

□ 디지털트윈

● ‘디지털트윈 코리아 전략’ 수립 (디플정위, '24.7)

□ 디지털 심화시대를 선도할 디지털 트윈 코리아 구현

- 디지털 심화시대를 선도할 디지털트윈 코리아 구현을 비전으로 제시
- 대외 기술 격차를 신속하게 해소하기 위해 디지털트윈의 핵심 요소기술 및 고단계 기술을 선제적으로 개발하고 쏠 산업군으로 확산

□ 블록체인

○ ‘블록체인 산업 진흥 전략’ 수립(관계부처 합동, '22.11)

□ 웹3 시대 선도를 위한 블록체인 핵심 인프라 구축

- 웹3 시대 블록체인 디지털 신뢰 생태계 조성을 위한 산업 생태계 기반 강화, 시장 활성화, 기술경쟁력 확보 등 추진
 - 국민 체감형 대형 프로젝트 발굴과 법·제도 정비, 공공서비스 개발을 위한 표준·개발 도구 마련, 산업고도화를 위한 핵심 기술개발과 검증 지원

○ 디지털 권리장전 수립(과기정통부 등 관계부처 합동, '23.9)

□ (공정한 접근과 기회의 균등)

- 데이터, 디지털 저작물 등의 디지털 자산이 정당한 법적 정책적 보호를 받는 ‘디지털 자산의 보호’, 디지털 격차 해소를 위한 ‘디지털 리터러시 향상’

□ (안전하고 신뢰할 수 있는 디지털 사회)

- 디지털 공동번영사회의 전제가 되는 안전과 신뢰 확보를 위해 디지털 위험이 체계적 시스템을 통해 관리

□ (디지털 권리장전)

- 디지털 환경에서의 권리 보장, 공정한 접근과 기회의 균등, 안전과 신뢰를 확보할 수 있는 디지털 혁신 등

○ 2025년도 국가연구개발 투자 방향 및 기준(안)(과기정통부, '24.3)

□ (사이버보안) 인공지능·클라우드 등 활용·확산에 따른 보안 분야 핵심기술 경쟁력

- 확보 및 주요 현안 공동 대응을 위해 국내외 R&D주체 간협력 강화
 - 인공지능 기반 보안기술 개발, 네트워크·클라우드 등 ICT 핵심인프라플랫폼 데이터 보호 강화

○ 제1차 국가전략기술 육성 기본계획(‘24.8)

□ 제1차 국가전략기술 육성기본계획(24-28) 12대 분야별 세부 정책 방향

- 사이버보안 정책투자방향 丙 산업·가상융합 보안(블록체인 기반 분산자율형 고신뢰 환경 기술개발)

○ ‘블록체인 산업 경쟁력 강화 방안(안)’ 마련 중(‘25.하)

□ (주요내용) AI·블록체인 융합 기반 자율형 고신뢰 환경 핵심기술 개발 추진

- AI·블록체인 기술 융합을 통해 공정성과 신뢰성을 제고할 수 있으며, 블록체인 기술 확장을 통해 대규모 데이터 환경에서도 빠르고 안전하게 AI의 신뢰성을 확보

- (디지털트윈) 산업 전반의 디지털 전환을 가속화하고, 미래 기술 기반 성장 동력을 확보하는 AI 기반 자율형 디지털 트윈 핵심기술 개발
 - 디지털 트윈 구축 단계를 자동화하고, AI를 통해 실 현장의 운영 및 현장 간 연계·협업이 가능한 자율 디지털 트윈 핵심기술 확보

- (블록체인) AI 데이터/모델 공유 및 거래를 위한 고신뢰 서비스 구현하고 AI·블록체인 융합 기술 기반 자율형 고신뢰 인프라 구축을 위한 핵심 기술 개발
 - AI 학습과 활용 과정에서 프라이버시를 보호하고 신뢰성을 확보하며, 사용자 중심의 데이터 및 모델 주권 보장 기술 개발
 - AI의 신뢰성 향상을 위해 블록체인 기술로 AI 데이터와 모델의 안전한 공유/협업을 지원, 탈중앙화된 환경에서 검증 가능한 분산 AI 시스템 구축
 - 블록체인 확장성 강화를 위해 AI를 활용, 트랜잭션 품질을 최적화하고, 스마트계약 오류 자동 검증 및 신뢰할 수 있는 AI 기반 오라클 구현

참고3

디지털융합 분야 중장기 R&D 방향

미션	고신뢰·초지능·초실감 핵심 기술의 확보를 통한 AI연계 디지털 융복합 추진																										
비전	인간 개입 없는 고신뢰·자율 지능화로 AI-디지털 융합 기술 선도국 도약																										
미래상	<div>As is (현재)</div> <div>인간의 개입·판단에 의존 현실 세계 중심·제한적 가상현실 활용 빅테크 주도 플랫폼으로 데이터 침해 위험 상존 고성능화 경쟁으로 인한 탄소 다배출</div> <div>⇒</div> <div>To Be (미래)</div> <div>AI·클라우드·빅데이터 기반의 자율 지능화 융합현실(현실과 가상의 완벽한 융합) 고신뢰 플랫폼 시대(경제, 인터넷, 거래 등) 저전력·고효율 기반의 그린 디지털 시대</div>																										
중장기 R&D 추진방향	<table><tr><th>구분</th><th>R&D 중장기 목표</th><th>R&D 추진방향</th></tr><tr><td>블록체인</td><td>웹3 환경 인프라, AI 융합 개발을 통해 블록체인 플랫폼의 보안성 및 고신뢰성 확보, 자동화 실현</td><td>웹3 기반신뢰 기술 확보 및 AI, IoT, 메타버스 등 他 분야 융합 기술 개발</td></tr><tr><td>디지털 트윈</td><td>5대 핵심기술 5단계의 자동화 및 자율연합·자율서비스 제공</td><td>초정밀·지능형 현실 동기화 기반 자율 문제해결 지원 기술개발</td></tr><tr><td>메타버스</td><td>현실세계에 이질감없이 융합되는 가상(디지털)화 기술로 편의성이 극대화되는 메타버스 실현</td><td>실세계에 융합된 가상(디지털)의 이질감을 해소하는 상호작용-혼합공간-디지털감각 기술개발</td></tr><tr><td>ESG/탄소중립</td><td>지속가능한 기술 및 서비스 발전을 위한 세계적 수준의 디지털 탄소중립 기술 확보</td><td>저전력·고효율 ICT 인프라 핵심기술 및 탄소중립 기반/응용 기술 확보</td></tr><tr><td>산업융합</td><td>인간 개입이 최소화되는 자율 지능화 실현</td><td>소산업 적용 가능한 AI 융합 기술 개발</td></tr></table>	구분	R&D 중장기 목표	R&D 추진방향	블록체인	웹3 환경 인프라, AI 융합 개발을 통해 블록체인 플랫폼의 보안성 및 고신뢰성 확보, 자동화 실현	웹3 기반신뢰 기술 확보 및 AI, IoT, 메타버스 등 他 분야 융합 기술 개발	디지털 트윈	5대 핵심기술 5단계의 자동화 및 자율연합·자율서비스 제공	초정밀·지능형 현실 동기화 기반 자율 문제해결 지원 기술개발	메타버스	현실세계에 이질감없이 융합되는 가상(디지털)화 기술로 편의성이 극대화되는 메타버스 실현	실세계에 융합된 가상(디지털)의 이질감을 해소하는 상호작용-혼합공간-디지털감각 기술개발	ESG/탄소중립	지속가능한 기술 및 서비스 발전을 위한 세계적 수준의 디지털 탄소중립 기술 확보	저전력·고효율 ICT 인프라 핵심기술 및 탄소중립 기반/응용 기술 확보	산업융합	인간 개입이 최소화되는 자율 지능화 실현	소산업 적용 가능한 AI 융합 기술 개발								
구분	R&D 중장기 목표	R&D 추진방향																									
블록체인	웹3 환경 인프라, AI 융합 개발을 통해 블록체인 플랫폼의 보안성 및 고신뢰성 확보, 자동화 실현	웹3 기반신뢰 기술 확보 및 AI, IoT, 메타버스 등 他 분야 융합 기술 개발																									
디지털 트윈	5대 핵심기술 5단계의 자동화 및 자율연합·자율서비스 제공	초정밀·지능형 현실 동기화 기반 자율 문제해결 지원 기술개발																									
메타버스	현실세계에 이질감없이 융합되는 가상(디지털)화 기술로 편의성이 극대화되는 메타버스 실현	실세계에 융합된 가상(디지털)의 이질감을 해소하는 상호작용-혼합공간-디지털감각 기술개발																									
ESG/탄소중립	지속가능한 기술 및 서비스 발전을 위한 세계적 수준의 디지털 탄소중립 기술 확보	저전력·고효율 ICT 인프라 핵심기술 및 탄소중립 기반/응용 기술 확보																									
산업융합	인간 개입이 최소화되는 자율 지능화 실현	소산업 적용 가능한 AI 융합 기술 개발																									
기술확보 목표	<table><tr><td rowspan="8">기술확보 목표</td><td>블록체인</td><td>고신뢰 웹3 기반 기술</td><td>고신뢰 웹3 구현을 위한 다계층·이종 네트워크 연결 기술 및 AI기반 계약·합의 기술 개발</td></tr><tr><td rowspan="2">디지털 트윈</td><td>초정밀·초지능</td><td>현실 특성을 정밀하게 반영하는 시뮬레이션 기술 및 단일·연합 트윈에서 자율적으로 문제 인지, 예측, 해결하는 초지능 기술 개발</td></tr><tr><td>연합</td><td>이종 디지털 트윈의 상호연동을 위한 연합기술 개발</td></tr><tr><td>메타버스</td><td>초실감 융합현실</td><td>현실과 가상이 완벽히 융합된 융합현실을 제공하는 핵심 기술 개발</td></tr><tr><td>ESG/탄소중립</td><td>그린 디지털 전환</td><td>데이터센터·네트워크의 에너지 효율화 핵심기술 개발 및 ESG/탄소중립 데이터 수집·분석·예측·의사결정 기술 고도화</td></tr><tr><td rowspan="4">산업융합</td><td>지능형 자율화</td><td>초지능 융합 기술을 통해 제조·농축수산·에너지 등 다양한 산업 분야의 전주기 지능형 자율화 실현</td></tr><tr><td>특화 AI융합</td><td>국방, 의료 등 특수한 산업분야를 위한 특화된 빅데이터·생성형 AI 개발 및 우주·심해 등 극한 환경용 디바이스 기술 개발</td></tr><tr><td>초정밀 예측</td><td>재해·재난 등을 예측·예방할 수 있는 재난 안전 빅데이터 구축과 AI기반 초정밀 재난·재해 예측 기술 개발</td></tr><tr><td>디지털 포용</td><td>AI, 로봇 기술 등을 통해 고령·장애를 극복하고 디지털 시대 자립을 지원하는 디지털 포용 기술 개발</td></tr></table>			기술확보 목표	블록체인	고신뢰 웹3 기반 기술	고신뢰 웹3 구현을 위한 다계층·이종 네트워크 연결 기술 및 AI기반 계약·합의 기술 개발	디지털 트윈	초정밀·초지능	현실 특성을 정밀하게 반영하는 시뮬레이션 기술 및 단일·연합 트윈에서 자율적으로 문제 인지, 예측, 해결하는 초지능 기술 개발	연합	이종 디지털 트윈의 상호연동을 위한 연합기술 개발	메타버스	초실감 융합현실	현실과 가상이 완벽히 융합된 융합현실을 제공하는 핵심 기술 개발	ESG/탄소중립	그린 디지털 전환	데이터센터·네트워크의 에너지 효율화 핵심기술 개발 및 ESG/탄소중립 데이터 수집·분석·예측·의사결정 기술 고도화	산업융합	지능형 자율화	초지능 융합 기술을 통해 제조·농축수산·에너지 등 다양한 산업 분야의 전주기 지능형 자율화 실현	특화 AI융합	국방, 의료 등 특수한 산업분야를 위한 특화된 빅데이터·생성형 AI 개발 및 우주·심해 등 극한 환경용 디바이스 기술 개발	초정밀 예측	재해·재난 등을 예측·예방할 수 있는 재난 안전 빅데이터 구축과 AI기반 초정밀 재난·재해 예측 기술 개발	디지털 포용	AI, 로봇 기술 등을 통해 고령·장애를 극복하고 디지털 시대 자립을 지원하는 디지털 포용 기술 개발
기술확보 목표	블록체인	고신뢰 웹3 기반 기술	고신뢰 웹3 구현을 위한 다계층·이종 네트워크 연결 기술 및 AI기반 계약·합의 기술 개발																								
	디지털 트윈	초정밀·초지능	현실 특성을 정밀하게 반영하는 시뮬레이션 기술 및 단일·연합 트윈에서 자율적으로 문제 인지, 예측, 해결하는 초지능 기술 개발																								
		연합	이종 디지털 트윈의 상호연동을 위한 연합기술 개발																								
	메타버스	초실감 융합현실	현실과 가상이 완벽히 융합된 융합현실을 제공하는 핵심 기술 개발																								
	ESG/탄소중립	그린 디지털 전환	데이터센터·네트워크의 에너지 효율화 핵심기술 개발 및 ESG/탄소중립 데이터 수집·분석·예측·의사결정 기술 고도화																								
	산업융합	지능형 자율화	초지능 융합 기술을 통해 제조·농축수산·에너지 등 다양한 산업 분야의 전주기 지능형 자율화 실현																								
		특화 AI융합	국방, 의료 등 특수한 산업분야를 위한 특화된 빅데이터·생성형 AI 개발 및 우주·심해 등 극한 환경용 디바이스 기술 개발																								
		초정밀 예측	재해·재난 등을 예측·예방할 수 있는 재난 안전 빅데이터 구축과 AI기반 초정밀 재난·재해 예측 기술 개발																								
디지털 포용		AI, 로봇 기술 등을 통해 고령·장애를 극복하고 디지털 시대 자립을 지원하는 디지털 포용 기술 개발																									

