알트레이어(Altlayer)

본 '주요내용설명서'는 가상자산의 발행주체 또는 운영주체가 작성한 가상자산 관련 중요사항을 설명하는 자료 원문의 주요 내용 및 가상자산 관련 중요사항에 대한 최신 변경내용을 기재한 한글 자료이며, 본 설명서가 업로드 되는 시점에 따라 자료 원문과 내용의 차이가 있을 수 있습니다. 보다 자세한 사항 및 최신 변경내용은 반드시 원문을 참고해 주시기 바랍니다.
(원문 링크)

개요

알트레이어(AltLayer)는 롤업(Rollup) 기술을 활용한 개방적이고 탈중앙화된 프로토콜로서 리스테이크 롤업(Restaked Rollup)을 통해 기존 롤업(OP Stack, Arbitrum Orbit, Polygon CDK 등)에 향상된 보안성, 탈중앙성, 상호운용성 등을 제공하며, 복잡한 소프트웨어 및 하드웨어 관리 없이 롤업을 구축할 수 있는 롤업 서비스(Rollup-as-a-Service, RaaS)를 제공하는 것을 목표로 한다. ALT 토큰은 경제적 보증, 거버넌스, 프로토콜 인센티브 및 프로토콜 수수료 등의 용도로 사용된다.

기술 및 특징

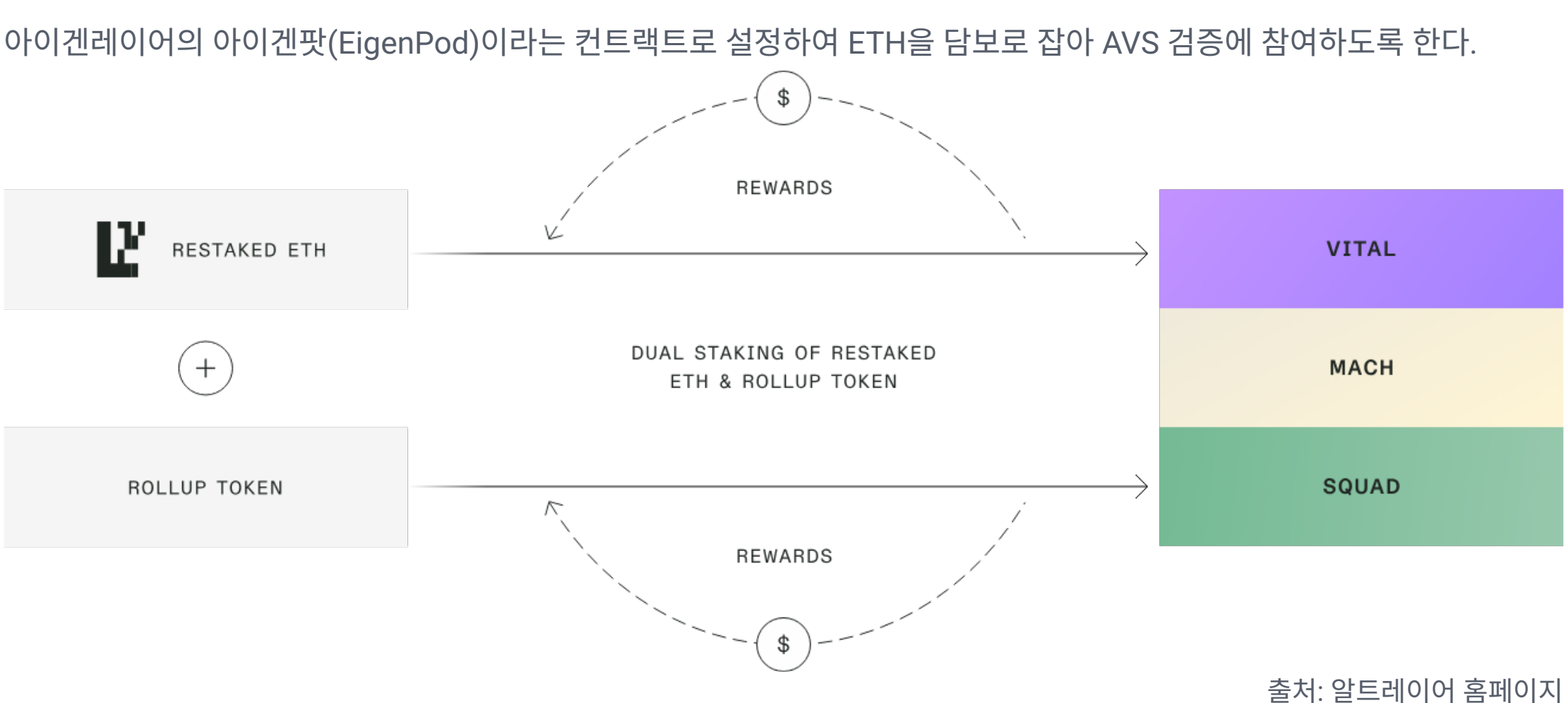
알트레이어는 롤업 인프라를 제공하는 프로젝트로, 리스테이크 롤업 및 RaaS를 통해 다양한 솔루션을 바탕으로 네트워크 보안을 강화하고 탈중앙화된 네트워크를 구축하는 것을 목표로 한다.

리스테이크 롤업

리스테이크 롤업은 OP Stack, Arbitrum Orbit, ZKSync의 ZKStack, Polygon CDK 등과 같은 롤업 스택을 사용한 롤업과 아이겐레이어(Eigenlayer)의 리스테이킹(Restaking) 메커니즘을 결합하여 네트워크 보안을 강화하고 탈중앙화된 네트워크를 구축하는 것을 목표로 한다.

