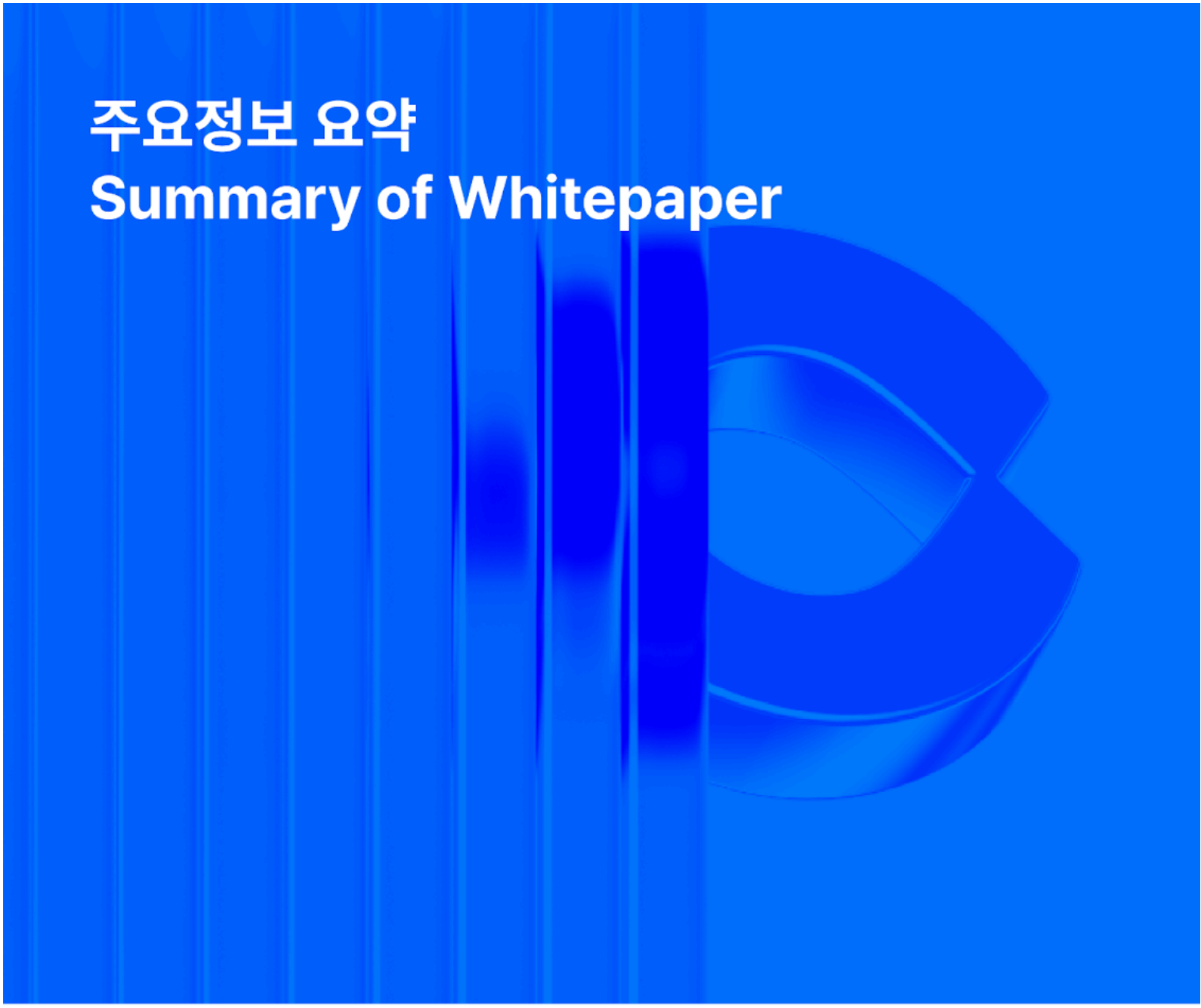
주요정보 요약
Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

coinone

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://yala.org/
참고문헌 (백서, Docs 등)	https://docs.yala.org/
	https://yala.org/whitepaper.pdf
	https://x.com/yalaorg/status/1945809197465309406

1. 프로젝트 정보

소개

Yala는 비트코인 보유자가 자산 소유권을 포기하지 않고도 DeFi 및 실물 자산(RWA)에서 실질 수익(real yield)을 얻을 수 있도록 하는 비트코인 네이티브 유동성 프로토콜입니다.

