Market Analysis Report

2023-3-3

코어닥스 리서치센터

Hot Issue

제로지식증명(Zero-Knowledge Proofs)에 대한 이해

가상자산 시장동향

비트코인 : 2022년 8월 전고점인 3,300만 원을 돌파하지 못하고 조정이 나오고 있는 상황이며, 미국의 경제지표 등 시장 여건에 따라 추가 조정 가능성

- MACD, TSI 등 기술지표들도 하락 추세 전환을 보이고 있어 하락장이 장기화될 가능성 있음.
- 미 연준의 매파적 행보가 강화될 것이라는 우려와 함께 미국 증권거래위원회의 가상자산에 대한 규제 리스크 확대로 약세장 지속 전망

이더리움 : 전고점 240만 원 돌파 못하고 조정장 형성

- 다양한 호재에도 가격 상승이 제한적이어서 당분간 약세장이 지속될 것으로 전망

폴리곤 : 2,000원 돌파 후 차익매물 출현 및 가상자산 시장의 전반적 약세에 따라 하락장 전환

- 기술지표들의 급격한 하락으로 조만간 과매도 구간 진입 예상

코어닥스 소식

시장감시 및 투자자보호 강화 위해 박시덕 후오비코리아 전 대표 영업

제로지식증명(Zero-Knowledge Proofs)에 대한 이해

김진원 상무이사(kjw99016@coredax.com)

폴리곤의 영지식증명 이더리움 가상머신 등의 사례와 같이 영지식증명(Zero-Knowledge Proofs)은 블록체인 커뮤니티에서 뜨거운 화제가 되어 왔다. 암호화의 도구로서 영지식증명은 분산화 되고 입증 가능하며, 사적인 통신을 위한 강력한 요소이다. 영지식증명의 사용 방법과 실제로 개인정보를 보존하는지는 제품의 사용 사례와 구현에 의해 크게 좌우된다.
이 글에서는 영지식증명의 개념, 롤업(rollup), ZK-VM 및 ZK-EVM과 같은 다양한 사용 사례에 대해 알아보고자 한다.

1) 영지식증명 소개(Zero-Knowledge Proof Intro)

□ 영지식증명은 당신이 무언가를 알고 있다는 것을 증명하는 방법이며, 영지식증명의 우수성은 증명 생성 자체보다는 검증의 편의성에 있음.

- 영지식증명은 당신이 알고 있는 것이나 거래가 무엇이었는지가 아니라 당신이 알고 있거나 거래가 옳다는 것을 증명함.
- (사례) 20개의 질문게임: 당신이 알고 있는 비밀단어를 추측하려고 하는 누군가와 게임을 하고 있는 경우
  - 일반적으로 본인이 알고 있는 단어를 말해야 하지만, 알고 있는 단어를 밝히지 않고도 그 단어를 알고 있다는 것을 증명하는 방식
  - 즉, 알고 있다는 것을 증명하기 위해 답이 무엇인지를 밝히기보다는 답을 알고 있다는 것을 증명하는 암호화된 증거를 제시

□ 암호학 및 컴퓨터 과학에 있어 영지식증명은 개인정보 보호 강화 및 스케일일, 투표 시스템, 디지털 시원확인 등 다양한 응용프로그램에서 사용 가능

□ 영지식으로 간주되는 요건은 완결성(completeness), 건전성(soundness), 영지식(zero-knowledge)임.

- 완결성: 진술이 참이면 검증자는 납득을 하고 추가적인 증거나 입증작업을 할 필요가 없음.
- 건전성: 진술이 거짓이면 아무리 부정행위를 해도 검증자를 설득할 수 없음.
- 영지식: 정보가 유출되지 않고 검증자가 배우는 모든 것은 그 진술이 사실이라는 것임.
- 여기서 중요한 특징은 정부가 유출되지 않고 주어진 진술의 정당성만 입증하면 된다는 것임.
- 즉, 내가 학생이고 학생 할인을 받을 자격이 있다는 것을 증명하고 싶다면, 검증자가 알게 되는 정보는 '학생 할인을 받을 자격이 있다'는 것 뿐임.

2) 블록체인 확장

□ 스케일링(Scaling)은 네트워크가 더 많은 연산자를 추가하여 인프라의 처리 능력을 높일 수 있는 능력을 의미

- 하지만 분산형 네트워크에서 노드(운영자)의 수가 증가하면 트랜잭션을 처리하는 용량이 훨씬 느려지고 비용이 증가하는 문제가 발생함.
- 또한 블록체인이 확장되지 않으면 속도가 느리거나, 비싸지거나, 심지어 최대 부하 과정에서 충돌이 발생할 수 있음.

□ 블록체인을 확장하는 데 사용할 수 있는 솔루션에는 여러가지 유형이 있음.

