

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

1. 헬스케어 산업에 적용된 새로운 블록체인 합의 알고리즘
2. DeFi 보안 통제와 중앙화 구조의 상호작용
3. 영국, 블록체인 프로젝트 직원 중 북한 기술 노동자 발견
4. Ripple과 파트너들, 케냐 가뭄 구호를 위한 블록체인 지원 시범 프로그램 실시
5. MiCA의 실수: EU 정책이 미국 달러의 지배를 촉진

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

헬스케어 산업에 적용된 새로운 블록체인 합의 알고리즘

- 'Proof of Visit (POV)'라는 새로운 합의 알고리즘을 도입하여 블록체인 네트워크의 효율성과 보안을 향상
- 특히 의료 산업에 초점을 맞추어, 환자의 방문 기록을 안전하게 관리하고 공유하는 데 활용될 수 있음

이스탄불 대학교 연구진은 블록체인 인프라를 활용하여 전자 건강 기록(EHR)을 안전하게 공유하고, 건강 데이터에 특화된 합의 알고리즘인 PoV(Proof of Visit)를 개발하여 데이터 공유를 위한 맞춤형 솔루션의 실현 가능성을 제시

▶ 병원 진단 및 진료, 약물, 처방 및 관련 개인 의료 데이터의 급격한 증가로 다양한 데이터 아키텍처의 필요성 대두

- 세계 인구 증가, 기술 발전, 유전자 연구, 디지털 의료 서비스, 의료 기기 등은 전자 건강 기록(Electronic Health Record, EHR)의 급속한 성장을 이끄는 요인으로 작용하고 있으며, 이에 따라 의료 데이터의 체계적인 관리와 안전한 활용을 위한 기술적 기반의 중요성이 강조됨
- 오늘날 중요한 문제 중 하나는 중앙 집중식 데이터베이스 시스템에 데이터를 저장하고, 이러한 센터를 통해서만 데이터의 정확성과 보안을 보장한다는 점이 단일 실패 지점, 보안 위협 등의 문제를 야기
- 또한, 센터 간의 통신 및 통합 문제로 인해 EHR 접근이 어려워 검사 및 실험실 결과와 같은 중요한 데이터가 중복될 수 있으며, 시민들은 자신의 EHR 공유에 대한 완전한 통제권을 갖지 못함
- 이러한 상황은 의료 프로세스에 결함과 지장을 초래하며, 시민의 동의 없이 개인 EHR을 공유하면 데이터 프라이버시 문제가 발생할 수 있음
- 그 외에도, 환자 데이터가 중앙 집중식으로 저장되는 시스템에서는 소프트웨어 변경으로 인해 환자 데이터 손실과 같은 문제가 발생하여 환자의 개인정보가 귀중하지 않고 부자적인 데이터로 취급되어 데이터가 불안정하게 관리될 위험이 존재

▶ 분산형 아키텍처를 갖춘 블록체인 기술은 의료 분야의 데이터 보안 및 개인정보 보호 개선에 상당한 잠재력 보유

- 블록체인 기술은 의료 분야의 데이터 보안 및 개인정보 보호 개선에 상당한 잠재력을 제공함
- PBFT(Practical Byzantine Fault Tolerance), PoW(Proof of Work), PoS(Proof of Stake)와 같은 기존 합의 알고리즘은 에너지 소비, 확장성, 데이터 개인정보 보호 측면에서 상당한 한계를 가지고 있으며, 특히 민감한 의료 데이터에서 더욱 심각
- 제안된 PoV(Proof of Visit) 알고리즘은 ▲ PoW 대비 에너지 소비 감소 ▲PBFT를 넘어선 확장성 향상 ▲PoS 대비 개인정보 보호 강화 등의 특징으로 개인정보 보호의 어려움을 해결
- AI, 대규모 언어 모델(Large Language Model, LLM)의 최근 발전은 의료 데이터에서의 개인정보 보호 문제 해결을 위한 실마리를 제공하고, IoT 기기는 실시간 환자 모니터링을 가능하게 했으며, 언어 모델은 분산형 학습을 통해 데이터 프라이버시를 보장

