

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

1. EU, MiCA 분석 보고서 발표... DeFi와 암호화폐 서비스 현황 조명
2. 2024 보안 위협 보고서: 영지식 솔루션과 Midnight 네트워크 솔루션
3. 블록체인 개발자, 암호화폐 규제를 놓고 미국 법무부에 법적 입장 표명
4. 암호화폐 담보 모기지: 블록체인 기술로 주택 소유를 혁신하다
5. 유럽의 디지털 미래: 지역 금융에서 스테이블코인의 역할

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[EU]

EU, MiCA 분석 보고서 발표... DeFi와 암호화폐 서비스 현황 조명

- DeFi의 시장 규모가 아직 니치(niche) 수준에 머물며 맞춤형 규제·감독 체계 마련이 시급함을 강조
- EU 신용기관들의 참여도가 낮지만, 규모가 커질 경우 본격적으로 시장에 진출할 가능성이 있음을 시사

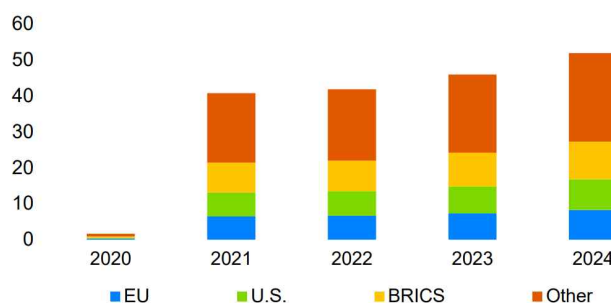
유럽은행감독청(EBA)과 유럽증권시장국(ESMA)이 MiCA 제142조에 따라 발표한 보고서는 DeFi·암호화폐 대출·차입·스테이킹 시장의 최신 동향과 이더리움 블록체인 의존도, 해킹·도난 및 AML/CFT 리스크 등을 종합적으로 분석하여, 탈중앙화 특성을 고려한 맞춤형 규제·감독 체계 마련과 투자자 보호 강화의 필요성을 강조하고 있음을 보임

▶ 유럽은행감독청(EBA)과 유럽증권시장국(ESMA)가 MiCA 제142조에 대한 분석 결과를 담은 보고서를 발표하며 DeFi·암호화폐 대출·차입·스테이킹 동향에 대해 조명

- EU는 MiCA(Markets in Crypto-Assets Regulation, 암호자산 시장 규제) 제 142조에서 다루는 특정 요소들에 관해 EBA(European Banking Authority, 유럽은행감독청)와 ESMA(European Securities and Markets Authority, 유럽증권시장국)가 수행한 분석 결과가 포함된 보고서를 발표
- 이는 EC(European Commission, 유럽위원회)가 암호자산의 최근 동향에 대해 유럽의회와 이사회에 제출할 보고서를 작성하는 데 있어 EBA와 ESMA가 기여한 내용을 포함
- 해당 보고서의 분석은 DeFi와 암호 대출, 차입 및 스테이킹에 관한 광범위한 연구를 바탕으로 이루어짐
- 또한 보고서는 분석적인 성격을 지녀 EC나 공동입법기관에 대한 구체적인 정책 권고안이나 입법 제안을 제시하지 않으며, 업계에서 제안하는 중앙화 및 DeFi 프로토콜과 같은 용어를 사용하지만, 이는 MiCAR 본문(서문 22항)에서 정의하는 실제 탈중앙화 수준에 관한 견해로 해석되어서는 안 될 것을 경고

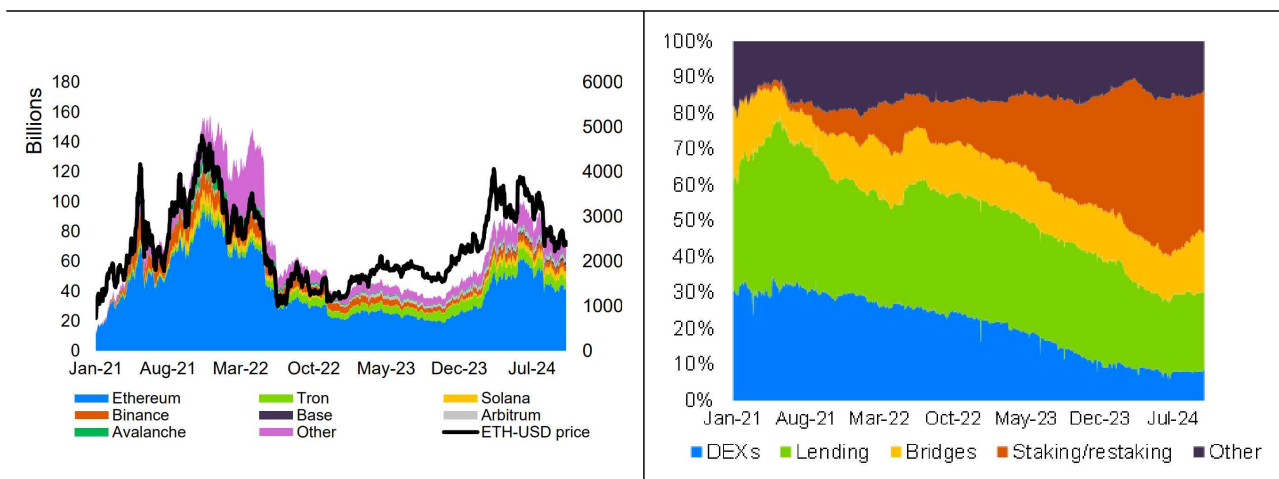
▶ 보고서의 첫 번째 장은 EU 소비자와 기업의 DeFi 참여에 초점을 맞추며, DeFi가 여전히 니치(niche) 시장 현상으로 남아있고, DeFi 프로토콜에 예치된 자산 규모가 암호 시장 가치의 4%를 차지한다고 밝힘

