

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

1. AI 코치 기반 블록체인 보안 운영 모델
2. 기술 매개 젠더 기반 폭력(TFGBV)에 대응하기 위한 법제 동향
3. DNA 저장 기술과 블록체인 기술을 결합한 데이터 영속성 인프라
4. 다언어 환경에서의 Trust - Safety 자동화 도구
5. 뉴질랜드, 중소기업 생산성 강화를 위한 AI 조언 파일럿

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

AI 코치 기반 블록체인 보안 운영 모델

- 블록체인 보안 운영은 자동 탐지 시스템에도 불구하고 최종 판단과 대응이 인간의 인지 능력에 크게 의존함
- AI 코치 네트워크를 통해 인지 붕괴를 완화하고 실수가 시스템적 사고로 확산되는 것을 차단하는 모델이 제시됨

블록체인 보안 운영에서 인간 운영자의 피로와 판단 편향으로 인한 오류를 완화하기 위해, 판단을 대체하지 않고 인지과정을 교정·보완하는 AI 코치 기반 협업 모델이 새로운 운영 대안으로 제시됨

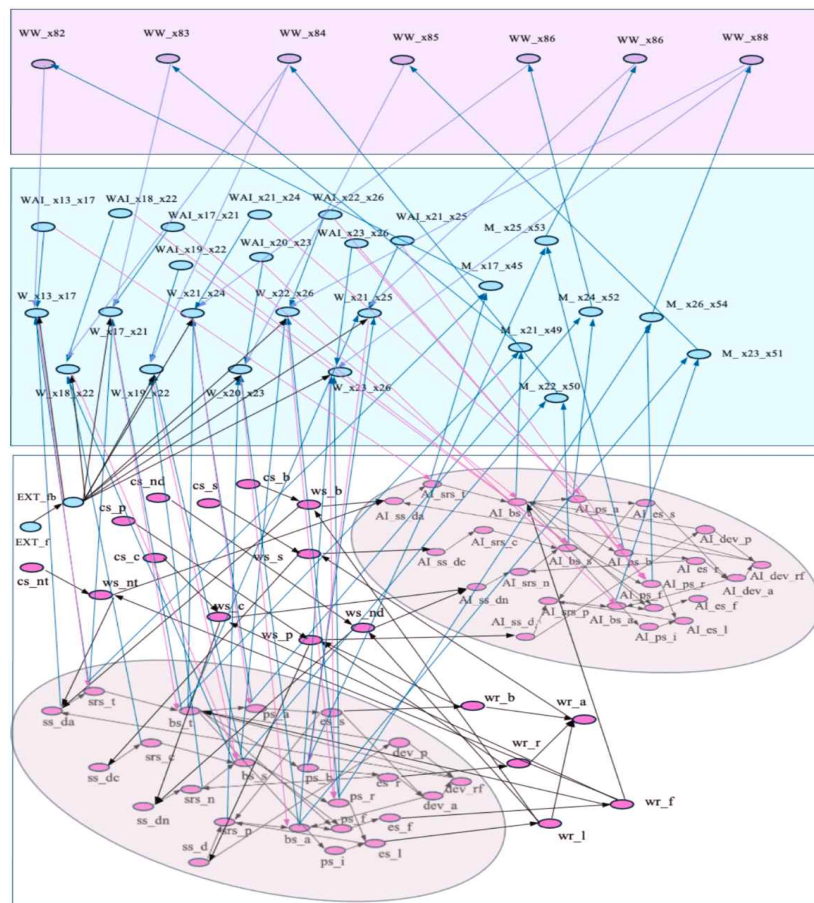
▶ **블록체인은 신뢰 인프라로 활용되고 있음에도 취약점이 존재하며, 이에 대한 인간의 대응에 한계가 존재함**

