Hello Future

The trust layer of the internet

Cooper Kunz
Developer Evangelist

cooper_kunz
Agenda

I. Overview of the Hedera Hashgraph public network
II. Foundations of the Hashgraph Consensus Algorithm
III. Users / projects building on Hedera
IV. How to start building your own applications
V. Q&A
Part 1 - Overview of the Hedera Hashgraph Public Network

@hashgraph
Enterprise adoption of public distributed ledgers

Performance  Security  Stability  Governance
Technology Overview

HASHGRAPH CONSENSUS & HEDERA NETWORK SERVICES
<table>
<thead>
<tr>
<th><strong>BLOCKCHAIN</strong></th>
<th><strong>HASHGRAPH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain is designed to be slow, as a security measure</td>
<td>Hashgraph is a distributed ledger, but not a blockchain</td>
</tr>
<tr>
<td>Proof-of-work puzzle adjusts to keep the system at a specific speed, as time is needed to determine which block of transactions to add to the chain</td>
<td>Combines a gossip protocol with virtual voting algorithm to efficiently and quickly achieve network consensus on transactions</td>
</tr>
<tr>
<td>Efforts to speed up blockchain all make security sacrifices</td>
<td>Asynchronous Byzantine fault tolerant (highest level of security for distributed networks)</td>
</tr>
<tr>
<td>Requires heavy electricity usage</td>
<td>Does not require heavy electricity usage</td>
</tr>
</tbody>
</table>
HEDERA MAINNET & MIRRORNET

MAINNET
• Can submit HAPI (Hedera API) transactions to the Hedera network
• Contributes to consensus on transactions
• Creates events on the Hedera network
• Requires HBAR cryptocurrency payment for transactions & queries

MIRRORNET
• Maintains a history of some or all of the Hedera network state and ledger of transactions
• Value-added services (managed read-only node, etc.)
• Enables analytical insight into an application’s state / transactions
• Publish and subscribe capabilities
## A third generation public distributed ledger

<table>
<thead>
<tr>
<th></th>
<th>1ST GENERATION</th>
<th>2ND GENERATION</th>
<th>3RD GENERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain</strong></td>
<td>Bitcoin</td>
<td>Ethereum</td>
<td>Hedera</td>
</tr>
<tr>
<td><strong>Transactions</strong></td>
<td>3+ TPS</td>
<td>12+ TPS</td>
<td>10,000+ TPS</td>
</tr>
<tr>
<td><strong>Average Fee</strong></td>
<td>$0.20 USD</td>
<td>$0.13 USD</td>
<td>$0.0001 USD</td>
</tr>
<tr>
<td><strong>Confirmation</strong></td>
<td>10-60 Minutes</td>
<td>10-20 Seconds</td>
<td>3-5 Seconds</td>
</tr>
</tbody>
</table>

- Cryptocurrency transactions. For Hedera, range shown for transactions not requiring a transaction record, but can receive a transaction receipt.
DAILY TRANSACTION POTENTIAL
Single shard, on-ledger

- Bitcoin: 432,000 txs
- Ethereum: 1,296,000 txs
- Ripple: 129,600,000 txs
- Hedera: 864,000,000 txs
Data Integrity

“Using Hedera Consensus Service, advertisers can be more confident that their data is both accurate and tamper-proof, aiding in the fight to reduce ad-fraud and recover the billions of dollars lost each year in wasted ad spend.”

Ian Mullins | CEO

REAL-TIME DATA
Transactions on Hedera are logged in real-time, making data accessible to applications and analytical tools.

VERIFIABLE TRANSACTIONS
Grant auditors, regulators, and partners the ability to verify application events with a transparent set of records.

LOW FEES
Logging events to Hedera costs just a fraction of a penny per event, ensuring access for web-scale applications without impacting the bottom line.
Micropayments

“Hedera is the only platform we’ve seen that can cope with the volume of split-second transactions that need to take place.”

Jiro Olcott | Director

CUSTOMIZABLE
Transactions of value in Hedera’s native cryptocurrency HBAR are expressed as code, enabling unique application experiences.