□ 기술발전 전망과 R&D 핵심이슈

블록체인

- 향후 6년간 블록체인의 핵심이슈를 고려한 ①블록체인 기반 기술, ②블록체인 응용 기술, ③블록체인 확장 기술로 분류하여 관련 기술에 초점을 맞추어 후보기술 설정

구분		개념
블록체인 기반 기술 (5)	서비스 적응형 다계층 합의 기술	○ 서비스별 별도의 블록체인을 활용하는 비효율성을 개선하기 위한 Non-monolithic 구조 기반 다계층 블록체인 합의 기술로서 서브체인 서비스 특화(실시간, 대용량, 프라이버시 보장) 합의 기술, 서비스 적응형 멀티체인 인터페이스 기술, 온디바이스 합의 기술, 웹 3 프로토콜 임베디드 합의 기술
	고속 대용량 블록체인 데이터 처리 기술	○ 고속 대용량 블록체인 데이터 처리 기술은 대규모 블록체인 분산원장 데이터를 효율적으로 저장, 처리, 분석 및 최적화하는 기술로 블록체인의 확장성과 효율성을 극대화하고, AI를 활용하여 데이터의 신속한 처리와 이상 탐지를 가능하게 하며, 사용자에게 직관적인 데이터 시각화를 제공하는 기술
	고신뢰 AI 기반 스마트 컨트랙트 기술	○ 고신뢰 AI 기반 스마트 컨트랙트 기술은 스마트 컨트랙트의 작성, 배포, 실행, 검증 및 최적화를 포함한 전 주기적 과정을 포함하는 기술로 AI와 고신뢰 컴퓨팅을 활용하여 스마트 컨트랙트의 안전성과 신뢰성을 극대화하고, 사용자 친화적인 스마트 컨트랙트 작성 및 실행 환경을 제공하는 기술
	인터 블록체인 네트워킹 최적화 기술	○ 웹3 환경에서 대규모 트랜잭션의 네트워크 전파 및 합의 도달 지연을 방지하기 위해 최소비용 최적경로를 보장하는 블록체인 간 네트워킹 최적화 기술로서 이기종 인터 블록체인 트랜잭션/블록 전파 경로 최적화 기술, 피어 노드 간 저지연 메시지 전송 기술, Layer 2 데이터 전파 경로 최적화 기술, 대용량 블록체인 데이터 고속 전송 기술
	블록체인 보안위협 대응기술	○ 참여자의 프라이버시를 보호하고 다양한 보안 위협에 효과적으로 대응하기 위한 보안 기술로서 영지식증명 생성/검증 효율성 향상 기술, 동형암호 기반 프라이버시 보호 기술, 양자내성 트랜잭션 서명 생성/검증 기술, TEE 기반 키 관리 기술, 블록체인 네트워크 레질리언스 확보 기술, AI를 활용한 블록체인 서비스 이상거래 탐지 기술
블록체인 응용 (4)	데이터 주권 보장 웹3 응용 기술	○ 웹 3 환경에서 앱이나 플러그인 없이 사용자들이 직접 분산 앱에서 발생한 디지털자산의 발행·거래·유통 지원 기술, 영구적 손실(Impermanent Loss)를 줄이기 위한 자동화된 마켓 메이커 기술 및 거버넌스 참여자 이탈에 따른 하여 최적화 문제 해결을 위한 DAO 운영 기술, 공개된 분산원장에서 프라이버시 노출로 인한 부작용 문제를 해결하는 기술
	자기 주권 신원인증 기술	○ 중앙집중식 신원인증 기술과는 달리 신원정보를 사용자가 직접 소유하고 관리하여 이용자의 신원을 인증·인가하고 권한을 통제하는 분산신원 증명 및 소유권 증명을 포함한 탈중앙화 신원인증 기술
	사용자 친화적 디지털지갑 기술	○ 디지털자산, 신원정보 등 개인 자산과 정보를 안전하게 보관하고 관리할 수 있는 안전한 키 복구·백업 및 디지털지갑의 사용자 이용경험 개선 및 양자 컴퓨터와 같은 고성능 컴퓨팅에 의한 비공개키 노출 위험성 방지를 위한 계정 추상화 기반 비공개키 보호 트랜잭션 서명 기술과 사용자 접근성보장을 위한 웹 브라우저 기반 지갑 기술, 글로벌 상호연동 지갑 기술

구분		개념
	실용형 블록체인 융합 기술	○ 블록체인의 활용성 확대를 위한 다양한 ICT 기술 및 타산업과의 융합을 통해 상호보완 및 융합창조 가치를 실현하기 위한 블록체인 기술 융합(AI, IoT, 5G-6G융합 등), 블록체인 산업 융합(메타버스, 물류, 콘텐츠, 핀테크 등) 기술
블록체인 확장 기술 (3)	신뢰성 보장 다계층/샤드 간 성능 확장 기술	○ 신뢰성 보장 다계층/샤드 간 성능 확장 기술은 블록체인 네트워크의 확장성과 성능을 극대화하기 위한 포괄적인 기술로 샤드 간 고신뢰 저지연 통신 기술, 고속 트랜잭션 샤드 구성 및 관리 기술, 이기종 인터 블록체인 기술을 포함하고, Layer-2 데이터 전파 경로 최적화 기술, Layer-2 상호운용성 기술, 적응형 Layer-2 스케일링 기술을 통합하여, 블록체인 네트워크의 성능과 효율성을 혁신적으로 개선하는 기술
	블록체인 데이터 중개 및 오라클 기술	○ 블록체인 기술의 확장성을 확보하여 블록체인 간의 속도 및 비용을 최적화하고 다양한 산업군에 적용할 수 있도록 신뢰를 보장하는 시스템 기술로서, Layer 1/2 구분 없이 데이터 교환이 가능한 통합상호운용성, 기존 인터넷과 블록체인 간 데이터 전송을 위한 인바운드/아웃바운드 오라클 기술, 자기주도 환경 지원을 위한 분산 신원 오라클 기술, 블록체인의 혼잡과 높은 거래 수수료를 최적화 하는 State Channels 기술
	블록체인 시스템 관리 및 운영을 위한 개발지원 기술	○ 웹 3 서비스 개발 환경을 간소화하고 활성화하며, 다양한 방면에 적용가능한 블록체인 기반 추적·규제 시스템의 표준 확보를 위한 클라우드 기반 SaaS/PaaS 관리 확장, 시스템 구성, 장애 분석·대응, 성능 모니터링, 블록체인 개발 지원 기술

디지털 트윈

- 향후 6년간 디지털 트윈 기술은 아래 5대 요소기술들에서 데이터 확보 효율화, 시뮬레이션 정확도 향상, 시각화 활용 최적화, 트윈 연합, 자율형 트윈 등의 기술을 선제적으로 개발 필요

구분	개념	
디지털 트윈 가상화 기술	<ul style="list-style-type: none"> 현실 세계를 구성하는 사람, 사물, 공간 등 구성요소의 디지털 정보화 및 객체화 기술 * 다차원 정보 시각화 기술, 가상센서 신뢰성 확보 기술 등 필요 	
디지털 트윈 동기화 기술	<ul style="list-style-type: none"> 현실세계와 가상세계에 존재하는 각 객체가 정적요소(공간·시각)와 동적요소(상태·행동·프로세스·예측)의 실시간·비실시간 상호 반영을 위한 기술 * 정보 무결성 유지기술, 고정밀 제어 액추에이터 기술 등 필요 	
디지털 트윈 모델링 및 시뮬레이션 기술	<ul style="list-style-type: none"> 가상화된 유무형의 객체정보를 기반으로 사람, 사물, 공간 등의 정보를 분석, 예측하는 기술 * 멀티모달 PINN 기반 범용 AI 모델링 기술, 모델링 가속화 기술 등 필요 	

