

Hbar 경제

Hbar의 두 가지 역할과 상세한 배포일정에 대한 분석

A large, stylized, light blue Hbar symbol (h) is positioned in the bottom right corner of the page. The symbol is rendered in a cursive, flowing font style.

헤데라 해시그래프(Hedera Hashgraph)는 개인정보를 수집하거나 매매하는 제3자의 외부 개입 없이도 사용자들이 온라인에서 효율적이고 안전하게 상호작용하고 거래할 수 있도록 분산원장 기술(DLT, Distributed Ledger Technology)을 적용한 퍼블릭 플랫폼입니다.

헤데라의 목표는 암호화폐 유통이 아닙니다. 기업 레벨의 다양한 탈중앙화 애플리케이션을 위한 안정적이고 신뢰할 수 있는 플랫폼을 제공하는 것입니다. 하지만 다른 퍼블릭 DLT 플랫폼이 그러하듯 기능적인 이유에서 암호화폐를 필요로 합니다.

그래서 헤데라의 코인 'Hbar'는 다음의 두 가지 핵심 기능을 수행하기 위해 개발되었습니다.

1. 헤데라의 코인 가중치와 지분증명 합의 메커니즘을 통해 사이버 공격으로부터 네트워크를 보호하는 기능
2. 플랫폼이 원활하게 작동하는 데 필요한 컴퓨팅 리소스를 구입하는 비용 및 리소스 제공의 인센티브가 되는 '연료' 기능

이 백서에서는 헤데라 플랫폼에서 Hbar를 사용하는 방법, 합의를 구축하고 트랜잭션 보안을 확보하는 데 있어 Hbar의 역할, 500억 개로 공급이 고정되어 있는 Hbar의 예상 분포를 설명합니다. 이 문서에 제시된 내용은 정보 제공 및 예시를 목적으로 하며, 추후 변경될 수 있습니다. 제3자로부터 제공받은 정보의 경우 헤데라가 신뢰할 수 있다고 간주하는 내용만을 문서에 포함하였지만, 독립적 검증을 거친 것은 아닙니다.

01.

개요

헤데라 테크놀로지

헤데라 플랫폼은 획기적인 분산형 합의 기술인 해시그래프 합의 알고리즘을 통해 작동합니다. 블록체인 및 다른 DLT와 같이 온라인 커뮤니티가 믿을 수 있는 공유 데이터베이스를 만들 수 있지만, 중간에서 개인정보를 관리하는 제3자가 필요하지 않습니다. 또한, 성능을 높이면 보안이 불안해지고 보안을 높이면 속도가 느려지기 때문에 성능과 보안 사이에서 타협할 수 밖에 없는 기존의 DLT 플랫폼과 달리 해시그래프는 우수한 성능과 보안 수준을 동시에 제공합니다. 해시그래프 알고리즘은 수학적으로 작업증명 블록체인보다 훨씬 빠른 속도로 트랜잭션을 처리하면서도 분산형 네트워크에 최고 수준의 보안을 제공하는 것으로 증명되었습니다.

블록체인 기반 플랫폼에 비해 월등한 속도와 우수한 안정성 덕분에 헤데라에서는 새로운 애플리케이션과 유스 케이스, 비즈니스 모델을 광범위하게 실현할 수 있습니다. 지금까지 다른 DLT 플랫폼에서는 볼 수 없었던 아주 작은 단위의 애드호크(Ad-hoc) 소액결제는 물론, 기기 간 트랜잭션도 가능합니다. 개발자와 기업은 헤데라 플랫폼의 암호화폐, 스마트 계약, 파일 서비스, 헤데라 컨센서스 서비스(출시 예정)를 활용하여 플랫폼 상에서 실행되는 애플리케이션을 만들 수 있습니다. 헤데라 플랫폼은 음악 스트리밍 서비스부터 제약 공급망 관리, 에너지 마이크로그리드, 멀티 플레이어 온라인 게임에 이르기까지 파격적으로 다양한 응용 분야를 지원합니다.

헤데라 거버닝 카운슬

헤데라 플랫폼은 다양한 산업 분야를 대표하며 세계 각 지역에 분포되어 있는 수준 높은 글로벌 기업들이 교대로 구성하는 헤데라 거버닝 카운슬에 의해 관리됩니다. 이들은 소프트웨어 업그레이드 및 네트워크 가격 책정과 관련된 주요 사항을 결정합니다. 헤데라는 이들에게 보수를 지급하거나 수익을 분배하지 않으며, 이들의 임기는 제한되어 있습니다. 이러한 방식으로 거버닝 카운슬은 플랫폼의 장기적 이익 측면에서 탈중앙화되고 합리적이며 안정적인 거버넌스를 구축합니다. 헤데라는 익명의 채굴자 또는 개발자 집단에 의해 지배되지 않으며, 기업 주도 구조를 통해 기존 퍼블릭 DLT 플랫폼의 관리에 악영향을 끼쳐왔던 이념적·개인적 분쟁의 위험을 감소시킵니다.

헤데라의 기술력과 거버닝 카운슬의 시너지 효과로 확장 가능하며 적용하기 편리한 플랫폼, 특히 기업에 의해 광범위하게 수용되고 채택될 수 있는 퍼블릭 DLT 플랫폼이 마침내 구현될 것입니다.

헤데라의 암호화폐, 'HBAR'

지난 2018년 8월에 출시한 헤데라 네트워크는 총 500억 개로 고정 공급된 Hbar를 헤데라 금고(Hedera Treasury) 계정에 예치하였습니다. 헤데라 금고는 암호화된 다중 서명 계정으로, 이곳에 예치된 Hbar는 거버닝 카운슬 위원 과반수에 의해 암호화된 서명이 이루어진 트랜잭션을 통해서만 외부로 이체할 수 있습니다. 이로써 코인에 대한 플랫폼의 권한이 탈중앙화되고, 대규모의 신뢰할 수 있는 독립적 주체들에게 분산됩니다.

헤데라 네트워크가 테스트 기간을 거치는 동안, 네트워크 액세스는 수백 명의 개발자와 사용자에게만 제한적으로 허용되었습니다. 네트워크를 테스트하기 위해 이들에게 배포된 소수의 Hbar를 제외한 나머지는 여전히 헤데라 카운슬이 안전하게 관리하는 금고 계정에 보관되어 있습니다.

헤데라는 2019년 여름에 테스트 프로그램을 완료했습니다. 9월 중순으로 예정되어 있는 오픈 액세스 이후로는 헤데라 네트워크에 계정을 만들고 싶은 사람이라면 누구나 네트워크에 액세스할 수 있게 될 것으로 기대하고 있습니다. 이를 기점으로 헤데라 금고 계정의 Hbar 역시 광범위하게 배포되기 시작할 것입니다. 더불어 암호화폐 거래소에서도 Hbar를 찾아볼 수 있게 되어 누구나 Hbar를 구매하고 헤데라 플랫폼에서 사용할 수 있게 될 예정입니다.

3장에서 자세하게 설명할 네트워크 보안상의 이유로, 헤데라 금고에 보관된 Hbar는 매우 느리고 신중한 계획에 따라 출시 및 배포되어야 합니다. 2019년 말까지 전체 공급량의 8% 미만이 배포될 예정이며, 첫 5년 동안의 공급량은 34% 미만으로 제한될 것으로 예상됩니다. 이는 네트워크를 모든 종류의 공격으로부터 보호하고 헤데라 카운슬이 아닌 시장 논리에 의해 Hbar의 가격이 결정되도록 보장하기 위한 메커니즘의 일환입니다.

