AEGIS VENTURES | 2024. 8. 21

Lumoz Network Review (1)
Part 1. ZKP & ZK Roll-up

Index

Ⅰ. 들어가며

가. 모듈러 블록체인의 등장

지난 몇 년간 다양한 레이어1 네트워크들이 등장하며 블록체인 업계에 혁신적인 변화를 가져왔지만, 모놀리틱 블록체인의 근본적인 확장성 문제는 여전히 해결되지 않은 과제로 남아있습니다. 모놀리틱 블록체인은 모든 트랜잭션 실행, 보안, 데이터 가용성을 단일 레이어에서 처리하기 때문에 확장성과 보안성 면에서 많은 제약이 따릅니다. 특히 트랜잭션 처리 속도와 효율성 면에서 한계가 뚜렷하며, 단일 거버넌스 구조로 인해 다양한 애플리케이션의 특성에 맞는 최적화가 어렵습니다.

이러한 문제를 해결하기 위해 셀레스티아(Celestia), 맨틀 네트워크(Mantle Network) 등 다양한 프로젝트들이 모듈러 블록체인 구조를 도입하였습니다. 이들은 트랜잭션 처리, 보안, 데이터 가용성을 각각 다른 레이어에서 처리하여 확장성과 효율성을 극대화하는 구조를 택함으로써 트랜잭션 처리 속도를 대폭 향상시키고 보안을 강화하고자 하였습니다.

나. Lumoz Network, ZK-RaaS 모듈식 컴퓨어 레이어

이러한 배경에서 등장한 Lumoz Network는 Rollup-As-a-Service(RaaS) 프로젝트로서 모듈러 블록체인의 롤업 체인을 쉽게 구축할 수 있도록 지원합니다. Lumoz는 특히 영지식 증명(ZKP)을 통해 보안성과 효율성을 높이고, AI 연산을 위한 컴퓨팅 파워를 제공하여 블록체인 기술의 한계를 극복하는 데 기여하고 있습니다.

Lumoz Network는 모듈러 컴퓨팅 레이어와 ZK-RaaS를 결합하여 블록체인과 AI 기술의 발전을 도모하고 있습니다. 탈중앙화 물리적 인프라 네트워크(DePIN)와의 통합을 통해 안전하고 유연한 컴퓨팅 플랫폼을 제공하여 다양한 사용자의 요구를 충족시킵니다. Lumoz는 영지식 증명(ZKP) 기술의 발전, 롤업 네트워크 개발 지원, 인공지능(AI)을 위한 연산 능력 제공에 집중하고 있으며, 이를 통해 ZK 컴퓨팅의 비용과 효율성 문제를 해결하고 있습니다.

Lumoz는 PoW와 PoS를 혼용한 독특한 합의 구조를 통해 ZKP의 증명 생성과 검증을 수행합니다. 이 구조는 대규모 연산을 필요로 하는 ZKP 프로세스를 안정적으로 처리하며 보안성을 강화합니다. Lumoz의 수익 구조는 이러한 검증 과정을 기반으로 ZK-Verifier 노드의 라이선스 판매와 ZKP 및 AI 관련 내부 수수료로 구성되어 있습니다. Lumoz는 모듈러 블록체인과 AI의 결합을 통해 블록체인과 AI 업계가 직면한 문제를 해결하는 데 중요한 역할을 수행하고자 합니다.

II. ZKP

가. RaaS Market Overview

RaaS란 "Roll-Up As a Service"의 약자로, Roll-Up[1] 기술을 서비스 형태로 제공하는 것을 의미합니다. Lumoz Network 역시 Zk-RaaS로 모듈러 컴퓨팅[2] 과 RaaS를 결합한 것이 특징입니다.