- 이러한 기술이 PoV와 결합하면 안전·효율적인 의료 데이터 관리를 위한 프레임워크를 구축할 수 있음

▶ 블록체인을 사용하여 의료 데이터를 공유하기 위한 특화된 합의 알고리즘을 개발하여 효과적인 의료 시스템 구축

[PoV에 필요한 블록 구조와 클래스]

Patient Information BLOCK INDEX Time Stamp Previous Block Hash Block hash BLOCK BODY SYSTrackingNo RoleName PatientId FirstName LastName Email Phone Adress Gender ICD10Code DrugCode	<pre> public class Block { public int BlockIndex { get; set; } public DateTime TimeStamp { get; set; } public string PreviousBlockHash { get; set; } public string CurrentBlockHash { get; set; } public string TransactionAsString { get; set; } [JsonIgnore] public List<Transaction> TransactionData = new List<Tra public int Nonce = 0; public Block(DateTime timeStamp, string previousHash) { BlockIndex = 0; TimeStamp = timeStamp; PreviousBlockHash = previousHash; //CurrentBlockHash = CalculateHash(); } public Block(DateTime timeStamp, string previousHash, I { BlockIndex = 0; TimeStamp = timeStamp; PreviousBlockHash = previousHash; TransactionData = transactionData; //CurrentBlockHash = CalculateHash(); } } </pre>
---	---

출처: Science Direct, 'New blockchain consensus algorithm applied on healthcare industry: Proof of Visit- (POV)', 2025.04.

- PoV는 의료 분야에 초점을 맞춰 개발된 합의 알고리즘으로 의료 서비스를 받는 시민과 의료 서비스 제공자 간의 방문 및 워크플로우를 기반으로 모델링
- PoV의 블록 검증에는 데이터 마이닝이 필요 없으며 따라서 높은 에너지 소비나 PoW와 같은 고가의 시스템이 필요하지 않음
- 또한 환자의 EHR은 EHR 데이터 접근 권한이 있는 노드에 저장되며, 블록체인의 모든 EHR 데이터를 각 노드에 저장할 필요는 없어 EHR 데이터의 SHA-256 해시 정보만 네트워크의 노드에 배포
- 결과적으로 네트워크의 각 노드는 모든 EHR 데이터를 저장하고 접근할 수 없으며, 이를 통해 EHR 데이터의 개인 정보 보호를 보장하고 블록체인에 블록을 추가하는 데 걸리는 시간을 감소
- 나아가 PoV 알고리즘은 무작위성을 제거하여 하드웨어 종속성을 없애는 것을 목표로 하며, 주문 서비스 및 Kafka 알고리즘과 같이 특정 노드가 아닌 전체 네트워크를 포함하는 합의 알고리즘을 제안

▶ PoV 알고리즘은 보안성, 효율성 등 서로 다른 운영 시나리오에 맞춰 조정된 세 가지 모델로 구성

- **PoV1(높은 보안 요구 사항)** PoV1 모델은 국가 의료 시스템과 같이 엄격한 데이터 검증과 강력한 보안이 요구되는 환경을 위해 설계되었으며, 권한 노드별 블록 검증을 우선시하여 분산 무결성을 유지하면서

중앙 집중식 감독을 보장할 수 있어 데이터 정확성과 보안이 중요한 시스템에 적합

- **PoV2(중간 리소스)** PoV2 모델은 중간 수준의 컴퓨팅 용량을 갖춘 지역 병원이나 의료 시설에 최적화되도록 설계되었으며, 가벼운 권한 노드가 블록 검증을 처리하도록 하여 리소스 소비를 줄이는 동시에 적정 수준의 보안 및 효율성을 보장하여 확장성과 리소스 가용성의 균형을 유지
- **PoV3(자원 제약 환경)** PoV3 모델은 소규모 진료소나 이동형 의료 시설에 맞춰 설계된 완전 분산형 모델로, 권한 노드를 제거하고 P2P 검증에 의존하여 분산성을 극대화하고 인프라 요구 사항을 최소화

[PoV 알고리즘 모델의 사용 사례 비교]

Table 3. PoV model's use cases.

