

**FACULDADE MULTIVIX VITÓRIA**

**ENGENHARIA DA COMPUTAÇÃO**

**Laboratório III – Programação Paralela e Distribuída**

Nome: Manoela de Paula Rangel Romanelli

Matrícula: 2213460

**Vitória**

**2025**

## SUMÁRIO

1. OBJETIVOS .....	3
2. TECNOLOGIAS UTILIZADAS.....	3
3. ARQUITETURA DO SISTEMA.....	3
4. METODOLOGIA DE IMPLEMENTAÇÃO.....	4
5. LÓGICA DE MINERAÇÃO .....	5
6. RESULTADOS.....	5
7. CONSIDERAÇÕES FINAIS E CONCLUSÃO .....	5

## 1. OBJETIVOS

O presente trabalho tem como objetivo desenvolver um sistema distribuído para mineração baseada em Prova de Trabalho (*Proof of Work – PoW*), utilizando comunicação entre múltiplos nós por meio do protocolo MQTT. O sistema opera de forma colaborativa, com um nó eleito como líder e os demais atuando como mineradores.

As funcionalidades principais do sistema são:

1. Eleição de Líder: Seleção de um nó responsável pela coordenação das atividades, definida a partir de um processo de votação distribuída.
2. Geração e Distribuição de Desafios: O líder cria desafios de PoW, os quais devem ser resolvidos pelos mineradores.
3. Validação de Soluções: O líder verifica as soluções enviadas pelos mineradores, determinando sua validade e retornando um feedback adequado.

## 2. TECNOLOGIAS UTILIZADAS

- MQTT – Protocolo leve baseado no modelo *publish/subscribe*, utilizado para a troca de mensagens entre os nós de forma assíncrona e desacoplada.
- Paho MQTT – Biblioteca Python responsável pela implementação dos clientes MQTT utilizados por cada nó.
- SHA-1 – Algoritmo de hash empregado para geração e validação das soluções submetidas aos desafios de mineração.

## 3. ARQUITETURA DO SISTEMA

A arquitetura consiste em múltiplos nós distribuídos, podendo cada um deles atuar como líder ou minerador, dependendo da fase do sistema. A comunicação entre esses nós é intermediada por um *broker* MQTT (EMQX), que gerencia e repassa mensagens enviadas pelos clientes.

O fluxo operacional pode ser dividido em três fases principais:

1. Inicialização: Cada nó anuncia sua presença ao sistema, permitindo a sincronização da rede.
2. Votação: Os nós participam de um processo de votação distribuída. Aquele com o maior *VoteID* é eleito líder.
3. Execução: O líder emite desafios de mineração. Os mineradores processam e enviam suas soluções. O líder valida cada solução e envia o resultado (aceito ou rejeitado).

#### 4. METODOLOGIA DE IMPLEMENTAÇÃO

A implementação é estruturada nas seguintes etapas:

- Fase 1 – Inicialização
  - Cada nó cria um *ClientID* único.
  - O nó envia uma mensagem de presença ao *broker*, informando que está disponível na rede.
  - Os nós aguardam até que todos estejam conectados antes de iniciar a votação.
- Fase 2 – Votação
  - Cada nó gera um *VoteID* aleatório.
  - Os votos são publicados no *broker*.
  - O nó com o maior *VoteID* é eleito e assume o papel de líder.
- Fase 3 – Execução
  - O líder cria e publica um desafio de mineração, definido por:
    - TransactionID, um identificador único;
    - Challenge, representando a dificuldade (quantidade de zeros à esquerda).

- Os mineradores tentam resolver o desafio variando o valor de *nonce* e calculando o hash SHA-1 resultante.
- Ao encontrar uma solução válida, o minerador a envia ao líder.
- O líder valida o hash e retorna o feedback (“aceito” ou “rejeitado”).

## 5. LÓGICA DE MINERAÇÃO

- O desafio consiste em concatenar *TransactionID* com um *nonce*.
- Os mineradores iteram valores de *nonce* até gerar um hash SHA-1 que atenda à dificuldade definida.
- A função *validar\_hash* garante que o hash gerado possui zeros à esquerda suficientes, conforme o valor de *Challenge*.

## 6. RESULTADOS

Ao identificar um *nonce* válido, o minerador envia sua solução ao líder. O líder recalcula o hash para verificar sua legitimidade.

A solução é:

- Aceita, caso o hash satisfaça a dificuldade especificada;
- Rejeitada, caso contrário.

Esse mecanismo assegura que a validação seja centralizada no nó líder, evitando conflitos entre mineradores.

## 7. CONSIDERAÇÕES FINAIS E CONCLUSÃO

Durante o desenvolvimento e testes do sistema de mineração distribuída, observou-se que desafios com dificuldades superiores a 5 (ou seja, hashes SHA-1 iniciando com mais de cinco zeros hexadecimais) resultavam em tempos de processamento excessivamente longos para os nós participantes. Cada incremento na dificuldade aumenta exponencialmente o número

esperado de tentativas necessárias para encontrar uma solução válida. Na prática, dificuldades acima desse limite ocasionavam:

- Tempo de mineração imprevisível ou extremamente prolongado;
- Aparente travamento dos processos, especialmente em máquinas convencionais;
- Redução significativa da responsividade e sincronização entre os nós.

Como o objetivo do projeto é avaliar mecanismos de coordenação distribuída, eleição, comunicação via Publish/Subscribe e comportamento colaborativo entre os nós a dificuldade máxima foi ajustada para 5. Essa decisão técnica mantém desafios suficientemente complexos para evidenciar o funcionamento da mineração, ao mesmo tempo em que garante estabilidade, previsibilidade e viabilidade para testes acadêmicos.

Com essa adaptação, a implementação do sistema de mineração distribuída utilizando MQTT demonstra a viabilidade da coordenação entre múltiplos nós em um ambiente descentralizado. Apesar de ser uma abordagem voltada para fins didáticos, o sistema pode ser ampliado com funcionalidades adicionais, tais como:

- Mecanismos de tolerância a falhas;
- Controle de tempo e limitação para resolução de desafios;
- Estratégias mais robustas de eleição de líder;
- Escalabilidade do número de nós participantes.

O projeto, portanto, oferece uma base sólida para estudos sobre sistemas distribuídos, coordenação entre processos e implementação prática de algoritmos distribuídos, evidenciando de forma clara os desafios e as soluções envolvidas na comunicação indireta através de middleware Publish/Subscribe.