SCALABLE TRANSACTIONS
The efficiency of hashgraph yields extremely fast cryptocurrency transactions with finality in seconds.

LOW FEES
Operationally efficient, resulting in low and predictable cryptocurrency transaction fees.
Decentralized Identity

"The success of a self-sovereign identity solution is driven by the platform it’s built upon. While choosing the underlying platform, we compared many options, and decided to build Earth.Id on Hedera."

Shiv Aggarwal | Co-Founder

OPEN STANDARDS
Hedera’s credentials follow the decentralized identifier and verifiable credentials standards under development at the W3C.

EMPOWER USERS
Credentials on a decentralized network can give users greater control over when and to whom their identity attributes are shared.

SCALE TO DEVICES
Hedera Consensus Service can scale to support high-volume device identity use cases.
Governance
THE HEDERA GOVERNING COUNCIL
The Hedera Governing Council
Building the future together.

Up to **39** leading global organizations

**11** unique industries, **1** university, and **1** non-profit across major markets

Every member required to run a network node

Members not compensated beyond network node payments

**2.6%** influence per member (equal vote)

**5** committees: Membership, Technical Steering & Product, Treasury Management & Coin Economics, Legal/Regulatory, Marketing

3-year maximum term, with up to 2 consecutive terms

First **38** additional members selected by Hedera; council membership committee will find replacements
Network decisions:

- Feature decisions *(what)*
- Product roadmap *(when)*
- Fee model
- Node incentives
- Manage treasury
Hedera’s Strong Governance

**Technical Controls**
- No Forks
- Ensures simultaneous software upgrade

**Legal Controls**
- Patents & IP protections
- No license required to use network
- Open code review
The Hedera Governing Council
Building the future together.
Meet the Team
CO-FOUNDERS & EXECUTIVE TEAM MEMBERS
The Founders

Mance Harmon  
CO-FOUNDER & CEO

Mance is Co-Founder and CEO of Hedera. His prior experience includes serving as the Head of Architecture at Ping Identity, Program Manager program for the Missile Defense Agency, Course Director for Cybersecurity at the US Air Force Academy, and research scientist in Machine Learning at Wright Laboratory. Mance received a MS in Computer Science from the University of Massachusetts and a BS in Computer Science from Mississippi State University.

Dr. Leemon Baird  
CO-FOUNDER & CHIEF SCIENTIST

Leemon is the inventor of the hashgraph distributed consensus algorithm, and is the Co-Founder and Chief Scientist of Hedera. Previously in his career he was Professor of Computer Science and has been the Co-Founder of several startups, including two identity-related startups. Leemon received his PhD in Computer Science from Carnegie Mellon University and has multiple patents and publications in computer security, machine learning, and mathematics.
Company Facts:

- **55+ employees**

Funding
- **$124M** raised from institutions and accredited crowdsale

HBAR
- **Total supply: 50B**

Developer Community
- **Mainnet applications: 33+**
- **Testnet developers: 8,000+**
- **Discord chat: 8,000+**

The Executive Team

- **Dr. Leemon Baird**
  - CO-FOUNDER & CHIEF SCIENTIST

- **Mance Harmon**
  - CO-FOUNDER & CEO

- **Christian Harker**
  - CHIEF MARKETING OFFICER

- **Natalie Furman**
  - GENERAL COUNSEL

- **Lionel Chocron**
  - CHIEF PRODUCT OFFICER

- **Zenobia Godschalk**
  - SENIOR VP, COMMUNICATIONS

- **Jordan Fried**
  - SENIOR VP, BUSINESS DEVELOPMENT

- **Mehernosh Mody**
  - SENIOR VP, ENGINEERING

- **Atul Mahamuni**
  - SENIOR VP, PRODUCT

- **Brett McDowell**
  - EXEC DIRECTOR, GOVERNING COUNCIL

- **Ken Anderson**
  - CHIEF DEVELOPER ADVOCATE

- **Nigel Clark**
  - SENIOR VP, INDUSTRIES & PARTNERS
Network Growth
HEDERA’S PATH TO A FULLY DECENTRALIZED NETWORK
NETWORK GROWTH OVER TIME
PHASE 1: Up to 39 council members