[체인별 TVL과 프로토콜 유형별 TVL 분석]



- DeFi 사용자 수, 인기 있는 DeFi 프로토콜과 탈중앙화 애플리케이션(DApp), 총 법정화폐·암호화폐 유로화 표시 거래량과 같이 EU 소비자와 기업의 참여 통계를 살펴봄으로써 EU의 DeFi 발전 현황을 평가
- 평가 결과, 전 세계와 EU에서 DeFi는 전체 암호화폐 자산 시가총액의 4%에 해당하는 금액이 DeFi 프로토콜에 묶여 있고, DeFi 활동이 소수의 대형 프로토콜에 집중되어 있다는 사실을 발견
- 현재 EU의 DeFi 사용자 수는 720만 명으로 추정되지만, 이 중 일부(15% 미만)만이 정기적으로 DeFi 활동에 참여하는 것으로 보이며, DeFi의 주요 사용 사례는 스테이킹, 대출 및 교환인 것으로 보임
- 데이터 제공업체 statista에 따르면 전 세계 DeFi 사용자는 5,400만 명으로 추산되며 EU의 사용자는 720만 명으로 EU 시민의 1.6%에 해당하며, 미국 인구의 2.2%에 해당하는 750만 명보다 낮은 수치를 보임

[체인별 TVL과 프로토콜 유형별 TVL 분석]

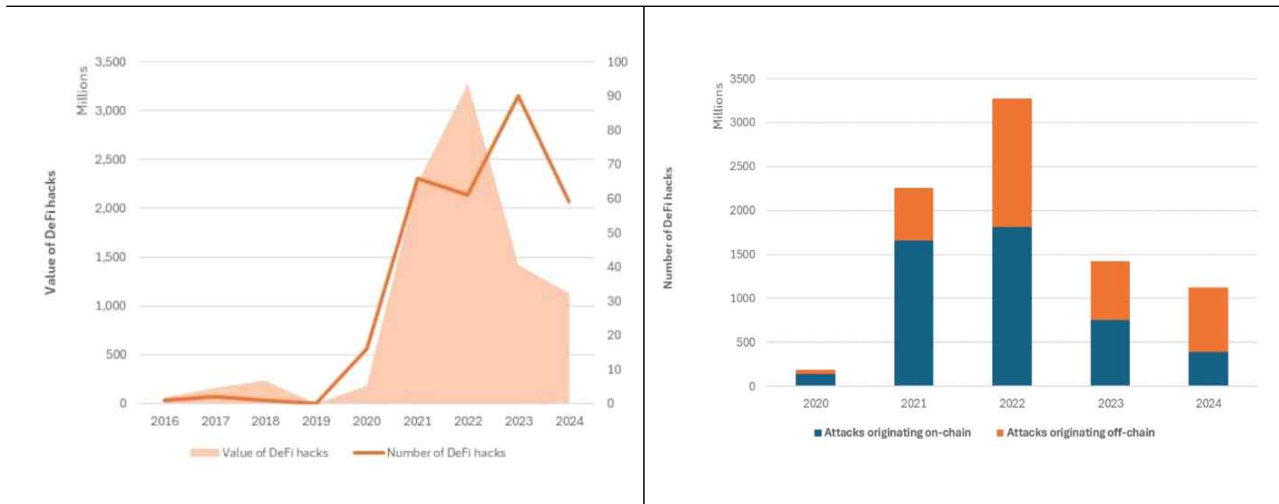


출처: ESMA, "Joint report on the recent developments in crypto-assets (Article 142 of MiCAR)" 2025.01.16.

- 보고서의 분석 결과, TVL 기준 DeFi 프로토콜 시장 규모의 약 60%는 이더리움 블록체인에 배포되어 있으며, 이는 블록체인의 기본 자산인 이더 가격과 TVL 간의 높은 상관관계에 기여함
- 이러한 상관관계는 일반적으로 이더 가격이 상승하면 DeFi에 대한 투자자의 관심이 높아지고, 반대로 DeFi 프로토콜에 예치된 자산이 이더 또는 Wrapped-이더 이기에 발생하는 자기 강화 매커니즘의 결과
- 2024년 9월 기준 스테이킹 프로토콜은 활동 유형별로 가장 큰 비중을 차지하며 전체 TVL의 39%를 차지했고, 이는 두 번째로 큰 유형인 대출 프로토콜(22%)의 두 배에 가까운 수치를 보임
- 스테이킹 프로토콜의 상대적 비중은 2021년 1월에는 거의 없었지만 2024년 9월 39%로 급성장 하였으며, 반대로 소위 DEX라고 부르는 탈중앙화 거래소 프로토콜과 같은 탈중앙화 금융의 다른 부문은 상대적 규모가 31%에서 8%로 축소되고 대출 프로토콜의 규모는 안정적으로 유지되었음을 보임
- 유로화 표시 스테이블코인은 DeFi 시장에서 아직 그 규모가 미미하며, 증거에 따르면 EU 금융 기관의 DeFi의 노출은 매우 제한적이라고 지적

- 또한, EU의 DeFi 도입률은 세계 평균보다 높지만, 미국이나 한국 등 다른 선진국보다 뒤쳐져 있음을 보임
- 보고서는 DeFi에 접근하는 여러 유형의 사업체(DeFi 애플리케이션 인터페이스, 셀프 커스텀 지갑, 중앙화 플랫폼)를 제시하고, 어떤 방식으로 디파이에 접근하는지는 활동 유형에 따라 달라진다고 설명

[DeFi의 암호화폐 도난 건수 및 규모와 공격 유형별 도난 규모]



출처: ESMA, "Joint report on the recent developments in crypto-assets (Article 142 of MiCAR)" 2025.01.16.