- 한 가지 접근법은 레이어 2(L2) 스케일링으로 알려져 있으며, 이는 레이어 1(L1)으로 알려진 메인 블록체인으로부터 트래픽을 리디렉션하기 위한 보조원장을 만드는 것을 포함함.
- L2 스케일링 솔루션은 결제 계층(주 계층 또는 L1)을 혼잡하게 하지 않고 블록체인으로 처리할 수 있는 거래량을 늘리는 것을 목표로 하며, 이를 위해 상태채널(State Channels), 롤업(Rollups), 플라즈마(Plasma), 사이드체인(Sidechains) 및 Validium/Volition 등 다양한 아키텍처를 제시함.
- 이러한 아키텍처들은 병렬로 트랜잭션 배치를 처리하는 것을 포함한 소위 네트워크 분할 전략이며, 가장 인기 있는 분할 전략은 샤딩임.

□ 샤딩은 메인 블록체인을 샤드라고 불리는 더 작고 관리하기 쉬운 조각으로 나누는 것을 의미함.

- 각 샤드는 네트워크 트랜잭션의 하위 집합을 처리하여 전체 네트워크의 속도와 효율성을 향상시키며, 이러한 하위집합은 근접성, 처리 유사성 또는 랜덤 분포를 기반으로 생성되어 워크로드의 균형을 맞춤.

3) 롤업 및 ZK

□ 롤업은 블록체인에서 가장 인기 있는 스케일링 솔루션 중 하나이며, 많은 수의 오프체인 트랜잭션을 집계한 다음 모든 오프체인 트랜잭션을 나타내는 메인 블록체인에 단일 트랜잭션을 제출하는 방식으로 작동함.

□ ZK 롤업 또는 영지식 롤업은 영지식증명을 사용하여 추가적인 보안 보장을 제공하는 특정유형의 롤업임.

- ZK 롤업에서 트랜잭션은 롤업에 의해 함께 번들되고 메인 체인의 스마트 계약에 의해 처리됨.
- 증명기(prover)는 거래가 유효하다는 증거를 생성하며, 이후 이 증명은 증명을 검증하는데 필요한 소량의 추가 데이터와 함께 메인 블록체인에 제출됨.
- 대부분의 ZK 롤업은 검증의 효율성을 위해 영지식증명을 사용하여 유효성을 검증하며, 영지식증명의 완결성과 건전성 속성을 사용하기 때문에 트랜잭션 해시에서 트랜잭션의 모든 정보를 공유하지 않음.

4) 가상머신(Virtual Machine)

□ 가상머신(Virtual Machine, VM)은 컴퓨터를 에뮬레이터하는 소프트웨어 프로그램으로 사용자가 시뮬레이션된 환경서 프로그램을 실행할 수 있도록 함.

- 개발자들은 코드를 실행하는 물리적 하드웨어에 대한 걱정 없이 VM에서 프로그램을 실행할 수 있음.

□ 이더리움 가상머신(Ethereum Virtual Machine, EVM)은 이더리움과 호환되는 블록체인에서 스마트 계약을 실행하는 특정 유형의 가상머신임.

- 스마트 계약은 디지털 자산 관리, 디지털 신원 확인, 금융계약 실행 등 다양한 업무를 수행할 수 있는 자체 실행 프로그램임.

□ ZK-EVM은 영지식증명을 사용하여 스마트 계약 실행을 위한 추가적인 보안 보증을 제공하는 EVM의 특별 버전임.

- ZK-EVM에서 영지식증명은 스마트 계약이 올바르게 실행되었는지 확인하는데 사용되며, 이는 현재 활성화된 대부분의 ZK 롤업에서 큰 문제가 되었음.
- 많은 ZK 롤업들이 기존 이더리움 툴링과 생태계를 활용해 스마트 계약을 구축하지 못하고 대신 스마트 계약을 지원하기 위해 자체 언어와 VM을 구축해야 하였음.
- ZK-EVM은 이를 해결하고 EVM 사양에 따라 스마트 계약이 올바르게 실행되었음을 증명하기 위해 설계되었으며, 이 과정에서 영지식증명은 임의의 EVM 명령이 정확한 계산을 확인하는데 사용됨.

□ 결론적으로 영지식증명은 보다 효율적인고 안전한 시스템을 가능하게 함으로써 블록체인 산업에 상당한 영향을 미치고 있음.

- 프라이버시와 확장성을 향상시킬 수 있는 잠재력을 가진 영지식증명이 앞으로 블록체인 지형을 어떻게 지속적으로 형성할 것인지 주목할 필요가 있음.

가상자산 시장 모니터

Bitcoin 대 KRW 차트

가격 시가총액 TradingView

〈자료: CoinMarketCap〉

■ 2023년 들어 상승 랠리를 나타내고 있으나 2022년 8월 전고점인 3,300만 원을 돌파하지 못하고 조정이 나오고 있는 상황이며, 미국의 경제지표 등 시장 여건에 따라 추가 조정 가능성

1) MACD, TSI 등 기술지표들도 하락 추세 전환을 나타내고 있어 하락 조정장이 장기화될 가능성도 있음.
2) 더욱이 미 연준의 매파적 행보가 한층 강화될 것이라는 우려와 함께 미국 증권거래위원회(SEC)의 가상자산에 대한 규제 리스크 확대로 약세장 지속 전망