롤업에는 옵티미스틱 롤업(Optimistic Rollup)과 영지식 롤업(Zero-Knowledge Rollup)이 있다. 이들은 레이어1에 게시되는 상태 루트값이 올바른지 확인하는 방법에 차이가 있다. 옵티미스틱 롤업은 사기 증명을 사용하고, 영지식 롤업은 영지식 증명을 사용한다. 사기 증명은 잘못된 업데이트가 있을 경우 누군가 사기 증명을 게시하여 이를 되돌릴 수 있는 방식으로, 특정 기간을 두고 사기 증명 게시가 없는 경우 해당 상태 루트가 올바르다고 간주한다. 이 방식은 계산량과 복잡도가 낮지만 즉각적인 확인이 어려워 빠른 출금이 어렵다는 단점이 있다. 반면, 영지식 증명은 암호화 증명을 사용하여 즉시 상태 루트가 올바르다는 것을 확인할 수 있는 방식이다. 계산량과 복잡도가 높지만 즉각적인 확인이 가능하여 빠른 출금이 가능하다는 장점이 있다.

아이겐레이어의 리스테이킹 메커니즘은 이더리움 블록체인에서 사용되는 스테이킹 토큰인 ETH을 다시 스테이킹하는 방식으로, 크게 두 가지 방식의 리스테이킹이 존재한다. 첫째, LST(Liquid Staking Token) 리스테이킹은 디지털 자산을 제공하는 사용자와 검증자(validator)를 연결해 주는 프로토콜인 LSP(Liquid Staking Protocol)에 사용자가 디지털 자산을 스테이킹할 때 받는 토큰인 stETH과 같은 LST를 아이겐레이어 스마트 컨트랙트에 스테이킹하여 리스테이킹을 하고 AVS 검증에 참여할 수 있게 한다. 둘째, 네이티브 리스테이킹은 사용자가 직접 ETH을 가지고 리스테이킹하는 방식으로, 사용자가 ETH을 이더리움 네트워크에 스테이킹할 때 스테이킹한 ETH을 다시 돌려받을 주소를 사용자의 주소가 아닌 아이겐레이어의 아이겐팟(EigenPod)이라는 컨트랙트로 설정하여 ETH을 담보로 잡아 AVS 검증에 참여하도록 한다.



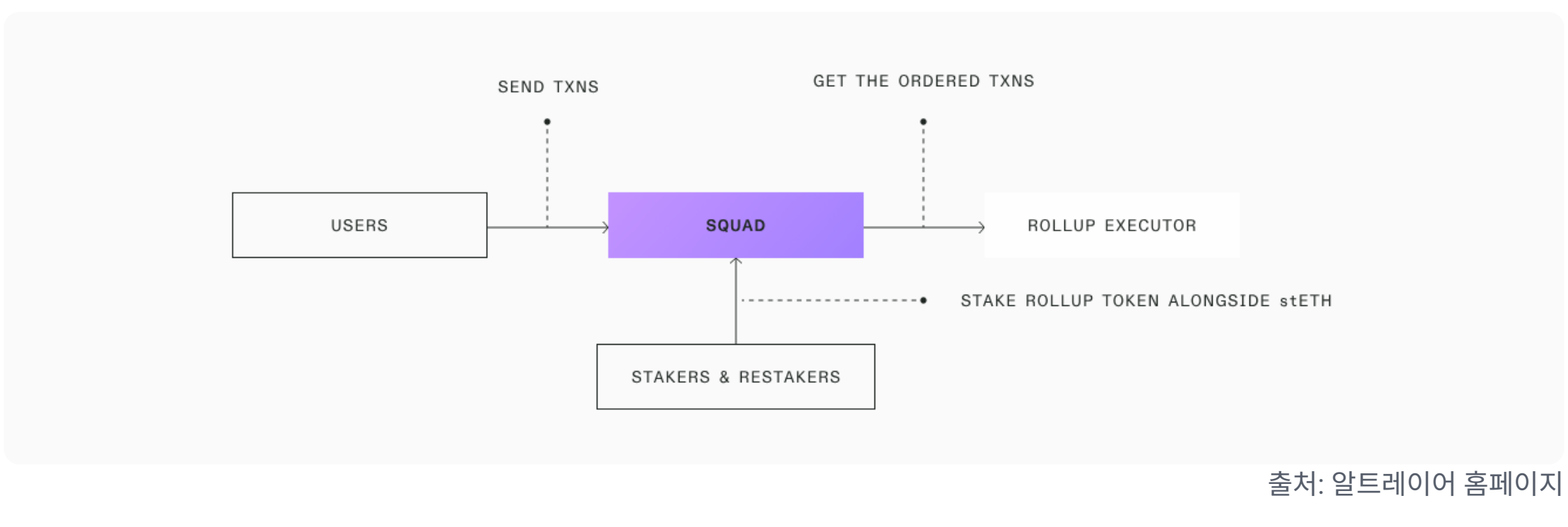
출처: 알트레이어 홈페이지

AVS(Active Validated Services)

