

FIRSTBLOCK-ATHON — PARTNER PROBLEM STATEMENTS

FIRSTBLOCK-ATHON · PARTNER PROBLEM STATEMENTS · 07 — 08 SEPT 2026 · Netlight, Regeringsgatan 25, 111 53 Stockholm

1. UNICEF

BACKGROUND

UNICEF delivers programmes that support the world's most vulnerable children and families. To strengthen transparency and accountability, we want to capture credible proof of impact directly from the field.

Examples include:

- Toilets constructed in communities
- Solar panels installed in schools
- Teacher training delivered in schools
- Vaccination drives conducted in villages
- Nutrition interventions for children and mothers in rural communities

THE CHALLENGE

UNICEF needs citizen-submitted proof that programme activities have taken place and are creating impact.

This proof could include photos, videos, GPS location, timestamps, survey attestations, or other field evidence. Submissions should come from people in the communities where the impact occurs.

Assume: there is a portal where micro tasks for proof collection are published.

TECHNICAL ASPECTS

01. No PII risk

Using zero-knowledge proofs or other privacy-preserving technologies, verify key attributes such as age and nationality of the citizen without exposing ANY personal data.

02. Proofs with integrity

Each proof should be timestamped and possibly GPS-stamped in a tamper-resistant way, with as little room as possible for third parties — or the reporters — to alter data before submission.

Think tamper-proof apps, hardware encryption, decentralised storage with hashes on-chain.

03. More eyes the better

Each proof can be attested on-chain by several people. Think Ethereum Attestation Service or similar.

04. Internet availability

Many target communities have limited or unreliable connectivity. Support offline submission: capture proof with no internet, submit automatically once the citizen reaches coverage.

05. Accessibility

Assume basic digital literacy — able to use WhatsApp or Facebook on a smartphone, nothing

advanced. UX and onboarding must abstract away Web3: think embedded wallets, paymasters for gasless transactions, LLM interfaces.

06. Open-source bias

Use the least proprietary software possible. You may start on proprietary stacks for speed, but be clear on which open-source alternatives can be used at scale.

BUSINESS CASE

UNICEF already runs U-Report, a Web2 platform built on RapidPro, to engage young people globally through surveys and polls. Both U-Report and RapidPro are open source.

The opportunity: extend this engagement model by building a module for U-Report that allows youth and community members to submit verified impact proofs and real-world event reports, while anchoring those proofs on-chain in a privacy-preserving manner.

EXPLORE SOLUTIONS

- Extend U-Report with a module for verified impact proofs and real-world event reports.
- Anchor those proofs on-chain in a privacy-preserving manner.
- Engage youth and community members already active on the platform.
- Plan for eventual integration with U-Report or RapidPro.

2. SWEDISH RED CROSS

Verifiable Information & AI — Protect trusted records and enable people to verify authentic humanitarian communications in an age of misinformation and AI-generated content.

PROBLEM STATEMENT

The Swedish Red Cross has over 18,000 volunteers in Sweden who currently rely on WhatsApp and traditional messaging platforms for communication, creating security and privacy concerns.

CHALLENGE

How can we build a secure peer-to-peer messaging platform on-chain that enables trusted communication for volunteers?

EXPLORE SOLUTIONS

- End-to-end encrypted messaging
- Blockchain identity and authentication
- Decentralised communication infrastructure
- Secure volunteer coordination
- Privacy-preserving messaging

3. SWEDISH RED CROSS

Continuity Across Borders — Enable displaced people to maintain access to humanitarian services as they move between countries and organisations.

PROBLEM STATEMENT

People moving across borders due to war, natural disasters or climate emergencies lose access to essential services. There is currently no shared system that enables continuity of services between different humanitarian organisations, or even across the Red Cross network internationally.

CHALLENGE

How can people moving across borders due to war, natural disasters or climate emergencies maintain continuity of essential services such as healthcare, medication, financial assistance and humanitarian support? Explore whether blockchain could provide a secure way for an individual's access to support to continue as they move from one location or country to another.

EXPLORE SOLUTIONS

- Portable, privacy-preserving digital identity for displaced people
- Verifiable credentials for service eligibility across organisations
- On-chain attestations of received support, without exposing PII
- Interoperability between humanitarian organisations and borders
- Offline-first access with sync once connectivity returns

4. SWEDISH RED CROSS

Secure Crisis Communication — Misinformation, Trusted Information & Verifiable AI.

PROBLEM STATEMENT

Create a secure, scalable communication infrastructure for humanitarian volunteers and crisis response. In an era of misinformation and AI-generated content, trusted humanitarian information must be protected and verifiable.

CHALLENGE

How can the Swedish Red Cross protect trusted information in an era of misinformation and AI-generated content?

TWO CONNECTED NEEDS

Preserving historical archives and information as an accessible record of truth, and creating verifiable communications so people can determine whether information claiming to come from the Swedish Red Cross is authentic and trustworthy.

