AI 에이전트 기술의 전자거래 산업 활용, 안정성 확보 및 제도 개선 방안

한국공학대학교 이영곤 교수

전자거래에서 활용되는 AI 에이전트의 정의와 범위

AI 에이전트(AI Agent)는 인공지능 기반 자율적으로 인식・판단・행동을 수행하는 소프트웨어 주체로서, 사용자의 명시적 개입 없이 거래・의사결정・콘텐츠 생성 등 다양한 업무를 자동 수행한다.

전자거래 산업에서는 AI 에이전트가 다음과 같은 기능적・산업적 범주로 확장되고 있다.

- 쇼핑 및 고객지원 에이전트
- 트레이딩 및 시장예측 에이전트
- 부정거래 탐지 및 신뢰 관리 에이전트
- 크리에이티브 및 생성형 에이전트
- 운영 및 거버넌스 보조 에이전트

전자거래에서 Web3와 AI 에이전트 활용 패턴

맞춤형 추천 + 소유권 기반 추천

AI는 고객의 구매・검색・행동 데이터를 분석하여 개인별로 선호할 가능성이 높은 상품을 추천하는 기술로, 고객 맞춤화(personalization)를 극대화하기 위해 사용된다.

Web3 환경에서는 고객이 보유한 NFT나 토큰화된 소유권 정보를 추천 알고리즘에 반영하여 “이 NFT를 가진 사용자는 이 상품에 관심이 있을 것”과 같은 맥락 기반 추천이 가능하다.

예를 들어 Adidas는 Bored Ape Yacht Club NFT 보유자에게 한정판 상품 접근권을 제공하여 NFT 기반 추천·혜택 시스템을 구현한다.

디지털 자산화(토큰화) + AI 기반 동적 가격/시장 예측

상품이나 서비스를 NFT·토큰 형태로 디지털 자산화(tokenization)하고, AI가 수요·희소성·거래 패턴을 분석하여 실시간으로 가격을 조정하는 동적 가격 책정(dynamic pricing) 기술이다.

시장의 변동성에 따라 "지금 수요가 급증하니 가격을 상향 조정" 또는 "이 시점에 한정 드롭 실시"와 같은 전략적 의사결정을 AI가 자동화한다. 예를 들어 Nike의 RTFKT 프로젝트는 한정판 디지털 스니커즈를 NFT로 발행하고, 수요 분석 기반의 실시간 가격 조정 기능을 실험하였다.

탈중앙 마켓플레이스 + AI 에이전트 거래

중앙 플랫폼이 아닌 스마트컨트랙트(smart contract)가 거래를 중개하는 탈중앙 마켓플레이스(Decentralized Marketplace)에서 AI 에이전트가 자동으로 상품 탐색, 가격 비교, 입찰 및 구매를 수행한다.

사용자는 AI 에이전트에게 조건만 설정하면 "가장 유리한 조건의 마켓에서 자동 구매"가 가능하며, 거래는 토큰 결제를 통해 즉시 완료된다. 예를 들어 OpenSea가 공개한 Web3 기반 마켓플레이스에서 MCP를 오픈했으며, AI 에이전트가 이를 활용해 자동 입찰, 최적가 탐색, NFT 포트폴리오 관리 등을 수행할 수 있다.

신원/소유권 검증 + AI 기반 부정거래 탐지

블록체인상의 거래 기록과 소유권 데이터를 활용하여 "누가 언제 어떤 자산을 소유했는가?"를 투명하게 검증하는 기술로, 위조나 가짜 소유권을 방지하기 위해 사용된다.

AI는 온체인 데이터의 이상 패턴을 학습하여 봇 거래, 사기 거래, 비정상적인 소유권 이전 등을 자동 감지함으로써 전자거래의 신뢰성을 강화한다. 예를 들어 NFT Marketplace에서 AI를 활용해 위조 이미지 NFT나 복제 토큰을 탐지하여 거래 차단하는 기능이 적용되고 있다.

- 사용자 데이터 마켓플레이스 + AI 모델 판매/재사용

개인이나 기업이 데이터를 NFT 또는 토큰으로 발행하여 거래하거나 공유하는 구조로, 데이터가 하나의 자산으로서 가치 교환의 대상이 된다.