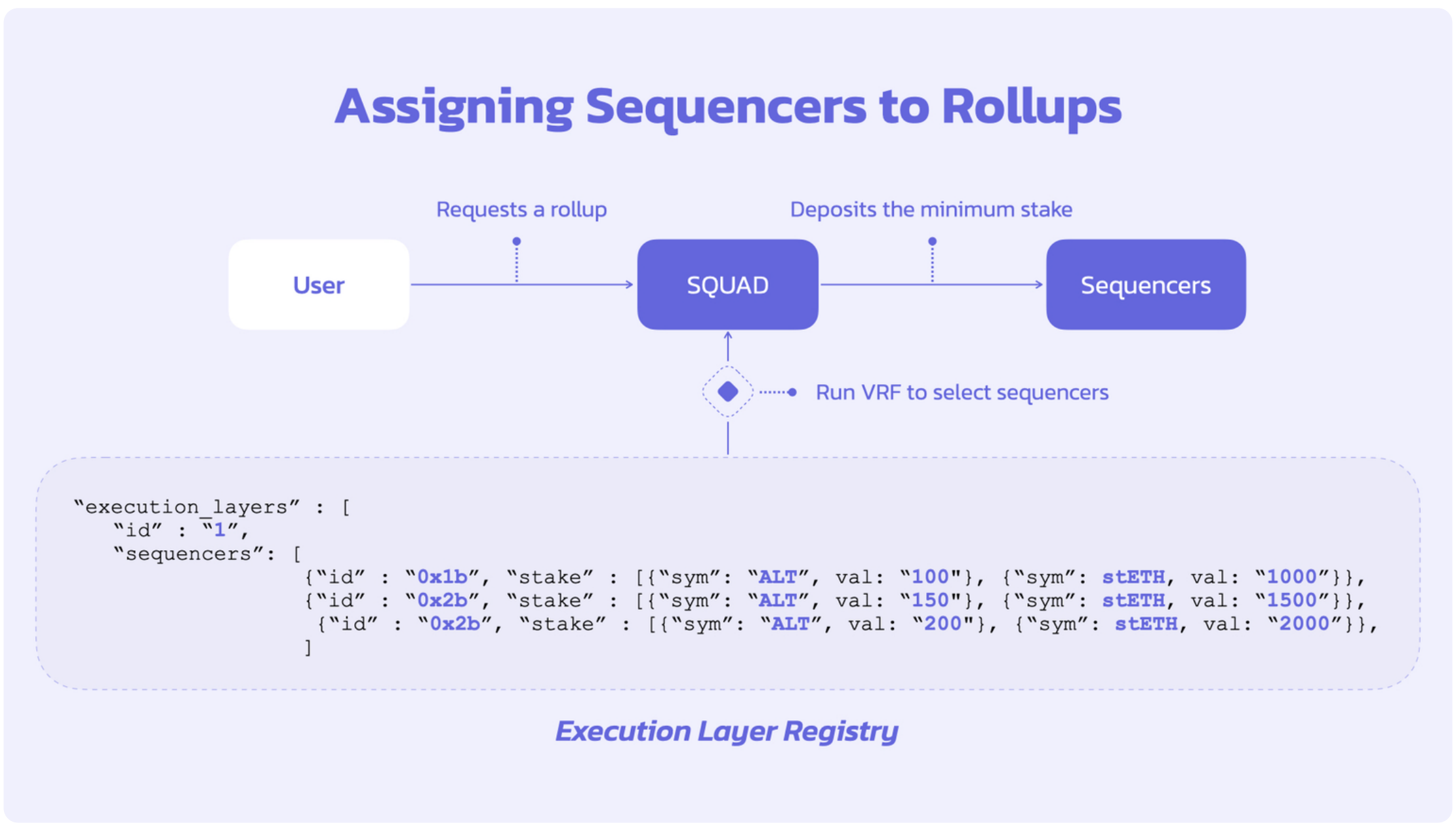
AVS는 이더리움의 기존 보안을 활용하여 다양한 블록체인 서비스의 보안을 강화하는 시스템으로, 이를 통해 새로운 프로젝트는 자체적인 검증 네트워크를 구축하지 않아도 되는 것을 목표로 한다.

SQUAD(탈중앙화된 시퀀싱(Sequencing)을 위한 AVS)

SQUAD는 탈중앙화된 시퀀싱(Sequencing)을 위한 AVS로, 알트레이어를 통해 롤업 메인넷을 만들고자 하는 애플리케이션 개발자가 롤업 생성을 요청하고 롤업에 필요한 시퀀서(sequencer) 수와 시퀀서가 맡길 담보가 되는 토큰과 그 양을 정할 수 있다. 시퀀서는 롤업 체인에서 트랜잭션의 순서를 결정하고, 이를 처리해 블록을 생성하는 역할을 하는 주체이다. 롤업 생성을 요청한 개발자가 정한 담보는 아이겐레이어를 통해 리스테이킹 되어야 하며, 롤업 요청을 받으면 SQUAD는 요구되는 최소한의 양 이상으로 아이겐레이어에 리스테이킹한 사용자 중 시퀀서를 VRF(Verifiable Random Function) 함수를 통해 랜덤으로 뽑는다.



