UNIVERSIDADE DE SÃO PAULO

ARQUITETURA E ESCALABILIDADE DAS CRIPTOMOEDAS BASEADAS EM BLOCKCHAIN

Aluno: Lucas Stefan Abe
Supervisor: Daniel Macedo Batista
BCC - IME

INTRODUÇÃO

As criptomoedas baseadas em blockchain são moedas digitais descentralizadas. Sua descentralização é atingida através de sistema que funciona em uma rede peer-to-peer sem autoridade central, criptografia e blockchain. Apesar dessas criptomoedas serem descentralizadas, existe o problema da escalabilidade. O objetivo deste trabalho é estudar a arquitetura e escalabilidade dessas criptomoedas.

BITCOIN

O Bitcoin foi a primeira criptomoeda baseada em blockchain a ser criada e permite pagamentos online através de sua moeda nativa, o bitcoin. Qualquer um pode participar da rede de forma anônima.

Criptografia

As criptomoedas em geral utilizam duas primitivas criptográficas:

- Função de hash criptográfico: É um algoritmo matemático que mapeia dados de tamanho arbitrário para uma cadeia de bits de um tamanho fixo (um hash) e é projetado para ser uma função unidirecional, ou seja, uma função que é inviável inverter

- Criptografia de chave pública: As criptomoedas em geral baseiam-se no esquema de criptografia de chave pública para controlar o acesso das criptomoedas pelos usuários. Nesse esquema existem duas chaves, uma chave privada e uma chave pública que é derivada da chave privada. A chave pública deriva o endereço da conta que é usado para receber fundos, já a chave privada é usada para enviar fundos para outro endereço através da assinatura digital de transações.

Blockchain

O Blockchain é um registro digital público distribuído de todas as transações do Bitcoin, que opera em uma rede peer-to-peer e é considerado imutável, todos os nós da rede armazenam uma cópia do blockchain e validam todas as transações. O registro é formado por blocos, que armazenam conjuntos de transações em uma tipo especial de árvore chamada árvore de merkle, e outros dados importantes (tempo de criação do bloco, hash do bloco anterior e etc). Cada bloco é identificado por um hash gerado a partir de dados do seu cabeçalho e possui o hash do bloco anterior. Dessa forma, todo bloco tem uma referência para o bloco anterior, formando uma cadeia de blocos.