Model	Key features	Ideal use case	Resource needs	Model
PoV1	High security, authority nodes	National healthcare systems	High	PoV1
PoV2	Balanced approach	Regional hospitals	Moderate	PoV2
PoV3	Fully decentralized	Small clinics, mobile health units	Low	PoV3

출처: Science Direct, 'New blockchain consensus algorithm applied on healthcare industry: Proof of Visit- (POV)', 2025.04.

▶ **AI, IoT 등 첨단 기술을 PoV에 통합하여 의료 데이터의 안전한 공유와 신뢰가능한 인사이트 제공 가능**

- 딥러닝 모델을 포함한 AI 알고리즘은 PoV에 통합되어 이상 징후를 탐지하고 의사결정을 향상시키는 데 활용될 수 있으며, AI 기능이 탑재된 스마트 계약은 개인정보 보호 규정을 준수하면서 의료 데이터 공유 계약을 자율적으로 실행할 수 있음
- 웨어러블 센서 등 IoT 기반 의료 기기는 대량의 실시간 데이터를 생성하며, 이를 PoV에 통합하면 데이터 수집 및 공유 과정을 간소화하고 환자 치료 결과와 운영 효율성을 향상시킬 수 있음
- 연합 학습(Federated Learning)은 데이터를 로컬에 유지한 채 모델 업데이트만 공유하여 개인정보를 보호하며 AI 모델을 학습할 수 있는 방식을 제공
- 최근 연구에서 블록체인과 대규모 언어 모델(LLM)의 통합이 탐구되고 있으며, 이는 AI 기반 의료 인사이트에 대한 신뢰를 높일 수 있는 가능성을 제시

- PoV(Proof of Visit) 알고리즘은 의료 서비스 환경에 최적화된 구조를 통해 EHR 데이터의 안전한 공유와 개인정보 보호를 동시에 달성할 수 있는 실현 가능한 블록체인 기반 솔루션으로 주목
- AI, IoT, 연합 학습, LLM 등 첨단 기술과의 융합을 통해 PoV 기반 의료 시스템은 의료 데이터 활용, 신뢰성 확보라는 측면에서 새로운 의료 인프라의 가능성을 제시

[출처]

- Science Direct, 'New blockchain consensus algorithm applied on healthcare industry: Proof of Visit-(POV)', 2025.04.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

DeFi 보안 통제와 중앙화 구조의 상호작용

- DeFi는 탈중앙화를 지향하지만, 실제로는 중앙화 요소가 존재하며, 위기 시에는 통제가 불가피할 수 있음
- 중앙화 자체보다 그 존재를 숨기거나 과장하는 방식이 문제이며, 사용자에게 구조와 리스크를 투명하게 전달하는 것이 신뢰 회복의 핵심으로 간주됨

DeFi와 온체인 금융은 탈중앙화를 핵심 가치로 내세우지만, Hyperliquid 사례에서 보듯 위기 상황에서는 중앙화된 통제가 작동할 수 있으며, 이는 사용자 기대와 현실 간의 간극을 드러내고, 탈중앙화의 이상과 구조적 현실 사이의 균형 조정 및 투명한 구조 설명의 필요성을 시사