구분	개념	
디지털 트윈 연합 기술	<ul style="list-style-type: none"> 디지털 트윈들이 데이터 및 기능을 공유하여 기존 서비스를 확장하거나 신규 서비스를 제공할 수 있도록 상호연합 및 협업하는 기술 * 트윈간 상호 운용성 제공기술, 자율형 디지털 트윈 연합기술 등 필요 	
디지털 트윈 서비스 기술	<ul style="list-style-type: none"> 서비스 전주기 관리를 위한 서비스 공통 요소 기술 및 관련 플랫폼 기술 * LoD를 고려한 3D 데이터 고속 표출기술, 생성형 AI 이용 자율형 트윈기술 등 필요 	

□ R&D 추진방향

블록체인


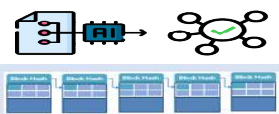
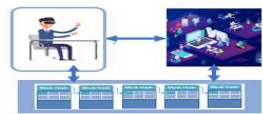
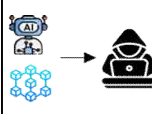


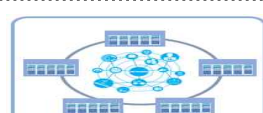

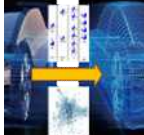



- 환경 분석 및 기술 발전 전망을 토대로 R&D 추진방향성을 도출
- R&D 추진방향은 기존 블록체인 기술을 발전적으로 고도화하면서 동시에 웹 3 라는 새로운 패러다임에 선제적으로 대응하는 방향으로 추진 필요

	As is (현재)	⇒	To Be (미래)
블록체인 기반기술	<ul style="list-style-type: none"> 고속 효율적 경량 합의구조 대용량 분산원장 개발 관점 스마트 컨트랙트 저지연 초고속 P2P 네트워킹 프라이버시 보호 		<ul style="list-style-type: none"> 대용량·이기종 노드들의 초저지연 합의구조 상호운용성 보장 및 이기종 트랜잭션 처리·저장·분석 현실 서비스 적용가능한 안전성·편의성 보장 스마트 컨트랙트 대규모 분산 노드 환경에서 지능형 최적 경로 네트워킹 영지식증명과 양자 내성 암호 적용 보안기술
블록체인 응용기술	<ul style="list-style-type: none"> 웹 2.0 응용서비스 분산ID 기반 신원인증 모바일 간편결제 및 인증 블록체인 산업·기술 융합 		<ul style="list-style-type: none"> 웹3 구현 탈중앙화와 디지털자산 생태계 기술 양도불가능 NFT 기반 신원인증 글로벌 범용 호환성 지원 지갑 AI·IoT·메타버스 융복합 초지능·초경험·초연결
블록체인 확장기술	<ul style="list-style-type: none"> 성능 확장 기술 블록체인 플랫폼 간 상호운용성 블록체인 개발·운영·관리 		<ul style="list-style-type: none"> Layer-2 고도화와 고성능 하드웨어 온·오프체인 및 가상·현실 상호운용성 서비스(XaaS)기반 통합 개발·운영·관리 효율화

디지털 트윈

As is (현재)	To Be (미래)
<ul style="list-style-type: none"> · (가상화) 사람이 쉽게 인지 가능한 영역에 대한 디지털 정보화 및 가시화 · (동기화) 고정된 환경에서 관제 및 원격 제어를 지원하는 양방향 동기화 · (모델링) 독립적 디지털 트윈 대상 수치 해석 기반 시뮬레이션 적용 · (연합) 특정 산업 분야에서 독립적으로 구축 및 운영 · (서비스) 사일로식 서비스 운영으로 인한 단방향 서비스 제공 	<ul style="list-style-type: none"> · (가상화) 비가시영역 내의 객체에 대한 초정밀 디지털 정보화 지원 · (동기화) 사전에 예측하기 어려운 환경 변화에도 복합추론을 통한 유연한 대응이 가능한 동기화 · (모델링) 복합 데이터와 AI 통합으로 다양한 분야에서 실시간 정밀 예측을 제공하는 고도화된 디지털 트윈 플랫폼 · (연합) 다양한 디지털 트윈 간 긴밀한 상호 연결과 지능적인 협업 가능 · (서비스) 다양한 서비스가 상호 연동하여 라이프 사이클 전주기의 최적 운영이 가능한 자율형 서비스 제공

□ 주요 마일스톤

구분		2024	2025	2026	2027	2028	2029	2030
블록체인	기술	블록체인·AI 거버넌스 기술		AI 활용 블록체인 데이터 분석 기술		AI 활용 이상 트랜잭션 탐지, 분석 및 시각화 기술		
				AI 활용 스마트 계약 취약점 탐지 및 개선 기술	AI 기반 블록체인 코드 취약점 자동화 검출 기술		AI 활용 사용자 중심 스마트 계약 자동 생성 기술	
		블록체인·AI(Federated Learning) 연계 기술		블록체인 기반 AI 안전성 보장 기술 <4순위>			블록체인 기반 딥페이크 대응기술 <2순위>	
				AI 활용 블록체인 서비스 이상거래 탐지 기술 AI-powered 블록체인 오라클 기술 <3순위>			블록체인 기반 AI Agent 생성물 진품 검증 기술	
	제품	인공지능 학습 탈중앙화 공유 플랫폼	AI 학습 데이터/모델 투명성 보장 플랫폼		몰입형 인터넷 신뢰 분산 플랫폼		AI 활용 이상 거래 탐지 시스템	
								
서비스	블록체인 기반 거대 모델 챗봇 서비스	AI 학습 데이터/모델 주권보장 및 보상 서비스 <5순위>		AI 생성 결과물 신뢰 검증 서비스 <1순위>		신뢰 기반 초지능·초경험·초연결 서비스		
								
디지털트윈	기술	멀티모달 AI 복합추론 기반 자율 동기화 및 객체화 기술						
		생성형 AI 기반 디지털 트윈 3D 모델 동기화 및 최적화 기술						
	제품					AI 학습과 생성형AI를 이용해 스스로 문제를 해결하는 자율형 트윈 기술		
				AI 기반 복합 추론 동기화 탑재 솔루션				AI를 활용한 자율형 솔루션
								
서비스			다차원 정보 자율시각화 서비스		초실시간 동기화 기반 공공안전 서비스			
								

□ 디지털트윈

구분	주요 동향
국내	<ul style="list-style-type: none"> ○ (네이버) 디지털 트윈 솔루션 '아크아이'를 통해 쇼핑몰, 공항, 지하철, 고층빌딩 등 공간을 디지털 트윈으로 구축하고자 하는 기업, 단체 등을 대상으로 전문 장비와 클라우드 인프라까지 통합 제공 <ul style="list-style-type: none"> * '21년부터 일본 소프트뱅크와 협업하여 도시 단위 고정밀 지도제작 등 해외 진출 확대 계획 ○ (포스코) 철강 제조 공정에서 발생하는 데이터를 수집하여 3D 디지털 트윈으로 구현, 생산 공정을 모니터링하고 예측 유지 보수를 수행 ○ (SK텔레콤) 제조업 경쟁력 강화를 위한 '디지털 얼라이언스' 출범('21) <ul style="list-style-type: none"> * 국내 20개 파트너사가 협력하여 국내 중견·중소 제조기업의 경쟁력 강화와 근로자 안전 제고에 도움이 될 '구독형 디지털 트윈 서비스' 출시를 목표로 함 ○ (KT) 국내 디지털 트윈 활성화를 위해 K-디지털 트윈 워킹그룹 출범('23) <ul style="list-style-type: none"> * 국내 19개 기업·기관·대학이 참여하며, KT는 클라우드 스트리밍 기술을 제공하고 5G 등 통신 최적화를 지원 * 건설·국토·유통·커머스·게임 메타버스 3개 그룹을 운영하며, DT별 리더를 선임해 그룹내 파트너사들과 다양한 협업 사례(Use case)를 만들어 낼 예정 ○ (LX) 데이터 통합 관리체계를 기반으로 모델링, 시뮬레이션이 가능한 디지털 트윈 플랫폼 보유: 도시 관제, 도시문제 예측, 하천침수 분석, 문화재 관리, 교통량 분석 등 ○ (두산중공업) 국내 최초로 디지털 트윈 기반 해상풍력발전 운영 및 유지보수 솔루션 개발 <ul style="list-style-type: none"> * 제주 풍력단지에 파일럿 테스트 후 단계별 확산 예정 ○ (쓰리아이) 설비·시공 관리자가 기존 360도 카메라와 스마트폰을 사용해 건물의 몰입형 디지털 트윈을 더 쉽고 빠르게 생성·관리·탐색할 수 있게 하는 솔루션·디지털 트윈 솔루션 비모(Beamo)개발 ○ (버넥트) 디지털 자산화된 3D 모델·애니메이션·영상·포인팅·드로잉·내레이션 기반 XR 기술과 XR 원격 협업 기술 '버넥트 리모트(Virnect Remote)' 보유
국외	<ul style="list-style-type: none"> ○ (GE/미국, 지멘스/독일, 다쏘/프랑스) 의료·헬스케어, 자동차, 에너지, 항공 등 산업 전반의 다양한 분야로 확대 중 ○ (IDTA/독일) 독일을 중심으로 IDTA(Industrial Digital Twin Association)가 결성되어 AAS(Asset Administration Shell) 디지털 트윈에 대한 구조(Architecture) 및 시나리오(Use case) 표준 개발, 오픈소스 및 테스트베드 운용, 호환성 인증체계 마련, 교육 등 활동 진행 ○ (SPHERE 프로젝트/EU) 유럽의 10개 국가, 18개 파트너가 참여하는 SPHERE 프로젝트는 BIM(Building Information Modelling) 기반 디지털 트윈 플랫폼 개발 ○ (SAP/독일) KAESER Kompressoren(독일) 회사와 협력하여 압축 공기 제조 과정에서 디지털 트윈을 활용한 모델링 & 시뮬레이션 기술을 개발 ○ (지멘스/독일) Electronics Works Amberg(EWA)는 클라우드 기반 개방형 IoT 플랫폼인 마인드 스피어에 디지털 트윈을 접목 ○ (마이크로소프트/미국) Azure를 통하여 건물, 공장, 농장, 에너지 네트워크, 철도, 경기장 등의 전체 환경(전체 도시)의 디지털 모델을 기반으로 디지털 트윈을 생성할 수 있는 PaaS(Platform as a Service) 제공 ○ (GE/미국) Predix 플랫폼은 산업 최적화를 위한 자산(자원, 에너지), 네트워크(그리드), 프로세스(제조) 등의 분야별 예측 분석으로 운영비용과 리스크 감소 ○ (엔비디아/미국) 옴니버스는 기후변화 예측을 위한 지구 디지털 트윈 등 산업 및 과학 응용 프로그램을 위한 대규모 시뮬레이션을 제공 ○ (다쏘/프랑스) 3D Experience는 제조, 생명과학·헬스, 인프라·도시 분야에서 제품 개선, 효율성 향상, 비용 절감을 지원하는 3D 모델링 및 시뮬레이션을 제공