Roll-Up Project Comparison Table					
프로젝트명	Lumoz Network	StarkWare	zkSync	Loopring	Scroll
주기능	Raas and Computing Power Platform	Layer-2 (zk-Rollup)	Layer-2 (Zk-Rollup)	DEX/Payment (Zk-Rollup)	Layer-2 (zk-Rollup)
Token Ticker	MoZ esMOZ	STARK	ZKS	LRC	SCROLL
EVM 호환	O	X	O	O	O
사용 ZK기술	Zk-SNARKs	STARKs	Zk-STARKs	Zk-SNARKS	Zk-SNARKs
특이점	-**모듈러 컴퓨팅** -빠른 확장성 -높은 상호운용성	-빠른 처리속도 -보안성 -Trusted setup 미존재 (zk-STARKs)	-낮은 가스비용 -빠른 지불능력	-빠른처리속도 -낮은 비용 -DEX 지원	-개발자친화적임

1 메인 체인의 데이터와 연산 부담을 줄이기 위해 거래 데이터를 오프체인에서 처리하고 검증한 후 집계하여 메인 체인에 업로드하는 기술

2 각 컴퓨팅 레이어가 분리되어 독립적으로 운영되며, 특정 기능에 최적화된 모듈들이 결합하여 전체 시스템을 구성하는 방식

나. ZKP(Zero Knowledge Proof)

1) ZKP의 정의

ZKP란 "Zero-Knowledge Proof"의 약자로, 검증자에게 간접적인 정보만을 통해 중요한 정보의 보유 여부를 증명하는 것을 의미하는 것으로, 이 과정에서 "중요한 정보의 제공 없이도 대상자를 식별할 수 있다."라는 점에서 Zero Knowledge라고 불립니다.

통상 퍼블릭 블록체인 상에서 활동(Transaction)은 **"송신인의 주소"**, **"수신인의 주소"**, **"거래 상세"** 등이 기록 및 익스플로러 상에 표기되는 형태로 이루어집니다. 블록체인의 특성상 위와 같은 활동은 모두가 열람 가능한 기록으로 남아 손쉽게 개인정보인 거래내역 등을 노출시켜 사생활의 침해 요인으로 기능할 수 있습니다.

ZKP는 위의 문제를 퍼블릭 블록체인 위에 암호화 레이어를 하나 추가함으로써 해결합니다. 유사한 ZK 프로덕트 중 초기 형태인 ZK-SNARKs(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)를 예시로 설명해 보도록 하겠습니다. ZK-SNARK의 플레이어는 통상 Verifier와 Prover로 대변될 수 있습니다. ZK 서비스에서 Verifier는 Prover의 검증요청을 검증하는 자로 공개되지 않은 다항함수를 암호로 가지고 있습니다. Prover는 검증요청자로 Verifier에게 암호로 제시된 다항함수에 대한 계수값을 제출하여 올바른 증명을 제출하였는지 적격 여부를 확인받습니다. 여기서 제출되는 계수값은 **"QAP"(Quadratic Arithmetic Program)**[3]를 만족하는 특정 다항식을 알고 있음을 증명하는 것을 의미합니다.

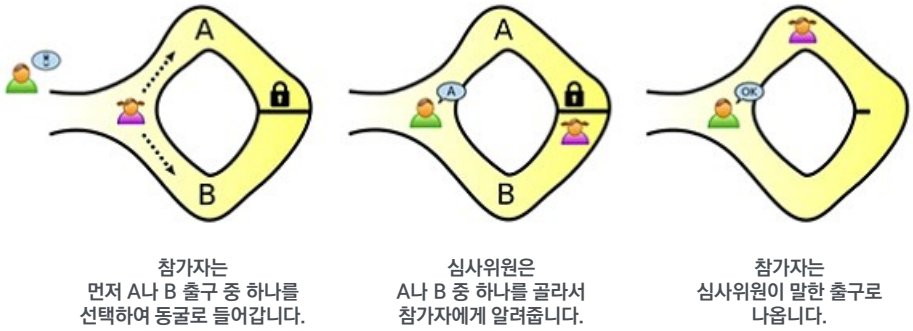
이 과정은 좀 더 구체적으로 서술하자면 타원곡선 암호화를 바탕으로 NP-Complete[4]한 대상들에 대해서 특정 Circuit을 만족하는 문제에 대한 솔루션을 찾는 과정입니다. 위의 조건을 만족하는 대상들을 Arithmetic Circuit[5]으로 변환한 뒤, 선형 랭크 형태인 R1CS(Rank-1 Constraint System)[6]으로 변환합니다. ZK-SNARK는 R1CS로 표현된 형태를 QAP의 형태로 변환하여 Verifier에게 주어지게 됩니다. Prover는 이 과정에서 필요한 결과값(해)를 Verifier에게 제공하여 증명하는 형태입니다.

