AEGIS VENTURES | 2024. 9. 12

Lumoz Network Review (2)
Part 2. Lumoz, ZK-RaaS 모듈식 컴퓨어 레이어

Index

Ⅰ. 들어가며

Part 1에서는 Lumoz Network의 기술적 기반을 이해하기 위해 영지식 증명(ZKP)과 ZK-Rollup의 개념을 심도 있게 다뤘습니다. ZKP는 검증자에게 중요한 정보를 직접적으로 제공하지 않으면서도 해당 정보를 보유하고 있음을 증명할 수 있는 방법으로, 퍼블릭 블록체인의 투명성과 프라이버시 보호를 동시에 달성하는 데 핵심적인 역할을 합니다. 또한, ZK-Rollup은 이러한 ZKP 기술을 활용해 Layer-2 솔루션으로서 블록체인의 확장성 문제를 해결하며, 비용 효율성을 크게 향상시키는 방법으로 주목받고 있습니다.

Part 2에서는 이러한 배경을 바탕으로, Lumoz Network가 ZK-RaaS(Zero-Knowledge Rollup as a Service) 솔루션을 통해 어떻게 모듈러 컴퓨팅을 구현하며, 다양한 블록체인 간의 상호운용성을 강화하는지, 그리고 ZK-Verifier 노드의 운영을 통해 네트워크의 보안성과 확장성을 어떻게 극대화하는지에 대해 자세히 살펴볼 것입니다. 특히, Lumoz의 독자적인 PoW/PoS 혼용 합의 알고리즘, Cross Roll-up, 그리고 ZK-Verifier Node의 판매 구조를 중심으로 Lumoz Network의 주요 특징을 분석할 것입니다.

II. Lumoz Network

가. Lumoz Network Overview

- Purpose : 탈중앙화 모듈러 컴퓨팅 네트워크 서비스 (ZKP, AI)
- Type : Node Service (for ZKP, AI)
- Token Ticker : MOZ, esMOZ(Incentive Point)
- Consensus Algorithm : PoW & PoS 혼용 합의구조
  - PoW : 증명 생성, PoS : 증명 검증
- Service
  - 모듈러 컴퓨팅 레이어를 이용한 Proving
  - Roll-up 간의 상호 운용성 강화 (Cross Roll up)
  - ZkVerifier Node 재판매