▶ DeFi와 탈중앙화 개념 사이의 오해 및 현실적 구조 차이에 대한 인식 필요성

- Web3 생태계에서의 탈중앙화 수준은, 네트워크의 보안성, 공정성, 검열 저항성을 판단하는 핵심 요소로 간주되며, 오랜 기간 동안 학계와 업계 모두에서 지속적인 분석과 평가의 대상으로 주목
- 이는 단일 실패 지점이 없는 대안적 시스템을 제공하겠다는 기술적 약속에 기인하며, 시간이 흐르면서 '나카모토 계수(Nakamoto Coefficient)'와 같은 지표를 통해 네트워크의 분산화 정도를 계량적으로 측정하려는 시도가 나타남
- 이러한 흐름과 병행하여, DeFi는 다양한 금융 상품과 연결되며, 실제 블록체인 기반 금융 애플리케이션은 각 제품의 보안 설계에 따라 상이한 수준의 내부 통제 체계를 보유
- 더불어 DAI는 가장 탈중앙화된 스테이블코인으로 간주되는 반면, USDC는 고도로 중앙화된 구조를 지니고 있어 "중앙화는 항상 부정적인가?"라는 근본적인 질문이 제기됨
- 이러한 문제의식은 최근 하이퍼리퀴드(Hyperliquid)가 유동성 위기에 직면하면서 재차 주목 받음
- 그 외에도 솔라나 기반의 밌코인 젤리(JELLY)는 외부 취약점이 아닌 플랫폼 자체의 구조적 메커니즘을 활용한 고위험 공격을 통해 최대 500%에 이르는 급등세를 기록
- 이로 인해 시장 상황은 급격히 악화되었고, 약 2억 3천만 달러 상당의 자금이 위험에 노출되면서, 탈중앙화의 실효성과 구조적 안정성에 대한 논의가 재차 주목받음

▶ 외부 청산자 부재로 인해 프로토콜이 손실 부담을 떠안게 된 구조적 한계

- 한 트레이더는 20배 레버리지를 활용하여 600만 달러 규모의 공매도 포지션을 개설한 후, 스팟 시장에서 대량 매수를 단행하여 JELLY 가격을 인위적으로 끌어올렸음
- 이로 인해 고의적으로 공매도 포지션이 청산되었으며, 해당 리스크는 프로토콜이 떠안게 되었으며, 외부 청산자가 없자 Hyperliquid의 내부 금고가 자동 메커니즘에 따라 해당 포지션을 떠맡게 되었음
- 혼란이 극심했던 시점에서 Hyperliquid는 392백만 JELLY를 시장가보다 낮은 \$0.0095에 강제 청산 하였으며, 이로 인해 703,000달러의 수익 창출 후 JELLY를 상장폐지


Alex Krüger 
 @krugermacro · Follow

Hyperliquid. What's the solution?


CRG 
 @MacroCRG

Damn, this is fkin wild. From what I can gather:

Someone shorted jellyjelly on hyperliquid

I assume pumped it himself onchain (smol coin)

Liquidating himself and thus forcing hyperliquid to inherit the toxic short position

Now jellyjelly is giga pumping and hyperliquid are

Value	Entry Price	Mark Price	PnL (ROE %)	Liq. Price	Margin	Funding
0.99926	0.011282	0.037601	-\$10,488,022.16 (-4,665.7%)	0.18485	\$749,049.96 (Cross)	\$0.00
57.48	14.918	14.864	+\$1,000.04 (+7.0%)	3.0613	\$14,292.87 (Cross)	\$0.00
30.78	0.002902	0.002864	-\$3,188.84 (-26.2%)	N/A	\$11,841.54 (Cross)	\$451.08
88.07	0.014948	0.014557	-\$4,848.60 (-52.3%)	N/A	\$8,653.40 (Cross)	\$44.25
53.57	143.87	141.87	-\$2,102.17 (-27.8%)	N/A	\$7,447.88 (Cross)	-\$1,150.18
5.84	2.0612	2.0367	-\$1,179.54 (-23.8%)	N/A	\$4,896.80 (Cross)	\$189.53
7.80	0.015224	0.014945	-\$1,594.62 (-36.7%)	N/A	\$4,270.89 (Cross)	\$3.60
1.04	87.873	87.182	-\$443.30 (-11.2%)	N/A	\$3,937.05 (Cross)	\$290.37
8.92	0.007229	0.007071	-\$1,541.54 (-43.7%)	N/A	\$3,449.45 (Cross)	-\$68.97
9.49	0.60567	0.57629	-\$3,365.76 (-97.0%)	N/A	\$3,300.67 (Cross)	\$35.10
5.86	0.52636	0.51292	-\$1,623.65 (-51.1%)	N/A	\$3,097.29 (Cross)	\$116.06
9.23	0.54916	0.54717	+\$218.87 (+7.2%)	533.25	\$3,008.96 (Cross)	\$184.75
8.18	1.3417	1.3208	-\$804.24 (-31.2%)	1,356.6	\$2,854.81 (Cross)	\$31.91
4.88	4.1069	4.0409	-\$778.81 (-27.9%)	N/A	\$2,798.93 (Cross)	\$1.81

1:22 AM · Mar 27, 2025

47 Reply Copy link

출처: Forbes, 'DeFi Not So Decentralized: Hot Take From The Hyperliquid Scandal', 2025.04.01.