- Avery Dennison
- IBM
- FIS
- Swirlds
- Google
- Wipro
- Boeing
- Deutsche Telekom
- Tata
- LG
- Zain
- DLA Piper
- NOMURA
- UCL
- Magalu
NETWORK GROWTH OVER TIME
PHASE 2: 100s of KYC'd permissioned nodes

NETWORK GROWTH OVER TIME
PHASE 2: 100s of KYC'd permissioned nodes

NETWORK GROWTH OVER TIME
PHASE 2: 100s of KYC'd permissioned nodes
NETWORK GROWTH OVER TIME
PHASE 3: 1000s of permissionless nodes
Roadmap
UPCOMING FEATURES & FUNCTIONALITY
Roadmap 2020 - 2021

2020
Q3
- OPEN SOURCE HEDERA NETWORK SERVICES
- HCS LATENCY IMPROVEMENTS

Q4
- ROSETTA API INTEGRATION
- ADDITIONAL NETWORK AUTOMATION: PHASE 1
- ADDITIONAL NETWORK AUTOMATION: PHASE 2

2021
- QUORUM PLUGIN
- STATE PROOFS FULL
- SCHEDULED TRANSACTIONS
- FULL MIRROR NODE
- ADDITIONAL NETWORK AUTOMATION: PHASE 3
- FULL MIRROR NODE
- DEVELOPER SDKS

- HEDERA NETWORK SERVICES
- STATE PROOFS ALPHA
- OPEN REVIEW HASHGRAPH
- HEDERA CONSENSUS SERVICE STABLECOIN DEMO
- HEDERA CONSENSUS SERVICE SCALING
- HARDWARE WALLET INTEGRATIONS
- EXCHANGE INTEGRATIONS
- PROOF-OF-ACTION MICROSERVICE V2
- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS
- HEDERA CONSENSUS SERVICE SCALING
- ROSETTA API INTEGRATION
- ADDITIONAL NETWORK AUTOMATION: PHASE 1
- ADDITIONAL NETWORK AUTOMATION: PHASE 2
- EXCHANGE INTEGRATIONS
- PROOF-OF-ACTION MICROSERVICE V2
- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS

- THIRD-PARTY WALLET & DIGITAL ASSET PLATFORM INTEGRATIONS
- HEDERA CONSENSUS SERVICE STABLECOIN DEMO
- HEDERA CONSENSUS SERVICE SCALING
- HARDWARE WALLET INTEGRATIONS
- EXCHANGE INTEGRATIONS
- PROOF-OF-ACTION MICROSERVICE V2
- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS

- OPEN REVIEW HASHGRAPH
- HEDERA CONSENSUS SERVICE STABLECOIN DEMO
- HEDERA CONSENSUS SERVICE SCALING
- HARDWARE WALLET INTEGRATIONS
- EXCHANGE INTEGRATIONS
- PROOF-OF-ACTION MICROSERVICE V2
- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS

- STATE PROOFS FULL
- SCHEDULED TRANSACTIONS
- FULL MIRROR NODE
- DEVELOPER SDKS

- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS
- HEDERA CONSENSUS SERVICE SCALING
- HARDWARE WALLET INTEGRATIONS
- EXCHANGE INTEGRATIONS
- PROOF-OF-ACTION MICROSERVICE V2
- HEDERA CONSENSUS SERVICE DEMO APPLICATIONS

- STATE PROOFS FULL
- SCHEDULED TRANSACTIONS
- FULL MIRROR NODE
- DEVELOPER SDKS
Part 2 - Foundations of the Hashgraph Consensus Algorithm
Virtual Voting

An algorithm that calculates (in a Byzantine resistant manner) the timestamp of transactions from 2/3 of the network or more
VOTING-BASED

Voting Based Consensus

ADVANTAGES
- Byzantine
- Immutable Audit
- DDoS Resilient
- Firewall / virus attack resilient
- Low computation (No PoW)
- High Availability

DISADVANTAGES
- Poor scalability (Impractical bandwidth requirements)
- Individual members can influence transaction access and order
- Low throughput