나. Lumoz Network, ZK-RaaS 모듈식 컴퓨어 레이어

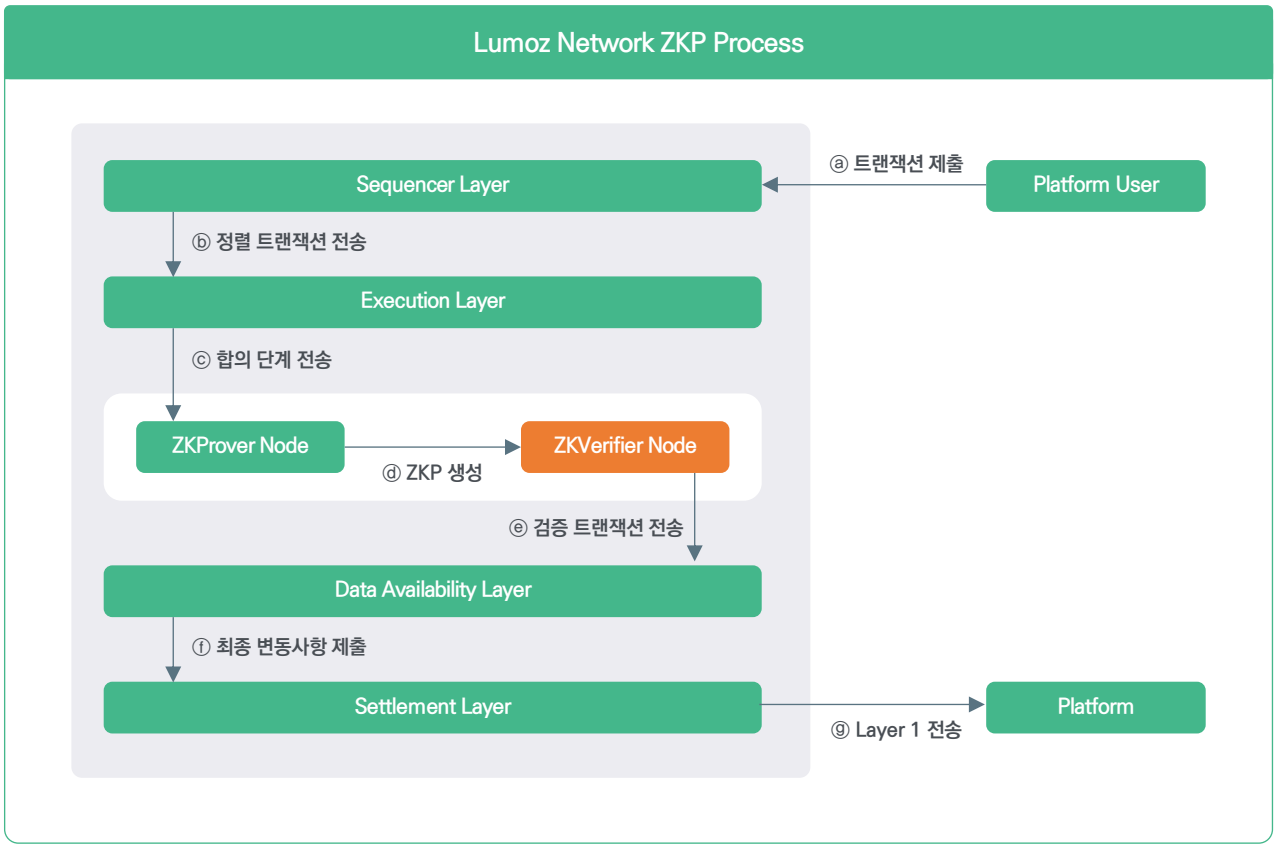
Lumoz Network는 ZK 인프라를 위한 ZK-RaaS 솔루션으로 모듈러 컴퓨팅(Modular Computing)을 기반으로 다양한 Layer-1에 대한 Roll Up을 제공합니다. 뿐만 아니라, zkEVM 기능을 제공하여 EVM을 지원하는 다른 Public Blockchain에 대한 접근을 더욱 용이하게 해줍니다. 서비스의 고객이 서로 다른 체인 간의 Roll up이 필요할 경우, 다종 체인에 대해 기 배포한 "Roll up System Contract" (이하 "RSC")[1]를 통하여 Lumoz Chain을 경유한 Cross roll-up 기능을 제공하여 사용자 편의성을 개선합니다.

Lumoz Network의 특이점은 Miner에 대해 PoW 합의 구조를 이용한 ZKP의 "증명생성"을 수행한다는 점과 Prover가 생성한 증명을 바탕으로 ZK-Verifier로 선정된 개별 노드들의 "검증"이 이루어진다는 점입니다.

Lumoz Network의 수익구조는 이 중 "검증" 부분을 담당할 Zk-Verifier 노드의 1) 라이선스를 판매하는 부분, 2) ZKP 혹은 AI와 관련한 내부 수수료 발생 등이 있습니다.

1 다양한 체인 간 Roll-up 기능을 제공하기 위해 배포된 스마트 계약

Ⅲ. Lumoz ZKP Modular Computing Process



Lumoz Network의 ZKP과정은 다음 6개의 단계로 이루어집니다.

