캐스퍼(CSPR)

주요내용설명서(국문백서)

Korean White Paper

2026년 3월 19일

Disclaimer

본 번역본은 2026년 3월 19일 기준의 캐스퍼(Casper) 백서와, 캐스퍼 홈페이지의 내용 중 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

빗썸

프로젝트 소개

캐스퍼(Casper)는 지분증명(PoS)[1] 합의 알고리즘과 웹어셈블리(와즘)[2]를 기반으로 작동하는 스마트 컨트랙트[3] 플랫폼으로, (제한된 메모리 환경 내에서) 튜링 완전성[4]을 지원합니다. 또한 누구나 참여할 수 있는 무허가형[5] 탈중앙화 퍼블릭 블록체인입니다.

네트워크의 합의 프로토콜인 주크(Zug)는 고전적인 비잔틴 장애 허용(BFT)[6] 프로토콜에 비해 여러 가지 이점을 제공합니다. 첫째, 주크는 한층 높은 수준의 완결성[7]을 지원합니다. 즉, 네트워크 통신 속도에 맞춰 단 몇 초 만에 모든 블록을 확정합니다. 둘째, 기존 BFT 모델에서는 불가능했던 방식으로 블록 완결성을 처리하여 높은 유연성을 확보했습니다.

또한 캐스퍼 네트워크는 기업과 개발자가 쉽게 도입할 수 있도록 최적화되어 있습니다. 블록체인 기술과 더불어 예측 가능한 수수료, 업그레이드 가능한 스마트 컨트랙트, 온체인 거버넌스, 유연한 프라이버시 설정, 개발자 친화적인 언어 등의 고유한 기능을 통해 비즈니스 운영을 지원합니다. 이러한 핵심 기능 덕분에 개발자와 기업은 블록체인 기술의 이점을 온전히 누릴 수 있습니다.

캐스퍼는 확장성 트릴레마[8] 역시 해결합니다. 특히 네트워크는 보안성, 탈중앙화, 높은 처리량[9]에 최적화되어 있습니다. 캐스퍼는 오픈소스 프로젝트와 기업에 선도적인 솔루션을 제공하기 위해 끊임없이 진화하며 이 모든 것을 달성해 나가고 있습니다. 캐스퍼는 이러한 기술적 완성도를 바탕으로 오픈소스 생태계와 기업 환경 모두를 아우르는 선도적인 솔루션을 제공하며 끊임없이 진화하고 있습니다.

[1] Proof-of-Stake, PoS
[2] WebAssembly (Wasm)
[3] Smart contract
[4] Turing-complete
[5] Permissionless
[6] Byzantine Fault Tolerance, BFT
[7] Finality
[8] Scalability Trilemma
[9] Throughput

캐스퍼의 작동 방식

캐스퍼는 트랜잭션을 검증하고 네트워크를 유지하기 위해 검증인 그룹을 기반으로 운영됩니다. 규모의 경제[10]를 위해 검증인을 중앙화해야 하는 작업증명(PoW)[11] 네트워크와 달리 캐스퍼는 검증인의 지리적 탈중앙화를 지원합니다. 캐스퍼의 검증인들은 스테이킹된 토큰을 바탕으로 트랜잭션을 검증하며 지분증명 합의 메커니즘에 참여한 대가로 캐스퍼 네트워크의 네이티브 토큰인 CSPR를 받습니다.

비즈니스 모델

캐스퍼 네트워크 설계 구조

캐스퍼는 '선 합의 후 실행' 방식을 채택한 계정 기반 모델[12]의 지분증명 블록체인 플랫폼입니다. 네트워크의 모든 데이터는 글로벌 스테이트(Global State)라는 구조에 저장되며 사용자는 트랜잭션에 포함된 세션 코드를 전송하여 이 글로벌 스테이트와 상호작용합니다. 특히 트랜잭션에 와즘 코드를 포함해 네트워크에서 직접 실행할 수 있기 때문에 개발자는 블록체인 전용 언어를 새로 배울 필요 없이 선호하는 일반 프로그래밍 언어를 그대로 사용할 수 있습니다.

