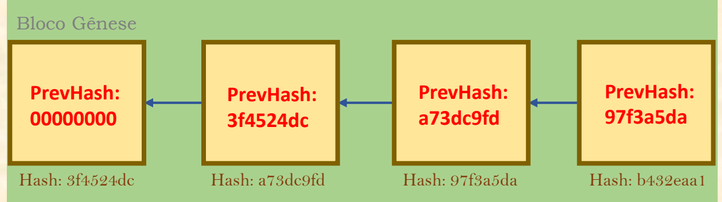
Blockchain e Ethereum
Aplicações e Vulnerabilidades

Frederico Lage Ferreira
Orientador: Prof. Dr. Routo Terada
Departamento de Ciência da Computação, Instituto de Matemática e Estatística, Universidade de São Paulo/USP

Blockchain

O que é?

Um banco de dados distribuído em uma rede de vários participantes, sem entidade central controladora e onde nenhum participante é mais confiável que qualquer outro. As informações estão organizadas em blocos encadeados entre si através de hashes criptográficos. Cada participante da rede (chamado de nó) contém uma cópia completa do banco de dados.



Blocos

Cada bloco tem uma cabeçalho e uma lista de transações. As transações são os eventos que o blockchain registra. O cabeçalho deve conter o hash do bloco anterior, uma marca temporal e informações adicionais de acordo com o sistema (raiz da árvore de Merkle, nonce, versão, nível de dificuldade da Prova de Trabalho e etc.). O hash do bloco anterior cria o encadeamento, já que irá afetar o hash do bloco subsequente e assim por diante, logo é impossível mudar um bloco antigo da cadeia sem mudar todos os subsequentes.

Exemplo de bloco do Bitcoin

Consenso

Por se tratar de um sistema distribuído, é necessário que haja consenso entre os nós. Sempre que um novo bloco é adicionado ao blockchain, cada nó irá validá-lo. Uma parte importante desse processo de validação é o mecanismo que decide se o criador de um novo bloco estava bem-intencionado. O mais utilizado é a Prova de Trabalho, na qual o processo de criação do bloco (chamado de **mineração**) demanda um alto gasto de tempo e energia mas, em contrapartida, recompensa o minerador por seu esforço. Assim, ocorre uma competição entre os participantes para obter essa recompensa, ao mesmo tempo em que cada um audita todos os demais. Esse método também torna economicamente inviável tentar corromper o blockchain alterando uma longa sequência de blocos.

Ethereum

O que é?

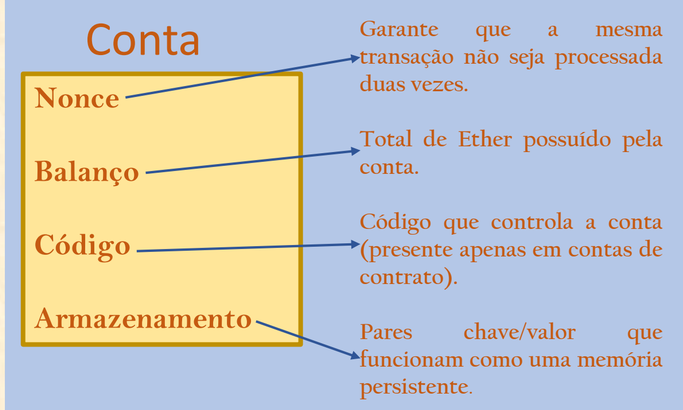
Plataforma dedicada ao desenvolvimento e implantação de aplicações descentralizadas (Smart Contracts). Estas são executadas de maneira inviolável, já que os nós da rede deverão entrar em consenso quanto ao resultado. Cada nó deve implementar a Ethereum Virtual Machine (EVM), uma máquina virtual Turing completa. Para recompensar a mineração e trocar valores, utiliza a criptomoeda Ether.

Gas

Computações custam *gas* (de *gasoline*). Um passo computacional simples custa 1 gas, operações mais complexas custam mais. Cada transação estabelece o máximo de unidades de gas que pode gastar e o valor em Ether que se dispõe a pagar por cada unidade gasta. Este valor corresponderá à taxa da transação. Gas não gasto ao final da transação é devolvido. Se o total enviado for insuficiente, as computações são revertidas, mas a taxa é perdida. Impede loops infinitos, ataques para sobrecarregar a rede e excessos de ineficiência.