출처: 알트레이어 홈페이지

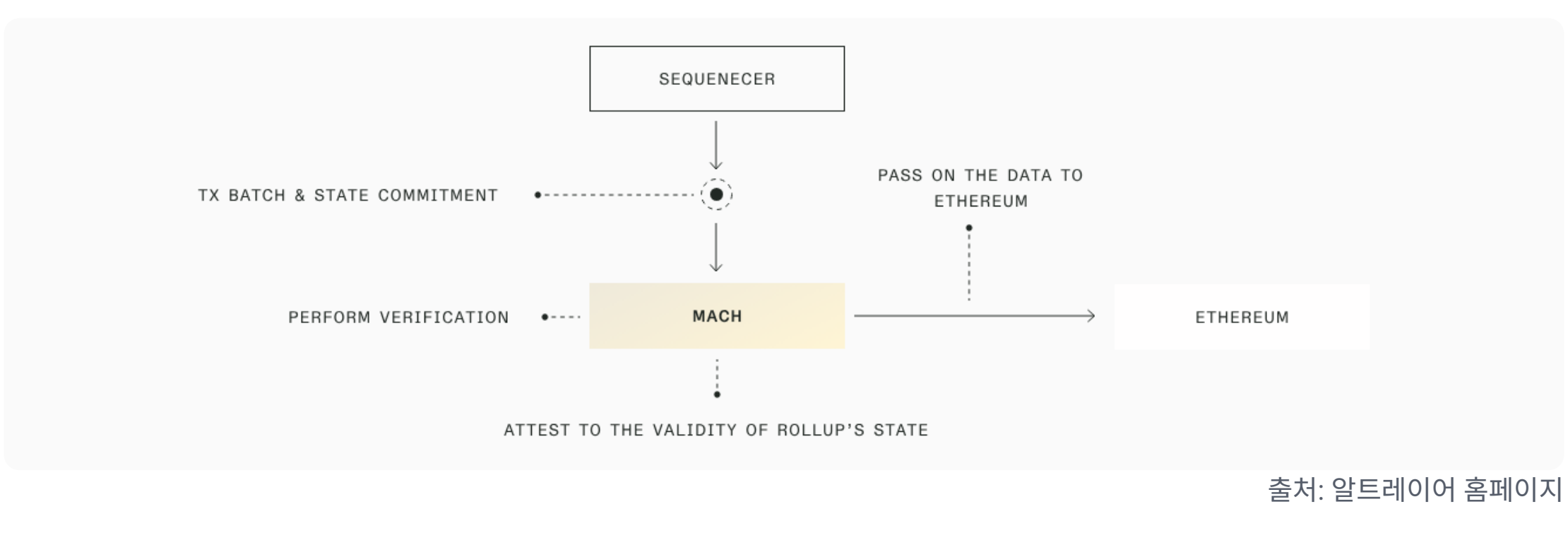

Assigning Sequencers to Rollups
Requests a rollup
Deposits the minimum stake
User
SQUAD
Sequencers
Run VRF to select sequencers
Execution Layer Registry

```
"execution_layers" : [
   "id" : "1",
   "sequencers": [
                  {"id" : "0x1b", "stake" : [{"sym": "ALT", val: "100"}, {"sym": stETH, val: "1000"}},
                  {"id" : "0x2b", "stake" : [{"sym": "ALT", val: "150"}, {"sym": stETH, val: "1500"}},
                   {"id" : "0x2b", "stake" : [{"sym": "ALT", val: "200"}, {"sym": stETH, val: "2000"}},
                  ]
```

출처: 알트레이어 독스

MACH(빠른 최종성 및 상호운용성을 위한 AVS)

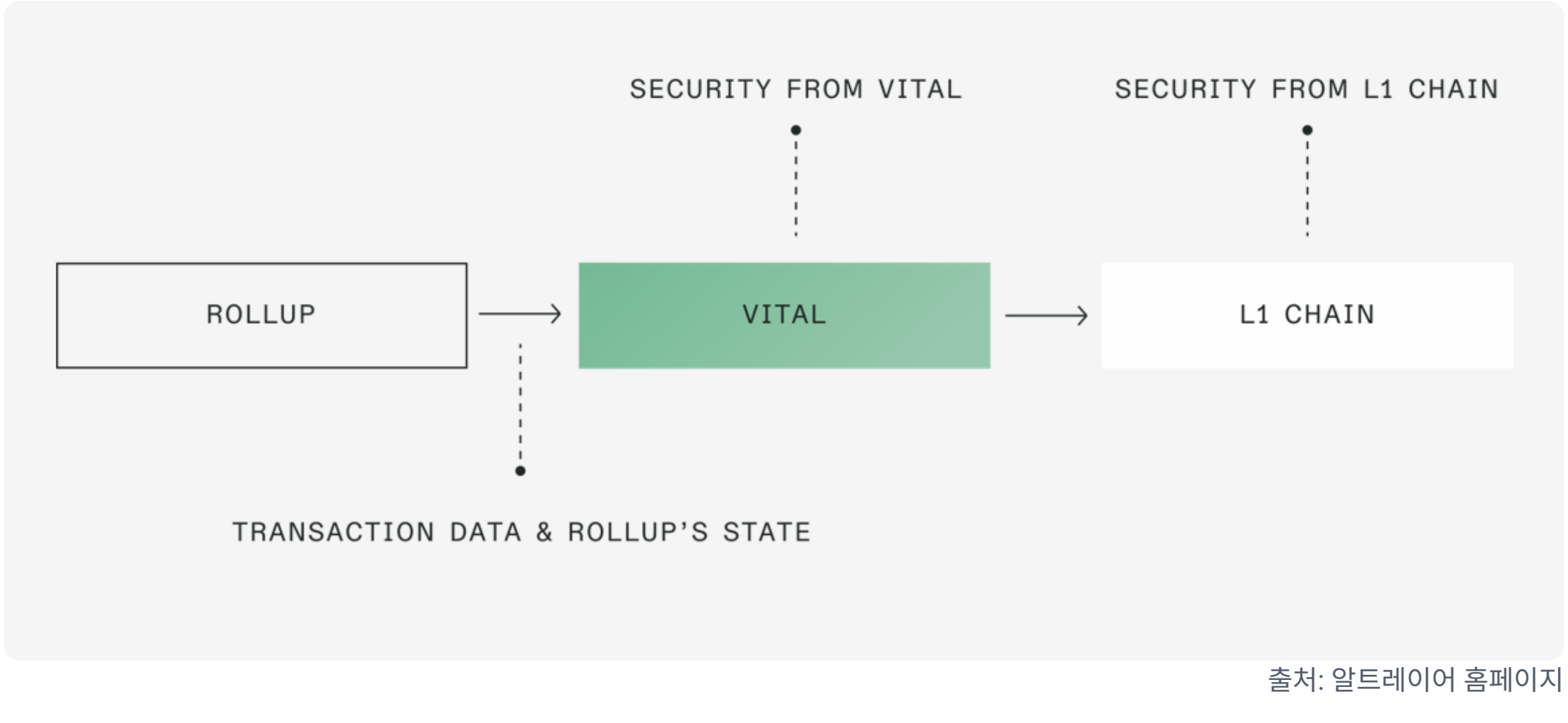
MACH는 롤업 최종성을 위해 롤업 상태의 유효성을 검증하여 롤업 운영자(rollup operator)가 상태 변환 기능을 올바르게 따랐는지 확인하는 것을 목표로 하는 플랫폼으로서, 롤업 트랜잭션에 대한 빠른 확인, 악의적인 네트워크 참여자를 처리할 수 있는 암호경제학적 보안, 영지식 롤업과 옵티미스틱 롤업 모두 지원, 그리고 다양한 증명 시스템과 런타임(runtime)을 지원하는 서비스를 제공한다.


