Blockchain como uma estrutura de dados

Olá, Habr!

Hoje gostaríamos de delinear um novo tópico para discussão, examinando brevemente o blockchain do ponto de vista da ciência da computação - como uma das estruturas de dados. Recentemente, o blockchain tem sido cada vez mais usado fora do segmento de criptomoedas , e essa tendência certamente merece atenção. Vamos conversar a respeito disso!

A tecnologia Blockchain pode ser explicada de muitas maneiras diferentes. Até recentemente, o blockchain era visto principalmente em termos de criptomoedas. Bitcoin é a primeira associação de blockchain que muitos de nós temos. Mas armazenar transações de criptomoedas é apenas um dos muitos casos de uso de blockchain. Neste artigo, vamos voltar atrás desse ponto de vista e considerar o blockchain no contexto mais geral da ciência da computação.

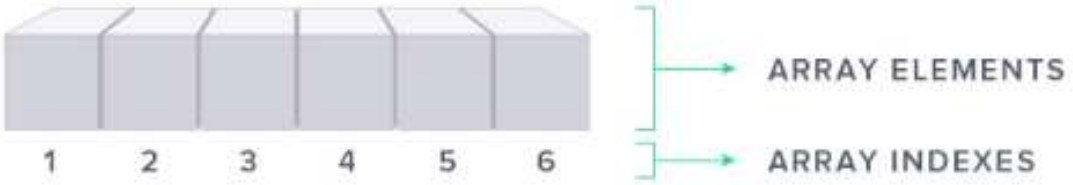
Blockchain é uma estrutura de dados

Uma estrutura de dados é uma forma de armazenar, organizar e gerenciar dados. A estrutura de dados permite acessar esses dados, adicioná-los, modificar e pesquisar os dados contidos nesta estrutura. As estruturas de dados mais comuns e básicas incluem *arrays* e *listas vinculadas* .

Array

A matriz contém vários elementos enumerados. Podem ser números, letras, palavras ou até arquivos inteiros. Graças aos índices, você pode se referir a cada elemento do

array. Portanto, se você deseja alterar uma entrada em uma matriz e sabe onde ela está, pode *acessá-la instantaneamente* .



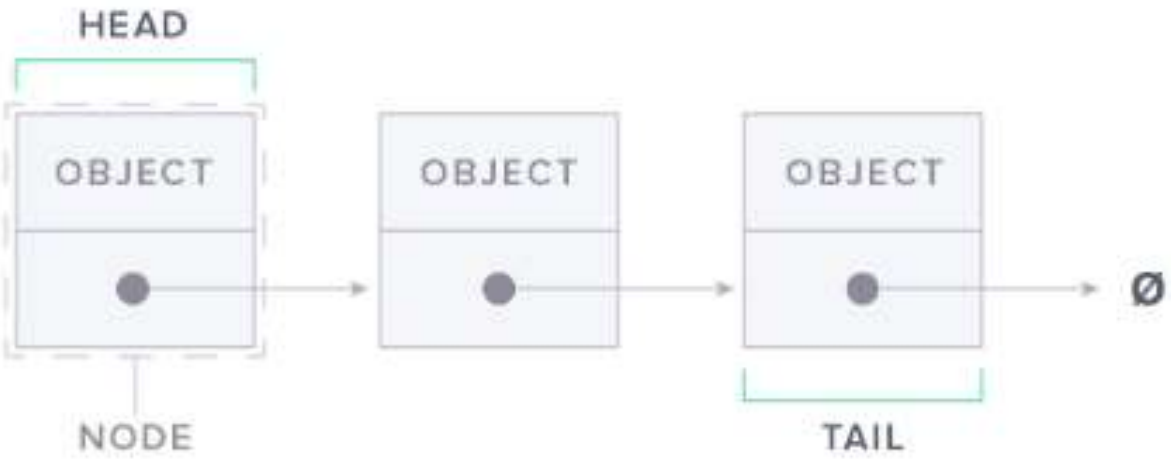
Matriz unidimensional com seis elementos

Listas Ligadas

Nós são itens de dados incluídos em uma lista vinculada. O nó contém pelo menos um objeto de dados e um ponteiro para o próximo item. A função de um ponteiro é dizer ao computador onde está o próximo item em uma determinada lista.

