

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

1. TrustChain: 신뢰할 수 있는 개인 정보 보호 스마트 계약 모델
2. Pectra 및 Fusaka 업그레이드는 이더리움에 어떤 의미가 있을까?
3. 두바이 AI 주간 개막: 알 올라마 장관, 모든 기업의 AI 우선시를 강조
4. 최신 FBI 보고서에서 밝혀진 사이버 범죄
5. 파리 블록체인 주간 요약: 활동 가중 블록체인 합의가 주목을 끌다

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

TrustChain, 신뢰할 수 있는 실행 환경을 갖춘 개인 정보 보호 스마트 계약 모델

- 스마트 계약의 개인정보 보호와 보안을 보장하기 위해 TEE 기반의 스마트 계약 모델인 TrustChain을 도입
- DAG(Directed Acycle Graph) 기반 원장의 이점과 TEE의 고성능을 결합하여 스마트 계약 성능을 향상시킴

연구진은 합의 메커니즘을 수정하여 민감 정보를 블록체인에 기록하지 않고, 실행 결과만을 저장하는 DAG(Directed Acyclic Graph) 기반 그래프의 이점을 고성능 TEE와 결합하여 처리 성능을 향상시킴

▶ 블록체인의 공개성과 정보 공유 구조로 인해 개인정보 보호 문제가 대두되며, 이를 해결하기 위해 연구진은 TEE 기반의 고성능 스마트 계약 시스템인 TrustChain을 제안함

- 블록체인의 급속한 발전으로 사물인터넷, 금융 등 다양한 분야에서 주목을 받고 있으나, 다수 사용자가 원장을 공유하는 특성으로 인해 거래 금액, 사적 계약 등 민감한 사용자 정보가 노출될 우려가 존재함
- 이러한 개인정보 노출 문제를 해결하기 위해, 연구진은 신뢰 실행 환경(Trusted Execution Environment, TEE)을 기반으로 한 고성능 스마트 계약* 모델인 TrustChain을 제안함
- * 스마트 계약: 계약 조건을 자동으로 실행하는 계산 가능한 거래 프로토콜

▶ 하이퍼레저 패브릭은 기존 블록체인과 다른 실행 중심 구조와 역할별 노드 구성으로 트랜잭션 처리 방식을 재구성한 프라이빗 블록체인 플랫폼임

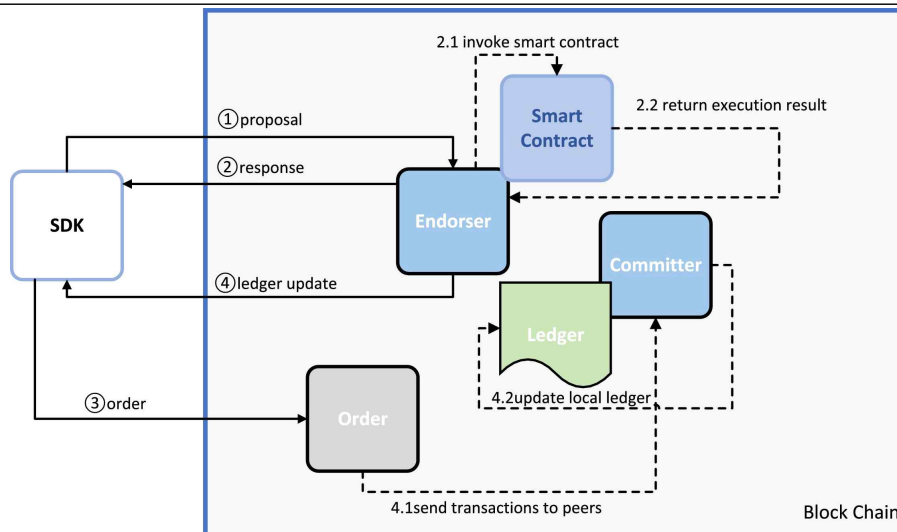
- 하이퍼레저 패브릭(Hyperledger Fabric)에서는 스마트 계약을 체인코드(Chaincode)라고 하며, 사용자는 체인코드를 통해 원장 데이터를 조작하고 상호작용할 수 있음
- Tendermint와 이더리움을 포함한 대부분의 블록체인 플랫폼은 '주문-실행(Order-Execute)' 아키텍처를 채택하여, 트랜잭션을 패키징한 후 각 노드에 전파하고 순차적으로 실행함
- 반면, 하이퍼레저 패브릭은 '실행-주문-검증(Execute-Order-Validate)' 아키텍처를 도입하여 트랜잭션 처리 흐름을 재구성함
- 하이퍼레저 패브릭의 노드 아키텍처는 작업에 따라 인도서(Endorsers), 커미터(Committers)로 구분되며, 추가적으로 오더러(Orderers)가 트랜잭션 정렬을 담당함

▶ 하이퍼레저 패브릭은 트랜잭션을 실행-주문-검증의 순서로 처리하여 성능과 유연성을 확보하며, 각 단계는 클라이언트와 노드 간의 상호작용을 통해 진행됨

- **(Execute 단계)** Execute 단계에서는 클라이언트가 트랜잭션을 발행하고, 이 트랜잭션 정보를 인도서(Endorser) 노드에 전송함
- 전송된 트랜잭션 정보를 수신한 인도서 노드는 트랜잭션 정보를 기반으로 트랜잭션을 실행하고, 그 결과를 검증하여 클라이언트에게 반환함

- 검증이 완료된 결과만 클라이언트에게 전달되어 이후 단계로 진행할 수 있는 기반을 마련함
- **(Order 단계)** 하이퍼레저 패브릭의 Order 단계는 클라이언트 검증 후 오더러 노드로 트랜잭션 전파 및 정렬하고, 클라이언트는 인도서로부터 받은 검증 결과를 수집한 후, 엔도스먼트 정책(Endorsement Policy) 충족 여부를 확인함
- 엔도스먼트 정책이 충족되면, 클라이언트는 트랜잭션을 모든 오더러(Orderer) 노드에 브로드캐스트함
오더러 노드는 합의 메커니즘을 이용해 트랜잭션을 정렬하는 과정을 수행함
- **(Validate 단계)** 하이퍼레저 패브릭의 Validate 단계는 커미터 노드의 최종 검증과 블록체인 반영하고, 오더러가 정렬한 트랜잭션을 블록 형태로 모든 커미터(Committer) 노드에 브로드캐스트함
- 커미터 노드는 수신한 블록 내 각 트랜잭션을 검증하여 입력과 출력이 현재 블록체인 상태와 일치하는지 확인하며, 검증이 완료된 후 해당 블록을 로컬 블록체인에 추가하여 상태를 업데이트함

[Hyperledger Fabric의 스마트 계약 작동 메커니즘]

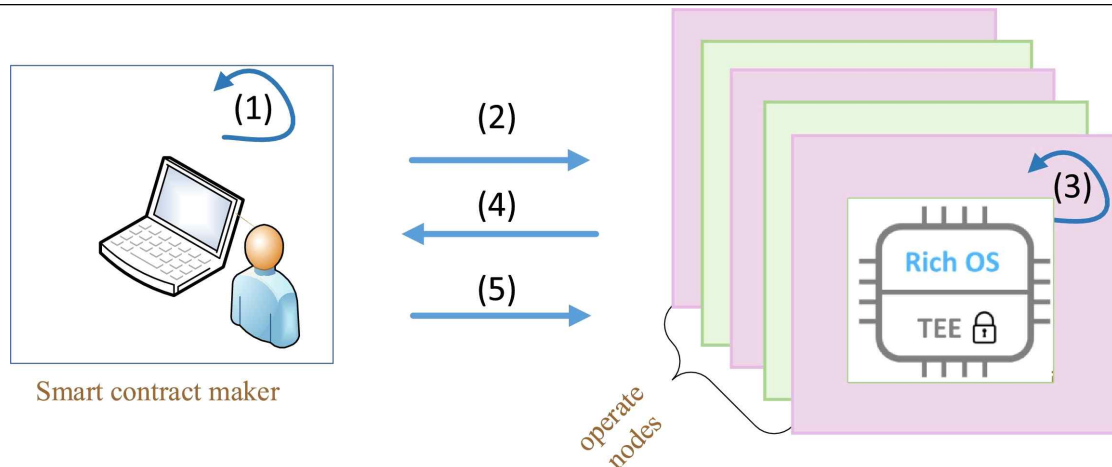


출처: Science Direct, 'TrustChain: A privacy protection smart contract model with Trusted Execution Environment', 2025.04.25.

▶ **TrustChain은 스마트 계약 코드의 프라이버시 보호와 무작위 노드 선택을 통해 보안을 확보하고, DAG 기반 원장을 활용하여 기존 블록체인 대비 35.4% 높은 처리량을 달성함**

- 결론적으로, 연구진들은 스마트 계약의 실질적으로 활용하기 위해서는 개인정보 보호 문제를 해결해야 하며, 이를 해결하기 위해 스마트 계약 코드와 온체인 데이터의 개인정보 보호를 실현하고자 신뢰 실행 환경(TEE)을 스마트 계약과 효과적으로 결합함
- 설계된 스마트 계약 코드는 블록체인에 저장되지 않고, 운영 노드의 TEE에 저장되어 코드 자체의 프라이버시를 보호하며, 또한, 검증 가능한 난수 함수(Verifiable Random Function)를 사용하여, 스마트 계약을 실행할 운영 노드 집합을 매번 무작위로 선정함으로써, 해당 노드들의 보안을 보장함

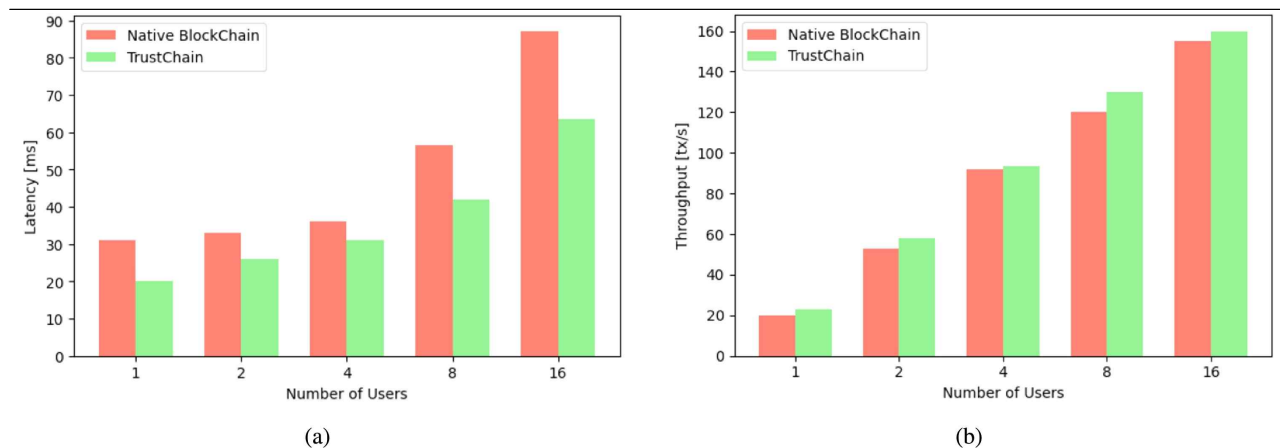
[타원 곡선 암호(ECC)를 기반으로 한 VRF 작동 메커니즘]



출처: Science Direct, 'TrustChain: A privacy protection smart contract model with Trusted Execution Environment', 2025.04.25.

- TEE는 개인정보 보호뿐만 아니라 고성능 처리 능력도 제공하는데, 이러한 장점을 활용해 스마트 계약의 처리량을 높이기 위해, 기존의 체인 원장 대신 방향성 비순환 그래프(DAG) 기반의 그래프 원장을 사용함
- 실제 분석과 실험을 통해, 이 구조는 강력한 프라이버시 보호 및 보안성은 물론 높은 성능을 발휘함이 입증되었으며, 결과적으로, 본 솔루션의 처리량은 기존 블록체인 대비 약 35.4% 향상됨

[시스템 사용자 수에 따른 통신 지연]



출처: Science Direct, 'TrustChain: A privacy protection smart contract model with Trusted Execution Environment', 2025.04.25.

- 블록체인의 공개성과 원장 공유 특성으로 인한 개인정보 보호 한계를 극복하기 위해, 신뢰 실행 환경(TEE) 기반의 TrustChain과 같은 보안 강화형 스마트 계약 모델이 필수적임을 보임
- 기존 체인 구조의 한계를 보완한 DAG 기반 원장과 TEE의 결합은 개인정보 보호는 물론 고성능을 동시에 달성할 수 있음을 실험적으로 입증하며, 스마트 계약의 실질적 활용 가능성을 크게 확장시킴

[출처]

- Science Direct, 'TrustChain: A privacy protection smart contract model with Trusted Execution Environment', 2025.04.25.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

Pectra 및 Fusaka 업그레이드는 이더리움에 어떤 의미가 있을까?

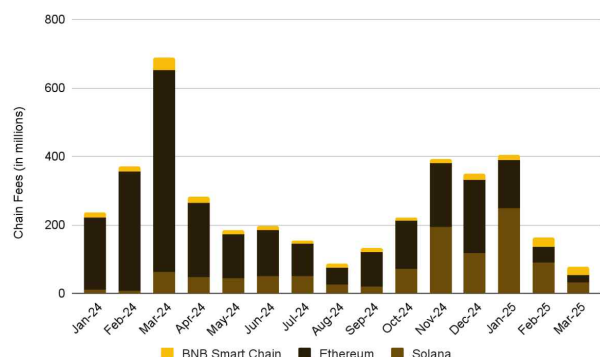
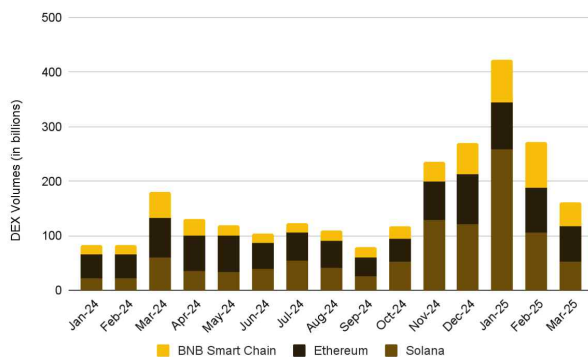
- 이더리움은 Layer 2 확장에 집중하고 있으나, 데이터 가용성 측면에서 Celestia, EigenDA 등과의 경쟁에서 뒤처지고 있으며, Layer 2의 부상으로 인해 이더리움 자체의 가치 축적 지속 가능성에 대한 우려가 제기

2025년 말 이더리움은 Pectra, Fusaka 업그레이드를 고려 중이며, Pectra는 스테이킹, 블롭(Blob) 처리, 계정 추상화의 특징을 가지고 Fusaka는 데이터 가용성 확장, EVM 업그레이드의 특징을 지님

▶ 이더리움은 최근 솔라나와 BNB 체인의 경쟁으로 입지가 흔들리고 있으며, 향후 업그레이드인 Pectra와 Fusaka는 L2 확장을 위한 데이터 가용성에 집중됨

- 이더리움은 오랜 기간 지배적인 레이어 1(L1) 블록체인으로 자리매김해왔지만, 최근 몇 달간 솔라나와 BNB 스마트 체인(BNB Smart Chain)과의 치열한 경쟁에 직면함
- 특히 솔라나는 경우에 따라 탈중앙화 거래소(DEX) 활동량과 체인 수수료 측면에서 이더리움을 앞섰으며, BNB 스마트 체인 또한 2025년 내내 그 격차를 꾸준히 좁혀오고 있음

[체인별 DEX 규모(좌), 체인별 수수료(우)]



출처: Binance, 'Pectra and Fusaka Upgrades: What Does It Mean for Ethereum?', 2025.04.16.

- 이더리움이 시장 내 입지를 일부 잃고 있는 이유 중 하나는 L1에서의 느리고 비싼 거래 비용으로, 이는 사용자 경험에 마찰을 유발함
- 또 하나의 주요 요인은, 레이어 2(L2)의 인기가 높아지면서 개발자의 관심과 유동성이 분산되고 있다는 점입니다. 또한 실행을 L2로 오프로드한 이후 L1로의 가치 포착이 줄어든 점도 문제로 지적됨
- 현재 이더리움 로드맵에는 ▲더 저렴한 거래 ▲강화된 보안 ▲개선된 사용자 경험 ▲미래 대응을 위한 기능 등 L1 업그레이드가 포함됨
- 그러나 현재로서는 L1에서 더 많은 L2를 수용할 수 있도록 데이터 가용성을 확장하는 데 초점이 맞춰짐
- 본 보고서에서는 2025년 5월과 연말에 각각 메인넷 적용이 예정된 Pectra와 Fusaka 업그레이드를 다루며, 두 업그레이드는 ETH를 '울트라사운드 머니(ultrasound money)'로 강화하거나, 검열 저항성을 높이는

코드를 포함하지 않으며, 대신 L2 확장을 위한 기반 마련을 목표로 함

▶ **Pectra 업그레이드는 스테이킹 한도 상향, 블록 용량 확대, 계정 추상화 도입을 통해 사용자 경험과 L2 확장 기반을 강화하는 대규모 업그레이드임**

- Pectra는 당초 2025년 3월 출시 예정이었으며, 총 11개의 EIP(Ethereum Improvement Proposal)*를 포함해 2024년 Dencun 이후 가장 큰 하드포크가 될 예정이었음
*EIP: 이더리움의 기능 개선 또는 추가를 위한 공식 제안서
- 하지만 개발자들은 범위가 지나치게 크다는 판단하에 업그레이드를 분할하기로 합의했고, 그 결과 두 번째 업그레이드인 Fusaka는 2025년 말로 연기됨
- 더불어 Holesky 및 Sepolia 테스트넷에서 발생한 이슈로 인해 Pectra의 출시도 함께 지연되었지만, Holesky가 Hoodi로 대체된 후에 안정적인 성능을 보이며 Pectra 업그레이드는 3월 26일 최종 확정됨
- Pectra의 핵심 개선 사항은 ▲스테이킹 ▲블록(Blob) ▲계정 추상화에 중점을 두며, 향후 영지식 암호화 및 비상태 클라이언트를 지원할 기반을 마련하게 됨
- **(Pectra #1 스테이킹)** 가장 핵심적인 코드 업그레이드는 EIP-7251로, 스테이킹의 최대 유효 잔액(MaxEB)을 기존 32 ETH에서 2,048 ETH까지 상향하는 것이 목표임
- 기존에는 32 ETH를 초과한 보상은 각 블록마다 검증자의 출금 주소로 자동 전송되었지만, 향후에도 최소 잔액 기준은 32 ETH로 유지되어 개인 검증자의 참여를 장려함
- 이전의 32 ETH 상한으로 인해, 많은 지분을 보유한 스테이킹 풀이나 중앙화 거래소는 보상을 극대화하기 위해 여러 검증자를 운영해야 했음
- 2025년 4월 1일 기준, 이더리움 메인넷에는 106만 개 이상의 검증자가 존재하며, 이는 지분증명(PoS) 전환 이후 지속적으로 증가한 수치임
- 표면적으로는 검증자 수 증가가 참여 확대처럼 보일 수 있지만, 실상은 소수 기관에 지분이 집중되어 진정한 의미의 탈중앙화가 제한된 상태임
- **(Pectra #2 블록(Blobs))** 블록은 EIP-4844를 통해 처음 도입되었으며, 이는 Dencun 업그레이드의 일환으로 L2가 더 저렴하게 이더리움 메인넷에 데이터를 게시할 수 있도록 설계되었으며, 이후 EIP-7691을 통해 블록의 타깃 및 최대 용량은 각각 3→6, 6→9로 확대될 예정임
- L2 솔루션은 데이터 가용성을 확보하기 위해, 이더리움 L1에 저비용으로 데이터를 게시하는 방법이 필요하며, 블록 용량의 확대는 결과적으로 게시 비용 절감과 사용자 거래 수수료 감소로 이어짐
- **(Pectra #3 계정 추상화)** EIP-7702는 ERC-4337의 정제된 형태로, 계정 추상화 기능을 강화하는 제안으로, 이를 통해 일반 사용자도 트랜잭션 번들링, 가스비 대납, 패스키 기반 인증을 사용할 수 있으며, 지출 한도 설정이나 키 분실 시 소셜 복구 메커니즘을 통해 지갑을 복구할 수도 있음
- 또한 EOA(외부 소유 계정)가 스마트 계약 코드를 일시적으로 지갑에 탑재할 수 있어, 특정 트랜잭션 중에만 실행 가능한 스마트 기능을 활용할 수 있게 됨

- 즉, 사용자는 스마트 계약 계정으로 전환하거나 권한을 위임하지 않고도 모든 기능을 사용할 수 있음
- 이 제안은 특히 초보자에게 더 친숙한 지갑 환경을 제공하며, 기존에는 스마트 계약 지갑 선택에 부담을 느꼈던 사용자들의 진입 장벽을 낮춤
- 또한 정책 엔진과 지갑 주소를 분리함으로써, 기존 주소를 유지한 채 EOA를 스마트 계약 계정으로 업그레이드할 수 있고, 이로써 가스비 대납, 소셜 복구 기능 등을 새 지갑 없이 활용할 수 있게 됨

▶ **Fusaka 업그레이드는 데이터 가용성 샘플링(PeerDAS)과 코드 구조 개선(EOF)을 통해 확장성과 네트워크 효율성을 높이는 후속 업그레이드임**

- Fusaka 테스트넷은 Pectra 메인넷 적용 이후 시작될 예정이며, PeerDAS(데이터 가용성 샘플링)과 EOF(Ethereum Object Format)를 포함한 전체 업그레이드는 2025년 말까지 완료될 것으로 예상됨
- **(Fusaka #1 PeerDAS)** EIP-7594를 기반으로 도입될 PeerDAS는 완전한 데이터 가용성 샘플링(DAS)을 위한 네트워킹 프로토콜로, 전체 데이터를 다운로드하지 않고도 노드가 블록 데이터의 가용성을 검증할 수 있도록 설계됨
- PeerDAS에서는 각 노드가 일부 블록 데이터를 저장하며, P2P 네트워크에서 여러 피어와 연결을 유지함
- 기존에는 ETH 노드가 각 블록의 모든 데이터를 다운로드해야 했기 때문에 네트워크 속도가 느려지고 진입 장벽이 높아 데이터 가용성 문제로 이어졌으며, 개인에게는 진입이 어려운 환경임
- 그러나 PeerDAS를 사용하면 각 노드는 전체 데이터의 일부분만 다운로드하고, 전체 데이터 존재 여부를 확인할 수 있어 노드가 처리해야 할 데이터 양이 줄고, 노드 운영 효율성과 접근성이 높아짐
- 또한 L1의 데이터 가용성에 의존하는 롤업(Roll-up) 구조에서 PeerDAS는 자원 부담을 줄이고, 더 많은 사용자 참여를 가능케 하여 네트워크의 분산성과 안정성을 강화함
- **(Fusaka #2 EOF)** 현재 이더리움의 EVM 바이트코드는 정해진 구조가 없어, 실행 시 매번 검증이 필요하고 효율이 떨어지는 문제가 존재함
- EOF는 계약 생성 시 코드 검증을 수행하며, 계정 내 별도의 버전 필드 없이도 관리를 가능하게 함
- 이는 ▲제어 흐름 변경 ▲계정 추상화 도입 등과 같은 기능의 수명주기 관리를 용이하게 하며, 구조화된 접근 방식은 과정을 단순화하고, 실행 시의 오버헤드를 줄임
- 궁극적으로는 개발자 경험과 사용자 안전성이 향상되며, 스마트 계약 작성이 더 쉽고 안전해져, 개발자가 오류나 취약점을 피하는 데 도움을 줌

- 이더리움은 솔라나·BNB 체인 등 경쟁 체인의 부상 속에서, Pectra와 Fusaka 업그레이드를 통해 L2 확장성과 효율성 강화를 중심으로 대응하고 있으며, 이는 기존 L1 한계를 보완하려는 전략적 전환으로 해석됨
- 특히 데이터 가용성(PeerDAS)과 계정 추상화(EIP-7702), 코드 구조 정비(EOF) 같은 기술적 개편은 네트워크의 분산성과 개발자 경험을 동시에 개선함으로써, 중장기적으로 생태계 경쟁력을 높이는 핵심 수단이 될 것으로 보임

[출처]

- Binance, 'Pectra and Fusaka Upgrades: What Does It Mean for Ethereum?', 2025.04.16.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[아랍에미리트]

두바이 AI 주간 개막: 알 올라마 장관, 모든 기업의 AI 우선시를 강조

- 두바이 인공지능 국무장관은 325개 기업이 AI 솔루션 기업 인증인 AI Seal을 획득했다고 밝힘
- 또한 장관은 "누가 최고 수준의 AI를 구축하고 있는지 알고 싶다"라고 말하며 AI 혁신의 품질을 강조함

두바이는 AI를 중심에 둔 디지털 경제 전략을 바탕으로 데이터센터 구축, 인재 양성, 글로벌 협력 행사 등을 종합적으로 추진하며, 세계적인 AI 허브로 도약하겠다는 미래 비전을 구체화하고 있음

▶ 두바이는 AI를 중심의 디지털 경제 전략을 선포하고, 인증 제도와 부처별 책임자 임명을 통해 산업·행정 전반에 걸친 AI 도입을 본격화함

- 인공지능·디지털경제·원격근무 담당 국무장관인 오마르 술탄 알 올라마는 두바이 AI 위크 개막식을 통해 두바이 경제의 미래는 인공지능(AI)을 기반으로 구축될 것임을 선언하며, 향후 디지털 경제에 속하는 모든 기업은 AI 우선 전략을 채택해야 한다고 강조함
- 두바이 정부는 보안성과 책임성을 갖춘 AI 솔루션 제공 기업 식별을 위해, '두바이 AI 인증(Seal)' 제도를 도입하여 325개 기업에 인증을 부여했으며, 이 인증은 정부뿐만 아니라 민간 부문에서 신뢰할 수 있는 AI 파트너를 찾는 데 도움이 될 거라 예상됨
- 두바이는 230명 이상의 최고 인공지능 책임자를 정부 부처에 임명하여 부서별 맞춤형 AI 전략을 개발을 진행 중이며, AI 도입으로 교육, 의료, 도시 서비스 개선 등 구체적 성과 창출을 목표로 하고 있음

▶ AI 도입을 바탕으로 데이터센터 구축, 인재 양성, 글로벌 협력 행사 등을 통해 AI 생태계를 조성하고 세계적인 AI 허브로 도약하려는 비전을 실현하고 있음

- 두바이는 지난 1년 동안 17개의 AI 전용 데이터센터를 구축하고, AI 프롬프트 엔지니어링 인재 100만 명 양성을 목표로 하는 'One Million Prompters' 캠페인을 출범하며, 세계에서 가장 비즈니스 친화적인 도시로서 AI 개발 허브가 되겠다는 목표를 밝힘
- 두바이 AI 위크는 AI 리트리트, 글로벌 프롬프트 엔지니어링 챔피언십, 학교 연계 AI 행사 등 다양한 프로그램으로 꾸며졌으며, 메타, 구글, 엔비디아, 오픈AI 등 주요 기업과 15개국 정부 대표단이 참여함
- 두바이는 인프라 투자, 글로벌 협력, 비전 제시를 통해 AI 시대를 선도할 계획임을 밝히며, "AI를 무시하는 자는 도태될 것"이라는 메시지를 참석자들에게 전달함

- 두바이는 AI 중심의 국가 전략을 통해 산업과 행정 전반에 걸친 디지털 전환을 가속화하고 있으며, 인증 제도와 전담 책임자 제도를 통해 체계적인 AI 도입을 추진 중임
- 데이터센터 구축, 인재 양성, 글로벌 협력 강화를 통해 두바이는 세계적인 AI 허브로 도약하려는 명확한 비전을 제시하며, AI를 국가 경쟁력의 핵심 자산으로 규정하고 있음

[출처]

- UNLOCK, 'Dubai AI Week Kicks Off: Minister Al Olama Says Every Company Must Go AI-First', 2025.04.21.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[미국]

최신 FBI 보고서에서 밝혀진 사이버 범죄

- FBI 인터넷 범죄 신고 센터(IC3)는 미국 전역의 개인 및 기업의 사이버 사기 및 디지털 위협 신고를 수집함
- 미국인들은 85만 9천 건 이상의 사이버 범죄와 사상 최대 규모인 166억 달러의 손실이 발생했음을 밝힘

2024년 사이버 범죄는 고령층과 암호화폐 투자자를 주요 표적으로 정교하게 진화하며 피해 규모가 역대 최고치를 기록하였으며, 이에 대응하기 위해 FBI는 암호화폐 사기 대응 이니셔티브를 확대하고 있음

▶ 2024년 사이버 범죄는 고령층과 암호화폐 투자자를 중심으로 급증하며, 특히 정교한 투자 사기 수법으로 인한 피해 규모가 사상 최고치를 기록함

- 2024년 FBI의 인터넷 범죄 신고 센터(IC3)는 859,532건의 사이버 범죄 신고를 접수하였으며, 이는 전년 대비 33% 증가한 총 166억 달러의 손실로 나타나며, 사이버 범죄의 규모가 날로 증가하고 있음을 보여줌
- 60세 이상의 노년층은 147,127건의 사이버 범죄 신고를 하였으며, 총 48억 달러의 손실을 입었는데, 이는 고령자들이 정부 기관 사칭, 투자 사기 등 사이버 범죄의 주요 표적이 되고 있음을 시사함
- 암호화폐 관련 사기는 2024년에만 93억 달러의 손실을 초래하였으며, 이는 전년 대비 66% 증가한 수치임
- 그 중 특히, 암호화폐 ATM과 QR 코드를 이용한 사기가 급증했으며, 2024년에는 이러한 수단을 이용한 사기로 246.7백만 달러의 손실이 발생했는데 이는 전년 대비 99% 증가한 수치임
- 투자 사기는 2024년에만 65.7억 달러의 손실을 기록하며, 사이버 범죄 중 가장 큰 피해규모임
- 이러한 투자 사기는 메시징 플랫폼, 데이팅 앱 등을 통해 시작되며, 피해자들에게 조작된 대시보드와 가짜 수익을 보여주고 더 많은 자금을 투자하게 함으로써 피해 금액을 기하급수적으로 늘림

▶ 사이버 범죄에 대응해 FBI는 암호화폐 사기 방지 이니셔티브를 강화하고 있으나, 실질적 피해 예방은 피해자의 신속한 신고와 협조에 달려 있음을 강조하고 있음

- FBI는 'Operation Level Up'과 같은 이니셔티브를 통해 암호화폐 사기를 방지하고 있으며, 2024년에는 4,300명 이상의 피해자를 식별하고 약 2.86억 달러의 잠재적 손실을 예방함
- 그러나 이러한 성공은 피해자들의 적극적인 신고에 달려 있으며, 또한 사기 피해를 입은 경우, FBI의 IC3 웹사이트를 통해 즉시 신고하는 것이 중요하다는 것을 강조함

- 사이버 범죄는 고령층과 암호화폐 투자자를 주요 표적으로 삼으며 정교화되고 있어, 개인의 경각심과 예방 교육이 그 어느 때보다 중요해지고 있음
- FBI의 대응이 성과를 내고 있지만, 실질적인 피해 예방은 사용자 스스로의 빠른 인식과 신고 참여에 달려 있다는 점에서 사회 전반의 인식 제고가 시급함

[출처]

- Forbes, 'Crypto Scams, Pig Butchering & Cybercrimes From The Latest FBI Report', 2025.04.25.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[프랑스]

파리 블록체인 주간 요약: 활동 가중 합의 알고리즘이 주목을 끌다

- 파리 블록체인 위크 2025는 업계 전문가들을 한자리에 모아 발표, 토론, 고위급 네트워킹을 활발히 진행
- 이 행사에서 새로운 합의 메커니즘인 활동 가중 합의 알고리즘(PoSA)이 공개되며 큰 주목을 받음

글로벌 Web3 기술 기관들인 Solana 재단, XRPL 등이 공식 파트너로 지원하는 파리 블록체인 위크 해커톤에서 300명 이상의 개발자들이 PoSA 모델을 활용한 새로운 탈중앙화 애플리케이션(DApp)을 개발

▶ 파리 블록체인 위크 2025에서는 PoSA 합의 모델을 중심으로 블록체인 생태계 내의 새로운 기준을 제시함

- 2025년 4월 8일부터 10일까지 프랑스 파리의 카루젤 뒤 루브르에서 개최된 파리 블록체인 위크 2025는 전 세계 95개국에서 약 9,600명의 참가자를 모아 Web3 혁신에 대한 심도 있는 논의와 네트워킹을 진행함
- 이 행사에서 Fastex의 웹3 프로그램 리더인 파벨 아라미안(Pavel Aramyan)은 바하무트(Bahamut)의 새로운 합의 메커니즘인 PoSA(Proof-of-Stake-and-Activity)를 소개하여 큰 주목을 받음
- PoSA는 기존의 지분 증명(PoS) 방식에 활동성을 추가하여, 검증자들이 스마트 계약을 배포하고 해당 계약이 사용될 때마다 '활동 점수'를 체크해 각 검증자의 스마트 계약의 빈도를 추적함
- 이 점수는 블록 제안자로 선정될 확률과 보상에 직접적인 영향을 미치며, 이로써 네트워크 참여도를 높이고, 탈중앙화를 강화하며, 블록체인 생태계의 공정성과 효율성을 향상시킴

▶ 한편, Fastex는 전통 금융과의 융합과 명확한 규제 필요성을 강조하며, 제도화를 위한 비전을 제시함

- Fastex의 결제 책임자인 메리 미리안은 포춘 500대 기업의 70%가 암호화폐 트렌드에 대한 관심이 높아지고 있다고 언급하며 전통적인 금융과 암호화폐의 융합을 강조함
- 그녀는 Fastex 카드를 마스터카드가 있는 모든 곳에서 일상적인 거래에 사용할 수 있다고 설명하며 결제 절차를 최대한 단순화하면서도 최대한 안전하게 유지하기 위해 집중하고 있다고 밝힘
- 4월 9일, Fastex의 최고 법률 책임자 바르단 카차트리안은 "디지털 자산이 글로벌 경제에 미치는 영향" 패널에 합류하여 기관이 토큰화된 화폐를 채택하려면 명확한 스테이블코인 규칙의 필수성을 강조함
- 그는 애니모카 캐피탈, 플립스터, 프리덱스, 페이비스의 대표들과 함께 광범위한 디지털 자산 통합을 지원하기 위한 명확한 규제 프레임워크의 중요성을 강조함

- PoSA와 같은 새로운 합의 모델은 블록체인 네트워크 참여와 보상 구조의 혁신을 이끌며, Web3 기술의 발전 방향에 실질적 기준을 제시함
- 전통 금융과 암호화폐의 융합, 그리고 디지털 자산 제도화를 위한 명확한 규제 프레임워크 마련이 Web3 생태계의 실생활 적용과 지속 가능한 성장을 위한 핵심 과제로 부상하고 있음

[출처]

- Cointelegraph, 'Activity-weighted blockchain consensus steals the show: Paris Blockchain Week recap', 2025.04.21.