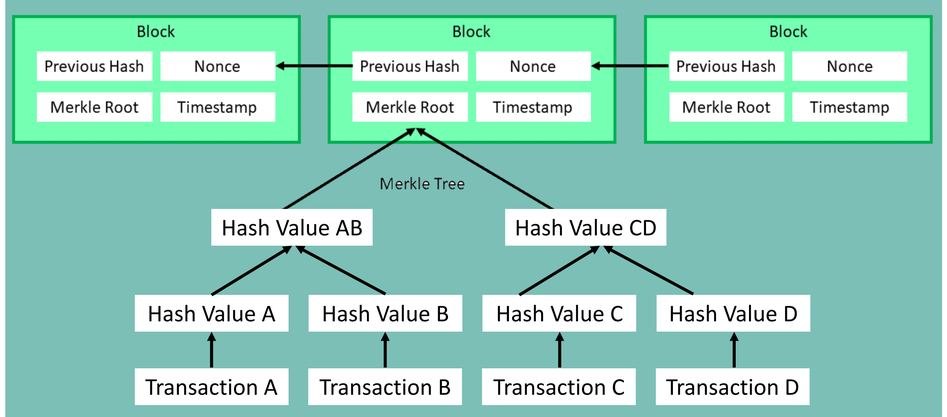


Ilustração simplificada do Blockchain

Mineração

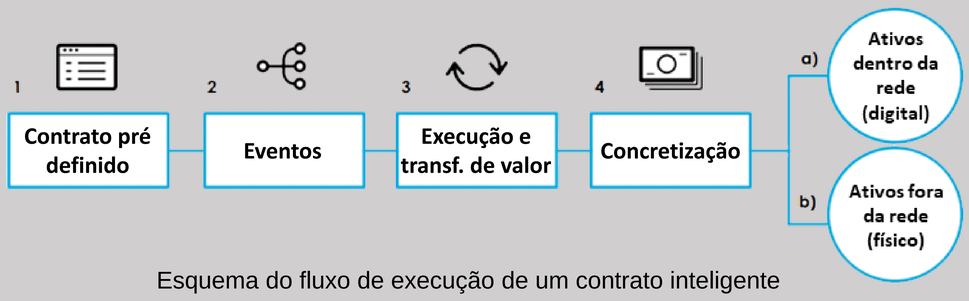
A inserção de novos blocos no Bitcoin é feita por um processo chamado mineração, que consiste em resolver um problema computacionalmente difícil chamado Prova de Trabalho, isso demanda uma quantidade significativa de recursos financeiros e computacionais. Os nós da rede que realizam essa tarefa são chamados de mineradores, e eles recebem um incentivo econômico quando inserem um novo bloco. Para alterar um bloco é necessário alterar todos os blocos seguintes e refazer toda a prova de trabalho, isso exige uma quantidade extremamente alta de recursos computacionais, por isso os dados armazenados no blockchain são considerados imutáveis.

ETHEREUM

Assim como o Bitcoin, o Ethereum é uma criptomoeda. Porém, existem algumas diferenças entre os dois, sendo que as distinções mais importantes se referem ao propósito e capacidades. O Bitcoin oferece uma aplicação particular da tecnologia do blockchain, um sistema de moeda digital peer to peer que permite pagamentos online. Já o Ethereum, apesar de também ser usado como moeda digital, foi criado com o propósito de funcionar como uma plataforma de computação distribuída que executa programas chamados contratos inteligentes.

Contratos inteligentes

Contrato inteligente é um termo utilizado para descrever programas de computador que facilitam a troca de dinheiro, conteúdo, propriedade, ações ou qualquer outra coisa de valor. Quando é armazenado no blockchain, um contratos inteligente é executado automaticamente quando eventos específicos são atingidos sem possibilidade de censura, fraude, tempo de inatividade ou interferência de terceiros.
O contrato inteligente funciona da seguinte forma: Primeiro é definido entre as partes o que colocar no código do contrato, esse contrato então é ativado quando eventos determinados no contrato ocorrem, feito isso ele é executado pelos nós da rede e pode ocorrer uma transferência de valores.



Esquema do fluxo de execução de um contrato inteligente

EVM

O núcleo da inovação do Ethereum é a EVM (Máquina Virtual do Ethereum), um ambiente de execução que está presente nos nós da rede do Ethereum. Esse ambiente é responsável por rodar os contratos inteligentes, que são códigos compilados de linguagens de script turing completas.

ESCALABILIDADE

Atualmente as criptomoedas baseadas em blockchain realizam apenas uma quantidade limitada de transações por segundo (limite de aproximadamente 7 no Bitcoin e 20 no Ethereum), isso se deve à sua arquitetura atual. Existe um limite de transações que podem ser incluídas em cada bloco e cada bloco é criado em um intervalo constante de tempo. Existem 3 principais propostas de solução para a escalabilidade

- **Aumento do limite do tamanho do bloco:** Propõe o aumento do limite do tamanho do bloco, para que seja possível colocar mais transações em um bloco.

- **Lightning Network:** A lightning network é uma solução que está sendo desenvolvida para o Bitcoin e permite pagamentos instantâneos entre duas partes com taxas baixíssimas. Essa solução consiste no uso de contratos inteligentes para criar uma rede de canais de pagamento entre usuários fora da rede do Bitcoin.

- **Sharding:** Consiste em dividir a rede em partições conforme a quantidade de nós aumenta, dessa forma em vez de validar e armazenar todo o histórico do blockchain, o nó somente valida e armazena o histórico de sua partição. Assim, as transações são processadas em paralelo e a capacidade de processamento de transações escala linearmente em relação a quantidade de nós da rede.

CONCLUSÃO

As criptomoedas representam uma grande inovação não só no ponto de vista financeiro, mas também do ponto de vista tecnológico. Existem inúmeras possibilidades à vista além de um sistema de pagamento online descentralizado. Os contratos inteligentes possuem potencial para desburocratizar sistemas que necessitam de confiança entre as partes, aumentando a eficiência através da automatização que contratos normais não possuem. A escalabilidade é essencial para a adoção em massa dessas criptomoedas, e pelos estudos deste trabalho já existem diversas propostas de solução sendo que cada uma possui seus prós e contras.