Se você olhar o primeiro item da lista e quiser se referir ao segundo, olhe para o ponteiro que o levará ao próximo nó. É mais fácil adicionar dados a uma lista encadeada do que a um array, uma vez que precisa ser expandido em um nó, e adicionar dados a um array aumentará o número de elementos neste array. Mas ao trabalhar com listas vinculadas, você não tem acesso instantâneo aos dados.

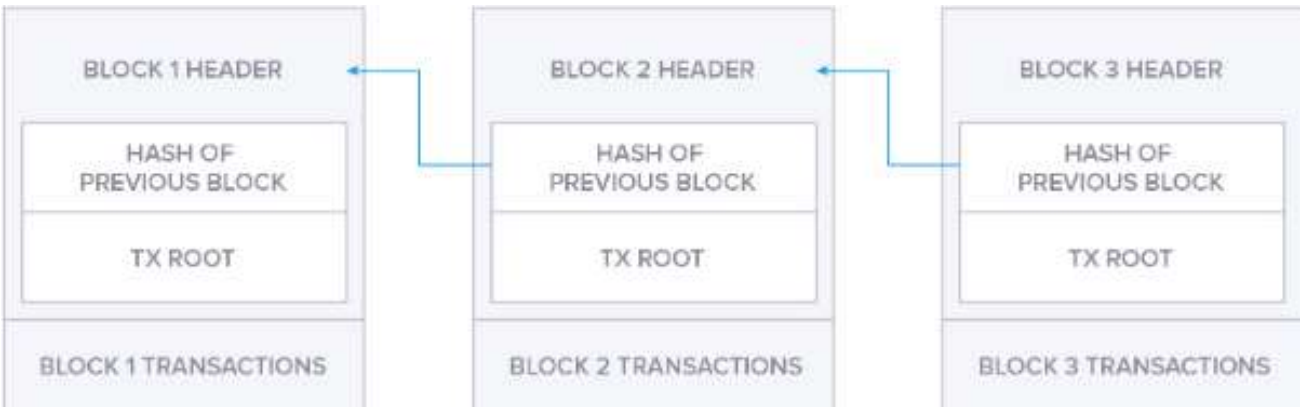
Se você estiver procurando por um item de dados específico em uma lista vinculada, você primeiro olha para o *primeiro nó* desta lista, seu *cabeçalho*... Se este não for o elemento que você estava procurando, siga o ponteiro que o levará ao próximo nó. Se este nó não contiver os dados que você está procurando, continue a seguir os links de nó a nó até encontrar os dados de que precisa.