AI는 해당 데이터를 학습하여 모델이나 서비스를 생성하고, 이를 다시 마켓플레이스에서 판매함으로써 데이터 제공자-모델 개발자-소비자 간 순환형 생태계를 형성한다. 예를 들어 Ocean Protocol은 사용자가 자신의 데이터를 안전하게 거래할 수 있도록 하는 Web3 기반 데이터 마켓플레이스를 운영한다.

- 옴니채널 경험 + 메타버스/웹3 통합 + AI 챗봇/버추얼 쇼핑 어시스턴트

메타버스, AR/VR, NFT 아이템 등을 활용해 물리적 매장과 디지털 공간을 통합한 옴니채널(Omnichannel) 경험을 제공하는 전자상거래 방식이다.

AI 챗봇 또는 버추얼 어시스턴트가 자연어로 고객 질문에 응답하고 실시간 상품 추천, 결제, 배송 안내까지 수행함으로써 몰입형 쇼핑 경험을 제공한다. 예를 들어 Gucci는 메타버스 내 버추얼 스토어에서 AI 기반 아바타 상담을 통해 고객 맞춤형 쇼핑 경험을 제공하였다.

AI 에이전트와 Web3 기반 전자거래 수행 시 기술적, 사회적 이슈

기술적 이슈 (Technical Issues)

신뢰성과 검증 가능성 부족은 AI 에이전트의 판단 과정이 블랙박스(비가시성)로 남아 의사결정 근거를 검증하기 어렵고, 스마트 컨트랙트와 상호작용 시 잘못된 파라미터 입력·오류 코드가 자산 손실로 직결될 위험이 존재한다.

상호운용성(Interoperability) 문제는 다양한 블록체인 네트워크, AI 모델, 데이터 표준 간 호환성 부재하며, AI 에이전트가 멀티 체인 환경에서 일관된 프로토콜을 인식·처리하기 어렵다.

보안 및 프라이버시 취약점은 지갑 키(private key) 탈취나 프롬프트 인젝션 공격을 통한 자율 에이전트 조작 위험이 존재하고, 온체인 공개 데이터와 AI 학습 데이터의 결합으로 개인정보 노출 가능성이 있다.

데이터 품질 및 위조 검증 문제는 Web3 환경에서는 신뢰할 수 있는 데이터 출처 검증이 어렵고, AI 학습용 데이터셋에 위조된 NFT·가짜 자산 정보가 포함될 수 있다.

스마트 컨트랙트 연계 취약성은 단일 체인 내에서 개별로 정상 동작하던 스마트 컨트랙트들이 연계(interaction)될 때 예상치 못한 상호작용(재진입, 상태 불일치, 파라미터 위·변조 등)이 발생하여 취약점이 드러나는 사례가 보고되고 있다.

사회적 이슈 (Social Issues)

사회적 신뢰 저하는 인간이 아닌 AI 에이전트가 거래·협상 주체로 등장하면서 책임 소재가 불명확할 수 있고, 오작동·오판에 따른 대중의 불신이 전체 Web3 생태계로 확산할 우려가 존재한다.

일자리 및 경제구조 변화는 자동화된 거래 에이전트 확산으로 브로커, 중개자, 리셀러 등의 역할이 축소되며, 윤리·투명성 문제는 AI가 차별적 데이터에 기반한 결정을 내릴 경우, 거래 상대방에게 불공정 결과를 초래할 수 있다.

사회적 남용 및 조작 위험은 자동 매수·매도 알고리즘을 통한 시장 교란(예: 가격 펌핑, 워시트레이드)과 자율 에이전트를 악용한 대규모 스캠·피싱 자동화 가능성이 존재한다.

법적 이슈 (Legal Issues)

법적 주체성 불명확은 AI 에이전트가 행한 거래의 법적 책임자가 누구인지 명시가 어렵다. 계약 유효성 및 증거력 문제는 AI 에이전트 간 체결된 스마트 컨트랙트가 법적으로 "유효한 계약의 의사 표시"로 인정될 수 있는지는 불분명하다.

소비자 보호 부재는 자동화된 거래에서 피해 발생 시 구제 절차나 책임 소재 불명확하며, 에이전트가 상대방의 의사결정을 오도하거나 기만할 경우 법적제재가 미비하다.

데이터 주권 및 개인정보 보호 위반 가능성은 AI 에이전트가 온체인·오프체인 데이터를 수집·분석하는 과정에서 GDPR, PIPA 등 개인정보 보호법을 위반할 소지가 존재한다.

