



**UNIVERSITÀ
DEGLI STUDI
DI UDINE**
HIC SUNT FUTURA

THE ADOPTION OF DLT AGAINST DISINFORMATION: SHOWCASING THE TRUTHSTER PROOF OF CONCEPT

Authors: M. Hascoşkan, M. Paier, F. Costantini, F. Crisci, M. Miculan

University of Udine, Italy

DLT2026 – 8th Distributed Ledger Technology Workshop

THE PROBLEM

- Disinformation erodes public trust and democratic discourse.
- Deepfakes make content almost impossible to verify.
- No reliable way to **verify, trace, and certify** multimedia content.

EXISTING SOLUTIONS & THE GAP

Existing DLT-for-journalism tools:

WordProof, ANSA check, News Provenance Project, Civil, Paragraph...

Limitations:

- Often specific to a single use-case
- Build brand trust, not creator empowerment
- They verify it after it is published
- Technology, law and news-production handled separately
- Compatible standards: C2PA, ISCC

OUR FOCUS: INTERVIEW-BASED JOURNALISM

We narrow the problem to **interview-based journalism**

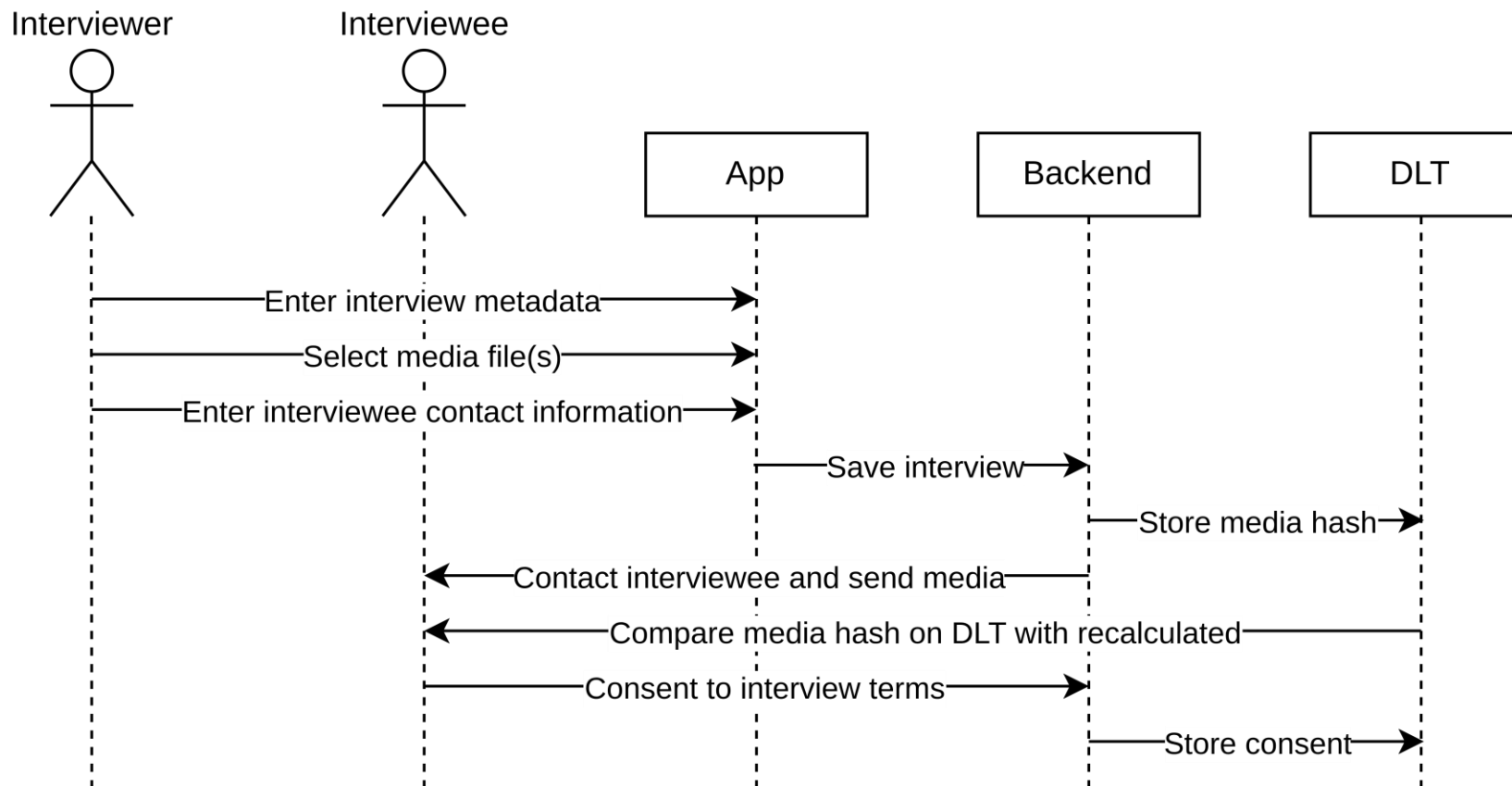
Why interviews?

