1.Introdução à blockchain

1.1 Estrutura de dados em 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 Blocos e 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.

A cadeia de blocos, por ser distribuída em múltiplos nós, torna-se altamente resistente a ataques e falhas únicas, pois exigiria a alteração simultânea e consensual de uma grande quantidade de cópias da cadeia para comprometer sua segurança.

1.3 Transações e registros distribuídos

As transações e registros distribuídos referem-se à maneira como as informações são compartilhadas e registradas de forma descentralizada em uma rede de nós. Uma transação em Blockchain é uma ação ou evento que ocorre na rede e que é registrada na cadeia de blocos.

Pode ser a transferência de criptomoedas, a execução de um contrato inteligente, o registro de um ativo ou qualquer interação que envolva a troca ou alteração de dados. As transações são registradas em blocos e possuem informações relevantes, como o remetente, o destinatário, o valor envolvido e outros detalhes específicos de cada tipo de transação.

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.

Dessa forma, todas as transações são compartilhadas e propagadas por toda a rede, tornando-as visíveis e acessíveis a todos os participantes.

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.

Outra vantagem da distribuição dos registros é a capacidade de auditoria e rastreabilidade. Como todas as transações são registradas e compartilhadas, é possível rastrear o histórico completo de uma transação desde o seu início até o estado atual. Isso é especialmente valioso em setores como a cadeia de suprimentos, onde é importante acompanhar a origem e o trajeto de um produto.

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.

Existem diferentes tipos de algoritmos de consenso utilizados em Blockchain, sendo os mais conhecidos descritos a seguir.

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.

Esse algoritmo é seguro, pois torna computacionalmente inviável reverter ou modificar blocos anteriores, uma vez que seria necessário recalcular todos os blocos subsequentes.

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.

Além disso, ele permite uma maior escalabilidade da rede, uma vez que a seleção do validador não depende do poder computacional, mas sim da participação financeira.

Além desses dois algoritmos, existem também outras variações e abordagens, como o Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), entre outros. Cada algoritmo de consenso tem suas próprias características e é escolhido com base nos requisitos e nas necessidades específicas da rede Blockchain em questão.

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.

5.1 Chave privada

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.

5.2 Chave pública

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.

5.3 Função hash

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.

Além disso, a função hash é determinística, o que significa que a mesma entrada sempre produzirá o mesmo hash. Na Blockchain, os hashes são usados para estabelecer a integridade dos blocos e criar uma conexão contínua entre eles. Cada bloco contém o hash do bloco anterior, formando uma cadeia de blocos.

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

5.4 Assinaturas digitais

Para realizar uma transação em Blockchain, o remetente utiliza sua chave privada para criar uma assinatura digital exclusiva para aquela transação específica. A assinatura digital é um valor criptográfico gerado pela aplicação de algoritmos à transação e à chave privada. Ela comprova que a transação foi realmente autorizada pelo proprietário da chave privada.

5.5 Verificação da 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.

6.Proteção da privacidade

A criptografia de chave pública e privada também é usada para proteger a privacidade dos participantes na rede Blockchain. Quando um participante deseja receber uma transação, ele compartilha sua chave pública com o remetente para que a transação seja criptografada e direcionada especificamente para ele. Somente o destinatário, com a posse da chave privada correspondente, poderá descriptografar e acessar o conteúdo da transação.

7.Tipos de blockchain

Existem diferentes tipos de Blockchain, cada um com suas características e implementações específicas.

7.1 Blockchain pública

A Blockchain Pública é um tipo de Blockchain descentralizada que permite a participação aberta e a transparência completa para qualquer pessoa que queira se envolver. Neste tipo de Blockchain, qualquer usuário pode participar como um nó na rede, realizar transações e verificar a integridade da cadeia de blocos.

Os principais componentes ou características são:

- **Participantes:** Na Blockchain Pública, qualquer pessoa pode participar como um nó na rede. Cada nó tem uma cópia completa da cadeia de blocos e ajuda a validar e confirmar as transações. Os participantes podem ser chamados de mineradores, validadores ou nós, dependendo do protocolo específico da Blockchain.
- **Transações:** Os usuários da Blockchain Pública podem criar e enviar transações para a rede. Uma transação contém informações, como o remetente, o destinatário e o valor a ser transferido. Antes de ser adicionada à Blockchain, a transação precisa ser verificada e validada pelos nós da rede.
- **Consenso:** Para garantir que todos os participantes cheguem a um consenso sobre o estado válido da cadeia de blocos, a Blockchain Pública usa algoritmos de consenso, como o Proof of Work (PoW) ou o Proof of Stake (PoS). Esses algoritmos asseguram que os nós concordem sobre quais transações são válidas e quais blocos devem ser adicionados à cadeia.
- **Mineração:** No caso do PoW, a mineração é o processo pelo qual os participantes (mineradores) competem para resolver um problema computacionalmente complexo. Esse processo envolve a solução de um quebra-cabeça criptográfico, e o primeiro participante a encontrar a solução

correta tem o direito de adicionar um novo bloco à cadeia. A mineração é recompensada com criptomoedas e incentiva a segurança e a integridade da rede.