EXPLORE SOLUTIONS

- Immutable archiving of historical records as an accessible source of truth
- Verifiable, cryptographically signed official communications
- On-chain provenance for published humanitarian information
- Authenticity checks anyone can run against tamper-proof records
- Secure, scalable crisis communication infrastructure for volunteers

5. HUNDSTALLET

PROBLEM STATEMENT

Hundstallet wants to engage younger generations in charitable giving through a more transparent and interactive donation experience.

CHALLENGE

How can we create a more engaging and transparent donation platform?

EXPLORE SOLUTIONS

- Blockchain-powered donation tracking
- Transparent use of funds
- Gamified donor engagement
- Digital rewards and community participation
- Impact dashboards

6. AIMS MANAGEMENT

PROBLEM STATEMENT

AI-generated content is rapidly increasing, making it more difficult for influencers and content creators to protect their identity and prove content authenticity.

CHALLENGE

How can Blockchain help secure creator identity and prevent deepfakes?

EXPLORE SOLUTIONS

- Blockchain identity verification
- Content authenticity certificates
- Deepfake detection
- Digital ownership verification
- Creator provenance

7. AI INSTITUTET

PROBLEM STATEMENT

As AI becomes more powerful, protecting and preserving the “Digital DNA” of human knowledge, inventions, and historical records has never been more important. Traditional databases are mutable, creating the risk that AI will rewrite digital history, alter original truths, and infringe on patent blueprints and intellectual property.

CHALLENGE

Design a Sovereign History Vault that protects digital truth and prevents AI from rewriting digital history. Your solution should build on the Three Alexandria Protocols as the foundation of the architecture.

WHY IT MATTERS

The Alexandria Protocols provide a framework for preserving digital truth through immutable, verifiable records secured by blockchain and advanced cryptography.

THREE ALEXANDRIA PROTOCOLS

01. DNA hashing

Generate a cryptographic fingerprint to preserve the integrity and authenticity of digital assets.

02. Immutable ledger

Register and verify digital records on an immutable blockchain ledger to ensure they remain tamper-proof and permanently traceable.

03. Post-quantum cryptography (PQC)

Secure digital assets against future quantum computing threats using next-generation cryptographic methods.

EXPLORE SOLUTIONS

- Build a Sovereign History Vault to capture and permanently preserve digital assets.
- Protect patents, research, literature, creative works, inventions, and historical records from manipulation.
- Prevent AI from rewriting or altering original source material.
- Verify AI-generated summaries, references, and knowledge against permanent, immutable records.
- Create a Sovereign Patent Proof Vault for intellectual property protection.
- Hash the Digital DNA of important events, inventions, and documents.
- Register digital assets on an Immutable Ledger.
- Secure records using Post-Quantum Cryptography (PQC).
- Develop solutions that preserve the integrity of human knowledge for future generations.

8. WORLD FOOD PROGRAMME-WFP

PROBLEM STATEMENT

Humanitarian operations face the challenge of data fragmentation: agencies operate in silos, with often re-registration workflows for beneficiaries. While "register once" is the goal, traditional centralised registries create systemic risk and violate agency sovereignty.

CHALLENGE

The Humanitarian Federated Biometric Deduplication: build a functional prototype of a Federated Deduplication Middleware that identifies potential duplicate registrations using cryptographic photo-summarisation.

THE PROBLEM STATEMENT

Each agency maintains their own policies, system and processes for registration. To maximise overall efficiency, it is important that they compare their data without exposing their privacy information. This challenge is even more difficult in regions when there is no reliable biographic data, and agencies need to use biometric recognition.

The system must facilitate interoperability across agency boundaries without ever sharing raw PII, without creating a centralised master beneficiary registry, and with a neutral (i.e., not owned by a specific agency) decentralised infrastructure.

TECHNICAL INFRASTRUCTURE PARAMETERS & CONSTRAINTS

Your architecture must strictly honour these humanitarian-grade structural boundaries:

01. The Summarisation Runway

You must utilise privacy-preserving primitives (e.g., utilising frameworks like Rarimo) to generate a non-reversible cryptographic summary of user photos. The summary must be mathematically unique enough to support comparison, yet strictly non-reversible.

02. The Federated Deduplication Middleware

Your architecture must mimic a distributed trust model. The middleware should serve as an analytical matching engine that identifies potential duplicates. It is structurally forbidden from hosting master beneficiary records or PII in the middleware layer.

03. The Result

The system output must be a structured deduplication report. Do not promote automatic deletion or modification of records.

WHAT TO DELIVER FOR THURSDAY'S JUDGING

The Live Middleware Demo: A functional, closed-loop prototype. It must simulate agencies and their subset of photos from people, generate photo-summaries, receive photo-summaries from two or more simulated agency endpoints, perform a deduplication sweep, and generate a deduplication result in a neutral decentralised infrastructure. Simulate at least 1000 user photos with around 10% of duplication.

Bonus point: Incorporate probabilistic confidence thresholds into the deduplication logic. For matches identified with lower confidence scores, demonstrate how additional mechanisms (e.g.,

multi-layered summarisation, secondary biographic validation) can be used to improve the result.