02.

네트워크 서비스 비용을 지불하고 노드 참여를 유도하기 위한 '연료'로서의 Hbar

모든 퍼블릭 DLT 플랫폼에는 탈중앙화 네트워크에서 노드 역할을 하는 컴퓨터가 필요합니다. 이 노드가 하는 역할은 크게 두 가지입니다.

1. 각 네트워크 사용자 계정의 잔액 공유 원장을 유지
2. 새로운 트랜잭션을 검증하고 실행하며 이를 시간 순서로 정렬하여 사용자 계정의 잔액을 최신 상태로 업데이트

각 노드는 플랫폼의 합의 알고리즘을 실행하고 트랜잭션을 처리하기 위한 컴퓨팅 성능을 제공해야 합니다. 컴퓨팅 성능을 제공하려면 비용이 들기 때문에, DLT 플랫폼은 그 대가로 노드에 플랫폼 자체의 암호화폐를 지불하는 것이 보통입니다.

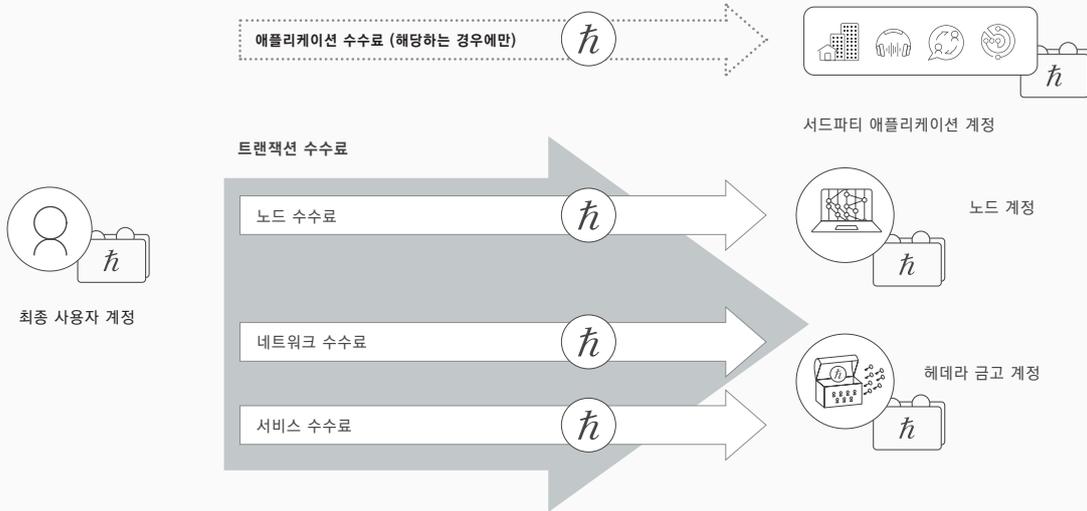
헤데라 네트워크에서 Hbar는 네트워크 서비스(트랜잭션 제출, 스마트 콘트랙트 실행, 파일 저장)에 필요한 비용을 지불하고 컴퓨팅 리소스(대역폭, 처리 성능, 메모리)를 제공하는 노드에 보상하는 '연료'로 사용됩니다. 이때의 회당 트랜잭션 수수료는 코인 1개에 최대 0.0001달러 수준으로, 플랫폼 고유의 소액결제를 촉진하는 효과를 가져올 것입니다.

헤데라 트랜잭션 경제는 비용과 인센티브의 균형을 맞추어 효율적인 자금 흐름을 만들어낼 수 있도록 설계되었습니다. 이 흐름은 크게 둘로 나눌 수 있습니다.

1. 최종 사용자(또는 최종 사용자가 되는 서드파티 앱)가 헤데라 계정으로 지불한 트랜잭션 수수료
2. 헤데라 계정에서 노드 호스트에 지불한 (a) 노드 보상과 Hbar 소유자가 노드에 프록시 스테이킹(Proxy-staking)^[1]한 금액에 대한 (b) 프록시 스테이킹 보상. 예를 들어, 앨리스가 밥에게 5개의 Hbar를 보낸다면, 이 5개의 Hbar는 헤데라 계정을 거치지 않고 밥에게 직접 전달되며, 앨리스는 트랜잭션이 이루어지게 하기 위해 노드 수수료와 네트워크 수수료, 서비스 수수료를 지불합니다.

¹ Proxy-staking is explained in Part III.

HBAR 트랜잭션 수수료



최종 사용자는 플랫폼 사용에 대한 수수료를 지불합니다. 수수료는 Hbar를 전송하거나 헤데라 해시그래프 원장에 데이터를 추가했을 때 발생합니다. 특정 작업에 대한 수수료는 사용되는 네트워크 서비스 유형(암호화폐, 스마트 계약, 파일 서비스)과 트랜잭션 처리에 소비되는 네트워크 리소스의 수준과 기간에 따라 달라집니다. 네트워크의 작업에 대한 전반적인 비용을 트랜잭션 수수료라고 하며, 이는 3개의 개별 수수료(노드 수수료, 네트워크 수수료, 서비스 수수료)로 구성됩니다. 각 수수료는 네트워크에서 트랜잭션을 제출하고 검증하는 방법과 관련이 있습니다. 추가로, 개발자들은 헤데라 플랫폼을 통해 자신이 개발하여 제공하는 애플리케이션을 이용하는 사용자들에게 애플리케이션 수수료를 부과할 수도 있습니다. 트랜잭션 수수료와 애플리케이션 수수료의 자세한 내용은 다음과 같습니다.

- 1. 노드 수수료.** 플랫폼에서 작업을 완료하고자 하는 사용자 또는 애플리케이션은 해당 트랜잭션을 단일 노드로 전송하고, 노드는 그것을 다시 네트워크에 제출합니다. 이때 노드는 매우 적은 양이지만 리소스와 전력을 소비하게 됩니다. 노드 수수료는 노드가 소비한 리소스를 보상하고 계속해서 이 중요한 역할을 수행하도록 인센티브를 부여합니다. 최초의 노드 수수료는 헤데라 카운슬에 의해 정해지겠지만, 점차 각 노드에 의해 자율적으로 적정한 수수료가 책정될 것입니다. 노드 수수료는 최종 사용자가 사용자의 트랜잭션을 제출한 노드의 계정으로 직접 지불합니다.
- 2. 네트워크 수수료.** 트랜잭션이 네트워크에 제출되고 나면 디지털 서명을 검증하는 노드를 거쳐 노드 간 통신이 이어지고, 네트워크가 합의에 도달할 때까지 노드의 메모리에 임시 저장됩니다. 이때 사용자가 트랜잭션에 대한 합의를 연산하는 데 이용된 노드에 지불하는 것이 네트워크 수수료입니다. 이 과정에서 소비되는 컴퓨팅 리소스는 트랜잭션 파일 크기와 디지털 서명의 수에 따라 달라질 수 있습니다. 네트워크 수수료는 사용자가 헤데라 금고 계정으로 지불하며, 이 금액의 일부는 노드 보상을 지불하는 등의 방식으로 참여 노드에 매일 분배됩니다. (이어서 더 자세히 설명하겠습니다.)
- 3. 서비스 수수료.** 서비스 수수료는 트랜잭션을 유지하거나 지원하는 지속적인 작업이 이루어졌을 때 네트워크에 대해 지불됩니다. 파일 서비스 트랜잭션의 경우, 플랫폼은 요청된 시간 동안 파일 크기를 저장하는 데 필요한 전력과 메모리 공간에 해당하는 수수료를 부과합니다. 스마트 계약의 경우에는 필요한 연산을 수행하기 위해 네트워크 노드에 필요한 처리 능력에 따라 수수료가 부과됩니다. 서비스 수수료는 사용자가 헤데라 금고 계정으로 지불하며, 이 금액의 일부는 노드 보상 지불 등으로 참여 노드에 매일 분배됩니다.