우리의 이름 (Our Name)
"Yala"는 산스크리트어로 "머무는 곳" 또는 "쉼터"를 의미합니다. 이는 비트코인을 생산적으로 쉬게 하면서 탈중앙화 금융(DeFi) 및 실물 자산(RWA) 수익을 얻을 수 있게 해주는 프로토콜의 이름으로 잘 어울립니다. 자산을 이리저리 옮기게 하는 대신, Yala는 비트코인이 작동할 수 있는 안정적인 기반을 제공합니다.

우리 팀 (Our Team)
저희 팀은 크립토와 전통 금융 모두에 걸친 전문 인력으로 구성되어 있습니다. 창립 멤버는 다음과 같습니다:

- MakerDAO 프로토콜 전 설계자 – DeFi에서 가장 견고한 담보 시스템을 설계한 인물들
- Circle 전 엔지니어링 리드 – 수십억 달러 규모의 규제된 스테이블코인 준비금을 관리한 인물들
- Microsoft 클라우드 인프라 전문가 – 보안 및 확장성에 중점
- Capital One 파생상품 트레이더 – RWA 시장에 대한 전문성 보유

이는 단순한 DeFi 팀이 아닙니다 — 서로 잘 교류하지 않던 두 세계를 연결하는 팀입니다.

우리의 비전: 비트코인 수익의 기준을 만들다
Yala의 미션은 간단합니다:
"비트코인의 주권을 침해하지 않으면서 생산성을 높이는 것."

우리는 비트코인이 고립된 자산 상태를 벗어나 100조 달러 이상의 RWA 시장에 안전하고 지속 가능하게 접근할 수 있도록 인프라를 구축하고 있습니다.

Yala는 세 가지 핵심 원칙에 기반합니다:

- 보안 (Secure): 당신의 비트코인은 비트코인 블록체인에 그대로 존재합니다. Yala는 신뢰 최소화 아키텍처를 사용해 커스터디 리스크 없이 효용을 실현합니다.
- 기관급 접근성 (Institutional-Grade Access): 고액 자산가 및 기관 투자자에게 전통적으로 한정되어 있던 전문 운용 RWA 수익 기회에 접근할 수 있습니다.
- 투명한 리스크 관리 (Transparent Risk Management): 모든 전략은 검증 가능한 담보 및 감사를 통해 입증된 성과 기반으로 운영됩니다 — 블랙박스 없이, 숨겨진 요소 없이.

Yala는 비트코인을 수동적 자산에서 전 세계 온체인 유동성의 능동적인 엔진으로 탈바꿈시킵니다.

시장 과제

비트코인은 원래 단순성, 보안성, 탈중앙화를 핵심으로 설계된 최초의 탈중앙화 암호화폐입니다. 그 스크립트 언어와 아키텍처는 복잡한 금융 로직이 아닌 P2P 가치 전송에 초점을 맞추고 있습니다. 그 결과 비트코인은 가장 안전하고 널리 인식된 디지털 자산이 되었지만, 빠르게 확장 중인 DeFi 생태계와는 여전히 단절된 상태입니다.

반면, 이더리움과 같은 블록체인은 스마트 계약 기능과 모듈형 설계를 통해 대출, 차입, 스테이킹 등 다양한 서비스를 지원하도록 발전해왔으며, 이는 DeFi의 비옥한 기반이 되었습니다. 이에 비트코인 보유자는 자산을 활용하기 위해 BTC를 매도하거나 래핑하여 다른 체인에서 사용하는 수밖에 없는 제한적인 선택지를 갖게 되었습니다.

