2023년 11월 01주

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

KISA 한국인터넷진흥원

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

비탈릭 부테린, 이더리움의 다양한 레이어 2 환경 분석 공개

- 이더리움 창립자 부테린은 블로그 게시물에서 끊임없이 확장되는 레이어 2(L2) 생태계 복잡성에 대해 상세히 설명
- L2 프로젝트의 지속적인 이질성 증가 전망, 보안과 확장성 측면에 초점을 맞춘 솔루션 간의 장단점 등을 제시

이더리움 레이어2(L2)* 생태계는 지난 한 해 동안 전례없이 급격한 성장과 다양성을 경험하였으며, 개발자 및 사용자는 다양한 솔루션 및 애플리케이션의 장단점과 특성을 이해하고 적합한 L2의 연결 유형을 파악할 필요

* L2: 이더리움 메인넷(L1)의 확장성 문제를 해결하기 위해 설계된 별도의 레이어로 블록체인의 보안성과 데이터 가용성을 L1에 위탁하는 대신 빠르고 저렴하게 트랜잭션을 실행하는 것을 목표로 함

▶ 이더리움 L2 이니셔티브의 변화하는 환경..L2 프로젝트가 더욱 다양해지고, 이질성이 증가할 것으로 전망

- 이더리움 공동 창립자 비탈릭 부테린(Vitalik Buterin)은 자신의 웹사이트에 게시한 '다양한 유형의 레이어 2'라는 제목의 글*에서 이더리움 L2 솔루션**의 현 상태와 주요 개념에 관한 상세한 설명을 제공(10.31.)

  * Vitalik Buterin's website, 'Different types of layer 2s', 2023.10.31.

  ** L2 솔루션은 구조와 암호화 방식에 따라 크게 롤업(rollup), 밸리디움(validium), 플라즈마(plasma), 스테이트 채널(state channel), 사이드체인(sidechain) 등으로 구분

- 부테린은 먼저 아비트럼(Arbitrum), 옵티미즘(Optimism), 스크롤(Scroll), 카카롯(Kakarot), 타이코(Taiko)와 같은 주목할 만한 프로젝트를 통해 이더리움 가상 머신(EVM)* 롤업(Rollup)** 생태계가 빠르게 발전하고 있으며, 보안을 개선하는 데 큰 진전을 이루었음을 강조

  * Ethereum Virtual Machine(EVM): 이더리움 네트워크에서 스마트 컨트랙트를 실행하기 위한 가상 머신

  ** 롤업: 이더리움 L2에서 여러 개별적인 트랜잭션들을 처리하고 그 결과값들을 하나로 묶은 뒤 L1에 저장하는 기술

- 또한 폴리곤(Polygon)과 같은 사이드체인(sidechain)* 개발자들이 이제 롤업으로 전환하고 있으며, 셀로(Celo)에서와 같이 레이어 1(L1) 프로젝트가 밸리디움(validiums)**으로 전환하는 추세를 보여주고 있다고 지적

  * 사이드체인: 양방향 브릿지를 통해 메인넷에 연결된 별개의 블록체인을 의미. 별도의 합의 알고리즘, 블록 생성 규칙, 검증자 노드를 보유해 보안이 취약할 수 있다는 약점이 있음

  ** 밸리디움: 영지식 증명을 통해 이더리움의 확장성을 높인 L2 솔루션으로 zk롤업(zkRollup)과 거의 동일하나 오프체인 저장 방식을 사용하는 것에서 차이가 있음

- 이에 더해 '거의 EVM'과 같은 지케이싱크(Zksync), 아비트럼 스타일러스(Arbitrum Stylus)와 같은 확장 기능, 스타크넷(Starknet), 퓨얼(Fuel) 등의 광범위한 노력으로 '단지 EVM이 아닌' 생태계 영역도 존재한다고 언급

- 부테린은 이렇듯 L2 생태계 내에서 프로젝트 이질성이 증가하는 현상에 주목하고, 다음과 같은 몇 가지 이유를 들어 이러한 추세가 지속될 것으로 예측

- 첫째, 일부 독립적인 L1 프로젝트는 점차 이더리움 생태계에 적응하고 있으나 L2로의 너무 빠른 전환으로 사용성을 저하시키거나 또는 너무 늦은 전환으로 추진력을 잃지 않기 위해 단계적인 전환을 원할 가능성이 높음

- 둘째, 중앙화 프로젝트들은 보안을 강화하기 위해 블록체인 기반 솔루션을 찾고 있지만 현실적으로 탈중앙화와 성능 요구사항의 균형을 맞추는 '중간 정도 수준'의 탈중앙화만 필요로 할 것임

- 셋째, 게임이나 소셜 미디어와 같은 비금융 애플리케이션은 탈중앙화를 수용하고 있지만 '중간 정도 수준'의 보안만 필요로 할 수 있음

- 또한 사용자 간 감내할 수 있는 수수료 차이를 중요한 주제로 지적하며, 현재 이더리움 L1 사용자는 적당한 롤업 수수료를 감내할 수 있지만, 비 블록체인 영역에서 온 신규 사용자는 특히 수수료가 없는 환경에서 전환할 때 적은 수수료도 받아들이기 어려울 가능성이 높다고 강조

▶ 보안과 확장성 측면에 초점을 맞춘 이더리움 L2 솔루션(롤업, 밸리디움, 비연결 시스템) 장단점 분석

- 부테린은 각 시스템 중에 어떤 것이 특정 애플리케이션에 적합한지에 대해 파악할 때 보안(security)과 확장성(scale)의 상충되는 측면을 고려할 수 있다고 제안

- 이와 같은 보안과 확장성 차원은 'L1에서 발행된 자산을 L2로 옮겼다가 다시 L1으로 옮길 수 있다는 보장이 어느 정도인지'에 대해 질문함으로써 파악할 수 있다고 언급

[롤업, 밸리디움, 비연결 시스템 간 비교]

시스템 유형	기술 속성	보안 보증	비용
롤업 (Rollup)	• 사기 증명(fruad proofs)* 또는 L1에 저장된 데이터인 ZK-SNARK**을 통해 증명된 계산	• 언제든지 자산을 L1으로 가져올 수 있음	• L1 데이터 가용성 + 오류를 포착하기 위한 SNARK 증명 또는 이중화(redundant) 실행
밸리디움 (Validium)	• ZK-SNARK을 통해 증명된 계산(사기 증명은 사용 불가), 서버 또는 기타 별도 시스템에 저장된 데이터	• 데이터 가용성 장애로 인해 자산이 손실될 수는 있지만 도난당하지는 않음	• SNARK 증명
비연결 시스템 (Disconnected System)	• 벌도의 체인(또는 서버)	• 한명 또는 소규모 그룹이 자금을 훔치거나 열쇠를 분실하지 않도록 신뢰해야 함	• 매우 저렴

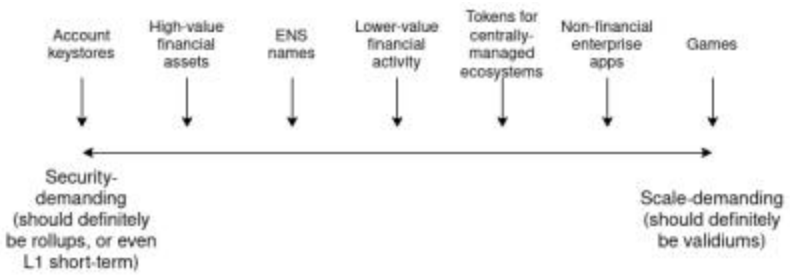
출처 : Vitalik Buterin's website, 'Different types of layer 2s', 2023.10.31.

* 사기 증명: 암호화 증명 방식으로 기본적으로 트랜잭션이 이상이 없다는 것을 전제로 별도의 검증 절차를 거치지 않지만 트랜잭션이 부정확하다는 것이 밝혀지면 기존 상태로 돌아가며 해당 트랜잭션에 대한 검증자를 처벌함

** ZK-SNARK: ZK 롤업의 유효성 검증 방식 중 하나로 SNARK는 증명이 간결하며, 증명 과정에서 증명하고자 하는 주체와 증명을 검증하는 주체 간 상호작용이 없고, 제시된 증명의 유효성 이외 검증 주체가 추가적인 정보를 얻지 못한다는 특징

- 한편 위와 같이 단순한 유형으로만 구분하지는 않으며 애플리케이션의 자체의 요구 사항에 따라 보안과 확장성 필요 정도가 달라지므로 스펙트럼 중간에 위치한 지점의 적절한 옵션을 선택할 수 있다고 제안

[애플리케이션 특성에 따른 보안과 확장성 요구]



출처 : Vitalik Buterin's website, 'Different types of layer 2s', 2023.10.31.

▶ **'이더리움과의 연결성' 관련 또 다른 주요 차원...신뢰없이 이더리움 읽기(Trsutlessly reading Ethereum)**

- 부테린은 매우 중요한 또 다른 연결 형태는 시스템이 이더리움 블록체인을 읽을 수 있는 능력과 관련이 있으며, 특히 이더리움 체인(L1)이 되돌아(revert) 가는 경우* 상위 체인(L2)을 되돌릴 수 있는 기능을 언급
  * 이와 같은 상황은 체인이 완성되지 않은 상태에서 일시적으로 발생하는 문제일 수도 있고, 너무 많은 검증자가 오프라인 상태이기 때문에 체인이 장기간 완성되지 않는 비활성 기간이기 때문일 수도 있음

- 그는 이더리움 체인이 되돌아가는 경우의 잠재적 위험을 해결하는 방법으로 ▲상위 체인이 이더리움의 확정된 블록만 읽을 수 있게 하거나 ▲이더리움이 되돌아가는 경우 상위 체인을 되돌릴 수 있게 하는 전략을 사용할 수 있다고 설명

- 첫 번째 전략의 경우 상위 체인이 이더리움의 확정된 블록만 읽을 수 있다면 체인을 되돌릴 필요가 없어지므로 문제가 해결된다고 함

- 하지만 예외적으로 이더리움에 대한 51% 공격*이 발생하여 호환되지 않는 두 개의 새로운 블록이 동시에 확정된 것처럼 보일 수 있는 상황에서 상위 체인이 잘못된 블록에 고정된다면 올바른 블록으로 전환하기 위해 되돌아가야 하지만, 이 경우에도 상위 체인을 하드포크하면 간단하게 처리할 수 있다고 설명
  * 51% 공격: 블록체인의 전체 노드 중 50%를 초과하는 해시 파워를 확보한 뒤 네트워크의 통제권을 갖고자 하는 공격

- 체인이 신뢰하지 않고* 이더리움을 읽을 수 있는 능력이 중요한 이유는 ▲이더리움(또는 다른 L2)에서 발행된 토큰을 해당 체인에 연결할 때 발생하는 보안 위험을 감소시키고 ▲계정 추상화(acount abstraction)** 지갑이 해당 체인에 자산을 안전하게 보관할 수 있게 해주기 때문이라고 함
  * 블록체인에서의 무신뢰성(turstless)은 서로를 신뢰할 필요 없이 알고리즘대로 실행되는 시스템을 의미
  ** 이더리움 계정 추상화: 외부 소유 계정(externally owned account)과 계약 계정(contract account)으로 구분되어 있는 기능을 통합시켜 트랜잭션 전송, 지갑 관리 등 계정의 다양하고 복잡한 동작을 단순화시키는 것

- 결론적으로 L2의 '이더리움과의 연결성(connectness to Ethereum)'에서 중요한 두 가지 차원으로 ▲(L2 자산을) 이더리움으로 인출할 때의 보안(security of withdrawing to Ethereum)과 ▲(L2의) 이더리움 읽기 보안(security of reading Ethereum)을 들 수 있다고 정리

- 그는 두가지 차원이 모두 중요하지만 고려해야 할 사항이 다르고, 두 경우 모두 정도의 스펙트럼이 존재한다고 지적

- 예를 들어 일부 애플리케이션은 높은 보안과 긴밀한 연결성이 중요하지만 다른 애플리케이션은 확장성을 높이기 위해 느슨한 수준의 보안이 허용되기도 하는데, 많은 경우 지금은 느슨한 연결로 시작하여 향후 10년 동안 기술이 발전함에 따라 더 긴밀한 연결로 이동하는 것이 최적일 수 있다는 의견을 제시

- 보안과 효율성을 강화하며 빠르게 진화하고 있는 이더리움의 L2 솔루션은 다양한 영역에서 각기 다른 목적의 달성을 위해 활용되며 프로젝트 별로 이질적인 형태를 띠면서 생태계를 확장
- 비탈릭 부테린은 L2 생태계의 포괄적 분석을 통해 보안과 확장성, 비용 등 다양한 솔루션 간 선택에 영향을 미칠 수 있는 측면들을 다뤄 정보에 입각한 결정을 내릴 수 있는 인사이트를 제공

[출처]

- Vitalik Buterin's website, 'Different types of layer 2s', 2023.10.31.
- Crypto.news, 'Vitalik Buterin publishes article discussing dimensions of connectedness to Ethereum', 2023.10.31.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[홍콩]

홍콩 금융관리국, 디지털 홍콩달러(e-HKD) 시범 프로그램 결과 발표

- 홍콩 금융관리국은 '22년 11월에 시작한 e-HKD 시범 프로그램의 1단계 종료 후 결과 보고서를 발간
- 시범 운영은 업계와 협력하여 e-HKD의 잠재적 사용 사례의 실행 가능성을 탐색하고 평가하기 위한 목적

홍콩은 '21년 e-HKD 프로젝트를 통해 소매 CBDC를 구현하기 위한 여정에 착수, '22년 1단계 시범 프로그램을 운영하며 6개 분야의 잠재적 용도를 탐색하였으나 도입 여부와 시기에 대해서는 아직 결정을 내리지 못함

▶ 금융, 결제, 기술 부문 16개 기업이 참여한 e-HKD 1단계 시범 프로그램의 주요 결과 및 평가를 제시

- 홍콩 금융관리국(Hong Kong Monetary Authority, 이하 HKMA)*은 '핀테크 2025' 전략**의 일환으로 CBDC를 위한 연구를 수행해 오고 있으며, '21년 'e-HKD 프로젝트'를 통해 소매용 CBDC 구현에 착수

  * 홍콩 금융관리국: 통화안정, 외환관리, 은행 건전성 감독 등을 목적으로 외환관리국과 은행감독국을 통합하여 설립된 정부 기관

  ** 핀테크 2025 전략: '21년 발표한 홍콩의 핀테크 육성 방안으로 핀테크 기술을 적용하여 모든 은행 업무의 디지털화 추진, 새로운 데이터 인프라 확충, CBDC 연구 강화 등을 주요 목표로 제시하고 있음

- e-HKD 프로젝트는 ▲(레일 1) 기반 계층(foundation layer) 개발 ▲(레일 2) 업계 시범 프로그램 및 반복적 개선(industry pilots & iterative enhancements) ▲(레일 3) 본격 출시(full launch)의 3레일 접근 방식을 취하고 있으며 이번에 종료된 e-HKD 시범 프로그램은 레일 2의 일환으로 수행된 1단계 프로그램에 해당

- 1단계 시범 프로그램은 HKMA와 16개 참여 기업이 협력하여 e-HKD의 잠재적 사용 사례의 상업적 실행 가능성을 탐색하기 위한 목적으로 약 1년 간 수행되었으며, 프로그램 종료 후 결과 보고서*를 발표

  * HKMA, 'e-HKD Pilot Programme – Phase 1 Report', 2023.10.

- 1단계에서는 본격적인 결제(full-fledged payments), 프로그래밍 가능한 결제(programmable payments), 오프라인 결제(offline payments), 토큰화 예금(tokenised deposits), 웹3 거래 결제(settlement of web3 transactions), 토큰화 자산 결제(settlement of tokenised assets) 등 6가지 범주의 소매 사용 사례에 중점

▶ 시범 프로그램의 참여 업체가 제안한 6가지 범주의 e-HKD 잠재적 사용 사례에 관한 검토

- **(참여 기업 및 사용 사례 선정)** 시범 프로그램에 선정된 기업은 총 16개로 6개 범주에 걸쳐 홍콩 국내 및 소매 사용 사례에 집중하는 총 14개의 시범 프로그램을 수행

- **(사례 1-본격적인 결제)** e-HKD는 새로운 형태의 중앙은행 화폐이자 '디지털 현금'에 가까운 것으로, 거래 비용이 거의 들지 않고 즉각적인 결제 완결성 등 실물 현금과 동일한 특성을 유지

- 또한 실물 현금 및 기타 전자 결제 수단과 유사한 방식으로 돈을 저장하고 이체할 수 있는 본격적인 결제 대안으로 사용될 수 있고, 전자 결제 중개자를 우회하여 비용과 시간 효율적 방식으로 결제를 처리

- 현재 판매자는 실시간 자금 수령 불가능 또는 잘못된 거래 발생 시 정산 오류 노출 문제를 가지고 있는데, 이는 결제 체인이 길고 카드 네트워크 및 유사한 솔루션에 대한 인터넷 결제 사용(예: 하루에 한 번 정산)으로 인해 발생하는 경우가 많음

- 참여 기업인 금융 그룹 HSBC는 거래 수준에서 즉각적인 최종 결제를 테스트하기 위해 프라이빗 블록체인 네트워크를 사용하여 소비자와 판매자 간에 가상의 e-HKD를 거래하는 시범 테스트를 진행

- 이 네트워크를 통해 소비자와 판매자 모두 중개자를 우회하여 더 빠르고 효율적인 결제 프로세스를 누릴 수 있을 뿐만 아니라 잠재적으로 거래 비용도 절감할 수 있음

- **(사례 2–프로그래밍 가능한 결제)** 스마트 컨트랙트 기능을 사용한 프로그래밍 가능한 결제는 소비자와 기업이 전자 계약에 직접 지침을 포함하여 사전 정의된 조건이 충족되면 결제를 시작할 수 있고, 해당 조건의 충족 여부에 대한 정보를 다방향으로 교환할 수 있게 됨

- **(소비자 보호 측면)** 홍콩의 소규모 판매자는 상품/서비스에 대해 현금 선불을 선호하는 경향이 있는데, 이는 소비자가 자금을 잃을 위험 및 판매자가 약속한 상품/서비스를 제공하지 않을 위험에 노출됨

- 이와 관련하여 프로그래밍 가능한 e-HKD는 소비자가 상품/서비스에 대해 단계적으로 결제하고 자금을 안전하게 보호할 수 있는 옵션을 제공할 수 있음

- 참여 기업인 중국건설은행(아시아)(China Construction Bank)과 중국은행(홍콩)(Bank of China)은 시범 운영을 통해 상품 또는 서비스 구매 용도의 소비자 선불금을 보관하기 위해 가상의 e-HKD를 사용하는 '소매 에스크로' 상품의 가능성을 탐색

- e-HKD를 사용하면 소비자가 자금을 선결제한 후 에스크로에 자금을 보관하고 조건이 충족된 경우에만 자동으로 사업자에게 대금을 지급할 수 있게 함

- 이를 통해 사업자는 아직 대금을 받지 못했지만 소비자가 대금을 지불했음을 확인할 수 있으므로 좋은 수준의 서비스를 유지하고 초기 소비자 신뢰를 구축할 수 있는 인센티브가 발생

- **(로열티 프로그램 및 타겟 지출 측면)** 프로그래밍 가능한 e-HKD는 소규모 판매자도 로열티 프로그램을 개선하고, 더 나은 소비자 인사이트를 확보함으로써 타겟 마케팅 지출을 강화할 수 있음

