## 1.Blockchain

A estrutura de dados em Blockchain é a base sobre a qual essa tecnologia é construída. Ela envolve a sequencialização das transações e a maneira como elas são agrupadas em blocos interconectados, formando uma cadeia imutável. Essa organização permite que cada transação seja rastreada e verificada de maneira confiável, desde a sua origem até o estado atual da Blockchain.

### 1.2 Cadeia de blocos

Na tecnologia Blockchain, os blocos são unidades fundamentais que compõem a estrutura de dados. Eles são responsáveis por armazenar informações sobre transações e eventos ocorridos na rede. Cada bloco contém um conjunto de dados, como transações, timestamps e outras informações relevantes, que são registradas de forma sequencial.

Cada bloco é conectado ao bloco anterior e ao bloco seguinte por meio de um mecanismo de referência, formando assim uma cadeia de blocos, daí o nome "Blockchain". Essa cadeia imutável de blocos permite que as transações sejam registradas de maneira ordenada e rastreável, garantindo a integridade e a confiabilidade das informações armazenadas.

**Quando um novo bloco é adicionado à Blockchain, ele recebe um identificador único chamado de hash**. O hash é gerado por meio de um algoritmo criptográfico que transforma os dados do bloco em uma sequência alfanumérica única. Esse hash serve como uma espécie de "impressão digital" do bloco, permitindo que qualquer alteração nos dados seja facilmente identificada.

Cada bloco contém o hash do bloco anterior. Essa referência ao bloco anterior cria uma conexão contínua entre os blocos, formando a cadeia de blocos. Essa estrutura é projetada de forma que, se houver uma tentativa de alterar os dados de um bloco, isso resultará em mudanças nos hashes subsequentes, tornando a alteração visível e invalidando a integridade da Blockchain.

Essa estrutura de blocos interligados em uma cadeia permite a verificação e validação das transações por toda a rede. Cada nó participante da Blockchain possui uma cópia da cadeia de blocos completa e pode verificar se os blocos e as transações são válidos seguindo as regras e os algoritmos de consenso estabelecidos.

### 1.3 Registros distribuídos

A distribuição dos registros ocorre porque cada nó participante da rede possui uma cópia completa da cadeia de blocos, que contém todas as transações já realizadas. Essa cópia é atualizada e sincronizada periodicamente com os outros nós da rede.

A distribuição dos registros em Blockchain traz algumas vantagens significativas. Primeiramente, ela elimina a necessidade de um intermediário

centralizado para validar e registrar as transações. Cada nó participante verifica a validade das transações por meio de regras e algoritmos pré-definidos. Isso aumenta a transparência e reduz a dependência de terceiros confiáveis.

A distribuição dos registros em vários nós torna a rede mais resiliente a falhas e ataques. Como não há um ponto central de falha, a rede pode continuar operando mesmo se alguns nós falharem ou forem comprometidos. A integridade dos registros é protegida pela natureza imutável da cadeia de blocos, que requer um consenso da maioria dos nós para validar uma transação.

**2.Algoritmos de consenso**

Os algoritmos de consenso são responsáveis por garantir que todos os nós da rede cheguem a um acordo sobre o estado válido da cadeia de blocos. Esses algoritmos permitem que os participantes cheguem a um consenso sobre quais transações são válidas e quais blocos devem ser adicionados à cadeia.

**3.*Proof of work***

É amplamente utilizado, principalmente no contexto das criptomoedas, como o Bitcoin. Nesse algoritmo, os participantes (ou mineradores) competem para resolver um problema computacionalmente complexo, conhecido como "quebra-cabeça criptográfico" ou "hash puzzle". O primeiro participante a encontrar a solução correta é recompensado com criptomoedas e tem o direito de adicionar um novo bloco à cadeia.

Exige que os participantes dediquem uma quantidade significativa de poder computacional para resolver o problema, o que implica altos custos energéticos. A dificuldade do problema é ajustada automaticamente para manter a taxa de criação de blocos constante ao longo do tempo.

**4.*Proof of stake***

A seleção do nó que cria o próximo bloco não é baseada na capacidade computacional, mas sim na participação do nó na rede. Nesse caso, a seleção do validador é determinada pela quantidade de criptomoedas que o nó possui e bloqueou como garantia (staking). Os participantes que possuem mais moedas têm mais chances de serem escolhidos para criar blocos e validar transações.

Isso incentiva os participantes a manterem suas moedas e agirem de maneira honesta, uma vez que qualquer comportamento malicioso pode resultar na perda de suas moedas como garantia. O Proof of Stake é considerado mais eficiente em termos de consumo de energia, em comparação ao Proof of Work.

**5.Criptografia e segurança em blockchain**

A criptografia assimétrica é um dos componentes essenciais da tecnologia Blockchain. Ela desempenha um papel fundamental na segurança e na autenticação das transações na rede.

A chave privada é um número aleatório e exclusivo gerado para cada participante da rede Blockchain. Ela é mantida em sigilo absoluto e é usada para assinar digitalmente transações. A chave privada deve ser protegida, pois qualquer pessoa que tenha acesso a ela pode assumir a identidade do proprietário e realizar transações em seu nome.

A chave pública é derivada da chave privada por meio de algoritmos matemáticos específicos. Ela é compartilhada publicamente com outros participantes da rede Blockchain. A chave pública é usada para verificar a autenticidade das assinaturas digitais feitas com a chave privada correspondente.

Na tecnologia Blockchain, a função hash é usada para garantir a integridade e a segurança das informações. Quando uma transação é registrada em um bloco, todos os dados relevantes da transação, como remetente, destinatário, valor e outros parâmetros, são processados pela função hash.

O resultado é um hash único que representa aquela transação específica. Qualquer alteração nos dados da transação resultará em um hash completamente diferente. A função hash é projetada de forma que seja computacionalmente inviável reverter o processo e obter os dados originais a partir do hash.

Qualquer modificação em um bloco anterior resultará em uma mudança no hash, o que invalidará toda a cadeia subsequente.

**6.Verificação de assinatura**

Para verificar a autenticidade de uma transação, os nós da rede Blockchain utilizam a chave pública correspondente ao endereço do remetente para verificar se a assinatura digital é válida. Isso é feito aplicando os algoritmos criptográficos à transação, à assinatura digital e à chave pública. Se a assinatura digital puder ser validada com sucesso, significa que a transação foi assinada com a chave privada correspondente à chave pública fornecida.