로 계산하기는 간단하지만 되돌리기는 매우 어려운 수학 함수를 기반으로 함

- 특히 CBDC와 RTGS* 시스템과 같은 국가 간 결제 시스템은 다양한 고객, 거래 및 시장 데이터의 이동이 불가피해 양자컴퓨팅 위협에 취약하다고 진단

- * 실시간 총액 결제(Real-Time Gross Settlement) : 한 은행에서 다른 은행으로 송금이 실시간으로 총액 기준으로 이루어지는 유형의 결제로 결제 위험을 줄이기 위해 대기 기간 없이 즉시 결제로 구현함

▶ 양자컴퓨팅 사이버보안 위협, ①네트워크 가로채기 ②신원 사칭 ③선취득/후해독 등 3가지 유형이 대표적

- WEF는 악의적 공격자는 양자컴퓨팅 기술을 이용해 CBDC 시스템의 네트워크 통신을 가로채 금융 자산 약탈에 나서고, 크게 3가지 방법이 주로 사용된다고 설명
- (네트워크 가로채기) 네트워크 및 무선 통신을 통해 전송되는 정보를 가로채는 방식
- (신원 사칭) 온라인에서 개인 사칭으로 인증 확인을 무력화하고, 권한 요구 작업을 수행하는 방식
- (선취득/후해독) 현재 이동하는 암호화된 데이터를 가로채서 저장했다가, 추후 양자컴퓨팅이 실용화되면 해독해 금융 자산을 약탈하는 방식

- WEF는 양자컴퓨팅 상용화되기 전이라고 여기고 위협의 심각성을 과소평가해서는 안 된다고 경고

- 허드슨 연구소의 '21년 연구*에 따르면, 이론적으로 미국 RTGS 시스템(페드와이어 펀드 서비스**)에 양자컴퓨팅 공격이 발생할 경우, 실질 GDP가 10~17% 감소하고 6개월간 경기 침체와 수조 달러의 간접 손실이 발생하는 것으로 나타남

- * Hudson Institute, Prosperity at Risk: The Quantum Computer Threat to the US Financial System, 2023.4

- ** Fedwire Funds Services : 미국 연방준비은행이 제공하는 실시간 총액 결제 시스템으로 지정 공휴일을 제외한 월요일부터 금요일까지 서비스를 제공하며 시간이 촉박한 고객 결제에 주로 사용됨

▶ 암호화 민첩성을 내재한 CBDC 시스템, 양자컴퓨팅의 사이버보안 위협 대안으로 권고

- WEF는 2030년까지 약 5,000대의 양자 컴퓨터가 운영될 것으로 예측하고, 양자컴퓨팅으로부터 핵심 인프라를 방어하는 대책 마련이 점점 중요해지고 있다고 강조
- WEF는 암호화 민첩성을 핵심 개념으로 제시하고, 이를 실시간 위협에 따라 암호화 알고리즘을 쉽게 조율 및 교체해 각종 공격 기술을 차단할 수 있는 능력으로 정의

- 암호화 민첩성 구현으로 현 비대칭 암호화를 보완할 수 있다고 강조하고, 가령, RSA 및 ECC를 ▲모듈-격자 기반 캡슐화 방식(ML-KEM/Kyber)* ▲모듈-격자 기반 디지털 서명 알고리즘 (ML-DSA**/ Dilithium) ▲무 상태 해시 기반 디지털 서명 알고리즘(SLH-DSA/SPHINCS+) 등의 격자 기반 알고리즘으로 보완을 조언

- * Key encapsulation mechanism(KEM) : 비대칭 알고리즘을 사용하여 데이터 전송에서 대칭 키를 보호하도록 설계된 암호화 프로토콜로, 통신 프로토콜을 외부 공격으로부터 보호할 수 있음

- ** Digital signature algorithm(DSA) : 전자 서명을 생성하고 검증하는 비대칭 암호화 알고리즘으로, 각 시스템에서 신원을 보호함