- 참여 기업인 항셍 은행(Hang Seng Bank), HSBC, 알리페이 홍콩(Alipay Financial Services)은 모든 규모의 판매자가 가상의 e-HKD로 로열티 프로그램을 구축, 실행할 수 있는 저비용 대안의 가능성을 탐색

- 스마트 컨트랙트를 사용하면 모든 규모의 판매자는 판매 시점에 자동으로 할인을 적용하는 옵션을 사용해 프로그램 관리를 위한 추가적 노력 없이도 소비자에게 할인 및 보상 프로그램을 제공할 수 있음

- 또한 금융기관에서 공통으로 사용되는 e-HKD를 통해 판매자는 결제 채널이나 금융기관에 관계없이 소비자를 보다 정확하고 비용 효율적으로 타겟팅할 수 있음

- **(투자 측면)** 프로그래밍 가능한 e-HKD를 사용하면 투자자는 투자 펀드에 가입할 때 더 빠른 처리 시간과 실시간 시장 가격에 더 가까운 가격을 누릴 수 있음

- 투자자는 일반적으로 펀드에 가입할 때 수표, 사전 펀딩, 주문 및 결제 등 여러 가지 과정을 완료해야 하며, 이 과정이 즉각적으로 수행되지 않음

- 참여 기업인 핀테크 기업 아르타-에말리(ARTA-Emali)는 가상의 e-HKD를 사용하여 펀드 주문의 원자 결제와 스마트 컨트랙트을 사용하여 운영 과정을 직관적인 방식으로 통합할 수 있는 기능을 탐색

- 이 과정에서 펀드 매니저는 투자자가 이미 주문을 선지급했다는 지식과 확신을 가지고 있기 때문에 위험에 덜 노출되며, 펀드 매니저는 시장가를 확보하고 주문을 최대한 빨리 체결하여 투자자의 자금을 수령하려는 인센티브가 있음

- 투자자는 주문을 더 빨리 체결하고 시장에 더 빨리 진입할 수 있어 토큰화 채권을 구매할 때와 같이 잠재적으로 하루의 이자 수입을 더 얻을 수 있음

- **(사례 3–오프라인 결제**) 전자 결제 수단을 통해 실시간으로 결제하는 대면 거래는 일반적으로 네트워크 연결이 요구되지만 홍콩의 높은 셀룰러 네트워크 보급률에도 불구하고 일부 상황에서 네트워크 연결이 간헐적으로 끊어지거나 또는 부족하면 실시간 검증에 의존하는 전자 결제 수단을 사용하지 못할 수 있음

- 참여 기업인 스탠다드차타드은행(Standard Chartered Bank)과 기세케+디브리언트(Giesecke+Devrient), 중국공상은행(아시아)(Industrial and Commercial Bank of China)은 오프라인과 온라인에서 소비자와 기업 간의 거래를 위해 물리적 및 전자적 매체를 통한 e-HKD의 저장과 거래 방식을 모색

- 가상의 e-HKD는 스마트폰 지갑과 실제 스마트 카드 내의 보안 요소를 사용하여 저장된 다음 이중 지출을 방지하는 안전장치와 함께 근거리 무선 통신(NFC)과 같은 기술을 사용하여 오프라인에서 거래할 수 있음

- 이러한 오프라인 거래는 최종적으로 정산되며 자금은 후속 오프라인 거래에서 즉시 사용할 수 있는데, 이는 거래가 일말에 조정되고 나중에 정산을 위해 상계되는 특정 결제 방식과 대조적

- **(사례 4-토큰화 예금)** 토큰화 예금은 일반적으로 은행에 예치된 돈이 해당 금융 기관의 대차대조표를 뒷받침하여 해당 기관의 자체 블록체인 원장에 발행되는 은행 예금의 디지털 표현을 지칭

- 예금자가 토큰화 예금을 다른 기관으로 이체할 때, 해당 기관은 가상적으로 HKMA 원장에 있는 수취인의 금융기관에 도매 CBDC를 사용해 은행 간 이체를 하는 동시에 자체 원장에 있는 토큰을 소각

- 참여 기업인 금융 그룹 비자(Visa)는 항셍은행 및 HSBC와 함께 토큰화 예금을 사용하여 다양한 비즈니스 시나리오에서 온어스(on-us)* 및 크로스체인 결제**의 원자성***과 상호 운용성을 시범적으로 조사
  * 온어스: 개시 금융기관과 수취 금융기관이 동일하고 은행 간 자금 이동이 없는 결제, 장부 이체라고도 함
  ** 크로스체인 결제: 서로 다른 블록체인 간 결제
  *** 결제의 원자성: 분산원장 기술을 기반으로 한 동시다발적이고 즉각적인 거래 결제

- 토큰화 예금이 가상의 도매 CBDC와 함께 사용되는 경우, 거래는 잠재적으로 24시간 내내 원자적인 방식으로 정산될 수 있음

- 이는 결제 시간과 담보 사용의 감소로 인해 거래 당사자의 유동성 관리를 개선하고, 거래 당사자가 실시간으로 거래 상태를 확인하고 후속 조치를 위해 보류 중인 거래를 식별할 수 있게 함으로써 전반적인 투명성 수준을 향상

- 분산원장기술(DLT)로 구축된 글로벌 환거래 네트워크를 사용하면 토큰화 예금을 단순한 결제 수단 이상으로 사용할 수 있고, 프로그래밍 가능한 토큰은 향후 금융 기관이 그룹 내 유동성 관리 및 회계와 같은 은행 내 사용 확대에도 유용하게 활용할 수 있음

- **(사례 5-웹3 거래 결제)** 웹3(Web3)는 탈중앙화, 토큰화, 블록체인 기반 플랫폼의 개념에 초점을 맞춘 차세대 인터넷의 가장 중요한 주제로서 이로 인해 디지털 자산과 관련된 새로운 유형의 거래가 등장

- e-HKD는 기존의 법정화폐 경제와 새로운 웹3 경제 사이의 가교 역할을 할 수 있으며, 탈중앙화 애플리케이션 및 블록체인 네트워크와의 통합을 지원해 웹3에서 보다 원활한 자금 조달 및 인출 지원

- 참여 기업인 마스터카드(Mastercard Asia/Pacific Ltd.)는 토큰화 자산 네트워크에서 실물 아이템 구매와 NFT의 교환을 시뮬레이션하고, 블록체인에서의 사용을 위해 e-HKD를 '랩핑(Wrapping)*'하는 방법을 탐색
  * 랩핑: 블록체인이 항상 상호 호환되는 것은 아니므로 다른 블록체인에서 사용할 수 있도록 토큰으로 변환하는 과정 의미

- '랩핑' 프로세스를 통해 e-HKD를 원래 플랫폼에서 벗어나 당사자가 원하는 해당 네트워크에서 안전하게 사용할 수 있고, 또한 스마트 컨트랙트를 사용하면 실물 상품의 성공적인 배송을 조건으로 결제가 이루어지도록 보장할 수 있음

- **(사례 6-토큰화 자산 결제)** 자산 소유자는 토큰화로 자산을 분할할 수 있으므로 한 명 이상의 구매자를 유치할 수 있으며, 잠재적 구매자는 각 자산의 세부 사항과 거래 내역을 잘 파악할 수 있어 안심

- 참여 기업인 푸본 은행(Fubon Bank)과 리플(Ripple)은 가상의 e-HKD를 사용하여 부동산 소유주에게 주택 담보 신용 한도를 부여하는 데 토큰화 부동산 자산을 사용하는 방법을 탐구

- 대출 프로토콜이 실행되면 부동산 담보권 토큰은 은행에서 주택담보대출을 발행할 때 담보로 사용되며, 인출을 위한 대출 금액은 소유주에게 e-HKD로 입금

- 토큰 담보 대출 모델은 대출 기관이 잠재적 부동산 소유주에게 보다 효율적인 서비스를 제공하여 추가적인 유동성을 확보할 수 있게 하고, 이는 다시 해당 시설의 이용을 촉진할 수 있음

▶ 시범 운영에 관한 평가..*e*-HKD의 고유한 가치 영역의 발견, 추후 주요 사용 사례에 대한 심층 분석 필요

- 이번 시범 프로그램을 통해 e-HKD로 소비자와 기업에 고유한 가치를 더하고 진화하는 미래의 수요를 해결할 수 있는 세 가지 핵심 영역으로 프로그래밍 가능성, 토큰화, 원자적 결제를 발견

- 다만, 시범 프로그램에서 e-HKD가 고유한 가치를 실현할 수 있었던 것은 참여자들의 준비와 생태계의 지원 조치와 같은 관련 전제 조건이 뒷받침되었기 때문에 가능했을 수 있다는 점에 유의해야 함

- 이러한 가치를 대규모로 실현할 가능성은 소매 결제 생태계의 관련 발전 속도에 따라 크게 달라질 수 있으며, 따라서 추가 조사가 필요

- 홍콩 행정부는 아직 CBDC의 도입 여부와 시기에 대한 정책 결정에 도달하지 않았고, 구현과 운영에 있어 정부와 업계가 취할 수 있는 역할에 대해 신중하게 고려해야 한다고 판단하고 있음

- 홍콩 금융관리국은 소매 CBDC 구현을 위한 프로젝트의 일환으로 홍콩 내 잠재적 사용 사례의 실행 가능성을 파악하고자 업계와 협력한 시범 프로그램을 운영하였으며, 최근 종료 결과를 발표
- 해당 프로그램에서는 6가지 범주의 다양한 e-HKD 의 결제 사례에 대해 살펴보았으며, 현재 생태계에 고유한 가치를 더할 수 있는 세가지 영역으로 프로그래밍 가능성, 토큰화, 원자적 결제를 강조

[출처]

- HKMA, 'e-HKD Pilot Programme – Phase 1 Report', 2023.10.
- Cryptoslate, 'Future of CBDCs in Hong Kong uncertain as pilot program concludes', 2023.10.30.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[홍콩]

홍콩, 토큰화를 새로운 규제 요건으로 채택할 예정

- 홍콩 금융 규제 당국은 웹3 시장 성장에 대한 정부의 의지를 강조하며, 토큰화 부문에 관한 계획을 언급
- 토큰화 부문 이외 가상자산의 송금 범위 확대, 스테이블코인 발행자 규제에도 집중하고 있음을 밝힘

올해 6월부터 암호자산 거래소에 대한 새로운 규제를 시작한 홍콩은 아시아의 웹3 허브를 구축하기 위한 노력을 지속하며 암호자산 규제 작업의 방향을 거래소를 넘어선 토큰화, 스테이블코인 등으로 확대할 계획

▶ 홍콩 규제 당국, 토큰화 기술의 위험 식별 및 토큰화 증권 중개인을 위한 안내 문서 발행 계획

- 홍콩의 금융 관계자들은 10월 30일부터 11월 5일까지 개최되는 홍콩 핀테크 위크 행사에서 규제 당국이 곧 토큰화에 관한 새로운 정부 회람 문서를 발행할 수 있다고 언급(11.01.)

- 홍콩은 아시아의 웹 3.0 허브가 되기 위한 노력을 계속하면서 토큰화 자산, 스테이블 코인, 암호자산 거래에 관한 더 많은 정책 문서와 회람을 발행할 것으로 예상

- 홍콩 금융서비스 및 재무국(Financial Services and the Treasury Bureau)* 크리스토퍼 후이(Christopher Hui) 국장은 핀테크 위크 행사에서 정부는 웹3 혁신을 계속 장려하고 있으며, 최근 JPEX 암호자산 거래소 사태**가 이러한 의지를 훼손하지 않았다고 언급
  * 금융 서비스 및 재무국: 홍콩의 15개 정책국 중 하나로, 재정 및 재무에 관한 정부 정책을 개발하고 실행
  ** JPEX는 홍콩 가상자산 라이선스를 가지고 있다고 거짓으로 홍보하며 운영하다 올해 9월 규제 당국에 사기 혐의로 고발

- 후이 국장은 홍콩증권선물위원회(Securities and Futures Commission, SFC)*가 곧 토큰화 증권 관련 활동 및 SFC가 승인한 투자 상품의 토큰화에 관여하는 중개업체에 대한 안내문을 발표할 예정이라고 덧붙임
  * 홍콩증권선물위원회: 증권, 선물 관련 홍보, 투자자 보호, 금융 범죄 예방 등을 목적으로 설립된 독립 법정기구

- 또한 규제 당국이 집중하고 있는 또 다른 분야는 거래 플랫폼에서 발생하는 거래를 넘어 가상자산의 매매까지 송금 범위를 확대하는 방안을 모색하는 것이라고 함

- 한편, 곧 홍콩 금융관리국(HKMA)과 스테이블코인 발행자에 대한 규제 체제에 대한 공동 협의를 발표할 예정이라고 밝힘

- 올해 9월 무허가 거래소 JPEX 사건으로 인한 피해액이 14억 3,000만 홍콩 달러에 달하며 홍콩 역사상 최대 금융 사기 사건으로 지목된 이래 업계는 규제당국의 거래소 규제가 강화될 것이라고 전망
- 금융서비스 및 재무국 국장은 JPEX 사건에도 불구하고 웹3에 대한 정부의 의지는 여전히 강하다고 강조하며 거래소를 넘어선 토큰화, 스테이블코인, 수탁 지갑 등으로 규제를 확대해 나갈 것이라 언급

[출처]

- The Block, 'Hong Kong plans to target tokenization with new regulatory requirements, officials say', 2023.11.01.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[EU]

EU, MiCA 규제에 따라 내년 디파이(DeFi) 평가 보고서 발행 예정

- EU 집행위원회가 MiCA에 따라 내년에 디파이의 장단점을 평가하는 세부 보고서 작성을 수행할 예정
- 향후 위험성 확인 후 법안을 제안할 수 있으나 현재 EU의 디파이 프로토콜에 직접적인 영향은 거의 없음

MiCA의 원래 의도는 암호화폐와 법정화폐를 연결하는 통로인 스테이블코인과 중앙화 거래소에 관한 포괄적인 규정을 만드는 것이었으며, EU 정책 입안자들은 디파이와 NFT에 대해서 시장이 좀 더 진화해야 한다고 판단

▶ 시장 초기 과도한 규제 방지 의도...한편 디파이를 MiCA에서 제외할 경우 발생할 수 있는 위험 인식 필요

- 컨설팅 업체 BCAS에 따르면 디파이 프로토콜은 EU MiCA의 적용 범위에서 제외되는 것으로 해석되지만 '완전히 탈중앙화'한 경우, 즉 어떤 개인이나 회사도 사용 중인 플랫폼을 통제하지 않는 경우에만 해당

- 혁신을 위한 암호자산 협의회(Crypto Council for Innovation)*의 EU 정책 책임자인 마크 포스터(Mark Foster)는 EU 집행위원회가 내년에 디파이의 장단점을 평가하는 세부 보고서 작성을 위임받을 것이라고 언급하였으며, 이는 EU에서 디파이의 다음 단계가 무엇인지 결정하는 데 도움이 될 것으로 보임
  * 혁신을 위한 암호자산 협의회(CCI): 미국 워싱턴에 기반을 둔 암호자산 업계 리더로 구성된 로비 그룹

- 포스터는 '만약 위험성이 확인된다면, EU가 다음 의회에서 디파이에 관한 법안을 제안할 수 있을 것'이라고 말했으나, 현재로서는 EU 내에서 디파이 프로토콜에 직접적인 영향은 거의 없다고 판단됨

- 이는 EU 정책 입안자들이 규제 방식을 결정하기 전에 시장이 진화하고 더 많이 이해되기를 바라면서 내린 정치적 결정이었으며, 디파이와 NFT는 시장 규모가 아직 작아 MiCA 규제의 우선 순위가 되지 못함

- 디지털 자산 관련 업체 키록(Keyrock)의 CEO인 케빈 드 파툴(Kevin de Patoul)은 MiCA에 대한 EU의 신중한 접근 방식이 상당한 이점을 가져다준다고 강조하며, 너무 일찍 과도하게 규제하여 혁신을 죽이는 것보다는 프레임워크에 잠재적인 공백을 두는 것이 더 바람직하다고 언급

- 하지만 파툴은 디파이를 MiCA에서 제외할 경우 '감독 공백, 소비자 보호, 위험 관리' 등에서 위험이 발생할 수 있다고 지적

- 이와 같은 위험을 완화하기 위해서는 디지털 자산 서비스 제공 업체가 사전에 높은 기준과 투명한 관행을 유지하는 것이 필수적이며, 모범 사례에 기반한 자율규제(self-regulation)가 매우 중요하다고 강조

- 현재로서는 디파이가 MiCA의 범위에서 벗어나 있으며, 내년 유럽위원회가 디파이 분야에 대한 세부 보고서를 작성하면 의회 의원들이 새로운 법안을 발의할 수 있는 기회가 발생할 것으로 보임
- 디파이가 규제 대상에 포함되지 않은 것은 정책 입안자들이 아직 규제 시기가 아니라고 판단하고 내린 의도적인 결정이지만 소비자 보호 등에서 위험이 발생할 가능성을 염두에 둘 필요성이 있다고 지적됨

[출처]

- Blockworks, 'EU's MiCA regulation defers decisions on DeFi', 2023.11.01.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

다자간 계산(MPC) 기술이 블록체인 혁신에 미치는 영향

- 최근 영지식 증명과 함께 블록체인에서의 개인정보 보호 문제를 해결하는 기술로 '다자간 계산'을 주목
- 다자간 계산은 여러 이해관계자가 관련된 상황에서 개인정보를 노출하지 않고도 협업을 가능케 함

블록체인이 성장함에 따라 투명성과 개인정보 보호 사이의 균형을 맞추기 위한 해결책으로 등장한 새로운 기술로 다자간 계산(Multiparty Computation)*이 주목받고 있으며 다양한 응용 분야 애플리케이션 개발 기대

* 다자간 계산: 서로 신뢰하지 않는 다수가 각자의 입력 값을 공유하지 않고, 암호화된 입력 값의 계산 결과를 출력하는 기술

▶ 영지식 증명과 더불어 블록체인에서 개인정보를 노출하지 않는 기술...여러 이해관계자의 협업에 강점

- 코인텔레그래프(cointelegraph)의 정보공유 커뮤니티 이노베이션 서클(innovation circle)은 영지식 증명(zero-knowledge proof)과 함께 블록체인에서의 개인정보 보호 문제에 관한 해결책으로 주목받는 '다자간 계산(MPC)'과 관련한 분석 기사를 게재*

  * Cointelegraph, 'Multiparty computation (MPC): Its effects on blockchain innovation', 2023.11.01.

