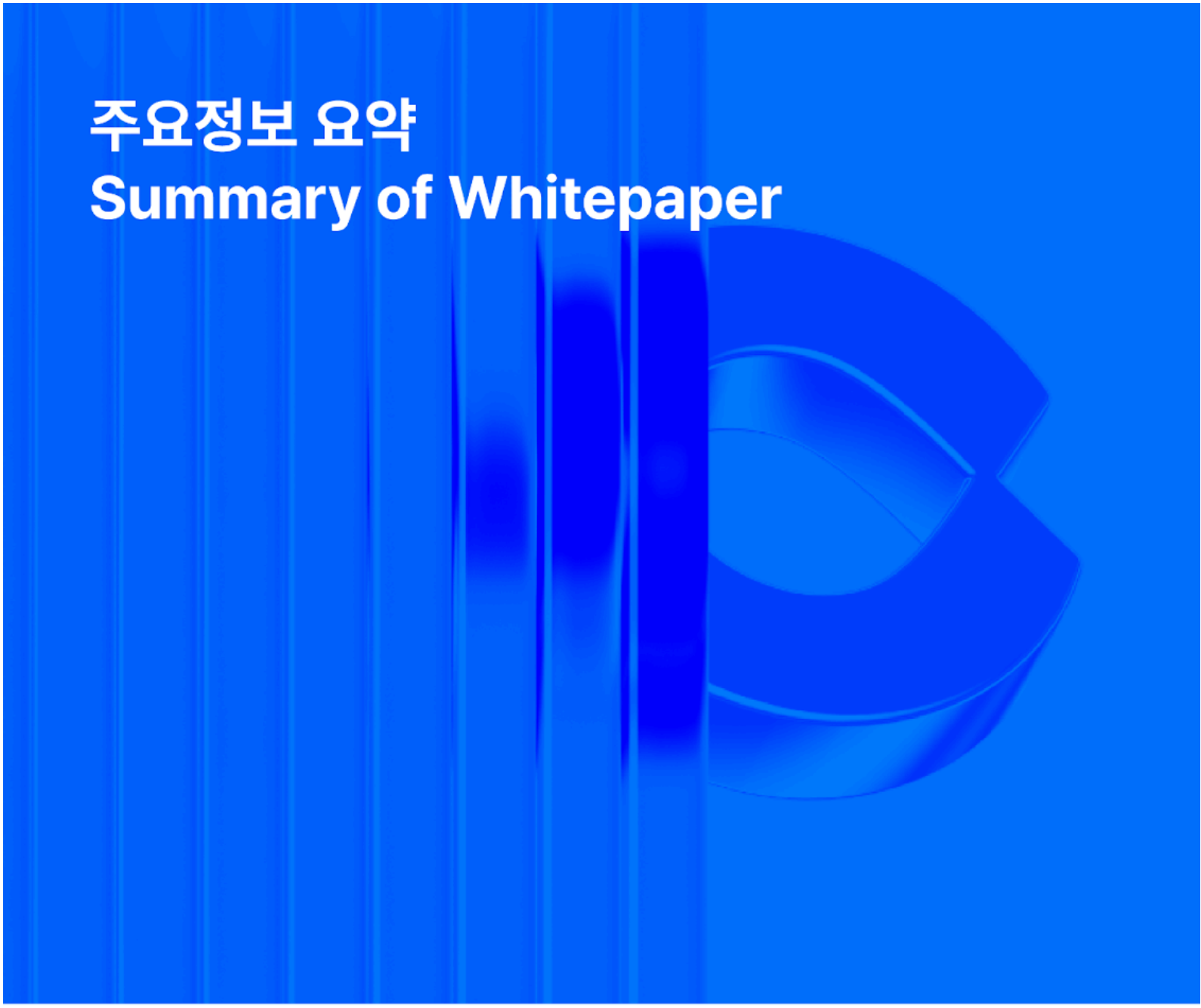
주요정보 요약
Summary of Whitepaper



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	Merlin Chain
홈페이지	https://merlinchain.io/
참고문헌 (백서, Docs 등)	https://docs.merlinchain.io/merlin-docs

1. 프로젝트 정보

소개

Merlin Chain은 여러 첨단 기술을 통합한 비트코인 레이어 2 솔루션입니다. 주요 기술로는 ZK-Rollup 네트워크, 탈중앙화 오라클 네트워크, 데이터 가용성(Data Availability), 그리고 온체인 비트코인 사기 방지 모듈(On-chain BTC fraud-proof modules)이 포함됩니다. Merlin의 핵심 목표는 자체 레이어 2 네트워크를 활용해 비트코인의 네이티브 자산, 프로토콜, 제품 등을 레이어 1에서 강화하는 데 있으며, 궁극적으로 "Make Bitcoin Fun Again"이라는 슬로건을 실현하는 것입니다.

