Trabalho de Implementação: Blockchain com Proof of Work e Merkle Tree

Objetivo

Desenvolver uma aplicação em C que implemente uma blockchain funcional. A blockchain deve utilizar o algoritmo **Proof of Work (PoW)** para validação de blocos e deve incorporar uma **Merkle Tree** para estruturar as transações de cada bloco. A aplicação deve incluir uma funcionalidade que permita verificar se uma transação específica está incluída em um bloco através do processo de **Proof of Inclusion**.

Requisitos

1. **Estrutura da Blockchain:**
   - Cada bloco deve conter:
     - Índice do bloco.
     - Timestamp da criação.
     - Hash do bloco anterior.
     - Raiz da Merkle Tree (Merkle Root) representando as transações.
     - Nonce para Proof of Work.
     - Hash do bloco atual.
2. **Transações:**
   - Cada bloco deve armazenar transações (strings representando dados ou informações).
   - Use a Merkle Tree para organizar as transações.

3. **Proof of Work:**
    - Utilize um critério de dificuldade ajustável, para indicar o número de zeros que o hash do bloco deve ter no início.
    - Implemente a lógica para encontrar um nonce que satisfaça o critério de PoW antes de adicionar um bloco à blockchain.
4. **Merkle Tree e Proof of Inclusion:**
    - Implemente uma Merkle Tree para cada bloco, estruturando as transações.
    - Desenvolva um método que permita verificar, com base no hash de uma transação e no caminho de prova (*proof path*), se ela está incluída no bloco.
5. **Interface do Programa:**
    - O programa deve permitir:
        (a) Inserir novas transações em um bloco.
        (b) Minerar (adicionar) um bloco à blockchain após resolver o Proof of Work.
        (c) Exibir os blocos da blockchain com suas transações e hashes.
        (d) Verificar se uma transação específica está incluída em um bloco, utilizando o Proof of Inclusion.
        (e) Simular um ataque à rede que altera uma transação do bloco inicial e informa quanto tempo levou para reajustar todos os nonces.

Exemplos de Operações

1. Inserir as transações **T1, T2, T3** em um novo bloco.
2. Minerar o bloco usando Proof of Work.
3. Verificar se **T2** está no bloco recém-minerado.
4. Exibir a blockchain, incluindo:
    - Índice dos blocos.

- Hashes dos blocos.
- Raízes das Merkle Trees.

Critérios de Avaliação

- Implementação correta do Proof of Work.
- Uso de Merkle Tree para transações.
- Funcionamento do Proof of Inclusion.
- Organização e clareza do código.
- Testes demonstrando a funcionalidade completa (criar um relatório com estes testes).

Entrega do trabalho

O trio responsável pela realização do trabalho deve enviar o código com relatório e apresentar até o dia 10/02/2024. O envio do código deve ser feito pelo menos 3 dias antes da apresentação.

Observação

Use bibliotecas adequadas para hashing (exemplo: OpenSSL para C). Certifique-se de documentar o código com comentários explicando as etapas principais.