〈상승 요인〉

1) BTC 기반의 NFT 생성을 가능하게 하는 오디널스 프로토콜(Ordinals Protocol) 등장으로 비트코인 블록체인을 기반으로 한 새로운 고부가가치 활용 가능성

〈하락 요인〉

1) 미국 가상자산거래소 크라켄, 미등록 서비스 제공 혐의로 SEC와 스테이킹 서비스 중단 및 벌금 3천만 달러 지급 합의와 함께 뉴욕금융감독국(NYDFS)의 팍소스 조사 등 규제 리스크 확대
2) 3월 14일 발표예정인 미국 소비자물가지수(CPI)에 따라 미 연준의 매파적 행보 강화 우려

가상자산 시장 모니터

Ethereum 대 KRW 차트

가격 시가총액 TradingView

〈자료: CoinMarketCap〉

■ 전고점인 240만원을 돌파하지 못하고 조정장이 형성되고 있으며, 다양한 호재에도 가격 상승 움직임이 제한적으로 당분간 약세장이 지속될 것으로 예상

1) 기술지표들의 하락 추세 전환 및 미국발 긴축경제 공포로 인해 조정 하락장이 이어질 것으로 전망

2) 1월 고용지표 호조와 인플레이션 고착화 조짐에 이어 경제회복에 대한 불확실성이 높아지는 가운데 2월 고용보고서에 따라 매파적 경제운용 정책이 강화될 것으로 보임.

〈상승 요인〉

1) 이더리움은 경쟁우위, 성장 모멘텀, 시장 리더십 등으로 가상자산 약세장을 극복해 나가고 있으며, 2023년 성장을 통해 디파이 시장을 주도할 것으로 예상

2) 미국 시카고상품거래소(CME)의 이더리움 파생상품 월간 거래량이 지속적으로 증가하고 있으며, 최근 약세장에도 불구하고 가상자산 거래소에서의 순유출이 나타나고 있음.

〈하락 요인〉

1) 미국 뉴욕검찰의 쿠코인 기소와 함께 이더리움을 미등록 증권으로 해석하는 등 규제 리스크 확대

가상자산 시장 모니터

Polygon 대 KRW 차트

가격 시가총액 TradingView

〈자료: CoinMarketCap〉

■ 2월 18일 2,000원을 돌파하였으나 이후 단기 급등에 따른 차익매물 출현 및 가상자산 시장의 전반적 약세 흐름에 따라 하락하며 조정이 나오고 있음.

1) 기술지표들은 급격한 하락세를 보이고 있으며, 조만간 과매도 구간에 진입할 것으로 보이며 1,300원 지지대 형성 여부가 향후 가격 흐름에 중요한 역할을 할 것으로 보임.
2) 레이어2의 경쟁 심화, 네트워크 속도, 인플레이션, 대형 투자자에 대한 지나친 편중도 가격 하락의 요인으로 작용할 가능성

〈상승 요인〉

1) 폴리곤 가격이 상승세를 이어가는 동안 대형 투자자인 고래들의 대규모 매수세 지속
2) 3월 27일 영지식증명을 탑재한 '영지식증명 이더리움 가상머신' 메인넷 베타 오픈 예정

〈하락 요인〉

1) 레이어2 프로젝트의 다양성 등에 따른 경쟁 심화와 함께 폴리곤 스테이킹 확대에 따른 유동성 부족으로 인한 가격 하락 가능성

가상자산 시장 모니터

□ 2023.2.25~2023.3.3 주요 가상자산 지표

가상자산	가격(₩)	7d%	7일 거래량(₩)	도미넌스
Bitcoin (BTC)	29,190,667.24	▼6.47%	148,599,902,938,172	42.06%
Ethereum (ETH)	2,045,969.37	▼5.24%	57,513,257,394,524	18.70%
Tether (USDT)	1,301.66	▼0.32%	306,911,525,639,782	6.92%
BNB (BNB)	379,157.91	▼6.73%	3,371,676,264,252	4.47%
USD Coin (USDC)	1,301.48	▼0.33%	26,086,802,489,399	4.20%
XRP (XRP)	476.56	▼6.26%	4,388,026,263,348	1.81%
Cardano (ADA)	439.99	▼11.80%	2,270,183,988,978	1.14%
Polygon (MATIC)	1,525.53	▼13.15%	4,415,525,711,445	0.99%
Dogecoin (DOGE)	98.78	▼10.66%	2,793,841,780,478	0.98%
Binance USD (BUSD)	1,301.78	▼0.32%	59,418,343,060,993	0.94%

자료 : CoinMarketCap, 2023년 3월 3일 18시 기준

코어닥스 소식

1 시장감시 및 투자자 보호 강화 위해 후오비코리아 박시덕 전 대표 영입

- 코어닥스는 시장감시 및 투자자 보호를 강화하기 위해 후오비코리아 박시덕 전 대표를 시장감시위원장으로 영입
- 빅시덕 시장감시위원장은 국민은행 및 후오비코리아 재직 경험을 살려 개인정보 보호와 함께 시장감시 및 내부통제 역량을 키워 투자자 보호를 강화하겠다고 밝힘.