Merlin Chain은 2024년 1월에 출시되었으며, Jeff Yin이 설립한 회사인 Bitmap Technology에서 시작된 신규 프로젝트입니다. 이 프로젝트의 목적은 비트코인을 대체하기보다 그 가치를 강화하고 확장하는 데에 있습니다.

핵심 모듈

Merlin 체인은 비트코인 네트워크 상의 레이어 2 솔루션으로서, 확장성, 효율성, 기능성을 강화하기 위해 다양한 혁신 기술을 조합하여 활용하고 있습니다. Merlin Chain의 5가지 핵심 모듈은 다음과 같습니다:

- ZK-Rollup 네트워크
- 탈중앙화 오라클 네트워크
- 데이터 가용성
- 2단계 ZKP 제출 메커니즘
- 비트코인 기반 사기 방지 모듈

ZK-Rollup 네트워크

Merlin 체인은 Taproot 기반의 집합형 제로 지식 증명(aggregated zero-knowledge proof)과 롤업 데이터를 비트코인 메인넷에 기록하는 방식의 솔루션을 제안합니다. 이를 통해 고도로 확장 가능한 ZK-Rollup을 구현하며, 비트코인 네트워크의 튜링 불완전성(Turing Incompleteness) 문제를 해결합니다.

이 네트워크는 거래 데이터를 묶어 집계(batch)하고 압축하여, Taproot 기반 제로 지식 증명을 사용해 비트코인 메인넷에 제출합니다. 핵심 구성 요소는 다음 세 가지입니다: 노드, zkProver, 데이터베이스. 이 구성 요소들은 데이터 처리 및 검증이 매끄럽게 이루어질 수 있도록 상호작용하며 다음과 같은 기능을 수행합니다:

- 노드

        - 거래 데이터를 처리하고 전송하며, zkProver 및 데이터베이스와 상호작용합니다.
        - Merkle Tree의 내용을 데이터베이스에 전송하고 저장합니다.
        - 거래 입력 데이터를 zkProver에 전달하여 처리하게 합니다.
        - zkProver와 상호작용하여 거래의 유효성과 정확성을 검증합니다.
    - zkProve
        - SNARK 기술을 활용하여 제로 지식 증명을 생성하고, 거래의 유효성과 정확성을 증명합니다.
        - 총 13종의 상태 머신을 포함하며, 주요 상태 머신과 BinarySM, StorageSM, MemorySM, ArithmeticSM 등과 같은 하위 상태 머신으로 구성됩니다.
        - PIL(Polynomial Identity Language)을 활용해 상태 전이 및 제약 조건을 다항식으로 변환하고, 이를 스마트 컨트랙트에서 검증합니다.
        - Merkle Root, 관련 sibling key, 해시 값 등의 정보를 바탕으로 검증 가능한 거래 증명을 생성합니다.
        - 생성된 증명을 노드로 다시 전송하여 추가 검증 및 기록을 수행하며, 거래의 합법성과 보안을 보장합니다.
    - 데이터베이스
        - Merkle Tree의 내용 및 거래 정보를 포함한 중요 데이터를 저장하는 역할을 합니다.
        - 노드가 전송한 Merkle Tree의 내용을 수신하고 저장합니다.
        - zkProver가 거래 증명을 생성하는 데 필요한 정보를 제공합니다.

이 모델이 Merlin에 가져오는 주요 이점은 다음과 같습니다.

- 보안: 비트코인의 보안성을 그대로 계승하며, L2 배치 처리 확장성을 제공함으로써 데이터가 비트코인에 영구히 고정되고 변조될 수 없습니다.
- EVM 호환성: 기존 스마트 계약 및 도구들과 호환되어 상호운용성을 보장합니다.
- 저비용: ZK 및 zkSNARK 기술을 사용해 L1 공간 소비를 줄이고, 거래 비용을 최적화합니다.
- 고성능: 잦은 유효성 증명을 통한 빠른 거래 최종성을 확보하며, 반복형 STARK를 기반으로 높은 사용자 수요와 동시성을 감당할 수 있는 확장성을 제공합니다.

