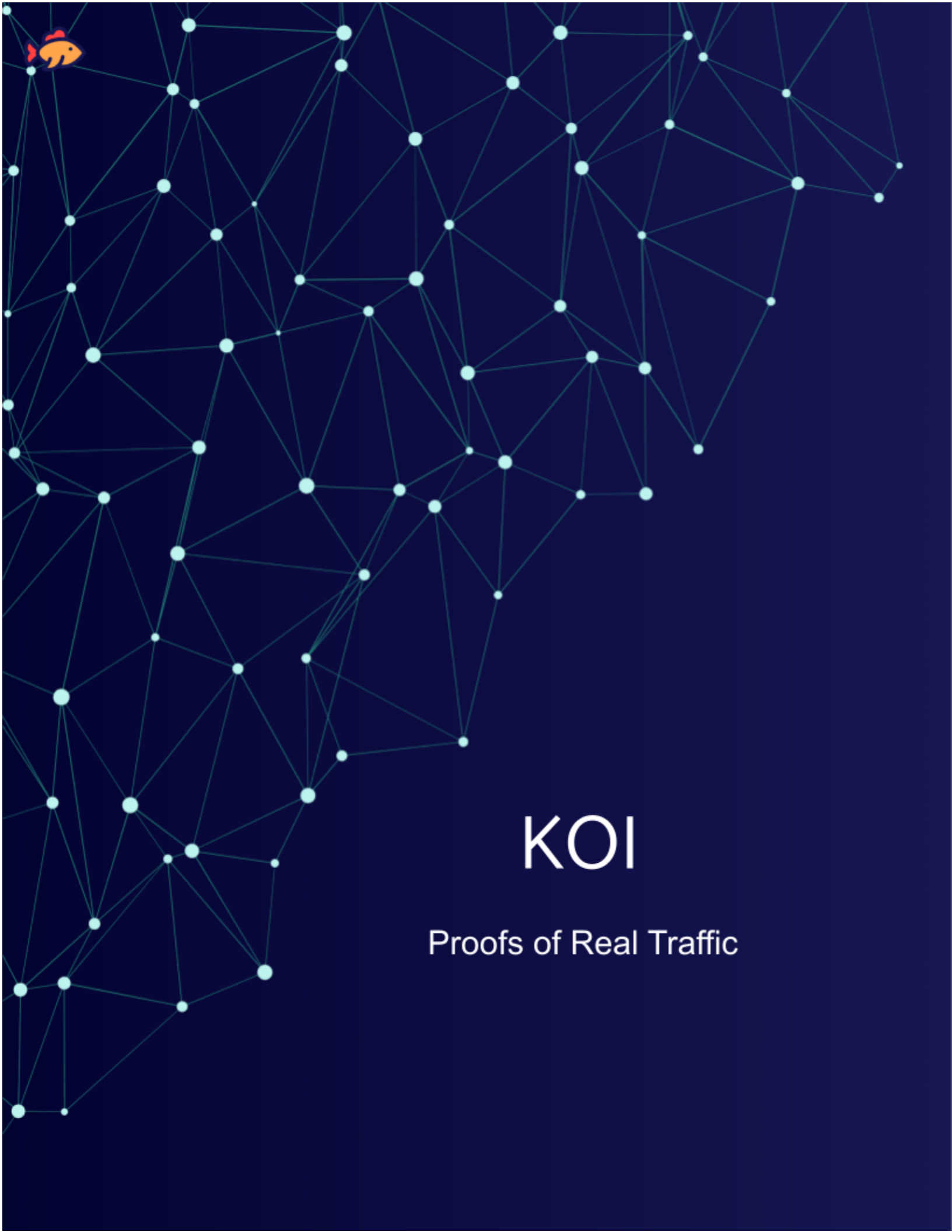


KOI

Proofs of Real Traffic

Verifiable Proof of Attention

The Koi Network has developed an innovative approach for traffic monitoring and reporting.