3 다항식들 간의 곱셈 관계를 통해 연산 과정을 표현하는 방식
4 모든 NP 문제를 다항 시간 내에 다른 문제로 변환할 수 있는 복잡도 이론상의 문제 집합
5 산술 연산을 노드로 표현한 회로 구조로, 주어진 연산 문제를 해결하기 위해 사용되는 모델
6 산술 회로의 각 연산 제약 조건을 선형 방정식 형태로 표현한 시스템

2) ZKP 예시 — 알리바바의 동굴 비유

알리바바의 동굴 비유는 Interactive한 Zero Knowledge Proof(이하 “ZKP”)를 이해하기 좋은 예시 중 하나입니다. 위의 모형에서 가정은 다음과 같습니다.

알리바바의 동굴 비유



1. 동굴은 연결되어 있는 루프 형태로 중간에 암호로 된 문으로 막혀있는 구조임.

2. 관찰자는 참가자가 어떤 경로로 나왔는지만 확인 가능함.

3. 관찰자는 참가자에게 특정 경로를 통하여 나올 것을 지시할 수 있음.

위 모형의 시뮬레이션은 다음 네 가지 경우로 구분됩니다.

	A 경로 퇴장	B 경로 퇴장
A 경로 지시	O	O/X
B 경로 지시	O/X	O

※ **파란색**: 암호를 알고 있는 경우

※ **빨간색**: 암호를 모르고 있는 경우

위의 경우에서 초기 1회 시행단계에서는 문의 암호를 알고 있는 사람은 100%의 확률로, 암호를 모르는 사람은 50%의 확률로 지시를 이행할 수 있습니다.

하지만 위의 테스트를 반복할 경우 암호를 모르는 사람은 (1/2)^(시행횟수)의 확률로 하락하게 됩니다. 위의 테스트를 반복할수록 암호를 모르는 자가 모든 테스트에 통과할 확률은 0%로 수렴하게 됩니다. 이 과정에서 관찰자는 참가자가 제출하는 암호가 일치하는지를 직접 확인하지 않더라도, 참가자가 암호를 알고 있는지 여부를 확인할 수 있습니다.

3) Interactive ZKP v. Non-Interactive ZKP

	Interactive (대화형)	Non-Interactive (비대화형)
메시지 빈도	N회 (N>1)	1회
증명의 크기	상대적으로 작음	상대적으로 큼
연산요구량	메시지 크기에 따라 동일	
병렬처리 가능여부	가능	불가
블록체인 적합도	낮음 (TX 개수 증가, 낮은 트래픽)	중간 (1회성 TX, 데이터 크기 ↑)
시간복잡도	K * O(n) : 선형 증가 * 증명의 크기에 따라 선형 증가하므로 동일 (k = 증명개수, O(n) = 개별 증명소요시간)	

상기 서술한 통상적인 ZKP는 크게 Interactive 형태와 Non-Interactive 형태로 구분될 수 있습니다. Interactive 형태는 Prover와 Verifier가 지속적으로 메지를 주고받아 상호작용하는 경우를 말하고, Non-Interactive 형태는 1회 메시지를 송신하여 적격(어떤 적격여부)여부를 증명하는 경우를 말합니다.

검증해야 할 내용이 많지 않거나(혹은 메시지의 길이가 길지 않은) 매우 높은 형태의 보안성이 요구되지 않는 상황에서 Non-Interactive의 형태는 강력한 효율성 및 목적 달성을 발휘합니다. 1회 검증을 통하여도 Interactive의 형태에서 검증할 양을 충분히 처리할 수 있기 때문입니다. 또한 쌍방 간 송수신이 지속적으로 유지되어야 하며 반복적으로 메시지를 주고받아야 하는 Interactive의 형태와 다르게 Non-Interactive의 형태의 경우에는 Verifier의 검증이 1회로 종결되므로 통신 비용이 상대적으로 절감되며, 높은 Latency[7] 가 요구되지 않으므로 서비스가 안정적인 특징을 가지고 있습니다.