탈중앙화 오라클 네트워크

Merlin 체인은 분산형 오라클 네트워크를 채택하고 있습니다. 시퀀서 노드(Sequencer nodes)는 거래를 수집하고 일괄 처리(batch processing)하며, 압축된 거래 데이터, ZK 상태 루트, 증명 데이터를 생성하는 역할을 합니다. 이 데이터는 오라클 네트워크를 통해 정리되어 비트코인의 Taproot에 업로드되며, 네트워크 전반에 걸쳐 공개적으로 접근 가능합니다. 구체적인 메커니즘은 다음과 같습니다:

- ZK 증명의 비트코인 확정을 위해 특별히 설계된 사기 방지(fraud-proof) 메커니즘을 구현합니다.
- 모든 원시 데이터는 오라클 네트워크에 저장되며, 이에 대응하는 상태 루트는 비트코인 네트워크에 기록됩니다.
- 사용자는 언제든지 Merlin 체인에 기록된 모든 집계 거래 데이터를 조회할 수 있습니다.
- ZK 증명을 통해 데이터의 정확성과 유효성을 특정 데이터 내용 노출 없이 검증할 수 있습니다.

Merlin Chain은 데이터와 권한의 탈중앙화를 통해 단일 실패 지점(SPoF) 및

중앙집중화로 인한 리스크를 방지합니다. 또한 멀티시그 및 콜드 스토리지 기술을 통해 예치 자산의 보안을 강화합니다. 스테이킹 및 보상 분배 절차는 모두 투명하고 개방되어 있어, 사용자가 자신의 스테이킹 상태와 예상 수익을 언제든지 확인할 수 있습니다.

스테이킹 노드 설계는 다음과 같습니다.

- 다양한 자산 지원: BTC, MERL, 기타 주요 BRC-20 자산의 스테이킹을 지원하여 유연성과 리스크 분산을 제공합니다.
- 스마트 계약 기반 관리: 모든 대리 스테이킹 및 보상 분배는 스마트 계약을 통해 자동화되며, 불변성과 공정성을 보장합니다.
- 실시간 모니터링: 사용자는 대리 스테이킹 현황 및 수익률을 실시간으로 확인할 수 있으며, 프록시 노드의 성능 지표도 열람할 수 있습니다.
- 유연한 출금 메커니즘: 사용자는 유동성을 확보할 수 있도록, 언제든 자산을 인출할 수 있는 유연한 출금 구조를 이용할 수 있습니다.

데이터 가용성

Merlin 팀은 Celestia 및 Nubit과 협력하여 현재의 데이터 가용성 솔루션을 최적화하고 있습니다. 이 협력은 블록 데이터의 검증 가능성과 네트워크 투명성, 신뢰성을 높이는 데 목적이 있습니다.

- 공개 데이터 가용성: 곧 도입될 데이터 가용성(DA) 솔루션은 공개 데이터 가용성을 보장하여 누구나 Merlin Chain의 상태 정보를 열람하고 저장할 수 있도록 합니다.
- 이력 데이터 저장: 데이터가 DA 네트워크에 게시되고 확정되면, 롤업 및 각종 응용 프로그램이 해당 데이터를 영구적으로 저장하는 역할을 수행합니다.
- 데이터 가용성 검증: 노드가 새로운 블록을 수신할 때마다, 해당 데이터가 완전하고 일관되게 네트워크 상에 존재하는지를 확인합니다.

2단계 ZKP 제출 메커니즘

Merlin 체인은 Lumoz에서 제안한 이단계 제로 지식 증명(ZKP) 제출 메커니즘을 채택하여 탈중앙화된 작업 증명(PoW)을 구현합니다.

- 해시 제출 단계 (Hash Submission)
    - Prover는 특정 시퀀스에 대한 ZKP를 생성하고, 먼저 해당 증명 및 주소에 대한 해시 값을 계산합니다.
    - 이 해시와 prover의 주소는 체인 레벨의 스마트 계약에 제출됩니다.
    - 증명은 해당 시퀀스에 대한 ZKP를 나타내고, 주소는 해당 prover를 식별합니다.
    - 초기 해시 제출은 누구나 자유롭게 할 수 있으며, T+10 블록 내에서 처리 및 승인됩니다.
    - T+11 블록 이후에는 새로운 prover가 해시를 추가 제출할 수 없습니다.
- ZKP 제출 단계 (ZKP Submission)
    - T+11 블록 이후에는 누구나 전체 ZKP를 제출할 수 있습니다.
    - 검증된 ZKP는 이전에 제출된 모든 해시들을 검증하는 데 사용됩니다.
    - prover는 자신의 스테이킹 비율에 따라 PoW 보상을 받게 됩니다.