- 블록체인이 성장함에 따라 개인정보 보호에 대한 필요성이 커지고 있는 가운데 영지식 증명은 비밀을 공개하지 않고 지식을 증명할 수 있는 기술로, 투명한 시스템에서 트랜잭션 개인정보 보호를 보장하는데 탁월하지만 대규모 네트워크에서는 리소스를 많이 차지할 수 있다는 한계가 존재

- 한편 다자간 계산은 협업에 관한 것으로, 여러 그룹이 각자의 퍼즐 조각을 보여주지 않고 함께 퍼즐을 맞추는 것과 같은 개념으로 설명할 수 있음

- 다자간 계산은 효율적이고 확장성이 뛰어나며 특정 사용 사례에서 영지식 증명보다 더 간소화할 수 있다는 장점이 존재

- 두 기술은 경쟁 관계라기보다는 영지식 증명이 방어를 강화하는 반면, 다자간 계산은 경계를 허물고 혁신을 통해 경쟁 우위를 제공한다는 점에서 다른 특징을 가짐

- 다자간 계산은 블록체인에서 단순히 데이터를 숨기는 것이 아니라 데이터를 노출하지 않고도 연산을 수행하고 협업이 가능하며, 특히 여러 이해관계자가 관련된 경우에서 효율성이 차별화됨

- 다자간 계산 기술이 블록체인에 통합되면 비밀 경매, 비밀 투표와 설문조사, 협업 머신러닝 모델 트레이닝 등 다양한 사례에 활용될 수 있고, 협업과 개인정보 보호가 상충되는 것이 아닌 동반자가 되는 환경을 조성 가능

- 업계가 규제 및 소비자 신뢰 측면에서 데이터 개인정보 보호의 중요성에 대해 인식함에 따라 관련 위험 없이 공유 데이터의 이점을 활용하는 다자간 계산과 같은 기술이 잠재적 해결책으로 부상
- 다자간 계산은 개인정보의 노출 없이 협업하는 그룹을 가능케 하며, 블록체인과 통합함으로써 매우 다양한 응용 애플리케이션으로 발전 가능하다는 점에서 혁신 잠재력을 보유

[출처]

- Cointelegraph, 'Multiparty computation (MPC): Its effects on blockchain innovation', 2023.11.01.

2023년 11월 02주

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

KISA 한국인터넷진흥원

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

블록체인 기반 신원으로 디파이(DeFi)의 신뢰 문제 해결

- 기관은 디파이에 관심이 높지만 거래 상대방 신원 확인에 관한 신뢰 부족으로 도입을 주저하는 상황
- 이에 대한 해결책으로 블록체인 기반으로 신원을 증명하는 블록체인 ID 프레임워크 도입이 제안됨

지난 몇 년간 디파이에 대한 지속적인 관심에도 불구하고, 기관들은 디파이 거래 시 블록체인의 익명성 원칙으로 상대방의 신원을 확인할 수 없다는 점에 대해 우려가 커 디파이 분야 진입을 주저하고 있는 상황

▶ 기관의 디파이에 관한 신뢰 우려 문제...블록체인 기반 신원 증명을 활용함으로써 해결

- 기관들이 여전히 디파이에 뛰어들기를 다소 주저하고 있는 가장 큰 원인 중 하나는 포괄적이고 명확한 규제가 없다는 것이지만, 규제는 신뢰 부족이라는 더 큰 문제 중 일부에 불과

- 최근 언스트 앤 영(Ernst & Young)의 보고서*에 따르면, 기관의 88%가 규제 불확실성을 디파이 분야 진입 시 가장 우려하는 점 중 하나로 꼽았으며, 그 다음으로 87%가 입증되고 신뢰할 수 있는 금융기관의 부족을 꼽음**

  * Ernst & Young LLP, 'Staying the course: institutional Investor sentiment toward blockchain and digital assets', 2023.04.

  ** 해당 설문조사는 '23년 2월 초 글로벌 256명의 기관 투자 의사결정권자를 대상으로 실시되었으며, 디지털 자산 및 관련 상품에 투자한 기업과 아직 투자하지 않은 기업이 모두 포함되었음

- 기관이 디파이에서 경험하는 신뢰와 관련된 문제 일부는 디파이 부문에 참여하는 사용자의 개인정보 보호를 보장하는 블록체인의 익명성과 관련이 있음

- 익명성은 블록체인의 기본 원칙이지만, 거래 상대방의 신원을 확인할 수 없고 결국 신뢰하지 못하는 기관의 저항을 불러일으키게 됨

- 기관과 고객의 자금이 모두 위험에 처해 있는 상황에서 거래 상대방이 진짜 당사자라는 확신이 없다면 기관이 블록체인을 완전히 수용하기를 기대하는 것은 불가능

- 따라서 기관이 블록체인을 도입하려면 안전하고 투명한 프라이빗 프레임워크를 제공하는 동시에 모든 참여자에게 일정한 책임 기준을 적용해야 함

- 규제 명확성은 신뢰와 책임성을 확립하는 데 있어 중요한 부분이며, 아직 부족하기는 하지만 관리 기관을 대신해 더 강력한 규제를 도입하는 것이 분명한 해결책이 될 수 있음

- 이제 남은 문제인 디파이에 신뢰를 도입하는 문제의 해결책으로 블록체인 기반으로 신원을 증명하는 방법을 활용할 수 있음

- 블록체인 ID 프레임워크는 신원 도용이나 사기의 위험을 줄임으로써 최적의 개인 정보 보호, 사이버 보안 및 고객 알기 규정(Know Your Customer, KYC) 준수를 보장

- 이는 모든 주체가 불필요하거나 사적인 정보를 공개할 필요 없이 상대방이 누구와 상호작용하는지 정확히 알 수 있다는 의미

- 이를 통해 모든 거래에 안전성과 투명성이 강화됨으로써 신뢰가 절실히 필요한 업계에서 신뢰를 강화할 수 있음

- 금융 세계는 사용자와 기업 간의 자본 관리와 흐름을 포함하므로, 거래 상대방이 자신이 주장하는 사용자인지 확인할 수 있는 것이 매우 중요하며, 그렇지 않으면 자금이 엉뚱한 사람에게 흘러 들어가 잠재적으로 큰 금전적 손실을 초래할 위험이 존재

- 따라서 업계가 사기 행위로부터 자금을 보호하고 개인정보가 유지될 것이라는 확신을 주지 못한다면 기관 투자자들이 디파이에 참여하는 데 의욕을 보이지 않는 것은 당연한 결과

- 블록체인 업계는 과거와 현재를 막론하고 신원 사칭과 관련된 사기가 만연해 있고, 한 예로 지난 10월, 한 웹3.0 게임 프로젝트에서 배우를 고용해 경영진인 것처럼 행세하며 160만 달러의 자금을 훔쳐 달아난 사건*을 들 수 있음

  * '23년 10월 게임 프로젝트 핀소울(FinSoul) 팀이 유급 배우를 고용해 경영진인 것처럼 속여 게임 플랫폼 개발을 목적으로 자금을 모집했으나 플랫폼 개발 대신 투자받은 160만 달러의 테더를 자신들에게 이체하고 자금을 세탁

- 이와 같은 사건은 신원 확인의 오용과 부재로 인한 위험성을 보여주는 대표적인 예시로서, 접근할 수 있고 신뢰할 수 있는 신원 확인 도구를 사용하면 이와 같은 사기 및 사기를 예방할 수 있음

- 기관은 모든 거래가 철저하게 검증되고 비공개적이며 투명하다는 것을 확신할 수 있을 뿐만 아니라, 고객과 파트너에게 이러한 확신을 제공하여 자체 네트워크 내에서 신뢰와 믿음을 구축할 수 있음

- 기관은 평판을 유지해야 하고 고객을 만족시켜야 하므로 고객을 안심시킬 수 없다면 사기가 난무하는 공간에 쉽게 진입할 수 없음

▶ 개인정보를 보호하면서 규정을 준수하는데 도움이 되는 영지식 증명 활용 블록체인 기반 ID

- 블록체인이 사용자에게 완전한 익명성을 제공할 수 있다고 선전되어 온 만큼, 디파이 업계에서는 신원 확인이 개인정보를 침해할 수 있다는 우려로 인해 신원 확인이 논쟁의 대상이었음

- 디파이가 금융 시스템을 더 나은 방향으로 재편할 수 있는 잠재력을 실현하기 위해서는 개인정보를 보호하는 디지털 신원 확인 방법을 활용해야 함

- 영지식 증명 기술은 증명을 제공하는 데 필요한 정보를 공개하지 않고도 한 당사자의 진술이 사실임을 증명할 수 있는 기술로서, 디파이가 안고 있는 신원 확인 문제를 해결할 구원투수로 부상

- 참여자는 민감한 정보를 실제로 제공하지 않고도 자신이 누구인지 증명할 수 있으므로 이를 통해 기관은 상대방에게 실제로 접근할 필요가 없는 민감한 정보를 공개하도록 요청하지 않고도 고객 알기 규정(KYC) 준수 요건을 충족

- 따라서 영지식 증명 기반 디지털 신원 솔루션은 기관이 디파이에 참여하는 데 필요한 신뢰와 확신을 제공할 뿐만 아니라, 엄격하게 높은 수준의 보안과 최소한의 위험으로 규제 요건을 충족할 수 있게 함

[영지식 증명 사례]

* 증명자(Prover)인 고객(Client)은 영지식 증명을 통해 자신의 은행 계좌에 10만 달러 이상의 금액이 있다는 것을 검증자(Verifier)인 투자 중개인(Investment Broker)에게 증명할 수 있으며, 이 과정에서 자신이 보유한 정확한 금액을 밝히지 않아도 됨

출처 : Horizon Academy Homepage, https://www.horizen.io/academy/zero-knowledge-proofs-zkp/#defi-kyc.

▶ 기업의 탈중앙화 ID 프레임워크와 디파이 도입...개별 비즈니스 모델에 맞는 기술 적용과 지원 노력 필요

- 블록체인 기반 신원 확인이 디파이에 대한 기관의 신뢰에 미치는 영향에 대해 논의하는 것과 이를 실행하는 것은 별개의 문제로 볼 수 있음
- 디파이 참여자는 ID 확인 레이어가 내장된 레이어 1(L1) 프로토콜을 구축하거나 개인정보 보호를 위한 확인 도구를 통합하여 프레임워크를 발전시키고, 제품에 접목해야 함
- 디파이에 관심을 갖고 있는 기관은 이 기술이 특정 비즈니스 모델에 직접적으로 어떻게 도움이 될 수 있는지 이해하려고 노력해야 하며, 온보딩 프로세스 전반에 걸쳐 지원이 필요할 수 있다는 점을 고려해야 함
- 일률적인 솔루션을 버리고 각 기관에 맞는 맞춤형 솔루션을 제공함으로써 기업은 디파이 채택을 더욱 촉진할 수 있음
- 물론 기관이 디파이 영역에 안전하게 진입할 수 있을 것이라는 믿음을 줄 수 있는 가장 중요한 부분은 강력한 신원 확인임
- 디파이는 금융의 새로운 시대를 열며 금융 세계에 더 큰 효율성과 투명성을 가져다주고 있으나 개인정보를 보호하는 디지털 인증 프레임워크를 통해 보안과 책임성을 우선시하지 않으면 그 잠재력을 충분히 발휘할 수 없음

- 신뢰 구축이 특히 중요한 금융 기업은 신원 확인의 오용과 부재로 인한 위험이 실재하는 블록체인 업계에 진입하는 것을 주저하고 있으며, 이에 대한 해결책으로 블록체인 기반 신원 증명 방식이 제안
- 블록체인 ID 프레임워크는 개인정보 보호, 사이버 보안 및 KYC 규정 준수를 보장하며, 모든 거래에 안전성과 투명성이 강화되어 업계에서 신뢰를 강화할 수 있어 기업의 디파이 도입 촉진에 큰 역할

[출처]

- Nasdaq, 'Solving DeFi's Trust Issues: Addressing the Anonymous Elephant With Blockchain-Based Identity', 2023.11.07.
- Horizon Academy Homepage, 'https://www.horizen.io/academy/zero-knowledge-proofs-zkp/#defi-kyc'.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

블록체인의 확장성: 레이어 1(L1)과 레이어 2(L2)의 비교

- 블록체인 네트워크가 성장하면서 증가하는 트랜잭션을 효율적으로 처리해야 하는 확장성 문제에 직면
- 탈중앙화, 보안, 확장성 간 상충 관계 속에서 확장성을 개선하고자 하는 다양한 기술적 노력이 지속

블록체인 분야는 이제 막 시작하는 단계로서 새로운 기술의 발전으로 당면 문제들이 다양한 방식으로 해결책을 찾아가고 있는 가운데, 현재의 환경과 미래 발전 방향에 대한 통찰력 있는 분석과 이해가 요구됨

▶ 지속해서 진화하고 있는 블록체인 분야...다양한 디파이(DeFi) 프로토콜 환경에 대한 분석과 이해 필요

- 코인텔레그래프 리서치(Cointelegraph Research)는 블록체인의 확장성 관점에서 최근 디파이 생태계의 레이어 1(L1)과 레이어 2(L2) 솔루션에 대한 포괄적인 분석을 제공하는 보고서*를 발표
  * Cointelegraph Research, 'Layer 1 vs. Layer 2: The blockchain scalability showdown', 2023.11.06.

- 탈중앙화 디지털 통화의 기본 틀을 마련한 비트코인에서 비롯된 암호화폐의 진화는 스마트 컨트랙트를 도입하여 더 복잡하고 프로그래밍이 가능한 거래를 가능하게 한 이더리움을 통해 큰 도약을 이룸

- 한편 탈중앙화 원장 기술의 진화는 이것으로 끝나지 않고, 확장성에 대한 필요성이 커지면서 새로운 L1 솔루션과 L2 솔루션, 크로스체인 간 통신을 촉진하는 멀티체인 접근 방식 등 다양한 대안이 등장

- 새로운 블록체인 네트워크가 폭발적으로 증가하고 있는 가운데 끊임없는 개발 속도를 따라잡기가 어려울 수 있지만 다양한 프로토콜에서 개발 중인 기술을 이해하는 것이 중요

▶ 블록체인의 확장성 트릴레마(trilemma) 문제

- 비트코인은 최초의 현대적 암호화폐로, '09년에 '블록체인 혁명'을 일으키며 암호화, P2P 거래소, 탈중앙화 원장 기술, 블록체인의 발전을 결합

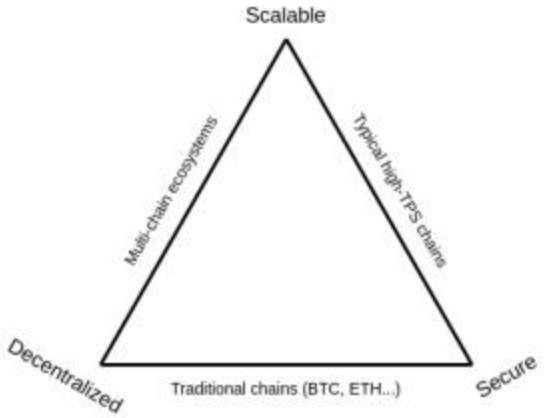
- 이후 비탈릭 부테린(Vitalik Buterin)이 이더리움을 공동 개발하면서 스마트 컨트랙트를 개발할 수 있었지만, 디지털 화폐가 기존 카드 거래와 경쟁할 수 있는 확장성은 여전히 부족*
  * 비자(Visa) 카드의 이론적 한계는 20,000TPS(초당 트랜잭션 수) 이상이지만 이더리움의 한계는 약 45TPS

- 탈중앙화 원장 프로토콜의 중요한 관심사인 확장성은 많은 수의 트랜잭션을 처리할 수 있는 능력을 의미하는데 블록체인이 처리해야 하는 트랜잭션의 양은 애플리케이션마다 다름

- 예를 들어, 빈도가 높은 거래, 공급망 유통, 게임 경제는 관련 네트워크에 높은 트랜잭션을 발생시키고, 낮은 수수료 환경이 필요하지만 블록체인 시스템의 바람직한 특성을 유지하면서 모두를 달성하는 것은 현실적으로 어려운 문제

- 이와 같은 문제는 블록체인 시스템 설계 시 ▲확장성 ▲보안 ▲탈중앙화라는 세 가지 특성 중 두 가지에 대해서만 최적화할 수 있음*을 의미하는 블록체인의 트릴레마(trilemma)가 존재함으로 인해 발생
  * 분산 처리를 위한 데이터베이스 샤딩(sharding)이나 기타 고급 기술을 사용하지 않고 단순한 네트워크를 설계할 때 해당

[블록체인의 확장성 트릴레마(trilemma)]



- 이더리움과 비트코인은 모두 탈중앙화되고 안전하지만 확장성이 부족하다는 단점이 존재하여 트릴레마의 삼각형 아래쪽 위치
- 반면에 확장성을 위해 탈중앙화를 희생하면 초당 수천 건의 트랜잭션을 처리하는 네트워크가 탄생하게 되지만 많은 트랜잭션을 처리하면 노드에 높은 하드웨어와 대역폭이 필요하게 되고, 이는 운영자 수 감소와 중앙 집중화로 이어짐
- 멀티체인 생태계는 크로스체인 통신 프로토콜을 통해 상호 운용이 가능한 여러 체인으로 트랜잭션 처리량을 분할하여 확장성 문제를 해결하고, 탈중앙화를 꾀할 수 있지만 보안성이 떨어진다는 문제

출처 : (왼쪽 그림) Vitalik Buterin's Homepage, 'Why sharding is great: demystifying the technical properties', 2021.04.07.
(오른쪽 설명) Cointelegraph Research, 'Layer 1 vs. Layer 2: The blockchain scalability showdown', 2023.11.06.