상기의 판단은 1개 증명에 대한 판단입니다. ZKP 서비스가 블록체인 상에서 자동화되기 위해서는 개별 메시지에서 증명이 되는 가짓수가 증가하여야 합니다. 예를 들어 “이름”, “계좌”, “금액” 등의 데이터들로 증명해야 할 대상이 증가할 경우가 이에 해당합니다. 독립적인 증명의 개수 증가는 다음의 비용함수 형태로 표현될 수 있습니다.

7 데이터 전송 시 지연되는 시간 또는 반응 속도

4) ZKP 비용 비교표

C(I) = 대화형 ZKP 비용함수　　C(NI) = 비대화형 ZKP 비용함수

G(n) = 증명생성시간　　B = 네트워크 대역폭　　S(n) = 단일증명크기
V(n) = 검증 시간　　k= 증명 개수

- C(I) = k X (G(n) + S(n)/B + v(n))
- C(I) = k X G(n) + k X (S(n) / B) + k X V(n)

위의 비용함수에 따르면 Non-Interactive 형태와 Interactive 형태의 총 소요비용은 차이가 없어 보일 수 있으나, 적용되는 환경에 다음의 변수들이 추가될 경우 Non-Interactive 형태의 한계가 드러납니다.

첫 번째, 복잡도 증가입니다. Non-Interactive 형태는 단일 메시지 내에 모든 증명과 정보가 포함되어야 하므로 메시지 내 포함되어 있는 증명 대상들이 상호 독립적이지 않고 종속적일 경우 생성에 있어서 총 생성 및 검증 시간이 그렇지 않은 경우보다 증가할 수 있습니다. 예를 들어, Interactive 형태에서 보안성 강화를 위해 첫 번째 증명에 대한 특성 값이 두 번째 증명의 특성 값에 영향을 미칠 경우에는 생성 및 검증에서 소요시간 증대 등의 문제가 발생할 수 있습니다.

두 번째, 증명 크기입니다. 만일 증명하는 대상이 동일하고 Interactive 형태에서 적격 대상에 대한 증명을 수행한다는 가정을 할 경우, 두 방식의 증명 크기 총량의 차이는 없습니다. 하지만, Non-Interactive 형태의 경우에는 단일 메시지에 모든 증명의 내용이 들어가게 되므로 단위 메시지의 크기는 Interactive 형태의 그것보다 크게 됩니다.

세 번째, 순차처리입니다. Interactive 형태의 경우에는 증명 과정을 순차적으로 거침에 따라 첫 증명이 실패할 경우, 그 이후의 증명을 수행하지 아니하여도 문제가 되지 않습니다. 이것은 네트워크 자원을 절약할 수 있는 장점을 갖습니다. 하지만 Non-Interactive의 경우에는 전체 메시지를 수령하고 그 증명들의 결괏값이 일치하는지 여부를 판단해야 하므로 네트워크 자원의 소모가 더 큽니다.

위의 세 개의 요인은 블록체인의 환경에서는 더욱 두드러질 수 있습니다. Public Blockchain은 1) 개별 블록의 사이즈가 크지 않고, 2) 단위 시간에 처리할 수 있는 블록 개수에 제한이 있다는 특징들이 있습니다. 특히 3) Blockchain에서는 개별 활동의 단위 기록에 대응하여 소요비용이 발생하는 구조를 가지고 있습니다.

5) ZKP Type별 한계

위의 특징으로 개별 ZKP Type은 다음의 문제를 가집니다.