이 메커니즘은 채굴자들이 온라인 상태를 유지하도록 유도하여, 안정적인 연산 환경을 조성하며 네트워크의 보안성과 신뢰성을 다음과 같은 방식으로 강화합니다:

- 레이스 공격 방지: 악의적인 참여자가 다량의 증명을 무작위로 제출하여 시스템을 교란하거나 손상시키는 것을 방지합니다.
- 지속적인 참여 유도: 보상을 통해 채굴자들이 연속적이고 안정적인 ZKP 연산을 제공하도록 장려함으로써, 전체 네트워크의 보안성과 신뢰성을 높입니다.
- 시스템 효율성 확보: 자원 낭비와 네트워크 혼잡을 줄이고, 전반적인 시스템 성능과 안정성을 개선합니다.

비트코인 기반 사기 방지 모듈

Merlin 체인은 데이터 무결성과 보안을 한층 강화하기 위해 사기 방지(Fraud Proof) 메커니즘을 도입합니다. 이 메커니즘은 Prover(증명자)와 Verifier(검증자) 두 역할을 기반으로 구성되며, 구현 절차는 다음과 같습니다:

- 사전 서명된 거래
  - Prover와 Verifier는 일련의 거래에 사전 서명하여, 챌린지-응답 기반의 검증 절차를 가능하게 합니다.
- 이진 회로 변환
  - Prover는 검증 대상 프로그램을 다수의 NAND 논리 게이트로 구성된 이진 회로로 변환하여 데이터의 무결성과 정확성을 확보합니다.
  - 각 논리 게이트는 동작 방식과 기능을 설명하는 leaf 스크립트를 포함합니다.
- Merkle Tree 제출
  - Prover는 각 논리 게이트의 leaf 스크립트를 대규모 이진 회로로 구성된 Merkle Tree에 삽입하고, 그 루트를 Taproot 주소에 제출합니다.
- 검증 절차
  - Verifier는 Taproot 주소에서 Merkle Root를 추출하여 유효성을 검증합니다.
  - 제출된 Merkle Root에 데이터 오류나 부정행위가 의심될 경우, Verifier는 챌린지-응답 절차를 발동할 수 있으며, Prover에게 해당 leaf 스크립트나 대체 증명을 요구합니다.
  - Prover는 제출된 Merkle Root의 정당성을 입증하기 위한 증거를 제공해야 합니다.
  - Verifier는 제출된 증거를 검토하여, 데이터의 유효성과 무결성을 최종 확인합니다.

이 외에 사용자 가이드, 중요 개념 등과 관련한 상세 내용은 여기에서 확인할 수 있습니다.

개발자 가이드

Merlin Chain은 Polygon CDK 위에 구축된 최초의 비트코인 레이어 2 솔루션으로, ZK-Rollup 네트워크, 탈중앙화 오라클 네트워크, 온체인 BTC 사기 방지 모듈 등을 완전히 통합하고 있습니다. 이러한 첨단 기술을 바탕으로 Merlin Chain은 비트코인 사용자에게 다음과 같은 이점을 제공합니다:

- 훨씬 낮은 수수료
- 간소화된 운영 구조
- 향상된 기능성

- 넓은 자산 호환성

Merlin의 사명은 비트코인의 고유 기능을 강화하여 사용성을 보다 효율적이고 즐겁게 만들며, 궁극적으로 “Make Bitcoin Fun Again”을 실현하는 데에 있습니다.

Merlin Chain은 다수의 이더리움 EIP, 프리컴파일, 오퍼코드를 지원합니다. 따라서 개발자는 기존 EVM 체인에서 사용되던 스마트 계약, 개발 도구, 지갑 등을 변경 없이 쉽게 배포할 수 있습니다. 이는 비트코인 생태계 자산을 포함한 환경 내에서 더욱 풍부한 개발 경험을 제공합니다.

본 섹션에서는 아래 내용을 포함한 Merlin Chain dApp 배포를 위한 튜토리얼 및 개발자 안내서를 포괄적으로 제공합니다:

- [Builder Guides]
- [Junior Builder Guides]
- [Run a Merlin Node (출시 예정)]

메인넷

항목명	값
네트워크 이름	Merlin Mainnet
설명	Merlin의 퍼블릭 메인넷
RPC URL	https://rpc.merlinchain.io * 속도 제한이 있으며, 프로덕션 백엔드 시스템에서는 권장되지 않음
체인 ID	4200
통화 심볼	BTC
블록 익스플로러	https://scan.merlinchain.io

수수료

Merlin Chain의 거래 수수료는 두 가지 요소로 구성됩니다:

- L2 거래 실행 수수료
- L1 보안 수수료

현재는 L2 실행 수수료만 부과되고 있으며, 이는 다른 EVM 호환 체인들과 유사한 가스 모델을 따릅니다. 각 거래는 일정량의 가스를 소비하며, 사용자는 거래 시 gas 단가(Gas Price)를 지정할 수 있습니다.