4. **애플리케이션 수수료 (선택사항).** 헤데라 플랫폼을 기반으로 애플리케이션을 구축하는 개발자들은 최종 사용자에게 제공되는 애플리케이션의 가치를 직접 수익화할 수 있습니다. 월렛 앱의 예를 들면, 입금하거나 인출한 금액에 대해 소량의 수수료를 청구하도록 설정할 수 있습니다. 운전자와 승객을 직접 연결해주는 차량 공유 디앱의 경우라면 운행 요금의 일정 퍼센트를 계산하여 수수료로 받을 수 있습니다. 기존의 다양한 애플리케이션과 같이 무료 서비스와 유료 서비스를 함께 제공하는 것도 가능합니다. 서드파티 개발자가 청구하고자 하는 수수료를 책정하면, 해당 애플리케이션의 최종 사용자가 개발자에게 수수료를 직접 지불하게 됩니다.

노드 보상과 프록시 스테이킹 보상

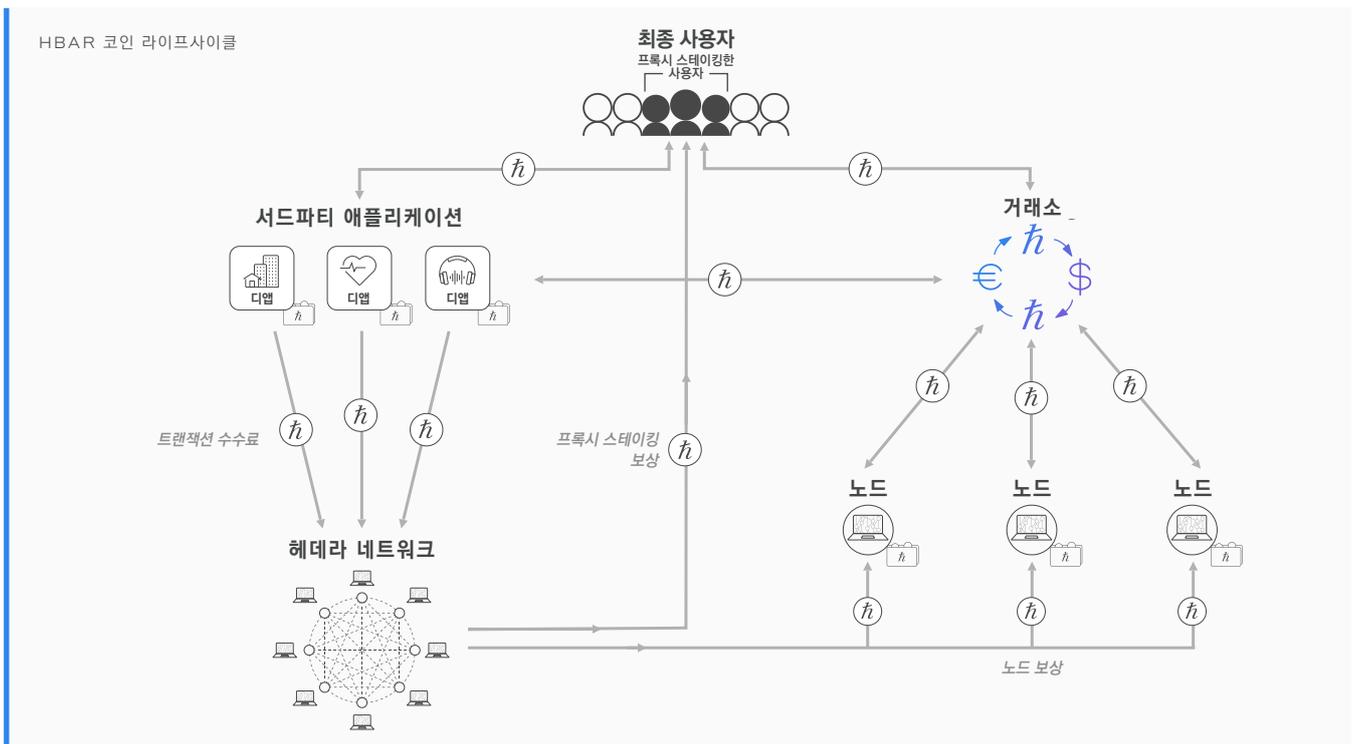
분산 네트워크는 노드가 트랜잭션 검증과 공유 원장 유지를 위해 리소스를 제공하도록 인센티브를 제공해야 합니다. 대부분의 DLT 플랫폼과 마찬가지로, 헤데라는 플랫폼 자체의 암호화폐로 노드에 대가를 지불합니다.

위에서 다루었던 것처럼 헤데라 금고는 트랜잭션을 처리하고 서비스를 수행하는 모든 노드를 대신하여 네트워크 수수료와 서비스 수수료를 징수합니다. 이렇게 모인 Hbar의 일부는 헤데라 계정에 잠시 예치되었다가 24시간마다 자동으로 노드 보상 및 프록시 스테이킹 보상을 위해 재분배될 것입니다. 해당 기간에 트랜잭션 검증에 참여한 모든 노드와 사용자 계정의 Hbar를 프록시 스테이킹한 사용자들이 재분배의 대상이 됩니다. (프록시 스테이킹에 대해서는 3장에서 자세히 설명합니다.)

이 노드 인센티브는 이른바 ‘승자 독식 네트워크’라고 할 수 있는 작업증명 방식보다 훨씬 효율적입니다. 작업증명 네트워크에서 모든 채굴 노드는 암호화 퍼즐을 해결하기 위해 전력을 소모하지만 오직 승자만이 대가를 차지하며, 다른 노드에서 소비된 모든 에너지는 그저 낭비되고 맙니다. 헤데라 네트워크에서는 쓸모없는 수학 문제에 노드의 전력을 낭비하는 대신 통신, 유효성 검증, 트랜잭션 지원에 직접 에너지를 사용합니다.

노드 보상은 노드에 의해 스테이킹 및 프록시 스테이킹된 Hbar의 양에 비례하여 분배됩니다. 사용자가 프록시 스테이킹한 코인에 대한 프록시 스테이킹 보상은 노드의 계정과 사용자의 계정에 50 대 50으로 분할 지급됩니다. 이 보상을 받기 위해서는 노드가 온라인 상태여야 하며, 직전 24시간 동안 합의에 참여했어야 합니다.

스테이킹 또는 프록시 스테이킹된 Hbar는 언제나 소유자의 권한 하에 있습니다. 소유자는 언제든지 그것을 사용할 수 있고, 프록시 스테이킹한 사용자는 언제든지 다른 노드로 프록시 스테이킹을 해제하거나 리디렉션할 수 있습니다.



헤데라 코인의 두 가지 역할



네트워크를 가동하는 '연료'

네트워크 서비스에 필요한 비용을 지불
(예: 트랜잭션 제출, 스마트 콘트랙트 실행, 파일 저장)

네트워크에 서비스를 제공하는 노드에 보상을 지급

\$0.01 미만의 소액결제에 이용



네트워크 보호 기능

악의적 행위자가 네트워크 전체 투표권의 3분의 1을 장악하면
DLT 플랫폼은 공격에 노출

헤데라의 지분증명 시스템은 코인 가중치 투표를 적용,
악의적 행위자가 투표권의 3분의 1을 장악하려면
전체 코인 공급량의 3분의 1을 사들여야 하므로 공격이 어려움

+

03.