▶ 확장성 문제를 해결하기 위한 다양한 레이어별 노력

- 프로토콜마다 확장성, 상호운용성, 개인정보 보호에 대한 다양한 해결책을 찾아내고 있는데, 일부 프로토콜은 L1으로서 이러한 문제에 대해 자체 기본 레이어 내에서 솔루션을 제공하고, 다른 프로토콜은 확장성을 높이기 위해 서로 다른 프로토콜을 연결하고자 하는 L0 또는 L2 솔루션을 구축

[다양한 레이어: L0, L1, L2]

Layer 0 (L0)*	Layer 1 (L1)	Layer 2 (L2)
L0 프로토콜 솔루션을 사용하면 개발자가 자체 생태계를 유지하면서 서로 다른 L1 및 L2 프로토콜의 다양한 요소를 결합하여 상호 운용성을 높일 수 있음	비트코인 및 이더리움과 같은 L1 블록체인은 타사의 L2 프로토콜과 함께 사용되는 기본 프로토콜 L1 블록체인, 메인넷, 프라이머리 체인이라고도 불림	L2 프로토콜을 사용하면 병렬 블록체인에서 검증을 거친 후 수천 개의 저 가치(low-value) 트랜잭션을 처리할 수 있으며, 기록은 메인 블록체인 또는 메인넷으로 전송되어 불변의 기록으로 남게 됨

출처 : Cointelegraph Research, 'Layer 1 vs. Layer 2: The blockchain scalability showdown', 2023.11.06.
* L0 프로토콜은 L1 블록체인이 구축되는 토대로서 블록체인 네트워크 및 애플리케이션을 위한 인프라 역할을 담당

- 반면, XRP 렛저(XRP Ledger)나 이오스(EOS)와 같은 다른 네트워크는 중앙화되어 있는 대신 보안과 확장성을 모두 갖추고 있지만 일정 수준의 신뢰가 필요하기 때문에 잠재적인 약점이 될 수 있음

▶ L1 프로토콜과 L2 프로토콜: 개념과 특성 비교

- **(L1 개념 및 특성)** L1 네트워크는 비트코인, 이더리움 네트워크와 같은 전통적인 블록체인을 의미하며, 다른 모든 블록체인의 기반이 되는 기본 프로토콜을 형성하고 거래 검증 방법, 데이터 저장 방법, 합의 달성 방법 등 네트워크의 핵심 규칙을 정의

- **(L2 개념 및 특성)** L2 네트워크는 L1 네트워크 위에 구축되는 보조 프레임워크 또는 프로토콜로서, L2 솔루션의 주요 목적은 메인 체인에서 트랜잭션을 분리하여 L1 블록체인의 확장성을 높여 혼잡을 완화하고 트랜잭션 수수료를 절감하는 것

- **(L2 아키텍처)** L2 아키텍처는 크게 낙관적 롤업(optimistic rollup)과 영지식 롤업(zero-knowledge rollup)으로 구분

[낙관적 롤업과 영지식 롤업 비교]

구분	내용
낙관적 롤업	• 낙관적 롤업은 이더리움으로 전송된 업데이트가 유효하다고 가정 • 지정된 이의 제기 기간에 누구나 사기 가능성이 있는 트랜잭션에 플래그를 지정할 수 있음 • 핵심 보안 전제는 적어도 한 명의 정직한 참여자가 존재한다는 것 • 이의 제기가 발생하면 분쟁 해결 절차가 시작되는데, 롤업 제출자와 이의 제기자는 모두 채권을 예치하며, 분쟁에서 패한 쪽이 몰수당함 • 이의 제기 기간 후 롤업 트랜잭션은 확정된 것으로 간주하며, 이더리움의 상태도 그에 상응하는 업데이트를 진행
영지식 (ZK) 롤업	• 영지식 증명을 사용해 민감한 입력을 공개하지 않고 오프체인 트랜잭션을 암호학적으로 인증 • 온체인 암호화 증명이 제출되고 검증되는데 이는 각 트랜잭션을 개별적으로 검증하는 것보다 더 간단한 과정 • 낙관적 롤업과 마찬가지로, 트랜잭션을 오프체인에서 일괄 처리하지만 ZK 롤업에서는 진위 증명만 검증이 필요 • 관련 기술의 지속적인 발전과 함께 계산 시간이 꾸준히 감소하고 있고 데이터 공개를 자제함으로써 개인정보를 보호할 수 있다는 장점 존재

출처 : Cointelegraph Research, 'Layer 1 vs. Layer 2: The blockchain scalability showdown', 2023.11.06. / 일부 내용 표로 정리

▶ L1 프로토콜과 L2 프로토콜: 처리량(throughput), 지연 시간(latency), 보안(security) 관점에서의 비교

- **(처리량)** 주어진 시간 동안 처리된 트랜잭션의 수를 의미하며, 일반적으로 초당 트랜잭션 수(TPS)로 측정

- 이더리움은 현재 약 15~20의 평균 TPS를 가지고 있으며, 향후 100,000 TPS 이상으로 확장할 계획

- 다른 L2 네트워크도 비슷한 계획을 가지고 있으며, 이미 TPS 측면에서 이더리움을 앞지르고 있으나, 네트워크를 비교할 때는 실제 L1 처리량뿐만 아니라 제안된 솔루션도 고려하는 것이 중요

- 예를 들어, 이더리움은 부분적으로 L2 네트워크와 프로토-댕크샤딩(proto-danksharding)*에 의존하여 처리량을 늘릴 계획인데, 이는 블록에 더 저렴한 데이터를 추가하여 사용자에게 더 저렴한 L2 트랜잭션을 제공하는 것을 목표로 하는 업그레이드를 의미
  * 프로토-댕크샤딩: 기존 롤업이 트랜잭션을 처리하면서 맞닥뜨린 비용 문제와 저장공간 부족 문제를 해결하기 위해 새로운 형태의 데이터를 도입하자는 제안으로 롤업을 더욱 가볍게 만들 수 있음

- 반면 다른 네트워크들은 높은 수준의 미래 처리량을 예상하지만, 언제 실현될지는 불분명

- **(지연시간)** 지연 시간은 트랜잭션이 승인되는 데 걸리는 시간을 의미하고, 새로운 블록이 블록체인에 추가되는 데 걸리는 시간인 블록 시간(블록 속도)의 영향을 많이 받음

- 그러나 한 번의 블록 확인이 반드시 트랜잭션이 최종적으로 확정된다는 것을 의미하지는 않는다는 점에 유의해야 하며, 여기서 '완결성(finality)*'이라는 개념이 등장
  * 완결성: 영구적으로 블록체인의 일부가 되어 변경하거나 제거할 수 없음을 의미

- 이상적으로 높은 처리량(많은 트랜잭션을 처리할 수 있음)과 낮은 지연 시간(개별 트랜잭션이 빠르게 확인됨)을 모두 갖춘 시스템을 원하지만 실제로는 이 두 가지를 절충해야 하는 경우가 많음*
  * 처리량을 늘리기 위해 블록 크기를 늘려 각 블록에 더 많은 트랜잭션을 포함할 수 있도록 하면 네트워크를 통해 전파되는 데 시간이 오래 걸리므로 지연 시간이 늘어날 수 있음. 반대로 블록 시간을 줄이면 지연 시간을 줄일 수 있지만, 체인 재구성(또는 포크(fork))이 더 자주 발생하여 네트워크 안정성과 보안에 영향을 미칠 수 있음

- 지연 시간은 L1마다 다르며 블록체인의 설계와 합의 메커니즘의 영향을 받는 경우가 많음*
  * 비트코인은 지연 시간이 길고 처리량이 상대적으로 낮고, 이더리움 2.0과 지분 증명을 사용하는 다른 블록체인은 높은 처리량과 낮은 지연 시간을 모두 달성하는 것을 목표로 하지만, 설계마다 나름의 장단점과 과제가 존재

- 한편, L2 네트워크는 하나의 누적 업데이트가 L1 체인에 다시 게시되기 전에 오프체인에서 확인되기 때문에 지연 시간이 L1 네트워크보다 훨씬 짧음

- 그러나 L1의 블록 시간에 의존하기 때문에 작업이 되돌릴 수 없게 되는 데 걸리는 시간은 더 오래 걸릴 수 있음

- **(보안)** 블록체인 보안은 일반적으로 데이터의 불변성(immutability), 무결성(integrity), 가용성(availability)을 보장하고 유지하는 네트워크의 능력을 의미하고, 여기에는 다양한 잠재적 공격에 저항하고 복구할 수 있는 능력이 포함

- L1은 합의 방식, 네트워크 규모, 노드 다양성, 코드 품질 등 다양한 요인으로 인해 보안에 차이가 존재하며, L1의 보안은 작업 증명 또는 지분 증명과 같은 합의 메커니즘의 사용, 네트워크 유지를 위해 제공되는 경제적 인센티브, 광범위한 탈중앙화 덕분에 강력한 경우가 많음

- 하지만 스테이킹된 자금의 양이 적은 비교적 새로운 지분 증명 네트워크 등 특정 L1은 악의적인 당사자가 네트워크의 과반수 지분을 확보하는 데 드는 비용이 적기 때문에 공격의 위험이 더 클 수 있음

- 한편 대부분의 L2는 L1의 보안을 물려받는 경향이 있으며, 이는 L1의 보안 메커니즘을 활용하여 자체 운영을 보호한다는 의미

▶ 블록체인 확장성 미래 시나리오...기본 신뢰 계층으로서의 L1과 일상적 트랜잭션 처리의 표준이 될 L2

- 이더리움의 공동 창립자 비탈릭 부테린을 비롯한 블록체인 사상가들은 이더리움(또는 유사한 L1)이 글로벌 결제 레이어로서 중요한 역할을 할 것으로 예상

- 이러한 위치는 이더리움의 핵심 가치 제안, 즉 단일 제어 지점이나 실패 지점이 없는 완전한 무허가 시스템으로 인해 더욱 공고해질 것이며, 정부와 기관이 이미 이더리움 또는 유사한 프로토콜을 채택함에 따라, 기본 신뢰 계층으로서의 이더리움의 입지가 점점 더 두드러지고 있음

- 그러나 네트워크가 혼잡한 시기에는 이더리움의 높은 거래 수수료가 일상적 거래 수단으로서의 한계를 노출

- 한편, L2 네트워크는 일반적으로 0.20달러 미만의 낮은 수수료와 추가적인 최적화 노력으로 인해 일상적인 블록체인 거래의 표준이 될 수 있는 가능성이 있고, 이더리움의 의도된 목적에 완벽하게 부합하는 확장성을 제공

- L2 네트워크가 일상적인 트랜잭션을 처리함에 따라 이더리움은 이러한 네트워크를 위한 안전하고 신뢰할 필요가 없는(trustless) 결제 레이어로서의 역할에 집중할 수 있게 됨

- 암호화폐 업계가 더 많은 사용자를 끌어들이는 데는 확장성이 가장 큰 걸림돌이 될 것으로 예상되며, 다양한 프로토콜은 확장성 수요를 맞추기 위해 노력하는 중
- 사용자 및 투자자가 정보에 입각한 결정을 내리기 위해서는 다양한 프로토콜에서 개발 중인 기술을 이해하는 것이 중요하며, 모든 프로토콜은 네트워크 개선을 위해 업그레이드될 수 있음을 인지해야 함

[출처]

- Cointelegraph Research, 'Layer 1 vs. Layer 2: The blockchain scalability showdown', 2023.11.06.
- Vitalik Buterin's Homepage, 'Why sharding is great: demystifying the technical properties', 2021.04.07.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[EU]

유럽의회, 스마트 컨트랙트 관련 논란 많은 데이터법 승인

- 승인된 법은 조건이 충족되면 자동으로 거래를 실행하는 스마트 컨트랙트를 중단시킬 수 있는 조항을 포함
- 논란의 여지가 많은 조항으로 인해 향후 법 시행이 블록체인 업계에 미칠 영향에 대해 우려가 큼

유럽의 데이터 공유 규칙을 설정하기 위해 만들어진 데이터법(Data Act)은 스마트 컨트랙트에 대한 '킬 스위치'* 조항을 포함하고 있으며, 업계는 블록체인의 불변성을 훼손시킬 수 있다고 우려

* kill switch : 일반적인 방식으로는 종료가 불가능한 위험에 처한 기기나 시스템 등을 외부 개입으로 비상 종료나 변경하는 메커니즘

▶ 논란의 여지가 있는 스마트 컨트랙트 관련 조항을 명시한 데이터법, 큰 표 차이로 유럽의회를 통과

- 유럽의회(European Parliament)는 스마트 컨트랙트 개발을 포함한 다양한 분야의 규칙을 규정하는 '데이터법(Data Act)'*에 찬성했으며(11.09.), 법으로 제정되기 위해서는 유럽이사회(European Council)의 공식 승인이 필요

  * 데이터 접근에 대한 장벽을 제거하여 혁신을 촉진하는 것으로 목표로 제안되었으며, IoT, 산업 기계 등 연결된 제품이나 관련 서비스를 통해 생성된 데이터를 공유하기 위한 규칙을 설정하고 있음

- 한편 데이터법에 포함된 일부 조항에서 다양한 데이터 공유를 위한 스마트 컨트랙트에 관한 필수 요건을 명시하고, 스마트 컨트랙트를 안전하게 종료하거나 중단할 수 있는 수단(킬 스위치)을 요구하고 있어 논란

- 일부 암호자산 업계 구성원들은 데이터법의 광범위한 요건에 반대하고 있는 가운데, 유럽 암호화폐 옹호단체 ECI(European Crypto Initiative)는 이 법이 스마트 콘트랙트 개발자와 배포자에게 기술적으로 법을 준수하기 어려운 조건에서 이를 준수해야 할 책임을 지게 요구하고 있다고 주장

- ECI는 스마트 컨트랙트에 대한 킬 스위치 조항과 관련해 스마트 컨트랙트는 외부로부터의 종료 가능성을 피하도록 설계되어 있으며, 컨트랙트를 종료하는 모든 수단은 악용 위험을 가중할 수 있다고 지적

- 또한 스마트 컨트랙트와 법적 컨트랙트를 동등하게 취급하는 법 조항과 스마트 컨트랙트가 영업 비밀 보호에 관한 규칙에 따라 데이터를 처리하도록 요구하는 조항에도 반대한다는 입장을 표명

- 향후 EU 정부 기관이 이러한 규칙을 어떻게 시행할지는 아직 불분명하지만 지나치게 엄격한 규칙은 유럽 블록체인 기업의 역외 이전을 부추길 가능성이 있다는 점을 인지해야 할 필요

- 유럽의회는 데이터 공유에 관한 규칙을 담고 있는 데이터법을 큰 표 차이로 승인하였으며, 법 초안 공개부터 논란이 많았던 스마트 컨트랙트 조항의 포함과 관련해 업계가 큰 우려를 표명하고 있음
- 업계 구성원들은 해당 법의 시행으로 대부분의 스마트 콘트랙트가 불법으로 치부될 가능성이 있으며, 스마트 컨트랙트의 중단 기능은 블록체인의 기본 개념인 불변성 원칙에 반하는 조항이라며 반발

[출처]

- Cryptoslate, 'European Parliament approves controversial Data Act, which may require kill switches on smart contracts', 2023.11.09.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[프랑스]

블록체인 기술 연구 및 교육 위한 프랑스 최초의 암호자산 연구소 출범

- 프랑스의 고등 교육기관인 레오나르도 다빈치 센터는 암호자산 분야를 전문으로 하는 연구소를 설립
- 연구소는 연구, 교육, 기업과의 파트너십을 결합하여 암호자산 금융의 세계를 이해하는 것을 목표로 함

암호자산 연구소(Institut des Crypto-Actifs)는 암호자산 연구개발, 암호자산 관련 전문 교육 및 경제 주체와의 파트너십 구축, 암호자산에 대해 더 나은 지식을 전파하기 위한 프로젝트 등을 수행할 예정

▶ 암호자산 전문 연구소...블록체인 기술의 책임 있는 개발과 채택을 촉진하고자 하는 비영리 단체

- 디지털 부문 관련 공인 학위를 제공하는 4개의 고등 교육 기관으로 구성된 레오나르도 다빈치 센터(Pôle Léonard de Vinci)는 암호자산 분야를 전문으로 하는 연구소를 공식 개소(11.08.)
- 암호자산 연구소는 블록체인 기술의 책임있는 개발과 채택을 촉진하는 것을 목표로 하는 비영리 단체이며, 연구 수행, 교육 제공, 대중과의 소통을 통해 이를 달성할 예정
- **(학술 연구)** 블록체인 및 암호자산 관련 첨단 연구를 지원하고 수행하는 것을 목표로 프랑스의 저명한 학술 기관의 전문가 11명으로 구성된 과학위원회를 발족
- 또 다른 전문가 위원회로 블록체인 보안 및 인프라 솔루션 개발 기업 렛저(Ledger)의 공동 설립자 니콜라스 바카(Nicolas Bacca) 등 업계 저명인사가 포함된 6명의 실무자위원회가 연구소 업무를 감독할 예정
- **(전문 교육)** 취업 시장에서 블록체인 분야 자격을 갖춘 전문가에 대한 수요가 증가함에 따라 암호화 금융과 관련된 광범위한 전문가들을 대상으로 지속적인 교육과정을 제공할 것이라고 밝힘
- **(파트너십)** 암호자산 개발에 참여하기를 원하는 기업과의 파트너십을 구축하여 최첨단 전문 지식과 여러 연구 조사의 혜택을 받아 가상자산 전용 시스템의 안전한 배포를 최적화할 수 있도록 지원할 예정
- **(홍보 및 대중화)** 연구소는 디지털 자산을 현명하게 홍보하고 대중화하기 위해 다양한 대중 이해관계자와의 정기 토론회, 암호자산 금융 역사에 관한 전시회 개최 등 다양한 프로젝트를 발굴할 계획
- 암호자산 연구소의 시릴 그룬스팬(Cyril Grunspan) 소장은 교육과 암호자산에 대한 공개 토론 촉진에 중점을 두고 있다고 강조하며, 블록체인 환경에서 지식 보급과 협업을 위한 허브 역할을 수행하기를 기대

- 블록체인과 암호자산에 초점을 맞춘 프랑스 최초의 암호자산 연구소가 공식 출범했으며, 블록체인 기술 관련 연구 및 차세대 전문가 양성 교육, 블록체인의 대중의 인식 향상에 힘쓸 예정
- 암호자산 전문 연구소의 출범은 프랑스가 블록체인 연구 및 교육 분야의 리더로 자리매김하는데 도움이 될 뿐만 아니라 전 세계 블록체인 산업에도 중요한 발전이 될 것으로 예상

[출처]

- Cryptonews, 'Institute of Crypto-Assets Launches in Paris to Advance Research and Education in Blockchain Technology', 2023.11.10.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

'27년까지 48개국이 OECD의 암호자산 보고 프레임워크에 참여 예정

- 6개 대륙의 48개 국가가 암호자산 관련 탈세에 맞서기 위해 새로운 세금 투명성 표준 제정을 약속
- 세무 당국 간 금융 계좌 정보 자동 교환을 위한 OECD 공통보고기준에 암호자산 보고 프레임워크를 추가

중국, 러시아, 터키, 인도 및 거의 모든 아프리카 국가는 협정에 서명하지 않았으나 탈세의 은신처가 없는 글로벌 자동 정보 교환 시스템을 강화하기 위해서는 여러 국가들의 동참이 요구됨

▶ 암호자산 거래소에 대한 글로벌 세무 당국 간 자동 정보 교환 제공...'27년부터 시행 예정

- 영국, 싱가포르, 룩셈부르크의 공동 성명 및 개별 발표에 따르면 '27년부터 암호자산 거래소의 탈세 방지를 위해 관할권 간 정보 자동 교환을 제공하는 조세 투명성 표준에 48개국이 참여하기로 약속

- 이 협약은 세무 당국 간의 금융 계좌 관련 정보 자동 교환을 위한 정보 표준인 OECD의 공통보고기준(CRS)에 지난 6월에 최종 합의된 OECD의 암호자산 보고 프레임워크(CARF)*를 추가한 것

  * CARF(Crypto-Asset Reporting Framework): G20의 지시에 따라 암호자산 시장의 급속한 성장에 대응하고 글로벌 세금 투명성 보장을 위해 개발되었으며, '22년 10월 G20 재무장관에게 전달

- 성명서에 따르면 2년간의 협상 끝에 '23년 3월 CARF에 대한 최종 합의에 도달했으며 이는 암호화폐 플랫폼이 납세자 정보를 세무 당국과 공유하기 시작해야 함을 의미

- 또한 현재 공유하지 않고 있는 납세자 정보를 공유하여 세무 당국이 세금 준수를 시행하기 위해 정보를 교환할 수 있도록 보장할 것이라고 밝힘

- 성명서는 일관되고 시의적절하며 광범위한 CARF 구현이 서명국의 세금 준수 보장 능력을 향상할 것이며, 공공 수입을 감소시키고 납세자의 부담을 증가시키는 탈세를 단속하는 데 도움이 될 것이라고 언급

- 서명국은 활성화된 암호자산 시장의 호스트 역할을 수행하며, CARF를 국내법으로 신속하게 전환하기 위해 노력할 계획

- 협정에 서명한 국가로는 아일랜드, 오스트리아, 프랑스, 독일, 이탈리아, 크로아티아, 일본, 한국, 미국, 캐나다 등이 있으며, 중국, 러시아, 터키, 인도는 암호자산에 관한 높은 관심에도 불구 서명하지 않음

- 48개 국가와 관할권이 '27년까지 암호화 자산과 관련된 정보의 보고 및 교환을 위해 OECD의 글로벌 조세 투명성 프레임워크를 구현할 계획이라고 함
- OECD 사무총장은 이에 대해 암호자산에 대한 국제 조율 조치는 중요한 진전이며, 투명성과 정보 교환을 통해 탈세를 방지하는 광범위하고 조율된 접근 방식의 중요한 이정표라고 평가

[출처]

- Coindesk, 'International Deal to Combat Crypto Tax Evasion to Start 2027 as 48 Countries Sign Up', 2023.11.10.
- Cryptonews, '48 Countries Join Forces to Combat Crypto Tax Evasion Starting in 2027', 2023.11.13.