- 2024년 Chainalysis의 분석 보고서에 따르면, 2021년 이후 암호화폐 자산 도난은 DeFi에서 가장 많이 발생하였으며, DeFi 해킹 횟수와 탈취된 암호자산 가치가 DeFi 시장 규모와 상관관계를 보인다고 지적
- 그 결과, 2021년과 2022년에 해킹 건수와 도난 금액이 증가하였으며, 공격자들은 프로토콜에서 각각 25억 달러와 31억 달러(전체 DeFi 시장 규모의 약 2%)를 도난하였으며, 2023년에는 DeFi 해킹의 규모와 건수가 디파이 시자의 위축과 맞물려 감소하였지만 사고당 평균 탈취 금액은 증가함
- 과거에는 DeFi 해킹의 대다수가 스마트 컨트랙트 취약점 공격과 같은 온체인 취약성에 기인했지만, 최근에는 사용자 개인키 탈취와 같은 오프체인 취약성이 더욱 높은 공격성을 보인다고 분석
- 또한 DeFi 프로토콜은 자금세탁/테러자금조달 측면에서 상당한 위험을 내포하고 있는데, 이는 글로벌 현물 암호화폐 거래량의 약 10%가 중앙화 거래소에서 발생하기 때문이라고 밝힘
- 이는 충분한 AML/CFT(자금세탁방지/테러자금조달방지) 통제가 부재하여 사용자가 신원 확인 절차 없이 실제로 거래할 수 있다는 점에서 기인하며 거래의 국경 간 특성으로 인해 위험이 더욱 커짐
- 잠재적으로 불법적인 자금이나 암호자산이 DeFi를 통해 이전되더라도 해당 프로토콜에 AML/CFT 점검이나 FIU(금융정보분석기구)에 보고 의무가 없기 때문에 위험성이 존재
- 보고서는 DeFi 프로토콜에서 KYC(Know Your Customer)를 적용하려는 시도에 대해 언급하며 MEV와 관련해서는 블록체인의 탈중앙화 특성으로 인해 이러한 활동이 디파이에서 광범위하게 발생하며, MEV가 초래하는 부정적 외부효과를 줄이기 위해서는 기술적 해결책을 고민해야 한다고 결론지음

▶ 보고서의 두 번째 장은 암호화폐의 대출, 차입, 스테이킹 시장에 존재하는 사업 모델에 대해 설명하며

세 가지 서비스 유형에 대해 중앙화·탈중앙화 형식에서 주요 사업 모델과 특성에 대해 분석

- **(암호화폐 대출)** 사용자가 특정 가치의 자산 또는 자금을 담보로 맡기는 대가로 공급자(대출자)가 사용자(차입자)에게 특정 암호화폐 자산을 전송하는 활동으로 구성되며 DeFi 프로토콜을 통해 제공
- 중앙화된 대출인 DeFi 대출은 담보에 과도하게 의존하며 거버넌스 계약의 중개자는 시장 참여자에 대한 신용도 확인을 수행하지 않음
- **(암호화폐 차입)** 암호화폐의 차입은 사용자(대출자)가 특정 가치의 암호화폐 자산을 다른 사용자 또는 제공자(차입자)에게 양도하고, 차입자가 향후에 추가 이자에 해당하는 가치를 대출자에게 반환하겠다는 약속의 대가로 이루어지는 활동을 의미
- 암호화폐 차입 서비스 제공은 중앙화된 기관 또는 DeFi 프로토콜을 통해 중개될 수 있으며, 이러한 기관은 종종 암호화폐 자산 보유에 대한 수익률을 추구하는 사용자를 모집하는 구조로 구성
- **(스테이킹)** 스테이킹은 본 보고서의 목적상 2024년 6월에 발표된 스테이킹 및 MiCA에 관한 위원회 QCA에 명시된 대로 "블록 보상을 생성할 수 있는 검증자 권한을 부여하는 대가로 PoS 및 유사 블록체인 합의 매커니즘의 운영을 지원하기 위해 암호자산을 고정하는 과정"을 의미
- 이러한 의미에서 지분 증명 또는 지분 증명과 유사한 블록체인의 네이티브 토큰만이 네트워크의 합의와 보안 프로토콜에 기여할 수 있으며, 이에 따라 스테이킹 과정을 수행할 수 있음
- '스테이킹 서비스' 라고도 하는 서비스형 검증자(VaaS)는 노드를 직접 운영하는 데 필요한 자본은 있지만 기술적 수단이 없는 사람에게 스테이킹에 대한 접근을 용이하게 해주는 주체를 의미
- 보고서는 암호 대출, 차입, 스테이킹 서비스가 EU 관할구역의 여러 CASP(암호자산서비스제공자)에 의해 제공되고 있으며, 이 중 일부 업체는 규제된 암호자산 서비스도 병행 제공하고 있음을 확인
- **(문제점)** 관련 서비스가 제공되는 과정에서 이용자는 수수료, 이자 또는 이율, 담보 요건 변경, 담보 또는 스테이킹 계정에 예치된 자산에 대해 서비스 공급자가 취할 수 있는 조치, 분쟁이나 파산 발생 시 권리와 책임과 같은 중요한 사항에 대해 정보를 충분히 제공받지 못할 수 있다고 지적
- 현재까지 EU의 신용 기관은 암호화폐 대출, 차입 및 스테이킹 서비스에 대해 매우 제한적이거나 관여하지 않은 것으로 보이며, SSM 신용 기관 중 약 5%만이 이러한 서비스 참여를 계획하고 있는 것으로 분석
- 암호화폐 대출, 차입 및 스테이킹 서비스에 대해 공통적으로 ▲소비자 보호 ▲법적 위험 ▲시장 위험 ▲운영 및 ICT 위험 ▲자금세탁/테러자금조달과 같은 잠재적인 위험이 있을 것으로 설명

