CHAINMAIL

ZKP Email Marketplace / Whistleblower Platform

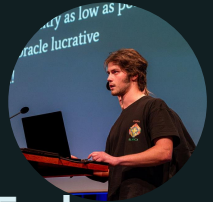
Goal

Enable confidential distribution of authenticated sensitive information

Team

Charlie

Jack



Fedor

ABSTRACT

Idea

We wanted to create a solution that enables trust-minimised transaction of provably verified emails.

By utilising DKIM signature verification & ZKPs, Chainmail enables the owners of sensitive emails to publicly prove the sender, redact their own details and list the data for sale.

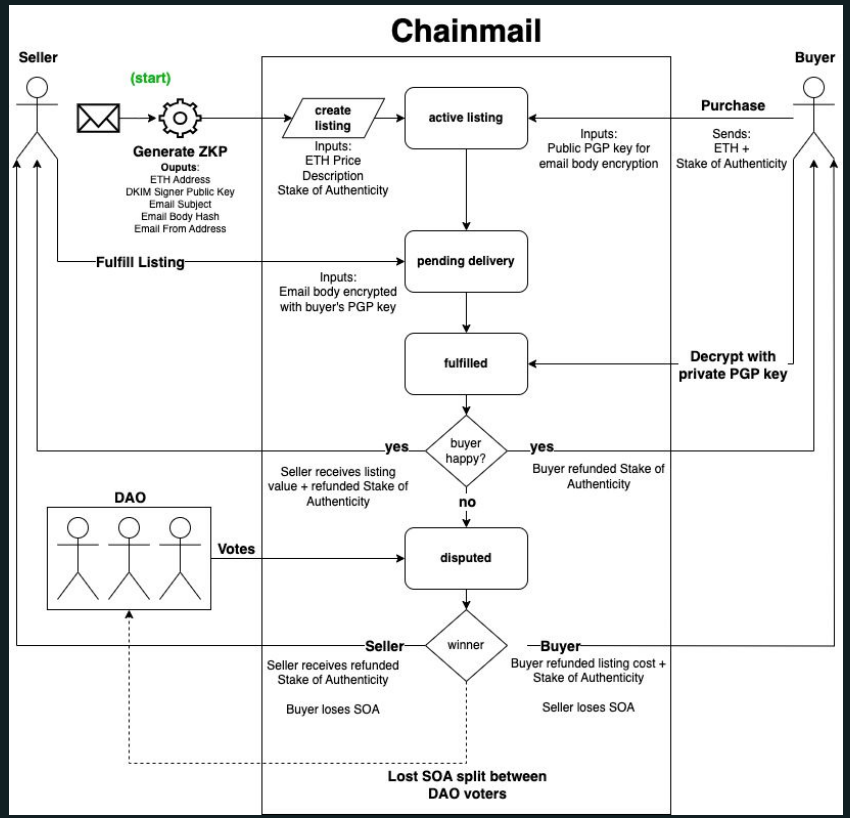
PROJECT

Flow

Interactions between buyer & seller are facilitated by smart-contract

Stake of Authenticity provides financial incentive to be honest

A DAO provides incentivised mediation



USE CASES

Anyone wishing to prove receipt of an email without disclosing their identity

Whistleblowing

Sellers: Persons in possession of information that may be of public interest but wish to retain anonymity

Buyers: Journalists, activist groups

Legal Disputes

Sellers: Law firms releasing information as public evidence whilst preserving privacy of involved parties

Buyers: Mediators, lawyers

DILEMMAS

Potential challenges

National Security

The service could be used by entities to distribute confidential security information between individuals or nations

Blackmail

Nefarious actors could market emails containing personally sensitive/private information

Dangerous Data

Emails containing information that could lead to direct harm from buyers with malicious intent

So what are we to do?

SOLUTIONS

Decentralising governance

Censorship 

Dangerous emails will need to be censored on the frontend. Decision making on the definition of dangerous will be delegated to a DAO

Curated Buyer List

To ensure the platform is used for its intended purpose, the DAO can curate the list of authorised buyers to transact on the platform

Thank you

:)