2023년 11월 03주

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

KISA 한국인터넷진흥원

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

IOSCO, 글로벌 디지털 자산 감독 추진 위한 18가지 정책 권고안 제시

- 글로벌 증권규제기관 협의체 IOSCO는 회원국의 관할권 내 암호자산 활동에 적용할 수 있는 권고안을 개발
- 모든 IOSCO 회원사가 일관되고 결과 중심적인 방식으로 해당 권고안을 적용, 채택할 것을 촉구

확정된 '원칙 기반' 및 '결과 중심' 가이드라인은 IOSCO* 회원 관할권의 규제 프레임워크를 조정하여 일관성을 추구하고, 디지털 자산 활동에서의 시장 무결성 및 투자자 보호에 관한 시급한 문제를 해결하는 것이 목표

* IOSCO(International Organization of Securities Commissions, 국제증권감독기구): 미국 상품선물거래위원회(CFTC)와 증권거래위원회(SEC)를 포함해 전 세계 증권 및 시장 규제 기관으로 구성

▶ 현재 관할권 간 차이를 인정하는 동시에 국경을 초월한 디지털 자산 활동 규제에 있어 일관성을 추구

• IOSCO는 회원국들이 관할권 내 암호자산 활동에 IOSCO의 증권 규제 목표 및 원칙*과 IOSCO 표준 등을 적절히 적용하고, 특히 암호자산 시장 내 시장 무결성 및 투자자 보호에 대한 광범위한 우려에 대응하기 위해 18개 권고안을 담은 보고서**를 발표(11.16.)

* IOSCO가 제시하는 증권 규제의 주요 목표 3가지는 투자자 보호, 시장의 공정성·효율성·투명성 보장, 시스템 리스크 감소이며, 규제기관과 관련된 원칙, 자율 규제를 위한 원칙, 증권 규제 집행 원칙 등 10개 부문 38개 원칙이 존재

** IOSCO, 'Policy Recommendations for Crypto and Digital Asset Markets, Final Report', 2023.11.16.

• IOSCO 이사회는 올해 5월 '암호자산 및 디지털 자산 시장에 관한 정책 권고안의 협의 보고서*'를 발표하고, 7월 말까지 제안된 사항에 관한 협의를 진행한 후 해당 결과를 반영하여 최종 권고안을 제시

* IOSCO, 'Policy Recommendations for Crypto and Digital Asset Markets Consultation Report', 2023.05.

• 권고안은 암호자산 서비스 제공자(Crypto Asset Service Provider, CASP)가 관여하는 6가지 주요 영역(▲활동과 기능의 수직적 통합으로 발생하는 이해 상충 ▲시장 조작, 내부자 거래, 사기 ▲국경 간 위험 및 규제 협력 ▲수탁 및 고객 자산 보호 ▲운영 및 기술적 위험 ▲소매 접근, 적합성 및 유통)을 다룸

• IOSCO는 현재 존재하는 관할권의 차이(정의 및 해석 측면)를 인정하여, 모든 규범적 분류체계에 일률적으로 적용하려는 시도 대신 위험을 완화하기 위한 기능적, 경제적 접근법을 통해 권고안을 수립

• IOSCO와 회원사들이 보유한 증권 시장 및 행위 규제기관으로서의 전문성을 바탕으로 기존 정책 프레임워크가 암호자산 시장에서 식별된 주요 위험에 어떻게 매핑되는지 검토하고 평가

• IOSCO의 목표 중 하나는 국경을 넘나드는 시장의 특성, 규제 차익 거래의 위험, 개인 투자자들이 지속적으로 노출되고 있는 심각한 피해 위험 등을 고려하여 회원사들이 암호자산 활동에 대한 규제 및 감독에 접근하는 방식에 대한 일관성을 제고하는 것

• 또한 '동일한 활동, 동일한 위험, 동일한 규제 결과'라는 원칙에 따라 개별 IOSCO 관할권 내에서 암호자산 시장과 증권 시장을 규제하는 방식에 있어 최적의 일관성을 장려하기 위해 노력하고 있음

• 본 권고안이 시장 참여자에게 직접적으로 적용되는 것은 아니지만, CASP와 모든 암호자산 시장 참여자는 등록/허가 및 국경 간 활동을 포함한 활동 수행 시 본 권고안을 신중하게 고려할 것을 적극 권장함

▶ **암호자산 서비스 제공자(CASP)의 서비스 및 활동과 관련된 18개 권고사항**

- **(권고안 1: 모든 규제기관을 대상으로 하는 주요 권고사항)** 규제 프레임워크는 ▲암호자산과 전통 금융 시장 간의 공평한 경쟁을 촉진하고 ▲규제 차익거래의 위험을 줄이기 위해 투자자 보호 및 시장 무결성 측면에서 전통 금융 시장에서 요구되는 것과 동일하거나 일관된 규제 결과를 달성하기 위해 노력해야 함

- 따라서 규제 당국이 규제 프레임워크의 적용 가능성과 적절성을 다음과 같은 측면에서 분석할 것을 권장(▲암호자산이 규제 대상 금융상품의 대체재이거나 대체재와 같은 역할을 하는 정도 ▲투자자들이 다른 금융 투자 활동을 암호자산 투자 활동으로 대체하는 정도)

- **(권고안 2, 3: 거버넌스 및 분쟁 공시 관련)** 많은 CASP는 일반적으로 거래소 거래, 중개, 시장 조성 및 기타 독점 거래, 마진 거래 제공, 수탁, 결제, 자산 재사용 등 여러 기능과 활동이 수직적으로 통합된 비즈니스 모델을 보유하고 있고, 이로 인해 발생하는 리스크가 존재

- 권고안 2('조직 거버넌스')는 CASP가 수직적 통합으로 인해 발생하는 이해 상충 문제를 효과적으로 해결하고 완화하기 위해 효과적인 거버넌스 및 조직 요건을 갖추어야 하며, 여기에는 기능 및 활동의 법적 분리, 별도 등록과 같은 조치가 필요할 수 있음을 명시

- 암호자산 거래 환경에서 CASP가 다양한 활동과 기능을 수행하는 경우, 투자자와 규제 당국은 고객과의 관계에서 CASP가 제공하는 정확한 활동과 기능, 역량을 이해하는 것이 중요하므로, 권고안 3('역할, 역량 및 거래 상충에 대한 공시')은 CASP가 각 역할과 역량을 정확하게 공시해야 한다고 명시

- **(권고안 4, 5: 주문 처리 및 거래 공시 관련)** 시장에서는 CASP를 일반적으로 '거래소'라고 부르지만 실제 시장 운영자(또는 거래장소)가 아닌 거래 중개자(브로커 및/또는 딜러)로 운영될 수 있음

- 권고안 4('고객 주문 처리')는 CASP가 고객 주문을 자신들에게 유리하게 처리하거나 특수관계인 거래에 관여할 수 있는 상황에 대비하여 CASP가 고객에게 최선의 이익이 되는 공정하고 질서정연하며 시기적절한 체결을 제공하는 시스템, 정책 및 절차를 구현해야 한다고 명시

- 권고안 5('시장 운영 요건')는 가격 발견과 경쟁을 촉진하기 위한 거래 공시의 투명성 요건을 명시하고 있으며, 이는 시장 운영자 역할을 하는 CASP뿐만 아니라 모든 CASP에 적용됨

- **(권고안 6, 7: 암호자산 상장 및 특정 주요 시장 활동 관련)** 많은 암호자산이 암호자산과 발행자에 대한 중요한 공시 없이 판매되고 있어 기존 금융 시장의 핵심 원칙인 정보에 입각한 의사결정을 촉진할 수 있는 정확하고 충분한 정보가 부족한 상황

- 권고안 6('거래 허가')은 CASP가 암호자산과 관련된 실질적, 절차적 상장 및 상장 폐지 기준을 채택하고 공개해야 한다고 명시

- 권고안 7('주요 시장 갈등 관리')은 CASP가 암호자산의 발행, 거래, 상장을 둘러싼 이해 상충을 관리하고 완화해야 하며, 이를 위해 자체 소유의 암호자산 또는 CASP 및 계열사와 중대한 이해관계를 갖는 암호자산을 상장하거나 거래하는 것을 금지해야 할 수 있다고 명시

- **(권고안 8-10: 악위적 행위 해결 관련)** 암호자산 시장은 ▲효과적인 시장 감시의 부재 ▲다단계 및 폰지 사기 등 조작적 시장 관행 ▲내부자 거래 및 내부 정보의 불법 공개 ▲허위 또는 불충분한 공시 등과 같이 시장 건전성을 악화시키는 위험이 존재

- 위와 같은 악의적 행위를 해결하기 위해 권고안 8~10('사기 및 시장 남용, 시장 감시, 비공개 정보 관리')은 시장 조작 행위를 식별 및 모니터링하고 내부 정보의 유출 및 오용을 방지하기 위한 효과적인 시스템과 통제가 있어야 함을 강조

- 규제 당국은 규제 보고를 개선하기 위한 지속적인 노력과 함께, 시장 투명성을 개선하고 효과적인 규제 보고와 시장 모니터링을 촉진하기 위해 CASP가 국제 데이터 표준을 준수하도록 장려해야 함

- **(권고안 11: 국경 간 협력 관련)** CASP는 종종 스스로를 국경 없는 방식으로 운영한다고 소개하며 규제 준수에 대해 양면적인 접근 방식을 취하는 경향이 있고, 이는 국제적인 조율된 규제 조치 없이는 지속될 것

- 따라서 규제 당국은 암호자산 발행, 거래 및 기타 활동의 국경을 초월하는 특성을 인식하여 다른 관할권의 규제 당국 및 관련 당국과 정보를 공유하고 협력할 수 있는 역량을 갖추어야 함

- 여기에는 다른 관할권의 규제 당국 및 관련 당국과 협력할 수 있는 협력 계약 및/또는 기타 메커니즘을 보유하는 것을 포함

- **(권고안 12-16: 고객 자금 및 자산 수탁 관련)** 수탁 관련 위험 및 고객 자금 및 자산 보호와 관련한 위험으로는 자산 분리, 자산의 재사용, 책임 및 소유권 문제 등이 존재

- CASP는 고객에게 관련 위험에 대한 명확하고 간결하며 非기술적인(non-technical) 공시를 제공해야 하며, 이러한 사항은 규제 프레임워크에 포함되어야 함

- 이와 같은 통제는 CASP가 고객 자금과 자산을 보유하는 경우 안전하게 보관하고 이전하며 자산의 부적절한 혼합 및 기타 잠재적 남용을 방지하는 데 도움

- **(권고안 17: 운영 및 기술적 위험의 관리 및 공시 관련)** 규제 당국은 CASP가 운영 및 기술 위험의 모든 주요 원천을 명확하고 간결하며 非기술적인 방식으로 공개하고, 이러한 위험을 관리 및 완화하기 위한 적절한 관리 프레임워크(예: 인력, 프로세스, 시스템 및 통제)를 갖출 것을 요구해야 함

- **(권고안 18: 소매 유통 관련)** 규제 당국은 CASP가 소매 고객과의 상호작용 및 거래와 관련하여 모든 암호자산 홍보 및 마케팅이 공정하고 명확하며 오해의 소지가 없는 방식으로 제공되도록 요구하거나 다른 관련 당국과 협력해야 함

- CASP는 암호자산 시장에 내재된 투기적 위험을 인지하고 이를 감수하기에 적합하다고 판단되는 소매 투자자를 성실히 평가하여 온보딩하고, 각 소매 고객에게 제공되는 특정 암호화 자산 상품 및 서비스의 적절성 및/또는 적합성 평가를 수행해야 함

▶ 전 세계적으로 일관되고 조율된 암호자산 규제 접근 방식을 개발해야 할 필요성 증대

- 최근 몇 년간 암호자산에 대한 글로벌 개인 투자자의 노출은 기하급수적으로 증가했으며, 기업과 투자자는 암호자산 시장의 취약성과 상호 연결성으로 인한 잦은 충격 이벤트로 상당한 손실에 노출됨

- 많은 투자자가 CASP를 통해 거래 활동을 하고 암호자산을 위탁 관리하는 환경에서 CASP는 투자자 보호와 시장 무결성을 달성하기 위한 관련 규제 프레임워크를 준수하려는 의지가 부족하고, 많은 경우 이러한 프레임워크를 회피하는 방식으로 운영한 사례가 많이 존재

• 암호자산 시장의 특성을 고려할 때, 규제 차익거래의 위험을 최소화하고 투자자 보호 및 시장 무결성을 유지하면서 혁신을 지원하기 위해서는 국제적인 규제 협력과 강력한 규제 표준을 적용하는 것이 중요

[디지털 자산에 대한 IOSCO의 18가지 권고안]

구분		주요 내용
1	모든 규제기관을 대상으로 하는 주요 권고 사항	규제 결과에 대한 공통 기준
2	조직 거버넌스	수직적으로 통합된 CASP 비즈니스 모델의 이해 상충 문제 해결
3	역할, 역량, 거래 상충 공시	CASP가 수행하는 각 역할과 역량을 정확하게 공시하도록 요구
4	주문 처리	CASP가 고객 주문을 공정하고 공평하게 처리하도록 보장
5	거래 공시	시장 운영자 또는 거래 중개자로 활동하는 CASP에 대한 투명성 요건
6	거래 허가	CASP 플랫폼에서 암호화폐 자산의 상장 및 상장 폐지에 대한 기준 설정
7	주요 시장 충돌 관리	암호화폐 자산의 주요 시장에서의 이해 상충 문제 해결
8	사기 및 시장 남용	조작적인 시장 관행을 식별하고 모니터링하는 시스템과 통제
9	시장 감시	시장 조작을 방지하기 위한 효과적인 시장 감시 시스템
10	중요 비공개 정보 관리	암호화폐 시장에서 내부자 정보의 오용을 방지
11	규제 협력 강화	암호화폐 자산 감독을 위한 국제 규제 협력 증진
12	주요 수탁 권고사항	CASP가 보유한 고객 자금과 자산을 보호
13	고객 자금과 자산의 분리 및 취급	고객 자산의 적절한 취급 및 보호
14	수탁 및 보관 약정 공시	고객 자산의 보관에 관한 명확한 공개
15	고객 자산 조정 및 독립적 보증	고객 자산의 조정 및 독립적 보증을 보장
16	고객 자금 및 자산 보안	고객 자산의 보안을 위한 통제 구현
17	운영 및 기술적 위험 관리 및 공시	CASP의 운영 및 기술적 위험 해결
18	소매 고객 적합성 평가 및 공시	소매 고객의 암호화폐 자산 투자 적합성을 평가하고 적절한 공시 보장

출처 : IOSCO, 'Policy Recommendations for Crypto and Digital Asset Markets, Final Report', 2023.11.16. / 일부 내용 표로 정리

- 시장 무결성 및 투자자 보호 문제로 인해 발생하는 위험은 투명성 부족과 전통 금융 부문과의 연계성 증가를 고려할 때 암호자산 시장을 넘어 잠재적으로 더 넓은 금융 안정성에도 영향을 미칠 수 있음
- IOSCO는 이러한 위험을 완화하기 위해 회원국 관할권의 규제 프레임워크 및 감독과 관련한 일관성을 제고하는 것을 목표로 디지털 자산 규제에 대한 18개 정책 권고안을 수립하여 발표

[출처]

- IOSCO, 'Policy Recommendations for Crypto and Digital Asset Markets, Final Report', 2023.11.16.
- Cryptoslate, 'Global securities regulators push for worldwide digital asset oversight with 18 new policy recommendations', 2023.11.17.

블록체인 기술·정책·산업 동향 디지털산업본부 블록체인산업단 블록체인정책팀

[싱가포르]

싱가포르 통화청(MAS), 도매 결제 위한 '실제' CBDC 발행 계획 발표

- MAS는 싱가포르 핀테크 페스티벌에서 내년 실제 도매 CBDC 발행을 시범적으로 실시할 계획이라 발표
- 이는 은행 자산의 토큰화를 포함해 디지털 송금을 위한 인프라를 구축하고자 하는 이니셔티브의 일환

MAS는 디지털 화폐의 안전하고 혁신적인 사용을 보장하기 위한 세 가지 이니셔티브로 디지털 싱가포르 달러에 필요한 인프라를 설명하는 청사진, 디지털 화폐 시범 확대, 도매 결제용 실제 CBDC 발행 계획을 발표

▶ 디지털 화폐 거래 촉진에 필요한 기술 인프라를 설명하는 오키드 청사진(Orchid Blueprint)

- **(배경)** MAS는 디지털 싱가포르 달러에 필요한 기술적 실현 가능성과 인프라를 탐색하기 위해 업계 파트너와 협력하여 '21년부터 다년간의 다단계 프로젝트인 '오키드 프로젝트(Project Orchid)'를 수행해 오고 있음

- 오키드 프로젝트의 첫 번째 단계는 프로그래밍 가능한 디지털 싱가포르 달러의 잠재적 사용 사례와 필요한 인프라를 발굴하는 것을 목표로 하였으며, '22년 11월 첫 번째 단계의 결과*가 발표된 바 있음
  * MAS, 'Project Orchid – Programmable Digital SGD', 2022.11.

- 두 번째 단계에서는 두 가지 접근 방식으로 ▲새로운 시나리오에서 목적 기반 화폐(PBM)* 사용을 확대하는 업계 주도의 디지털 화폐 시범사업을 수행하고 ▲디지털 화폐를 싱가포르의 결제 및 금융 시스템에 효과적으로 통합할 수 있는 방법을 검토하기 위한 업계 그룹을 구성하는 작업을 수행
  * Purpose Bound Money: 프로그래밍 가능한 화폐의 개념과 기능을 기반으로 한 조건 지정 프로토콜을 의미

- **(주요 내용)** 이번 발표된 '오키드 청사진*'은 산업 그룹과 함께 수행한 시범사업의 결과와 업계의 피드백에서 얻은 교훈을 바탕으로 싱가포르에서 디지털 화폐의 건전한 사용을 위한 인프라 구성요소를 자세히 설명
  * MAS, 'Orchid Blueprint - Infrastructure for safe and innovate use of digital money in Singapore', 2023.11.16.