- CBDC 시스템의 ▲네트워크 ▲애플리케이션 ▲데이터 흐름(Data Flow) ▲코드 4개 계층에 KEM과 DSA를

구현해 양자컴퓨팅 3대 위협을 완화할 수 있음

▶ **CBDC 시스템 설계 및 구축에서 양자컴퓨팅 내성 전략 수립 필요, 정부의 적극적인 역할 주문**

- WEF는 CBDC 설계 및 구축에서 양자컴퓨팅 보안 위협을 충분히 고려한 내성 전략 수립을 권고하고, 이와 관련된 5가지 고려 사항을 제시
- **(고려 1)** 새로운 위협을 충분히 고려해 양자 보안 위험 분석을 수행하고 대응 역량을 결정
- **(고려 2)** 정기 업그레이드를 위해 시스템 내 관련 암호화 메커니즘 목록을 구축하는 암호화 자재 목록 (CBOM)을 작성
 - * Cryptographic Bill Of Materials : 암호화 자산과 해당 종속성을 설명하는 개체 모델로 소프트웨어 자재 명세서(SBOM)의 사이버 공급망 표준(CycloneDX)의 확장으로서 암호화 자산을 모형화하는 개념이 포함됨
- **(고려 3)** 모바일 단말기 등 네트워크 엔드 포인트 보호를 위해 CBDC 시스템에 대한 접근 권한이 부여된 기관에 엄격한 사이버 복원력 조치를 부과
- **(고려 4)** 네트워크 및 애플리케이션 수준에서 트래픽을 캡슐화하고 소프트웨어 개발 라이프사이클에 특정 라이브러리 사용을 포함해 안전하고 민첩한 애플리케이션 개발을 촉진
- **(고려 5)** DLT 기반일 경우, 데이터 스토리지를 여러 데이터 센터 또는 노드에 공유하여 데이터 이중화를 구현하고, 양자컴퓨팅 보안 위협을 보장할 수 있는 배포된 키 관련 예방 조치 수행

▶ **양자컴퓨팅 보안 강화를 위한 글로벌 움직임 활발..BIS, 암호화 민첩성 구현 프로젝트 결과 공개**

- WEF는 CBDC를 포함한 차세대 국가 결제 시스템을 각종 사이버 위협으로부터 안전하기 보호하기 위한 국제적인 노력이 활발하게 전개됨을 강조하고, 적극적인 관심과 참여를 권고
- (WEF) '24년 1월 양자 경제 네트워크(Quantum Economy Network)를 구성해 금융 부문을 위한 글로벌 규제 접근 방식에 관한 지침*을 발표('24.1)
 - * Quantum Security for the Financial Sector: Informing Global Regulatory Approaches : 백서는 민간기업과 규제 당국에 양자 보안에 대해 협력적이고 조화로운 접근을 보장하는 지침을 제공
- (BIS) '24년 1월 양자컴퓨팅 사이버 위협을 테스트한 리프 프로젝트(Project Leal) 첫 번째 결과 보고서를 발표하고, 암호화 민첩성 개념 구현이 가능함을 증명
- WEF는 중앙은행 CBDC 구축에서 양자컴퓨팅 보안 위협을 해소하기 위해서는 암호화 민첩성 개념이 핵심이며, 이를 위해 공공 및 민간 협력을 통한 사이버 본원력 구현이 필수라고 강조

- WEF가 '30년까지 약 5,000대의 양자 컴퓨터가 운영될 것으로 예측하고, 양자컴퓨팅에 취약한 CBDC 인프라를 방어하는 대책 마련이 점점 중요해지고 있다고 강조
- WEF는 CBDC 설계 및 구축에서 양자컴퓨팅 보안 위협을 충분히 고려한 암호화 민첩성을 중심으로 한 내성 전략 수립을 강조하고, 이와 관련된 글로벌 활동에 적극적인 참여와 관심이 요구된다고 권고

[출처]

- WEF, 'Safeguarding central bank digital currency systems in the post-quantum computing age' 2024.05.21.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

블록체인, 고객 신원 확인(KYC) 데이터 보안 기술로 주목

- 크립토뉴스(Cryptonews)는 블록체인이 '고객 신원 확인(Know Your Customer, KYC)' 솔루션 시장에서 개인정보와 이용자 데이터 보안 기술로 주목받는 배경과 최근 동향 및 주요 사례들을 보도

블록체인 전문매체 크립토뉴스가 고객 신원 확인(KYC) 시장 현황을 진단하고, '재사용 가능한(reusable)' KYC 솔루션 시장 성장에 블록체인이 기여할 수 있는 이유와 주요 기업 사례가 포함된 이슈 분석 기사를 게재