- DeFi 프로토콜을 통한 해킹·도난 및 AML/CFT 리스크가 더욱 명확해지면서, EU 내 규제 기관들은 DeFi 특유의 탈중앙화 특성과 기술적 취약점을 고려한 맞춤형 규제·감독 체계 마련이 필요함을 인식
- 투자자 보호 측면에서 최소한의 정보 제공 의무, 위험 고지 강화, 분쟁 해결 절차 마련 등이 중요해지며, 일부 CASP(암호자산서비스제공자)의 관련 서비스에 대한 명확한 가이드라인을 마련할 필요성 대두
- 현재 EU의 신용기관들은 암호화폐 대출·차입·스테이킹 서비스에 대한 참여도가 낮으나, DeFi 규모와 활용 사례가 늘어나면서 이들이 관련 시장에 본격적으로 진출할 가능성이 존재

[출처]

- ESMA, "Joint report on the recent developments in crypto-assets (Article 142 of MiCAR)" 2025.01.16.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

2024 보안 위협 보고서: 영지식 솔루션과 Midnight 네트워크 솔루션

- Verizon 보고서에 따르면 Web2와 Web3 부문에 강력한 보안 및 프라이버시 솔루션의 필요성 부각
- Midnight 네트워크는 영지식 증명과 선택적 데이터 공개 기능을 통해 보안 규정 준수 기능 강화

2024년 Web2와 Web3 생태계에서 대규모 보안 사고와 개인정보 침해가 발생해 보다 강력한 프라이버시·보안 솔루션의 필요성이 부각된 가운데, Midnight 네트워크는 영지식 증명과 선택적 데이터 공개 기능을 통해 민감한 데이터 노출 없이 규정 준수 및 거버넌스 투표 등의 기능을 제공하여 차세대 블록체인 플랫폼으로 주목

▶ 보고서는 Web2와 Web3에서 발생한 몇 가지 주요 보안 사고와 영향을 받은 사용자 및 해결 솔루션 소개

- Verizon의 2024년 데이터 침해 조사 보고서*에 따르면, Web2 측에서는 소셜 엔지니어링, 소프트웨어 취약성 및 맬웨어를 통한 보안 사고가 3만 건 이상, 데이터 침해가 1만 건 이상 발생함
- * Verizon, "2024 Data Breach Investigations Report" 2024
- 이러한 공격의 평균 손실 비용은 488만 달러에 달하며, 이는 랜섬웨어에 지불된 금액과 다운타임으로 인해 손해로, 이러한 데이터 침해는 2024년 1~3분기 동안 약 11억 2,000만 명의 사용자에게 영향을 미침
- Web3 또한 2024년 한 해 동안 총 12억 6천만 달러의 손실이 발생하였으며, 공격은 주로 스마트 계약의 검증 및 확인 절차의 부재나 인프라 또는 개인 키 관리에 대한 미흡함으로 인해서 발생

[2024년 Web2 및 Web3 보안 현황]

State of Security in 2024

THE BLOCK PRO · RESEARCH

Number of Users Affected Per Quarter

Crypto Hacked Per Quarter (in USD)



출처: The Block, "Research Unlock: Security Breaches in 2024: Zero Knowledge Solutions & Midnight Network" 2025.01.13.

- 안전하고 개인 정보를 보호하는 솔루션에 대한 필요성이 커짐에 따라 IOG는 쿠키 없는 환경과 선택적 데이터 공개를 가능하게 하는 기능을 갖춘 차세대 블록체인인 Midnight 네트워크를 개발
- Midnight 네트워크는 Cardano 블록체인의 파트너 체인으로, Zero-Knowledge Proofs(ZKPs, 영지식 증명)을 활용하여 사용자 데이터를 보호하고 악의적인 행위자로부터 데이터를 보호하는 거래를 보장

▶ Web2 및 Web3은 다양한 보안 위협에 직면해있으며, 이에 대한 보안 과제와 사례에 대한 연구 진행

[Web2 분야의 공격 기법]

분류	공격 기법	설명
Web2	피싱 공격	- 피싱 공격은 공격자가 사용자를 속여 로그인 자격 증명이나 재무 세부 정보와 같은 민감한 정보를 공개하도록 할 때 발생 - 이러한 공격은, 신뢰할 수 있는 기관을 모방하는 사기성 이메일, 메시지 또는 웹사이트를 통해 수행 - 예를 들어, 공격자는 은행에서 보낸 것처럼 가장한 이메일을 보내 사용자를 계좌 세부 정보를 수집하는 가짜 웹사이트로 안내
	중간자 공격(MITM)	- 중간자 공격은 공격자가 두 당사자 간의 통신을 가로채고 그들의 지식 없이 잠재적으로 변경할 때 발생 - 이는 보안되지 않거나 암호화가 제대로 되지 않은 네트워크에서 종종 발생하여 공격자가 로그인 자격 증명, 재무 데이터 또는 개인 메시지와 같은 민감한 정보를 훔칠 수 있는 위험 존재
	SQL 주입	- SQL 주입은 공격자가 악성 SQL 코드를 주입하여 데이터베이스를 조작하고 시스템에 대한 무단 액세스를 얻는 기술 - 공격자는 종종 OR 및 AND와 같은 논리 연산자와 결합된 SQL 명령을 사용하여 애플리케이션의 입력 필드의 취약성을 악용
	XSS(크로스 사이트 스크립팅)	- 크로스 사이트 스크립팅은 사용자가 악성 URL을 클릭하여 해당 기기에서 악성 코드를 실행하는 경우 발생 - 이를 통해 세션 세부 정보, 쿠키 및 개인 정보가 공격자에게 제공되고 이를 사용하여 모든 웹사이트에서 인증을 받을 수 있음
	IDOR	- IDOR은 사용자의 입력에 따라 사용자 시스템의 객체를 참조하는 전형적인 실수로 발생하는 공격 유형 - 이로 인해 시스템에서 악의적인 입력이 처리되어 개인 정보가 노출될 수 있으며, 이는 사용자 정보 또는 서버에 저장된 모든 파일을 대상으로 함
	CSRF	- 크로스 사이트 요청 위조는 요청이 합법적인지 여부를 인증하는 CSRF 토큰이 URL에 첨부되지 않아 공격자가 사용자를 대신하여 작업을 수행할 수 없을 때 발생 - 은행 송금이나 기타 악의적인 활동이 포함될 수 있음
	민감한 정보 노출	- 사용자의 비밀번호와 신용카드 정보와 같은 개인 정보는 SHA-256 또는 RSA와 같은 알고리즘을 사용하여 서버 측에서 해시되어야 합니다. 이를 무시하면 사용자는 공격과 데이터 유출에 취약해질 수 있습니다.
	맬웨어 공격	- 맬웨어 공격에는 시스템을 방해, 손상 또는 무단으로 액세스하도록 설계된 악성 소프트웨어가 포함 - 맬웨어는 종종 이메일 첨부 파일, 악성 링크 또는 감염된 다운로드를 통해 전달
	보안 오류	- 보안 오류 구성 취약점은 애플리케이션의 부적절하거나 불완전한 구성으로 인해 발생 - 민감한 도메인 노출, 알려진 취약점이 있는 오래된 소프트웨어 실행, 불필요한 서비스 활성화, 스택 추적 노출 및 공격자가 악용할 수 있는 기타 오류 구성 등이 포함

[Web3 분야의 공격 기법]

분류	공격 기법	설명
Web3	입력 검증	- 입력 검증은 사용자가 제공한 입력이 예상치 못한 동작으로 이어지지 않도록 스마트 계약 수준에서 처리해야 하며, 입력 검증에 실패하면 취약성이 노출되어 자금 도난, 가스 비용 부풀리기 또는 계약이 응답하지 않게 만드는 서비스 거부(DoS) 공격과 같은 악용이 가능해짐 - 예를 들어, 숫자 입력 검증을 소홀히 하면 공격자가 오버플로 또는 언더플로 오류를 트리거하여 계약의 기능과 논리가 중단될 수 있음
	수학적 오류	- 수학적 오류는 토큰 잔액 사용을 포함하여 스마트 계약 수준에서 수행되는 모든 계산을 의미하며, Solidity는 기본적으로 소수점을 지원하지 않으므로 반올림 오류가 발생하여 의도치 않은 결과를 초래할 수 있음
	오라클 조작	- 오라클 조작은 의도치 않은 토큰 가격으로 이어지는 Web3에서 가장 악명 높은 공격 중 하나이며, 이는 프로토콜에 내부 오라클이 있거나, 가격을 제대로 검증하지 않는 서비스를 사용하거나, 신뢰할 수 없는 검증자 또는 네트워크 참여자가 있는 경우 발생 - DeFi 생태계에서 포지션 크기와 청산 임계값을 계산할 때 큰 영향을 미칠 수 있으며, 이러한 조작은 플래시 대출을 사용하여 실행할 수도 있으며, 이는 자산의 가치를 인위적으로 부풀려 공격자가 DeFi 프로토콜을 조작하는 데 도움이 될 수 있음
	접근 제어 부족	- 접근 제어 또는 특정 역할에 따른 권한 정의는 모든 애플리케이션에서 중요하며, 부적절한 액세스 제어를 통해 악의적인 행위자가 의도치 않게 액세스하여 승인되지 않은 코드를 실행할 수 있음 - 특정 역할에 부적절한 액세스 권한을 부여하지 않는 것이 중요하며, 여러 역할을 사용하여 계약의 공격 표면을 줄임으로써 특수 액세스 권한이 있는 EOA(외부 소유 계정)가 손상되더라도 악용을 최소화
	재진입 공격	- 재진입 공격은 계약의 기능이 실행 중 및 상태 업데이트를 마무리하기 전에 외부 호출을 허용할 때 발생하며, 이를 통해 공격자는 동일한 계약 상태를 사용하고 인출과 같은 특정 악의적인 행동을 반복하여 계약의 자금을 고갈시킬 수 있음
	리플레이 공격	- 리플레이 공격은 공격자가 실제 발신자가 수행한 유효한 거래나 동작을 리플레이할 때 발생하며, 공격자는 원래 발신자가 보낸 메시지를 가로채거나 캡처하여 네트워크에 다시 브로드캐스트하여 인증을 얻거나 네트워크에서 악의적인 동작을 수행함
	프런트러닝 공격	- 프런트러닝은 공격자가 특정 자산의 가격에 영향을 줄 수 있는 거래를 알아차리고 더 높은 가스 가격으로 거래를 보내는 경우 발생하며, 이를 통해 새로운 거래가 먼저 실행되고 프런트러너는 원래 보낸 사람의 거래의 업데이트된 가격에서 이익을 얻을 수 있음
	거버넌스 공격	- 거버넌스 공격은 해커가 DAO를 통해 악의적인 거래를 실행할 수 있는 충분한 투표권을 얻을 때 발생하며, 공격자는 플래시 대출을 통해 토큰을 획득하여 이를 수행할 수 있음 - 이를 방지하기 위해 프로젝트는 일반적으로 변조할 수 없는 엄격한 거버넌스 프레임워크를 사용해야 함