비트코인의 아키텍처적 선택—즉 탈중앙화와 보안을 확장성보다 우선시한 설계—는 직접적인 DeFi 통합을 어렵게 만들었습니다. 라이트닝이나 사이드체인 같은 레이어 2 솔루션이 부분적인 개선을 제공하기는 하지만, 사용자 경험, 상호운용성, 유동성 깊이 면에서 종종 타협을 요구합니다.

비트코인 보유자를 위한 실물자산 수익 개방
Yala는 이 간극을 메우는 비트코인 네이티브 유동성 프로토콜입니다.

Yala는 비트코인 보유자가 자산의 보관 권한(custody)을 포기하지 않고도 DeFi와 실물자산(RWA)에서 실질 수익(real yield) 을 얻을 수 있도록 지원합니다.
Yala의 안정적이고 모듈형인 인프라를 통해, 사용자는 비트코인을 예치하고 $YU를 민트할 수 있으며, 이는 비트코인 기반 스테이블코인으로서 크로스체인 유동성과 수익성의 관문 역할을 합니다.

Yala를 통해 사용자는 다음을 수행할 수 있습니다:

- 비트코인을 예치하고 $YU 민팅: 과담보 기반의 퍼미션리스 메커니즘을 통해 매끄럽게 실행 가능
- $YU를 다양한 체인에서 활용: EVM 및 비-EVM 체인 모두에서 대출, 스테이킹, AMM 유동성 공급 등 DeFi 수익 전략에 참여
- 실물자산 수익 기회에 접근: 토큰화된 부동산이나 신용 시장 등과 연계된 RWA 파트너를 통해 실질 수익 노출
- BTC 네이티브 스테이킹 참여: 유동 스테이킹 옵션으로 비활성 BTC를 온체인 수익 자산으로 전환

Yala의 미션
Yala의 미션은 세상에서 가장 저활용된 자산인 비트코인을, 전 세계 온체인 유동성의 기반으로 전환시키는 것입니다. 이를 위한 설계 철학은 다음과 같습니다:

- 보안성 (Secure): 비트코인의 핵심 가치에 뿌리를 둔, 신뢰 최소화 인프라 기반 구축
- 조합성 (Composable): 주요 블록체인 생태계 및 RWA 네트워크와 상호운용 가능
- 자본 효율성 (Capital-Efficient): $YU 및 BTC 네이티브 스테이킹 레이어를 활용한 이중 수익 전략 지원
- 탈중앙성 (Decentralized): 커뮤니티에 의해 거버넌스되고, 투명하게 운영됨

얄라 비트코인 브릿지

핵심 설계 원칙
Yala Bridge는 전통적인 브릿지 구현에서 나타나는 보안 및 중앙화 문제를 해결하기 위해 특별히 설계된 크로스체인 비트코인 통합의 중대한 진보입니다. 기존 커스터디 방식의

브릿지와 달리, Yala는 비트코인의 보안 보장을 훼손하지 않기 위해 임계값 암호 기술(threshold cryptography)을 활용한 탈중앙화 공증 시스템(notary system)을 구현했습니다.

이를 통해 사용자는 탈중앙화와 자기보관(self-custody)이라는 비트코인의 핵심 가치를 희생하지 않고도, 비트코인을 담보로 이더리움 DeFi 생태계에 접근할 수 있습니다.

기술 아키텍처

1. BTC 예치 및 암호학적 증명

브릿지 프로세스는 고급 암호 증명 기법이 포함된 비트코인 예치 절차로 시작됩니다. 사용자는 임계값 서명 방식으로 생성된 P2WSH 주소로 BTC를 전송하며, 이 트랜잭션에는 OP_RETURN 필드에 목적 블록체인의 주소 정보가 포함됩니다.

이 예치는 중앙 커스터디 기관으로의 자산 이전이 불필요하며, 스크립트에는 시간 잠금(time-locked) 복구 경로가 포함되어 있어, 브릿지 실패 시 일정 시간이 지나면 사용자가 비트코인을 스스로 회수할 수 있도록 보장합니다.