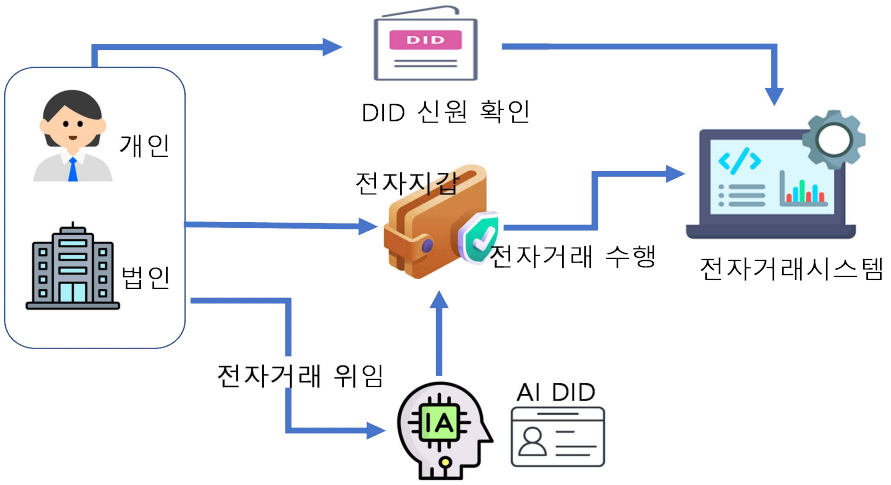
조세·금융 규제 불확실성은 에이전트가 수행한 디지털 자산 거래의 과세 기준, 보고 의무가 불명확하며, 탈중앙화된 거래소나 스마트컨트랙트에 대한 금융 감독의 관할 문제가 발생할 수 있다.

안정성 확보 및 제도개선 방안

법적 주체성(소유・책임 귀속)

자산 소유권은 '지갑 소유자(법인/자연인)' 로 명시: 에이전트는 법인격이 없으므로, 지갑의 법적 소유자(회사, DAO 법인 래퍼, 신탁 등)를 계약서/스마트컨트랙트 메타데이터에 식별자(DID)로 명기한다.

역할・권한 위임 구조 문서화: "에이전트=위임 실행자", "지갑 소유자=최종 책임자" 를 약관/온체인 정책에 명시한다. (한도・유효기간・취소권)



- 개인과 법인은 DID를 통해 신원증명
- 전자지갑 소유자에게 거래에 따른 책임 귀속
- AI 에이전트는 법적 추제가 될 수 없으므로 전자지갑 소유자의 위임을 받아 전자거래 실행 (자체 DID를 가지고 신원증명은 가능)

상호운용성 보장

AI 에이전트와 Web3 체계의 상호운용성은 표준 인터페이스(MCP 등) 를 중심으로 실현할 수 있다. 구체적으로는 스마트컨트랙트 호출・이벤트・오라클 응답에 대해 공통의 메시지・메타데이터 스키마(JSON-LD/ABI 기반)를 도입한다.

데이터 무결성과 신원 검증은 DID·VC 기반의 인증(authentication)과 서명된 메시지로 확보하며, 모든 트랜잭션에는 타임스탬프 및 nonce 값을 포함한다. 거버넌스·업그레이드·운영 정책(권한 범위·한도·모니터링) 메타데이터를 온체인에 명시해 운영·감사 가능성을 확보한다.

보안/오용 리스크(오작동·사기·손실)

스마트컨트랙트 보안 기본기 의무화로 OWASP Smart Contract Top10·SWC 기반 설계/퍼징/감사(듀얼감사 권장) 및 버그바운티를 상시화한다.

스마트 컨트랙스 작성 단계에서 최소권한 원칙, 명확한 인터페이스 규격 및 엄격한 입력 검증을 의무화하여 컨트랙트 간 불필요한 노출과 상태 불일치를 차단한다.

운영 세이프가드로 서킷브레이커, 일일 손실 캡, 슬리피지/가격 괴리 한도, 긴급 일시 정지(pause), 시뮬레이션 실행(pre-trade preview)을 계약에 내장한다.

지갑·권한 통제에선 트랜잭션 세션키/다중 승인·역할 분리, 위험 점수 기준 HITL(human-in-the-loop) 의무화—고액/고위험 거래는 사람 승인이 필수이다.

AI 모델 안전관리로 데이터 편향/프롬프트 주입/데이터 중독 테스트, 레드팀·사후 로그, 모델·프롬프트·지식소스 버전을 고정한다.

거버넌스(질서·감사·변경 관리)

AIMS 도입은 ISO/IEC 42001로 AI 경영시스템을 깔고, 위험·통제·감사·개선 사이클을 제도화(보드 레벨 책임자 지정)한다.

온체인 정책 거버넌스로 DAO형 의사결정에 쿼럼·위임 한도·타임락·비상 거부권을 설계하고, 파라미터(수수료·한도) 변경은 온체인 투명 로그로 감사한다.

신원·자격 연성 결합으로 참여자·에이전트·오라클 운영자에게 VC로 "누가 무엇을 할 권한이 있는지"를 최소 공개(Selective Disclosure)로 증명한다.

윤리(허위 행위·사회적 신뢰)

봇·에이전트 라벨링은 사람인 척 금지, 에이전트임을 UI·영수증·트랜잭션 메모에 명확하게 고지한다.(광고·스폰서 추천은 표기)

출처·진본성(프로비넌스)은 추천·결정의 데이터 출처·근거(요약)를 기록·열람 가능하게 하고, 모델·지식 업데이트 이력을 공개한다.

최소수집·영지식증명(ZK) 적용은 연령/거주·KYC 확인은 VC+ZK로 필요 사실만 증명한다.(전체 신원 노출 금지)

결론 및 시사점

법적 주체 명확화와 제도 정비 필요

AI 에이전트의 법적 행위능력은 현재 부재하므로, 지갑 소유자(법인·개인) 중심의 책임 구조를 명확히 해야 한다. DID(탈중앙 신원)·VC(검증 가능한 증명)를 통한 위임·소유권 명시 제도 마련 및 「전자상거래법」·「전자문서법」 등 기존 프레임워크에 스마트컨트랙트 법적 효력 명문화가 필요하다.

거래 안정성과 기술 신뢰 확보

Web3 거래는 코드 기반 자동 이행 구조이므로, 스마트컨트랙트 보안감사 의무화 및 취약점 공개제도 도입이 필요하다. AI 모델의 오작동·편향에 대응하기 위해 AI 안전성 검증·로그 관리 기준(NIST AI RMF, ISO/IEC 42001 등) 도입을 권장하며, DID 기반 인증·서명·결제 프로세스를 국내 전자결제(PG) 인프라와 연동하도록 기술 가이드라인 제정이 필요하다.

거버넌스와 감독 체계의 실질적 도입

DAO형 조직, 자동화 에이전트 등 탈중앙 주체에 대한 감독·감사 체계 마련이 필요하며, 서비스 제공자는 에이전트 운영 내역(트랜잭션·의사결정 로그)을 투명하게 공개하고 감사 가능성을 확보한다. 또한, 개인정보보호위원회·금융위원회 등 관련 부처 협업을 통한 “AI + Web3 거래 통합 가이드라인” 신설이 필요하다.

사회적 신뢰와 윤리적 설계 강화

AI 에이전트가 인간을 흉내 내거나 기만적으로 행동하지 않도록 에이전트 표시(Disclosure) 의무화가 필요하다. 데이터 수집·추천·거래 과정의 출처·근거(프로비넌스) 공개를 통해 투명성을 확보

하며, ZK-Proof 등 프라이버시 보호형 인증 기술을 활용해 이용자 신뢰 기반을 강화하고, 윤리적 사용 원칙(공정・책임・비차별)을 정책화해야 한다.

<참고 자료>

https://www.aboutamazon.com/news/retail/amazon-rufus

https://about.nike.com/en/newsroom/releases/nike-launches-swoosh-a-new-digital-community-and-experience

https://decrypt.co/137011/nike-unveils-first-swoosh-nft-collection-for-members

https://www.ledgerinsights.com/starbucks-web3-loyalty-nfts/

https://www.w3.org/TR/did-1.0/

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-a

https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

https://owasp.org/www-project-smart-contract-top-10/?utm_source=chatgpt.com

https://www.iso.org/standard/42001?utm_source=chatgpt.com

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm_source=chatgpt.com