▶ **Midnight 네트워크는 데이터 보호 및 개인 정보 보호 기능을 활성화하여 Web3에 보안 개선사항을 제공**

- **(실제 자산의 토큰화)** 데이터의 안전하고 비공개 처리가 실제 자산의 토큰화에 필수적이며, 이러한 자산에 대한 소유권 세부 정보는 검증되고 안전하게 저장되어야므로, 이를 위해 영지식 증명 및 비공개 상태 관리를 통해 소유권 세부 정보 검증 및 상태 관리를 효과적이고 효율적으로 수행
- **(상호 운용성)** Midnight 네트워크는 재귀적 증명과 Cardano 및 Ethereum과 같은 네트워크와 호환되는 BLS 서명 체계를 허용하는 개선된 Halo2 프레임워크를 사용
- **(기업 채택을 위한 향상된 개인 정보 보호)** 기업들은 민감한 운영, 독점 또는 고객 데이터를 노출하는 것에 대한 우려로 인해 블록체인 기술을 도입하는 데 어려움을 겪고 있음
- Midnight 네트워크는 개인 정보를 보호하는 스마트 계약을 허용하고 민감한 정보를 완전히 오프체인으로 보관하는 동시에 복잡한 워크플로 및 거래를 허용함으로써 향상된 개인 정보 보호 기능을 제공함
- **(분산형 ID(DID))** 분산형 ID는 Midnight 네트워크 및 영지식 증명의 가장 강력한 사용 사례 중 하나이며, 사용자는 이를 통해 개인 정보를 공개하지 않고도 자신의 신원을 증명할 수 있음
- 이러한 기술은 사용자가 다양한 형태의 감시와 그에 따른 정보 탈취를 방지할 수 있으며, Midnight 네트워크는 영지식과 선택적 데이터 공개를 결합하여 사용자가 필요한 것보다 더 많은 정보를 공유하지 않고도 자신의 신원을 증명할 수 있는 기능을 제공
- **(개선된 거버넌스 시스템)** 투명한 온체인 투표는 프라이버시를 침해할 수 있으므로, Midnight 네트워크의 아키텍처는 암호화 증명을 통해 기밀성과 책임을 보장하며, 유권자가 선호도나 보유 자산을 공개하지 않고도 투표할 수 있어 거버넌스 조작 위험을 줄일 수 있음
- DAO는 프라이버시를 유지하면서 공정한 의사 결정을 촉진하기 때문에 이로부터 큰 이점 제공 받음
- **(규정 준수)** 블록체인 시스템은 종종 익명성이라는 특성으로 인해 규제 기관의 조사를 받는데, 이는 때때로 불법 활동 과정에서 사용될 수 있는 여지를 제공함
- Midnight 네트워크를 사용하면 기업은 민감한 데이터를 노출하지 않고도 AML(자금 세탁 방지) 또는 KYC(고객 확인) 규정을 준수한다는 것을 증명할 수 있어 불법 활동을 방지할 수 있는 기능 제공
- **(데이터 보호 블록체인)** 온체인과 오프체인 상태의 공존과 상호 작용을 통해 사용자가 민감한 데이터를 보호하고 보관하고 퍼블릭 블록체인에 절대로 공개되지 않는 시스템을 구축
- **(사용의 용이성)** Midnight 네트워크는 개발자에게 익숙하고 배우기 용이한 Typescript 기반 도메인 특정 언어인 Compact를 사용하여 애플리케이션을 배포할 수 있어 개발자의 작업 난이도를 완화

- 2024년의 사건은 Web2와 Web3 생태계에 더욱 강력한 프라이버시 및 보안 솔루션의 필요성을 강조하며, 대규모 데이터 침해에서 블록체인 프로토콜에 대한 개선된 기술적 보호 조치의 필요성을 보여줌
- Midnight 네트워크는 영지식 증명, 선택적 정보 공개와 같은 기능을 통해 보안 문제를 해결할 수 있는 프레임워크를 제공하며, 모듈형 아키텍처를 통해 스마트 계약은 개인 및 공개 상태와 상호 작용하여 개발자에게 유연성을 보장

[출처]

- TheBlock, 'Research Unlock: Security Breaches in 2024: Zero Knowledge Solutions & Midnight Network' 2025.01.13.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

블록체인 개발자, 암호화폐 규제를 놓고 미국 법무부에 법적 입장 표명

- 블록체인의 투명성과 프라이버시 문제가 충돌하며 이를 해결하기 위한 프라이버시 강화 솔루션 주목
- 스마트 계약 보안 취약점과 양자 컴퓨팅의 위협에 대한 감사 및 양자 내성 알고리즘 연구 필요성 강조

블록체인 개발자 마이클 르웰런의 비보관형 분산 플랫폼의 규제 적용 범위에 대한 소송 결과는 혁신과 규제의 균형을 놓고 벌어지는 미국 내 논쟁과 암호화폐 혁신의 미래에 중대한 영향을 미칠 것으로 전망

