zKML

GeneratedArt

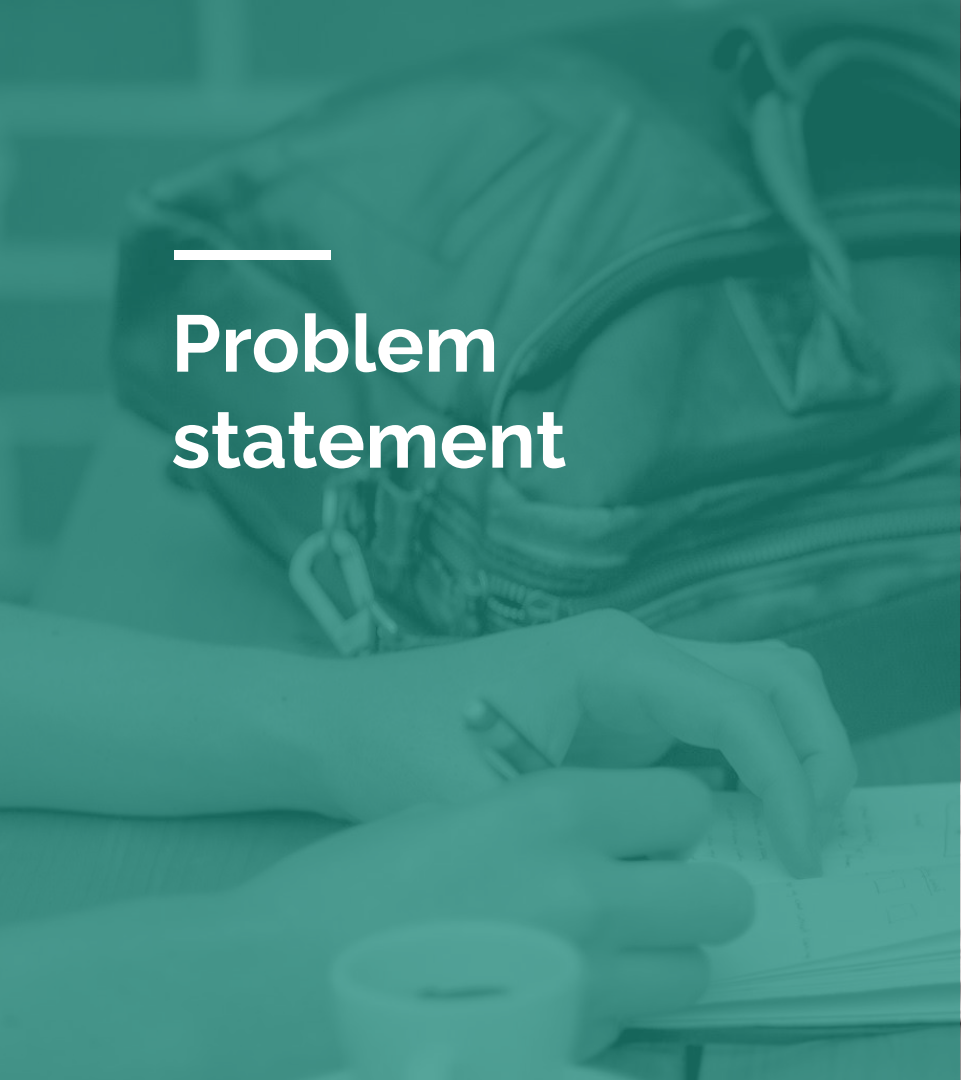
GenerativeFinance
GeFi.io

Privacy-Preserving Machine Learning
with Zero-Know

Team

Vladimir Komendantskiy
Guillaume Lauzier

Outline



Problem statement

Data Privacy Concerns

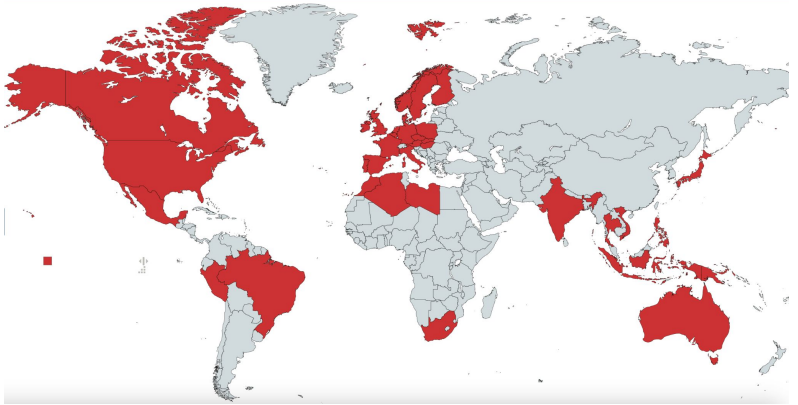
Trust Issues

Lack of Verifiable Proof

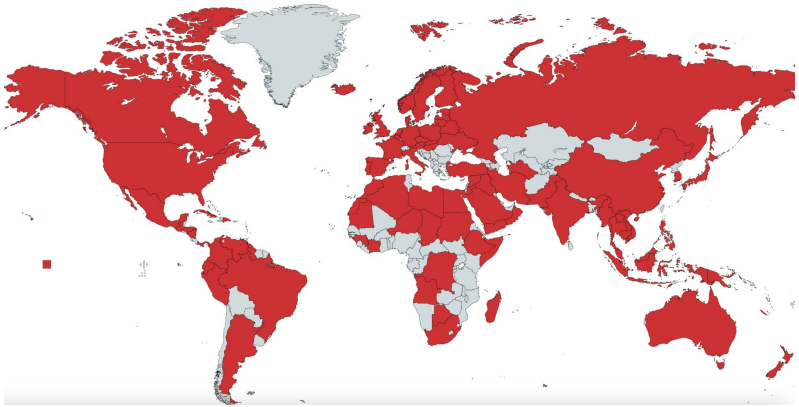
The Privacy Barrier to Global Data Collaboration

Sensitive data remains siloed due to privacy concerns, blocking global collaboration. Privacy-preserving machine learning can unlock secure, worldwide data sharing.