▶ 딥페이크 같은 인공지능(AI) 기술을 활용한 사기 증가와 신원(identity) 관련 컴플라이언스 관리가 매우 중요해진 시점에서 KYC 솔루션 시장이 급성장할 것으로 전망되나, 문제점도 존재

- 시장조사업체 Grand View Research는 준법 경영에 대한 중요성과 금융기관 신원 관련 사기 증가로 '21년 29.3억 달러이던 KYC 소프트웨어 시장 규모가 향후 6년간 연평균 20.8%로 성장할 것으로 전망
- 그러나 KYC를 요구하는 기업과 금융기관들이 늘어나면서, 이용자들은 신분증 및 사진 제출 같은 개인 정보 노출이 수반되는 동일하고 반복되는 KYC 본인 확인 인증 과정에 직면
- 이와 관련, 디지털 신원 확인 스타트업 트린식(Trinsic)의 라일리 휴즈(Riley Hughes) 대표는 한 사람이 여러 앱과 플랫폼에서 10번 정도 KYC를 요청받을 가능성이 있으며, 실물 신분증 제출을 요구받을 경우 40%는 거부한다고 지적
- 블록체인 기술 기업 치아 네트워크(Chia Network)의 비샬 카푸어(Vishal Kapoor) 최고운영책임자는 크립토뉴스와의 인터뷰에서 기업 입장에서 KYC를 구현하는데 비용 부담이 상당하다고 분석*
- * Beta News의 최근 보도에 의하면, 기업의 KYC 관련 비용이 전체 자금세탁방지(Anti Money Laundering, AML) 규정 준수 비용의 40%에 달하며, 은행의 경우 연간 총 570만 달러에 육박

▶ 여러 플랫폼에서 반복 인증할 필요 없이 한 번으로 고객 신원 확인 절차를 간소화시킬 수 있는 재사용 가능한(resuable) KYC 솔루션이 대안으로 부상

- 신원인증 SW 기업 트린식의 라일리 휴즈 대표는 재사용 가능한 KYC 솔루션이 반복된 인증에 따른 이용자 불편과 인증에 소요되는 시간을 절감시켜 준다고 평가
- 또한 실제로 자사가 재활용 가능한 KYC를 기반으로 '신원 수용 네트워크(identity acceptance network)'를 출시했고, 이를 통해 10배 빠른 고객 신원 확인 절차가 가능해지고 사기 피해를 줄일 수 있다고 평가
- 휴즈 대표에 의하면, 트린식은 주요 공항에서 생체인식 방식으로 여행 서류를 검수하는 기술 기업인 클리어(CLEAR)를 포함해 다수 업체들과 신원 수용 네트워크 참여를 위한 파트너십을 체결
- 휴즈 대표는 "이용자가 당사 신원 수용 네트워크에 참여 중인 기업에서 한번 인증을 받은 경우, 네트워크에 참여한 다른 기업·플랫폼에서 다시 받을 필요 없이 기존 인증을 활용할 수 있다"고 설명
- 가령, 클리어 서비스 이용 고객이 신원 수용 네트워크에 참여하는 다른 기업들의 플랫폼을 이용하고자

할 경우, 새롭게 KYC를 거칠 필요 없이 클리어에서 받은 KYC 인증을 재활용 가능

[트린식의 재활용 KYC 기반 신원 수용 네트워크 개념도]