□ 블록체인의 ① 기반 기술

구분	주요 동향
국내	<ul style="list-style-type: none"> ○ (분산합의 알고리즘 기술) 오픈소스 블록체인 플랫폼(이더리움, EOS 등)을 도입하여 허가형 블록체인으로 사용하는 사례가 주를 이루고 있으며, PBFT를 변형한 합의 기술들이 개발되고 있음 <ul style="list-style-type: none"> - 파라메타(구 아이콘루프)에서는 엔터프라이즈 환경에 적합한 블록체인 엔진인 루프체인을 개발하고 자체 개발한 LFT 합의 프로토콜 탑재(LFT 합의 프로토콜은 PBFT와 매우 유사한 구조를 가지고 있지만 합의 메시지 교환 단계를 2단계로 단축) - 심버스는 미리 자격이 검증된 수십 개의 노드들이 참여하여 합의하는 방식인 심센서스라는 BFT 합의 알고리즘 개발 - 루니버스는 이더리움 기반 POA 프로토콜과 하이퍼레저(Hyperledger) 기반 IBFT 프로토콜을 일부 수정하여 적용 - ETRI에서는 탈중앙화 블록체인에 사용할 수 있는 BFT 합의 알고리즘인 BADA 개발 ○ (다계층·지능형 분산합의 기술) 단일 합의체 구성을 확장하여 다중 합의체 구성이 가능한 분산합의 기술이 개발되고 있음 <ul style="list-style-type: none"> - ETRI에서는 동적으로 다중 합의체를 구성할 수 있는 분산합의 기술을 개발 중에 있음
	② 분산원장 기술 <ul style="list-style-type: none"> ○ (트랜잭션 처리 기술) <ul style="list-style-type: none"> - (Deconomy) 국내 대표적인 블록체인 포럼인 Deconomy를 통해 다양한 원장 구조가 논의 - (ChainToB) 국내 기업이 개발한 BaaS(Blockchain-as-a-Service), 다양한 원장 구조를 지원한다고 발표하였지만 추가 업데이트는 없는 상태 ○ (탈중앙 스토리지 기술) <ul style="list-style-type: none"> - 한국지능정보화진흥원(NIA)은 블록체인 기반의 불변 원장 기술 개발에 주력하고 있음. 데이터의 변조를 방지하고 무결성을 보장하는 데 중점 ○ (분산원장 저장 기술) <ul style="list-style-type: none"> - 스마트시티 프로젝트: 부산, 대구, 인천, 성남 등에서 시험적으로 진행되고 있는 블록체인 기반 스마트시티 프로젝트에서 사용하는 원장구조를 통해 최신 R&D 방향성 이해
	<ul style="list-style-type: none"> ○ (분산원장 분석 기술) <ul style="list-style-type: none"> - 한국의 블록체인 스타트업들은 실시간으로 블록체인 네트워크를 모니터링하고 트랜잭션을 분석하는 기술을 개발하고 있으며 이를 통해 사용자는 거래의 동향과 이상징후를 즉시 파악
	③ 스마트 컨트랙트 기술 <ul style="list-style-type: none"> ○ (스마트 컨트랙트 언어·기반 기술) <ul style="list-style-type: none"> - 이더리움(Ethereum)의 Solidity와 같은 스마트 컨트랙트 전용 언어의 발전과 함께, 다양한 블록체인 플랫폼에서 스마트 컨트랙트를 지원하기 위한 새로운 언어·도구들 등장 - 국내에서는 스마트 컨트랙트 언어 또는 플랫폼에 관련 연구는 활발하지 않으며 허가형 블록체인을 중심으로 스마트 컨트랙트 기반 기술 중 관리 도구 관련 연구와 개발이 진행 ○ (스마트 컨트랙트 검증 기술) <ul style="list-style-type: none"> - 최근 스마트 컨트랙트 검증 기술은 전통적인 방법과 딥러닝의 고급 기능을 결합하여 스마트 컨트랙트에서 취약점 탐지의 효율성과 정확성을 모두 향상시키는 통합된 접근 방식으로 발전하고 있음 - 국내에서도 딥러닝 등 다양한 기법을 이용한 취약점 발견 논문들이 발표되고 있으며 고려대에서 "스마트 컨트랙트의 개발·배포·실행의 전주기적 취약점 개선 기술 개발" 과제를 진행 중 ○ (스마트 컨트랙트 실행 기술) <ul style="list-style-type: none"> - 스마트 컨트랙트 실행 기술은 위험 상황을 탐지·모니터링, 회피, 처리 기술로 코드를 실행하기 전에 분석하는 정적 분석, 스마트 컨트랙트를 실제로 실행하면서 취약점을 찾아내는 동작 분석, 이미 발생한 트랜잭션을 분석하여 의심스러운 활동이나 패턴을 찾아내는 포렌식 분석 등으로 구분 - 국내에서도 고려대, 전남대, 이화여대, 정적 분석, 동적 분석 관련 논문들이 발표
	④ 블록체인 네트워킹 기술 <ul style="list-style-type: none"> ○ 블록체인 노드 간 메시지 전달 최적화 및 블록 동기화 문제 해결을 위한 기술이 개발되고 있음 <ul style="list-style-type: none"> - 포스텍 송황준 교수팀에서 '블록체인 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발' 과제 수행 중 ('21~'25)

구분	주요 동향
	<ul style="list-style-type: none"> - 구조화된(Structured) 노드 연결을 제안하고, 연결 최적화에 필요한 노드 간 딜레이 추론을 위해 네트워크 좌표 시스템을 활용 - KAIST 강민석 교수팀에서 비트코인의 블록 동기화 문제에 대한 측정 논문 발표('22) <p>⑤ 블록체인 보안 기술</p> <p>o (프라이버시 보호 기술)</p> <ul style="list-style-type: none"> - (아이콘루프) DID 기반의 '마이아이디' 서비스 개발. 한국인터넷진흥원(KISA)의 블록체인 공공선도 시범사업에 선정(출처: 아이콘루프 공식 웹사이트) - (라온시큐어) DID 기술을 활용하여 다양한 디지털 신분증 서비스 제공(출처: 라온시큐어 공식 보도자료) - (SK텔레콤) '이니셜'이라는 DID 기반 서비스를 통해 디지털 아이덴티티 보호에 주력(출처: SK텔레콤 공식 보도자료) - (서울대학교 및 삼성SDS) ZKP를 활용한 개인정보보호 기술을 공동 연구 및 개발(출처: 서울대학교 산학협력단) - (LG CNS) Ring Signatures를 이용한 개인정보보호 및 익명성 유지 기술을 연구 중(출처: LG CNS 블로그) - (씨피랩스) 다양한 블록체인 기반 개인정보보호 솔루션을 개발 및 제공(출처: 코인플러스 공식 웹사이트) - (지크립토) 퍼블릭 블록체인과 영지식증명 기술을 활용한 zkVoting 투표앱을 통해 비밀 투표, 종단간 검증, 투표 조작 방지 지원. 공개 블록체인에서 세계 최초로 익명성과 감사를 지원하는 디지털자산 거래 지갑 앱(Azeroth) 출시 <p>o (네트워크 보안 기술)</p> <ul style="list-style-type: none"> - KISA의 블록체인 보안 가이드라인 제정 및 업데이트: 한국인터넷진흥원(KISA)은 블록체인 기술의 안전한 적용과 활용을 위한 보안 가이드라인을 제공하고 있으며, P2P 네트워크 보안, 스마트 컨트랙트 취약점 관리, 시스템 보안 등 다양한 분야에 지속적으로 업데이트 진행 중 - 블록체인 기반 네트워크 성능 및 보안 기술 연구개발: 국내 다수의 대학 및 연구소에서 블록체인 네트워크의 성능과 보안을 개선하기 위한 연구를 진행하고 있으며 더 빠르고 안전한 블록체인 네트워크 프로토콜 개발을 목표로 추진 - 국내 기업들의 블록체인 보안 솔루션 개발: 다수의 국내 기업들은 블록체인 네트워크 보안 솔루션 개발에 집중하고 있으며 이러한 솔루션은 네트워크 취약점을 방지하고, 공격으로부터 블록체인 시스템을 보호하는 데 중 <p>o (시스템 보안 기술)</p> <ul style="list-style-type: none"> - 국가 주도의 양자내성 암호학 연구: 국내에서는 정부 주도로 양자 컴퓨터에 대한 내성을 갖는 암호 기술 개발에 중점을 두고 있으며 미래 양자컴퓨팅 위협으로부터 블록체인 시스템을 보호하는 데 중요한 역할 - 위메이드: 서틱(Certik)과 같은 전문 보안 감사 기관을 활용하여, 사용자와 투자자들에게 자사의 플랫폼이 안전하다는 확신을 제공하고, 블록체인 및 스마트 컨트랙트의 보안 수준을 높여 해킹 및 기타 사이버 위협으로부터 자산을 보호 <p>o (소프트웨어 보안 기술)</p> <ul style="list-style-type: none"> - PASS: 한국정보통신기술협회(TTA)와 협력하여 개발된 블록체인 기반의 신원인증 시스템 - 업비트: 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 제정한 정보보호 관리체계에 대한 국제 보안 표준 인증 'ISO27001', 'ISO27017', 'ISO27018'을 획득하였고, BitGo의 멀티 시그니처 월렛을 사용, 카카오페이를 이용한 2채널 추가인증을 이용. 외부 전문기관을 통해 주기적인 보안 감사를 받아 시스템의 취약점을 찾아내고 개선. 이용자 자산 대부분을 온라인에서 분리된 콜드월렛(Cold Wallet)에 보관하여 해킹 위협으로부터 자산을 보호. 업비트 해킹사건 사례처럼 ISMS 심사를 받아도 보안 문제 발생 가능성에 대한 주의
국외	<p>① 합의 기술</p> <p>o (분산합의 알고리즘 기술) 퍼블릭 블록체인을 대상으로 한 합의 프로토콜이 지속적으로 개발되고 있음</p> <ul style="list-style-type: none"> - 초기에는 POW 중심의 합의 알고리즘이 주를 이루었지만, 현재는 대부분 지분증명 기반 합의 알고리즘 - 특히 PBFT의 단순 변형은 대규모 노드가 참여하는 환경에서는 적합하지 않기 때문에 대규모 노드가 참여하는 방식에서도 동작하는 신규 BFT 알고리즘이 다수 개발됨(알고란드의 BA*, 이더리움의 GASPER 등) - 단순히 합의 프로토콜에 그치지 않고 다양한 암호학 기법(VRF, BLS, 영지식증명 등)과