ⓐ **트랜잭션 제출**: ZK 서비스의 사용자는 자신이 블록체인상에서 수행한 활동(Transaction)을 시퀀서 레이어[2]로 제출

ⓑ **정렬 트랜잭션 전송**: 시퀀서 레이어의 시퀀서[3]는 제출된 활동을 수집 및 정렬하여 블록화

ⓒ **Consensus Layer 제출**: 정렬된 활동을 롤업 블록으로 종합한 뒤 이를 ZK-Prover Node에게 전송

ⓓ **ZKP 생성**: ZK-Prover Node는 전송받은 활동에 대해 ZKP를 생성하여 ZK-Verifier Node에게 전송

ⓔ **검증 트랜잭션 전송**: ZK-Verifier는 ZK-Prover로부터 전송받은 ZKP를 검증한 뒤 이를 데이터 가용성 레이어[4]로 전송

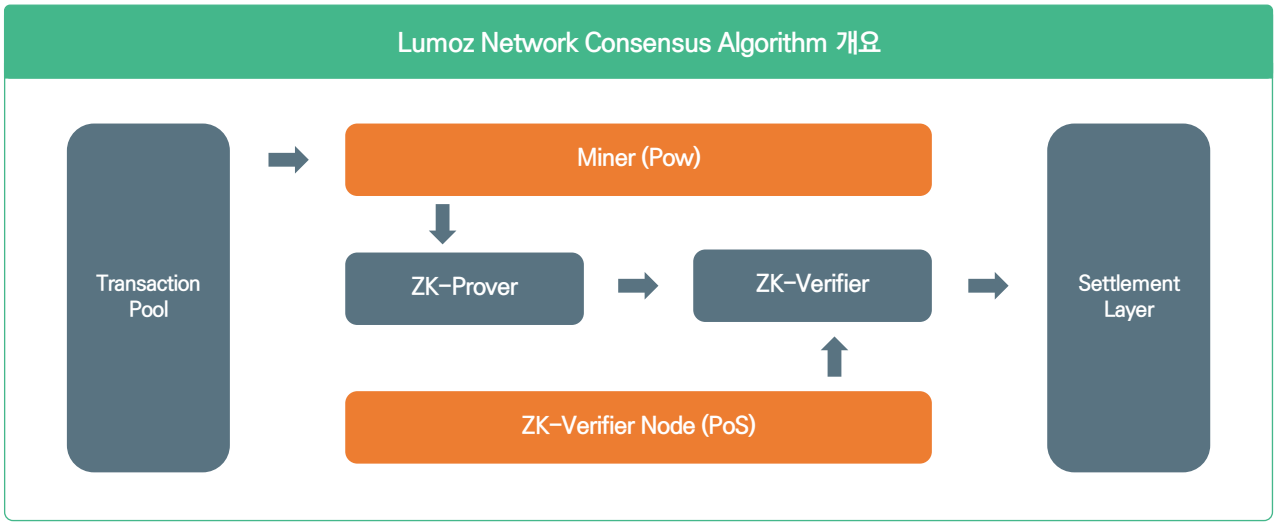
ⓖ **Layer 1 기록:** Settlement Layer에서는 전송받은 검증된 활동내역을 시퀀서를 통하여 Layer 1인 메인체인에 이전

위의 6개의 사이클을 경유하여 발생 ZKP 활동에 대한 내용들을 Platform에 기록합니다.

2 트랜잭션을 수집하고 정렬하는 역할을 하는 블록체인의 레이어
3 트랜잭션을 수집, 정렬, 블록화하는 역할을 담당하는 노드
4 검증된 트랜잭션 데이터를 저장하고 접근 가능하게 하는 레이어

Ⅳ. Lumoz Network의 특징

가. 독자적인 PoW/PoS 혼용 합의 알고리즘



Lumoz Network의 합의 알고리즘에서 독특한 점은 **PoW/PoS를 혼용**하여 사용한다는 점입니다. Lumoz Network의 독특한 혼합 합의 알고리즘은, ZKP 특유의 대량 연산을 손쉽게 만들고 검증결과에 대한 보안성을 강화시키는데 기여합니다.

두 합의 알고리즘 중 PoW는 ZK-Prover를 대상으로 하고, PoS는 ZK-Verifier를 대상으로 하는 알고리즘입니다. ZKP의 과정에서 필수적인 과정은 "ZKP 증명을 생성"하고 생성된 증명을 "검증"하는 과정입니다. 해당 과정을 통해서 적절하게 검증되었다고 판단되는 활동들을 종합해서 Lumoz Chain에서 Layer-1으로 해당 활동을 이전하는 과정을 거칩니다.