Merlin Chain은 이더리움의 EIP-1559 이전 가스 모델을 사용합니다. 사용자는 거래 실행 시 다음 두 항목만 지정하면 됩니다: Gas Price, Gas Limit.

- 기본 가스 토큰: BTC (Merlin_BTC)
- MERL 토큰도 AA 지갑 내에서 가스 비용으로 사용 가능
- 단, BTC는 18자리 소수(기존 8자리와 다름)를 사용하여 EVM 호환 체인과의

일관성을 유지

비트코인 네트워크에서 Merlin Chain으로 자산을 전송하려면 다음과 같은 브릿지를 사용할 수 있습니다:

- 공식 브릿지: https://merlinchain.io/bridge
- 커뮤니티 기반 브릿지(사용자 책임 하에 이용):
  - https://unicross.xyz/bridge
  - https://meson.fi

2. 토큰 이코노미

가상자산 소개

MERL은 Merlin Chain 생태계의 네이티브 토큰으로서 거버넌스, 보안, 거래 수수료, 스테이킹, 유동성 및 담보 등 다방면에서 핵심적 역할을 하며, Merlin Chain의 지속적 성공과 성장에 결정적인 역할을 합니다.

- 거버넌스

MERL 보유자는 Merlin Chain에서의 주요 제안에 대해 투표할 수 있는 권리를 가지며, 참여자 집단의 의사를 반영한 커뮤니티 기반 거버넌스를 실현합니다.

- 스테이킹

MERL 스테이킹을 통해 네트워크의 보안성을 강화할 수 있습니다. 이는 Sybil 공격을 방지하고, 악의적 참여자에 대한 슬래싱, 참여자와 생태계 성공 간의 연계를 유도합니다.

- 트랜잭션 수수료

MERL은 Merlin Chain 기반의 레이어3 네트워크에서 거래 수수료 지불에 사용됩니다. 이를 통해 네트워크 내 원활한 경제 활동을 지원합니다.

- 합의 노드 위임

MERL 보유자는 자신이 직접 MERL을 스테이킹하거나, 합의 노드에 위임할 수 있으며, 이는 네트워크의 분산성과 확장성을 지원하는 핵심 요소입니다.

- 유동성 및 담보

MERL은 생태계 내 유동성과 담보 자산으로 사용될 수 있으며, 대출 및 기타 금융 메커니즘을 지원하여 네트워크의 안정성을 높입니다.

발행량 및 유통량계획

MERL의 총 공급량은 2,100,000,000개이며, TGE(Token Generation Event) 시점부터 시작하여 4년에 걸쳐 점진적으로 유통됩니다. 초기 4년간의 토큰 분배는 다음과 같습니다:

분배율

분류	총 발행량 대비 비율	설명
Merlin’s Seal 참가자	20.00% (420,000,000 MERL)	Merlin’s Seal 이벤트 참여자 대상 에어드랍

퍼블릭 세일	1.00% (21,000,000 MERL)	People’s Launchpad를 통한 퍼블릭 세일 할당
프라이빗 투자자	15.23% (319,830,000 MERL)	프라이빗 투자자 A 라운드(1.33%) 및 B 라운드(13.90%)에 배정
어드바이저	3.00% (63,000,000 MERL)	프로젝트 어드바이저에게 할당
팀	4.20% (88,200,000 MERL)	프로젝트 팀에 할당
커뮤니티	16.57% (348,000,000 MERL)	생태계 계획 및 커뮤니티 리워드 용도
생태계	40.00% (840,000,000 MERL)	생태계 개발 보조금 및 애플리케이션 성장 유인책으로 사용

베스팅 일정

분류	초기 언락	분배 일정
Merlin’s Seal 참가자	TGE 시점에 50%	이후 5개월간: 25%, 12.5%, 6.25%, 3.125%, 3.125%
퍼블릭 세일	TGE 시점에 50%	이후 5개월간: 25%, 12.5%, 6.25%, 3.125%, 3.125%
프라이빗 투자자	없음	A 라운드: 6개월 락업 후 18개월간 분배 B 라운드: 12개월 락업 후 36개월간 분배
어드바이저	없음	락업 후 30개월 동안 분배
팀	없음	락업 후 24개월 동안 분배
커뮤니티	없음	48개월 동안 분배
생태계	없음	48개월 동안 분배

MERL의 주요 마일스톤은 여기에서 확인할 수 있습니다.

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