Before zKML implementation



After zKML implementation



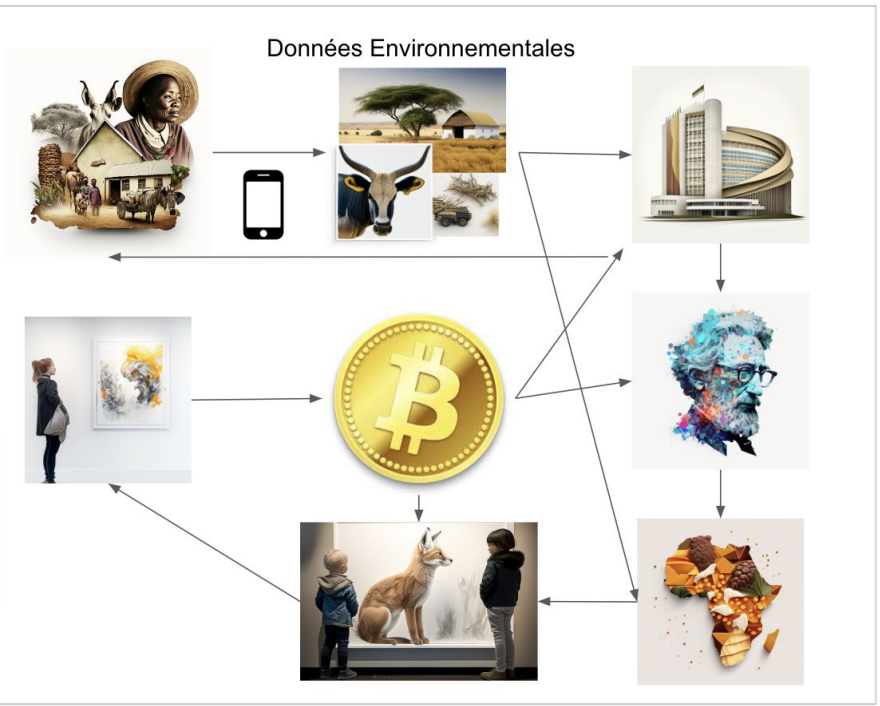
Use cases / user stories

- ➔ **Healthcare**: Securely predicting pandemic responses using privacy-preserving machine learning to protect patient data.
- ➔ **Finance**: Running collaborative financial models without exposing sensitive financial information.
- ➔ **Art**: Leveraging real-world data for generative art funding while safeguarding individual privacy.