여기서 "증명을 생성"하는 과정은 많은 컴퓨팅 파워가 요구됩니다. 통상 Layer-1에서의 PoW의 과정은 특정한 문제를 해결하고 이에 따른 블록 생성 권한을 얻어, 1) 채굴 보상 2) 수수료 보상을 수취하는 구조입니다. 하지만 Lumoz Network에서의 PoW는 증명 생성자(이하 "Miner")에 대해 증명의 생성에 기여한 것에 대한 보상 및 합의의 과정입니다. PoW는 2단계로 이루어집니다. Lumoz Network 상에서 Miner가 일정 시간 동안 컴퓨팅 파워를 투입하여 proofhash(proof/address 결합 형태)[5]를 생성합니다. 기간 경과 후 원본 증명에 대해 검증하고 프로토콜은 해당 Miner에 대해 지분에 따른 esMoz Token을 분배합니다.

"검증"의 단계는 생성된 증명을 검증하는 과정입니다. Lumoz Network의 검증 단계는 통상적인 Layer-1의 PoS 구조(2/3 이상의 합의)에서와 같이, 개별 노드 ZK-verifier 노드들에 대해 1) 생성된 증명을 2) 지분 규모에 따라 3) 검증을 수행하고 이에 따라 esMoz를 분배 받습니다.

5 증명 데이터와 주소를 결합하여 생성된 해시 값

나. Cross Roll-up을 통한 상호운용성 강화

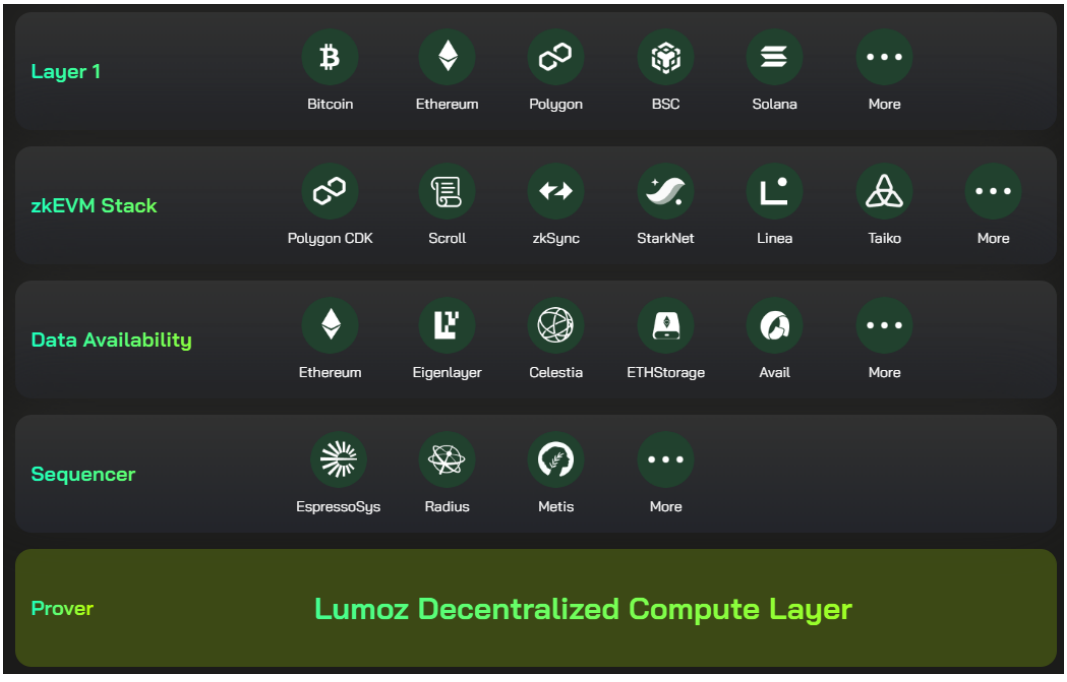
Cross Roll-up은 서로 다른 Roll-up 플랫폼 간의 상호운용성을 강화시켜주는 기능입니다. 이를 위해서는 다음의 기능이 요구됩니다.