SEQUENECER
TX BATCH & STATE COMMITMENT
PASS ON THE DATA TO ETHEREUM
PERFORM VERIFICATION
MACH
ETHEREUM
ATTEST TO THE VALIDITY OF ROLLUP'S STATE

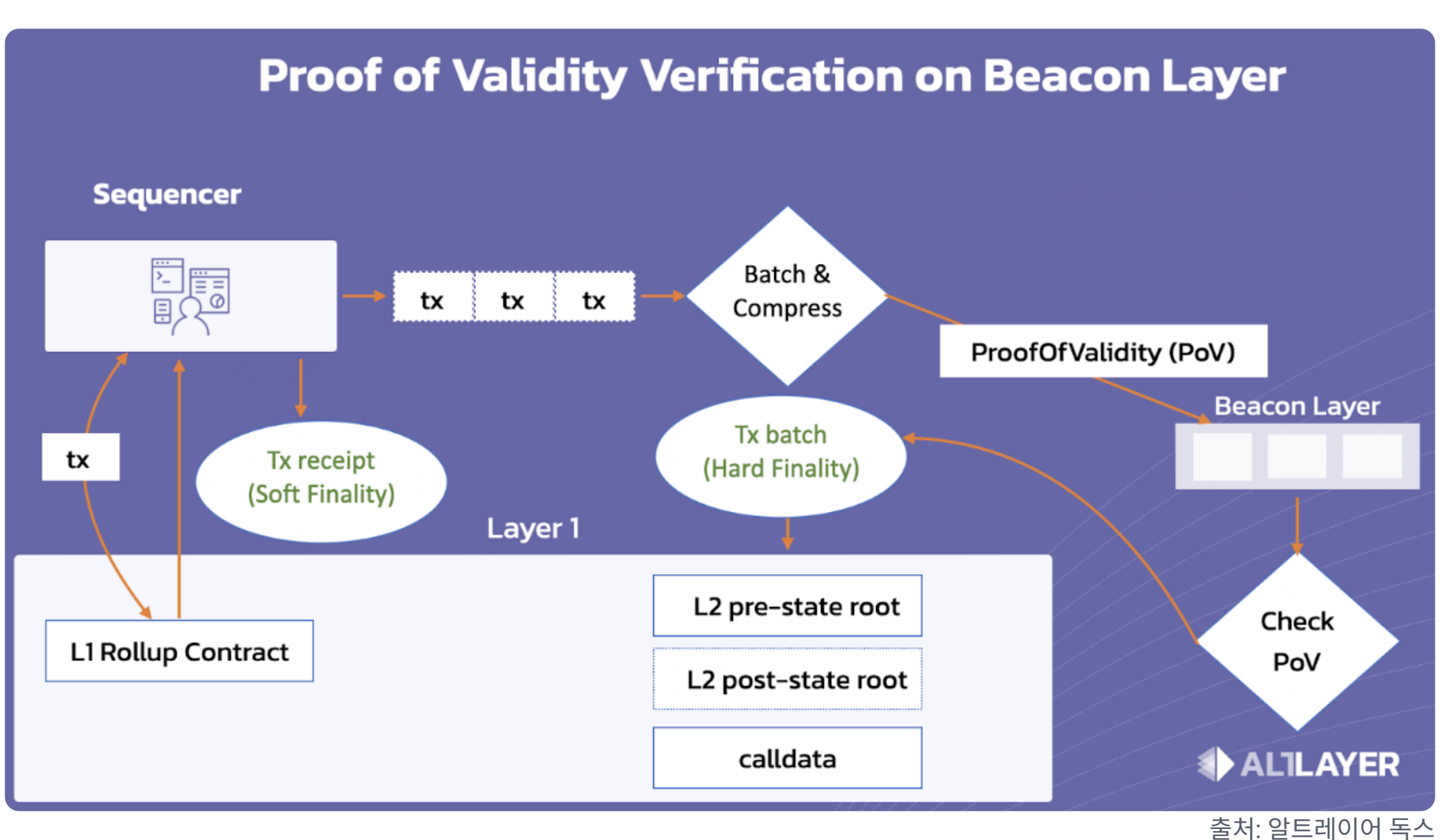
출처: 알트레이어 홈페이지

VITAL(롤업 상태의 탈중앙화 검증을 위한 AVS)

VITAL은 롤업 상태의 탈중앙화 검증을 위한 AVS의 역할을 하는 플랫폼으로서, AVS에 등록된 운영자 네트워크를 기반으로 롤업을 위한 검증 레이어 역할을 한다. VITAL 운영자들은 상태 변환의 유효성을 유효성 증명(Proof of Validity, PoV)을 통해 검증하며, 유효성 증명은 VITAL 운영자가 전체 상태에 접근하지 않고도 롤업에 대한 상태 변환을 검증할 수 있도록 한다. 또한, VITAL 운영자는 새로운 상태 루트를 생성하고 시퀀서가 올린 상태 루트가 자신이 생성한 상태 루트와 동일한지 비교한다. 롤업 네트워크는 상태 변환이 옳다는 증거를 롤업 블록 6개마다 PoV 블록이라는 특수 블록으로 VITAL에 제출하고, 이를 검증하기 위해 VITAL 운영자는 상태 변환 검증 함수(State Transition Validation Function, STVF)를 실행한다. STVF 함수에 PoV 블록을 입력으로 넣고 유효성을 검증한 다음, 만약 유효하다면 VITAL은 트랜잭션 묶음(batch)과 이전의 상태 루트와 새로운 상태 루트를 레이어 1에 제출한다.