COLLECTE DE FONDS

TOKENOMICS

- Données Démographiques
- Données Environnementales
- Données sur la Santé
- Données Économiques
- Données Éducatives
- Données Historiques
- Données de Recherche
- Histoires Personnelles et Témoignages



Solution Proposal

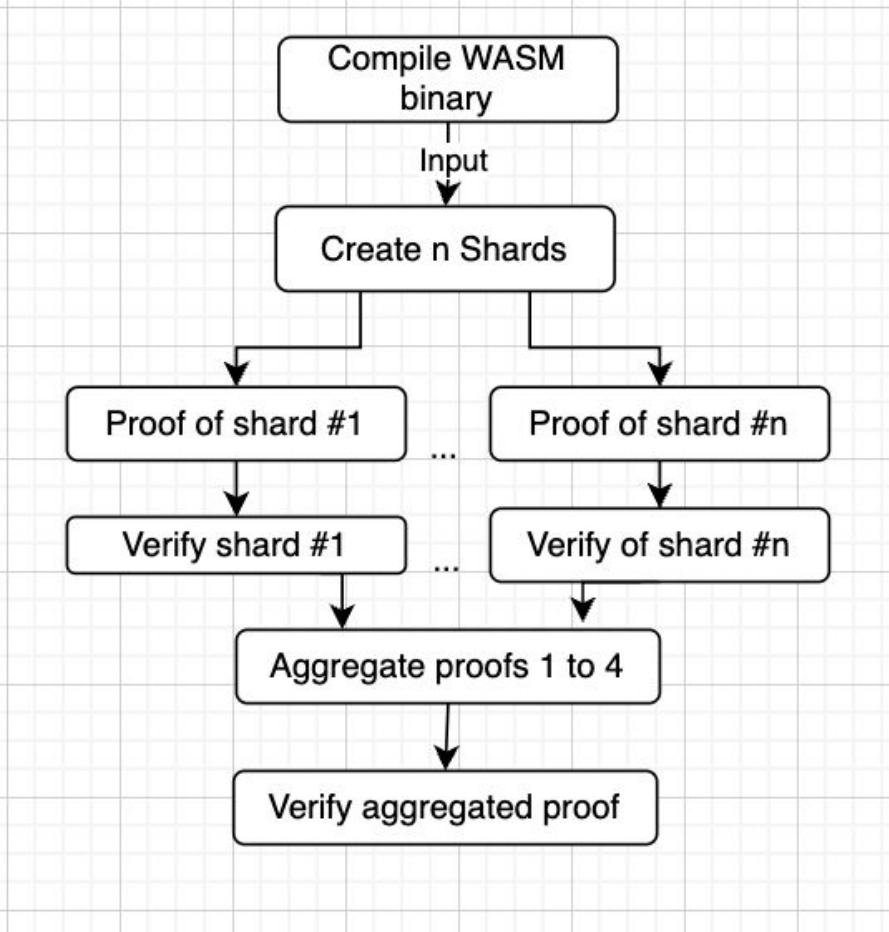
Zero-Knowledge Proof Mechanism

Proof Generation: Local proofs are generated for each shard, ensuring data privacy by keeping sensitive information within the participant's environment.

Proof Verification: Proofs are verified using public values, enabling trustless collaboration among participants.

Elapsed Time: The system minimizes the time required for proof generation and verification, making it suitable for practical applications.

Proof of Concept Implementation



Information architecture

Git Repo: https://github.com/guillaumelauzier/zkml-montreal/

Next Steps

What next?

- ➔ **Aggregation**: Consolidate proofs, enable on-chain storage, and integrate tokenization for secure, incentivized collaboration.
- ➔ **Federated Learning**: Decentralize model training across participants, preserving privacy while collaboratively improving model accuracy without sharing raw data.
- ➔ **Git Repos Integration**: Seamlessly connect version control with decentralized development, enabling collaborative coding, continuous integration, and secure, trackable contributions across repositories.

Questions?