코인 가중치와 지분증명 합의를 통한 Hbar의 네트워크 보호

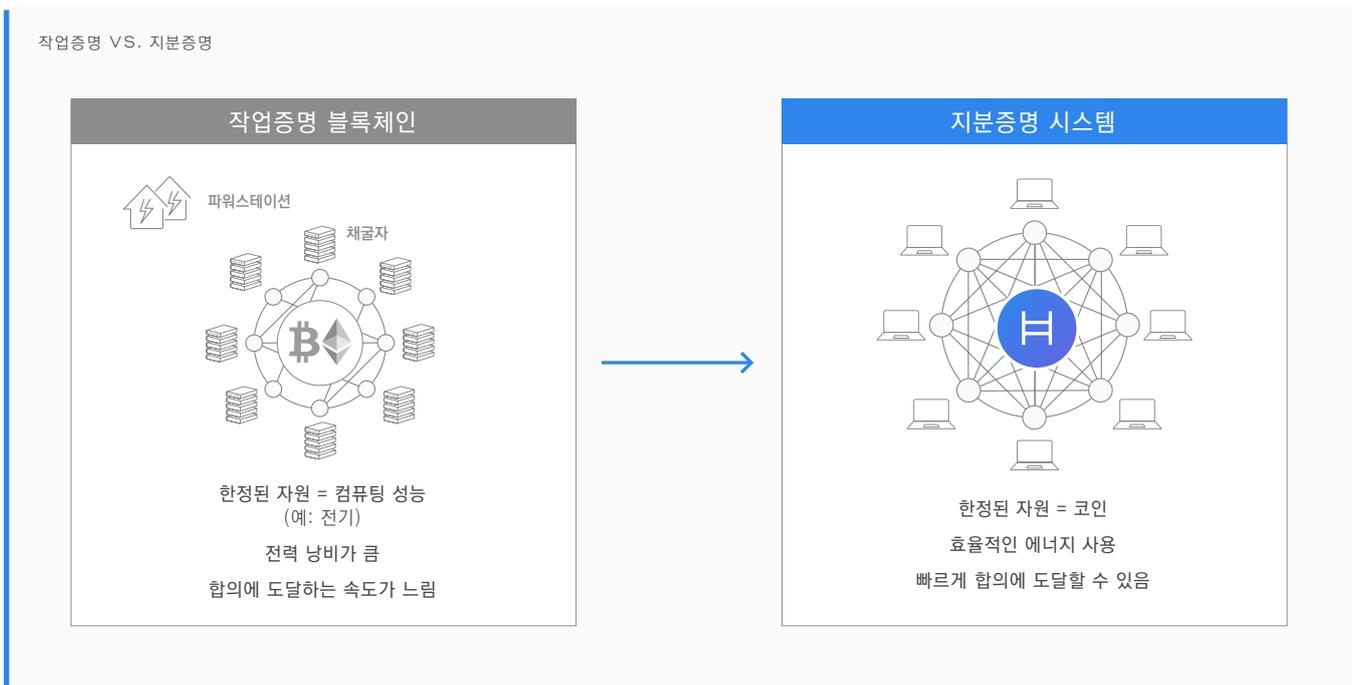
Hbar는 코인 가중치와 지분증명 합의를 적용함으로써 사이버 공격으로부터 네트워크를 보호합니다.

모든 퍼블릭 DLT에는 한정된 자원이 필요합니다.

공개된 개방형 DLT 네트워크에서는 누구든지 합의에 참여하는 노드를 실행할 수 있습니다. 따라서, 악의적 참여자가 네트워크를 중단시키고 트랜잭션에 대한 합의에 도달하지 못하게 하는 경우에 항상 대비해야 합니다. 해커들은 합의를 위한 네트워크 전체 투표권의 3분의 1을 장악함으로써 네트워크를 공격할 수 있습니다. 퍼블릭 DLT 네트워크는 이러한 공격으로부터 네트워크를 보호하기 위해 한정된 자원을 필요로 합니다.

작업증명 네트워크에 필요한 자원: 컴퓨팅 성능과 전력

비트코인이나 이더리움과 같은 작업증명 블록체인에서 필요로 하는 한정된 자원은 컴퓨팅 성능과 관련된 전력 소비량입니다. 네트워크 노드('채굴자')는 트랜잭션을 '블록'으로 그룹화하고, 다음 블록을 원장에 추가하기 위해 경쟁하여 끊임없이 이어지는 변경 불가능한 블록체인을 만듭니다. 승자에게는 암호화해가 지급되기 때문에 노드는 이 작업에 수행할 인센티브를 부여받습니다. 암호화된 퍼즐 등의 작업증명 메커니즘은 부하를 일으킴으로써 시스템 속도를 늦추어 네트워크가 주문에 대한 합의에 도달하기 전에 블록이 추가되는 것을 방지하도록 설계되었습니다. 이 퍼즐을 풀기 위해서는 상당한 컴퓨팅 성능이 필요하고, 이는 막대한 전력을 필요로 합니다. 이 시스템에서 악의의 공격자가 합의 과정을 방해하는 데 필요한 노드를 차지하려면 엄청난 금액을 들여 다량의 컴퓨터 하드웨어를 사들이고 어마어마한 전력 소비량을 감수해야만 합니다.



² 모든 분산형 네트워크는 악의적인 공격자가 네트워크 투표권의 3분의 1을 통제하면 해킹될 수 있습니다.

지분증명 네트워크에 필요한 자원: 해당 네트워크의 암호화폐

반면, 지분증명 방식 DLT 시스템에서는 해당 플랫폼의 디지털 코인이 한정된 자원으로 쓰입니다. 그리고 트랜잭션을 검증하는 노드의 능력은 노드가 보유한 코인의 양 즉, 지분에 비례합니다. 합의에 도달하는 데 필요한 노드의 지분의 양이나 방법을 정의하는 방식은 플랫폼마다 다르지만, 반드시 플랫폼의 알고리즘을 통해 발생하며 어떤 식으로든 암호화폐 지분 보유량에 비례하게 됩니다.

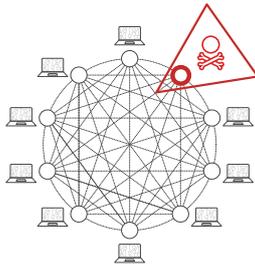
지분증명 시스템에서 모든 플랫폼의 코인은 네트워크가 출시하는 시점에 생성됩니다. (헤데라 네트워크가 오픈할 때 500억 개의 Hbar를 생성한 것과 마찬가지로입니다.) 코인은 값비싸고 비효율적인 컴퓨터 연산을 통해 새롭게 '채굴'되지 않습니다. 결과적으로 지분증명 시스템은 작업증명 방식보다 훨씬 저렴한 비용으로 훨씬 빠르게 트랜잭션을 처리할 수 있습니다.

합의에 대한 코인 가중치 투표로 사이버 공격을 방지

헤데라는 지분증명 방식의 네트워크로, 그 코인인 Hbar는 네트워크를 보호하기 위한 자원으로 이용됩니다. 해시그래프 합의 알고리즘을 사용하는 모든 분산 원장은 네트워크상 투표권의 3분의 2 이상에 의해 트랜잭션이 검증될 때 합의에 도달합니다. 이때 악의적인 공격자가 네트워크를 방해하기 위해서는 전체 투표권의 3분의 1을 확보해야 합니다.