- 블록체인은 탈중앙성과 무결성을 기반으로 금융·공공·산업 전반에서 신뢰 인프라로 활용되고 있으나, 실제 운영환경에서는 합의 지연, 스마트 컨트랙트 취약점과 같은 다양한 문제가 지속적으로 발생함
- 이러한 사건들은 자동 탐지 시스템에 의해 감지되더라도, 최종적인 판단과 대응은 보안 운영 인력의 인지적 결정에 크게 의존함
- 문제는 이러한 인간 중심의 대응 구조가 피로(fatigue), 경보 과잉(alert fatigue), 장시간 집중 저하와 같은 인지적 한계에 취약하다는 점임
- 또한, 기존 연구에서도 보안 감시 업무에서 시간이 경과할수록 위협 인지 정확도와 대응 속도가 급격히 저하된다는 사실이 반복적으로 보고되어 옴
- 네덜란드 Vrije 대학 연구진은 이러한 문제의식에서 출발하여, 인간의 판단을 대체하는 AI가 아니라 인간의 '정신 모델'을 보완·교정하는 AI 코치라는 개념을 제시함

▶ **네덜란드 대학의 연구진은 인간 운영자의 인지적 한계점을 극복하기 위해 AI 코치 네트워크를 설계함**

- 연구진은 인간 운영자의 인지 과정을 하나의 동적 네트워크로 모델링하고, 이를 병렬적으로 모사하는 AI 코치 네트워크를 설계함
- 이 모델은 인지 과정을 맥락 인식, 감지, 위험 표현, 신념 형성, 준비, 실행 피드백이라는 단계로 분해하고, 시간에 따라 가중치가 변화하는 적응형 구조로 설계됨
- AI 코치는 운영자와 동일한 구조의 '내부 예측 모델'을 유지하며, 실제 운영자의 판단과 자신의 예측 간 차이를 지속적으로 감시하여 차이가 발생하면 AI가 직접 명령을 내리는 대신, 지식 수전에서 연결 가중치를 조정하여 운영자의 판단 기준이 다시 안정적인 상태로 수렴하도록 유도함
- 이는 인간의 학습·망각·재학습 과정을 계산적으로 구현한 것으로, 특히 피로가 누적되는 상황에서 지식 붕괴를 막는 역할을 함
- 이 구조는 단순 자동화나 알림 추천을 넘어 메타 수준에서 인간의 의사결정 품질을 유지하는 AI 코칭 매커니즘이라는 점에서 차별성을 가짐

[AI 코치 모델의 다중 네트워크 아키텍처]



출처 : Science Direct, 'Optimising blockchain security: Computational analysis of adaptive AI coaching',
2026.01.16.

▶ AI 코치의 아키텍처는 3개의 계층으로 구성되어 인간의 인지 흐름을 재현하도록 설계됨

- AI 코치의 다중 네트워크 아키텍처는 운영자의 인간의 인지 흐름을 그대로 재현하도록 설계되었으며, 그에 대한 AI 코치의 지원이 어떻게 연결되어 작동하는지를 보여줌
- 네트워크는 ▲기저 계층(base-level), ▲중간 상위 계층(intermediate higher-level), ▲최상위 계층(upper higher-level)의 세 개의 계층으로 구성됨
- 우선, 기저 계층에는 운영자의 정신 모델 상태, AI 코치의 정신 모델 상태, 그리고 외부 환경 상태가 포함되어 실제 사건의 인지, 판단 형성, 행동 실행이 이루어짐
- 다음으로, 중간 상위 계층에는 정신 모델의 지식을 표현하는 가중치 상태(W-states, WAI-states)와 함께, AI 코치가 인간과 AI의 의사결정을 비교 및 감시하는 모니터링 상태(M-states)가 위치함
- 마지막으로, 최상위 계층에는 2차 적응 상태인 WW-states가 존재하며, 이는 의사결정 누락이나 오류가 감지되었을 때 언제, 어떤 방식으로 인간과 AI의 커뮤니케이션을 수행할지 제어함
- 이러한 교정을 위한 커뮤니케이션은 사회적 학습이나 지시의 형태로 이루어지며, 인간의 판단을 직접 대체하기보다는 학습을 유도하는 방식으로 작동함

▶ **AI 코치 모델에 대한 성능 평가 결과, 인간의 실수를 완전히 제거하지는 않지만 실수가 시스템적 사고로 확산되는 것을 효과적으로 차단하는 역할을 수행할 수 있을 정도의 성능을 보이는 것을 확인함**

- 연구진들은 제안한 모델을 다양한 시뮬레이션 시나리오에 적용하여 AI 코치의 효과를 검증하며 스마트 컨트랙트 이상, 노드 장애 등 블록체인 보안에서 핵심적인 사건들이 반복적으로 발생하는 환경을 가정하고 AI 코치가 있는 경우와 없는 경우를 비교 분석함
- 그 결과, AI 코치가 활성화된 경우에는 피로 구간에서도 위험 긴급도, 시스템 신뢰도, 책임 인식과 같은 핵심 신념 상태가 높은 수준으로 유지됨
- 반면 AI 코치가 없는 경우에는 피로가 누적되면서 위험 인식이 급격히 붕괴되고, 경고 발송이나 접근 차단과 같은 필수 대응이 실행되지 않는 현상이 관찰됨
- 특히 What-If 분석과 확률 기반 위험 평가 결과, AI 코치가 없는 경우 전체 위험 점수가 코치가 있는 경우 대비하여 약 94% 높게 나타남
- 이는 단순히 반응 속도의 차이가 아니라, 위험을 과소평가하는 인간 전문가의 실패 가능성 자체가 크게 증가함을 의미함
- 즉, AI 코치는 인간의 실수를 완전히 제거하지는 않지만, 실수가 시스템적 사고로 확산되는 것을 효과적으로 차단하는 역할을 수행함

▶ **결과적으로, AI 코치는 인간의 블록체인 운영의 신뢰성과 지속 가능성을 높이는 핵심 요소로 자리잡음**

- 연구진들은 블록체인 보안에서 AI의 역할을 '자동 탐지 도구'에서 '인지적 동반자'로 확장한다는 점에서 중요한 시사점을 제공함
- 즉 제안된 AI코치는 인간을 대체하지 않고, 인간의 판단 책임을 유지한 채 그 판단이 왜곡되거나 붕괴되는 지점을 보정해주며 인간·AI 협업이 나아갈 수 있는 현실적인 방향을 제시함
- 향후 실제 SOC 환경에서의 실증 검증, 사용자 수용성 분석, 대규모 시스템 성능 평가가 필요하며, 이미 계산적 모델링과 위험 분석을 통해 강력한 개념적·정량적 근거를 제시함
- 결론적으로, 적응형 AI 코칭은 블록체인 보안 운영의 신뢰성과 지속 가능성을 높이는 핵심 요소로 자리잡을 가능성이 크며, 이는 사이버 보안 전반으로도 확장될 수 있는 중요한 연구 성과로 보여짐

- 블록체인 보안은 완전 자동화보다 인간 판단을 전제로 한 인지 보완형 AI 협업 모델이 운영 안정성과 신뢰성을 동시에 높일 수 있음을 시사하며, 복잡한 보안 환경에서 인간-AI 역할 분담의 중요성이 부각됨
- 향후 보안 정책과 시스템 설계에서는 기술 성능 중심 접근을 넘어, 운영자의 피로·학습·판단 지속성을 함께 고려한 인간 중심 보안 아키텍처가 핵심 경쟁 요소로 작용할 가능성이 큼

[출처]

- Science Direct, 'Optimising blockchain security: Computational analysis of adaptive AI coaching', 2026.01.16.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체�평가팀

[EU]

기술 매개 젠더 기반 폭력(TFGBV)에 대응하기 위한 법제 동향

- TFGBV는 온라인 성희롱·비동의 이미지 공유 등 다양한 형태로 확산되며 국제적 인권 문제로 부상함
- 여성차별철폐협약과 이스탄불 협약을 중심으로 한 국제 규범은 TFGBV 대응을 국가의 책무로 명시함

TFGBV가 오프라인 젠더 기반 폭력의 연장선이자 중대한 인권 문제로 인식되며, 국제 협약과 EU 법제를 중심으로 디지털 환경을 포괄하는 규제·보호 체계가 점진적으로 확장되고 있음

▶ 전 세계 입법자들에게 있어 기술 매개 젠더 기반 폭력에 대응하기 위한 법률 마련은 매우 중요한 문제임

- 전 세계 입법자들은 기술 매개 젠더 기반 폭력(Tech-Facilitated Gender-Based Violence, TFGBV)에 대응하기 위해 권리를 보장하는 방법을 어떻게 확립할 것인지에 대해 고심해 옴
 - TFGBV가 근본적인 인권 문제라는 인식이 확산되고, 유럽인권재판소가 Buturuga v. Romania 사건과 같은 판례를 통해 TFGBV를 명시적으로 인정하게 되며 기존 법률과 새로운 법률 다수가 관련성을 가짐
 - 또한 국제 및 EU 차원에서는 TFGBV 해결과 관련된 여러 규정 실사(due diligence) 의무나 법적 해석이 존재하며, 프레임워크끼리 서로 영향을 주고받거나 상호 의존적인 접근 방식을 취하고 있음
 - 이러한 프레임워크 전반에 걸쳐서 TFGBV가 오프라인에서 발생하는 젠더 기반 폭력의 연장선이며, 다양한 형태로 나타날 수 있다는 인식이 존재함
 - 이러한 인식에 따라 TFGBV에는 언어적 학대, 폭력 위협, 실제로 발생하였거나, 실제로 발생하지 않은 사건을 합성한 이미지·영상 공유, 스토킹, 데이터 절도, 독싱(doxing)*, 젠더화된 허위정보 등이 포함됨
- * 독싱(doxing): 동의 없이 개인의 정보를 온라인에 게시하거나 공유하는 행위

▶ 여성차별철폐협약은 TFGBV에 대응하기 위한 프레임워크가 목적인 미국의 여러 조치의 기반이 됨

- 젠더 기반 폭력(GBV)을 다루는 가장 광범위한 인권 규범인 여성차별철폐협약(CEDAW)은 TFGBV에 대응하기 위한 규범적 프레임워크 강화를 목적으로 한 미국의 여러 조치의 기반이 됨
- 특히 CEDAW의 일반권고 제35호는 '온라인 폭력'을 인정하고, 협약이 온라인 및 기타 디지털 환경을 포함한 모든 인간 상호작용의 영역에서 GBV를 근절할 것을 국가에 요구하고 있음
- 이러한 국제 차원의 연성법(soft law)에 대한 노력은 다른 국제기구 내에서 이루어진 실질적인 발전에 의해 뒷받침되어 옴

▶ 이스탄불 협약은 모든 형태의 젠더 기반 폭력에 대해 4P(예방·보호·기소·정책) 접근을 요구하며, GREVIO는 온라인 성희롱·사이버 스토킹 등 TFGBV를 이스탄불 협약의 범위로 해석하여 감독 및 평가함

- 여성 및 가정폭력 예방·근절에 관한 협약, 즉 이스탄불 협약은 젠더 기반 폭력에 가장 포괄적인 인권 조약으로, 체약국은 이 협약에 따라 모든 형태의 GBV에 대응하고 '4P' 접근법'을 채택해야 함

- 즉, 젠더 기반 폭력의 예방(Prevent), 피해자 보호(Protect), 가해자 기소(Prosecute), 그리고 조정된 노력을 강화하기 위한 종합 정책 채택(Policies)에 대한 접근법을 준수해야 함
- 협약 이행을 감독하는 기구는 여성 및 가정폭력 대응 전문가 그룹(GREVIO)으로, 젠더 기반 폭력의 디지털 차원에 초점을 맞추었으며, 특정 형태의 TFGBV가 이스탄불 협약의 범위에 포함된다고 결론지음
- 여기에는 동의하지 않은 이미지 공유를 포함한 온라인 성희롱, 스토킹, 그리고 강압이나 위협을 통해 개인의 심리적 불안감을 증가시키는 행위와 같은 디지털 차원의 심리적 폭력이 포함됨
- 이는 부다페스트 협약 제2조(불법 접근)의 체약국이 컴퓨터 시스템 전체는 일부에 대해 정당한 권한 없이 고의적으로 접근하는 행위를 범죄로 규정해야 한다고 명시된 것과 연관이 있음
- 즉, 보안 조치가 침해되고 데이터 취득 또는 기타 부정한 의도를 가진 경우 범죄가 성립될 수 있으므로 TFGBV 맥락에서의 사이버 스토킹 역시 해당 조항에 따라 이해될 수 있음
- 각국이 권고에 따라 어떠한 법적 변화를 채택했는지는 현재 활발히 변화하는 과정에 있으며, GREVIO에 의해 주기적으로 평가될 예정임
- 그러나, 이스탄불 협약은 국제적으로 구속력 있는 조약으로서 점점 더 큰 압박을 받고 있으며, 네 개의 EU 회원국(불가리아, 슬로바키아, 헝가리, 리투아니아)은 협약 비준을 거부하고, 2025년 10월에는 라트비아 정부가 협약 탈퇴 의사를 밝히기도 하였음

▶ **기존 사이버범죄 입법의 활용이 2027년 EU 전역에서 발효될 EU 지침 채택 과정에서 중요한 요소로 인식됨**

- 기존 사이버범죄 입법의 활용은 2027년 EU 전역에서 발효될 여성에 대한 폭력 및 가정폭력 관련 EU 지침(Directive) 채택 과정에서도 중요한 요소로 인식됨
- EU 입법자들은 범죄에 대한 정의 및 제재에 관한 최소 기준을 설정을 허용하는 EU 기능조약(TFEU) 제83조 1항을 법적 근거로 삼음
- EU 지침의 채택은 GBV에 대응하기 위한 EU 차원의 법적 프레임워크를 구축하는 데 있어 환영할 만한 진전이었으며, 2023년 EU가 이스탄불 협약에 가입함으로써 실질적으로 가능해짐
- CDT Europe은 해당 EU 지침의 이점과 TFGBV의 특정 형태에 대해 설정된 최소 형사 기준이 지니는 잠재적 법적 문제점을 광범위하게 분석함
- 분석 결과에 대해 요약하자면, 이 지침은 사이버 스토킹 및 동의하지 않은 이미지 공유와 관련하여 이스탄불 협약의 기준과 부합하나, 지침 조항은 회원국별로 이행되므로 단편화 될 가능성이 존재함
- 또한 사이버 괴롭힘 및 증오 선동과 관련된 조항은 표현의 자유를 보호하기 위한 국제 기준, 예컨대 시민적 및 정치적 권리에 관한 국제규약(ICCPR)과 라바트 행동계획(Rabat Plan of Action)에 부합하도록 추가적인 안전장치가 보완된 필요가 있음

▶ **디지털서비스법은 TFGBV와 관련된 주요 지침을 직접적으로 보완하나, 실제 실사 노력은 정체되고 있음**

- 모든 중개 서비스(온라인 플랫폼 포함)에 적용되는 규칙을 설정하는 수평적 규제인 디지털

서비스법(DSA)은 TFGBV와 관련된 주요 지침을 직접적으로 보완함

- 기존 EU 및 회원국 법률에 의한 불법 콘텐츠 대응 의무 외에도, 초대형 온라인 플랫폼(VLOPs) 및 초대형 온라인 검색엔진(VLOSEs)으로부터 초래되는 TFGBV 형태를 평가하는 DSA의 실사가 매우 중요해짐
- 이에 따라, 위험 완화 조치와 함께 TFGBV에 관한 자율적 행동강령도 가까운 시일 내에 마련될 예정임
- 그러나, 현재까지 관련 온라인 플랫폼들이 수행한 1차 위험 평가 결과를 보면, 신고 및 콘텐츠 조정 정책과 같은 일부 완화 조치는 도입된 것으로 나타남
- 그럼에도 불구하고, 1차 위험 평가 보고서와 이후 음란 콘텐츠를 호스팅하는 VLOP의 위험 평가 보고서에 대한 GBV의 평가 방식에는 상당한 불일치가 존재하며, 이는 DSA의 실사 노력이 정체되고 있음을 보여줌

▶ **관련 프레임워크를 통합시키는 것이 중요하며 이를 위해 인력 확보 등 다양한 조치를 채택할 수 있음**

- 결국 관련 프레임워크의 범위가 넓은 만큼, 특히 EU 내에서 감독 책임이 상호 교류가 거의 없는 다양한 규제 기관에 분산되어 있다는 점을 고려할 때, 이러한 규칙들의 집행을 어떻게 통합시킬 것인지가 중요함
- 통합적인 접근 방식은 회원국 간 상충되는 해석을 방지하는 데에도 도움이 될 것이며, EU 전역에서 모든 사람에게 법 아래 동등한 보호를 제공하고 의도치 않은 피해자들이 생기지 않도록 할 수 있음
- 이를 위해서는 관련 규제 기관들이 시민사회 단체와의 소통 채널, 정보 공유, 협의 체계를 수립할 필요가 있으며 포괄적인 접근이 모든 집행 조치의 중심이 되도록 하기 위해 다음과 같은 조치를 채택할 수 있음
- **(조치 #1 인력 확보)** 집행을 담당하는 EU 및 국가 규제 기관 내에서 젠더 전문성을 갖춘 인력을 강화하고 각 기관의 집행팀과 협력할 수 있도록 충분한 인력을 확보해야 함
- **(조치 #2 DG 협력)** 지침 제43조에 규정된 연합 차원의 협력이, 각각 DSA 집행과 향후 TFGBV 행동강령 수립을 담당하는 DG Connect 및 DG Justice와의 협력을 명시적으로 포함하도록 보장해야 함
- **(조치 #3 데이터 제공)** 기업들이 DSA 제40조에 따른 의무를 이행하여 보안과 개인정보 보호를 유지하는 방식으로 플랫폼 관련 데이터를 연구자들에게 더 많이 제공하도록 협조해야 함
- **(조치 #4 시민사회 단체와의 협의)** 시민사회 단체, 특히 성평등 및 LGBTQI+ 단체와 규제 기관 간에 협의를 통해 위험 평가 및 완화 조치가 적절하며 기본권을 의도치 않게 침해하지 않도록 해야 함

- 디지털 환경에서의 젠더 기반 폭력은 개별 플랫폼의 자율 규제를 넘어, 국가 및 초국가적 인권 보호 체계 차원에서의 개입 필요성이 점차 강화되고 있음
- 국제 협약과 EU 법제의 적용 범위 확대는 온라인 폭력 대응이 단순한 콘텐츠 관리 문제가 아닌, 기본권 보호와 직결된 공공 정책 영역으로 자리 잡고 있음을 시사함

[출처]

- CDT, 'Building an Harmonised Legal Framework to Address Tech-Facilitated Gender-Based Violence', 2026.01.14.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

DNA 저장 기술과 블록체인 기술을 결합한 데이터 영속성 인프라

- DNA 저장 기술은 대용량 데이터를 수천 년 단위로 보존할 수 있는 물리적 매체로 현실화 됨
- 블록체인의 무결성과 DNA 저장의 초장기 안정성을 결합하여 문명 단위의 데이터 영속성과 신뢰성을 확보할 수 있음

DNA 저장 기술과 블록체인의 결합은 대규모 데이터를 에너지 소비 없이 수천 년 단위로 보존·검증할 수 있는 구조를 가능하게 하며, 초장기 데이터 신뢰 인프라로서의 잠재력을 부각시킴

▶ **DNA 저장 기술에 혁신이 일어나며 카세트당 최대 60페타바이트의 데이터를 안정적으로 저장할 수 있게됨**

- 2025년 DNA 저장 기술이 현실화되며 기업들이 저장 인프라를 재고하게 될 수준의 혁신이 일어남
- 특히, Atlas Eon 100이라는 세계 최초의 엔터프라이즈 규모 DNA 아카이브 서비스가 상용화되며, 이를 통해 1개의 카세트당 36~60페타바이트에 달하는 대용량 데이터에 대해 밀레니엄급 안정성을 보장함
- 또한 이러한 압도적인 안정성을 통해 데이터를 영구 보관하면서 추가 에너지 소비가 전혀 없는 콜드 저장(cold storage)이 가능해지며, 블록체인의 영구성과 결합해 단순한 저장 매체의 변화가 아닌 수천 년 단위의 데이터 영속성을 확보할 수 있는 물리적 기반을 제공한다는 점에서 큰 의미를 가짐
- 이때, 블록체인 기술 자체는 변조 불가능하고 검열 저항성을 제공하는 장점이 있지만, 무한히 증가하는 저장 요구량이라는 현실적인 한계를 마주하고 있음
- 이러한 저장 증가 속도는 시간이 지날수록 블록체인 운영 비용과 저장 부담을 가중시키며, 전통적인 저장 매체나 분산 복제 모델만으로는 영구 보존을 보장하기 어려움
- 그러나 DNA 저장은 한 번 데이터를 쓰면 추가 에너지 없이 수천 년 동안 데이터를 유지할 수 있기 때문에 이러한 딜레마를 근본적으로 뒤집을 수 있는 잠재력을 지님
- 특히 DNA 저장과 블록체인의 결합은 체인 스냅샷을 주기적으로 DNA 매체에 기록하는 형태로 구현하여 핵심 메타데이터를 DNA에 삽입함으로써 미래의 검증 가능성을 유지함
- 결론적으로 DNA 저장과 블록체인의 결합은 단순한 기술 연계가 아닌 문명적 규모의 데이터 인프라 혁신을 의미하며, 기업은 영구적인 디지털 원장(블록체인)과 물리적 저장(DNA)을 결합해 경쟁자들이 모방할 수 없는 가장 오래 검증 가능한 데이터를 갖출 수 있을 것으로 전망됨