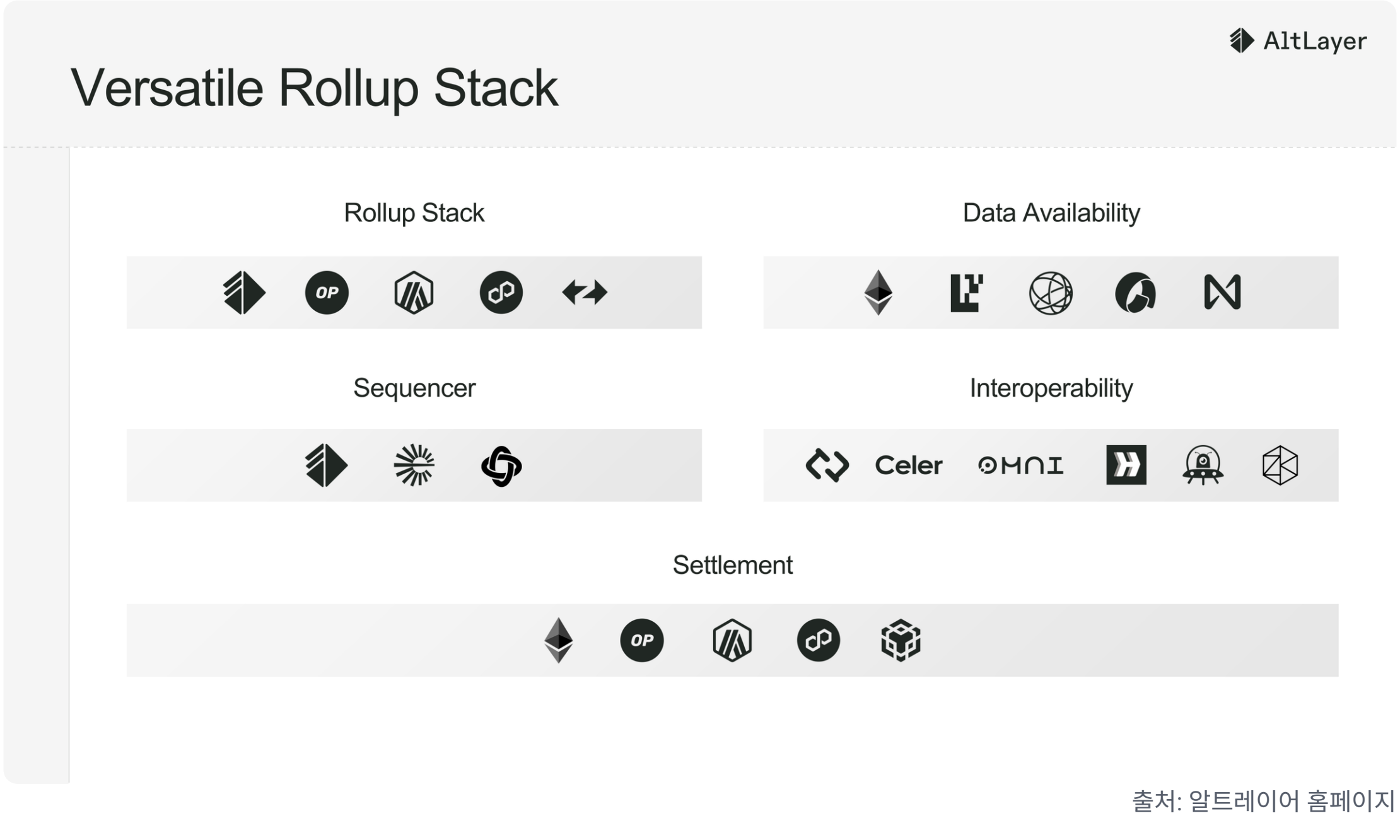
출처: 알트레이어 홈페이지



출처: 알트레이어 독스

RaaS(Rollup-as-a-Service)

RaaS는 새로운 애플리케이션 맞춤형 롤업을 출시할 수 있도록 도와주는 서비스로, 사용자는 복잡한 소프트웨어 및 하드웨어 관리를 하지 않아도 된다. 알트레이어는 맞춤형 롤업 출시를 위한 SDK(Software Development Kit)나 대시보드를 제공하고, 롤업 운영을 위한 노드를 찾아주며, 코드 구축 및 관리 서비스를 제공한다. 또한 알트레이어는 모든 주요 롤업 스택(Rollup stack), 데이터 가용성 계층(Data availability layers), 결제 계층(Settlement layer), 탈중앙화된 시퀀서(decentralized sequencer) 및 상호운용성 브릿지(interoperability bridges)를 지원한다. 사용자는 알트레이어를 통해 다양한 모듈식(Modular) 롤업 솔루션을 골라 맞춤형 롤업을 출시할 수 있다.



출처: 알트레이어 홈페이지

토큰 유틸리티

토큰 이코노미

ALT는 경제적 보증, 거버넌스, 프로토콜 인센티브 및 프로토콜 수수료에 사용된다.