Interactive ZKP 형태는 2, 3번과 같이 앞서 언급한 블록체인의 결점을 고려하면 치명적인 문제점을 가지고 있습니다. Interactive ZKP 형태는 Prover와 Verifier가 증명을 검증하고 그 결과를 기록하는 절차를 반복하여야 합니다. 이러한 과정은 통상적으로 블록체인상 기록되는 활동의 개수를 증가시켜 Min(활동비용)을 검증 횟수만큼 증가시키는 문제를 가지고 오게 됩니다. 또한 낮은 Throughput은 지속적으로 메시지를 주고받아야 하는 Interactive 환경에서 검증의 종결까지 상당한 시간을 소요하게 하기 때문에 서비스의 안정성을 떨어뜨리게 됩니다. 이에 반해 Non-Interactive 형태의 방법은 일회성 송수신으로 검증이 종결되므로 네트워크 관점, 활동에 따른 비용 관점에서 상대적으로 안정적입니다.

Non-Interactive 형태의 ZKP 관점에서는 Public Blockchain에서 처리될 수 있는 대역폭은 "단위 시간당 생성되는 블록의 개수 X 블록의 크기"로 정의될 수 있습니다. 검증 과정에서 필요한 데이터가 크다는 것은 다음의 문제를 야기할 수 있습니다.

- **(블록점유율)** layer-1의 블록사이즈보다 큰 데이터 저장이 불가하므로 검증 결과를 분리해서 저장해야 함.
- **(TX Fee)** Layer-1의 블록사이즈와 비슷한 데이터를 저장할 경우, 높은 활동 비용을 지불해야할 수 있음.
- **(Lead Time)** Layer-1의 블록사이즈를 초과하는 데이터를 기록해야 하는 경우 블록생성 2주기 이상의 소요시간이 필요
- **(MEV, 공급자)** MEV 관점에서 생성 활동을 위해 지불된 비용이 충분하지 않을 경우 블록생성자가 활동을 블록에 담지 않아, 지속적으로 활동 기록이 지연될 수 있음.

Ⅲ. ZK Roll-up

가. ZK Roll-up의 정의

	Blockchain Consensus (Layer 1)	ZKP Consensus (Layer 2, Roll up)
공통점	플랫폼 내에서 특정한 합의를 구성하는 방법	
목적	탈중앙화 된 분산원장을 반영구적으로 유지 관리하기 위함	ZKP를 목적으로 제출된 활동을 ZKP로 검증
노드 종류	Validating Node Mining Node Full Node, Archive Node 등	Verifier Node, Prove Node 등
노드의 기능	트랜잭션 검증, 블록 검증, 블록 생성, 분산원장 유지	ZK Prove & Verify

ZK Roll-Up는 Layer-1에서 예상되는 ZKP의 한계 중 "비용 문제" 및 "인프라 한계" 문제를 해결할 수 있는 솔루션입니다. Roll-Up은 블록체인 Layer-2에서 사용되는 방법으로 중 하나로 활동에 대한 개별 검증은 Layer-2(오프체인)에서 수행하고 검증이 완료된 결과 값들을 압축하여 Layer-1(온체인)상에 기록하는 것입니다. 이러한 접근 방법은 ZKP에서 요구되는 과다한 연산이나 높은 저장용량의 문제를 일정 부분 해소해 줍니다.

나. ZK Roll-up의 장점

Roll-up은 다음의 장점들을 가지고 있습니다.

가) **(용량 확대)** ZKP 과정에서 발생하는 "모든 데이터"를 온체인에 업로드 할 필요가 없음.

나) **(연산속도 개선)** Layer-1 상에서 연산을 수행하지 않고 Layer-2 단계에서 ZK에 필요한 연산을 수행하므로 온체인 Throughput에 제약을 덜 받음.

다) Layer-1 상에서 ZKP연산을 수행하지 않고 Layer-2에서 연산한 뒤 Layer-1으로 전송하므로, Layer-1에 별다른 Prover와 Verifier를 노드를 구성하지 않아도 됨.

라) Layer-2에 검증 데이터를 저장하므로 Layer-1단에 요구 저장공간이 작음.

마) Layer-1이 가진 분산원장 보안성을 계수할 수 있음.

위와 같은 Roll-up의 특징들은 Interactive ZKP 형태와 Non-Interactive ZKP 형태에서 발생하는 취약점을 효율적으로 해결할 수 있습니다. 하지만 신뢰할 수 있는 Prover와 Verifier에 대한 선정의 문제에 대한 솔루션으로는 한계가 있습니다.