- 결과적으로 플랫폼의 존속은 유지되었지만 탈중앙화 프로토콜이 위기 상황에서 중앙화된 대응을 취할 수 있음을 보여준 사례로 남았음

▶ 온체인 금융은 탈중앙화 기능을 배제하며, 중앙화 요소가 보안 기능으로 작동하는 사례들과 그 정당성에 대해 논의

- DeFi는 본질적으로 탈중앙화를 핵심 가치로 내세우는 다양한 금융 프로토콜들을 포함하고 있으나, 실제 운용 구조를 살펴보면 각 프로토콜마다 거버넌스, 접근 권한, 보안 설계 등에서 상이한 수준의 통제 체계를 보유
- 이른바 '탈중앙화 금융(DeFi)'은 단순한 토큰 거래를 넘어 탈중앙화 거래소(DEX), 대출·차입 플랫폼, 무기한 선물(perpetual contracts, 또는 perp), 그리고 스테이블코인 등 광범위한 범주의 프로토콜들을 아우르며, 그 범위와 복잡성이 점차 확대
- 따라서, 탈중앙화를 전면에 내세우는 자체가 문제라기보다는, 해당 프로토콜이 실제로 구현하는 분산화 수준을 과장하거나 사용자에게 오인될 수 있도록 전달하는 방식이 더 큰 문제로 지적됨

▶ **DeFi와 온체인 금융은 탈중앙화를 지양하나, Hyperliquid 사례와 같이 위기 상황에서는 중앙화된 통제 시스템이 작동할 수 있어 사용자의 기대와 현실 사이의 균형 조정의 필요성을 보여줌**

- 프로토콜의 탈중앙화 기능에 대해 사람들을 오도하는 것은 잘못된 일이지만, 블록체인 기반 금융의 더 넓은 스펙트럼을 고려한다면 중앙화는 도움이 될 수 있음
- 그러나 Hyperliquid가 위기 시기에 한 대응은 사용자들로 하여금 “탈중앙화 프로토콜이 왜 이런 결정을 내렸는가”라는 의문을 유발하였으며, 탈중앙화의 이상과 현실 사이의 균형 조정이 필요함을 강조
- Hyperliquid 사건은 DeFi 플랫폼들이 실제로 탈중앙화된 상태로 작동하다가도 위기 상황에서 통제력을 행사하게 되는 이중적 구조를 드러냄
- 예를 들어, 온체인 금융은 탈중앙화 구조에 반드시 의존하지 않으며, 일반적으로 중앙화된 수탁자나 거래 상대방이 개입하는 프로세스를 포함
- 수탁자, 브로커, 관리자 등이 탈중앙화되지 않은 경우에도 금융 부문은 블록체인의 투명성과 자동화 등 주요 혜택을 충분히 활용하는 혜택을 누릴 수 있음
- 이러한 맥락에서, 우리는 이제 완전히 탈중앙화된 플랫폼이 실현할 수 있는 가능성과 동시에 동반될 수 있는 구조적·보안적 위험 요인을 명확히 구분하고, 양자의 균형 속에서 블록체인 기술의 적용 방식을 재정의해야 할 시점에 도달했음을 의미

▶ **탈중앙화를 내세우는 DeFi 프로젝트는 중앙화 요소의 존재를 숨기지 말고 투명하게 전달해야 하며, 신뢰 회복을 위해 통제 구조와 위험 요소에 대한 명확한 설명이 필수적**