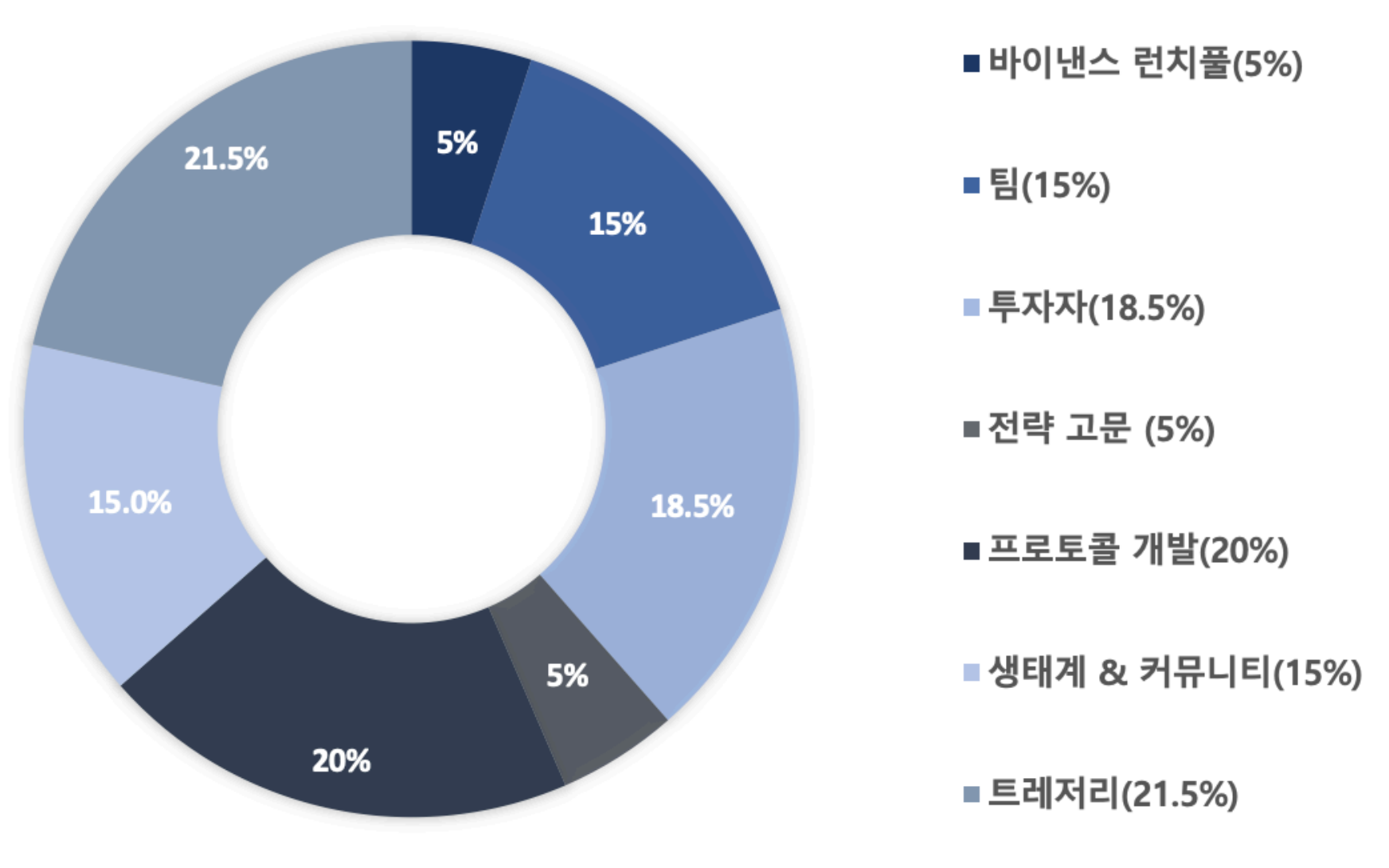
- 경제적 보증: ALT는 리스테이킹된 자산과 함께 경제적 지분을 제공하는 데 사용된다. 이 지분은 악의적인 행위가 감지되면 슬래싱(Slashing)된다.
- 거버넌스: ALT 보유자는 거버넌스 결정에 투표할 수 있다.
- 프로토콜 인센티브: 알트레이어 생태계의 운영자는 서비스에 대한 보상으로 ALT 토큰을 받을 수 있다.
- 프로토콜 수수료: 네트워크 참여자는 네트워크 내 서비스 비용을 ALT 토큰으로 지불해야 한다.

토큰 분배

아래 유통량 관련 정보는 프로젝트 팀이 대외적으로 공개하거나 프로젝트 팀이 업비트에 제공한 자료 등에 기초하고 있기 때문에, 차후 프로젝트의 사정에 따라 유통량 계획은 변경될 수 있습니다. 기준일 이후 업데이트 되는 유통량 관련 정보는 반드시 프로젝트의 공식 웹사이트, 커뮤니케이션 채널 등을 확인해주시기 바랍니다.

알트레이어에서 사용하는 가상자산인 ALT의 총발행량 100억 개는 다음과 같이 분배되었다.