트랜잭션은 기본적으로 해당 사용자 계정의 실행 환경 내에서 처리되지만 필요에 따라 독립적인 환경에서 실행되는 와즘 컨트랙트를 호출할 수도 있습니다. 계정 정보를 제외한 사용자의 관련 데이터는 글로벌 스테이트 내에 위조 불가 참조(Unforgeable Reference, URef) 형태로 저장됩니다. 개별 노드가 특정 트랜잭션의 유효성을 승인하면, 이를 생성될 블록에 포함시키고 네트워크 전체가 합의에 도달할 때까지 노드 간에 전파[13]합니다. 합의가 완료된 직후 네트워크는 트랜잭션에 포함된 와즘 코드를 실행합니다.

[10] Economies of scale

[11] Proof-of-Work, PoW

[12] Account-based model

[13] Gossip

실행 구조

캐스퍼 네트워크는 근본적으로 탈중앙화된 연산 플랫폼입니다. 본 섹션에서는 캐스퍼의 연산 모델이 가진 핵심 구조를 설명합니다.

연산 작업량 측정

네트워크 상의 모든 연산은 와즘 인터프리터[14]를 통해 처리됩니다. 따라서 와즘으로 컴파일[15]할 수 있는 언어라면 무엇이든 캐스퍼 블록체인의 스마트 컨트랙트 개발 언어로 활용할 수 있습니다. 이더리움과 마찬가지로 캐스퍼 역시 네트워크 내 모든 노드가 연산 작업량을 동일한 기준으로 측정하기 위해 가스[16] 개념을 사용합니다. 각각의 와즘 연산 코드(옵코드)[17]에는 고유한 가스 비용이 책정되어 있으며 인터프리터가 코드를 실행할 때마다 런타임[18] 환경에서 소모된 가스량을 실시간으로 추적합니다.

모든 트랜잭션 실행에는 유한한 끝이 존재합니다. 연산이 강제 종료되기 전까지 최대로 사용할 수 있는 가스량, 즉 가스 한도가 명확히 설정되어 있기 때문입니다. 트랜잭션 수수료를 지불하는 방식은 별도의 결제 실행 세션을 통해 결정되며 가스 한도 역시 트랜잭션에 명시된 결제 코드가 실행되면서 설정됩니다.

연산 비용의 측정 단위는 가스이지만 실제 수수료 결제는 토큰의 최소 단위인 모트[19]로 이루어집니다. 따라서 가스와 모트 간에는 일정한 교환 비율이 존재합니다.

***참고**

캐스퍼 네트워크는 연산 자원을 효율적으로 배분하고 건전한 런타임 경제 시스템을 조성하기 위해 유연하게 조정 가능한 수수료, 환불 및 가격 책정 정책을 지원합니다. 또한 선 합의 후 실행 모델은 사용자가 가스 소비를 최적화하도록 유도하며 비정상적인 트랜잭션이 불필요하게 블록 공간을 낭비하는 것을 방지합니다.

---

[14] Interpreter

[15] Compile

[16] Gas

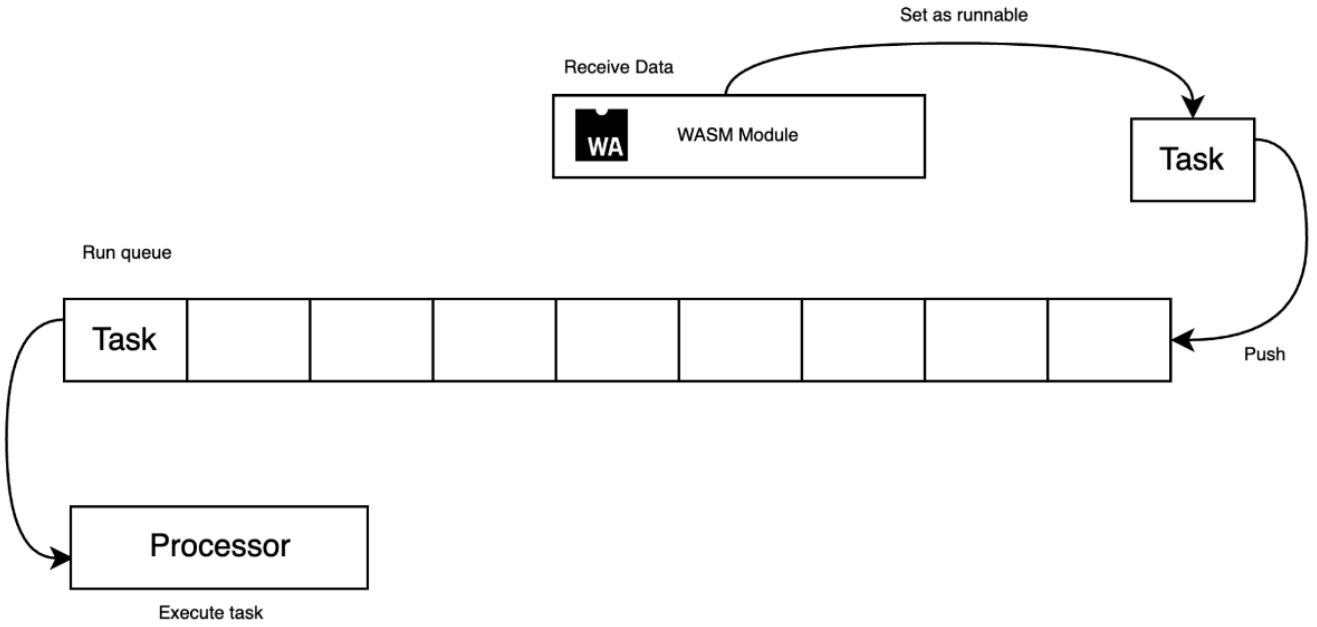
[17] Opcode (Operation code)

