 **CENTRO DE ENSINO SUPERIOR DE JUIZ DE FORA**

**CES/JF**

**CURSO SISTEMAS DE INFORMAÇÃO**

**JONAS ANTÔNIO GOMES VICENTE**

**TRABALHO DE ESTRUTURA DE DADOS**

**RESUMO DO TEXTO SOBRE BLOCKCHAIN**

**JUIZ DE FORA-MG**

**2017**

**Introdução:**

A estrutura Blockchain é uma lista de blocos re-ligados e ordenados de transações que pode ser armazenada em um arquivo flat ou em simples bancos de dados, a exemplo do bitcoin, que armazena seu blockchain no banco de dados da Google. Cada bloco é ligado referindo-se ao bloco anterior, dessa forma, o blockchain pode ser visto como uma pilha. Essa visualização cria a altura, que é a distância entre qualquer bloco e o primeiro bloco, sendo o topo o bloco que foi inserido por último.

Os blocos são identificados por um hash criptografado no cabeçalho de cada bloco. No cabeçalho, ainda temos uma referência ao bloco anterior, que é chamado de bloco pai. Cada bloco pode possuir apenas um pai, mas pode conter diversos filhos temporariamente, que é uma situação que ocorre quando blocos diferentes são descobertos por de modo quase simultâneo por diversos mineradores.

O campo da hash do bloco anterior afeta os demais blocos, ou seja, se a identidade de um bloco pai é alterada, consequentemente a identidade do filho será também. Tais mudanças afetam todas as gerações de blocos do blockchain, forçando que os cálculos sejam refeitos, o que exige um grande processamento, tornando-se um aspecto da segurança do bitcoin.

**A estrutura de um bloco:**

O bloco é um container de estruturas de dados que agrega transações que são incluídas no blockchain. O bloco contém um cabeçalho, possui a referência ao bloco anterior, de modo que o conecte ao mesmo. Também possui metadados além de possuir um hash responsável por resumir todas as transações do bloco.

Identificadores de blocos: Hash do cabeçalho do bloco e altura do bloco

O primeiro identificador de um bloco é a hash criptografada criada no cabeçalho. A hash gerada possui 32 bytes. Um segundo meio de identificar o bloco é a partir da sua posição no blockchain, medida pela sua altura no bloco. Como já mencionado, o blockchain funciona como uma pilha, portanto, o primeiro bloco colocado recebe o índice 0 (zero) e os demais recebem seu incrementos no índice. O método da altura não possibilita identificar um bloco unicamente em todos os casos, pois mais de um bloco pode possuir a mesma altura no blockchain.

**Bloco de Criação:**

O bloco de Criação é o primeiro bloco criado na blockchain. É o bloco ancestral de todos os outros blocos na estrutura, ou seja, se percorrer todos os blocos do fim para o início, chegaremos eventualmente a esse bloco. Não pode ser alterado, pois é codificado dentro do software do cliente bitcoin.

**Merkle Trees:**

Cada bloco contém um sumário com todas as transações no bloco utilizando a merkle tree. Essa estrutura é uma árvore binária com a criptografia de hash, e é utilizada para resumir e verificar de modo mais eficiente os dados.

A árvore é construída de modo recursivo com pares de hash até que exista apenas uma hash, que é chamada de root ou de merkle root.

Por se tratar de uma árvore binária, é necessário um número par de folhas, que são as transações. Caso o número seja ímpar, a última transação é duplicada, assim a árvore estará completamente balanceada.

**Merkle Trees e Verificação Simplificada de Pagamento (SPV):**

As árvores Merkle são também usadas para efetuar a SPV. Esse nós de SPV não possuem todas as transações e não baixam os blocos por completo, somente o bloco de cabeçalho é baixado.

**Referências:**

*Antonopoulos*, *Andreas M.* Mastering Bitcoin. O’Reilly Media, 2013. Disponível em: <<http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#block_header>>. Acesso em: 15 nov. 2017.