2. 다중 임계값 검증 프레임워크

예치 후에는 분산형 공증 프로토콜 기반의 정교한 다중 검증 구조가 작동합니다.

- 결정적 검증자 선택:

Bitcoin 블록 해시에서 생성된 검증 가능한 난수 함수(VRF)를 사용해 11명의 공증인 중 9명을 무작위로 선택합니다. 이 방식은 검증자 담합 및 공격 가능성을 낮춥니다.

- 크로스체인 증명:

선택된 공증인들은 해당 BTC 트랜잭션의 포함 및 6 컨펌 이상 완료 여부를 독립적으로 검증한 뒤, 임계값 서명으로 증명합니다.

- 다단계 검증:

(a) UTXO 존재, (b) 스크립트 구성의 적절성, (c) 컨펌 깊이, (d) 목적지 주소 확인 등을 독립 경로로 중첩 검증합니다.

3. Cubist 하드웨어 기반 스마트 계약 기술 적용

Yala Bridge의 보안은 Cubist의 하드웨어 보안 스마트 계약(CubeSigner) 기술을 기반으로 합니다. 이는 일반적인 멀티시그 또는 MPC 설정이 아닌, 비트코인 상의 스마트 계약과 유사한 보안 정책을 하드웨어 수준에서 적용하는 방식입니다.

- 정책 기반 키 관리:

키는 보안 하드웨어에 저장되며, 정교한 사용 정책에 따라 작동합니다. 이는 비트코인에서 정책 기반 자산 흐름 제어를 실현합니다.

- 하드웨어 보안 보장:

개인 키는 일반 메모리에 노출되지 않으며, 모든 트랜잭션은 사전 정의된 정책을 따라야 합니다.

- 프로그램 기반 자산 흐름 제어:

① 예치된 BTC는 담보로 사용되거나 원래 예치자에게만 반환 가능
② 거버넌스 변경은 다자 승인이 필요하며, 타임 딜레이 적용
③ 특정 트랜잭션 제한 및 타이밍 제약으로 공격 위험 완화

- 내장 복구 메커니즘:

필수적인 시간 잠금 복구 경로(time-locked recovery path)가 포함되어 있어, 사용자에게 자산 최종 통제권이 유지됩니다.

YBTC 민팅 프로세스

검증이 완료되면, 대상 체인의 스마트 계약이 YBTC(토큰화된 비트코인)를 사용자의 주소로 민팅합니다. 이 과정에는 다음과 같은 보안 기능이 포함됩니다:

- 원자성 보장: 민팅은 완전 실행되거나 전면 취소되므로, 시스템 불일치를 방지합니다.
- 공급 검증: 계약은 시스템 내 잠긴 BTC에 대해 암호학적으로 커밋된 공급량을 유지합니다.
- 공증 검증: 민팅 전, 공증인 서명의 임계값 도달 여부를 암호학적으로 검증합니다.

보안 고려사항

Yala Bridge는 크로스체인 브릿지의 주요 공격 벡터를 해결하도록 설계되었습니다:

- 브릿지 침해 저항성:

일부 노드가 손상되어도 임계값 서명 구조로 인해 불법 민팅이나 자산 탈취가 불가합니다. 토큰 인센티브와 패널티 메커니즘으로 정직한 행위를 유도합니다.

- 체인 재편성 방어:

Bitcoin 측에서 6 컨펌 요구는 재편성 공격에 대한 통계적 안전성을 제공하며, 공증인 검증이 추가적 보호를 제공합니다.

- 경제적 보안:

검증자는 상당한 담보를 스테이킹해야 하며, 악의적 행위에 대한 패널티가 존재합니다. 이는 브릿지 TVL에 따라 확장 가능한 경제적 공격 억제력을 형성합니다.

- 출구 보장:

대부분 브릿지와 달리, Yala는 시간 잠금 기반 복구 경로를 통해 사용자가 언제든 자산을 회수할 수 있는 암호학적 보장을 제공합니다.