[18] Runtime

[19] Mote

캐스퍼 네트워크 런타임

와즘 모듈은 자체적인 선형 메모리[20]를 읽고 쓰는 것 외에는 외부 환경에 어떠한 영향도 직접 미칠 수 없도록 설계되어 있습니다. 따라서 글로벌 스테이트 데이터를 읽거나 쓰는 등 네트워크 상에서 유의미한 작업을 수행하려면 와즘 모듈이 현재 실행 중인 호스트 환경으로부터 필요한 함수를 반드시 호출해 와야만 합니다. 이러한 모든 외부 상호작용 기능은 캐스퍼가 제공하는 전용 인터페이스인 캐스퍼 외부 FFI(Casper External FFI[21])를 통해 사용할 수 있습니다.



[와즘 기반 트랜잭션 실행 흐름도]

계정

캐스퍼 블록체인은 온체인 상의 계정 기반 모델을 사용하며 각 계정은 특정 공개 키[22]에서 파생된 고유한 계정 해시[23]를 통해 식별됩니다. 글로벌 스테이트의 트라이[24] 저장소 구조상 모든 키는 동일한 길이를 가져야 합니다. 따라서 계정 해시는 네트워크가 지원하는 다양한 형태의 공개키들을 일관되게 처리(추상화)하기 위해 32바이트 길이로 변환된 데이터입니다.

[20] Linear memory

[21] Foreign Function Interface, FFI

[22] Public key

[23] AccountHash

[24] Trie

캐스퍼 플랫폼은 계정 생성 및 트랜잭션 서명을 위해 다음 두 가지 유형의 키를 지원합니다.

- Ed25519 키: 에드워즈 곡선 디지털 서명 알고리즘(EdDSA)[25]을 사용하며, 길이는 66바이트입니다.
- Secp256k1 키: 이더리움 키로 널리 알려져 있으며, 길이는 68바이트입니다.

기본적으로 블록체인 네트워크와 상호작용하려면 계정 생성 시 사용했던 공개키와 연결된 키 페어[26]로 암호화 서명을 마친 트랜잭션 형태를 거쳐야 합니다. 캐스퍼 블록체인 상의 모든 사용자 활동, 즉 시스템 상의 트랜잭션은 반드시 특정 계정에서 출발해야 합니다. 각 계정은 고유한 실행 환경을 가지며, 이곳에 유용한 스마트 컨트랙트 참조값, 지표, 블록체인 내 다른 곳에서 수집된 데이터 등을 로컬 상태로 저장할 수 있습니다. 또한 모든 계정은 CSPR을 보관하기 위한 전용 공간인 메인 지갑을 보유합니다.

위조 불가 참조(URef)

URef라는 키는 계정을 제외한 모든 값을 저장할 때 사용됩니다. 또한 와즘 환경에서 쓰이는 URef에는 권한 정보가 들어 있습니다. 키에 저장된 값을 허락 없이 사용하는 것을 방지하기 위해서입니다. 런타임은 이 권한 정보를 추적합니다. 즉, 악의적인 와즘이 자신에게 없는 권한을 가진 URef를 생성하려 한다면 이는 위조 불가 참조를 위조(Forge)하려는 시도에 해당합니다. 이때 런타임은 위조된 URef 오류를 발생시킵니다. URef의 권한은 컨트랙트를 호출하는 과정에서 전달될 수 있습니다. 이를 통해 URef에 저장된 데이터를 통제된 방식으로 공유할 수 있습니다. 이 키를 나타내는 32바이트 길이의 식별자는 런타임이 무작위로 생성합니다.