▶ 비보관형 분산 플랫폼 규제 소송을 통해 암호화폐 혁신과 감독 사이의 핵심 분수령이 될 것으로 전망

- 저명한 미국 블록체인 개발자인 마이클 르웰런이 미국 법무부(DOJ)를 상대로 소송을 제기하였으며, 바이든 행정부의 규제적 접근 방식이 암호화폐 부문의 혁신을 저해하고 있다고 주장
- 이러한 소송은 연방 자금 전송법의 해석에 초점을 맞추고 있으며, DOJ가 암호화폐 개발을 규제하는 데 있어 과도한 권한을 행사하여 자신의 Pharos 프로토콜과 같은 분산형 플랫폼의 성장을 위협한다고 주장
- Pharos는 보증 계약, 즉 기금을 보유하고 기금 목표가 충족되지 않을 경우 기부자에게 자동으로 환불하는 스마트 계약 시스템을 활용하며, 이러한 비보관 모델은 르웰런이 사용자 기금을 통제하거나 보유하지 않는다는 것을 의미하고, 이를 통해 엄격한 규제 검토에서 면제되어야 한다고 주장
- 르웰런의 비보관형 플랫폼에 대한 DOJ의 규제 조치 증가에 대한 우려를 강조하며, 2022년 미국 정부가 금지한 개인 정보 보호 도구인 Tornado Cash 사례를 DOJ가 혁신을 방해할 수 있는 방법의 예로 주장
- 르웰런의 소송 결과는 미국 암호화폐 개발의 미래에 중대한 영향을 미칠 수 있으며, 법원이 Lewellen에게 유리한 판결을 내리면 Pharos와 같은 비보관형 도구가 기존 금융 서비스와 동일한 규제 요구 사항을 따르지 않으므로 블록체인 분야에서 혁신을 위한 더 유리한 환경을 조성할 것이라고 분석
- Lewellen의 법적 도전은 DeFi Education Fund와 Coin Center를 포함한 다양한 업계 옹호자들의 지지를 얻었으며, 이러한 조직은 분산형 플랫폼의 고유한 특성을 인식하는 더 명확한 규제 프레임워크의 필요성을 강조
- 암호화폐 산업이 계속 진화함에 따라 이 사건의 결과는 앞으로 수년간 규제 환경을 형성할 가능성이 높으며, 이번 법적 싸움은 빠르게 변화하는 블록체인 기술 세계에서 혁신과 규제 감독의 필요성을 가장 잘 균형 잡는 방법에 대한 지속적인 논쟁에서 중요한 순간으로써 조명받음

- 르웰런의 소송은 연방 자금 전송법 등 기존 규제 체계가 비보관형 플랫폼의 특수성을 얼마나 반영해야 하는지에 대한 쟁점을 제기하였으며, 르웰런이 승소할 경우 암호화폐 개발 및 혁신에 활로를 열어줄 가능성이 높음을 시사
- 르웰런이 언급한 Tornado Cash 금지 사례처럼, 현재 미국의 규제 당국은 자금 세탁 및 불법 활동 방지의 목적으로 분산형 프로토콜에 대한 감독을 강화하며 이는 DeFi·프라이버시의 규제 방향성과 혁신의 균형 필요성을 대두

[출처]

- Blockchain Magazine, 'Blockchain Developer Takes Legal Stand Against DOJ Over Crypto Regulations', 2025.01.18.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

암호화폐 담보 모기지: 블록체인 기술로 주택 소유를 혁신하다

- 암호화폐가 소유권을 유지하며 대출에 대한 가치를 활용할 수 있으므로 주택 대출의 대안으로 주목
- 대출의 주요 프로세스를 자동화하는 스마트 계약으로 대출자와 차용인 간의 신뢰성, 투명성, 안정성을 강화

암호화폐 담보 모기지는 블록체인 기술의 투명성과 효율성을 활용하여 주택 대출 생태계를 혁신하고, 차용자와 대출자 모두에게 새로운 기회를 창출할 잠재력을 지니므로써 전통 금융 대비 효율성을 높일 것으로 기대

▶ 암호화폐 담보 모기지가 주택 대출의 효율성을 높여 새로운 금융 기회를 제공하는 혁신적 대안으로 부상

- 투기적 투자로 여겨졌던 암호화폐는 빠르게 변혁적인 금융 혁신을 위한 도구로 진화하고 있으며, 이러한 혁신 중에서 암호화폐 기반 모기지는 블록체인 기술에 의해 주택 대출에 대한 유망한 대안으로 부상하여 주택 시장을 재편하고 구매자와 대출자 모두에게 기회를 창출
- 2012년, BTCJam은 비트코인 담보 대출이라는 개념을 도입하여 개인이 비트코인을 담보로 사용하여 자금을 빌릴 수 있도록 하였으며, 2016년까지 120개국 이상에서 16,000건 이상의 대출을 제공
- 이러한 암호화폐 도입 사례는 대출을 확보하기 위한 실행 가능한 도구로서의 잠재력을 입증하는 데 도움이 되었으며, 주택 시장에서 블록체인 기술을 보다 광범위하게 통합할 수 있는 가능성을 보임
- 암호화폐 담보 모기지는 신용 점수나 소득 내역과 같은 전통적인 요소 대신 암호화폐를 담보로 사용하는 주택 대출로, 대출자는 디지털 자산을 현금화하여 부동산 매수 자금을 조달하는 대신 암호화폐를 담보로 제공하여 소유권을 유지하는 동시에 대출에 대한 가치를 활용할 수 있음
- 블록체인 기술은 암호화폐 담보 모기지의 보안, 투명성 및 효율성을 강화하며, 대출 지급, 담보 가치 추적 및 상환 조건 시행과 같은 주요 프로세스를 자동화하는 스마트 계약을 사용하여 효율성을 제공
- 차용인이 암호화폐를 담보로 제공하면 스마트 계약이 자동으로 대출을 해제하며, 담보 가치를 모니터링하여 가치가 하락하면 마진 콜 또는 청산을 발생시키는 기능을 제공함으로써 서류 작업을 줄여 신속하게 처리하며, 안전하고 검증 가능한 거래를 보장함으로써 대출자와 차용인 간의 신뢰를 강화

