

카테고리

플랫폼 코인

토큰 발행량

총 발행량 28,704,026,601

총 유통량 20,269,969,386

토큰 분배율

Mining 100%

로드맵

- Upgrade consensus to follow the DAGKNIGHT protocol
- KASPA Rust Language Coding
- Mobile Wallet Development
- Further increase blocks per seconds and transactions per second
- Integrate Kaspa for use on Ledger
- 2023 White Paper
- Archival Node Improvements
- Smart Contracts Implementation

명세서

# 카스파

티커 KAS

## 작업증명(PoW) 기반의 블록체인으로 확장성을 해결하는 프로젝트

### DAG를 활용한 블록 생성속도 개선과 kHeavyHash 해시함수를 통한 효율적인 채굴 방식 도입

카스파(Kaspa)는 BlockDAG(Block Directed Acyclic Graph) 기반의 작업증명(PoW) 방식을 채택한 오픈소스 레이어1 프로젝트입니다. 대다수의 프로젝트는 트랜잭션의 처리 속도 개선을 위해 탈중앙화의 원칙을 희생하는 경향이 있지만, 카스파는 이러한 확장성 문제를 완전히 탈중앙화된 환경에서 해결하려고 합니다. 프로젝트 내에서 KAS는 카스파의 작업증명 방식의 채굴 보상 및 거래 수수료로 활용되고 있습니다. 이로써 KAS는 프로젝트의 경제 생태계를 지원하며 다양한 영역에서 활용될 수 있습니다.

카스파는 기존의 전통적인 블록체인과는 다르게 블록을 선형으로 연결하는 BlockDAG 방식을 통해 작업증명이 제공하는 탈중앙화된 보안성을 유지하면서도 블록 생성 속도를 향상시킵니다. 이를 통해 블록을 병렬로 생성하여 짧은 시간(현재 초당 1블록) 내에 많은 거래를 처리할 수 있습니다. 카스파는 이러한 BlockDAG 방식을 나카모토 합의 과정을 일반화한 PHANTOM/GHOSTDAG 프로토콜을 사용하여 구현합니다. 나카모토 합의란 비트코인의 블록 연결과정에서 동시에 두 블록이 생성되어 갈라지는 현상이 발생하면 어떤 체인을 유효한 것으로 판단할지 결정하는 긴 체인 규칙(Longest chain Rule)을 포함한 합의과정을 의미합니다. 여기서 선택되지 않은 고립된 블록(Orphan Block)은 더 이상 유용하지 않게 되어 다음과 같은 문제가 발생합니다.

- 고립된 블록을 생성하는 과정에 채굴자가 소비한 연산 작업 비용의 낭비
- 의도적으로 고립된 블록을 유효한 체인으로 유도하려는 채굴자의 악의적인 공격

카스파는 PHANTOM/GHOSTDAG 프로토콜을 통해 고립된 블록을 포함한 분기된 체인을 모두 선행 블록(Parents Block)으로 활용하고 이는 새로 생성되는 블록과 연결되어 그래프와 같은 구조를 형성합니다. 이는 고립된 블록의 연산 작업 비용을 활용하고 채굴자의 악의적인 공격을 방어하면서도 많은 거래를 처리할 수 있도록 합니다. PHANTOM은 BlockDAG 내에서 블록의 관계와 순서를 결정하는 규칙을 제시하며, 이를 효율적으로 구현하기 위해 탐욕 알고리즘(Greedy algorithm)을 적용한 PHANTOM/GHOSTDAG를 실제 메커니즘으로 활용합니다.

더불어, KAS 채굴과 관련하여 카스파는 환경적으로 부정적인 영향으로 최소화하면서 탈중앙화를 유지하기 위해 작업증명의 해시함수로 kHeavyHash를 선택하였습니다. 이는 SHA-256 등 일반적으로 사용되는 해시함수보다 에너지 효율적이며 와트당 높은 해시파워를 지원하여 KAS 채굴을 효율적으로 수행할 수 있습니다.

마지막으로, 카스파는 완전히 탈중앙화된 오픈소스 프로젝트로, 누구나 참여할 수 있으며 탈중앙화된 웹과 더 나은 사회를 위해 만들어졌습니다. 기여자들은 개발자 기금과 커뮤니티 자금을 운영하며 참여와 기여에 대한 커뮤니티 보상을 제공하여 카스파 생태계의 발전에 기여하고 있습니다.

---

프로젝트 핵심인력

---

이름	약력
Yonatan Sompolinsky	Founder
Michael Sutton	Core Developer
Mike Zak	Core Developer
Elichai Turkel	Core Developer
Ori Newman	Core Developer
Shai Wyborski	Researcher

---

---

## 법적고지서

본 자료는 투자를 유도하거나 권장할 목적이 아니라 투자자들의 투자 판단에 참고가 되는 정보제공을 목적으로 배포되는 자료입니다. 본 자료에 수록된 내용은 당사 리서치센터가 신뢰할 수 있는 자료 및 정보로부터 얻은 것이나 오차가 발생할 수 있으며, 당사는 어떠한 경우에도 정확성이나 완벽성을 보장하지 않습니다.

따라서 본 자료를 이용하실 때는 본인의 판단으로 본 자료와 관련한 투자의 최종 결정을 하시기를 바랍니다. 당사는 본 자료의 내용에 의거하여 행해진 일체의 투자행위에 대하여 어떠한 책임도 지지 않습니다.

본 자료에 나타난 정보, 의견, 예측은 본 자료가 작성된 날짜 기준이며 통지 없이 변경될 수 있습니다. 과거 실적은 미래 실적에 대한 지침이 아니며 미래 수익은 보장되지 않습니다. 경우에 따라 원본의 손실이 발생할 수도 있습니다. 아울러 당사는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.

본 자료에 나타난 모든 의견은 자료작성자의 개인적인 견해로서, 외부의 부당한 압력이나 간섭 없이 작성되었습니다. 당사는 본 자료를 작성하는데 관여하지 않았으며 본 자료에 나타난 견해는 당사의 견해와 다를 수 있습니다. 따라서 당사는 본 자료와 다른 의견을 제시할 수도 있습니다.

본 자료는 어떠한 경우에도 고객의 투자결과에 대한 법적 책임소재의 증빙자료로 사용될 수 없습니다. 본 자료의 저작권은 당사에게 있고, 어떠한 경우에도 당사의 허락 없이 복사, 대여, 재배포될 수 없습니다.