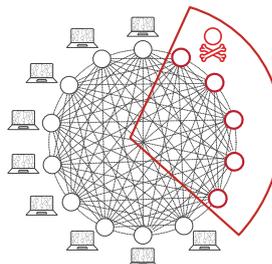
코인 가중치 투표

A 시나리오: 코인 가중치 없음 - 공격 임계치: 노드의 1/3



- 총 10개의 노드
- 1개의 노드를 악의적 행위자가 운영
- ▶ 총노드의 1/10이 악의적 (10% < 33.3%)

✓ 합의에 도달

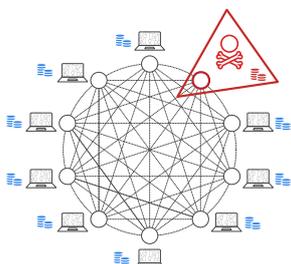


- 총 14개의 노드
- 5개의 노드를 악의적 행위자가 운영
- ▶ 총노드의 5/14가 악의적 (36% > 33.3%)

✗ 네트워크가 공격에 노출

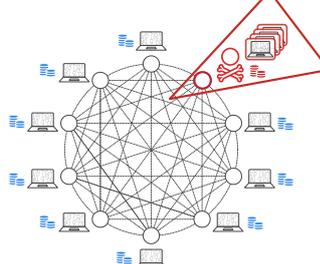
✗ 시빌 어택에 취약

B 시나리오: 코인 가중치 투표를 적용한 지분증명 네트워크 - 공격 임계치: 코인의 1/3



- 총 10개의 노드, 100개의 코인
- 1개의 노드가 10개의 코인을 보유
- 1개의 노드를 악의적 행위자가 운영
- ▶ 총 10/100개의 코인을 보유한 1개의 노드가 악의적 (10% < 33.3%)

✓ 합의에 도달



- 총 14개의 노드
- 5개의 노드를 악의적 행위자가 운영
- 총 코인의 수는 100개로 변하지 않음
- ▶ 총 10/100개의 코인을 보유한 5개의 노드가 악의적 (10% < 33.3%)

✓ 합의에 도달

✓ 시빌 어택으로부터 안전

- 분산형 네트워크에서는 트랜잭션이 네트워크 전체 투표권의 2/3 이상에 의해 검증되었을 때 합의에 도달
- 공격에 성공하려면 악의적 행위자가 투표권의 1/3을 통제해야 함
- 코인 가중치를 적용한 지분증명 투표 시스템은 투표권의 1/3을 통제하는 것을 어렵게 하여 시빌 어택에 대비함

³ 참고: 헤데라 거버닝 카운슬은 트랜잭션 검증을 위한 노드 투표에 재량권을 행사하지 않습니다. 헤데라 플랫폼에서 카운슬 위원들이 개별 대표를 통해 실시하는 투표는 '거버넌스'에 한하며, 트랜잭션에 대한 합의는 해시그래프 합의 알고리즘에 따라 자동으로 실행되는 노드의 투표를 따릅니다. 초기에는 카운슬이 노드를 운영하지만, 이때도 노드의 '투표'는 알고리즘에 따라 자동으로 실행됩니다.

개인적이고 허가된 DLT 네트워크에서는 모든 노드 호스트가 서로 알려져 있고 신뢰할 수 있으며, 노드 1개당 1표로 투표권을 계산할 수 있습니다. 노드의 3분의 2 이상에 의해 트랜잭션이 검증되면 네트워크는 합의에 도달하고 해당 거래가 공유된 분산 원장에 배치될 수 있게 됩니다. 하지만 공개 원장에서는 누구나 노드를 설정할 수 있습니다. 이때 노드와 투표권을 1:1로 계산한다면 악의적 공격자가 거의 아무런 비용 없이도 소위 '양말 인형'이라고 부르는 가상 노드를 마구 생성하여 투표권의 3분의 1을 확보하고 네트워크를 방해할 수 있게 되는데, 이것을 '시빌 어택'이라고 합니다.

시빌 어택으로부터 네트워크를 보호하기 위해 헤데라는 합의에 참여하는 노드의 투표권을 Hbar 1개당 1표로 책정하였습니다. 노드가 트랜잭션을 네트워크에 제출하면 트랜잭션의 유효성을 검증하는 임의의 노드로 내용이 전달됩니다. 각 노드의 표는 스테이킹 또는 프록시 스테이킹된 Hbar의 수에 따라 가중치가 주어지고, 총 코인 공급량의 3분의 2 이상에 해당하는 노드에 의해 트랜잭션이 검증되면 합의에 도달합니다. 코인 가중치 시스템에서는 공격자가 가상 노드를 아무리 생성해도 Hbar의 지분량은 변하지 않는다는 점을 이용하여 시빌 어택을 방지합니다. 해커가 이 시스템을 공격하려면 전체 코인 공급량의 3분의 1을 사들인 다음 스테이킹해야만 하기 때문입니다.

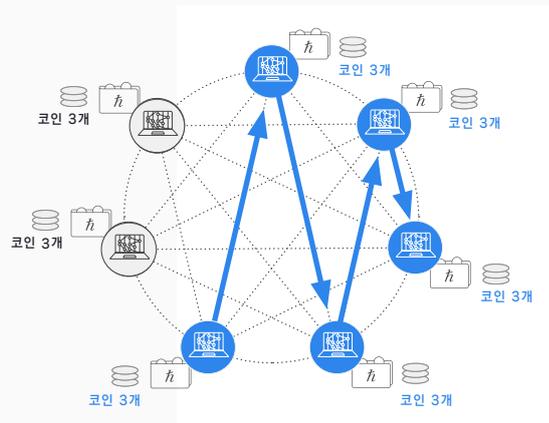
한편, 노드 수가 아니라 스테이킹된 Hbar의 지분에 의해 합의가 이루어지기 때문에, 이것이 계산되는 동안 노드가 온라인인지 오프라인인지 여부는 문제가 되지 않습니다.

헤데라 네트워크의 코인 가중치 투표

코인 공급량의 3분의 2 이상에 해당하는 노드에 의해 트랜잭션이 검증되면 합의에 도달

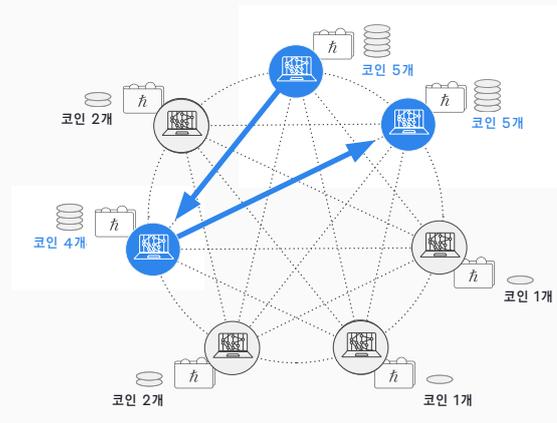
예시 1

- 각 노드에 코인을 공평하게 분배 (노드 당 코인 3개)
- 5개의 노드가 트랜잭션을 검증하면 합의에 도달 (5×3=15, 총 21개 중 15개의 코인 = 71.4% > 66.6%)



예시 2

- 각 노드에 코인을 임의로 분배
- 14개의 코인을 보유한 노드가 트랜잭션을 검증하면 합의에 도달 (총 20개 중 14개의 코인 = 70% > 66.6%)