EXAMPLES
- None – not practical
Hashgraph Virtual Voting Consensus

ADVANTAGES

• Byzantine
• High Throughput (100,000s tps)
• Immutable Audit
• DDoS Resilient
• Firewall / virus attack resilient
• Fairness of transaction access and order
• Fair Timestamps
• Low computation (No PoW)
• High Availability
• Scalable

EXAMPLES

• Hedera Hashgraph
Gossip about Gossip

Talking about the history of how nodes have talked to each other
Gossip about gossip

Bob

Hank

Gina

Frank

Ellen

Alice

Carol

Dave

Gossip about Gossip

Alice Bob Carol Dave Ellen Frank Gina Hank
Gossip about gossip

Gossip about Gossip
Gossip about gossip

Gossip about Gossip

- Hank
- Alice
- Bob
- Gina
- Carol
- Frank
- Dave
- Ellen
- Bob
- Carol
- Dave
- Ellen
- Frank
- Gina
- Hank
GOSSIP ABOUT GOSSIP

Share events unknown to each other during gossip

Gossip about Gossip

- Alice learns through gossip about gossip
- Alice doesn’t yet know
- Alice already knows
Gossip about Gossip

The hashgraph gives each node the entire history of who has talked to who and when.

- Each node can put themselves in the place of any other node just by looking at their own hashgraph.
- Each node runs the same consensus algorithm, using the hashgraph as an input.
- Because all nodes use the same algorithm and inputs, the community reaches a consensus on order and timestamp.
- No need to send multiple ballots and receipts over the network as in historical voting models.

All nodes have the same picture of the hashgraph, except for the very latest events which will eventually sync.
Virtual Voting

Within the context of the hashgraph
**Rounds and witnesses**

- **Round**: Created when the supermajority of witnesses in the previous round can be strongly seen
- **Witness**: First event in a round for a given node
- **Red events are witnesses**
Virtual Voting

**Famous witnesses**

- Famous witnesses: means lots of people see it in the next round
- B2 is seen by A3 (through B3)
- B2 is also seen by C3 (via D3 and B3)
- Seen by A3 + B3 + C3 + D3 means it’s **famous** (unanimously so)
- This is repeated for all witness events
- But this “fame” is only the **opinion** of each event
Virtual Voting

Counting votes

- Strongly seen: To strongly see someone, you have to see them through a supermajority. That means more than two-thirds of the population (or stake as we will see later).

- Vote counting is performed by witness events.

- B4 can strongly see A3 via paths through A, B and D which is a supermajority.
VIRTUAL VOTING

Counting votes

- Strongly seen: To strongly see someone, you have to see them through a supermajority. That means more than two-thirds of the population (or stake as we will see later)

- B4 can also strongly see B3 through A, B and D
VIRTUAL VOTING

Counting votes

• Strongly seen: To strongly see someone, you have to see them through a supermajority. That means more than two-thirds of the population (or stake as we will see later)

• And C3 through A, B and D
Counting votes

• Strongly seen: To strongly see someone, you have to see them through a supermajority. That means more than two-thirds of the population (or stake as we will see later)

• And finally D3 through A, B, C and D

• We can therefore conclude that B2 is indeed famous after vote counting
VIRTUAL VOTING

Famous Witnesses

After a few rounds of voting, we’ve determined which events are famous (green) and which aren’t (blue)

If a decision cannot be made in a round, we try again in the following round

Every node performs this calculation **independently**, and they all come to the same result
Virtual Voting

Transaction ordering

- Any event may contain transactions to process, even non-witness events.
- Consensus timestamp of black event is median of earliest time other events could see the black one (median of D2, B2 and the black event).
- Events are thus put in order for transaction processing.
Proof of Stake with Proxying

“an algorithm that calculates (in a Byzantine resistant manner) the timestamp of transactions from 2/3 of the network or more”