출처 : Trinsic

▶ 재활용 가능한 KYC에 블록체인 기술을 접목시, 이용자 개인 정보와 데이터 보안 강화

- 신원 확인 기술 업체이자, 트린식의 신원 수용 네트워크에 참여하고 있는 덴티티(Dentity)는 KYC를 위한 이용자 자격 증명을 비트코인 블록체인에 저장한다고 언급
- 덴티티의 제프리 슈워츠(Jeffrey Schwartz) 대표는 크립토뉴스와의 인터뷰에서 “우리는 발급자 진위를 확인하기 위해 탈중앙화된 식별자(decentralized identifiers, DID)를 온체인에 저장한다”고 언급
- 블록체인 기술 기업 치아 네트워크의 비살 카푸어(Vishal Kapoor) 최고운영책임자(COO)도 KYC 제공 업체가 검증 가능한 자격증명 토큰을 온체인에서 발행하여 KYC를 수행할 수 있도록 하고 있다고 설명
- 카푸어 COO는 “서비스 업체들은 사용자를 대상으로 개인 정보 공개를 요구하지 않고도, 신뢰할 수 있는 KYC 제공자를 통해 사용자가 KYC 검증을 거쳤는지 확인할 수 있다”고 언급
- 또한 신원 관련 사기가 증가하고 개인정보 보호에 대한 관심과 수요가 높아지고 있는데,* 블록체인이 민감한 개인 정보를 보호하고, 외부 접점을 최소화시키는 대안이 될 수 있다고 평가
- * 보안 업체 Panda Security는 '20년 3월 이후 전 세계적으로 100억 건 이상의 개인 기록이 노출되었다고 집계
- 카푸어 COO는 온체인에서 VC(verifiable credentials)와 DID(decentralized identifiers)를 사용하면 데이터 노출 위험 없이 자신의 VC를 보관하고 누구에게 공유할지 또는 공유해야 할지 결정 가능하다고 설명

▶ 재활용 가능한 KYC에 대한 사이버보안 위험이 증가함에 따라 온체인 데이터 저장이 대안으로 부상

- 재활용 가능한 KYC가 이용자의 본인 확인 과정상 불편함을 해소시켜 준다는 점에서 주목받고 있지만, 사이버보안 위험 대응을 포함해 여러 측면에서 선결 과제도 존재
- '24년 2월 로이터(Reuters) 통신은 사이버 범죄자들이 여전히 자동화된 KYC 확인(automated KYC checks)을 빠르게 악용하여 사용자 정보를 위험에 빠뜨릴 수 있다고 지적*
- * Reuters, KYC Update: Firms marketing super-fast customer on-boarding are vulnerable to account-opening, mule attacks, 2024.02.08
- 이에 따라, 온체인 데이터 저장이 재활용 가능한 KYC 관련 이용자 데이터 보안을 강화하는 대안으로 부상하고 있으며, 블록체인 기술을 KYC 자격 증명에 활용하려는 사례들이 등장

- 실제 딜로이트 스위스(Deloitte Switzerland)가 탈중앙화 전문 기업과 협력해 '23년부터 디지털 자산의 글로벌 자금 조달을 위해 재활용 가능한 KYC 자격 증명을 발급하기 시작한 것이 대표적 사례
- 구체적으로 딜로이트는 블록체인 플랫폼 폴카닷(Polkadot)을 기반으로 하는 탈중앙화 펀딩 프로토콜인 폴리멕(Polimec)을 활용하여 재활용 가능한 KYC 자격 증명 발급 기능을 구현
- 폴리멕의 루카 폰 뷔텐바흐(Luca von Wyttenbach) 공동 창업자는 크립토뉴스와의 인터뷰에서 딜로이트가 KYC 자격 증명을 발급하고 사용자가 이를 관리하면서 다양한 온라인 서비스에서 활용할 수 있다고 설명
- 또한 폴리멕 기반 KYC 자격 증명을 통해 이용자는 디지털 본인 주권 신원(digital self-sovereign identity)을 확립하고, 웹사이트나 서비스 업체들도 공유된 KYC 데이터를 신뢰할 수 있게 된다고 설명