- 중앙화된 요소의 존재가 본질적으로 문제가 되는 것이 아니라, 해당 요소가 존재함에도 불구하고 이를 숨기거나 과장하여 탈중앙화를 주장하는 것이 문제
- Circle과 같은 기관이 악용 사례 발생 시 USDC를 동결할 수 있는 권한은 중앙화된 통제 장치이지만, 이는 불법 활동 차단이나 사용자 자산 보호 측면에서 중요한 보안적 기능을 수행
- 반면, 사람들이 프로토콜을 신뢰하고 그 탈중앙화라는 명분을 염두에 두고 사용하면 일부 트레이더들이 Hyperliquid의 이 문제 해결 방식에 불만을 품는 것은 당연시됨
- DeFi에 대한 신뢰를 회복하기 위해서는, 사용자들이 기대하는 탈중앙화 수준과 실제 구조 사이의 차이를 명확히 설명하고, 프로젝트의 통제 방식과 위험요소를 투명하게 전달하는 노력이 필요

- 탈중앙화는 이상적인 가치로 기능하지만, 실제 DeFi와 온체인 금융의 운영 구조는 다양한 수준의 중앙화 요소를 포함하고 있으며, 위기 상황에서 중앙화된 개입이 작동할 수 있다는 점에서 사용자 기대와 현실 간의 조율이 필요
- 중앙화된 통제 장치 자체가 문제가 되기보다는, 이를 숨기거나 과장하여 탈중앙화된 것처럼 포장하는 방식이 DeFi 신뢰를 훼손하며, 구조적 통제 수준과 리스크를 투명하게 공개하는 것이 생태계의 지속 가능성을 위한 핵심 조건

[출처]

- Forbes, 'DeFi Not So Decentralized: Hot Take From The Hyperliquid Scandal', 2025.04.01.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[영국, 북한]

영국, 블록체인 프로젝트 직원 중 북한 기술 노동자 발견

- 미국의 단속으로 인해 북한의 가짜 노동자들이 자금 흐름을 유지해야 하는 압박을 받으면서 강탈 시도가 증가
- 구글에 따르면, 북한과 관련된 사기성 기술 종사자들이 당국의 감시가 강화되자 미국 이외의 블록체인 회사로 침투 작전을 확대하고 있으며, 그 중 일부는 영국의 암호화폐 프로젝트에도 침투한 것으로 나타남

GTIG는 2023년 말 이후 북한 기술 인력의 금전적 압박이 커지면서 더 대형 조직을 대상으로 한 갈취 시도가 증가했다고 밝혔으며, 해고된 IT 인력이 이전 고용주에게 민감 데이터를 공개하거나 경쟁사에 넘기겠다고 협박하는 사례가 증가하고 있어 내부 소스코드, 지적 재산, 프로젝트 문서를 무기로 삼고 있음

▶ 미국의 감시 강화로 인해 북한 IT 인력의 블록체인 업계 침투가 글로벌화되는 추세

- 구글 위협 인텔리전스 그룹(Google Threat Intelligence Group, GTIG)의 자문관 제이미 콜리어는 4월 2일 발표한 보고서를 통해 북한 연계 사기성 기술 인력이 미국 외 블록체인 기업으로 범위를 확장하고 있다고 밝힘
- 미국의 감시 강화와 자격 확인 절차의 엄격함으로 인해, 이들은 위조 신분으로 국제 인물표를 구축해 잠입 유연성을 높이고 있으며, 일부는 영국 내 블록체인 프로젝트에 채용되어 활동한 정황을 확인
- 콜리어의 발언에 따르면, 북한 관련 인력은 단순 웹 개발뿐만 아니라 인공지능 웹 애플리케이션과 블록체인 기반 채용 마켓플레이스 같은 첨단 프로젝트에도 침투한 것으로 드러남
- 한 인력은 유럽 내 12개 이상의 가짜 신분을 활용했고, 독일과 포르투갈 직업사이트의 사용자 계정 접근 정보와 위조 여권을 제작하는 중개인 관련 자료 또한 발견
- 북한 노동자들은 합법적인 근로자로 위장하여 기업에 침투하며, 수익을 북한 정권에 송금하는 구조이며, 이로 인해 해당 기업은 스파이 행위, 데이터 유출, 운영 중단 등 다양한 보안 리스크에 직면
- 2024년 1월, 미국 법무부는 최소 64개 미국 기업에 침투한 북한 국적자 2명을 기소함
- 미국 재무부 산하 해외자산통제국(OFAC)도 북한 정권의 원격 IT 근로자 위장 활동과 관련된 프런트 기업에 대해 제재를 가함
- 2024년 3월 13일에는 최소 3명의 암호화폐 창업자가 딥페이크와 가짜 줌 회의 등을 통해 기밀 자료를 탈취하려는 북한 해커의 시도를 막아냈다고 보고

