Project Proposal: Decentralized Authentication System

Student Name: İsa KOÇAN

Student Number: 22011056

Project Title: Passwordless Identity Management: Sign-In with Ethereum (SIWE)

Abstract: This project replaces traditional passwords with cryptographic wallet signatures. By removing stored passwords from the server, it eliminates the risk of data breaches and credential theft.

1. Problem Statement

- **Honey Pot Risk:** Centralized databases are prime targets; one hack exposes millions of passwords.
- **Password Reuse:** Users reuse passwords everywhere. A breach in one low-security site compromises their important accounts.

2. Proposed Solution A passwordless login system using Ethereum wallets (e.g., MetaMask). Users prove identity by signing a random one-time code (nonce). The server verifies this signature mathematically without ever storing or receiving private data.

3. Technical Architecture

- **Frontend:** React interface using **Ethers.js** for wallet interaction.
- **Backend:** Node.js (Express) server verifying signatures via ecrecover.
- **Mechanism:** Off-Chain verification (Zero gas fees) using unique Nonces to prevent replay attacks.

4. Key Outcomes

- **Hack-Proof Database:** Only public addresses are stored. There are no passwords to steal.
- **High Security:** Eliminates weak password and phishing risks.
- **Better UX:** Fast, one-click login experience.