- 기존에 투기적 자산으로만 인식되던 암호화폐가 모기지의 담보 자산으로 활용되며, 디지털 자산을 현금화하지 않고도 주택을 구입할 수 있는 금융 모델이 형성되어 주택금융에 대한 접근성 향상 및 투자 전략의 다양성 제공
- 스마트 계약을 통해 대출 지급, 담보 가치 추적, 상환 조건 시행 등 주요 프로세스를 자동화함으로써 서류 작업을 줄이고, 신속한 처리와 신뢰 기반의 거래를 가능하게 하여 전통 금융 대비 효율성을 크게 높일 것으로 기대

[출처]

- Unlock, 'Crypto-Backed Mortgages: Revolutionizing Homeownership with Blockchain Technology', 2025.01.18.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[EU]

유럽의 디지털 미래: 지역 금융에서 스테이블 코인의 역할

- 스테이블코인을 활용한 낮은 비용·즉각적인 거래가 고객 경험을 개선하고 금융 환경을 재편하고 있음
- MiCA 도입으로 규정 준수 발행자가 신뢰도를 높이고 스테이블코인을 통해 변동성을 줄여 수익성을 개선

스테이블코인은 안정성, 효율성, 민첩성을 제공하여 유럽의 디지털 전환에서의 중요한 역할을 수행하며, 강력한 규제 지원과 사용 사례를 갖춘 스테이블코인은 유럽의 금융적 미래의 초석을 나타내며 글로벌 금융 통합을 위한 모델을 제공

▶ 유럽에서 스테이블코인이 신속하고 저렴한 결제 수단으로 부상하며 금융 환경 전반을 재편할 잠재력을 보임

- Chianalysis의 보고서*에 따르면 스테이블코인은 최근 몇 달 동안 온체인 거래의 50-75%를 차지하였으며, 유럽이 스테이블코인으로의 디지털 통화 전환의 선두 주자로 부상

* "Stablecoins dominate market share, Bitcoin grows, and merchant services thrive in Central, Northern, & Western Europe" 2024.10.23.

- 2023년 7월에서 2024년 6월 사이에 유럽은 온체인 가치로 9,872억 5,000만 달러를 기록했으며, 이는 전 세계 암호화폐 거래의 21.7%를 차지하여 유럽이 암호화폐 경제에서 영향력을 키우고 있음을 보여주며, 스테이블코인이 이러한 모멘텀을 주도하고 금융 환경을 재편하고 있음을 보임

- 스테이블코인은 국제 무역에 종사하는 기업을 위한 국경 간 결제 처리에 혁명을 일으키고 있으며, 기존 결제 시스템보다 훨씬 낮은 가격에 즉각적인 거래를 제공하여 거래 범위를 확대하고 고객 경험을 개선

- BVNK의 보고서*에 따르면, 기업이 이러한 자금을 효과적으로 재투자할 경우, 2027년까지 동일한 경로에서 29억 달러의 추가 수익을 볼 수 있으며, 이는 총 국경 간 지불량의 약 10%를 차지함

* "The decade of digital dollars Unlocking economic efficiency with stablecoins"

- 스테이블코인은 암호화폐 회사에서의 재무 운영에 더 많이 사용되고 있으며, 암호화폐 관련 변동성을 줄여 신뢰할 수 있는 가치 저장소 역할을 통해 기업은 유동성을 관리하고 원활한 재무 운영을 유지

- 스테이블코인은 금융 프로세스를 보다 원활하게 만들고 기존 은행 시스템에 의존할 필요성을 줄여 빠른 거래가 중요한 iGaming 및 재휴 마케팅과 같은 산업에서 스테이블코인은 보다 빠른 지급과 낮은 운영 비용을 제공하여 수익성을 높이고 이해관계자 간의 신뢰를 구축하는 역할을 수행

- 유럽의 스테이블코인의 미래는 다양한 플레이어와 규제 변화를 수반하며, MiCA 규정의 도입으로 Circle의 USDC와 같은 규정 준수 발행자는 이미 엄격한 규제 기준을 충족하고 강력한 기관 지원을 받고 있음

- 온체인 거래의 상당 부분을 차지하게 된 스테이블 코인은 빠른 거래 속도와 낮은 수수료로 기업의 국경 간 결제 프로세스를 혁신하고 있으며, 향후 다양한 영역으로 활용 범위가 확장될 것으로 예상
- MiCA 규정 등 유럽의 규제 체계가 마련되고 Circle의 USDC와 같은 규정 준수 발행자가 등장함에 따라 스테이블 코인은 변동성이라는 약점을 극복하고 신뢰할 수 있는 가치 저장 및 지급 수단으로 자리잡을 것으로 전망

[출처]

- Mpost, 'Europe's Digital Future: The Role of Stablecoins in The Regional Finance', 2025.01.17.