- Identifiable individuals
- Conditions of production can be recorded
- Consent can be captured at the moment of creation
- Authenticity, authorship, consent, privacy & rights become tightly linked
- Scope: we certify **provenance & consent**, not factual truth

THE IDEA:

**create a way to enable journalists to easily
certify media content on the fly, while
respecting relevant regulations**

SEQUENCE DIAGRAM



TWO CERTIFICATION FLOWS

STRUCTURED FLOW

Guided, for structured interviews:

- upload media file
- enter metadata
- identify interviewee
- wait for consent expression
- certify

FAST FLOW

For time-critical scenarios:

- record
- review
- [attach consent]
- certify

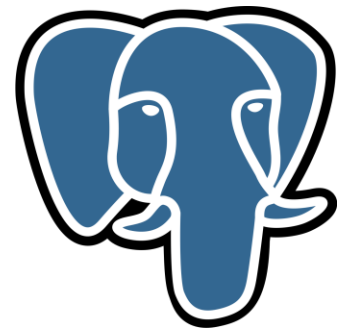
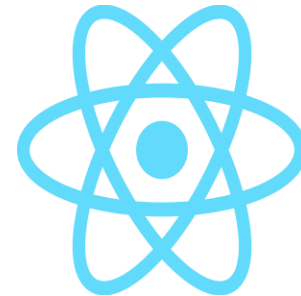
IMPLEMENTATION

