Universidade Federal do Pará
Instituto de Ciências Exatas e Naturais
Faculdade de Computação
Laboratório de Sistemas Distribuídos

Implementação de uma Criptomoeda/Transação Distribuída Simplificada (Bitcoin-like)

Introdução

As criptomoedas representam um dos exemplos mais relevantes de sistemas distribuídos em larga escala, envolvendo conceitos como replicação de dados, consenso, tolerância a falhas, comunicação entre processos e concorrência.
Este trabalho tem como objetivo a implementação de um sistema distribuído inspirado no Bitcoin, porém simplificado, com foco nos fundamentos de Sistemas Distribuídos.

Objetivo Geral

Desenvolver um sistema distribuído de criptomoeda/transação simplificada, executando em múltiplos computadores do laboratório, no qual cada computador representa um nó da rede, mantendo uma cópia local de uma blockchain, comunicando-se com outros nós por meio de sockets e utilizando um mecanismo simples de consenso.
Cada grupo ficará responsável por manter um nó da rede e manter todas as informações necessárias para que participe da blockchain.

Organização do Trabalho

- O trabalho deverá ser realizado em grupos de até 3 estudantes.
- Cada grupo deverá implementar um sistema funcional e demonstrável no ambiente do laboratório utilizando os softwares bases disponíveis.
- Todas as linguagens de programação são permitidas, dando preferência para C, C++, C# e Python.
- A comunicação entre os nós deve ser obrigatoriamente através de sockets e as mensagens devem ser serializadas com JSON.
- Todos os integrantes do grupo devem participar ativamente do desenvolvimento e da apresentação.

Descrição do Sistema

Nó da Rede (Node)

Cada nó da rede deverá:

- Executar como um processo independente.
- Utilizar uma porta configurável e única para todos os nós da rede.
- Conhecer ao menos um nó inicial (*bootstrap*).
- Manter localmente:
    - uma cópia da blockchain;
    - um conjunto de transações pendentes.
- Não deve existir servidor central.

Transações

As transações devem possuir, no mínimo, os seguintes campos:

- identificador único;
- origem;
- destino;
- valor;
- *timestamp*.

As regras aplicáveis as transações são:

- Ter somente valores positivos, ou seja, não permitir valores negativos;
- não permitir saldo negativo em nenhuma hipótese.

Blocos

Cada bloco da blockchain deve obrigatoriamente conter:

- índice do bloco;
- *hash* do bloco anterior;
- lista de transações;
- *nonce*;
- *timestamp*;
- *hash* do bloco atual.

O *hash* deve ser gerado utilizando SHA-256.

Blockchain

A blockchain deve obedecer aos seguintes parâmetros:

- existir um bloco gênesis fixo;
- cada bloco deve referenciar corretamente o *hash* do bloco anterior;
- a cadeia válida é aquela que possui todos os blocos válidos;

Consenso Distribuído

Será utilizado um **Proof of Work simplificado**, com as seguintes características:

- Para minerar um bloco, o nó deve encontrar um valor de *nonce* tal que o *hash* do bloco comece com "000".
- A dificuldade será fixa.
- O primeiro nó a encontrar um bloco válido deverá:
    - adicioná-lo à sua blockchain;
    - propagá-lo para os demais nós.

Blocos recebidos devem ser validados antes de serem aceitos.

Protocolo de Comunicação

O sistema deverá implementar os seguintes tipos de mensagens:

- NEW_TRANSACTION – envio de uma nova transação.
- NEW_BLOCK – envio de um bloco minerado.
- REQUEST_CHAIN – solicitação da blockchain completa.
- RESPONSE_CHAIN – envio da blockchain para sincronização.

O protocolo deve ser discutido com os outros grupos para que haja consenso e totalmente documentado no relatório.

Planejamento das Atividades

Para que todos os grupos possam desenvolver suas atividades de forma cadenciada, sugere-se o seguinte cronograma a ser desenvolvido por semana:

Semana 1 (4h)

- Criação da estrutura básica do nó.
- Comunicação entre processos via sockets.
- Testes de envio e recebimento de mensagens simples.

Semana 2 (4h)

- Implementação da estrutura de bloco.
- Implementação da blockchain local.
- Validação da cadeia.

Semana 3 (4h)

- Implementação de transações.
- Pool de transações.
- Propagação de transações entre nós.

Semana 4 (4h)

- Implementação do Proof of Work.
- Criação e propagação de blocos.
- Aceitação de blocos remotos.

Semana 5 (4h)

- Entrada tardia de nós na rede.
- Sincronização da blockchain.
- Resolução simples de conflitos (cadeia mais longa).

Semana 6 (4h)

- Apresentação do sistema em funcionamento.
- Entrega do relatório técnico e código fonte.

Entregáveis

Cada grupo deverá entregar:

1. Código fonte completo do sistema.
2. Relatório técnico, contendo:
    - descrição da arquitetura;
    - protocolo de comunicação;
    - mecanismo de consenso;
    - limitações do sistema;
    - dificuldades encontradas.
3. Demonstração prática do funcionamento do sistema em laboratório.
    - Todos os grupos tem que apresentar em conjunto para que o sistema desenvolvido em cada um funcione em um sistema distribuído.

Critérios de Avaliação

Critério	Peso
Comunicação distribuída funcional	25%
Implementação correta da blockchain	25%
Consenso e mineração	20%
Tratamento básico de falhas	15%
Relatório e apresentação	15%