[디지털 화폐의 주요 인프라 구성요소]

구분	주요 내용
결제 원장	디지털 송금을 기록하는 원장으로, 기본 프로그래밍 기능 및 디지털 토큰의 원자 결제와 같은 기능을 지원
토큰화 브릿지	기존 계정 기반 결제 시스템과 토큰화된 형태의 디지털 화폐와 호환되는 원장을 연결
프로그래밍 가능 프로토콜	디지털 화폐의 사용 조건을 지정하는 공통 프로토콜로 목적 기반 화폐(PBM)를 사용
이름 서비스(Name Service)	다루기 어려운 지갑 주소와 검증을 위한 읽기 쉽고 의미 있는 대체 이름 식별자 사이를 변환

출처 : MAS, 'Orchid Blueprint - Infrastructure for safe and innovate use of digital money in Singapore', 2023.11.16./일부 내용을 표로 정리

- 오키드 청사진은 디지털 화폐의 지속 가능하고 책임감 있는 혁신에 필요한 사람, 프로세스, 기술 전반의 명확성을 촉진하기 위한 설계 고려 사항을 통합하고 있음

- **(동기)** 업계 전반의 청사진을 통해 초기에 조율된 접근 방식을 제공함으로써 서로 다른 인프라, 플랫폼, 서비스 간의 상호운용성에 소요되는 불필요한 투자 및 비효율성을 제거하고자 함

▶ **오키드 청사진의 세부 내용...디지털 화폐의 형태와 주요 인프라 구성 요소에 대한 설명**

- **(디지털 화폐 형태)** 오키드 청사진은 크게 규제 대상 스테이블코인, 토큰화 은행 부채, CBDC 형태의 디지털 화폐와 관련이 있음

- 오키드 청사진은 MAS가 제안한 스테이블코인 활동에 대한 규제 프레임워크에 따라 가치 안정성에 대한 규제를 받게 될 단일 통화 스테이블코인을 지원할 예정이며, 해당 스테이블코인은 'MAS 규제 스테이블코인'으로 인정됨

- 오키드 청사진은 MAS의 규제를 받는 은행이 발행하는 토큰화 은행 부채(Tokenized Bank Liabilities, TBL)를 지원할 것이며, 이는 발행 은행의 대차 대조표에 의해 뒷받침되는 토큰으로, 준비 자산 풀에 의해 뒷받침되는 스테이블코인과는 다름

- 또한 오키드 청사진은 MAS가 발행하는 CBDC를 지원할 예정이며, CBDC는 ▲오늘날 일반인이 현금과 같이 접근할 수 있는 소매용 CBDC와 ▲은행 간 고액 거래 결제를 위해 일부 금융기관 그룹에 한해 접근과 사용이 제한되는 도매용 CBDC로 구분

- **(주요 인프라 구성요소)** 오키드 청사진이 정의한 싱가포르 디지털 화폐 인프라의 구성요소는 크게 4가지(결제원장, 토큰화 브릿지, 프로그래밍 가능한 프로토콜, 이름 서비스)임

- 결제원장은 일반적으로 분산원장기술(DLT)을 기반으로 구현되지만, 오키드 청사진의 맥락에서 논의된 개념은 비 DLT 원장에도 적용할 수 있도록 설계

- 또한 해당 분야의 발전이 유동적임을 고려하여 특정 플랫폼이나 기술을 전제로 하지 않고, 상호운용성과 디지털 화폐의 안전한 사용을 달성할 수 있는 원장 인프라의 최소 사양을 결정하는데 초점

- 토큰화 브릿지는 기존 시장 인프라와 토큰 기반 시스템을 연결하는 역할을 하는 구성요소로서 다양한 결제원장 구현과 호환되도록 설계하여 해당 원장에서 디지털 화폐의 발행과 상환을 용이하게 함

- 디지털 화폐의 새로운 가능성을 고려하여 토큰화 형태의 디지털 화폐에 대한 두 가지 기본 원칙으로 ▲독점적인 표준과 인프라를 요구할 가능성을 줄이는 '공통 토큰 표준'을 구현하고 ▲시스템 설계 시 디지털 화폐 구성요소의 모듈성과 자율성을 지원하는 구성 가능성(composability)을 추구

- 프로그래밍 가능한 프로토콜은 활동이 실행될 일련의 논리 또는 조건을 미리 정의할 수 있게 하며, MAS에서 제안한 표준 프로토콜인 목적 기반 화폐(PBM)를 예로 들 수 있음

- PBM은 다양한 원장 기술과 다양한 형태의 화폐에서 작동하도록 설계되었으며, 이를 공통 표준으로 채택하면 서로 다른 지갑을 사용하는 소비자들이 전용 애플리케이션 없이 디지털 화폐를 이체할 수 있게 됨

- 이름 서비스는 사람이 읽기 어려운 긴 문자열로 구성된 기본 식별자로 대상 지갑 주소를 사용하는 데 있어서 발생할 수 있는 오류와 어려움을 줄이기 위해 도입하는 새로운 식별자 서비스

- 오키드 이름 서비스(Orchid Name Service, ONS)는 의미가 있고 사람이 읽을 수 있는 이름을 지갑 주소로 변환하는 서비스로 구상되었으며, 현재의 결제 수단과 유사한 사용자 경험 및 다양한 사례로 확장할 수 있는 기능 제공이 목표

▶ **디지털 화폐의 광범위한 적용 가능성 테스트를 위한 오키드 프로젝트의 디지털 화폐 시범 운영 확대**

- 싱가포르에서 PBM과 디지털 화폐의 광범위한 적용 가능성을 테스트하기 위해 MAS는 오키드 프로젝트의 디지털 화폐 시범 운영을 확대할 예정

- 관련 인프라 구성요소와 상업적 모델 검토를 위해 업계 참여자들과 4가지 새로운 시범 운영(토큰화 은행 부채, 지갑 상호운용성, 공급업체 파이낸싱, 기관 결제 제어)에 착수

- **(토큰화 은행 부채)** OCBC(Oversea-Chinese Banking Corporation)와 UOB(United Overseas Bank)*는 한 은행에서 발행한 토큰을 다른 은행에서 소매 결제에 사용할 수 있도록 하는 가능성을 모색 중
  * OCBC와 UOB는 싱가포르의 3대 지역 은행에 포함

- **(지갑 상호운용성)** 앤트 인터내셔널(Ant International), 파즈(Fazz), 그랩(Grab)*은 PBM 개념을 사용하여 알리페이(Alipay) 사용자가 그랩페이(GrabPay) 가맹점에서 결제할 수 있도록 하는 시범 서비스를 시작할 예정
  * 앤트 인터내셔널은 싱가포르에 본사를 둔 디지털 결제 및 금융 서비스 기업, 파즈는 동남아시아 디지털 금융 서비스 그룹, 그랩은 동남아시아의 대표적인 슈퍼 애플리케이션(차량 호출 서비스)을 제공하는 기업으로 웹3 지갑 서비스 확대

- **(공급업체 파이낸싱)** 아마존(Amazon)과 HSBC 은행은 아마존에서 판매자에게 지급하는 대금을 토큰화하는 데 PBM을 사용하는 방안을 모색

- **(기관 결제 제어)** JP 모건(JP Morgan)은 은행이 합의된 신탁 생태계의 일부인 경우 은행의 기관 고객이 예금 토큰을 보유하여 발행 은행 외부의 고객에게 이체할 수 있도록 결제 제어를 사용하는 방안을 모색

▶ **금융 업계의 디지털 화폐 시범 운영을 보완하기 위한 은행 간 도매 결제용 실제 CBDC 개발 착수**

- 소매 및 기업 사용자를 대상으로 한 금융 업계의 디지털 화폐 시범 운영을 보완하기 위해 MAS는 내년에 은행 간 도매 결제용 CBDC 개발에 착수할 예정

- MAS는 이전에 테스트 환경에서 CBDC 발행을 시뮬레이션한 바 있으나, 도매 CBDC의 실제 발행을 실시하는 것은 처음

- 첫 번째 시범 운영에서는 시중 은행 간 소매 결제에 실제 도매 CBDC를 사용할 것이고, 향후 시범 운영에는 국가 간 증권 거래 결제를 위한 실제 도매 CBDC 사용이 포함될 수 있음

- MAS의 라비 메논(Ravi Menon) 총재는 결제에서 사용하기 위한 중앙은행 디지털 화폐의 실제 발행은 '16년부터 시작된 MAS의 디지털 화폐 여정에서 중요한 이정표가 될 것이라고 밝힘

- 국내 결제를 위한 CBDC를 모색 중인 싱가포르 통화청은 디지털 화폐에 대한 3가지 새로운 이니셔티브를 발표하였으며, 이 중 내년도 도매용 CBDC를 실제 발행하는 시범사업의 시행이 포함
- 시범 프로그램을 통해 은행은 대차 대조표에 채권으로 표시되는 토큰화 부채를 발행하여 고객과 판매자 간 거래할 수 있게 하고, 도매 CBDC의 자동 이체를 통해 정산하는 과정을 거칠 것이라고 함

[출처]

- Cryptoslate, 'Singapore's MAS reveals plan to issue 'live' CBDC for wholesale settlement, 2023.11.16.
- MAS, 'Orchid Blueprint - Infrastructure for safe and innovate use of digital money in Singapore', 2023.11.16.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

비탈릭 부테린, 기술 향상을 통해 플라즈마 스케일링의 부활 예고

- 부테린은 '17년 소개된 블록체인 확장 프레임워크인 플라즈마(Plasma)가 다시 주목받을 수 있다고 언급
- 롤업(Rollup) 기술에 가려져 있던 플라즈마가 유효성 증명의 발전으로 이전의 단점을 완화할 것으로 기대

비탈릭 부테린은 최근 개인 홈페이지 게시물에서 한때 주목받았던 확장성 솔루션인 플라즈마(Plasma)의 개념을 재조명하고, 새로운 기술 발전과 함께 블록체인 생태계에서 부활할 수 있는 가능성을 강조

▶ 유효성 증명의 발전...새로운 기능을 갖춘 플라즈마가 진화하는 블록체인 환경에서 중요한 역할 담당할 것

- 비탈릭 부테린은 '17년에 처음 소개된 블록체인 확장 프레임워크인 플라즈마(Plasma)가 본질적인 기술 한계로 인해 롤업(Rollup)*에 가려져 있었으나, 유효성 증명, 특히 ZK-SNARK**의 발전으로 인해 플라즈마의 이전 단점을 완화하고 다시 주목받을 가능성이 높다고 판단

  * 롤업: 이더리움 L2에서 여러 개별적인 트랜잭션들을 처리하고 그 결과값들을 하나로 묶은 뒤 L1에 저장하는 기술

  ** ZK-SNARK: ZK 롤업의 유효성 검증 방식 중 하나로 증명이 간결하며, 증명 과정에서 증명하고자 하는 주체와 증명을 검증하는 주체 간 상호작용이 없고, 제시된 증명의 유효성 이외 검증 주체가 추가적인 정보를 얻지 못한다는 특징

- 플라즈마는 이더리움 메인넷의 '하위' 체인으로 간주되며, 자체적인 블록 검증 메커니즘을 사용해 이더리움 외부에서 트랜잭션을 실행한 다음 주기적으로 최종 상태를 메인넷에 게시하는 블록체인 확장 솔루션의 일종으로*, 온체인(on-chain) 데이터 가용성에 의해 병목 현상이 발생하지 않는다는 특징

  * 널리 사용되는 확장 솔루션인 아비트럼(Arbitrum) 등과 달리 계산된 데이터를 압축된 상태로 메인넷에 다시 게시

- 한편 플라즈마 네트워크는 클라이언트 측 데이터 스토리지에 대한 과도한 비용과 간편 결제 이상의 기능을 수행하기 어려운 애플리케이션의 한계로 인해 기존 롤업 솔루션에서 고려되지 않았고, 일반화된 이더리움 가상 머신(Ethereum Virtual Machine, EVM)에 적용하기 어려운 문제가 존재했음

- 부테린은 유효성 증명(ZK-SNARK)이 플라즈마를 결제에 적용하는 데 있어 가장 큰 난제였던 클라이언트 측 데이터 저장 문제를 효율적으로 해결하고, EVM을 실행하는 플라즈마와 유사한 체인을 만들 수 있는 다양한 도구를 제공함으로써 플라즈마에 대한 우려를 해소할 수 있다고 강조

- 설계의 중요한 문제를 해결해도 악의적 행위자와 같은 우려는 여전히 존재할 수 있지만 그럼에도 플라즈마는 블록체인 분야에서 여전히 과소평가된 디자인이며 거래 수수료를 크게 완화하는 데 도움을 줄 것으로 평가

- 최근 부테린은 데이터 가용성 문제를 해결하기 위해 기존 출시된 확장 솔루션인 플라즈마를 재조명하고, 발전된 유효성 증명 기술의 적용으로 설계 상 단점을 해결할 수 있다고 강조
- 롤업은 여전히 최고 표준이며, 뛰어난 보안 특성을 가지지만 플라즈마는 데이터 가용성 문제를 피해 수수료를 크게 절감하고, 유효성 증명이 없는 체인을 위한 중요한 보안 업그레이드가 될 수 있다고 주장

[출처]

- Cryptoslate, 'Vitalik Buterin signals potential Plasma scaling resurgence with tech enhancements', 2023.11.14.
- Blockworks, 'What is Plasma and why is Vitalik Buterin into it all over again?', 2023.11.16.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

IMF 총재, CBDC가 현금을 대체할 수 있다고 언급

- IMF 총재는 싱가포르 핀테크 페스티벌에서 CBDC의 이점에 대해 강조하며 공공부문의 도입 준비를 촉구
- 또한 CBDC가 섬나라 경제에서 유통 비용이 많이 드는 현금을 대체할 수 있다고 언급

현 국제통화기금(IMF)* 총재는 5년 전 전임 총재가 변화의 바람에 따라 정책 입안자에게 CBDC를 사용할 것을 독려했던 연설을 언급하며 현재 공공부문이 CBDC 관련 결제 플랫폼 배포 준비를 지속해야 한다고 지적

* IMF(International Monetary Fund): 국제 통화 시스템의 안정성 보장을 위해 경제 및 금융 발전에 대한 감독을 수행하고, 회원국의 금융위기 시 기금 지원을 제공하는 국제기구

▶ IMF 게오르기에바 총재...CBDC를 고려하고 있는 중앙은행이 '기업가'처럼 행동할 것을 강조

- 싱가포르 핀테크 페스티벌(Singapore Fintech Festival)에서 연설한 IMF의 크리스탈리나 게오르기에바(Kristalina Georgieva) 총재는 정책 입안자들에게 CBDC를 계속 도입하고 수용할 것을 요청(11.15.)
- 게오르기에바 총재는 전임 총재였던 크리스틴 라가르드(Christine Largarde)의 연설 이후 5년이 지난 지금 CBDC에 대한 업데이트 현황을 제공하기 위해 참석했다고 밝힘
- 현재 많은 국가가 CBDC 도입을 연구하고 있으며, 디지털 화폐 개발을 안내하기 위한 규제를 개발하고 있지만 아직 사용 사례에 대한 불확실성이 높고 종착지에 도달하지는 못했다고 지적
- 일부 국가는 현재 CBDC 사용 가능성이 희박해 보이지만, 그 국가들조차도 잠재적으로 CBDC를 배포할 수 있는 가능성을 열어두어야 하며, 지금은 되돌아갈 때가 아니라고 언급
- 또한 공공부문이 앞으로 CBDC와 관련한 결제 플랫폼을 배포할 준비를 계속해야 한다고 강조하면서 이러한 플랫폼이 처음부터 국경 간 결제를 용이하게 하도록 설계되어야 한다고 주장
- 게오르기에바 총재는 CBDC의 이점에 대해 (싱가포르와 같은) 섬나라 경제에서 유통 비용이 많이 드는 현금을 대체할 수 있고, 선진국 경제에는 회복력을 제공할 수 있으며, 은행 계좌를 보유한 사람이 거의 없는 곳에서 금융 포용성을 향상시킬 수 있다고 설명
- 덧붙여 CBDC에 관심이 있는 중앙은행들에게 '좀 더 기업가처럼 생각해야 한다'고 촉구하며, 커뮤니케이션 전략과 배포, 통합, 채택에 대한 인센티브가 설계 고려 사항만큼이나 중요하다고 강조

- IMF는 회원국에 기술 지원을 제공하는 등 CBDC 개발에 깊이 관여하고 있으며, 수십 개의 관할권에서 개발 중인 다양한 CBDC 시스템 간 상호운용성 보장을 위한 글로벌 CBDC 플랫폼 개발에 노력 중
- IMF 총재는 CBDC에 관한 공공부문의 보다 적극적인 움직임을 촉구하며, 촉매제 역할을 하고, 안전과 효율성을 보장하며, 분열에 대응하기 위한 좀 더 많은 지침을 제공해야 할 시점이라고 언급

[출처]

- Blockworks, 'CBDCs can 'replace cash,' IMF says', 2023.11.15.
- CNBC, 'IMF says central bank digital currencies can replace cash: 'This is not the time to turn back'', 2023.11.16.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

부동산 비즈니스를 변화시킬 수 있는 블록체인

- 블록체인 기술은 운영에 투명성, 보안, 효율성을 더해 부동산 부문에 혁신을 일으킬 잠재력을 보유
- 소유권 및 데이터 관리, 자산의 토큰화, 거래 간소화, 평가 및 감정, 이력 및 출처 증명 등에 활용 가능

블록체인 기술은 서류 작업 감소부터 신속한 소유권 확인에 이르기까지 오래된 부동산 비즈니스를 혁신할 수 있는 가능성이 높지만 규제 장벽 및 비효율성을 통해 이익을 얻는 사람들의 저항과 같은 과제에 직면

▶ 기술 발전 및 규제 진화에 따라 부동산 업계에서 블록체인의 미래는 유망하지만 직면 과제 해결이 중요

- 부동산 산업은 오랫동안 현대 경제의 초석으로서 개인과 기업에 귀중한 자산과 투자 기회를 제공해 왔으나 그 중요성에도 불구하고 업계는 비효율성, 투명성 부족, 번거로운 절차 등 수많은 문제가 산적

- 블록체인 기술은 거래를 간소화하고 보안을 강화하며 비교할 수 없는 투명성을 제공함으로써 업계의 여러 문제를 해결하고 거래, 자산 관리, 데이터 저장 방식을 변화시켜 잠재적 판도를 바꿀 수 있을 것으로 평가

- 부동산 분야에서 블록체인은 ▲탈중앙화 및 변경 불가능한 원장을 통한 부동산 소유권 관리 ▲부동산 자산을 토큰화하여 부분 소유권과 유동성 제공 ▲스마트 컨트랙트로 부동산 매매와 임대 등 거래 간소화 ▲정확하고 투명한 부동산 평가 및 감정 ▲감사 가능한 과거 이력 및 출처 증명 등에서 활용 가능

- 한편 부동산 업계는 블록체인이 널리 채택되는 데 있어서 ▲규제 및 법적 장애물 ▲기존 시스템에서 전환하는 데 드는 비용 ▲민감한 개인 및 금융 정보에 대한 보안 문제 ▲변화에 대한 이해 관계자들의 저항 ▲블록체인 기술의 전문성 부족 등과 같은 몇 가지 과제들이 산재

- 한편 아랍에미리트*, 에스토니아**, 조지아*** 등의 국가에서는 이미 부동산 분야를 포함해 여러 분야에 걸쳐 블록체인 기술을 효과적으로 채택해 비용 절감과 효율성을 향상시키고 있는 사례를 보유
  * 아랍에미리트 정부는 거래의 50%를 블록체인으로 전환하는 것을 목표로 '21년 에미리트 블록체인 전략을 시작, 이를 통해 서류 작업이 줄어들고 비용이 절감되며 효율성이 향상
  ** 에스토니아는 블록체인을 도입하여 의료 기록과 사법, 입법, 보안 및 상업용 코드 시스템을 보호하는 데 블록체인을 활용하고 있으며, 기술 도입으로 공공서비스의 효율성 향상, 데이터 무결성 개선, 관료주의 감소 등의 혜택 발생
  *** 조지아는 블록체인을 부동산과 관련된 정부 거래를 검증하는 데 사용하여 관련 서비스의 보안과 대응력 개선 중

- 부동산 분야에 블록체인을 활용하면 더 많은 사용자를 유치하고, 신뢰를 강화하며, 프로세스를 간소화하고, 중개업체가 자문 분야에서 미래지향적이고 혁신적인 플레이어로 자리매김할 수 있을 것으로 예상

- 블록체인 기술은 탈중앙화, 투명성, 보안, 스마트 컨트랙트와 같은 특징을 바탕으로 부동산 비즈니스 운영에 투명성, 보안, 효율성을 더해 업계의 혁신을 일으킬 수 있는 잠재력을 보유했다고 평가됨
- 부동산 부문에서 블록체인의 미래는 더욱 유망해 질 것으로 보이며, 기술 채택에 걸림돌이 되는 주요 과제들을 해결한다면 보다 효율적, 포용적, 신뢰할 수 있는 산업을 위한 길을 열어줄 것으로 기대

[출처]

- Forkast, 'Blockchain can transform the real estate business — if we remove the roadblocks in its way', 2023.11.16.