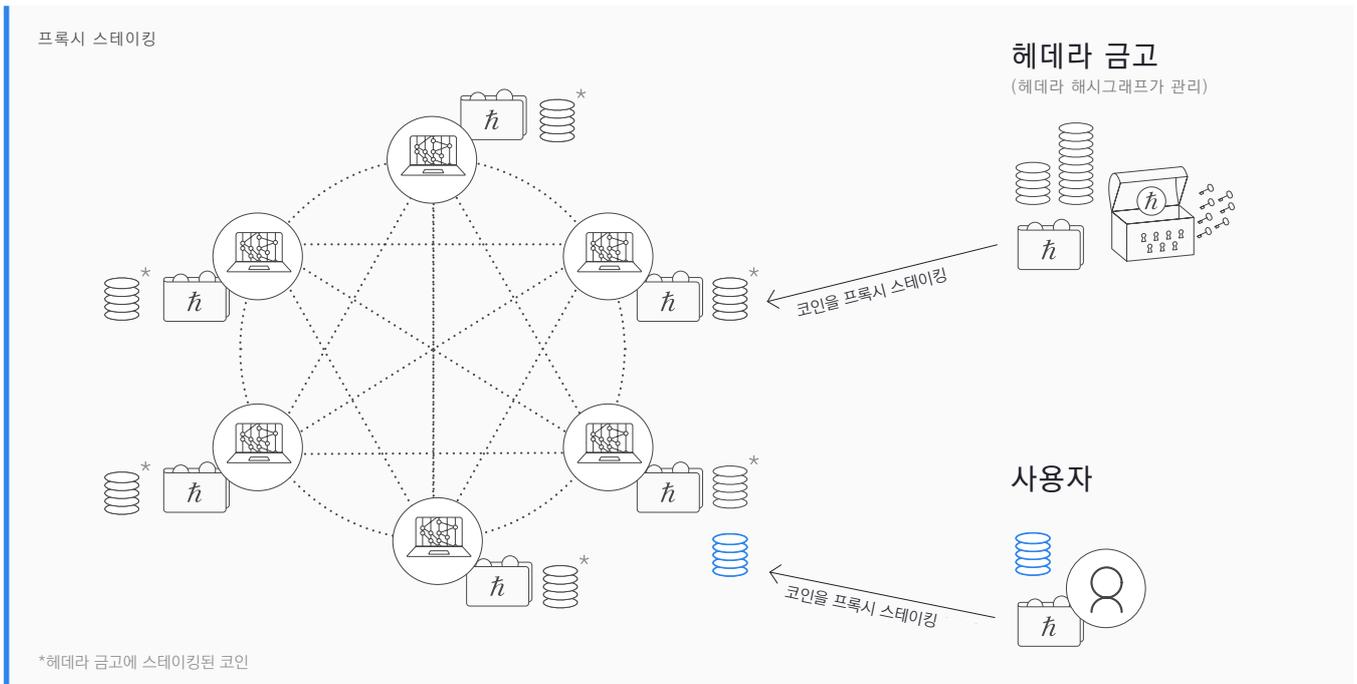
스테이킹과 프록시 스테이킹

헤데라의 코인 가중치 합의 알고리즘은 총 Hbar 공급량의 3분의 2 이상을 대표하는 노드에 의해 트랜잭션이 검증되어야 하므로 실제로 그만큼의 코인이 노드에 스테이킹되어 있는 것이 중요합니다. 문제는 헤데라 네트워크의 모든 사용자가 트랜잭션 비용을 위해 Hbar를 보유하고 있기는 하지만 그들 중 대부분이 노드를 직접 운영하지는 않는다는 것입니다.

'프록시 스테이킹'은 노드를 운영하지 않는 Hbar 소유자들이 다른 사용자가 운영하는 노드에 자신의 코인을 가상으로 스테이킹하고, 합의에 기여한 보상을 얻는 것입니다. 노드에 프록시 스테이킹된 Hbar는 트랜잭션을 검증할 때 해당 노드의 지분 즉, 투표권의 일부로 간주됩니다.

노드 보상 지급은 (프록시 스테이킹을 포함하여) 스테이킹한 총 Hbar의 양에 비례하여 노드에 지급되며, 프록시 스테이킹한 Hbar의 소유자와 노드 간에 분배될 예정입니다. 이처럼 이익을 얻을 수 있기 때문에 노드를 운영하지 않더라도 프록시 스테이킹에 참여할 동기를 가지게 됩니다.

프록시 스테이킹된 Hbar에 대한 모든 권한은 소유자에게 있습니다. 노드는 프록시 스테이킹된 Hbar를 사용할 수 없으며, 소유자는 언제든지 프록시 스테이킹을 해제하거나 다른 노드로 옮길 수 있으며 Hbar를 사용할 수도 있습니다.



* 네트워크 최초 공개 시점에서는 네트워크 사용자의 프록시 스테이킹 기능 이용이 제한되지만, 플랫폼 개발 단계에 따라 추후 추가될 예정입니다.

04.

Hbar의 배포와 헤데라 금고 관리

지난 2018년 8월 24일, 헤데라 메인넷의 런칭과 함께 생성된 총 500억 개의 Hbar는 헤데라 금고에 예치되었습니다.

네트워크를 출시하기 전, 헤데라는 네트워크가 지속적이고도 안전하게 성장할 수 있도록 Hbar 배포 일정을 개발하였습니다. 이 일정은 다음의 주요 사항을 고려하여 정해졌습니다.

- 규정 준수
- 네트워크 보안
- 탈중앙화
- 중앙집중식 의사결정이 아닌 시장에 의한 소매 거래 및 가격 결정

공개된 일정에 따르면, Hbar의 배포는 다가올 오픈 액세스부터 2033년 8월, 네트워크 출시 15주년까지 느리고도 신중하게 진행될 계획입니다.

초기 HBAR 할당 및 공급

주의 : 이 장에서는 Hbar의 초기 할당과 배포 일정을 안내합니다. 현재 헤데라는 오픈 액세스부터 2033년 8월까지 Hbar 공급량을 배포할 계획입니다. 헤데라의 배포 일정은 예상치 못한 사업상의 변화 또는 규제 변경으로 인해 달라질 수 있으며, 헤데라는 추후 발생할 수 있는 변경사항으로 인한 투자 손실에 대해 책임을 지지 않습니다.

헤데라 플랫폼의 개발과 네트워크의 초기 운영 자금을 지원하기 위해 헤데라는 미래 토큰 구매 약정(Simple Agreements for Future Tokens, SAFTs) 형태의 투자를 받아 총 1억 2천 4백만 달러를 모금했습니다. SAFT는 미래 판매가격에 대한 할인이 아닌 토큰당 고정된 가격으로 제공되었습니다. SAFT의 초기 2라운드는 3~4년의 긴 공급 일정을 가지고 있으며, 최종 라운드는 투자자들에게 4년 또는 8개월 공급 일정 가운데 선택할 수 있도록 옵션이 제공되었습니다. 첫 2개 시드 라운드에서 토큰의 가격은 0달러에 가까웠고, 3번째 라운드에서는 공급 일정에 따라 4년에 걸쳐 9.6센트에 구매하거나, 8개월 동안 12센트로 구매하도록 책정하였습니다.

한편, 헤데라는 창업자와 직원, 자문위원, 전략 파트너, 초기 개발자 및 네트워크 이용자에게 비용 부담 없이 코인을 할당해 왔습니다.

현재 전체 공급량의 54%가 할당되지 않은 상태로 남아있습니다.