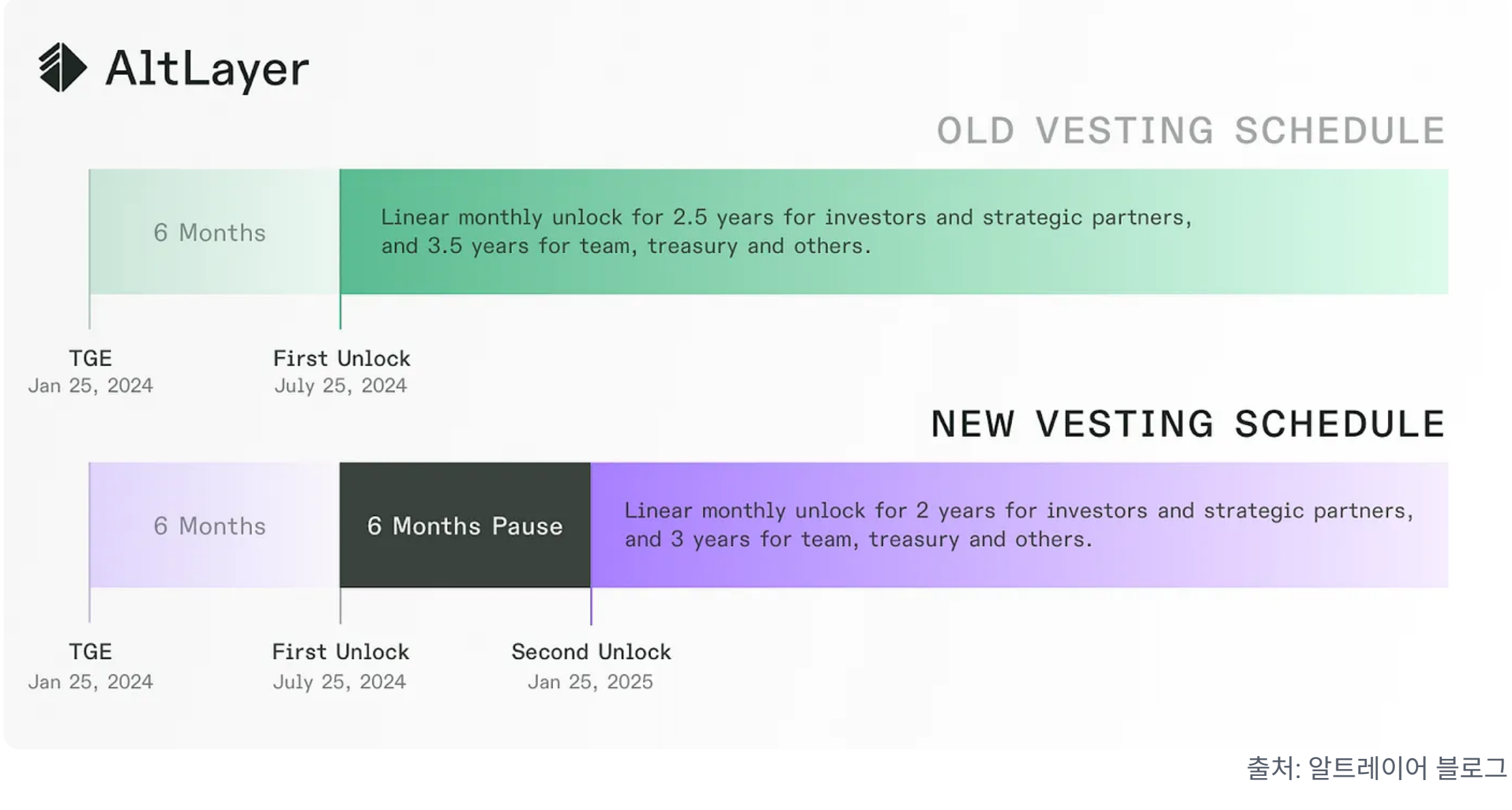
- 바이낸스 런치풀(5%)
- 팀(15%)
- 투자자(18.5%)
- 전략 고문(5%)
- 프로토콜 개발(20%)
- 생태계 및 커뮤니티(15%)
- 트레저리(21.5%)



출처: 알트레이어 제공, 업비트 재구성

ALT의 첫 번째 언락은 2024.07.25에 이루어졌으며, 이후 진행되는 베스팅 일정을 6개월 뒤인 2025.01.25로 연기했다.

2025.01.25부터 투자자와 전략 파트너에게는 2년간 월별 선형 베스팅을 적용하고 팀, 고문, 트레저리 및 기타 이해관계자에게는 3년간 월별 선형 베스팅을 적용한다.


AltLayer
OLD VESTING SCHEDULE
6 Months
Linear monthly unlock for 2.5 years for investors and strategic partners, and 3.5 years for team, treasury and others.
TGE
Jan 25, 2024
First Unlock
July 25, 2024
NEW VESTING SCHEDULE
6 Months
6 Months Pause
Linear monthly unlock for 2 years for investors and strategic partners, and 3 years for team, treasury and others.
TGE
Jan 25, 2024
First Unlock
July 25, 2024
Second Unlock
Jan 25, 2025

출처: 알트레이어 블로그

참고 문헌

- 알트레이어 독스
- 알트레이어 홈페이지
- 알트레이어 블로그

2025.08.25 19:06 업데이트

· 본 자료는 두나무(이하 당사)가 거래지원한 가상자산과 관련하여 작성한 것으로 이용자에게 투자를 권장하거나 유도할 목적이 없으며, 이용자의 투자 판단에 참고가 되는 정보 제공을 목적으로 작성되었습니다.

· 본 자료는 제3자로부터 제공받거나 제3자가 작성한 원문을 참고하여 작성 당시의 당사의 신뢰할 수 있는 내용 및 정보를 바탕으로 작성되었으나, 오차가 있을 수 있고 상이한 정보가 포함되어 있을 수 있습니다. 이에 당사는 어떠한 경우에도 정보의 정확성이나 완전성을 보장하지 않으며, 필요한 경우 이용자는 발행인이 직접 작성·공개한 정보를 통해 사실 여부를 확인하여야 합니다.

· 당사는 본 자료가 공개 되기 이전 제3자에게 사전 제공한 사실이 없습니다. 본 자료의 발행인을 포함하여 그 누구도 본 가상자산의 가치 또는 지급을 보증하지 않습니다. 본 가상자산은 시장 상황, 기술적 변화, 규제 동향 등에 따라 가치가 크게 변동할 수 있으며, 가상자산 투자는 원본 손실이 발생할 수 있습니다.

· 당사는 본 자료와 관련한 이용자의 투자 결과 일체에 대하여 어떠한 책임도 지지 않습니다.

· 본 자료는 어떠한 경우에도 이용자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다. 본 자료의 저작권은 당사에 있고, 국내 코인마켓거래소가 본 자료의 출처를 정확하게 명기하여 사용하는 경우 외에는 어떤 형태로든 당사의 동의 없이 복제, 변형, 재배포 될 수 없습니다.

UPbit Copyright © 2017 - 2024 Dunamu Inc. All rights reserved.