

**FACULDADE MULTIVIX VITÓRIA**  
**ENGENHARIA DA COMPUTAÇÃO**

**José Renato da Silva Lima, 1-2213760**

**Pedro Henrique Araujo da Silva, 1-2212765**

**Elyan Vinícius Ferreira Lopes, 1-2213858**

**Comunicação Indireta Pub/Sub + Eleição e Coordenação**

**Vitória**

**2025**

## 1. Objetivo do Trabalho

O objetivo deste trabalho é a implementação de um sistema distribuído de mineração de provas de trabalho (PoW) com comunicação entre múltiplos nós via MQTT, onde um nó é eleito como líder e os outros atuam como mineradores. O sistema deve ser capaz de realizar as seguintes operações:

1. Eleição de Líder: Um nó é escolhido aleatoriamente como líder por meio de um processo de votação.
2. Geração e Mineração de Desafios: O líder cria desafios (provas de trabalho) e os mineradores tentam resolvê-los.
3. Validação de Soluções: O líder valida as soluções propostas pelos mineradores e retorna um feedback sobre a aceitação ou rejeição das soluções.

## 2. Tecnologias Utilizadas

MQTT: Protocolo de comunicação baseado no padrão Publish/Subscribe, utilizado para a troca de mensagens entre os nós do sistema.

Paho MQTT: Biblioteca Python para implementação do cliente MQTT.

SHA-1: Algoritmo de hash utilizado para gerar as soluções dos desafios e validar a dificuldade.

## 3. Arquitetura do Sistema

O sistema é composto por múltiplos nós distribuídos que podem atuar como mineradores ou líderes. O processo de comunicação entre os nós é feito através de um broker MQTT (neste caso, o EMQX), que gerencia as mensagens enviadas entre os nós. O fluxo do sistema é o seguinte:

1. Fase de Inicialização: Cada nó se identifica e compartilha sua presença com os outros nós. Quando todos os nós estão conectados, a rede é sincronizada.
2. Fase de Votação: Os nós votam para escolher o líder. O nó com o maior VotID é eleito como líder.
3. Fase de Execução: O líder cria desafios de mineração. Os mineradores tentam resolver os desafios e enviar suas soluções para o líder, que valida as soluções e envia um feedback (aceitação ou rejeição).

## 4. Descrição da Implementação

A implementação segue as seguintes etapas:

- Fase 1: Inicialização
  - Cada nó gera um ClientID único e envia uma mensagem de presença para o broker MQTT, anunciando sua chegada.
  - Os nós se sincronizam até que todos estejam conectados.
- Fase 2: Votação

- Cada nó gera um VotetID aleatório e envia o seu voto para o broker.
  - O nó com o maior VotetID é eleito como líder.
- Fase 3: Execução
    - O líder gera um desafio de mineração com um identificador de transação (TransactionID) e um valor de dificuldade (Challenge).
    - Os mineradores tentam encontrar uma solução válida para o desafio, gerando diferentes valores de nonce e verificando o hash resultante.
    - O líder valida as soluções enviadas pelos mineradores e retorna um feedback (se a solução é válida ou inválida).

## 5. Lógica de Mineração (PoW)

- Cada desafio consiste em uma string formada por TransactionID e nonce.
- O minerador tenta encontrar um valor de nonce tal que o hash SHA-1 da string resultante tenha zeros à esquerda suficientes para atender à dificuldade especificada.
- A função validar\_hash é utilizada para verificar se o hash gerado atende à dificuldade do desafio.

## 6. Resultados e Feedback

Quando um minerador encontra uma solução válida, ele envia a solução para o líder, que valida o hash gerado. O líder então envia um feedback com a mensagem de aceitação ou rejeição. A aceitação ocorre quando o hash gerado pelo minerador atende à dificuldade especificada no desafio.

## 7. Considerações Finais

A implementação do sistema de mineração distribuído com MQTT permite que múltiplos nós colaborem para resolver desafios de prova de trabalho de forma eficiente. Embora o sistema tenha sido projetado para fins educacionais, ele pode ser estendido e melhorado com a inclusão de mais funcionalidades, como tolerância a falhas, controle de tempos de resposta e melhorias no algoritmo de eleição de líder.