- DNA 저장과 블록체인의 결합은 기존 디지털 저장 방식의 한계를 넘어서는 초장기 데이터 보존·검증 인프라로 발전할 잠재력을 보이며, 공공·산업 분야에서 새로운 활용 가능성을 제시함
- 다만 기술의 현실적 확산을 위해서는 저장·검증 표준 수립과 함께, 어떤 데이터를 어떤 목적으로 영구 보존할 것인지에 대한 제도적 합의가 병행될 필요가 있음

[출처]

- CoinGeek, 'DNA storage meets blockchain permanence in the enterprise era', 2026.01.15.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[글로벌]

다언어 환경에서의 Trust – Safety 자동화 도구

- 자동화된 Trust & Safety 도구는 영어 데이터에 과도하게 의존하고 있어, 일부 언어 환경의 맥락을 반영하지 못함
- 데이터 대표성 확보와 지역 커뮤니티와의 협력 없이는 공정한 콘텐츠 조정이 어려우며 제3자를 통한 대응이 필요함

영어 중심 데이터에 기반한 자동화된 Trust & Safety 도구는 저자원 언어와 지역적 맥락을 충분히 반영하지 못하고 있어, 데이터 대표성 확보와 외부 전문가 협력이 핵심 과제로 부상함

▶ 디지털 플랫폼이 전 세계 사용자들의 일상적 소통 공간으로 자리잡으며 신뢰·안전 도구가 중요해짐

- 디지털 플랫폼이 전 세계 사용자들의 일상적 소통 공간으로 자리잡으며 신뢰·안전(Trust & Safety, T&S) 도구의 역할이 매우 중요해짐
- 그러나 자동화된 콘텐츠 검출과 조정 시스템은 여전히 영어 중심으로 설계되어 있으며, 영어 이외의 언어 환경에서는 심각한 성능 저하를 보이는 경우가 많음
- CDT(Center for Democracy & Technology)가 2024년부터 2025년까지 AI 전문가와 데이터 어노테이터들을 대상으로 진행한 다수의 라운드테이블 연구는 이러한 구조적 한계를 명확히 보여줌
- 특히 저자원(low-resource)이지만 실제 사용자는 매우 많은 언어 환경에서 자동화된 T&S 도구가 공정하고 효과적으로 작동하지 못하고 있다는 점이 핵심 문제로 지적됨
- 이러한 문제의 근본에는 데이터의 부족뿐 아니라 데이터의 '대표성 결여'가 자리하고 있어 영어가 아닌 언어로 구축된 데이터셋은 실제 온라인 이용자들이 사용하는 언어를 충분히 반영하지 못함
- 또한 여성, 성소수자, 인종적 소수자와 같이 온라인에서 상대적으로 덜 드러나는 화자들의 표현 방식과 관점이 데이터에서 배제되면서 자동화된 도구가 이들의 발화를 오해하거나 인식하지 못함
- 이러한 문제를 해결하기 위해서는 제3자가 개발한 도구와 데이터셋을 검증·활용할 수 있는 체계적인 경로 마련이 필요성이 강조됨
- 이를 위해 독립적인 연구 기관, 오픈소스 커뮤니티, 글로벌 연구 네트워크와의 연결이 중요하며, 이를 임시로 처리하는 현재 방식에서 벗어나 구조화된 검증 프로세스를 갖출 필요가 있음