다. Trusted Setup ZKP v. Non-Trusted Setup ZKP

Prover와 Verifier 중 Prover의 초기 선정에 대한 문제와 관련해서는 ZKP는 두 가지 방법이 존재합니다. 하나는 Trusted Setup ZKP와 다른 하나는 Non-Trusted Setup ZKP로 구분될 수 있습니다. 두 방식의 주된 차이는 ZKP의 초기 설정 과정에서의 매개변수에 대한 Prover의 인지 여부입니다.

Trusted Setup ZKP는 키값의 정보를 가지고 있는(Trusted Setup 된) 제3자를 둡니다. 제3자는 Prover에게 매개변수를 제공합니다. Trusted Setup ZKP에서는 증명크기가 크지 않고 검증속도가 빠르다는 장점을 가지고 있습니다.

하지만, 악의적인 Prover가 해당 매개변수 값을 수령할 경우 값을 유출할 수 있는 가능성이 존재합니다. 악의적인 Prover가 존재하는 ZKP 프로토콜에서는 검증결과의 보안을 보장할 수 없습니다. 또한 Prover가 악의적이지 않다 하더라도 증명 생성 단계에서 QAP에 따른 매개변수가 파기되지 않을 경우 알고리즘 자체에 문제가 될 수 있다는 보안의 한계를 갖습니다.

정리하자면, Trusted Setup ZKP 프로토콜은 Prover에게 고도의 신뢰를 요구하고 Prover 선정의 제약으로 기능하기 때문에 많은 Prover를 프로토콜 내에 둘 수 없습니다. 또한 Prover에 대한 무조건적인 신뢰를 기대하는 프로토콜은 Blockchain이 지향하는 탈중앙화 및 자동화와 어긋납니다.

이런 특징으로 Trusted Setup ZKP는 Public Blockchain을 위한 ZKP 구조로는 취약합니다. Trusted Setup ZKP 형태의 대표적인 알고리즘으로는 ZK-SNARKs가 있습니다.

이와 대조적으로 Non-Trusted ZKP는 신뢰할 수 있는 제3자를 두지 않아 초기 설정 과정에서 증명의 키 값이 유출되어도 문제가 되지 않는 구조입니다. 대신 매개변수를 생성하는 과정에서 더 복잡한 증명에 대한 값을 제공해야 하므로 그 연산의 시간이 Trusted ZKP에 비하여 더 길고 더 많은 연산량을 요구한다는 특징이 있습니다.

대표적인 알고리즘으로는 ZK-STARKs(Zero-Knowledge Scalable Transparent Arguments of Knowledge)가 있습니다. ZK-STARKs는 ZK-SNARKs에 비하여 더 고도의 연산을 요구하는 증명을 통해 검증을 수행합니다. ZK-STARKs는 다음의 프로세스로 검증이 이루어집니다.

1) NP Complete한 문제를 다항식으로 변환
2) Verifier는 Prover에게 다수의 해를 요구하고 이에 대해 Prover가 값을 계산하여 응답
3) Verifier는 이에 대한 일관성을 검증

Prover와 Verifier는 FFT(Fast Fourier Transform)을 통해 증명의 해를 제출 및 검증하고, 특히 Verifier는 Prover를 대상으로 다항식의 값의 일관성을 평가합니다.

ZK-STARKs는 ZK-SNARKs와 다르게 컴퓨팅 파워가 있는 누구든 임의의 Prover와 Verifier가 될 수 있습니다. 다수의 충분한 연산능력을 가진 자들이 Verifier로 선정될 수 있다는 특징은 빠른 증명 검증 및 분산화 된 자동화 ZKP 구조로 적합성을 지닙니다. 또한 검증 과정에 2개 이상의 Verifier가 참여할 수 있다는 특징은 빠른 검증 속도를 제공합니다.

위와 같은 특징의 ZK-STARKs는 블록체인에 ZKP의 기능을 적용함에 있어 유효합니다.