▶ 재활용 가능한 KYC 채택 확산과 보다 안전한 데이터 보안이 시장 확산의 선결과제

- 현재 블록체인 기술 기반의 재활용 가능한 KYC 솔루션들이 실제 활용되는 사례들이 있으나, 시장 확산을 위한 선결 과제도 남아있다는 지적 제기
- 탈중앙화된 신원 플랫폼인 아이도스 네트워크(idOS Network)의 공동 설립자인 올리안 라이틀로프(Julian Leitloff)는 무엇보다도 이용자와 서비스 제공업체들이 재사용 가능한 KYC 솔루션을 도입하도록 유도하는 것이 최대 당면 과제라고 지적
- 또한 재활용 가능한 KYC에서 개인정보 보호와 데이터 보안을 보장하려는 노력이 강화되고, 표준화된 신원 형식 장려를 통해 상호운용성을 보장하는 것이 중요하다는 견해도 존재
- 라이틀로프는 재활용 가능한 KYC가 여러 플랫폼에서 공유되는 경우에도 이용자 데이터와 개인 정보에 대한 보안이 유지되어야 하며, 자사의 경우 고급 암호화 기술로 이용자 데이터를 보호하고 있다고 설명
- 아울러 '검증가능한 W3C 자격 증명(W3C Verifiable Credentials)' 같은 표준화된 신원 포맷 사용 장려, 분산형 스토리지 네트워크 활용한 데이터 가용성 제고와 중앙 집중식 장애 발생 리스크 완화를 주문
- 트린식의 라일리 휴즈 대표도 자사의 신원 수용 네트워크(Identity Acceptance Network)가 파트너십을 전제로 하는 것이며, 해당 과정에서 상호운용성 확보가 핵심이라고 강조

- Cryptonews가 인공지능(AI) 기술 발전과 딥페이크(deepfake) 사기범죄 증가 속에서 중요성이 높아지고 있는 고객 본인 확인(Know Your Customer, KYC) 솔루션 시장의 현황과 블록체인 기술의 접목 동향에 대해 보도
- 이에 의하면, 여러 플랫폼서비스에서 동일한 과정을 반복적으로 거쳐야 하는 불편함과 비용 부담으로 인해 기존의 고객 확인 인증을 반복하여 활용할 수 있는 '재활용 가능한(reusable)' KYC가 주목을 받는 상황
- 그러나 재활용 가능한 KYC에 대한 사이버보안 리스크가 높아지고 있고, 개인 정보와 이용자 데이터 보호가 중요한 과제로 부상한 상황에서 블록체인 기반의 온체인 데이터 저장이 대안으로 부상

[출처]

- Cryptonews, 'Blockchain Technology Helps Enable Reusable KYC Solutions', 2024.5.23.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[미국]

미국 하원, 블록체인 지원 담은 FIT 21 법안 압도적 찬성으로 통과

- 의회를 통과한 첫 번째 암호화폐 법안으로 주목, 암호화폐 업계는 이정표적인 입법 성과로 평가
- 백악관·SEC, 기존 증권 시장 혼란과 사용자 보호 미흡을 이유로 반대...상원 통과 여부는 불투명

미국 하원이 블록체인의 기술 발전을 지원하는 내용의 '21세기 금융혁신기술법(FIT 21*)' 발의안을 압도적 지지(찬성 279, 반대 136)로 통과시켰고, 업계는 의회를 처음 통과한 블록체인 법안으로서 높이 평가

* Financial Innovation and Technology for the 21st Century Act,

▶ 의회를 통과한 첫 번째 암호화폐 법안으로 주목, 백악관·SEC 등은 법안 도입 반대해 상원 처리 불투명

- 동 발의안은 암호화폐 시장에 대한 규제를 확립하는 선언적인 내용을 담고 있어 암호화폐 업계는 이번 하원 통과가 당파를 초월해 암호화폐 자산을 지지하는 진영의 정책적 승리*라고 평가
 - * 바이든 대통령은 정책 성명에서 동 법안에 반대했지만, 거부권 행사는 언급하지 않음
- FIT 21법안은 하원 농업위원회와 금융서비스위원회가 작성한 발의안으로 증권 요건에서 벗어난 암호화폐 자산을 디지털 상품으로 분류해 파생상품 규제기관인 상품선물거래위원회(CFTC)가 규제하는 방안을 제시
- 동 발의안은 ▲암호화폐 시장 규제 체제 확립 ▲소비자 보호 장치 마련 ▲디지털 자산 규제기관으로서 CFTC 지정 ▲암호화폐 토큰을 증권 또는 상품으로 분류 등의 내용이 담김
- FIT 21법안은 미국 암호화폐 규제가 다른 권역에 비해 뒤처졌다는 평가 속에 증권거래위원회(SEC)와 암호화폐 업계가 심각한 갈등 중인 상황에서 의회를 통과한 첫 번째 암호화폐 법안으로 주목
- 하지만 상원 법안이 없어 상원 통과를 낙관할 수 없는 상황이며, 게리 겐슬러(Gary Genlser) SEC 위원장은 이번 법안이 불필요할 뿐만 아니라 기존 증권 규정을 위태롭게 한다고 주장하며 강력하게 반대
- 백악관 역시 FIT 21법안이 특정 암호화폐 거래에 참여하는 투자자 보호 요건이 부족해 해당 법안 도입에 찬성하지 않는다고 발표하고, 정부 기관과 의회의 협력으로 세부 사항 조율을 희망한다고 언급
- 반면, 블록체인 협회 크리스틴 스미스(Kristin Smith) 회장은 FIT 21법안의 하원 통과는 미국 암호화폐 산업에 대한 의회 논의의 진전이자 새로운 분수령이라고 환영 입장을 발표