- 북한 IT 인력은 미국의 감시 강화 이후 위조 신분과 국제 인물표를 활용해 유럽 등 글로벌 블록체인 기업으로 침투 범위를 확장하고 있으며, 단순 개발을 넘어 첨단 프로젝트에도 깊숙이 관여하고 있어 보안 위협이 다변화
- 기업 내부에 침투한 북한 기술 인력은 해고 후 지적 재산과 내부 데이터를 무기로 협박하거나 유출 위협을 가함에 따라, 블록체인 기업은 채용 단계에서의 정밀한 신원 검증과 내부 정보 보호 체계 강화가 시급한 과제로 부상

[출처]

- Cointelegraph, 'North Korea tech workers found among staff at UK blockchain projects', 2025.04.02.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[케냐]

Ripple과 파트너들, 케냐 가뭄 구호를 위한 블록체인 지원 시범 프로그램 실시

- 블록체인 기술을 통해 모든 거래가 공개 원장에 기록되어 자금 분배의 투명성을 보장 및 행정 비용 절감
- 위성 기반 식생 지수(NDVI)를 사용하여 가뭄 위험을 조기에 감지하고, 조건이 임계값 이하로 떨어지면 자동으로 지원금을 지급하여 위기가 심화되기 전에 지원이 이루어지도록 함

리플은 RLUSD 스테이블코인과 스마트 계약 기반 시스템을 통해 케냐 가뭄 피해 지역에 위성 데이터 연동 자동지급 방식으로 선제적 구호금을 전달함으로써, 투명성, 속도, 금융 접근성을 동시에 개선하는 블록체인 기반 재난 대응 모델을 제시

▶ 리플의 RLUSD 스테이블코인을 활용한 케냐의 극심한 가뭄 피해 지역을 위한 블록체인 구호금 전달 시스템

- 리플은 투자기관인 머시코어 벤처스 및 금융 플랫폼을 운영하는 DIVA 도네이트와 협력하여, 케냐의 가뭄 피해 지역 주민들을 위한 블록체인 기반 구호 지원 시스템을 도입
- 본 프로젝트는 라이키피아 카운티 북부 지역의 유목민 커뮤니티를 대상으로 하며, 블록체인 인프라와 스마트 계약을 통해 투명하고 신속한 지원금 지급을 실현
- RLUSD라는 미국 달러에 연동된 스테이블코인을 활용하여, 재난 대응 속도를 높이는 방안으로 주목
- 이번 프로젝트는 NDVI(Normalized Difference Vegetation Index, 정규화 식생 지수)를 기반으로 한 위성 관측 데이터를 활용하여 풀 상태 및 생육 밀도를 지속적으로 모니터링하는 시스템을 활용
- NDVI 수치가 임계값 이하로 떨어지면, 시스템은 자동으로 등록된 수혜자에게 RLUSD를 지급함
- 이때, 약 75달러 상당의 RLUSD가 각 가구에 전달되며, 이는 가축 한 마리의 6개월간 사료 및 급수 확보에 필요한 금액에 해당하며, 결과적으로 재난 발생 이전 단계에서 선제적으로 지원이 이루어지는 구조
- 이 블록체인 기반 한 시스템은 거래 내역을 공공 원장에 기록하여 모든 이해관계자가 자금 흐름을 추적할 수 있도록 설계되었고, 스마트 계약을 통해 중간 관리자 없이 자동 실행이 가능하며, 이로 인해 행정 비용 절감과 자금 유용 방지 효과를 기대
- RLUSD 기반 구조는 은행 서비스에 접근이 어려운 지역 주민들에게 디지털 방식으로 직접적인 금융 지원을 제공하는 형태임