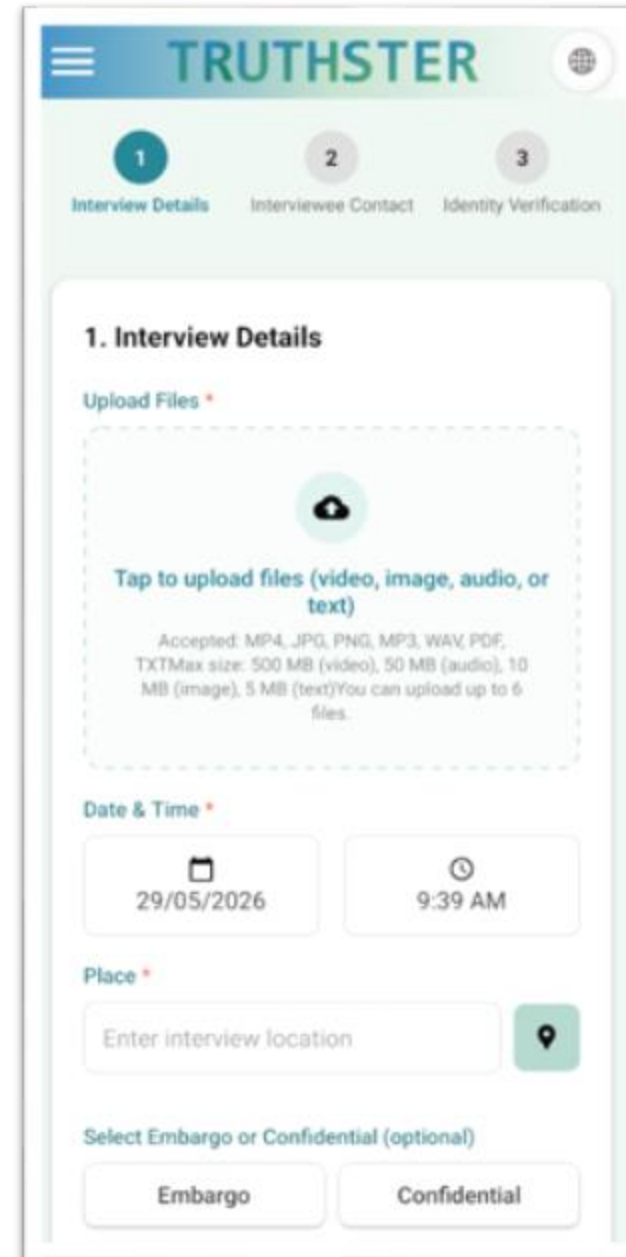
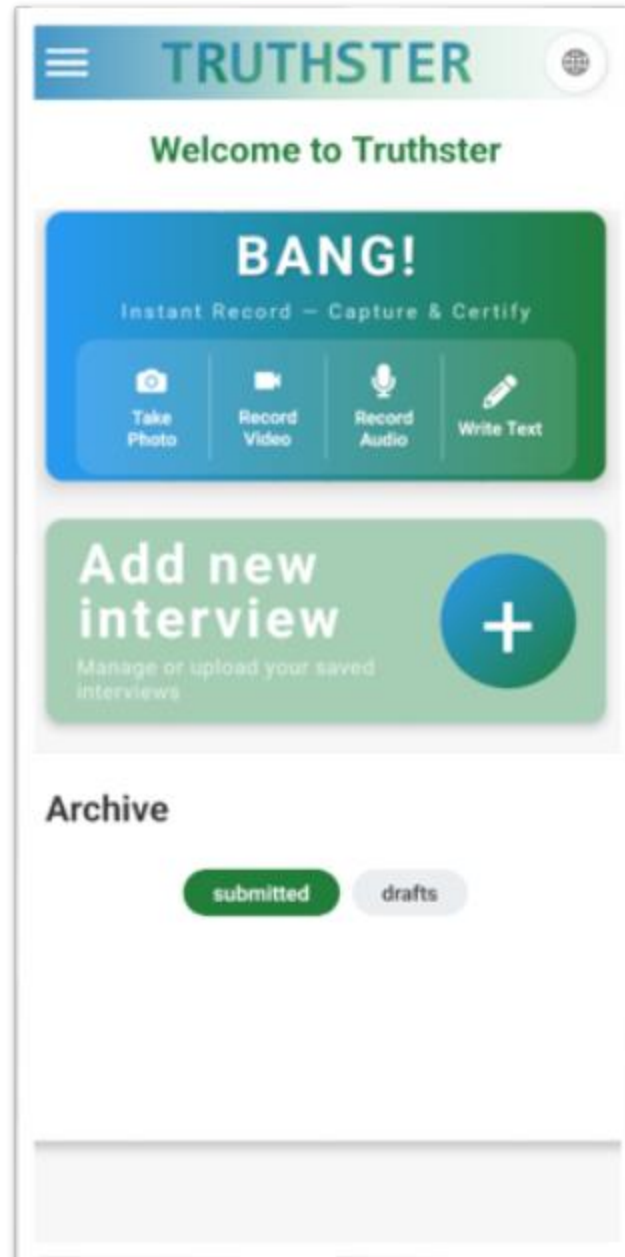
Frontend: React Native + Expo (web + mobile)

Backend: Go

Ledger: Ethereum (*for the PoC*)

Database: PostgreSQL





ON-CHAIN / OFF-CHAIN SPLIT

On-chain (Ethereum):

Only **cryptographic hashes** of media, consent, and metadata

Off-chain (PostgreSQL):

mutable data — user credentials, access logs, configs

Why? → privacy + scalability + tamper-evidence

Any change to original data → mismatch with the hash → tampering detected

CONSENT & RIGHTS / SMART CONTRACTS

- Consent captured at creation, verifiable, linked to the media
- Smart contracts represent consent conditions & usage rights
- Interviewee can delegate recording to the backend — **no personal wallet needed**
- Proofs verifiable by the interviewee before consent is recorded

DATA ERASURE

- The problem: blockchain never changes, but GDPR allows deletion
- No personal data on-chain — only **salted hashes**
- Personal data stays **off-chain** (database)
- To delete: remove off-chain data + **discard the salt**
- Without the salt → the hash means nothing → data is "forgotten"
- Result: immutability **and** the right to be forgotten

CONCLUSION

- Truthster integrates authenticity, provenance, consent & rights into the creation workflow
- Dual-flow design + DLT-backed certification
- Blockchain as decentralized trust anchor; privacy & scalability preserved
- Next step: empirical validation

LIMITATIONS & FUTURE WORK

This is a **proof of concept** — evaluation is the next step

Future work:

- Performance evaluation (latency, transaction cost, scalability)
- Usability study with real journalists
- Comparison with permissioned DLTs / Layer-2 solutions

THANK YOU / QUESTIONS

Thank you! Any question?

Contact:

- miray.hascoskan@uniud.it
- matteo.paier@uniud.it