블록 구조

블록은 네트워크 노드 간에 캐스퍼 네트워크의 상태 정보를 전달하는 주요 데이터 구조입니다.

데이터 필드

블록은 다음과 같이 구성됩니다.

[25] Edwards-curve Digital Signature Algorithm, EdDSA

[26] Key-pair

- 블록 해시 (block_hash)
- 헤더 (header)
- 본문 (body)

토큰

캐스퍼는 하이웨이(Highway) 또는 주크 합의 메커니즘을 사용할 수 있는 탈중앙화 지분증명 블록체인 플랫폼입니다. 이 시스템이 작동하려면 가치의 단위가 필요합니다. 사용자는 연산 비용을 지불해야 하며, 검증인은 예치할 지분[27]을 보유해야 하기 때문입니다. 블록체인 환경에서 이 가치의 단위가 바로 토큰입니다.

토크노믹스

***아래 내용은 2023년 캐스퍼 재단이 공식 홈페이지에 공시한 'Update on Circulating Supply' 내용을 중심으로 작성됐습니다.**

유통량 업데이트는 모든 코인리스트 판매 토큰, 잠금 해제된 프라이빗 검증인 판매 토큰, 개발자 및 생태계 인센티브에 사용되는 토큰, 캐스퍼랩스와 캐스퍼 협회가 보유한 잠금 해제 토큰이 보고 유통량에 포함된다는 의미입니다. 따라서 보고된 총토큰 유통량은 약 104억 CSPR이 될 것입니다. 이 중 약 83억 개(CSPR 유통량의 80%)의 토큰이 현재 네트워크에 스테이킹 및 결합되어 있습니다.(역자: 본 번역서 작성 시점(2026년 3월 19일) 기준 약 144억 CSPR이며, 실시간 유통량은 cspr.live에서 확인할 수 있습니다)

업데이트된 유통량 보고 방법은 캐스퍼 생태계의 총발행량을 늘리지 않을 것이고, 다른 영향을 미치지 않을 것 입니다. 토큰은 이미 전송 가능하고, 공급량에 새로 추가되는 코인은 없습니다.

[27] Stake

캐스퍼 메인넷 출시

2021년 3월 31일, 캐스퍼 검증자의 제네시스 블록[28]이 캐스퍼 메인넷을 출시했습니다. 지난 18개월 동안 85,000개 이상의 캐스퍼 계정, 18,400개 이상의 위임자[29], 200개 이상의 노드, 540,000건 이상의 네이티브 토큰[30] 전송 등 네트워크는 엄청난 성장을 보여줬습니다. 현재, 전체 발행된 CSPR 토큰의 약 74%가 네트워크에 스테이킹 및 결합되어[31] 있으며, 플랫폼에 뛰어난 보안을 제공하고 있습니다. 캐스퍼의 텔레그램 채널(캐스퍼 메인 채널, 다양한 지역/언어 채널 포함)에는 100,000명 이상의 회원이 있습니다. 캐스퍼랩스 및 캐스퍼 네트워크의 트위터 채널에는 188,000명 이상의 팔로워가 있으며, 캐스퍼의 디스코드 채널에는 31,500명 이상의 회원이 있습니다. 또한, 네이티브 웹3.0 프로젝트와 다양한 규모의 혁신적인 기업들이 점점 더 빠른 속도로 캐스퍼를 레이어[32] 체인으로 채택하고 있습니다.
2022년 여름에 캐스퍼는 몇 가지 중요한 사건을 경험했습니다. 8월 5일에는 네트워크에서 백만 번째 블록이 생성된 것을 축하했습니다. 8월 28일은 코인리스트에서 진행된 공개 토큰 세일의 토큰이 최종적으로 선택되고 출시되는 날이기도 했습니다.

업데이트에 대한 세부 사항

캐스퍼의 메인 네트워크 출시 이후 지금까지는 토큰이 제네시스 지갑에서 전송된 경우에만 유통량으로 집계되었습니다. 이에 따라 보고된 유통량보다 더 많은 토큰이 네트워크에 스테이킹 되는 등의 이상한 현상이 발생했습니다. 이에 따라 캐스퍼 커뮤니티와 가상자산 커뮤니티는 계속해서 혼란을 겪고 있습니다.