- 크로스체인 브릿지
- 메세징 프로토콜
- 데이터 가용성 레이어
- 검증 및 합의 레이어
- 트랜잭션 라우팅

위의 기능을 통해 Roll-up A 플랫폼의 사용자가 Roll-up B 플랫폼으로 특정 가상자산을 이전할 수 있습니다. 크로스 체인 브릿지에서 특정 가상자산을 Wrapping하여 이를 Roll-up B로 전송하고, B에서 랩핑된 자산과 대응되는 자산을 생성하여 거래하는 구조입니다.

Lumoz Network는 Cross Roll-up을 위한 개별 기능들을 갖추고 있어 Cross Roll-up을 지원합니다. 또한 다른 프로젝트에서 갖고 잊지 못한 "Lumoz Decnetralized Compute Layer"를 레이어로 두고 있습니다. 이는 타 Roll-up 프로젝트가 갖지 못한 기능으로, Roll-up 시장 일반에서 발생하는 활동을 더 효율적으로 처리할 수 있습니다. 특히 이런 특징은 개발자들로 하여금 손쉽게 Lumoz Network를 통해 개발할 수 있는 환경을 제공합니다.

ZKP Modular Stack



다. ZK-Verifier Node

Lumoz Network의 ZKP 검증 노드는 PoS 형태를 취하고 있습니다. ZKP의 결과에 대한 검증은 라이선스 판매를 통해 구성된 ZK-verifier 집단의 2/3 이상의 동의로 이루어집니다. (PoS)

라이선스 구매 → 도커 설치 → 운영

V. Lumoz ZK-Verifier Node Sales

가. Lumoz ZK-Verifier Node Sales Conditions

판매 조건	수량	내용
OKX Launchpad	800개	Tier 4 단계 수준에 해당하는 가격으로 특정 활동을 수행할 경우 노드 라이선스를 인수할 수 있는 권한이 발생
Public Sales Round	9,200개	개당 200USD(Tier 1)에서 시작하여 개당 704USD(Tier 10)
합계	100,000개	

나. Lumoz ZK-Verifier Node Sale Tier Structure

Tier	Node Price (USD)	Nodes Per Tier	Nodes Sold (Accumulated)	Real Time Tier FDV	Implied Tier FDV (100%)
1	200	8,000	8,000	6.4	80
2	230	9,000	17,000	15.6	92
3	265	10,000	27,000	28.6	105.8
4	304	12,000	39,000	47.5	121.7
5	350	12,000	51,000	71.4	139.9
6	402	12,000	63,000	101.4	160.9
7	463	10,000	73,000	135.1	185
8	532	10,000	83,000	176.1	212.8
9	612	9,000	92,000	225.1	244.7
10	704	8,000	100,000	281.4	281.4

- *FDV: Full Diluted Valuation*
- *초기 프로모션 조건*

Ⅵ. Lumoz Roadmap

일자	주요 이슈	내용
’23. 5. 1.	Pre-Alpha Testnet Launching	• Lumoz Network 프로덕트 초기 모델 제안 • PoS/PoW 등의 아이디어 설정
’23. 8. 30.	Alpha Testnet Launching	• Lumoz Testnet 런칭 • 검증인과 채굴자 모집 시작
‘23. 10. 13.	Lumoz Rebranding	• 기존 Opside에서 Lumoz로 브랜드명 변경
‘23. 10. 25	Community Governance Introduce	• 커뮤니티 기반의 zkVerifier 노드 활성화 제안 • zkVerifier의 거버넌스 참여 제안
‘24. 6. 13.	ZK-Verifier Node Sale start	• ZK verifier Node 초기 판매 수량 확정
‘24. 6. 15.	Node Sales Condition Update	• (수정) 총 노드 판매 수량 조정
‘24. 8.	TGE	• Lumoz Token Minting

Ⅶ. Token Detail

가. MOZ Token

Moz Token은 주된 플랫폼 가상자산입니다. Moz Token은 1) 트랜잭션 수수료 2) zkProver 연산 자원 비용 등의 방법으로 플랫폼 상에서 사용됩니다.