Motivation

Public data incentivization has been attempted by dozens of projects over the past ~5 years since the creation of Ethereum. Unfortunately, they all had one thing in common: they were unable to track traffic in a reliable or consistent manner. Permanent archival storage now presents a solution to this issue, by ensuring that traffic proofs can be stored as a means of consensus and a historical representation of the value of particular knowledge over time.

Goals

In conceiving of the best way to verify attention and traffic, we identified three key issues:

1. Spam and non-human agent filters are needed to remove illegitimate traffic from the rewards model.

2. Conspiracy between Gateway owners and content creators can falsify traffic logs and monopolize rewards.

3. Deliberate falsified traffic by content creators can receive rewards unfairly (i.e., a sybil attack)

Solution

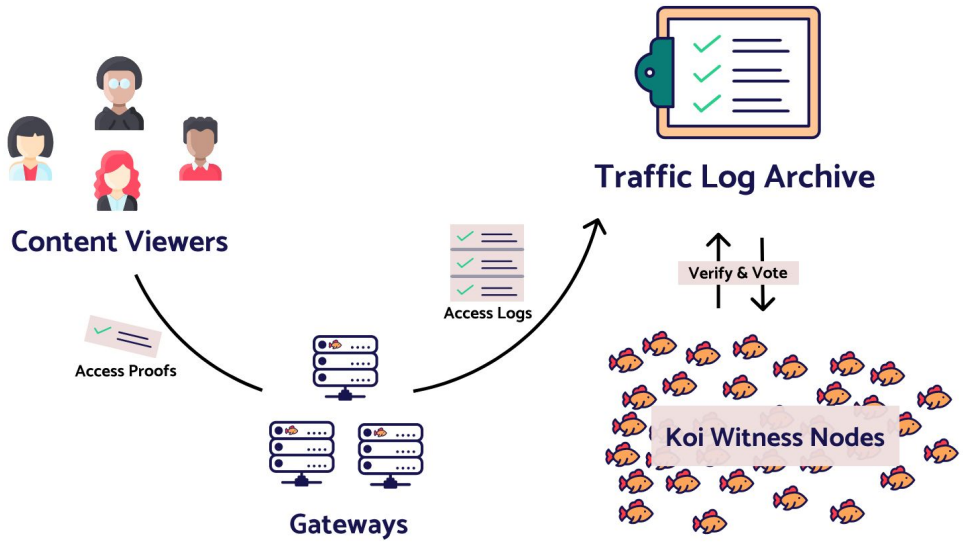
In order to make the network as reliable as possible, gateways can opt to provide additional security and verifiable logs to receive priority and a greater share of daily KOI rewards. The end-users who view this content can then opt into tracking themselves as **'bellwether' nodes,** and submit verifiable proof of access as they browse. These proofs are submitted as headers on standard HTTP requests, allowing them to be compatible with a range of existing technologies, just by installing the Koi Middleware.

investors@openkoi.com

Koi Labs Inc.

Proofs of Real Traffic (PoRT)

In order to fully avoid any risk of traffic falsification, Gateways can optionally implement a Proof-of-Real-Traffic header on all content requests. The header is submitted by Content Viewers as a standard HTTP call header when the browser requests certain content, and includes a low-difficulty hash of the requester's IP address, the resource URL, and other metadata.



Traffic Gateways can register to Koi to begin collecting access proofs from viewers, who submit them in exchange for network status.

Initially, the difficulty of this hash can be optimized to improve the reliability of the system, but as time progresses, the reliability (and reputation) of the individual 'bellwether' nodes will be sufficient that they do not need to submit proof hashes at all, and can simply sign their traffic requests. These signatures are equally difficult to falsify, and can eventually replace the proof of work model altogether.

Verification & Accountability

During the Koi attention rewards process, Koi Nodes fetch traffic logs from the Gateways and verify the hashes match the given metadata. Since hash verification is trivially simple compared to generation, this provides an efficient means of resolving any doubt about the authenticity of the traffic log data and ensures that Koi can reliably and fairly reward content creators.