What defines “the network”? 
Hint: It’s not node(s)
Proxy Staking with Proxying

• No Leader or Delegate Election
• Number of nodes is irrelevant... stake held by nodes is
• No deposits / locking / slashing / bonding
• Any account can proxy its tokens to another account / node (and continue spending / earning tokens)
• Voting weight = (node’s own stake + proxied stake) ÷ total hbar
• Every node participates in consensus
• Protects network against Sybil attacks
Hashgraph is a consensus algorithm

- Architectured from ground up to be fast, fair, and secure
- Achieves gold standard of security without performance trade-offs
- Gossip about gossip with virtual voting to quickly achieve consensus with 100% certainty
- Efficient in bandwidth and computation (no PoW)
- Leaderless
Part 3 - Users / Projects That Are Building on Hedera
Hedera Today
APPLICATIONS, DEVELOPERS, & NETWORK ACTIVITY
8,000+ DEVELOPERS
Attending global hackathons, meetups, and active in Discord.

35+ APPLICATIONS
In production on Hedera mainnet, since open access on Sept. 2019

~1,000,000 MILLION TXS/DAY
Surpassing the daily transaction volume of Ethereum.
INDUSTRY & USE CASE
ADVERTISING | REAL-TIME FRAUD DETECTION

Real-time auditing at scale to eliminate advertising fraud and remove costly intermediaries.

“Hedera has proven it has the scale, speed and reliability to handle all of the live advert tracking data and programmatic event data that we have been handling in recent campaigns.”

IAN MULLINS | FOUNDER & CEO

QUICK FACTS

MITIGATE AD FRAUD by providing a full, auditable trail of events, programmatical verified by a 3rd party to create trust between brands and media buyers.

LOW COST FOR CONSENSUS on transactions ($0.0001) means AdsDax can create a viable and scalable business model for the advertising industry.

HIGH TRANSACTION THROUGHPUT with fast finality handles millions of daily advertising events.

CHRONOLOGICAL ORDERING OF TRANSACTIONS with timestamps enables analytical insight & transparency for both fraud detection and remittance.

MORE INFORMATION
HEDERA.COM/USERS/ADSDAX
**CHALLENGE**

Coupon and associated promotional data is fragmented, non-standardized, and rife with fraud. Without the necessary controls, transparency or trust, the industry usage of this promotional vehicle has decreased in recent years.

**SOLUTION**

The Coupon Bureau can bring its standardization and added efficiencies to the marketplace with transparency and trust. By allowing 3rd party validation and audit capabilities among authorized stakeholders, the industry will be able to have confidence in this centralized, agnostic solution.

"Only Hedera Hashgraph was able to provide the real-time, tamper-proof logging capabilities that we needed to bring transparency, trust, agnosticism and industry oversight to a platform that connects all coupon industry stakeholders"

**BRANDI JOHNSON | CEO**
“Public ledgers provide a good option for regulators, allowing them to achieve the compliance and transparency they need in a secure, high-performance network designed for collaboration.”

JIM NASR | VP, TECHNOLOGY & INNOVATION

**Quick Facts**

**Reduce the Frequency of Drug Shortages** and offer better predictability, with an end-to-end transparent trail of events across all supply chain parties.

**High Transaction Throughput & Finality** in seconds makes it easy to handle changes in supply chain velocity.

**Fair (Chronological) Ordering** of transactions and timestamps enables tracking, tracing, and auditing, with precision.

**Live Health Application** for tracking the deadly coronavirus in real-time with Hedera Hashgraph’s public distributed ledger.

**More Information**

HEDERA.COM/USERS/ACOER
Deepak Chopra Leverages Blockchain To Fight Covid-19 Mental Health Crisis

Today, Deepak Chopra, mental health advocate, is launching a fast, secure, and cost-effective solution for buying and selling high value assets using blockchain technology and the Hedera Hashgraph.
Part 4 -
How To Get Started Building Your Own Applications on Hedera

@hashgraph
Part 5 - Q&A

Additional Resources -

Sign up for a test account - portal.hedera.com
Getting started guides - hedera.com/get-started
Discord chat - hedera.com/discord
Tutorials - youtube.com/channel/UCIhE4NYpaX9E9SssFnwrjww
Twitter - @hashgraph
Email - cooper@hedera.com

@hashgraph