- 미국 하원이 블록체인에 대한 새로운 규제 체계 도입 등을 담은 발의안을 통과시켜 암호화폐 법안이 처음으로 미국 의회를 통과했고, 관련 업계는 새로운 분수령이라 평가하고 환영 입장을 발표
- 동 발의안은 암호화폐 규제 기간과 소비자 보호 장치 마련 등 포괄적인 내용을 담고 있지만, 백악관과 기존 규제기관인 SEC 등이 반대하고 있어 상원 통과 여부가 불투명한 상태로 평가됨

[출처]

- Coindesk, 'U.S. House Approves Crypto FIT 21 Bill With Wave of Democratic Support', 2024.05.23.
- Coindesk, 'U.S. House Passes Bill Banning Federal Reserve From Issuing a CBDC', 2024.05.24.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[미국]

美 하원, 의회 승인 없이 CBDC 발행을 금지하는 법안 가결

- 미 하원이 디지털 달러 발행에 대한 연방준비제도의 권한을 제한하는 'CBDC 감시방지법(안)'을 표결
- 동 법(안)은 원내 다수당인 공화당의 전폭적인 지지를 받으며 찬성 216표, 반대 192표로 가결

하원 원내대표 Tom Emmer의원(공화당 소속)이 발의한 'CBDC 감시방지법(안)'이 찬성 216표, 반대 192표로 가결

▶ 미 하원은 연방준비제도(Federal Reserve, Fed)가 의회의 명시적인 승인 없이 디지털 달러 또는 중앙은행 디지털화폐(CBDC)를 발행하는 것을 금지하는 법안인 'CBDC 감시방지법(안)*(HR 5403)'을 승인

* CBDC Anti-Surveillance State Act

- 하원 내 다수당인 공화당 소속 의원들은 정부가 국민의 재정을 통제하는데 CBDC가 사용될 수 있다는 우려를 표명하며 이를 방지하기 위한 동 법(안)을 지지
- Fed는 아직 디지털 달러 출시에 대한 명확한 계획을 공개한 바 없으나, 트럼프 전 대통령을 비롯한 공화당원들은 디지털 달러에 대한 정부의 과도한 개입 가능성에 대해 지속적으로 우려를 표명
- 법안을 발의한 Emmer의원은 디지털 달러(미국 CBDC)가 정부에게 금융 거래를 추적하고 정치적으로 바람직하지 않다고 간주되는 활동을 잠재적으로 제한하는 권한을 부여함으로써 정부의 '감시 도구'로 활용될 위험성을 지적
- 현재 차기 대통령 후보인 트럼프 전 대통령은 재선될 경우 디지털 화폐 발행을 금지할 것이라고 공언하며 디지털 화폐에 대한 강력한 반대 입장을 표명
- 트럼프 전 대통령은 디지털 화폐가 발행될 경우, 연방정부가 국민의 자산에 대한 절대적인 통제권을 가지게 된다고 경고하며, 국민의 자산을 가져갈 수 있고 국민은 자신의 자산이 사라진 사실조차 알 수 없을 것이라고 지적
- 한편, 전미은행가협회(ABA)는 표결에 앞서 하원 지도부에 동 법안을 지지할 것을 촉구
- 이번 표결은 전날 진행된 '21세기 금융혁신기술법안(FIT21)*'에 대한 표결이 민주당 의원 71명과 공화당 의원 208명이 찬성해 압도적인 초당적 지지를 받은 것과 비교됨
- * 현물시장 및 디지털 자산에 대한 상품선물거래위원회(CFTC)의 규제 권한을 확대