2. 토큰 이코노미

가상자산 소개

$YALA 토큰은 세 가지 핵심 기능을 수행합니다: 참여 유인, 프로토콜 인프라 보안, 거버넌스 기능 제공.

$YALA는 Yala 크레딧 시스템을 구동하는 거버넌스 및 유틸리티 토큰으로, 탈중앙화된 의사결정 구조의 기반이 되며, 생태계 전반에 걸쳐 다양한 유틸리티를 제공하고, 스트레스 상황에서 시스템 재자본화의 역할도 수행합니다.

핵심 토큰 유틸리티

1. 스태빌리티 풀 보상 (Stability Pool Rewards)

$YU를 스태빌리티 풀에 예치하면 청산 시 시스템 부채를 보전하며, 이에 대한 보상으로 $YALA, 청산 담보 일부, 안정성 수수료를 받습니다. 이는 프로토콜 리스크 관리의 핵심 축을 이룹니다.

2. 암호경제 기반 보안 (Cryptoeconomic Security)

$YALA는 노터리 브릿지의 크로스체인 시스템과 $YU 스테이블코인의 안정성을 LayerZero 기반 분산 검증 네트워크를 통해 보호하며, 이 과정에서 스테이킹된 $YALA가 사용됩니다.

3. 거버넌스 진화 (Governance Evolution)

프로토콜이 탈중앙화됨에 따라 $YALA는 핵심 거버넌스 도구로 기능합니다. 토큰 보유자는 프로토콜 매개변수 투표, 개선 제안 제출, $veYALA를 통한 게이지 가중치 투표(보상 배분 방향 설정)에 참여할 수 있습니다.

거버넌스 프레임워크

프로토콜은 세 가지 제안 유형에 따라 운영됩니다:

1. 핵심 프로토콜 변경: 유통량의 5% 이상 필요, 투표 기간 7일, 정족수 50%

2. 매개변수 조정: 제안 기준 1%, 투표 기간 3일, 정족수 20%
3. 긴급 제안: 다중 서명으로 시작, 24시간 이내 투표, 승인률 67% 이상 필요

$YALA 보유자는 전문가, 커뮤니티 구성원, 자동화 전략 등에 자신의 투표권을 위임할 수 있습니다.

생태계 개발 전략

- $YU 유동성 풀, $YALA 거래쌍, 크로스체인 브릿지에 전략적 자금 지원
- 개발자 보조금: 통합, 도구, 보안 감사, 리서치 지원
- 커뮤니티 프로그램: 버그 바운티, 교육, 앰배서더 리워드, 거버넌스 참여 인센티브

지속가능성 설계

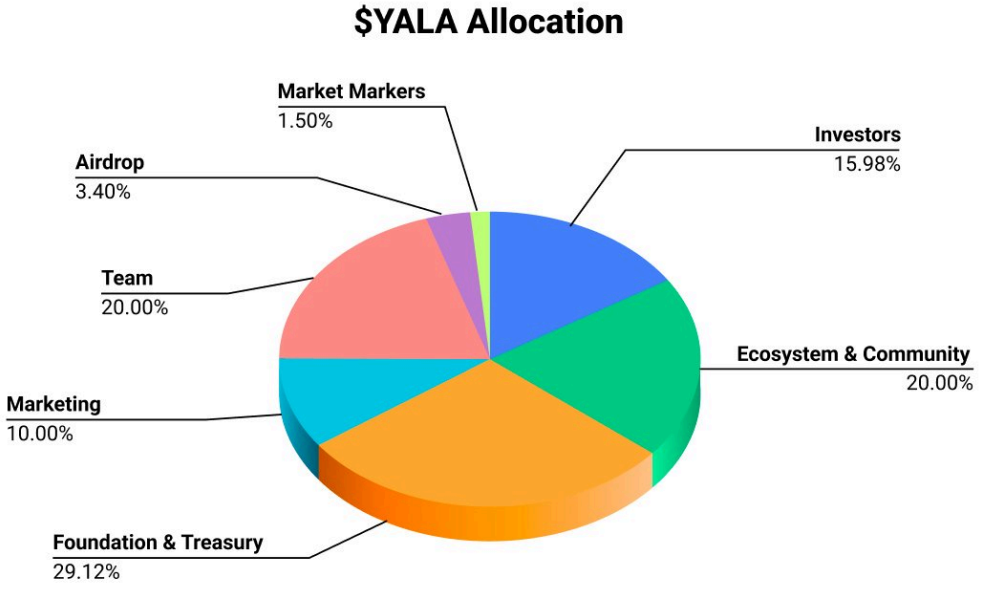
- 프로토콜 수수료는 토큰 매입 수요를 유도하며, 엄격한 베스팅 스케줄로 공급 충격을 방지
- $YALA 유틸리티는 지속적으로 확장되며, 트레저리는 시장 안정성 확보를 위한 전략적 대응 자산 역할을 수행합니다.