Lista ligada de três nós

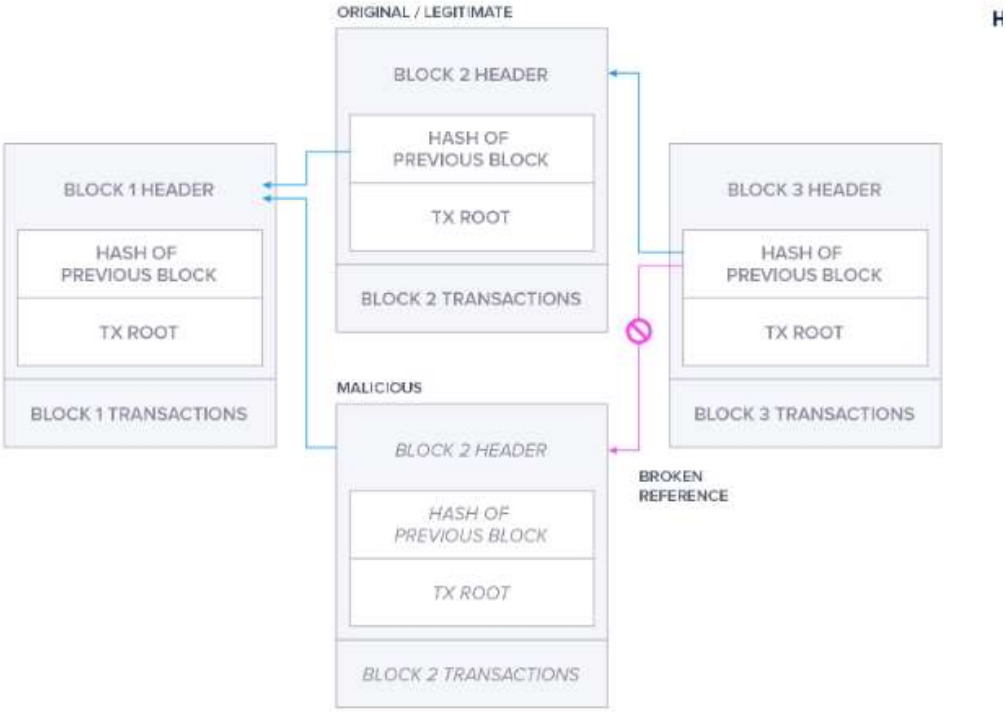
Blockchain

No contexto de estruturas de dados, blockchain mais se assemelha a uma lista vinculada. Além disso, no blockchain, os dados são divididos em contêineres chamados *blocos* . Os blocos são bastante semelhantes *aos nós da* lista vinculada. Cada bloco contém um link que é um hash do bloco anterior. Ele atua como um link para o bloco anterior e ajuda a manter a ordem na cadeia de blocos.



A principal diferença entre o blockchain e a lista vinculada é que cada link no blockchain é criptograficamente seguro. Você pode ter ouvido o termo "anexar apenas" aplicado ao blockchain. Isso significa que você pode adicionar novos dados ao blockchain apenas completando a cadeia pela frente. A validade dos links

protegidos é verificada constantemente. Se fosse possível inserir um bloco malicioso no meio do blockchain, por exemplo, entre os blocos 1 e 3 no diagrama abaixo, seria possível colocar um link para o bloco anterior 1, mas não para o próximo bloco 3.



Cada novo bloco é construído sobre o existente, e este procedimento é geralmente chamado de confirmação. Quanto mais antigo for o bloco, mais confirmações ele terá. Cada confirmação torna difícil adulterar os dados do bloco. No diagrama a seguir, o Bloco 2 tem uma confirmação. Para falsificar os dados no bloco 2, você terá que recriar um bloco válido contendo um novo link válido. Após cada próxima confirmação, você terá que recriar outro bloco. Assim, quanto mais antigo for o bloco, maior será a confiança de que nenhuma alteração será feita neste bloco.

Os links entre os blocos dependem não apenas da ordem dos blocos, mas também dos dados contidos em cada bloco. Não é possível adicionar ou remover dados de um bloco no blockchain. É nessa propriedade que se baseia a confiança de que nada acontecerá com os dados colocados no blockchain. Naturalmente, qualquer falsificação é óbvia na estrutura de dados do blockchain. Qualquer alteração feita nos links de quebra de dados para todos os blocos subsequentes.

Embora seja impossível excluir ou alterar dados no blockchain, é fácil adicionar dados a um novo bloco anexado à cadeia. Por exemplo, uma nova transação pode ser adicionada ao blockchain da criptomoeda. A transação é fácil de verificar porque

todas as transações anteriores registradas na rede são imutáveis. Quando um valor de X é exigido do endereço Y, o saldo desse endereço deve ter um valor de pelo menos X.

As criptomoedas são apenas uma aplicação particular da tecnologia blockchain. O Blockchain está se tornando rapidamente uma opção cada vez mais viável para o gerenciamento da cadeia de suprimentos, gerenciamento de frota e outros fins.

Conclusão

Blockchain é um método de armazenamento de dados aplicável em ciência da computação. Os elementos do blockchain - seus blocos - são criptograficamente vinculados uns aos outros. Não é possível alterar os dados após terem sido gravados no bloco. Este é o valor do blockchain. É um registro imutável no qual você pode armazenar dados com segurança enquanto opera em um ambiente não confiável.

Eu gostaria de terminar este artigo com um tweet contendo a quintessência das propriedades da tecnologia blockchain e ilustrando seu lugar entre outras estruturas de dados.

> , , .
>
> , , . , – — @NickSzabo4

More articles:

- Como um banco de dados mal configurado nos permitiu capturar uma nuvem inteira com 25 mil hosts
- Reescrevendo o histórico do repositório de código ou por que às vezes você pode usar o git push -f
- As alegrias de possuir um endereço de e-mail curto
- Implementação de CI / CD e DevOps na empresa (no nosso caso, Rostelecom)
- Nossas descobertas durante um ano de migração do GitLab.com para o Kubernetes