Descrierea temei la alegere

Echipa Dima Cristian, Zamfir Cezara, Muscalu David, grupa 341

Tema:

Sistem de identitate academică anonimă bazat pe **Zero-Knowledge Proofs (ZKPs)**, care permite unui student să demonstreze anumite proprietăți despre statutul său fără a dezvălui date personale.

Fiecare utilizator primește un **secret criptografic**, din care se generează un angajament commitment = Poseidon(secret, attributes). Acest commitment este introdus în mai multe **Merkle trees tematice** (ex.: UNIBUC, FMI, Anul 3, Media≥8), ale căror rădăcini sunt publice.

zk-Selective Disclosure: studentul generează o dovadă SNARK care arată că angajamentul său se află într-un Merkle tree corespunzător predicate-ului ales (ex.: “student în anul 3”), fără a dezvălui identitatea sau celelalte atribute. Circuitul verifică membership-ul și predicate-ul, iar ca public inputs primește doar root și predicate_id.

zk-Range Proof: nota este descompusă în biți într-un circuit Circom, permițând verificarea condiției grade ≥ 80 fără expunerea valorii exacte; public se expune doar commitGrade = Poseidon(secret, grade).

anti-Sybil: circuitul generează un nullifier = Poseidon(secret) care este stocat on-chain; contractul permite emiterea unui singur SBT per nullifier, prevenind duplicarea credentialelor fără a compromite anonimitatea.

Smart-contractul verifică SNARK-ul, range proof-ul, nullifier-ul și emite un **Soulbound Token** care atestă validitatea predicate-ului demonstrat.