Hedera™ Hashgraph

HALA SYSTEMS

Seeking Justice with Tamper-Proof Evidence on Hedera Hashgraph

HEDERA HASHGRAPH, LLC

TABLE OF CONTENTS

01. REDEFINING TRUTH IN A DIGITAL AGE **3**

02. TAMPER-PROOF EVIDENCE **4**

Remove Centralized Control 4

Verifiable Provenance 4

03. EXPLORING PUBLIC LEDGERS **5**

04. CONTENT AUTHENTICITY WITH HEDERA **6**

Architecture 6

Hedera Consensus Service 6

05. APPLYING THIS ARCHITECTURE **7**

01.

REDEFINING TRUTH IN A DIGITAL AGE

When the world first came online we were able to trust a photograph or video with our own eyes. Fast forward a few decades and we're rapidly entering into a new era defined by fake news and deep fakes. The ability to readily manipulate content forces us to rethink the notion of truth. Of data as evidence.

Thankfully, new technologies like blockchain and distributed ledgers have since emerged to evolve our ability to trust data. Rooted in innovations in computer science, these decentralized networks provide us with an opportunity to remove potential points of manipulation to better ensure the authenticity of content.

While it can be reasonably thought that not all images or videos require this level of trust, some clearly do. Consider a humanitarian crisis. When a video recording the time or location of an event can alter an opportunity for justice, we must reconsider our working model and the tools available to us.

Hala Systems was founded on a belief that technology can work to better protect and support civilians. Sentry is Hala's early warning system that generates credible, real-time, situational awareness of threats in the toughest places on earth. Sentry uses artificial intelligence (AI) to instantaneously validate information from multiple sources, allowing stakeholders to detect, identify, and predict threats.

With 3.8 billion smartphones worldwide, each with a camera, Hala Systems can use Sentry to empower civilians to place undeniable truth in their own hands. For that to be possible, each image and video capture must be armed with immutable, tamper-proof data.

2M+

PEOPLE WARNED

140

WARNINGS DAILY

250K

REDUCTION IN PEOPLE FACING TRAUMA

02.

TAMPER-PROOF EVIDENCE

At scale, Hala Systems can register millions of events per day consisting of video, photo, and audio files. With each click, metadata is emitted that provides powerful context including the originating device, the time it was captured, location, and more. Traditionally, this data would be stored in a centralized database increasing the opportunity for its manipulation, loss, or worse, putting the originator in harm's way.

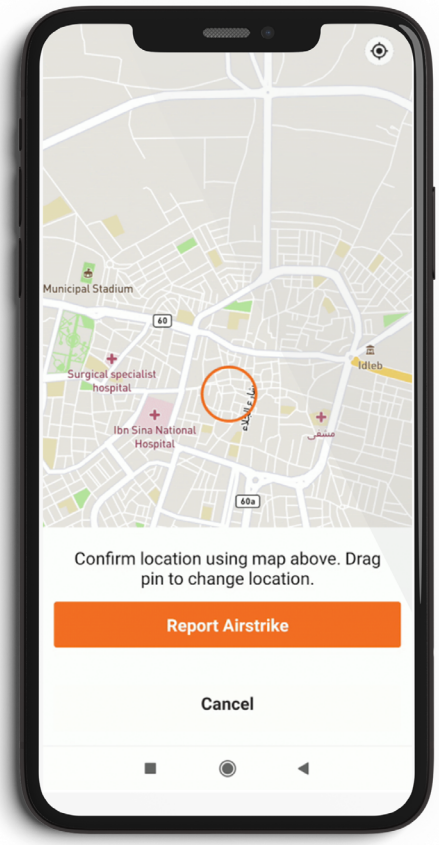
When it comes to important events, like the very ones Sentry is monitoring, the team wanted to ensure this data was trusted between the civilians first capturing the image to its potential use in a court of law.

To enhance the trust and integrity of their data, Hala looked beyond a traditional centralized database to meet a new set of requirements and establish a set of tamper-proof records using a public ledger.

Remove Centralized Control

Storing data in a centralized database requires a certain level of trust – trust that the database is secured properly and that the data itself won't be tampered with or deleted after being written.

For Hala Systems they wanted a solution that would act as an impartial observer, not controlled by them or a single entity, but distributed and decentralized across many neutral parties. This decentralized nature, coupled with its immutable property provides assurances by multiple independent parties for who sent the data, when it was recorded, and what it was detailing.



Verifiable provenance

Hala Systems' devices provide valuable information alongside each input and capture, supporting over 30 data points to provide key evidence of the location and time an image was taken. With each transaction sent, the data needed to have a high enough level of data integrity and traceability to be held up as evidence in a court of law.

This decentralized and immutable nature of a distributed ledger provides assurances to who sent the data, when.

03.

EXPLORING DISTRIBUTED LEDGERS

Blockchain and distributed ledgers use decentralized infrastructure to enable a greater level of trust by having each transaction be recorded by multiple independent parties. Initially, Hala explored the smart contract platform, Ethereum. Ethereum achieves probabilistic consensus - the act of the connected set of computers reaching agreement on a transaction's validity - through a common mechanism called proof of work. Hala quickly realized that Ethereum's smart contracts with highly variable fees and slow confirmations times weren't the right fit for their use case.