현재 모든 코인리스트 판매 토큰이 배포되고 대부분의 CSPR이 잠금 해제된 상태에서 캐스퍼 협회는 유통량 보고 방법론을 재검토했습니다. 따라서 앞으로 캐스퍼는 잠금 해제되고 이동 가능해진[33] 모든 토큰을 유통량 보고에 반영할 것입니다. 유통량 보고 방법론을 업데이트한 레이어1 블록체인은 캐스퍼가 처음이 아닙니다. 실제로 여러 블록체인이 보고 방식을 변경했습니다.

[28] Genesis block
[29] Delegator
[30] Native token
[31] Bonded
[32] Layer 1
[33] Transferable

유통량 조건

이번 업데이트를 통해 다음 토큰은 유통량의 일부로 보고됩니다.

- 모든 코인리스트 및 검증자 판매 토큰
- 개발자 및 생태계 인센티브를 위해 예약된 토큰
- 원래 캐스퍼 협회에 할당되어 캐스퍼 협회가 보유한 토큰
- 원래 캐스퍼 랩스에 할당되어 캐스퍼 랩스가 보유한 토큰

반면, 유통량에 포함되지 않은 나머지 토큰은 캐스퍼 협회와 캐스퍼 랩스의 수령되지 않은 팀 토큰과 향후 팀원 및 어드바이저의 토큰으로 구성됩니다.

업데이트에 따른 주요 변화

유통량 보고 방법의 업데이트에서 주목할 만한 결과는 총 유통 토큰 수가 약 104억 CSPR이 될 것이며, 이 중 83억 토큰(CSPR 유통량의 80%, 총발행량의 74%)이 현재 네트워크에 스테이킹 및 연결되어 있는 것입니다 (역자: 본 번역서 작성 시점(2026년 3월 19일) 기준 약 144억 CSPR이며, 실시간 유통량은 cspr.live에서 확인할 수 있습니다).

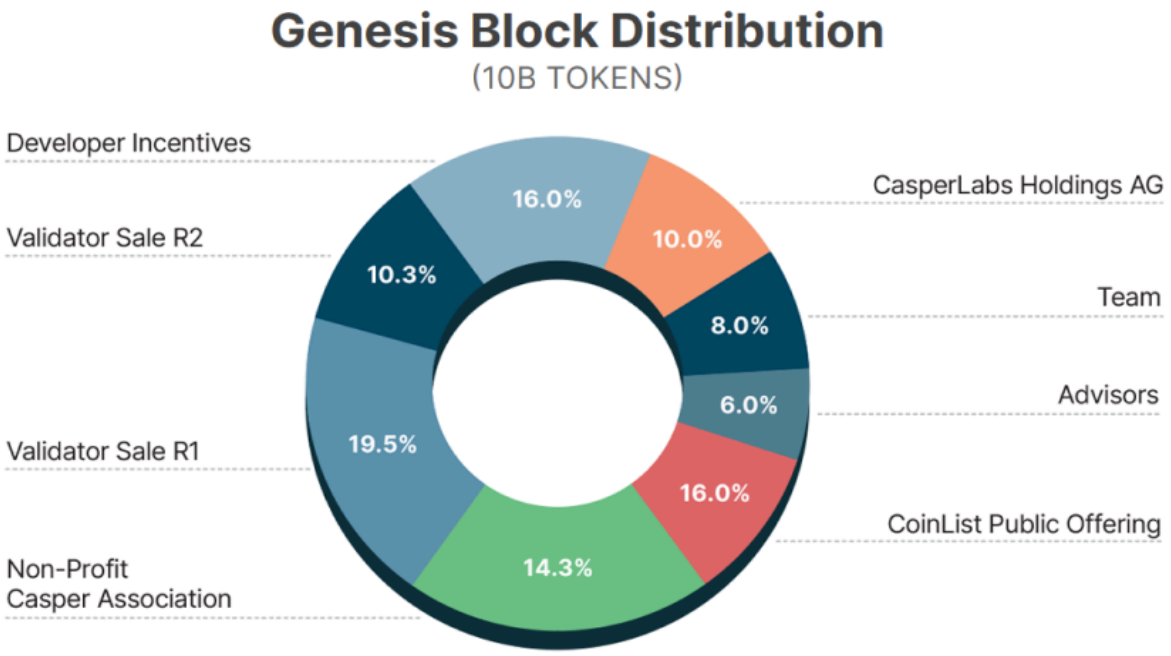
앞으로 유통량의 일부로 보고될 토큰은 이미 잠금 해제되어 이동이 가능합니다. 이번 업데이트를 통해 캐스퍼는 다른 주요 블록체인의 유통량을 보고하는 방식과 더 맞춰지게 되었습니다.

