Relatório sobre BlockChain

Como funciona

- O que é um Hash (SHA-256):

Um hash é uma espécie de "impressão digital" gerada a partir de dados digitais. Ele possui as seguintes características principais:
*Tamanho fixo: O hash gerado sempre tem o mesmo número de caracteres, independentemente do tamanho do dado de origem.
*Determinismo: A mesma entrada sempre produzirá o mesmo hash.
*Sensibilidade a alterações: Qualquer modificação, mesmo mínima, no conteúdo original resulta em um hash completamente diferente.
*Distribuição uniforme: Todos os hashes possíveis têm aproximadamente a mesma probabilidade de ocorrer, tornando difícil prever o resultado para um dado específico.
Exemplo:
Ao gerar o hash para a palavra "Anders", o resultado será único para essa entrada específica.

- O que é um Bloco:

É uma unidade que contém:
*Um número identificador.
*Um número aleatório chamado Nonce.
*Dados armazenados.
*O hash do bloco é calculado com base em todos esses dados.

- Como validar um bloco:

Para que seja considerado válido, seu hash deve atender alguma condição.
Exemplo: começar com um número específico de zeros.

- Mineração do bloco:

É o ajuste do Nonce até que o hash atenda ao critério de validade.

- O que é uma Blockchain:

Uma blockchain é uma cadeia de blocos, onde:
Cada bloco possui um hash que referencia o bloco anterior.
O primeiro bloco (gênesis) não tem um hash anterior válido, sendo definido como zeros.

- Proteção do bloco:

Alterar um bloco invalida todos os subsequentes, pois o hash do bloco modificado muda, quebrando os links da cadeia.
Para corrigir, seria necessário recalcular os hashes de todos os blocos seguintes.
Além disso, a alteração precisaria ser aceita pela maioria dos nós da rede, tornando o processo ainda mais difícil conforme a cadeia cresce.

- Blockchain Distribuída:

Cada nó (ou peer) na rede possui uma cópia completa da blockchain.
Alterações ilegítimas em uma cópia podem ser detectadas ao comparar com as cópias dos outros nós.

Chaves públicas e privadas / assinatura

- O que são Chaves Públicas e Privadas

Chave privada: Um número muito grande e aleatório, mantido em sigilo. É essencial para a segurança do sistema.
Chave pública: Derivada da chave privada e pode ser compartilhada. Não permite deduzir a chave privada.

- Assinaturas de Mensagens:

A mensagem é enviada junto com a assinatura gerada pela chave privada do remetente. A validação é feita com a chave pública do remetente, comprovando a autoria e a integridade da mensagem.

- Exemplo de Assinatura de Transação:

Estrutura da mensagem:
Origem: Chave pública do remetente.
Destino: Chave pública do destinatário.
Valor: Quantia transferida.
Assinatura:
A chave privada do remetente gera uma assinatura vinculada à mensagem.
Validação:
A assinatura é verificada com a chave pública do remetente.

- Proteção na Blockchain

Qualquer alteração na mensagem invalida a assinatura desta.
Apenas o proprietário da chave privada pode assinar transações associadas ao seu saldo.
Alterações em uma transação invalidam sua assinatura.
Mineradores não podem recriar assinaturas válidas para transações adulteradas.