2023년 11월 04주

글로벌 블록체인 기술·정책·산업 동향

Global Blockchain Tech, Policy & Industry Trends

블록체인 기술·정책·산업

CONTENTS

KISA 한국인터넷진흥원

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

웹3에서 안전을 유지하는 법: 댑(dapp) 보안 가이드

- 블록체인 기술을 기반으로 스마트 컨트랙트를 통해 작동하는 댑(dapp)과 관련한 위험이 증가하는 중
- 웹3 환경과 댑의 주요 보안 위협으로 피싱(phishing) 공격, 소셜 엔지니어링, 업데이트 지연 등이 지적

웹3의 확장과 함께 댑(dapp)*과 관련한 보안 위험이 증가하고 있는 상황에서 보안 활동은 사전 위험 식별, 전략적 블록체인 설계의 선택, 정기적인 검사, 지속적인 학습을 포함하는 지속적 프로세스로서 다루어야 할 필요

* 댑(dapp): 탈중앙화(decentralized)와 애플리케이션(application)의 합성어로 분산형 네트워크에 구축된 애플리케이션

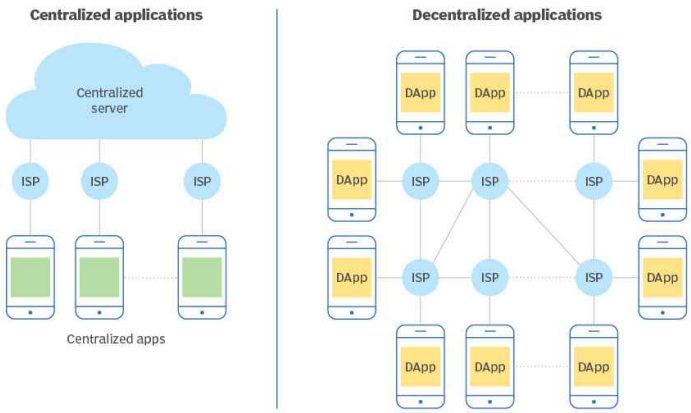
▶ 새로운 웹3 기술의 최전선에서 기존의 앱에 대응하여 블록체인 기능을 수행하는 dapp

- 흔히 댑 또는 디앱(dapp)이라고 불리는 탈중앙화 애플리케이션은 블록체인에서 실행되는 앱 내 특정 작업을 수행하기 위해 상호 연결된 스마트 컨트랙트를 사용하며, 현재의 인터넷(웹2)과 발전 중인 웹3를 잇는 다리 역할을 담당

- dapp은 블록체인 기술 고유의 보안성, 투명성, 삭제 불가능성을 활용하여 사용자에게 개인정보보호 강화와 데이터 및 디지털 자산에 대한 통제권을 부여하며, 소셜 미디어, 금융, 게임 등 다양한 분야에서 기존 앱에 대응하여 블록체인 기능을 수행

- dapp을 사용하는 방식은 일반 앱과 비슷해 보일 수 있지만, dapp은 하나의 큰 서버에 저장되는 대신 블록체인 네트워크의 '노드'라고 불리는 여러 컴퓨터에 분산되어 있음

[기존의 앱과 dapp의 차이]



출처 : TechTarget, 'Blockchain for business: The ultimated enterprise guide - decentralized application(DApp)', 2023.06.

▶ 웹3와 dapp의 주요 보안 위험...피싱 공격, 소셜 엔지니어링, 프로토콜 및 브리지 공격, 업데이트 지연 등

- 웹3의 빠른 확장이 가져온 새로운 보안 문제와 관련하여 일부 보안 결함은 웹2와 웹3 인프라 간 상호작용에서 비롯되는 반면, 다른 보안 결함은 블록체인 및 IPFS(InterPlanetary File System)*과 같은 프로토콜에 내재되어 있음

  * IPFS: 분산형 파일 시스템에서 데이터를 저장하고 공유하기 위한 프로토콜로 탈중앙화, P2P 방식의 네트워크

- 또한 웹3는 네트워크 합의에 의존하기 때문에 보안 취약점을 수정하는 속도가 느려질 수 있다는 특징

- 주요 보안 위험으로 ▲피싱 공격 ▲소셜 엔지니어링 ▲암호화되지 않고 확인되지 않은 API 쿼리 ▲프로토콜 및 브리지 공격 ▲중앙집중식 거래소(CEX) ▲계정 및 모바일 지갑 도난 ▲멀웨어 및 키로거(keylogger)* ▲분산형 데이터 스토리지의 개인정보보호 문제 ▲업데이트 지연 ▲스마트 컨트랙트의 보안 취약점 등이 지적

  * 키로거(keylogger): 하드웨어 기기 및 소프트웨어를 통해 컴퓨터의 모든 키보드 입력 내용을 캡쳐하는 것

[웹3 및 dapp의 주요 보안 위험]

보안 위험	주요 내용
피싱 공격	• 악의적인 공격자가 사기성 웹사이트나 소셜 미디어 계정을 만들어 사용자를 속여 개인 키나 기타 기밀 정보를 공개하도록 유도할 때 발생
소셜 엔지니어링	• 사이버 범죄자가 사용자를 속여 로그인 자격 증명을 공유하도록 유도하는 방법
암호화되지 않고 확인되지 않은 API 쿼리	• 웹3 애플리케이션은 연결 끝(connection ends)을 인증하지 않는 API 호출과 응답에 의존하는 경우 다수 • 웹3는 모든 네트워크 노드가 저장된 데이터와 직접 인터페이스할 수 있는 완전한 탈중앙화를 제안하지만 웹3 애플리케이션 프론트엔드(front-end)에는 여전히 사용자와 상호작용하기 위한 웹2 기술이 필요 • 많은 웹3 API 쿼리는 암호화 방식으로 서명되지 않기 때문에 온패스(on-path) 공격*, 데이터 가로채기 및 기타 위협에 노출될 수 있음
프로토콜 및 브리지 공격	• 모든 웹 3가 블록체인 위에 바로 구축되는 것은 아니고, 여러 네트워크에는 레이어 2(L2)라고 하는 플랫폼이 그 위에 구축되어 있음 • 또한 서로 다른 네트워크 간의 통신을 가능하게 하는 프로토콜인 브리지가 존재 • 해커는 L2 프로토콜과 브리지를 모두 취약점으로 간주하여 공격할 수 있음
중앙집중식 거래소(CEX)	• 중앙 집중식 거래소는 암호자산 거래에 편리함을 제공하지만, 대량의 자금을 보유하고 있기 때문에 해커의 표적이 되는 경우 다수
계정 및 모바일 지갑 도난	• 암호자산 또는 NFT 지갑에 대한 공격은 일반적으로 해커가 사용자의 개인 키에 액세스하거나 피싱을 통해 사용자를 속여 개인 키를 넘겨줄 때 발생
멀웨어 및 키로거(keylogger)	• 해커가 사용자 자격 증명과 개인 키에 불법적으로 접근하기 위해 사용하는 소프트웨어 도구
분산형 데이터 스토리지의 개인정보보호 문제	• 웹2 모델에서의 데이터베이스 접근이 매우 제한적이었던 것과 달리, 블록체인에서는 연결된 모든 노드가 블록체인의 데이터에 접근할 수 있음 • 데이터가 익명화되어 있더라도 수많은 보안 및 개인정보 보호 문제가 발생
업데이트 지연	• 웹3의 탈중앙화 특성으로 인해 전체 네트워크가 모든 변경 사항을 승인해야 하므로 보안 결함이 발견된 후에도 보안 결함이 지속될 수 있음
스마트 컨트랙트의 보안 취약점	• 다른 코드와 마찬가지로 스마트 컨트랙트에도 사용자 데이터나 자금을 노출시킬 수 있는 심각한 보안 결함이 있을 수 있음

* 온패스 공격: 공격자가 네트워크 통신 경로 상에 위치해 통신을 가로채거나 조작하는 공격

출처 : Cryoto.news, 'Staying safe in web3: your guide to dapps security', 2023.11.21. / 일부 내용 표로 정리

▶ 웹3의 새로운 취약점 분류 기준..스마트 컨트랙트 설계 실패, 잘못된 코딩, 인프라 취약점 강조

- 블록체인 보안 플랫폼 이뮨파이(Immunefi)가 얼마전 웹 서밋(Web Summit) 2023에서 발표한(11.17.) 보고서*에 따르면 웹3에서 가장 큰 피해를 주는 취약점의 근본 원인은 크게 ▲스마트 컨트랙트의 설계 실패 ▲컨트랙트의 잘못된 코딩 ▲인프라 취약점으로 구분 가능하다고 함

  * Immunefi, 'The True Origin of Hacks – Top Web3 Vulnerabilities', 2023.11.

- 이뮨파이는 스마트 컨트랙트 프로토콜은 충분한 관심을 받지만, 주로 간과되기 쉬운 인프라 수준에서 위험이 발생할 수 있다고 지적

- 보고서에 따르면, '22년 해킹으로 인한 금전적 손실의 거의 절반이 개인 키(private key) 처리 불량과 같은 인프라 문제로 인해 발생하였고, 전체 사고의 약 37.5%가 액세스 제어, 입력 유효성 검사, 계산 오류 등과 같은 스마트 컨트랙트 관련 부분에서의 개발자의 실수로 인해 발생한 것으로 나타남

- 이뮨파이 플랫폼의 미첼 아마도르(Mitchell Amador) CEO는 기본 인프라가 취약하면 잘 설계된 스마트 컨트랙트도 손상될 수 있으며, 이는 상당한 손실로 이어질 수 있다고 강조함

- 또한 블록체인은 개방적이고 권한이 없는 환경으로 기존 웹 환경에서와 같이 인프라에 몰래 침입한 사람뿐만 아니라 계약을 볼 수 있는 사람, 제품을 망칠 수 있는 사람 등 모든 사람으로부터 보호해야 한다고 언급
- 블록체인 보안 회사인 웹3 안티바이러스(Web3 Antivirus)의 설립자 알렉스 둘럽(Alex Dulub)은 웹3 및 dapp의 진정한 위협은 불완전한 스마트 컨트랙트 로직에서 발생하는 취약점이라고 지적

- 둘럽은 개발자가 특정 요구 사항을 사용하여 스마트 컨트랙트의 작동 방식을 정의할 수 있지만, 의도하지 않은 방식으로 사용될 위험은 항상 존재한다고 설명하며, 해커들은 더욱 창의적으로 스마트 컨트랙트와 프로젝트를 실험하고 불일치하는 부분을 찾아 악용하고 있음을 강조

- 또한 안타깝게도 자동 도구나 분석기로 이러한 복잡한 문제를 탐지하는 것은 거의 불가능하므로, 최선의 방법은 엄격한 테스트, 신중한 로직 개발, 모든 잠재적 사용 시나리오 분석, 철저한 감사, 버그 바운티(bug bounty)* 프로그램 시행이라고 언급
  * 버그 바운티: 기업의 소프트웨어 등을 해킹해 보안 취약점을 발견하고 최초로 신고한 사람에게 보상을 지급하는 것

▶ 웹3 공간에서 사용자의 보안 조치…사칭 경계, 계정 잔액 확인, 새로운 dapp 다운로드 및 설치 주의 등

- **(사칭(impersonation)에 대한 경계 늦추지 않기)** 피싱 공격자들이 누군가를 사칭하여 피해자들을 속이는 행위가 자주 발생하므로 이를 간과하면 심각한 결과를 초래할 수 있음

- **(계정 잔액 추적하기)** 사소해 보일 수 있지만 웹3의 보안 위협을 완화하는 근본적인 방법으로, 새로운 플랫폼에서 지갑 서명을 사용한 후에는 계정 잔액을 확인하는 것이 가장 좋은 방법임

- **(의심스러운 거래 및 무단 액세스 신고)** 의심스러운 거래나 무단 액세스를 발견하면 즉시 탈중앙화 금융기관 또는 dapp 플랫폼 제공업체에 신고해야 함

- **(dapp 다운로드 및 설치 주의)** 새로운 애플리케이션을 다운로드하고 설치할 때 신뢰할 수 있는 출처를 이용하고, 낯설거나 신뢰할 수 없는 웹사이트의 소프트웨어는 피하는 것이 바람직함

- **(개인 키 보안 강화)** 암호자산이 해커의 표적이 되는 경우가 많기 때문에, 전문가들은 사용자가 개인 키를 완전히 제어할 수 있는 지갑에 자금을 보관할 것을 권장

- 웹3 사용자는 개인 키 보안을 강화하기 위해 잠재적인 키로거(keylogger)*로부터 안전하게 키를 오프라인에 저장하는 하드웨어 지갑이나 콜드 스토리지 솔루션을 사용할 수 있음

- 스마트 컨트랙트를 사용하여 애플리케이션 내에서 특정 작업을 수행하는 dapp은 웹3의 확산으로 소셜 미디어, 금융, 게임 등에서 활용되며 빠르게 성장하고 있으나 동시에 관련 보안 위험도 증가하고 있음
- 전문가들은 웹3 및 dapp의 진정한 위협은 불완전한 스마트 컨트랙트의 작동 방식에서 발생하는 취약점이라고 지적하며, 이와 함께 기본 인프라의 취약점도 중요하게 고려해야 한다고 강조

[출처]

- Cryoto.news, ‘Staying safe in web3: your guide to dapps security’, 2023.11.21.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

소셜 미디어와 디파이를 연결하는 소셜파이(SocialFi)

- 웹3의 탈중앙화 원칙을 기반으로 하는 소셜파이(SocialFi)는 소셜 미디어와 디파이(탈중앙화 금융)를 융합한 개념
- 소셜파이의 주요 목표는 사용자가 자신의 데이터를 소유, 소셜 미디어에서 수익을 창출할 수 있도록 하는 것

실시간으로 생성되는 방대한 양의 사용자 데이터로부터 창출되는 수익의 분배가 대부분 중앙집중식 기관의 통제 하에 이루어지고, 데이터를 생성한 개인은 최소한의 혜택만 얻게되는 웹2 영역의 과제를 해결 가능

▶ 웹2에서 웹3로의 진화...웹3의 탈중앙화 특성과 소셜 미디어 기능의 융합으로 소셜파이(SocialFi) 등장

- 21세기 내내 온라인 세계를 지배해 온 웹 2세대의 기업은 검색 엔진을 도입한 이후 소셜 미디어를 우리 생활에 도입했으며, 사용자 데이터의 막대한 가치를 깨닫고 사용자를 하나의 제품으로 취급하기 시작

- 웹2의 혁신 중 소셜 미디어는 가장 수익성이 높았으며, 이 분야에서의 성공한 사람들은 수십억 달러의 광고 수익과 구독료를 창출했으나, 안타깝게도 소셜 상호작용과 콘텐츠 제작을 통해 수익을 창출하는 기업들은 대부분의 수익 분배를 통제하는 거대 기업으로 성장하여 독과점 체제를 형성

- 또한 몇 년 전 페이스북과 관련된 케임브리지 애널리티카 사건*에서 볼 수 있듯이 사용자 정보가 동의 없이 상품화되고 거래되면서 개인 데이터 보호에 대한 우려를 불러일으키고 있음
  * Cambridge Analytica data scandal: '16년 초 영국 데이터 분석 회사 케임브리지 애널리티카가 페이스북 가입자 수백만 명의 프로필을 동의없이 수집하여 정치적 선전에 이용하려고 했다는 사실이 밝혀지면서 물의를 일으킴

- 예전 정적 웹 페이지가 있는 읽기 전용 환경과 같았던 웹1은 블로그와 소셜미디어를 통해 상호 작용할 수 있는 읽기-쓰기 기능을 제공하는 웹2로 진화했으며, 웹3는 여기서 한 단계 더 나아가 읽기-쓰기-소유 기능까지 제공하게 됨

- 여기서 '소유'는 웹3 토큰을 소유하는 것을 넘어 데이터와 이를 수익화하여 이익을 창출할 수 있는 도구를 소유하는 것을 의미

- 데이터를 소유하고 노력으로 수익을 창출할 수 있는 새로운 능력으로 인해 디파이 요소 및 암호자산 세계와 웹2를 결합한 흥미로운 기술 분야(예: 게임파이(GameFi), 소셜파이(SocialFi))가 생겨나고 있음

▶ 소셜파이의 개념 및 특징...탈중앙화 방식으로 소셜 미디어에서 사용자가 생산한 콘텐츠를 소유하고 운영

- 소셜파이는 소셜 미디어(Social Media)와 디파이(DeFi, 탈중앙화 금융)를 결합한 개념으로 소셜파이 플랫폼*은 소셜 미디어 네트워크와 사용자가 생산한 콘텐츠를 생성, 관리, 소유하는데 있어 웹3의 탈중앙화 접근 방식을 취함
  * 플랫폼은 중앙화 검열을 방지하도록 설계된 DAO(탈중앙화 자율조직)의 형태

- 소셜파이의 핵심은 콘텐츠 제작자, 인플루언서, 참여자들이 자신의 데이터를 더 잘 통제하고, 자신을 표현할 자유를 누리고, 소셜 미디어에서의 존재감과 상호 작용을 통해 수익을 창출할 수 있는 기회를 가진다는 것

- 일반적으로 이러한 플랫폼의 수익은 암호자산의 형태로 발생하며, 신원 관리와 디지털 소유권은 NFT(Non-Fungible Token, 대체 불가능한 토큰)을 통해 촉진됨

- 최근 몇 년간 블록체인 기술의 발전 덕분에 소셜파이 인프라는 소셜 미디어 상호작용에 필요한 대량의 트랜잭션을 효과적으로 처리할 수 있게 됨

▶ 웹2 기반 소셜 미디어의 문제점을 해결하는 소셜파이...수익 분배, 개인 브랜드 창출, 디지털 소유권과 추적

- **(웹2 기반 소셜 미디어의 문제)** 소셜 미디어에서는 실시간으로 방대한 양의 귀중한 사용자 데이터가 발생하지만 기존의 방식으로는 사용자 데이터에서 발생하는 대부분의 수익을 중앙집중식 기관이 차지하고, 해당 데이터를 생성한 개인은 최소한의 혜택만 얻게되는 문제가 존재

- 개인이 자신의 브랜드로 수익을 창출할 수 있는 능력과 관련하여, 웹2 기반의 소셜 미디어에서도 많은 인플루언서들이 강력한 개인 브랜드 자산을 구축하며, 이는 수익으로 연결되기도 하지만 광고나 비즈니스 벤처를 통한 간접적인 수익 창출이 대부분이었음

- 또한 표준화된 디지털 소유권 규정이 없기 때문에 웹2 소셜 미디어 환경에서는 콘텐츠 복제 및 지적 재산권 도용에 대한 취약성이 발생할 수 있으며, 이는 온라인에서 작품을 공유하는 콘텐츠 크리에이터나 아티스트에게 특히 중요한 문제