In search of a more scalable alternative, both technically and financially, the team found Hedera. The Hedera network uses a faster, more secure alternative to blockchain, called hashgraph. The hashgraph consensus algorithm and data structure allows for the public ledger to operate more efficiently, with higher throughput and drastically lower costs.

	BITCOIN BTC	ETHEREUM ETH	HEDERA HBAR
TRANSACTIONS PER SECOND	3+ TPS	12+ TPS	10,000+ TPS
AVERAGE FEE	$2.99 USD	$2.89 USD	$0.0001 USD
TRANSACTIONS CONFIRMATION	10-60 MINUTES	10-20 SECONDS	3-5 SECONDS (w/finality)

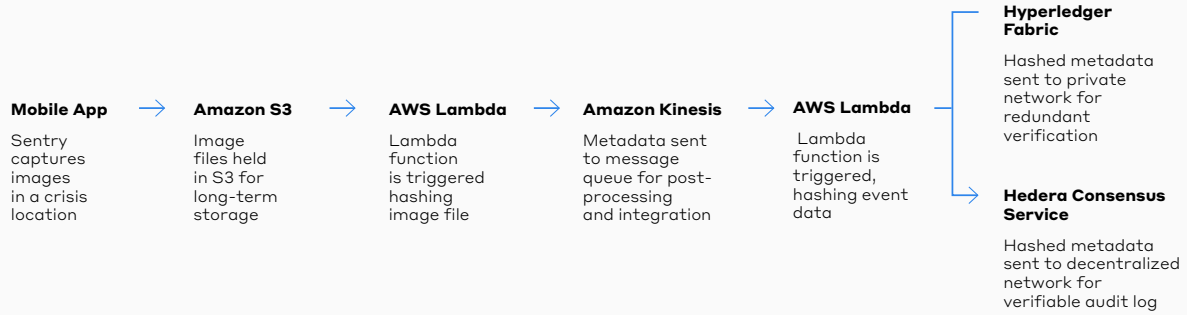
04.

CONTENT AUTHENTICITY WITH HEDERA

Hala Systems uses Hedera to manage the metadata of user inputted and created media produced in conflict zones. This provides external parties wanting to verify the information with credible details surrounding the who, what, where, and when of an event.

Architecture

Each event logged to Hedera Consensus Service is signed by the issuing device's keys and receives a consensus timestamp by the whole of the Hedera network. This ensures that the data is better able to be trusted by supporting third parties and, if needed, the broader public due to its immutable and tamper-proof properties.



When an image is captured in the field using the Hala Systems App, the image is added to a centralized file storage in Amazon Web Services (AWS). For Hala to enhance the trustworthiness of the image, it takes a hash of the image using an AWS Lambda function, the output of which is sent to a Kinesis message queue. This hash flows through Kinesis using another Lambda function and is simultaneously written to a private blockchain using the IBM Blockchain Platform, and Hedera Consensus Service. Hala Systems uses the IBM Blockchain Platform to act as their internal repository, preserving additional metadata to augment the auditable hash data sent to Hedera Consensus Service. With these two sets of records any 3rd party can verify the information on the public ledger to match the image and, if necessary, its accompanying data stored on the private ledger.

Hedera Consensus Service

Hedera Consensus Service is a scalable event log, well suited for sending small amounts of data, like an image's metadata, to the decentralized Hedera network.

Each transaction sent to Hedera benefits from tamper-proof provenance and traceability to achieve extremely high levels of data integrity. By logging a hash of the image file to Hedera, Hala and its auditors are able to verify that the image—and its associated metadata—was unaltered.

Hedera™ Hashgraph

HASHGRAPH

Every Hedera network service relies on the hashgraph consensus algorithm for achieving distributed consensus. Hashgraph introduced two Innovative concepts to achieve what may be the most efficient form of consensus mathematically possible – gossip about gossip and virtual voting. Not only is hashgraph efficient, but also highly secure; having proven to be asynchronous Byzantine fault tolerance to have greater resiliency in more situations than alternative consensus algorithms.

LEARN MORE ABOUT HASHGRAPH

05.

APPLYING THIS ARCHITECTURE

Fraudulent content is a growing global concern. While best served for content that requires high-levels of trust, like security footage, this paradigm is likely to continue through to many other industries now that it can be cost effectively applied.

SOCIAL MEDIA

The provenance of a post can better determine its intentions. To better educate their users on the history of a post, and its virality, social media sites can share trusted, transparent data of its origination.

DEVICE MANUFACTURING

Cameras can create a competitive advantage by leveraging a tamper-proof log of its output. With it, surveillance, news providers, and more will be able to provide a more informed and trusted source for the content.

DIGITAL CONTENT

Media creation apps are able to give their users the ability to denote original and unique work. Able to build upon this to establish usage rights and more.

Hedera is a decentralized public network on which developers can build secure, fair applications with near real-time finality. The platform is owned and governed by a council of the world's leading organizations including Avery Dennison, Boeing, Deutsche Telekom, DLA Piper, FIS (WorldPay), Google, IBM, LG Electronics, Magalu, Nomura, Swirlds, Tata Communications, University College London (UCL), Wipro, and Zain Group. To undertand how distributed ledger solutions can be applied within your industry learn more at hedera.com.