나. esMOZ

Lumoz Network의 1) zkProver 및 zkVerifier의 보상, 2) 거버넌스 등의 목적으로 사용됩니다.

esMOZ Token의 독특한 점은 수취에서 교환 시점까지 기간에 따라 교환비율이 달라진다는 점입니다. 가득 이후 10일이 경과할 경우 100%의 교환비를 보장받으나 수취한 직후 교환 시 10%의 교환비를 적용받게 됩니다.

※ 위와 같은 요소는 보상이 실제 현금화로 이어지는 기간을 지연시키는 역할을 수행함.

Ⅷ. Conclusion

토크노믹스 및 수익 구조

통상적인 컴퓨팅 파워의 거래 구조는 데이터 센터를 통해 대역폭을 계약하고 기간에 따라 정해진 용량만큼 사용하는 것으로 이루어져 왔습니다. Lumoz Network의 경우에는 개별 사용에 따라 MoZ를 이용하여 대가를 지불하고, 지불한 대가가 Prover/Verifier에게 분배되는 구조로 이루어집니다. 전체적인 토큰 플로우에서 토큰 투자자에게 중요한 변수는 “사업적 성과”입니다. Lumoz Network는 Prover 및 검증 플랫폼으로 1) 처리 Transaction의 개수 2) 유지 사용자 수 3) 연계 플랫폼의 활성화 등이 수익에 대한 주요 변인으로 작용합니다.

보안성

Lumoz Network가 Cross Roll-up상 zkEVM Stack에서 다루는 프로젝트들은 ZK-SNARKs 기술을 사용하고 있습니다. ZK-STARKs의 지원 여부가 불명확하므로, Prover Node의 선정 부분에서 개선할 부분이 필요합니다. 이후 ZK-STARKs가 적용될 경우, 더 목적 적합한 ZK 서비스가 제공 가능할 것으로 판단됩니다.

시장 확대 관점

Lumoz Network는 Prover 노드를 통해 확보된 컴퓨팅 파워를 이용하여 단순 ZKP뿐만 아니라 AI를 위한 컴퓨팅 파워를 제공합니다. 이는 ZKP의 수요가 감소한다 하더라도 증가하는 AI 수요가 뒷받침된다는 점에 있어서 타겟 시장의 확대로 기능할 수 있습니다. 또한 AI와 ZKP의 시장 선호가 서로 다른 시점에 주기성을 갖고 발생한다는 점에서 개별 시장리스크를 헷징하는 기능을 수행하므로 토큰 시스템의 안정성에 기여할 수 있습니다.

초기 진입 관점

’24년 비트코인 등이 반감기 등의 이유로 채산성이 감소하였습니다. 채굴장의 초기 투자비용을 매몰비용으로 간주할 경우, Prover로 전환된 채굴자들의 기대수익은 신규 사업 진입자에 비해서 낮은 편입니다. Lumoz Network에서는 비트코인 채굴장 등에서 발생하는 컴퓨팅 파워를 적은 비용으로 Prover로 전환할 가능성이 높습니다. 이는 단기적인 Prover Node 모집에 용이하고 단기적 Lumoz Network의 안정성 확보에 용이합니다.

설비 투자 관점

AI 트렌드가 확대됨에 따라 데이터 센터들의 설비자산이 증가되는 추세입니다. 또한 기존 AI 서비스 개발을 위해 확보된 데이터센터의 처리 가용 능력의 유휴 비율은 높습니다. Lumoz Network가 Moz Token 및 기 Mining 설비자산을 통해 확보한 초기 Rent가 만료될 경우 데이터센터에 비해 가격 경쟁력이 떨어질 수 있습니다. 이는 시스템 일반의 중장기적 리스크로 확대될 수 있습니다.