Homework 9

zkApps 2

In your teams discuss the sudoku example from the previous homework.

1. Does sudoku.ts solve the puzzle ?
2. Which lines in sudoku.ts indicate that a solution is correct
3. Is it possible to submit a correct solution, but have the proof rejected as false ?
4. If the prover altered the code, could they cheat and claim they had a solution, when in fact they didn't ?
5. Listen to the podcast episode about Mina and zkApps.

1) The `sudoku.ts` file doesn't actually solve the sudoku; it's a zkapp that generates proofs of knowing the solution and verifies them.

2) this.isSolved.set(Bool(true));

3) In a properly designed zk-SNARK-based application (zkapp), it should not be possible to submit a correct solution and have the proof rejected as false. However, if there are implementation errors or vulnerabilities, it might be possible for a malicious actor to submit an invalid proof that is erroneously accepted. Therefore, it's crucial to ensure that the zk-SNARK implementation is secure and well-audited to prevent such issues.

4) If the prover has the ability to alter the code or manipulate the zk-SNARK implementation, they might be able to cheat and claim they found a solution when they didn't. Security of a zk-SNARK system relies on the integrity of both the prover and verifier components. If the prover can modify the code, they could potentially generate fraudulent proofs that convince the verifier even if they haven't solved the problem.