- **Confirmação de transações:** Após a mineração de um novo bloco, as transações contidas nesse bloco são confirmadas e consideradas válidas. O bloco é adicionado à cadeia de blocos existente e distribuído para todos os nós da rede. Essa confirmação garante que as transações sejam registradas de forma imutável e permanente na Blockchain.
- **Auditoria e transparência:** Devido à natureza pública da Blockchain, todas as transações e blocos são visíveis para todos os participantes da rede. Isso permite uma auditoria transparente, pois qualquer pessoa pode verificar a validade e a integridade das transações e acompanhar o histórico completo de transações.
- **Segurança:** A segurança da Blockchain Pública é garantida pela descentralização e pelo consenso distribuído entre os nós da rede. Como cada nó tem uma cópia da cadeia de blocos e valida as transações, é extremamente difícil comprometer a segurança da rede, tornando-a resistente a ataques maliciosos.

7.2 Blockchain privada

É um tipo de Blockchain que é operada e controlada por uma única organização ou um grupo restrito de organizações. Diferente da Blockchain Pública, onde qualquer pessoa pode participar, a Blockchain Privada limita o acesso e as permissões aos participantes autorizados.

Funciona com os seguintes componentes e características:

- **Participantes:** Na Blockchain Privada, o acesso à rede é restrito apenas aos participantes autorizados. Esses participantes podem ser organizações, instituições financeiras, empresas ou indivíduos específicos. O número de participantes é geralmente menor do que em uma Blockchain Pública.
- **Permissões:** A Blockchain Privada impõe restrições de acesso e permissões para ler, escrever e validar as transações. Isso é alcançado por meio de mecanismos de autenticação e controle de acesso. Os participantes autorizados são identificados e verificados antes de serem concedidas as permissões necessárias.
- **Governança:** A governança da Blockchain Privada é definida pela organização ou pelas organizações responsáveis pela operação da rede. As regras e os protocolos que governam o funcionamento da Blockchain são estabelecidos internamente e podem variar de acordo com os requisitos e objetivos

específicos da organização. A governança inclui aspectos como a definição de consenso, atualizações de software, políticas de segurança e resolução de disputas.

- **Consenso:** Para chegar a um consenso sobre as transações na Blockchain Privada, diferentes algoritmos de consenso podem ser implementados. Além dos algoritmos tradicionais, como o Proof of Work (PoW) ou Proof of Stake (PoS), outros mecanismos de consenso, como votação, algoritmos de confiança ou algoritmos personalizados, podem ser utilizados. A escolha do algoritmo de consenso depende dos requisitos de segurança, escalabilidade e eficiência da organização.
- **Escalabilidade:** A Blockchain Privada geralmente é projetada para ter melhor escalabilidade em comparação com as Blockchains Públicas. Como o número de participantes é menor e a rede é controlada internamente, a comunicação e a coordenação podem ser mais eficientes. Isso permite um processamento mais rápido das transações e uma maior capacidade de lidar com um volume maior de dados.
- **Privacidade:** As informações compartilhadas na rede são visíveis apenas para os participantes autorizados. Diferentes mecanismos de criptografia e compartilhamento seletivo de dados podem ser utilizados para garantir a confidencialidade das transações. Isso é especialmente relevante em setores onde informações sensíveis são envolvidas, como saúde, finanças e negócios.
- **Casos de uso:** A Blockchain Privada é frequentemente adotada por empresas e organizações que desejam ter controle total sobre sua rede, dados e processos. Ela pode ser aplicada em diversos casos de uso, como cadeia de suprimentos, gerenciamento de ativos, registros de propriedade, votações eletrônicas e muito mais.

7.3 Blockchain de consórcio ou federada

É um tipo de Blockchain que combina características das Blockchains pública e privada. Nesse modelo, a rede é operada e controlada por um consórcio de várias organizações em vez de ser aberta a qualquer pessoa.

Abaixo, como funciona a Blockchain de Consórcio ou Federada:

- **Participantes do consórcio:** