Hedera™ Hashgraph

UNDERSTANDING DECENTRALIZATION OF HEDERA HASHGRAPH

Decentralization of consensus:

The path to permissionless network nodes

TABLE OF CONTENTS

01.

——

INTRODUCTION

Public distributed ledger technologies offer the opportunity for a complete overhaul and advancement of the web never before possible, enabling trusted and secure value creation and transfer, ownership of data, and identity management.

Hedera Hashgraph, LLC ("Hedera") believes that complete decentralization is paramount for the efficacy of a public distributed ledger's adoption by businesses, individuals, universities, governments, non-profit organizations, and more. And that the path towards complete decentralization of a public network is methodical.

Decentralization of consensus and reaching permissionless network nodes is one of the four parts of that complete path. The other three are decentralization of governance, development of the codebase (not yet available), and the application ecosystem (not yet available).

Any stakeholder participating in a public network, including its node participants, application developers, and end-users, requires the network nodes to be in a fully permissionless state to realize the primary benefit of public distributed ledger technologies: trust between parties who may not know or trust each other.

This whitepaper defines decentralization requirements when it comes to nodes on the Hedera network and describes how Hedera will further continue progressing along its path to meet them.

Hedera™ Hashgraph

___

# DECENTRALIZATION OF CONSENSUS: THE PATH TO PERMISSIONLESS

Hedera Hashgraph is a proof-of-stake network that aims to use permissionless nodes and a widespread coin distribution to ensure the network's security while working to achieve complete decentralization.

The goal of becoming a permissionless network is to allow any business or individual to anonymously deploy a Hedera mainnet consensus node and earn hbars. Node operators are compensated for their bandwidth, storage, and compute used to validate transactions on the Hedera network — this is the truest form of decentralized consensus that can be achieved by a public network. Widespread coin distribution ensures decentralized ownership of hbars, the Hedera network's native cryptocurrency, so no attacker or group of attackers can amass control over one-third of the coins, which may result in network disruption.

Throughout this section, we'll focus on permissionless nodes and coin distribution, including their roles in further progressing towards and maintaining decentralization.

THE PATH TO PERMISSIONLESS NETWORK NODES

Distributed ledgers are "private" or "public", and the networks on which the ledgers reside are "permissioned" or "permissionless" — they can be any combination of any of the two, as depicted by the quadrant in Figure 1 below.
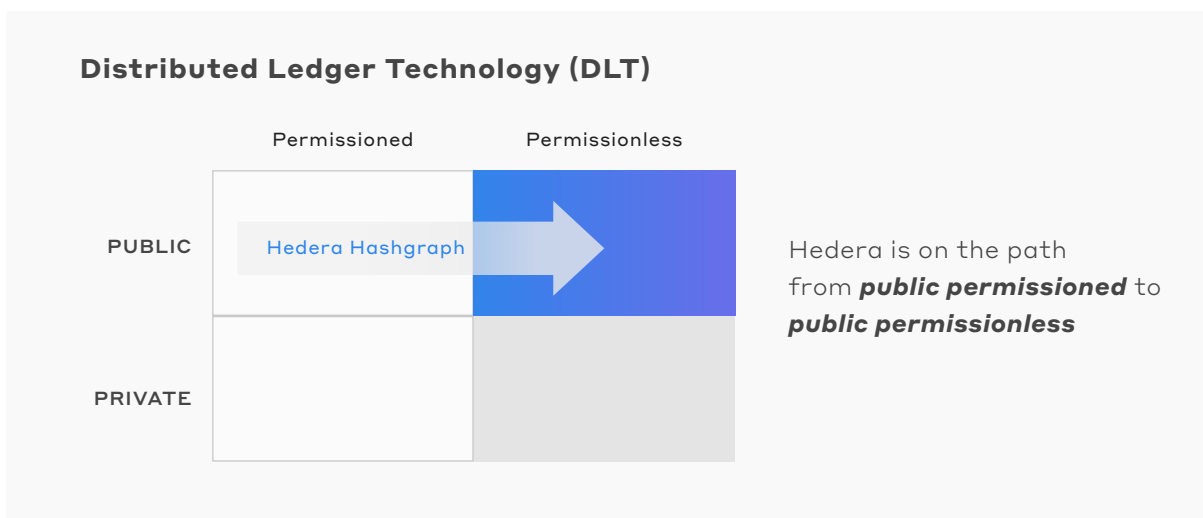
Today, the Hedera network resides in the upper left quadrant as a public permissioned network. Consensus nodes that facilitate the network's transactions and manage its state are operated by Hedera Governing Council members, all of which have all been invited to join as network operators. As the security, stability, and incentives of the Hedera network mature, the network will relax permissions by opening node operations to more entities and individuals.

PRIVATE / PERMISSIONED:

This type of network offers little decentralization. Participants must be invited to perform transactions on the network. The network nodes facilitating those transactions must also be invited to join the network and meet specific criteria or provide identification. Any party can also be removed without warning at any time.

R3 CORDA   HYPERLEDGER FABRIC   QUORUM

PRIVATE / PERMISSIONLESS:

Requires that those making transactions on the network applications be invited to join and can be removed without warning at any time. The nodes that constitute the network and run said applications can freely and anonymously join and contribute, typically in exchange for a network's native cryptocurrency.

HOLOCHAIN   LTO NETWORK   MONET

PUBLIC / PERMISSIONED:

Anyone is allowed to make transactions on the network and may come and go at any time, without having to notify anyone, reveal their identity, or meet specific requirements. The nodes which constitute the network and facilitate those transactions must be invited to join the network.

EOS   RIPPLE   HEDERA HASHGRAPH

PUBLIC / PERMISSIONLESS:

This type of network is the most decentralized. Applications can be deployed in production or removed without notifying anyone, revealing their identity, or meeting any application criteria requirements. Additionally, the nodes which constitute the network can freely and anonymously join and contribute, typically in exchange for a network's native cryptocurrency.

BITCOIN   ETHEREUM   HEDERA HASHGRAPH
                                       Not Yet Available

The Hedera network will always remain public and eventually become permissionless for consensus. Any individual or organization will be able to run a node anonymously and earn hbars for supporting the network. assisting with network operations. To deliver on Hedera's commitment to permissionless nodes, the network will progress through three phases of decentralization:

Phase 1 of Hedera's network evolution:
Permissioned Hedera Council member consensus nodes

Hedera Hashgraph is a public DLT network available for developers and end users to create accounts and deploy decentralized applications.

During its initial phase, Hedera mainnet consensus nodes are permissioned, owned, and operated by Hedera Council members (with occasional support by Hedera for a transitional period). This ensures that Hedera Council members are not only governing the network but also directly participating in the network.

When new Council members join and stand up their nodes, these new nodes are typically operated jointly by the member and Hedera for a transitional period before the Council member takes over node operations itself. Council members are responsible for the infrastructure and operations of their node, though Hedera may also provide technical support from time to time during this initial phase.*

Permissioned Council Member Nodes
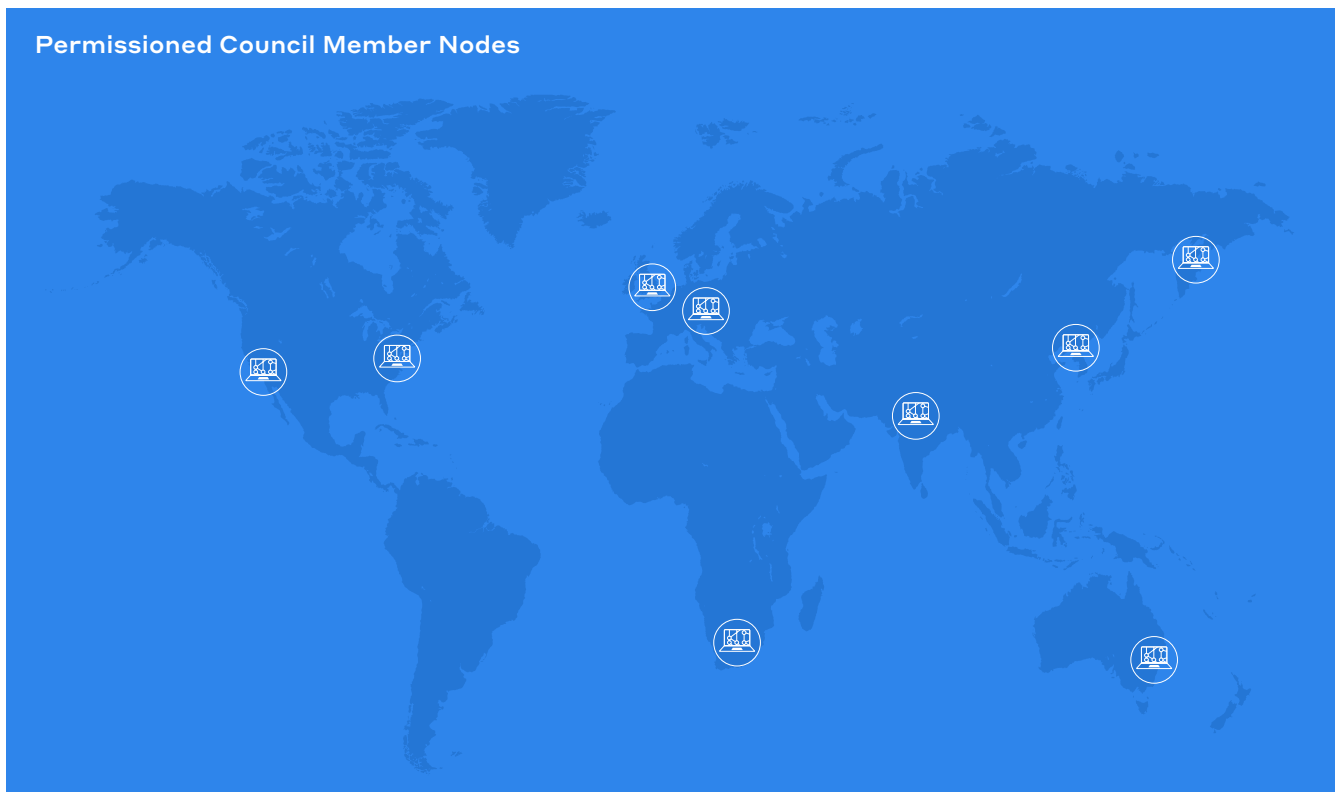
* Note: This section was updated to remove a reference to a potential whitepaper that was never published and clarify the role Hedera plays in establishing new network nodes for Council members as well as providing occasional technical support.

Phase 2 of Hedera's network evolution:
Many permissioned consensus nodes

When the Hedera network's security, stability, and incentives are determined to be sufficient by the Hedera Governing Council, peripheral parties and organizations will be invited to join the Hedera mainnet as permissioned consensus node operators and earn hbar cryptocurrency. The invited parties might include ecosystem partners, non-profit organizations, and other known and trusted entities. By this time, the Hedera mainnet code will have update, connect, and reconnect capabilities that will mitigate downtime for scheduled maintenance and allow node operators to upgrade their nodes independently.

Permissioned Council Member and Other Nodes
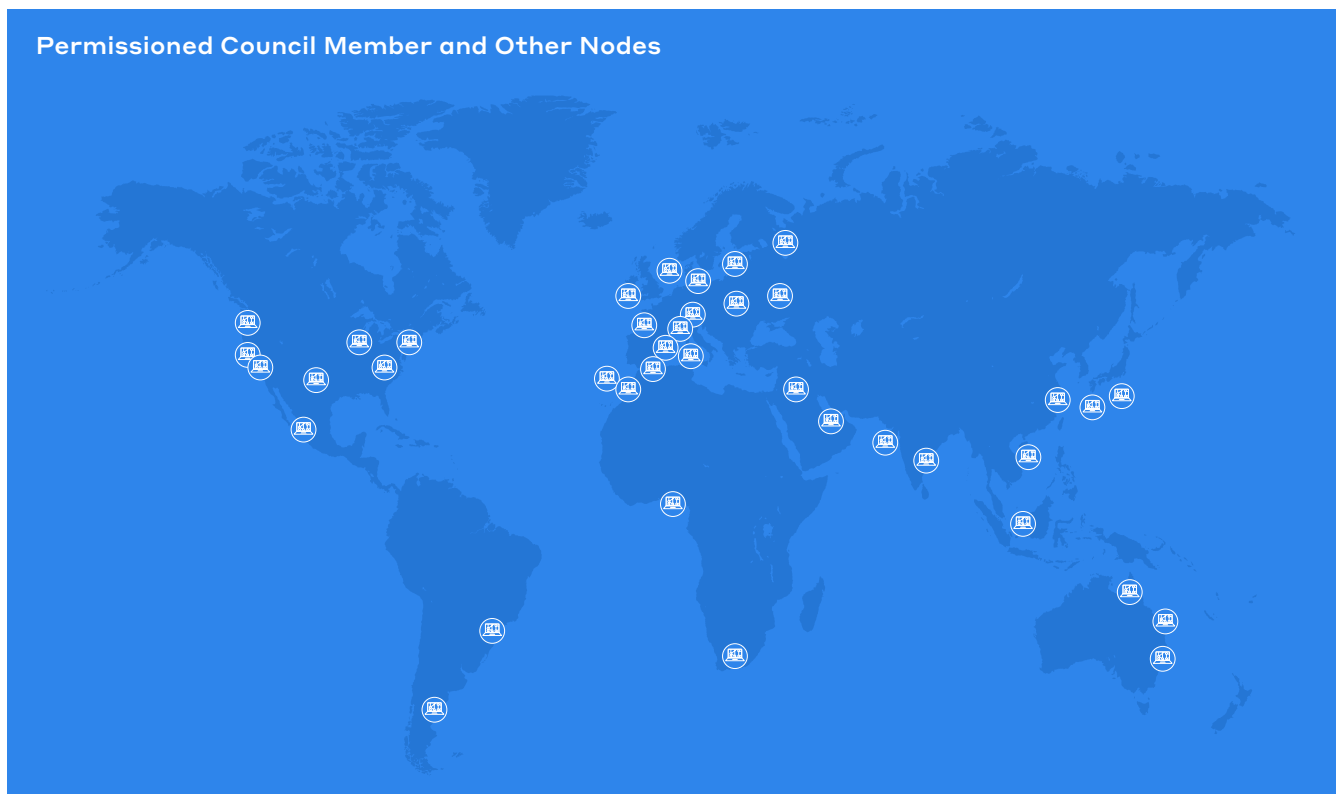
Phase 3 of Hedera's network evolution:
Permissionless nodes

Once the Hedera Governing Council has reached 39 members and up to hundreds of permissioned consensus nodes are live on the mainnet, the Hedera network will enter the final phase of decentralization and become a fully permissionless network.

Any person or organization will be able to run a Hedera mainnet consensus node with anonymity. All node operators receive hbars for the computing, bandwidth, and storage resources they use in contributing to consensus and providing services. Hedera expects that after reaching a permissionless mainnet, Hedera's network can expand to thousands of geographically distributed nodes.

Permissionless Nodes

Hedera™ Hashgraph

WIDESPREAD DISTRIBUTION OF HBAR CRYPTOCURRENCY

The Hedera network was launched in August 2018. At that time, the platform's total fixed supply of 50 billion hbars was minted and placed into the Hedera Treasury account. The Hedera Treasury is a cryptographically secure, multi-signature account, and hbars can only be transferred out of it when a majority of the Council members sign a transaction; this ensures that management of the network's native cryptocurrency is decentralized.

The utility of hbars on Hedera's proof-of-stake network

Hbar is used for network security and as "fuel" to pay for network services.

NETWORK PROTECTION

As a proof-of-stake network, hbars function as the limited resource to protect the network by staking them to nodes for voting power. The hashgraph algorithm achieves consensus on a transaction when the transaction is validated by more than two-thirds of the network's voting power.

Hbar cryptocurrency represents the "stake" of voting power in Hedera's proof-of-stake consensus model — more coins equal more voting power over consensus. Thus, to ensure the network's security, hbars need to be widely distributed so no attacker or group of attackers can amass control over one-third of the coins.

NETWORK FUEL

Anyone performing transactions on the Hedera network use hbars as a "fuel" to pay for network services (i.e., to send or receive hbars, tokenize assets, write data to the ledger, etc.) and reward network nodes for providing their computing resources (bandwidth, processing power, memory) to the network. Due to hashgraph consensus's efficiencies, transaction fees will remain low and consistent; for example, currently, a cryptocurrency transfer currently costs USD $0.0001 (paid in hbars).

A wide distribution of hbars for permissionless network protection

Until hbars are sufficiently distributed, Hedera will remain a permissioned network. To maintain the security of the network, the network will remain permissioned until the total value of all the circulating coins is high enough to be too expensive for a malicious user (or group of users) to buy one-third of the total supply to conduct an attack.

To ensure the network's protection, hbars need to be widely distributed so no attacker or group of attackers can amass control over one-third of the coins. The slow release schedule is intended to provide for the stable and orderly growth of the network to reach scale without sacrificing the safety necessary for a truly useful and widespread network.

You can learn more about hbars on the HBAR page of the Hedera website at
hedera.com/hbar

The monthly coin distribution reports can be found in Hedera's help center:
help.hedera.com/hc/en-us/articles/360002789198

STAKING AND PROXY STAKING OF HBARS

Proxy staking on the Hedera network will allow millions of account holders to stake hbars to directly participate in validating a transaction and reaching consensus, even if not running a node on the network. Nodes will receive rewards for both node operation and staking hbars, while proxy stakers receive rewards for choosing reliable network nodes to which they stake their hbars.

Once proxy staking is available, anyone holding hbars can stake them to a Hedera node. It's anticipated that the ecosystem of wallets, exchanges, custody providers, and other applications will support the ability to proxy stake hbars.

CONCLUSION

Decentralization is not a single, swift movement. It is a continuously evolving path that requires thoughtful planning and execution. This whitepaper outlined steps that Hedera has already taken and will continue to execute to ensure decentralized consensus of network node participants, where no single authority has too much control over the network coming to consensus. The entire path to decentralization will take years and is essential if Hedera is to achieve its vision of becoming the trust layer of the internet.

Follow the Hedera **blog**, **roadmap**, **network status**, and **council meeting minutes** for relevant updates and progress on Hedera's path to decentralization.

Hedera™
Hashgraph