- 이에 더해 웹2 플랫폼은 유해한 콘텐츠로부터 사용자를 보호하기 위해 콘텐츠 크리에이터에게 특정 주제에 대한 토론을 제한하는 등 중앙집중식 통제를 가하는 경우가 많음

- **(웹3 기반 소셜파이의 해결책)** 결제원장은 일반적으로 분산원장기술(DLT)을 기반으로 구현되지만, 오키드 청사진의 맥락에서 논의된 개념은 비 DLT 원장에도 적용할 수 있도록 설계

- **(디지털 소유권 및 신원 확인)** 프로필 사진 대체 불가능 토큰(PFP NFT)*의 등장으로 새로운 형태의 디지털 신원 확인이 도입되었으며, 사용자는 소셜파이 프로필을 만들 때 NFT를 프로필 사진으로 활용하고, 디지털 지갑을 연결해 소유권을 증명할 수 있음

  * Profile Picture Non-Fungible Token: 온라인에서 자신을 표현하기 위해 사용하는 디지털 예술 작품으로 블록체인을 통해 작품의 진품을 인증할 수 있음. 소셜 미디어 사용자들이 특정 커뮤니티에 소속되어 있음을 알리기 위해 사용하는 경우가 많음

- 신원 확인 외에도, PFP NFT는 생활 조언이나 투자 트랜드와 같은 고유한 가치를 제공하는 소셜파이 내 특정 커뮤니티에 대한 독점 액세스 권한을 부여할 수 있음

- 또한, NFT 컬렉션을 출시하는 아티스트는 작품 판매 수익을 소셜 토큰 보유자와 공유하여 팔로워 증가와 매출 증대를 장려할 수 있음

- **(절제와 표현의 자유)** 소셜파이는 온체인 데이터 라벨링을 통해 탈중앙화된 중재를 구현함으로써 적절한 콘텐츠 관리와 표현의 자유 사이의 균형을 맞추는 것을 목표로 함

- 소셜 플랫폼에서 공개적으로 볼 수 있는 모든 게시물은 블록체인에 저장되어 주제와 언어적 특성에 따라 데이터를 분석하고 태그를 지정할 수 있음

- 이러한 게시물에 대한 의사 결정 권한은 네트워크 노드가 가지고 있으며, 각 노드는 특정 레이블을 차단하고 다른 노드와 상호 작용할 수 있지만, 노드가 유해한 콘텐츠에 참여하고 지지하기로 선택한 경우 운영자가 법적 책임을 지게 됨

- 따라서 소셜파이에서 중재는 중앙 당국이나 중개자에게 의존하지 않고, 개별 사용자에게 통제권과 책임이 주어짐

▶ **소셜파이의 장애물...사용자간 영향력 불균형, 인프라 확장성, 지속 가능한 수익 모델**

- **(사용자간 영향력 불균형)** 기본적으로 소셜파이는 개인 브랜드 가치를 디지털 화폐 또는 토큰으로 전환하게 되는데, 이 과정이 이미 유명한 개인에게 있어서는 쉽게 이루어지므로 소셜파이를 통해 콘텐츠 제작과 사용자 유치에 있어 독점적인 지위를 유지할 수 있음

- 그에 비해 신규 사용자나 일반 개인은 커뮤니티와 콘텐츠에 접근하는 데 도움이 필요하고, 이들은 사용자를 끌어들이기 위해 더 풍부하고 매력적인 콘텐츠를 만들어야 함

- 결과적으로, 콘텐츠가 반드시 실질적인 가치를 제공하지 않더라도 영향력과 수익 잠재력이 소수에게 집중될 수 있음

- **(인프라 확장성)** 대표적인 소셜 미디어인 페이스북(Facebook)은 분당 510,000개의 댓글, 293,000개의 상태 업데이트, 4백만 개의 좋아요, 136,000개의 이미지 업로드 등 매일 4 페타바이트(Petabyte, PB)*에 달하는 엄청난 양의 데이터를 생성

  * 페타바이트: 바이트(byte)의 10^{15}배를 의미하는 디지털 데이터 용량 단위, 1,000 테라바이트와 동일

- 이러한 방대한 데이터 스트림을 처리하는 것은 방대한 양의 정보를 구축하고 처리하는 데 필수적인 블록체인 기술의 중요한 과제가 됨

- 한 예로 소셜파이 애플리케이션 구축 전문 블록체인 레이어인 디소(DeSo)는 소셜파이에 특화된 설계 덕분에 기존의 대부분의 레이어 1(L1) 체인에 비해 확장성이 뛰어나다고 주장

- 이 프로젝트는 인덱싱(indexing), 블록 크기 관리, 워프 동기화(warp sync), 샤딩(sharding) 등 확장성 문제를 해결하기 위한 다양한 솔루션을 채택하고 있음**

  * 워프 동기화는 모든 노드가 전체 트랜잭션 내역을 확인할 필요 없이 검증된 트랜잭션을 가능하게 하고, 샤딩은 병렬 처리를 용이하게 하여 효율성을 크게 향상시킴

  ** 디소는 이러한 기술을 통해 10억 명의 사용자를 수용할 수 있도록 플랫폼을 확장할 수 있을 것으로 낙관

- 그러나 모든 소셜파이 프로젝트가 동일하게 효과적인 지원 방법을 찾은 것은 아니기 때문에 확장성은 소셜파이의 지속 가능한 성장을 위한 중요한 과제임

- **(지속 가능한 수익 모델)** 디파이와 파생 비즈니스 모델에서 가장 큰 도전 과제는 지속 가능한 수익 모델을 만드는 것

- 게임파이(GameFi)*와 소셜파이는 참여자들에게 상당한 수익을 안겨주었지만, 이러한 수익의 대부분은 단기적인 것으로 입증

  * 소셜파이와 유사하게 게임과 디파이가 합쳐진 개념으로 게임을 통해 플레이어가 소유하게 되는 다양한 자산으로부터 수익을 창출할 수 있음

- 소셜파이는 아직 소규모의 실험 단계로서, 광범위한 채택을 달성하기 전에 여러 시장 주기와 예상치 못한 사건을 극복해야 함

▶ 소셜파이 생태계 기본 구성 요소인 소셜 토큰...개인 토큰, 커뮤니티 토큰, 소셜 플랫폼 토큰으로 구분

- 개인 토큰, 커뮤니티 토큰, 소셜 플랫폼 토큰으로 구분되는 소셜 토큰은 소셜파이 생태계에서 중추적인 역할을 하며 사용자, 커뮤니티, 소셜 플랫폼 모두에게 다양한 상호작용과 경험을 가능하게 한다는 특징

- **(개인 토큰)** 유명인(예술가, 기업가, 크리에이터 등)이 팬 커뮤니티와 소통하고 육성하는 데 주로 사용

- 사용자는 자신의 이름으로 개인 토큰을 만들고, 가격 구조를 설정하고, 팬층에 배포할 수 있으며, 개인 토큰을 소유하면 팬들은 사용자가 공개하는 비공개 그룹이나 독점 콘텐츠에 액세스할 수 있음

- **(커뮤니티 토큰)** 개인 토큰과 유사하지만 개인 대신 특정 커뮤니티를 위한 토큰으로 특정 커뮤니티의 구성원을 묶어 참여 특권을 제공하고 커뮤니티 전체의 성장과 발전에 기여

- **(소셜 플랫폼 토큰)** 소셜 플랫폼 자체에서 발행하는 토큰으로 기업은 담보, 잠금(locking) 메커니즘, 커뮤니티 거버넌스 등 다양한 목적으로 이러한 토큰을 활용
  * 예를 들어, 탈중앙화된 음악 플랫폼인 오디우스(Audius)에서는 사용자가 시스템 기능에 액세스하고 이를 활용하는 데 사용할 수 있는 오디오(AUDIO) 토큰을 발행

- 소셜파이는 끊임없이 진화하는 웹3 기술 환경에서 유망한 분야로, 소셜 작용, 콘텐츠 제작, 커뮤니티 참여에 대한 새로운 접근 방식을 제공
- 소셜파이는 아직 초기 실험 단계로서, 업계의 장기적인 생존을 위해서는 참여자간 영향력 격차, 블록체인의 확장성, 지속 가능한 수익 모델 구축 등의 극복 과제를 해결할 필요성

[출처]

- Cryptopolitan 'Exploring the world of SocialFi: Bridging social media and DeFi in Web3', 2023.11.22.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

'24년 이후 자산 토큰화의 전개

- 암호자산 시장의 암흑기를 지나 세계 각국 정부와 규제 당국이 실물 자산을 바라보는 시각이 바뀌고 있음
- 실물 자산의 토큰화가 향후 모든 산업에서 가치의 이전, 결제, 저장 방식을 재편할 수 있을 것으로 예상

각국 정부가 암호자산의 변동성에 대한 노출을 줄이면서도 향상된 유동성, 부분 소유권, 글로벌 접근성과 같은 블록체인 기술의 이점을 모색하면서 민간뿐만 아니라 공공 부문에서도 토큰화에 대한 관심이 눈에 띄게 증가

▶ 실물 자산의 토큰화..최근 전 세계 관할권에서 블록체인 기술을 활용하기 위해 규제 변화를 고려하는 상황

- '18-'19년 암호자산 시장의 암흑기를 겪으며 금융 기관 간 암호자산 부문에 대한 회의론과 거부감이 지배적이었으나, '24년에 가까워지면서 눈에 띄는 변화가 감지되고 있음
- 정부와 규제 기관이 블록체인 기술의 이점을 활용하면서도 시장 위험을 줄일 수 있는 방안을 모색하기 시작하면서 토큰화가 매력적인 방안으로 점점 더 많이 인식되고 있음
- 글로벌 시장 조사 기관인 보스턴 컨설팅 그룹(Boston Consulting Group)은 '30년까지 자산 토큰화 시장이 수조 달러 규모의 시장이 될 것으로 예측
- 실제 작년 몇몇 금융 강국들은 귀금속, 예술품, 부동산과 같은 고가치 자산의 소유권을 블록체인에 통합하여 실물 자산을 토큰화하는 개념을 받아들임
- 투자자뿐만 아니라 은행 및 정부도 제도적 프레임워크 내에서 토큰화 금융 상품의 사용을 점점 더 많이 고려하고 있는 가운데 주목할만한 점은 인프라 선택에 있어 다수가 퍼블릭 블록체인을 채택하고 있다는 것
- 이러한 결정은 탈중앙화 네트워크 보안과 잠재력에 대한 신뢰가 커지고 있음을 보여주는 것으로, 몇 년 전의 우려 분위기와 대조적이라고 할 수 있음
- 올해 뱅크 오브 아메리카(Bank of America)가 발표한 연구에 따르면 실물 자산의 토큰화가 '디지털 자산 채택의 핵심 동인'이며, 향후 모든 산업에서 가치의 이전, 결제, 저장 방식을 재편할 수 있을 것으로 예상
- 완전한 디지털 자산 수용까지는 더 많은 시간이 필요할 것으로 보이나, 최근 전 세계 관할권에서 각자의 필요에 따라 실물 자산 토큰화의 활용 및 출시를 위한 규제 변화를 고려하는 상황을 목격하고 있음

- 웹3의 진화로 인해 블록체인 기술은 우리 일상 생활에 더 깊숙하게 통합될 것으로 예측되며, 각국 정부도 새로운 수익원 창출과 비용 절감을 위해 블록체인 기술의 활용에 관심을 갖고 있음
- 상품, 주식, 부동산 등 실물 자산의 토큰화는 민간 및 공공 부문 모두에서 블록체인 기술의 이점을 얻을 수 있는 유용한 방안으로 인식되고 있으며, 보다 적극적으로 토큰화 활용을 구체화할 것으로 예상

[출처]

• Forkast, 'What asset tokenization will look like in 2024 and beyond', 2023.11.20.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[글로벌]

계정 추상화 개념을 롤업 생태계에 통합시키려는 이더리움 네트워크의 노력

- 이더리움 재단의 알렉산더 포셋(Alexander Forshtat)이 롤업 솔루션에 최초로 계정 추상화 개념 도입을 제안
- L1과 L2 환경을 통합하여 보다 효율적인 생태계를 만드는 데 매우 중요한 역할을 수행할 것으로 기대

사용자 계정과 스마트 컨트랙트를 원활하게 통합하여 이더리움 네트워크 내 전반적인 기능과 사용자 경험을 향상시키는 계정 추상화*는 올해 3월 메인넷에서의 구현을 기반으로 L2 롤업 솔루션에도 확장될 예정

* 계정 추상화(Account Abstraction, AA): 외부 소유 계정(externally owned account)과 계약 계정(contract account)으로 구분되어 있는 기능을 통합시켜 트랜잭션 전송, 지갑 관리 등 계정의 다양하고 복잡한 동작을 단순화시키는 것

▶ 이더리움의 '네이티브 계정 추상화 도입을 위한 로드맵'...운영 간소화, 지속적인 생태계 개발 촉진 가능

- 이더리움은 계정 추상화(AA)를 롤업(rollup)* 생태계에 통합하는 노력을 하고 있으며, 이는 레이어 2(L2) 솔루션에 계정 추상화를 통합하려는 첫 번째 시도로 주목
  * 롤업: 이더리움 L2에서 여러 개별적인 트랜잭션들을 처리하고 그 결과값들을 하나로 묶은 뒤 L1에 저장하는 기술

- '23년 3월, 이더리움 메인넷에 계정 추상화 기능이 배포되었으며, 이를 통해 새로운 종류의 스마트 컨트랙트 계정을 위한 길을 열고, 탈중앙화 앱(dapp)의 환경을 혁신할 것으로 기대

- 이더리움 L2 롤업 솔루션으로 계정 추상화 기능이 확장되면 L1과 L2 환경을 통합하여 보다 응집력 있고, 효율적인 생태계를 만들고, 운영을 간소화할 수 있게 됨으로써 웹3 부문의 지속적 발전을 촉진할 것

- 롤업에서 계정 추상화 기능을 성공적으로 구현하기 위해서는 엔트리포인트 주소(EntryPoint Address) 변경, 유효성 검증 사용자 작업 함수(validateUserOp function) 재작성, 트랜잭션 로직 개선과 같은 세 가지 주요 수정이 필요

- 해당 제안서의 작성자는 네이티브 계정 추상화의 표준화 과정에서 커뮤니티의 참여 중요성을 강조하고 있으며, 커뮤니티와의 협력은 L1 및 L2 네트워크에서 계정 추상화의 성공적인 채택과 효과를 위해 필수적

- 이더리움 커뮤니티는 이번 개발에 상당한 피드백과 기여를 제공하며 높은 관심을 보였고, 이러한 적극적인 참여는 계정 추상화의 발전 중요성과 블록체인 부문에 미칠 잠재적 영향이 클 것을 짐작할 수 있음

- 이더리움은 지속적인 기술 도약을 토대로 블록체인과 탈중앙화 시스템의 미래 형성에 중요한 역할을 담당할 것으로 전망

- 이더리움이 최초로 계정 추상화를 L2 롤업 생태계에 통합하려는 시도는 현재 진행 중인 이더리움의 진화에 있어 큰 진전을 의미하는 것으로 커뮤니티도 높은 관심과 적극적인 참여를 보이고 있음
- 이더리움 L1 및 L2에 계정 추상화가 성공적으로 구현되면 이더리움 네트워크 확장성과 기능을 향상시키고 보다 사용자 친화적인 경험을 제공할 수 있을 것으로 전망됨

[출처]

- Cryptopolitan, 'Ethereum unveils game-changing account abstraction in rollups', 2023.11.19.

블록체인 기술·정책·산업 동향

디지털산업본부 블록체인산업단 블록체인정책팀

[미국]

바이낸스, 막대한 과징금 납부와 규정 준수 약속으로 새로운 출발 강조

- 바이낸스는 성명을 통해 미 법무부 및 기타 기관의 조사 결과와 관련, 잘못을 인정하고 새출발 의지를 보임
- 고객 신원 확인 제도 및 IP 차단 시행, 법 집행기관과의 협력, 정보 공유를 위한 팀 구성 등 노력 강조

글로벌 최대 암호자산 거래소 바이낸스(Binance)는 미국 금융서비스업 등록 불이행, 은행보안법(BSA) 위반, 국제비상경제권법(IEEPA) 위반 관련 재판에서 유죄를 인정하고, 43억 달러 상당의 벌금을 내기로 연방 정부와 합의

▶ 미국 역사상 가장 큰 규모의 기업 과징금 납부...이에 더해 조직 구조 개편과 엄격한 규정 준수를 약속

- 바이낸스는 미국 법무부로부터 금융법 위반 등으로 43억 달러의 과징금을 부과받은 가운데, 최근 성명에서 법무부 및 기타 기관의 조사 결과와 관련하여 과거 규정 준수 위반에 대한 자사의 잘못을 인정하고, 새로운 출발을 위해 마련한 자구책을 발표(11.21.)

- 바이낸스는 사용자 자금 유용과 시장 조작 관여에 대한 혐의는 없다고 강조하며, 사용자 자산에 대응하는 1:1 지원, 항상 100% 인출 허용, 자체 암호자산 주소에 대한 투명성 등에 대해 약속

- 덧붙여 최근의 구조조정 노력과 준법감시 관련 리더십을 보강한 사실을 설명하고, 바이낸스 설립자이자 CEO였던 창펑 자오(Changpeng Zhao)의 사임* 후 차기 CEO로 바이낸스 지역 총괄인 리처드 텡(Richard Teng)을 선임한다고 밝힘
  * 법무부와의 합의에 따라 창펑 자오는 3년 동안 바이낸스 운영에서 공식적으로 물러나지만 보유 지분은 유지

- 신임 텡 CEO는 X에서 지난 30년간 금융 서비스 및 규제 기관에서의 경험을 바탕으로 ▲사용자들이 회사의 재무 건전성, 보안, 안전성에 대해 안심할 수 있도록 하고 ▲규제기관과 협력하여 혁신 촉진과 소비자 보호를 제공하는 높은 기준을 유지하며 ▲웹3 성장과 채택을 촉진하는 데 집중할 것이라고 언급

- 한편 바이낸스는 금융서비스업 등록을 하지 않아 효과적인 자금세탁방지(Anti Money Laundering, AML) 정책을 수립하지 않았다는 법무부의 주장에 관해서는 최근 AML 도구와 기능을 확장했다고 언급

- 또한 국제비상경제권법(IEEPA)을 위반해 사용자가 제재 대상 사용자 및 제재 지역의 사용자와의 거래를 통제하지 않았다는 혐의에 대해서는 독립적 제재 팀 운영, 고객확인제도(KYC)와 IP 차단 시행, 타사 도구 사용 실시간 거래 모니터링, 법 집행기관과 협력하고 정보를 공유하는 전문 팀 보유 등을 강조

- 바이낸스는 구체적인 혐의에 대해 이의를 제기하지 않고 유죄를 인정하였으며, 40억 달러가 넘는 과징금을 납부하고, 3년 간의 모니터 요원을 고용하며, 규정 준수를 개선하는 데 동의
- 또한 규제 기관에서의 오랜 경력을 보유한 새로운 CEO 선임을 통해 사용자 신뢰 개선, 규제 준수 강화와 동시에 웹3 시장 확대에 집중하며, 새로운 페이지로 나아가겠다는 의지를 내보이고 있음

[출처]

- Cointelegraph, 'Binance names Richard Teng CEO amid Changpeng Zhao's forced departure', 2023.11.21.
- Cryptoslate 'Binance's new chapter begins with hefty fines and compliance commitments', 2023.11.22.