- 'CBDC 감시방지법안'은 디지털 달러가 정부의 금융 거래 추적 및 정치적 활동 제한 등을 가능하게 할 감시 도구로 사용될 위험성에 주목
- 연방준비제도는 현재 디지털 달러 출시 계획을 공개한 바 없으나, 동 법안이 가결됨에 따라 의회의 명시적 승인 없는 디지털 달러 또는 CBDC의 발행이 불가

[출처]

- Cryptonews, 'US House Votes to Block Federal Reserve's Digital Dollar Plans', 2024.05.23.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

국제결제은행 산하 위원회, 2024/25 추진 프로그램에 토큰화 및 CBDC 포함

- 국제결제은행 산하의 경제 및 시장 인프라위원회가 2024/25 추진 프로그램의 전략적 우선순위를 발표
- 중점 분야 중 하나인 '지급·청산·결제에서의 디지털 혁신'을 촉진하기 위해 토큰화 및 CBDC 관련 작업을 추진

국제결제은행이 2024/25 추진 프로그램의 전략적 우선순위에 토큰화 및 중앙은행 디지털화폐(CBDC)를 포함

▶ **국제결제은행(Bank for International Settlements, BIS)* 산하의 경제 및 시장 인프라위원회(Committee on Payments and Market Infrastructures, CPMI)가 2024/25 추진 업무 프로그램의 전략적 우선순위를 발표**

- * 국제금융 안정을 목적으로 중앙은행과 다른 기관 간 협력 증진을 도모하고 지원하기 위해 설립된 국제기구
- CPMI가 발표한 세 가지 중점 분야에 '지급(payment)·청산(clearing)·결제(settlement)에서의 디지털 혁신'이 포함된 가운데 디지털 혁신을 위해 토큰화 및 CBDC 관련 작업을 추진
- CPMI는 지급·청산·결제에서의 디지털 혁신과 관련하여, 화폐 및 결제의 맥락에서 토큰화를 모색 중에 있으며, G20과 함께 BIS 보고서를 발표할 예정
- 또한, CPMI는 국경 간 상호운용이 가능한 CBDC 도입을 위한 기술 및 정책 옵션과 이상적인 시점에 대한 분석을 진행 중이며, 국제증권감독기구(IOSCO)와 함께 스테이블코인 분석 시 다중 통화 및 자산 연동 스테이블코인을 포함하도록 범위를 확장할 계획
- '지급·청산·결제에서의 디지털 혁신' 외에 CPMI가 발표한 다른 두 가지 중점 분야에는 '금융시장 인프라(FMI)에 대한 리스크' 및 '국경 간 결제'가 포함
- FMI 리스크와 관련하여, CPMI는 분장원장기술(DLT)을 사용하여 FMI의 리스크를 평가하기 위해 IOSCO와 공동 작업을 진행 중이며, FMI 리스크에 포함되는 외환 결제 리스크를 줄이기 위해 외환동시결제(PVP)를 사용함에 있어 새로운 DLT 기반 인프라의 중요성을 앞서 확인
- '국경 간 결제'와 관련하여 CPMI는 결제 시스템의 상호연결 속도를 향상하는데 초점을 맞추고 있음
- 한편, BIS 혁신 허브(BIS Innovation Hub)는 7개 중앙은행과 함께 기존의 환거래 बैं킹 모델을 사용하여 국경 간 결제를 촉진하기 위한 토큰화 프로젝트인 '아고라 프로젝트(Project Agorá)'를 진행 중*
- * 실질적인 토큰화의 역할을 고려할 경우, 전략적 우선순위 중 '국경 간 결제'가 아닌 '디지털 혁신'의 범주에 포함

- 국제결제은행(BIS) 산하의 경제 및 시장 인프라위원회(CPMI)가 발표한 전략적 중점 분야에는 디지털 혁신, 금융시장 인프라에 대한 리스크, 국경 간 결제가 포함
- CPMI는 토큰화 및 CBDC를 통한 디지털 혁신을 추진 중인 가운데 BIS 혁신 허브는 7개 중앙은행과 함께 국경 간 결제를 촉진하기 위한 토큰화 프로젝트인 아고라 프로젝트를 진행 중

[출처]

- Ledger Insights, 'CPMI work program includes tokenization, CBDC', 2024.05.23.