- 스테이블코인과 스마트 계약을 활용한 블록체인 기반 구호 시스템은 재난 발생 전 조기 대응을 가능하게 하고, 행정 비용 절감 및 자금 투명성을 확보하는 새로운 공공지원 모델로 주목
- 은행 인프라가 부족한 지역에서도 디지털 자산을 통해 직접적인 금융 지원이 가능해짐에 따라, 스테이블코인은 단순 결제 수단을 넘어 인도주의 및 개발금융 수단으로서의 가능성을 보임

[출처]

- Cointrust, 'Ripple and Partners Pilot Blockchain Aid for Kenyan Drought Relief', 2025.04.05.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[유럽]

MiCA의 실수: EU 정책이 미국 달러의 지배를 촉진

- MiCA는 유로화 기반 스테이블코인에 대한 엄격한 규제를 도입하여, 이러한 스테이블코인의 성장을 저해
- 현재 스테이블코인 시장의 99% 이상이 미국 달러에 연동되어 있으며, MiCA의 규제로 인해 유로 기반 스테이블코인의 경쟁력이 약화되어 달러 기반 스테이블코인의 지배력이 더욱 강화될 수 있음

EU는 중앙은행 디지털화폐(CBDC)인 디지털 유로를 통해 유로의 영향력을 강화하려 하지만, 정부 주도의 이러한 시도가 민간 부문의 혁신에 비해 효율성과 적응력에서 뒤처질 수 있다는 우려를 제기

▶ 유럽의 의도치 않은 MiCA 규제가 CBDC 우선정책에 힘을 실으면서 유로화 경쟁력 약화로 이어지는 결과 발생

- 유럽연합의 암호자산 시장법(MiCA)은 암호화폐 시장 내 명확성·안정성 확보를 위한 규제 체계로 설계됨
- 그러나 이 규제는 유로화 기반 스테이블코인에 대해 과도하게 제한적인 입장을 취해서, 결과적으로 미국 달러화 기반 스테이블코인의 세계적 지배력을 더욱 공고히 하는 결과를 초래함
- 현재 스테이블코인 시장의 99% 이상이 미국 달러에 연동되어 있으며, MiCA는 이러한 시장 구조에 도전하는 것이 아니라 이를 강화하는 방향으로 작용
- MiCA는 공식적으로 “우리는 스테이블코인을 원하지 않는다”라고 선언하지 않았지만, 현실적으로는 유로화 스테이블코인을 실행 불가능하게 만드는 수준의 규제를 도입
- 이는 민간 스테이블코인 개발을 억제하고 CBDC에 힘을 실어주는 간접적 정책 수단으로 해석 가능
- 이렇게 형성된 환경은 결국 미국 달러 기반 스테이블코인에 대한 글로벌 의존도를 더욱 강화시키게 되었으며, 미국은 민간 주도의 스테이블코인을 장려하며 혁신성과 유연성을 유지하고 있음
- 미 정부는 중앙은행 디지털화폐(CBDC) 도입을 미루는 대신, 민간 부문이 주도하는 기술 발전을 지원함으로써 글로벌 경쟁력 유지에 초점을 맞추고 있음
- MiCA를 통한 규제 중심 접근은 자본·인재·혁신의 이탈을 초래하고 있으며, 이는 결국 유럽이 차세대 글로벌 금융 인프라 질서에서 수동적 역할에 머무르게 되는 결과로 이어질 수 있음
- 유로화가 국제적 입지를 확보하기 위해서는 보다 민간 주도의 혁신을 허용하고, 스테이블코인 생태계를 적극적으로 육성하는 정책 전환이 필요

- 유럽의 MiCA 규제는 유로화 기반 스테이블코인에 과도한 제약을 가함으로써 미국 달러 기반 스테이블코인의 지배력을 오히려 강화시키고 있으며, 이는 유럽의 디지털 금융 주도권 상실로 이어짐
- 국제 금융 질서에서 유로화의 경쟁력을 확보하기 위해서는 민간 주도의 스테이블코인 혁신을 허용하고, 규제보다는 생태계 육성 중심의 정책 전환이 시급

[출처]

- CryptoSlate, 'MiCA's mistake: EU policy encourages US dollar dominance', 2025.04.05.