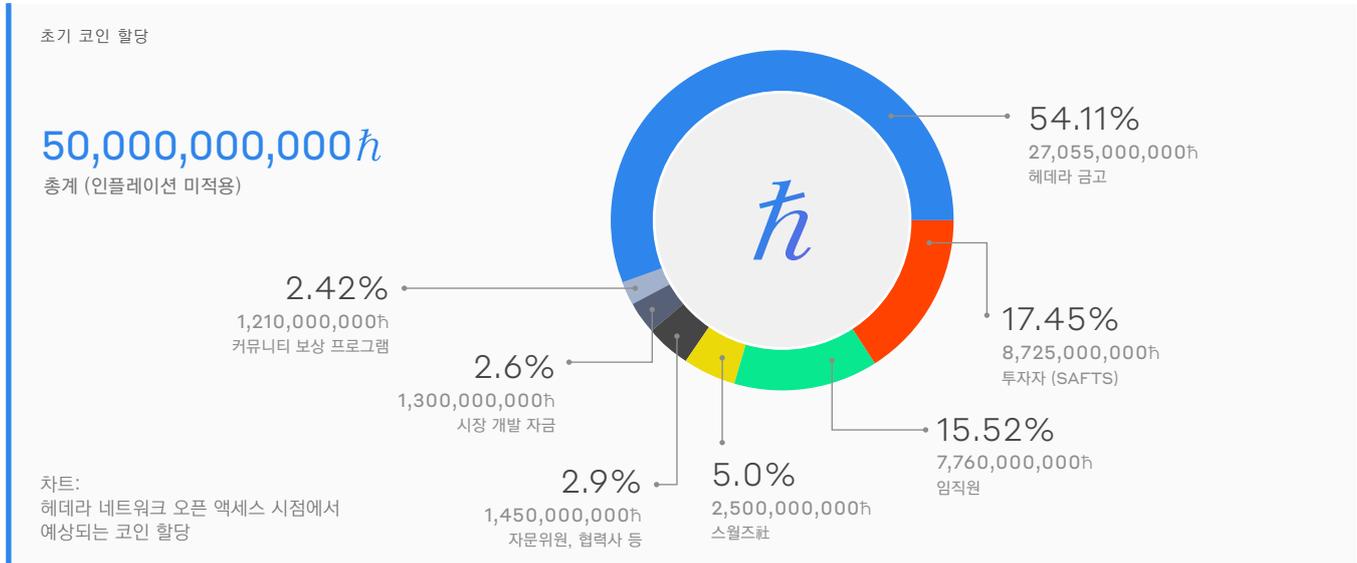
첫 5년간의 코인 할당 및 배포 계획

연도	SAFT 시드 라운드	SAFT 3라운드	헤데라 팀*	커뮤니티 보상 프로그램**	자문위원, 협력사 등	시장 개발 자금	스텔즈社	금고 보관분	공급 증가량	총 공급	% 순환율
오픈 액세스 시점	194,062,857	185,263,841	0	1,208,333,333	1,957,864	0	0	0	1,589,617,895	1,589,617,895	3.18%
1주 차 종료 후	194,062,857	0	0	0	12,957,865	0	0	0	207,020,722	1,796,638,617	3.59%
남은 2019년	658,221,234	273,510,244	381,806,450	0	135,277,192	7,297,952	60,000,000	450,000,000	1,966,113,072	3,762,751,689	7.53%
2020	2,076,801,486	322,018,909	1,680,957,394	0	280,153,579	88,902,294	122,717,936	431,279,328	5,002,830,926	8,765,582,615	17.53%
2021	1,956,904,787	48,508,723	439,526,433	0	114,622,450	145,200,650	299,369,682	479,929,740	3,484,062,465	12,249,645,080	24.50%
2022	1,450,322,972	48,508,723	490,577,959	0	75,811,488	145,200,650	168,146,581	479,929,740	2,858,498,113	15,108,143,193	30.22%
2023	693,987,432	48,508,717	1,156,170,025	0	168,033,196	251,562,259	226,955,235	981,609,047	3,526,825,911	18,634,969,104	37.27%

표: 오픈 액세스가 예정된 2019년 9월 16일부터 2023년 12월 31일까지 예상되는 배포 일정과 유형별 할당

* 현재 팀이 보유한 토큰에 2022년까지 채용을 위한 예산을 합산

** 2억 830만여 개의 Hbar가 헤데라의 커뮤니티 테스트 프로그램의 일환으로 커뮤니티에 배포 중이며, 10억 개는 커미션 프로그램을 위해 별도 할당됨



오픈 액세스 이후

2019년 여름, 헤데라 플랫폼은 진행 중인 테스트 단계를 완료하고 누구나 헤데라 계정을 만들고 네트워크를 사용할 수 있도록 완전히 공개할 예정입니다. 이와 함께 헤데라는 SAFT 투자자, 직원, 자문위원, 협력사에 Hbar를 초기 배포할 계획입니다.

이때 전체 공급량의 3.18%에 해당하는 Hbar가 배포된 다음 순환 유통될 것으로 기대됩니다. 이러한 방식을 순환 공급이라고 합니다. 오픈 액세스로부터 일주일 뒤에는 전체 Hbar 공급량의 3.59%가 배포되어 유통될 것입니다.

SAFT 및 직원, 자문위원, 협력사와의 계약에 따른 배포는 최대 6년까지 다양한 약정 기간에 걸쳐 배포될 것입니다. 공동 창업자 및 초기 고위 임원이 가장 긴 일정 에 따라 할당을 받습니다.

2020년 1월 1일 이전까지 헤데라의 공동 창업자인 리먼 베어드(Leemon Baird)와 맨스 하몬(Mance Harmon)에게 직원 보조금으로 주어지는 Hbar는 없습니다. 리먼과 맨스가 SAFT 지분을 보유하고 있기 때문에 이에 따른 소정의 Hbar가 주어지지만, 그들이 받게 될 전체 Hbar의 76%를 메인넷 출시 5주년이 되는 2023년 8월 이후까지 지연 출시할 계획입니다.

현재 직원으로 근무하고 있는 다른 초기 고위 임원들이 직원 보조금 명목으로 받은 Hbar 역시 2020년 1월 1일 이후에 배포될 예정이며, 2023년 8월까지 그들이 보유한 Hbar의 상당량이 지연 출시되는 것에 동의했습니다.

한편, 헤데라의 SAFT 시드 라운드 투자자들은 3~4년에 걸쳐 일 단위 내지 월 단위로 간격을 두는 일관된 배포 일정에 동의했습니다. 기존 SAFT 배포 일정대로 오픈 액세스 날짜에 토큰의 40%를 출시하는 대신, 초기 SAFT 투자자들은 첫 주에 최대 10%의 코인을 받습니다. 나머지는 36개월에서 48개월에 걸쳐 균등 하게 배분되며 별론 페이먼트는 없는 조건입니다

안전한 탈중앙화를 위한 Hbar의 배포 일정

헤데라가 생각하는 안전한 탈중앙화를 위한 4가지 핵심요건은 다음과 같습니다.

1. 탈중앙화된 거버넌스
2. 네트워크 유틸리티
3. 비허가형 노드
4. 코인의 분산

헤데라의 탈중앙화된 거버넌스에 대해서는 [이 문서](#)에서 자세히 다루고 있으니 참고해 주십시오. 네트워크 유틸리티란 네트워크가 그 자체로 유용하고 사용자에게 가치를 제공해야 한다는 의미입니다. 백서의 목적에 부합하기 위해 이번 장에서는 비허가형 노드와 코인의 분산, 그리고 이 두 요소가 탈중앙화를 안전하게 달성하고 유지하는 데 어떤 역할을 하는지를 중점적으로 다루겠습니다.

개인이나 기업이 노드를 실행하기 위해 권한이 필요한 것을 ‘허가형 노드’라고 합니다. 반대로 ‘비허가형 노드’ 방식에서는 네트워크상의 누구나 노드를 운영할 수 있습니다. 퍼블릭 네트워크에서는 노드를 누가 운영하고 있는지에 따라 허가형 또는 비허가형으로 실행할 수 있습니다. 헤데라의 탈중앙화 경로는 소수의 허가형 노드에서 시작하여 시간이 지남에 따라 그 수가 늘어나게 됩니다. 점차 노드를 운영하기 위해 필요한 권한이 완화되고, 최종적으로는 플랫폼이 완전히 비허가형 노드로 전환되어 누구나 노드를 운영할 수 있게 됩니다. 이것이 익명의 노드들로 완전히 탈중앙화된 네트워크를 구현하기 위한 헤데라 탈중앙화 로드맵의 최종 목표입니다.

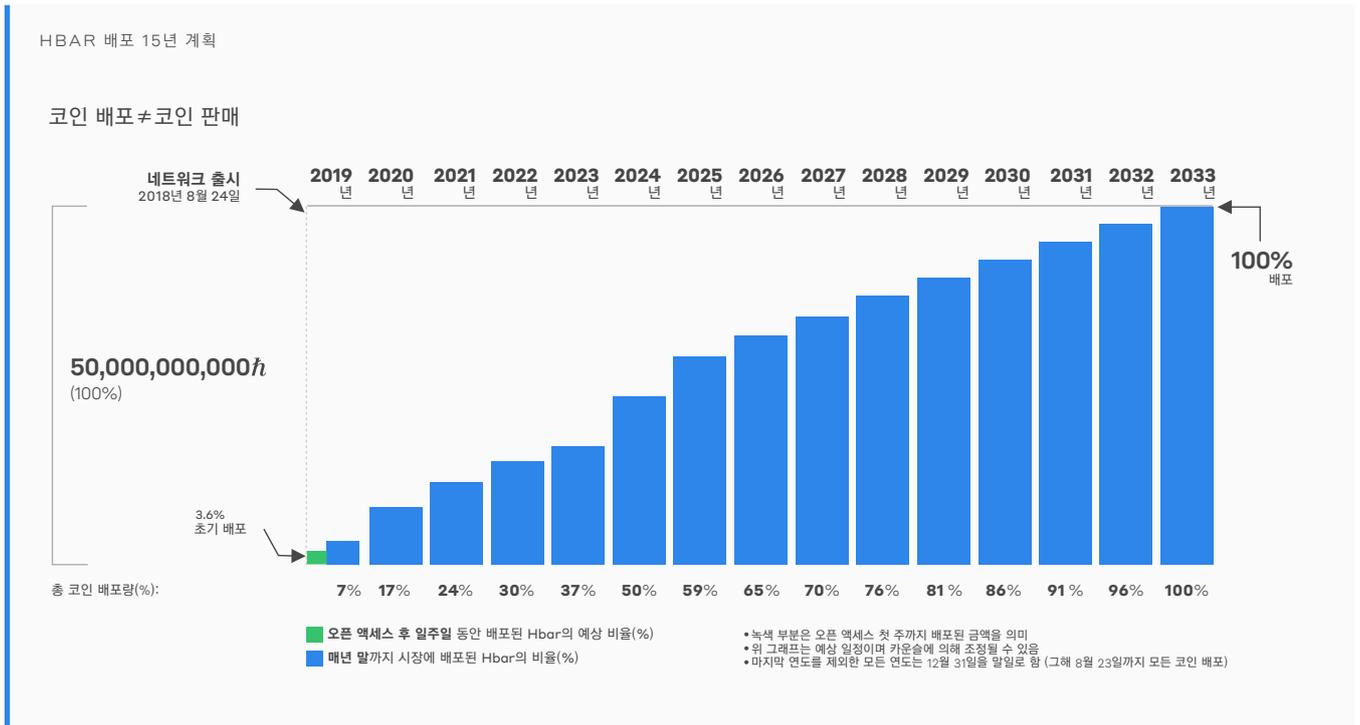
지속적인 탈중앙화를 추구하기 위해서는 비허가형 노드와 더불어 코인이 널리 분산되어야 합니다. 코인은 지분증명 네트워크의 지분이며 네트워크가 합의를 결정하는 방법이기도 합니다. 지분이 클수록 합의에 대해 가중치를 부여받습니다. 분산된 합의를 위해서는 분산된 지분이 필요하며, 결과적으로 분산된 코인이 필요한 이유입니다. 따라서 Hbar는 악의의 공격자가 3분의 1의 지분을 확보할 수 없도록 널리 분산되어야 합니다.

헤데라는 ‘비허가형 노드 추구’와 ‘코인의 광범위한 분산 추구’라는 두 방법을 조합하여 발전된 탈중앙화를 달성하는 동시에 네트워크 보안을 확보하고자 합니다.

먼저, 헤데라는 네트워크를 호스팅할 권한이 있는 노드에서 권한이 없는 노드로 이동하는 일정을 제어할 것입니다. 코인의 집중도는 노드의 허가 여부와 관계없이 스테이킹된 양에 따라 결정됩니다. 네트워크의 보안을 위해, 유통되고 있는 코인의 시가총액이 충분히 높아져서 악의의 공격자가 시빌 어택을 실행하는 데 필요한 3분의 1의 코인을 사들이기 어려워질 때까지는 네트워크가 허가형으로 운영될 수 있습니다.



둘째, Hbar 코인은 네트워크가 출시된 2018년 8월부터 15년에 걸쳐 느리고 안정적으로 공급될 것입니다. 오픈 액세스와 함께 최초 배포되는 Hbar는 전체 500억 개의 3.18%, 최대 15억 9천만 개에 한정될 것으로 예상됩니다. 2019년 말까지 전체 Hbar의 7.53%가 배포되고 2023년 중순까지도 전체 Hbar의 33%를 밀도는 양만이 배포될 예정입니다. 2023년부터는 10년에 걸쳐 헤데라 금고에 남은 Hbar가 배포되어 유통될 것으로 전망하고 있습니다.



이 느린 일정은 헤데라 플랫폼이 안정적이고 질서 있게 성장하여 진정으로 유용하고 널리 사랑받는 플랫폼이 될 수 있도록 보안을 희생하지 않으면서 규모를 확장하기 위해 신중하게 계획된 것입니다. 헤데라 플랫폼은 신뢰할 수 있고 사용자에게 권한을 부여하며 안전한 온라인 세계를 약속합니다. 이는 또한 사용자가 코인을 통해 과도한 투기를 시도하지 않도록 짜인 일정이기도 합니다. 코인의 배포 일정이 다양한 거버닝 카운슬 위원 조합의 투표와 서명을 통해서만 변경될 수 있도록 하고, 이를 공개적으로 안내하여 전체 코인 유통량의 투명성과 예측 가능성을 높임으로써 정보 비대칭성을 최소화하고 시장 조작에 대항하는 것입니다.



지속 가능한 탈중앙화 네트워크를 위한 헤데라의 방법론에 대한 자세한 내용은 해시그래프 합의 알고리즘의 투자자인 리먼 베어드 박사의 웹 세미나를 참고해 주십시오.

유튜브 바로가기 : youtube.com/hederahashgraph



Hedera™
Hashgraph

What future will you build?

© 2019 Hedera Hashgraph, LLC. All rights reserved.

The Hedera Hashgraph logo is a trademark of Hedera Hashgraph, LLC. All other company and product names may be trademarks of the respective companies with which they are associated.