구분	주요 동향
	<p>연계하여 성능/보안을 향상시키기 위한 기술 개발이 이루어지고 있음</p> <ul style="list-style-type: none"> ○ (다계층·지능형 분산합의 기술) 성능 향상을 위한 새로운 합의 알고리즘이 지속적으로 개발되고 있음 <ul style="list-style-type: none"> - 솔라나 PoH, hashgraph 등 성능 향상을 위한 분산합의 기술 개발이 지속적으로 진행되고 있으며, 특히 샤딩, Layer-2 기술(라이트닝 네트워크, 롤업 등)에 대한 연구 개발이 매우 활발 <p>② 분산원장 기술</p> <ul style="list-style-type: none"> ○ (트랜잭션 처리 기술) <ul style="list-style-type: none"> - UTXO-based Ledgers: 비트코인에서 사용되며, 트랜잭션 출력의 사용 여부를 통해 상태를 관리 - State-based Ledgers: 이더리움에서 사용되며, EVM을 통한 스마트 컨트랙트 실행 가능 - Interoperable Blockchains: Polkadot과 Cosmos가 대표적인 사례 - DAG (Directed Acyclic Graph): IOTA는 DAG 기술을 사용하여 확장성과 속도 개선 - Industry-specific ledgers: 리플(Ripple)은 금융 산업에 특화된 블록체인을 제공 ○ (탈중앙 스토리지 기술) <ul style="list-style-type: none"> - Elliptic Curve Digital Signature Algorithm (ECDSA): 대부분의 블록체인에서 사용되는 디지털 서명 알고리즘 - 상호운용성: Chainlink, Polkadot, Cosmos는 블록체인 간의 연결성을 높이는 데 초점 - 미국의 Protocol Labs는 Filecoin을 통해서 IPFS(InterPlanetary File System)를 제공하는 솔루션 개발. 데이터 저장의 분산화를 촉진하고 보다 효율적인 데이터 공유 방식을 제공 ○ (분산원장 저장 기술) <ul style="list-style-type: none"> - Directed Acyclic Graphs (DAG): IOTA와 Hedera Hashgraph에 적용, 블록 생성 시간을 줄이고 병렬 처리 가능 - Secure Multi-Party Computation (SMPC): 데이터를 안전하게 공유 및 처리할 수 있는 방법 제공 - 아마존의 Quantum Ledger Database (QLDB): 아마존은 Quantum Ledger Database (QLDB)를 개발하여 중앙화된 데이터베이스의 신뢰성과 블록체인 기술의 불변성을 결합하였으며 높은 처리 속도와 데이터 무결성 제공 - Hyperledger Fabric의 데이터 스토리지 개선 - IBM은 Hyperledger Fabric의 데이터 스토리지와 트랜잭션 처리 능력을 향상시키기 위해 지속적인 개선 작업 진행. 특히 다중버전 동시성 제어(MVCC) 기술을 활용하여 높은 처리량과 낮은 지연 시간 달성 - 웹 3 인프라 측면에서 데이터를 탈중앙화하여 관리할 수 있는 Solid 프로젝트 추진 중. 사용자가 어떤 앱을 사용하든 사용자의 데이터는 사용자가 지정한 저장소에 저장되고 이 데이터를 사업자가 사용하기 원할 때에는 사용자의 승인을 받은 후 접근하여 사용하는 구조 ○ (분산원장 분석 기술) <ul style="list-style-type: none"> - Chainalysis의 거래 패턴 분석: Chainalysis는 블록체인 데이터를 분석하여 거래 패턴을 파악하는 기술 선도. Chainalysis 솔루션은 의심스러운 활동을 탐지하고 금융 범죄 예방에 기여 - IBM 블록체인 분석 도구: IBM은 블록체인 데이터 분석 도구를 제공하고 있으며 기업들이 블록체인 네트워크에서 발생하는 거래와 상호작용을 더 잘 이해하고 최적화할 수 있도록 지원 <p>③ 스마트 컨트랙트 기술</p> <ul style="list-style-type: none"> ○ (스마트 컨트랙트 언어·기반 기술) <ul style="list-style-type: none"> - 이더리움의 Solidity와 같은 스마트 컨트랙트 전용 언어 발전과 함께, 다양한 블록체인 플랫폼에서 스마트 컨트랙트를 지원하기 위한 Vyper, Michelson, Clarity 등 새로운 언어 및 도구들이 등장 - 가장 큰 스마트 컨트랙트 네트워크인 이더리움과 고성능 스마트 컨트랙트 플랫폼인 아발란체, 팬텀, 솔라나, 이더리움의 Layer-2 솔루션인 아비트럼, 옵티미즘, 베이스 등이 스마트 컨트랙트 관련 새로운 기술과 개선된 성능을 제공 ○ (스마트 컨트랙트 검증 기술) <ul style="list-style-type: none"> - 취약점 탐지를 위한 스마트 컨트랙트의 구문 및 의미 기능을 융합하고, 딥러닝을 점점 더 많이 활용하고 있으며, 동적 분석 등의 전통적인 취약점 탐지 방법을 실제 블록체인 시스템에서 실행하여 정확성을 개선 - 해외에서도 다양한 기법을 기반으로 하는 취약점 탐지 연구가 발표되고 있으며 실제 제품에 적용하는 기업도 늘어나고 있음. 대표적인 기업으로는 북미를 기반으로 하는 Consensys, CertiK, Quantstamp, 유럽을 기반으로 하는 Hacken, Chainsecurity, 아시아를 기반으로 하는 SlowMist 등

구분	주요 동향
	<ul style="list-style-type: none"> ○ (스마트 컨트랙트 실행 기술) <ul style="list-style-type: none"> - 해외에서는 관련 논문이 많이 발표되고 있으며, MythX, SmratDec 등이 정적 분석 서비스를 제공하고 Trail of Bits, OpenZeppelin 등은 동적 분석 서비스를 제공하며, 포렌식 분석 서비스를 제공하는 회사는 많지 않지만 Chainalysis, CipherTrace, Elliptic 등 블록체인 감사 외에 포렌식 분석 서비스를 제공 ④ 블록체인 네트워킹 기술 <ul style="list-style-type: none"> ○ 트랜잭션 및 블록 전파시간 단축 기술이 학계에서 지속적으로 연구 추진 <ul style="list-style-type: none"> - 트랜잭션 전파시간 단축을 위한 프로토콜 연구를 캐나다 UBC, 중국 Tree-Graph Blockchain Research Institute에서 각각 우수 학술대회에 발표 ('19~'20) - 구조화된 네트워크 연결을 통한 블록 전파시간 단축 연구를 독일 TU Berlin에서 상위 SCI 저널에 게재 ('23) - 트랜잭션 전파시간 단축을 위한 개별 노드의 피어 연결 전략 연구를 미국 CMU(Carnegie Mellon University)에서 우수 학술대회에 발표 ('23) ⑤ 블록체인 보안 기술 <ul style="list-style-type: none"> ○ (프라이버시 보호 기술) <ul style="list-style-type: none"> - Microsoft: 'ION' 프로젝트를 통해 DID 기술 개발 및 확산에 주력 (출처: Microsoft 공식 블로그) - uPort: 이더리움 기반의 DID 솔루션을 개발하여 디지털 아이덴티티 보호에 기여 (출처: uPort 공식 웹사이트) - Ontology: 분산 아이덴티티 프레임워크를 통해 다양한 DID 솔루션 제공. (출처: Ontology 공식 웹사이트) - Zcash: ZKP 기술을 활용하여 트랜잭션의 익명성을 보장하는 암호화폐 (출처: Zcash 공식 웹사이트) - Monero: Ring Signatures를 활용한 익명성 보호 기술을 적용한 암호화폐 (출처: Monero 공식 웹사이트) - Ethereum's zk-SNARKs: ZKP를 활용한 개인정보 보호 기술을 이더리움 네트워크에서 실험 및 적용 (출처: Ethereum 공식 문서) ○ (네트워크 보안 기술) <ul style="list-style-type: none"> - 블록체인 기반의 웹 3 보안 프로토콜: 웹 3은 블록체인 기술을 기반으로 분산화된 인터넷의 새로운 형태. 웹 3 환경에서 네트워크 보안은 핵심적인 이슈로 부상하고 있으며 여러 기업과 연구기관이 관련 보안 프로토콜 개발 진행 중 - P2P 네트워크 보안 프로토콜 표준화: 전세계적으로 블록체인 기술의 기반이 되는 P2P 네트워크의 안정성과 보안을 강화하기 위한 노력의 일환으로 P2P 네트워크 보안 프로토콜의 표준화 작업이 진행 중 - 블록체인 네트워크의 실시간 보안 컴플라이언스 기술: 국제적으로 많은 기업들이 블록체인 네트워크의 실시간 보안 컴플라이언스를 위한 기술 개발에 박차. 블록체인 네트워크의 보안 취약점을 실시간으로 감지하고 해결하는 데 중점 ○ (시스템 보안 기술) <ul style="list-style-type: none"> - Quantum-Resistant Algorithms: 양자 컴퓨터의 위협에 대비하여, Post-Quantum Cryptography가 연구되고 있음 - Threshold Signatures: 다수의 참가자가 트랜잭션을 승인해야 하는 다중 서명의 발전 형태 ○ (소프트웨어 보안 기술) <ul style="list-style-type: none"> - Smart Contract Vulnerabilities: DAO 해킹은 스마트 컨트랙트의 취약점 대표 사례 - 51% Attacks: Ethereum Classic은 51% 공격에 취약 - Sybil Attacks 및 Eclipse Attacks: 비트코인과 같은 P2P 아키텍처에서 네트워크 무결성에 영향을 미치는 이론적 취약점

□ 블록체인 [②응용 기술]

구분	주요 동향
국내	<ul style="list-style-type: none"> ① 웹 3 응용 기술 <ul style="list-style-type: none"> ○ (블록체인 연계 소셜 서비스) 서비스 내 재화를 가상자산으로 발행하는 소셜 서비스 <ul style="list-style-type: none"> - 국내 웹사이트인 디시인사이드는 사용자의 게시물을 클레이튼 NFT로 발행하는 기능을 제공 - 국내 게임사인 위메이드는 자사의 게임 IP인 미르와 블록체인을 결합하여 게임 내 재화를 가상자산으로 발행 및 거래할 수 있는 생태계 개발 중 ○ (웹 3 상호운용성 기술) 국외에서는 탈중앙화 금융 서비스의 상호운용과 관련된 기술이 다양하게 개발되고 있으나 국내에서는 아직 소극적인 모습