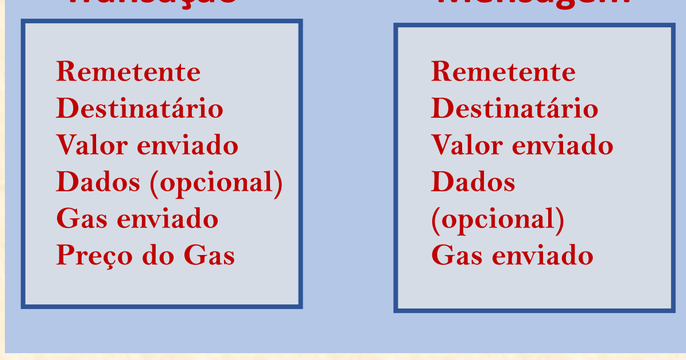
Contas

O estado do Ethereum é uma coleção de contas. Contas externas são aquelas controladas por um usuário que possui a chave privada correspondente, contas de contrato são controladas por seus próprios códigos.



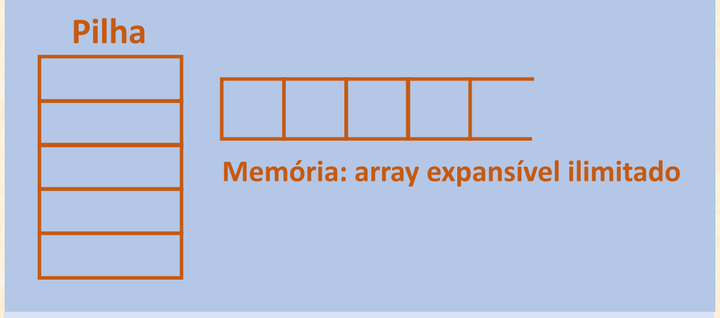
Transações e Mensagens

Transações são enviadas apenas por contas externas. Necessariamente são elas que dão inicio a uma computação, podendo ou não enviar dados adicionais (como argumentos de um programa) e são registradas nos blocos. Mensagens são uma forma de comunicação virtual entre contas de contrato, permitindo que diferentes programas interajam entre si.



EVM

Máquina virtual definida por Gavin Wood, possui operações matemáticas, lógicas, *jumps* e acesso à memória e a um pilha típicas de computadores modernos. Também possui uma variedade de operações específicas para acessar informações das transações e mensagens, bem como para permitir a comunicação entre contratos.



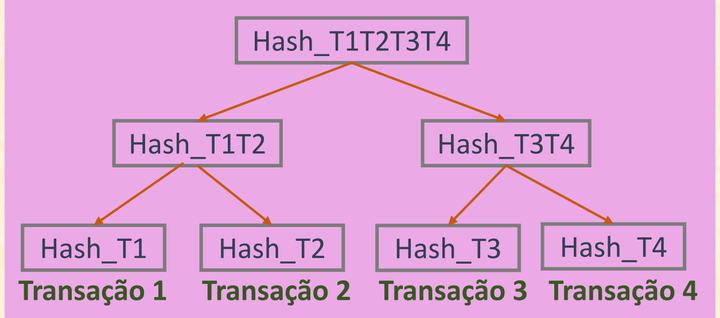
Linguagens do Ethereum

Atualmente suporta 3 linguagens: Serpent (baseada em Python), LLL (baseada em Lisp) e Solidity (baseada em C++ e Javascript). Todas são compiladas para o chamado EVM code, semelhante a uma linguagem de assembly baseada em pilhas.

Conceitos auxiliares

Árvore de Merkle

Uma estrutura de dados que permite organizar pedaços de informação em ordem e autenticar sua presença e localização com mais eficiência. Consiste em uma árvore de hashes, com a informação nas folhas e hashes nos nós.



Hash criptográfico

Uma função de hash converte entradas de tamanho variável em saídas de tamanho fixo. Uma função de hash criptográfica é tal que, conhecendo o resultado, seja muito difícil deduzir a entrada. Logo, é simples verificar se uma certa entrada resulta no hash esperado mas, tendo o hash esperado, é muito difícil construir uma entrada falsa que resulte no mesmo hash.

Chave pública e privada

Na criptografia assimétrica, gera-se um par de chaves, uma pública e uma privada. Mensagens encriptadas com a chave pública, só podem ser decriptadas pelo possuidor da chave privada correta. Além disso, o possuidor da chave privada pode assinar suas mensagens de modo tal que qualquer um com a chave pública pode verificar sua identidade.