발행량 및 유통량계획

토큰 분배

총 공급량은 1,000,000,000개로, Yala 생태계의 이해관계자 간 장기적 지속 가능성과 이익 정렬을 고려하여 설계되었습니다.

- 투자자(15.98%): 1년 락업 후, 18개월간 분기별 베스팅
- 생태계 및 커뮤니티(20%): TGE 시점에 45% 분배, 이후 24개월간 선형 베스팅
- 재단 및 트레저리(29.12%): TGE 시점에 30% 분배, 1년 락업 후 36개월간 선형 베스팅
- 마케팅(10%): TGE 시점에 20% 분배, 1년 락업 후 24개월간 선형 베스팅
- 팀(20%): 1년 락업 후 24개월간 매월 선형 베스팅
- 에어드랍(3.4%): TGE 시점에 전량 해제
- 마켓 메이커(1.5%): 마켓 메이킹 계약에 따라 배분

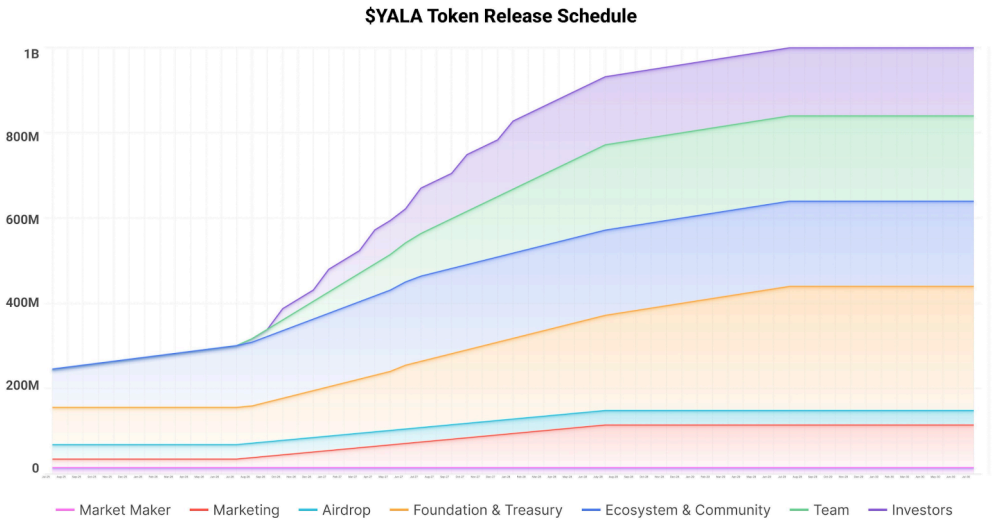


출처: YALA X

토큰 출시 일정

1년 차: 에어드랍 및 생태계 일부 물량만 배분. 투자자 및 팀 물량은 전면 락업.
2년 차: 투자자(18개월), 팀(24개월) 스케줄에 따라 순차적 해제 시작.

3년 차 이후: 대부분의 토큰이 유통되며, 트레저리는 전략적으로 유동성 공급을 이어감.



출처: YALA X

위험고지 안내
Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.

coinone