- 글로벌 플랫폼의 안전 정책은 영어 중심 자동화를 넘어, 언어·문화·지역별 위험 양상을 반영하는 정밀한 대응 체계로의 전환이 요구되고 있음
- 데이터 대표성 확보와 외부 전문가·지역 커뮤니티와의 협력은 기술적 개선을 넘어, 플랫폼 책임성과 거버넌스 신뢰를 좌우하는 핵심 요소로 인식될 필요가 있음

[출처]

- CDT, 'Better Global Tools, Better Global Communities: Recommendations for Trust & Safety Teams When Building and Procuring Multilingual Tools', 2026.01.12.

블록체인 기술·정책·산업 동향

디지털안전지원본부 신기술안전단 블록체인정책팀

[뉴질랜드]

뉴질랜드, 중소기업 생산성 강화를 위한 AI 조언 파일럿

- 뉴질랜드 정부는 중소기업의 반복 업무 부담을 해소하기 위해 전문가 지원 중심의 AI 조언 파일럿 프로그램을 도입함
- 해당 파일럿은 자금 지원과 컨설팅을 결합해 AI를 실질적인 경영 도구로 정착시키는 것을 목표로 함

뉴질랜드는 전문가 컨설팅과 공동 자금 지원을 결합한 AI 조언 파일럿을 통해, 중소 기업의 AI 도입 장벽을 낮추고 실질적인 생산성 향상을 도모하고 있음

▶ 뉴질랜드 정부는 인공지능 활용을 통해 중소기업의 생산성을 높이기 위한 시책을 발표함

- 뉴질랜드 정부는 기술 진화 속도에 발맞춰 인공지능(AI) 활용을 통해 중소기업의 생산성을 높이기 위한 새로운 시책을 발표함
- 이러한 시책의 배경에는 디지털 기술이 기업 활동 전반에 걸쳐 확산되며 많은 중소기업이 반복적인 업무나 정보 정리, 고객 응대 등의 작업에 상당한 인력과 시간이 소요된다는 문제점이 있음
- 이러한 문제점을 해결하기 위해 뉴질랜드 정부는 AI 조언 파일럿(AI Advisory Pilot) 프로그램을 도입하여 경험이 풍부한 전문가들의 실질적인 지원을 제공함으로써 고객 요구에 맞춘 전략을 수립하도록 도움
- 뉴질랜드 정부는 이러한 AI 도구가 단순한 자동화 이상의 생산성 향상 효과를 낼 수 있다고 보고 생성형 AI의 채택만으로 2038년까지 최대 NZ\$760억(약 15%의 GDP 기여)의 경제적 효과가 가능하다고 전망함
- 이를 위해 정부는 향후 7년간 NZ\$7,000만 이상을 연구·응용 분야에 투자하고, 세계 수준의 전문성을 개발해 국가 경쟁력을 강화할 계획임
- 참여 자격을 갖춘 기업에게는 최대 NZ\$15,000 까지 50% 공동 자금 지원이 제공되며, 정부의 기존 지원 네트워크인 Regional Business Partner Network를 통해 최소 6개월간 진행될 예정임
- 이 파일럿의 도입은 단순한 자금 지원 프로그램을 넘어, 중소기업이 AI 도구를 일상 운영에 적극적으로 통합하도록 유도하는 실질적 계기가 될 전망이다
- 정부는 이번 파일럿을 통해 얻은 성과를 바탕으로, 향후 AI 수용 추진 전략을 보다 확장하고 정교화함으로써 뉴질랜드 전반의 생산성 증대·혁신 촉진·경제 성장 가속화라는 목표를 달성하려 함

- 뉴질랜드 사례는 AI 확산 정책에서 기술 도입 장벽을 낮추기 위해, 전문가 컨설팅과 현장 밀착형 지원 모델이 효과적일 수 있음을 보여줌
- 중소기업 대상 AI 정책은 단기적 도입 성과보다, 지속 가능한 활용 역량 축적과 생산성 구조 개선을 목표로 설계될 필요성이 커질 것으로 전망됨

[출처]

- OpenGov, 'New AI Pilot to Boost Small Businesses Productivity', 2026.01.14.