# Implementing Privacy-Preserving Infrastructure to Verify Personhood Credentials

## 1. Background

In recent years on social media, amalgamations with six fingers and unnatural limbs betray AI's attempt to portray humanity. However, where is the line between content created by a human versus an AI? When will AI be able to believably mimic human behavior? As AI systems grow indistinguishable from humans online, there is growing uncertainty about whether other users online are real humans on the other side of the screen. To safeguard humanity in a future where AI may dominate digital spaces, we need innovative solutions to reliably distinguish real people online. Allowing for a future of the internet where users can be verifiably human while maintaining their personal anonymity is crucial to protect them from bad actors while maintaining online relationships. As a joint venture between three labs at Mines, we seek to carry out this mission through cutting-edge research in online credentials implemented in a shared web interface.

## 2. Project Description

This project seeks to develop privacy-preserving technology that allows individuals to prove their humanity without exposing personally identifiable information. The primary objective is to implement a decentralized identity infrastructure (complemented by a front-end infrastructure developed concurrently by external, related teams) that provides backend support for securely issuing, storing, and managing verifiable personhood credentials. Key components of this infrastructure include:

1. Decentralized credential storage: Implement a simplified decentralized storage method for securely storing user credentials.
2. Credential issuance and verification: Develop a secure and privacy-preserving protocol for issuing and verifying credentials.
3. API development for external integration: Create a minimal set of secure APIs (e.g., RESTful APIs) to demonstrate backend functionality for issuing, retrieving, and verifying credentials.

### *2.1. Project Goals*

- Develop a decentralized backend infrastructure prototype capable of securely storing and verifying user credentials.
- Implement basic privacy-preserving protocols that demonstrate secure issuance and verification of personhood credentials.
- Provide minimal API-based integration capabilities for external or frontend applications to interact with backend components.

### *2.2 Other Requirements*

- The prototype should respond promptly to credential verification requests.
- The API endpoints should be well-documented, clearly designed, and easy to understand by other developers.

- Produce clear instructions for deployment and running the prototype (e.g., README.md file) to make transition to future groups easier.

*2.3. Ethical Requirement*

All team members will be required to sign a non-disclosure agreement (NDA) upon onboarding to ensure confidentiality and responsible handling of project-related information.

3. **Desired Skill Set**

- Programming languages such as: Kotlin, Python, Node.js, Go, and/or Java.
- Decentralized storage: IPFS or similar blockchain simulator.
- APIs: RESTful web APIs (Express.js, Flask, or similar).
- Cryptographic libraries: Python's hashlib, Node's crypto module, or similar.
- **Note:** Any level of experience (including none) with any of the following is completely acceptable. Our sponsors have experience in all of these areas and are happy to help you.

4. **Preferred Team Size**: 4 students

5. **Location of Work**: Mines Campus Research Labs

6. **Primary Client Liaison**: Dan Ortiz, Undergraduate Student, and Andrew Plute, Undergraduate Student (**Additional Collaborators:** Prof. Guannan Liu, Prof. Chuan Yue, Dr. Alemitu Bezabih, Prof. Estelle Smith)