구분	주요 동향
	<ul style="list-style-type: none"> - 한국전자기술연구원은 웹 3 서비스에서 담보물, 보증금 등으로 제공된 자산에 대한 권리를 NFT로 발행하여 자산에 유동성을 제공하고, 다른 웹 3 서비스에서 활용할 수 있는 Perpetual contract NFT 기술 연구 진행 중 o (DAO 기술) 과기정통부는 2023 블록체인 진흥주년을 통해 '블록체인 산업 진흥법(가칭)' 제정을 통한 제도 정비(안)을 발표 - 디지털자산(NFT 등), 블록체인 기반 탈중앙자율조직(DAO 등)에 대한 구체적인 법적 지위 및 명확한 기준 추진 예정 <p>② 신원인증 기술</p> <ul style="list-style-type: none"> o (DID 기반 서비스) DID를 이용하여 신원 증명 플랫폼 개발 <ul style="list-style-type: none"> - 라온시큐어와 LG CNS가 공동으로 DID 기반 모바일 운전면허증 발급 - 인프라 블록체인은 코로나 19 백신 접종을 증명할 수 있는 DID 발급 o (분산신원증명 기술) <ul style="list-style-type: none"> - 행안부는 모바일 운전면허증 발급 시행. 블록체인을 통해 신원정보의 진위 여부 확인, 자기 정보 결정권 강화 - 라온시큐어는 분산신원증명 플랫폼 '옴니원'을 기반으로 e-병무지갑 서비스를 제공하며, 모바일 공무원증, 모바일 운전면허증 등 행정안전부 모바일 신분증 서비스를 구축하였으며, '옴니원 디지털 ID' 플랫폼을 통해 클라우드 기반 신원·자격증명 통합 서비스 제공 - 씨피랩스(구 코인플러그)는 투표 서비스 '더폴', 출입관리 시스템 '메타패스', 분산신원증명 지갑 앱 '마이키펜' 등을 출시하였으며, 메타패스는 공무원연금공단 모바일 사원증 시스템 구축 o (소유권 증명 기술) <ul style="list-style-type: none"> - 블로코 엑스와의지는 SBT(Soul Bound Token) 오픈 배지 사업을 확장하여 CCTV 3.0이라는 웹 3 인증 서비스 제공 - 분산신원증명(DID) 기술 및 표준화 포럼에서는 NFT 저작권 권리 표시 표준화 방안 및 탈중앙화 신원 관리 시스템 보안 요구사항, 검증 가능한 크리덴셜 규격, DID 상호연동 가이드라인 등 표준화 이슈에 대해 활발한 논의 진행 중 <p>③ 디지털 지갑 기술</p> <ul style="list-style-type: none"> o (블록체인 지갑 기술) <ul style="list-style-type: none"> - 카카오에서는 자회사 그라운드X를 통해 블록체인 기반의 '클레이(Klay)'와 블록체인 지갑 '클립' 출시 - SK텔레콤은 블록체인 데이터 분석 서비스 크립토크트를 운영하는 팀블랙버드와 가상자산 지갑 개발을 위한 사업 제휴 계약 체결 - 삼성전자는 갤럭시 스마트폰에 콜드월렛을 대체하는 블록체인 키스토어와 가상자산을 관리할 수 있는 블록체인 월렛을 탑재하였으며, 삼성페이에 블록체인 지갑을 연동하고 주요 거래소의 가상자산 모니터링 기능 개발 - 안랩 블록체인컴퍼니는 웹 3 지갑 ABC 월렛을 통해 여러 블록체인 네트워크를 지원하고, NFT 전송 기능 제공 - 지크립토는 zk-SNARK 기술을 활용하여 익명성과 감사를 지원하는 디지털자산 거래 지갑 앱인 Azeroth을 통해 디지털자산의 공개·익명 거래 및 감사 기능을 지원 o (신원증명 지갑 기술) <ul style="list-style-type: none"> - 씨피랩스는 위메이드와 협력하여 위퍼블릭월렛을 개발하여 DID/SBT 기반의 신원/자격증명과 잔고증명 기능 제공 - 심버스랩스는 DID를 기반으로 한 QR 인증이 추가된 지갑 솔트(Salt) v1.5를 개발하였으며, 심버스 기반의 ID 뿐만 아니라 비트코인 및 이더리움 주소도 통합하여 제공 o (키관리 기술) <ul style="list-style-type: none"> - 심버스랩스에서 개발한 탈중앙화 지갑 솔트는 키스토어 저장을 통해 계정을 복구하고 분산 저장 방식을 활용하여 안전성과 보안성 강화 - 안랩 블록체인컴퍼니는 ABC 월렛에 Secure MPC 기술을 적용하여 보안성 향상 <p>④ 블록체인 융합 기술</p> <ul style="list-style-type: none"> o (탈중앙 거래 기술) 해외의 탈중앙 거래 기술을 빠르게 흡수한 서비스 제공이 주를 이루고 있음 - 클레이튼은 유니스왑의 constant product market, liquidity concentration 등을 활용하여

구분	주요 동향
	<p>탈중앙 거래 서비스인 클레이스왑(KLAKswap)을 제공</p> <ul style="list-style-type: none"> ○ (블록체인 기술 융합) <ul style="list-style-type: none"> - 과기정통부는 '메타버스·NFT 보안협의체' 발족(2022.7), 안전하고 신뢰할 수 있는 메타버스·NFT 서비스 이용 환경을 구축하고, 보안사고 예방, 이용자 보호를 위한 대응 방향과 보안 지침을 마련 - 보건복지부는 '26년까지 5년간 총 135억원을 투입하여 디지털트윈을 의료 분야에 적용 - KETI 메타버스 사업단 출범(2021.11), VR·AR·XR, Data, Network, AI, 블록체인 등 가상융합세계 구현을 위한 메타버스 핵심 기술 분야의 R&D 프로젝트 기회 발굴과 기술 개발 추진
국외	<p>① 웹 3 응용 기술</p> <ul style="list-style-type: none"> ○ (블록체인 연계 소셜 서비스) 자신이 작성한 글의 서명을 블록체인에 기록하고, IPFS에 저장하여 NFT 발행이 가능한 소셜 서비스 <ul style="list-style-type: none"> - 웹 3 기반 출판 서비스인 Mirror는 사용자가 작성한 글을 블록체인에 저장하고, NFT 발행하는 기능 제공 ○ (웹 3 상호운용성 기술) 특정 웹 3 서비스에서 발행된 토큰을 다른 웹 3 서비스에서 활용할 수 있는 '결합성(composability)' 기술이 다양하게 개발 <ul style="list-style-type: none"> - 탈중앙화 금융 서비스 커브 파이낸스의 DAO에서 투표권으로 사용되는 거버넌스 토큰을 확보하기 위한 경쟁인 Curve war가 대표적인 사례로서, 복수의 웹 3 서비스에서 다른 웹 3 서비스의 토큰을 예치할 때 보상을 지급하는 상호운용 서비스가 다양하게 개발 ○ (DAO 기술) DAO 개발에 사용되는 도구 개발 및 DAO를 이용한 응용 기술 개발이 주를 이루고 있음 <ul style="list-style-type: none"> - Aragon Project는 웹 3 서비스에서 DAO의 생성, 관리, 확장에 사용할 수 있는 개발도구 제공 - Snapshot은 Off-chain Voting 플랫폼으로, Uniswap, Optimism, Aave 등 여러 웹 3 서비스에서 운영중인 DAO에서 가스 수수료 없이 Proposal, Voting이 가능한 프로토콜 제공 - 일본자민당은 'The web3 White Paper'(2023.4)을 발표하면서 DAO의 법적 지위를 명확히 할 수 있는 특별법 제정 권고 ○ 탈중앙화 및 사용자 소유권을 강화하는 형태로 응용 기술이 지속적으로 개발되고 있음 <ul style="list-style-type: none"> - 스팀잇은 블록체인 기반의 SNS로 클릭 수에 따라 암호화폐인 스팀 코인으로 보상받으며, 글을 추천하거나 비추천하는 투표활동 및 스팀파워를 보유하는 것만으로도 스팀 코인을 보상 받음 - 이더메일은 사용자 간 익명 P2P 이메일 전송과 스팸 메일의 원천적 차단이 가능 - Brave 브라우저는 모든 광고와 트래커를 차단함으로써 온라인 프라이버시를 보장하는 블록체인 기반 브라우저 기술이며, DApp과 상호작용 가능한 암호화폐 월렛을 내장 <p>② 신원인증 기술</p> <ul style="list-style-type: none"> ○ (소유권 증명 기술) <ul style="list-style-type: none"> - 이더리움 창시자인 비탈릭 부테린은 지갑에 귀속되어 전송과 매매가 불가능한 SBT(Soul Bound Token)라는 새로운 개념의 토큰을 제안하였으며, SBT는 NFT의 데이터에 개인의 신원을 인증할 수 있는 정보를 담는 방식으로 제작 ○ (NFT를 이용한 신원인증) 신원인증 기술로 DID 기술이 주목받았으나, NFT 시장의 급격한 성장과 간편한 사용으로 NFT를 이용한 신원인증 기술이 활발하게 연구 <ul style="list-style-type: none"> - Soul Bound NFT(SBT)는 비탈릭 부테린이 2022년에 제안한 거래 불가능한 NFT로, NFT 보유자가 자격, 방문 등을 증명하기 위해 사용 - Verifiable credential NFT는 자격증명(여권, 운전면허, 신원정보 등)에 필요한 정보를 담고 있는 NFT를 발행하고, 암호화적인 방법으로 자격증명 정보를 검증하는 방식을 사용 ○ (생체정보를 결합한 신원인증 기술) ChatGPT 개발자 샘 올트먼이 개발한 안구 스캔과 가상자산을 결합한 신원인증 기술 <ul style="list-style-type: none"> - 특수 제작한 장비로 생체정보를 데이터화하고 블록체인에 기록하여 DApp에서 사용할 수 있는 '디지털 여권' 발급 <p>③ 디지털 지갑 기술</p> <ul style="list-style-type: none"> ○ (ERC-4337) Account abstract 표준으로 제안된 ERC-4337이 적용된 지갑 개발 <ul style="list-style-type: none"> - ERC-4337 기능이 지갑에 적용되어 분실한 개인 키 복구, ERC-20 토큰을 이용한 거래 수수료 지급 등이 가능 - 기존 이더리움 디지털 서명 방식은 양자컴퓨팅에 취약했으나, ERC-4337을 적용하면 이더리움 프로토콜이 아닌 이더리움 가상 머신에서 검증하기 때문에 양자 내성이 있는 디지털 서명을 합의 알고리즘 변경 없이 사용 가능