CSPR 초기 토크노믹스

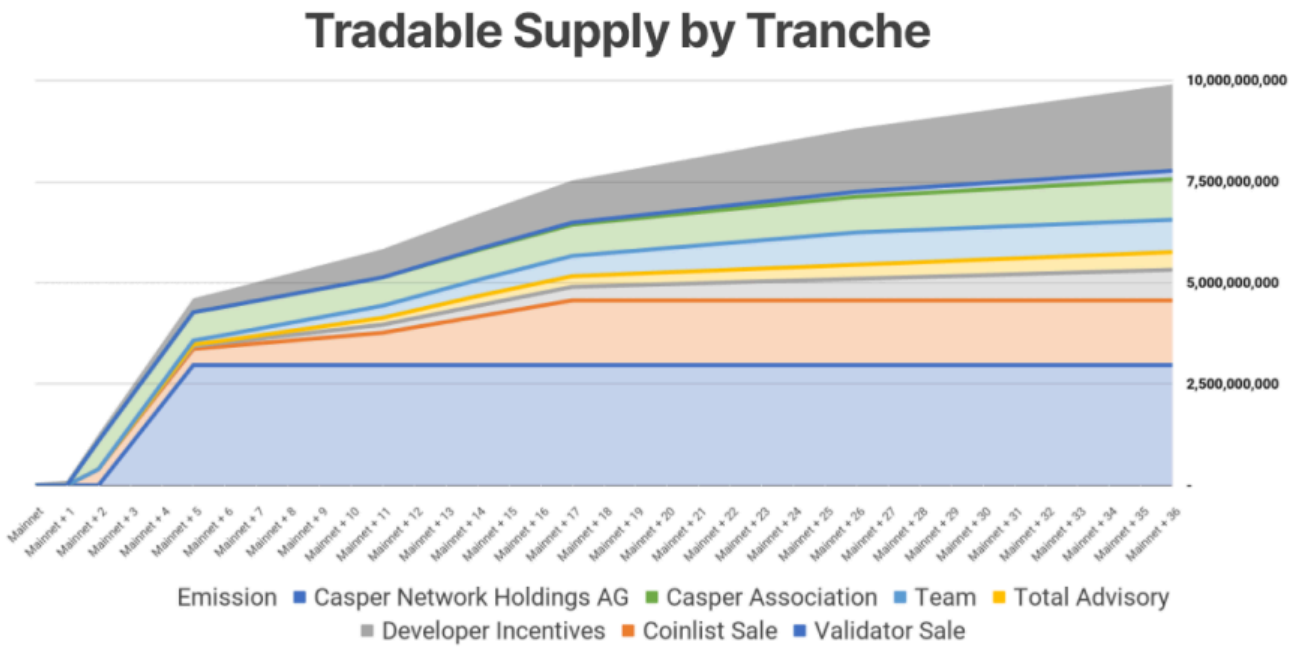
CSPR은 캐스퍼 네트워크의 기본 토큰입니다. 네트워크 참여자는 이를 사용하여 수수료를 지불하고, 네트워크 거래를 처리하는 검증인에게 보상을 제공합니다. 캐스퍼는 탁월한 성능과 확장성을 제공하기 위해 지분증명(PoS)[34] 모델을 채택합니다.

어떠한 개인이나 단체도 공개 토큰 판매를 통해 토큰의 1% 이상을 취득할 수 없습니다. 토큰은 다음과 같은 방식으로 할당됩니다(관련 법률 및 규정에 따름).

[34] Proof-of-Stake, PoS



[초기 토큰 분배]



[CSPR 유통 일정]

로드맵

캐스퍼는 별도 로드맵을 공지하고 있지 않으나, 블로그 및 X(구 트위터)를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 블로그 https://www.casper.network/news
- X(구 트위터) https://x.com/Casper_Network
- 텔레그램 https://t.me/casperblockchain

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.