구분	주요 동향
	<ul style="list-style-type: none"> ○ (신원증명 지갑 기술) <ul style="list-style-type: none"> - 갤럭시는 디지털 신원을 제공하는 블록체인 인프라 프로젝트이며 갤럭시 ID로 프로필과 디지털 여권을 발급받을 수 있으며, 유틸리티 토큰인 GAL로 거버넌스에 참여하거나 디지털자산을 거래하고 수수료 지불 가능 ④ 블록체인 융합 기술 <ul style="list-style-type: none"> ○ (탈중앙 거래 기술) 유니스왑, 커브 파이낸스 등의 탈중앙금융 관련 서비스에서 자동화된 마켓(Automated market maker, AMM) 알고리즘을 이용하여 중앙화된 브로커 없이 자산 거래 서비스 제공 <ul style="list-style-type: none"> - 유니스왑은 AMM으로 사용되는 constant product market maker 알고리즘을 개발하여 많은 탈중앙화 금융 서비스에 영향을 주었으며, 현재 유동성 공급과 사용자 환경을 개선한 4번째 프로토콜 업데이트인 v4를 준비 - 커브 파이낸스는 유니스왑의 constant product market maker 알고리즘을 개선하여 가격이 고정된 스테이블코인 거래에 최적화된 프로토콜을 개발. v1에서는 스테이블코인의 탈중앙 거래에 프로토콜이 한정되었지만, v2에서는 여러 토큰에 적용할 수 있는 개선된 market maker 프로토콜 개발 ○ (메타버스·NFT) 블록체인 기반 또는 연계하여 메타버스와 NFT 융복합 추진 <ul style="list-style-type: none"> - META, MS 등 빅테크 기업들이 '메타버스' 관련 표준 개발을 위한 '메타버스 표준화 포럼 (Metaverse Standards Forum)' 출범('22.6) - 미국우정공사(USPS)는 운송 품질 개선을 위해 NFT 활용 계획('21.4)

□ 블록체인 [③ 확장 기술]

구분	주요 동향
국내	<p>① 성능 확장 기술</p> <ul style="list-style-type: none"> ○ (Layer-2 확장 기술) <ul style="list-style-type: none"> - 기존 블록체인을 확장하고 보안 보장성을 상속하는 별도 구축된 블록체인으로 트랜잭션은 유효한 것으로 가정하지만 필요한 경우 Layer-1 체인에서 검증이 가능한 옵티미스틱 롤업, ZK(Zero Knowledge) 롤업이 대표적이며, 현재 옵티미스틱 롤업이 많이 사용되지만 ZK 롤업의 비중이 점점 커지고 있음 - 메인 블록체인에서 특정 거래 처리 작업을 오프로드하여 확장성을 개선하고 수수료를 낮추며 확인 시간을 단축. 국내에서는 옵티미스틱 롤업 기반의 크로마(위메이드), 타이탄 (토카막 네트워크) 등이 출시되었고, 클레이튼과 메타랩스가 ZK 롤업 기반의 Layer-2 솔루션을 개발 중 - 클레이튼 재단은 이더리움 기반 Layer-2 스케일링 솔루션 개발사인 '메타랩스'와 양해각서 체결을 통해 Layer-2와 Layer-3의 높은 거래 처리 역량, 수수료 측면 효율성을 클레이튼 메인넷 상에서 실현할 수 있도록 상호 협력 ○ (샤딩 기술) <ul style="list-style-type: none"> - 트랜잭션 병렬처리가 가능한 더 작고 독립적인 샤드로 나누어 처리량을 향상시켜 블록체인 확장성을 향상. 완전 복제 방식에 비하여 더 적은 노드가 합의에 참여하므로, 보안성을 위해 샤드 내 합의 알고리즘을 견고하게 설계하는 것과 여러 개의 샤드에 영향을 미치는 크로스 샤드(Cross-Shard) 트랜잭션을 효율적으로 처리하는 방향으로 연구가 진행. 국내는 한양대를 중심으로 "대규모 노드에서 블록 단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발" 과제를 진행 중 ○ (블록체인 하드웨어 기술) <ul style="list-style-type: none"> - ASIC, GPU 등의 전용 하드웨어를 이용하여 보다 빠르고 에너지 효율적으로 블록을 생성하고 처리하는 연구가 진행되어 왔으며 최근에는 안전한 다자간 컴퓨팅(MPC) 및 신뢰할 수 있는 실행 환경(TEE)과 같은 기술을 사용하여 블록체인의 컴퓨팅 부담을 완화하여 복잡한 작업을 더 빠르고 고확장성 처리 가능. 펜타 시큐리티, 인피닛블록 등이 MPC 기반 지갑 솔루션을 출시했거나 개발 중 <p>② 블록체인 연동 기술</p> <ul style="list-style-type: none"> ○ (온·오프체인 연동 기술) 블록체인의 활용 범위와 서비스가 다양해지면서, 개인정보보호, 기타 삭제가 필요한 데이터, 기밀성 요구 데이터, 처리속도 개선, 대용량 데이터 저장, 서비스 특수성 등으로 오프체인 활용과 온·오프체인 연동 기술이 활발하게 연구 진행

구분	주요 동향
	<ul style="list-style-type: none"> - 개인정보는 개인정보보호법과 위치정보법에 근거하여 그 목적과 기간이 만료되었을 경우 파기되어야 하지만 블록체인의 속성상 수정·삭제가 불가능. 부산 블록체인 규제자유특구 실증사업을 통해 개인정보 및 위치정보 파기 방법에 오프체인 방식을 허용하는 방식으로 규제 개선 - 삼성 SDS Nexledger는 Off-Chain Manager를 통해 오프체인 기반으로 대용량 데이터 처리가 가능하도록 설계. 오프체인 기술을 통해 파일을 공유할 때는 오프체인 파일은 각 조직별로 갖고 있는 별도의 키를 통해 암호화하고 암호화된 파일은 TLS 통신을 통해 암호화된 전송 구간에서 공유함으로써 보안 확보 o (블록체인 간 연동 기술) 블록체인 상호운용성은 메인체인 기반의 서브체인 구성의 'L2', 서로 다른 메인체인 간 강연결인 '인터체인', 메인체인과 연결된 서브체인 형태의 '사이드체인', 서로 다른 메인체인 간 약연결인 '크로스 체인' 유형으로 구분 - 세종텔레콤의 블루브릭은 이더리움 기반 메인넷을 구현하여 서비스 그룹별 사이드체인 무한 추가가 가능한 멀티 사이드체인 구조와 병렬화 구조를 통해 확장성, 호환성, 안정성 확보 - 파라메타는 블록체인 간 통신 및 상호작용이 가능한 인터체인(Interchain) 기술, BTP (Blockchain Transmission Protocol)를 통해 체인에 구매받지 않고 확장 가능한 크로스체인 상호운용성 솔루션 제공 <p>③ 블록체인 관리 및 개발지원 기술</p> <ul style="list-style-type: none"> o (시스템 구성 기술) <ul style="list-style-type: none"> - 코인플러그의 메타디움 엔터프라이즈는 물리서버와 클라우드 등 다양한 구축 형태를 지원하며 서비스 환경에 맞춰 퍼블릭·프라이빗 블록체인을 지원하며, 기업 컴플라이언스 요구 조건을 충족하는 권한, 암호화 기능을 지원 - 토피도(Torpedo)의 BizFrame BCM은 블록체인 네트워크 구성 지원. Hyperledger Fabric 기반의 블록체인 네트워크를 구축하고 Docker Container 기반의 노드(Peer, Orderer, CA) 구성, 기업 내 자체 블록체인 네트워크 구성 또는 협력기업과의 컨소시엄 블록체인 네트워크 구성 지원 o (장애 분석·대응 기술) <ul style="list-style-type: none"> - 미디움 엠디엘(MDL) 솔루션은 Kubernetes 컨테이너 orchestration 툴을 통한 블록체인 및 모니터링 도구 배포 및 관리를 지원하고 Kubernetes 기능을 활용하여 BaaS(Blockchain as a Service)와 같은 기능으로 확장 가능 o (성능 모니터링 기술) <ul style="list-style-type: none"> - 오퍼스엠의 LedgerMaster 2.0은 하이브리드 블록체인 시스템 작동 이상 여부를 확인하고 전반적인 네트워크 상태는 물론 각 노드별, 노드에 설치되어 있는 프로그램 상태도 모니터링 - 디지털존 다큐체인(DocuChain)은 트랜잭션, 블록, 노드 자원, 네트워크 현황 등 실시간 모니터링 기능을 제공하며 비즈니스 로직 데이터와 블록체인 데이터 간 추적 가능 o (블록체인 개발 지원 기술) 웹 3 비즈니스 환경 도래에 따른 다양한 기술 및 기능을 지원하고 있으며 해외에서는 클라우드 기반의 BaaS가 확산되는 추세 <ul style="list-style-type: none"> - 과기정통부는 블록체인 서비스를 쉽게 개발하고 운용할 수 있는 표준 인프라인 K-BTF (Korea-Blockchain Trust Framework) 도입 발표. K-BTF를 통해 블록체인 간 데이터의 상호운용이 필수적인 웹 3 시대를 대비하고 국내 블록체인 산업의 진흥 유도 - LG CNS의 모나체인은 하이퍼레저 패브릭 기반으로 서비스 기획부터 개발, 배포, 확장, 관리에 이르는 전 영역을 아우르는 서비스 포트폴리오를 제공. 특히 블록체인 개발 지원을 위해 애플리케이션 개발 프레임워크, 엔터프라이즈 연계 모듈, 상호운용성 모듈, 토큰 모델 프레임워크 제공 - 파라메타는 개발자가 보다 손쉽게 블록체인을 개발할 수 있도록 개발자 친화적인 최신 기술 제공. Blockchain Sample & Guide, 다양한 개발언어 지원(JAVA, Python, Solidity), Ethereum Tools와 높은 호환성, 다양한 형태의 노드 제공(풀 노드, 라이트 노드, 프록시 노드, 시뮬레이션 노드 등) - 세종텔레콤은 블록체인 도입에 어려움을 겪고 있는 기업에게 Enterprise Middleware, FabricTool, 모니터링 툴 등을 패키지 형태로 제공 - 최근에는 클라우드 기반으로 개발 지원 및 운영 환경을 제공하는 BaaS가 주목을 받고 있으며 국내 업체로는 람다 256의 루니버스 등이 있음
국외	<p>① 성능 확장 기술</p> <ul style="list-style-type: none"> o (레이어2 확장 기술) <ul style="list-style-type: none"> - 해외에서는 다양한 Layer-2 솔루션이 출시되어 경쟁하고 있으며. 옵티미즘과 아비트럼, ZK(Zero Knowledge) 싱크, 스타크웨어, 폴리곤 등이 대표적 서비스. 옵티미즘은 OP 스택이라는 오픈소스를 바탕으로 한 Layer-2 구축을 지원하고 아비트럼은 4가지 핵심

구분	주요 동향
	<p>제품과 아비트럼 오빗을 통해 Layer-3 롤업 구현 가능. ZK싱크는 옵티미즘과 유사하지만 하이퍼체인을 통해 Layer-3 간 하이브리트지를 사용해 확장성 문제를 해결하고 있고 스타크웨어는 프랙탈 스케일링을 통해, 폴리곤은 zkEVM 등을 통해 상호운용성 제공</p> <p>○ (샤딩 기술)</p> <ul style="list-style-type: none"> - 샤딩 관련한 다양한 논문과 구현체가 나오고 있고 사례로는 샤드 내에서 합의 안정성을 위해 모든 샤드의 블록 내역을 저장하는 MPT 개념을 도입한 Monoxide, 신뢰 실행 환경(Trusted Execution Environment)를 도입하여 PBFT 합의 과정의 안정성을 높인 TEEChain, VRF(Verifiable Random Function)을 사용하여 샤드를 나누는 기술을 적용한 OmniLedger 등이 있음 <p>○ (블록체인 하드웨어 기술)</p> <ul style="list-style-type: none"> - 암호화폐에 대한 안전한 저장소를 제공하는 하드웨어 지갑의 수요는 계속해서 늘어나고 있고, Ledger Nano S/X, Trezor Model T 등이 출시되었고, NVIDIA GeForce RTX, AMD Radeon RX 등의 GPU를 이용하여 블록체인 채굴 속도를 높이고, 고성능 SSD를 사용하여 대용량 블록체인 데이터를 읽고 쓸 때 블록체인 노드 동작 속도를 크게 향상시키고 있음. 또한 TEE를 위해 Intel SGX를 사용하여 블록체인의 보안성을 높이는 연구가 진행되고 이를 적용한 TEEChain 등이 있음 <p>② 블록체인 연동 기술</p> <p>○ (온·오프체인 연동 기술) 오프체인은 온체인의 한계점을 보완하기 위한 목적으로서, 해외에서는 블록체인 기반의 IPFS와 같은 분산형 스토리지가 주목</p> <ul style="list-style-type: none"> - 디지털 작품이 NFT로 발행될 때 NFT는 블록체인에 저장되지만 원본 작품이 중앙저장소에 저장된다는 한계점이 꾸준히 제기. 최근에는 NFT 원본 작품을 IPFS(InterPlanetary File System)에 저장하려는 시도가 확산 - 대표적인 오프체인 거래처리 기법으로 'Public Blockchain + Decentralized Storage', Hyperledger Fabric 'Private Data Collections', Quorum 'Privacy Manager' 등이 활용 - 코인베이스 CEO 브라이언 암스트롱은 사용자의 개인정보 보호 수준을 높이고 민감한 금융정보 노출 위험을 줄이기 위해 오프체인 트랜잭션은 메인 블록체인 네트워크 외부에서 수행 필요성을 주장 <p>○ (블록체인 간 연동 기술) 블록체인 서비스가 확산 및 다양해지면서 데이터와 서비스 또는 전자화폐가 상호 연동되는 상호운용성 또는 상호 연동성 기술이 중요</p> <ul style="list-style-type: none"> - 미국 연방준비제도가사회는 최근 결제 시스템에 대한 논문을 발표하며 결제 시스템의 상호운용성에 대한 개요를 제공하고, 제시된 프레임워크를 CBDC와 스테이블코인에 적용 - EU EBSI(EU Blockchain Service Infrastructure)는 블록체인 기술을 활용하여 EU 국경 간 정보 공유 및 공공 서비스 혁신을 위한 기반 인프라로 활용되고 있으며 특히 국경을 초월한 공공 서비스 활용을 위해 상호운용성 보장 개방형 표준을 기반으로 함 - 캐나다 AION은 퍼블릭 프라이빗 블록체인 기관들이 AION을 통해 네트워크를 구성하는 것을 목표로 함 - 체인과 체인간의 SPOF(Single Point Of Failure) 발생을 방지하기 위해 블록체인 활용. SWIFT는 체인링크의 CCIP 프로토콜로 금융망과 체인 간을 연동. 씨티은행, 뉴욕멜론은행 등 다수 금융기관 참여하여 프라이빗과 퍼블릭 체인간의 연동 지원. <p>③ 블록체인 관리 및 개발지원 기술</p> <p>○ (시스템 구성 기술) 블록체인 시스템도 대부분 클라우드 기반으로 구축되고 있으며 시스템 구성에 따른 기능 및 기술 역시 클라우드에서 제공하는 도구 활용</p> <ul style="list-style-type: none"> - 중국의 BSN(Blockchain-Based Service Network)은 블록체인 서비스를 개발, 배포, 운영, 유지 관리하는데 필요한 클라우드, 포털, 플랫폼 및 개발 프레임워크를 하나의 포털 내에서 모두 처리할 수 있는 환경 제공. BSN은 크게 공공 도시 노드, 블록체인 프레임워크, BSN 포털로 구성 - EU의 EBSI는 노드 운영자들의 접근 용이 및 이용 편리성을 위해 EBSI Node Operator in Pilot Network Compliance Statement, Node Operators Operational Book, SLA를 제공. SLA 항목에는 복원력, 가용성 및 성능 요구사항에 대한 자세한 사양뿐만 아니라, 하드웨어, 운영 체제, 보안 시스템, 네트워크, 기본 소프트웨어 및 EBSI 특정 소프트웨어 포함 <p>○ (장애 분석·대응 기술) 블록체인의 장애는 네트워크, 노드, 스마트 컨트랙트 요소에서 발생하고 있으며 표준 프로세스와 스마트 컨트랙트 감사를 통해서 대응</p> <ul style="list-style-type: none"> - EU EBSI는 NOOB(Node Operators Operational Book)을 통해 표준 프로세스 및 최소한의 기술 요구사항을 제시함으로써 실행·성능에 관한 문제를 선제적 해결 - 스마트 컨트랙트의 신뢰성 확보를 위해 스마트 컨트랙트 감사(Audit) 시장도 확장되고 있음

구분	주요 동향
	<p>으며 스마트 컨트랙트 전문기업 서틱(Certik)은 정형 검증 및 수학적 방법을 통해 다양한 웹 3 프로젝트의 정확성 증명</p> <ul style="list-style-type: none"> o (성능 모니터링 기술) 개별 플랫폼들도 성능 및 상태 모니터링 기능을 제공하고 있지만 최근에는 BaaS를 기반으로 한 모니터링 기능 및 기술이 보편화 <ul style="list-style-type: none"> - 알케미(Alchemy)는 슈퍼노드 기능을 통해 개발환경을 구성하고 상태를 모니터링하며 급증하는 트래픽이 오류없이 처리되도록 지원 - EU EBSI(Europe Blockchain Service Infrastructure)는 SLA(서비스 수준 계약)을 통해 서비스 목표 달성과 분산 거버넌스 모델에 대한 네트워크 준수를 가능하게 함. SLA 포함 항목으로 탄력성, 가용성, 보안, 응답 지연 등 제시 o (블록체인 개발 지원 기술) 복잡한 인프라 구축, 웹 3, 스마트 컨트랙트, PKMS(Private Key Management Service), 각종 보안 이슈 등 블록체인 특유의 복잡한 서비스 개발 과정으로 인해 간편하고 편리한 개발 환경을 제공하는 BaaS가 크게 주목받고 있음 <ul style="list-style-type: none"> - BaaS는 제공하는 서비스 유형과 종류에 따라 크게 설치형 BaaS와 종합형 BaaS로 구분되며, 설치형 BaaS는 인프라 클라우드를 보유한 업체들이 주로 제공하고 있으며 종합형 BaaS는 블록체인 설치 및 운영뿐만 아니라 블록체인 서비스 개발에 필요한 부가기능과 개발 환경도 제공 - 중국의 BSN과 EU의 EBSI는 온라인 기반으로 편리하게 서비스 개발 및 배포·운영이 가능한 개발 지원 환경을 제공 - EU EBSI(Europe Blockchain Service Infrastructure)는 다양한 API를 제공하여 쉽게 기능을 수행할 수 있는 환경 제공 (8개의 API 제공, Authorization, DID Registry, Timestamp, Trusted Polices Registry, Conformance, Ledger, Trusted Issuers Registry, Trusted Schemas Registry) - 중국 BSN(Blockchain-based Service Network)은 3가지 구성요소(Public City Nodes, Blockchain Framework, BSN Portal)를 제공. Public City Nodes는 시스템 리소스를 제공하는 데이터 센터 공급자, Blockchain Framework는 다양한 블록체인 플랫폼(Consortium, Public) 지원, BSN Portal은 리소스 구매 뿐만 아니라 애플리케이션 게시 및 운영

□ 2026년 중점 기획방향

- (디지털트윈) 산업 전반의 디지털 전환을 가속화하고 미래 기술 기반의 성장 동력을 확보하는 자율 디지털트윈 핵심기술 개발
 - ▲모델/메타데이터 자동 생성 기술 등 구축자동화 기술, ▲거대 행동모델 기반 자율 운용기술 및 요소 재구성 기술 개발
- (블록체인) 블록체인과 AI 기술을 융합하여 AI 기술의 신뢰성 확보 및 AI 산업 활성화 지원 및 기존 블록체인 성능 및 안전성 강화 기술 개발
 - AI 데이터/모델의 투명성 문제를 해결하기 위한 AI 데이터 학습 검증 및 신뢰성 보장 기술 개발 추진
 - AI 데이터 주권보장 문제 해결을 위해, AI 데이터/모델의 ID체계 및 추적기술을 적용한 사용자 중심 AI 데이터/모델 주권 보장 기술 개발
 - 중앙화된 AI 인프라 문제를 해결하기 위한 경량 클라이언트 기반 탈중앙화 AI(DAI, Decentralized AI) 기술 개발
 - 블록체인 성능 문제를 해결하기 위한 QoT 보장 블록체인 기술 개발

□ 2026년 투자계획

(단위:백만원)

구분		'25년 예산	'26년 예산	비고
세부사업	내역사업			
AI기반 개방형 자율 디지털트윈 핵심기술 개발	AI기반 개방형 자율 디지털트윈 핵심기술 개발	-	6,600	-
AI·블록체인 융합 기반 자율형 고 신뢰 핵심기술 개발	AI·블록체인 융합 기반 자율형 고 신뢰 핵심기술 개발	-	4,985	

* '26년 예산은 신청금액으로, 추후 변경 가능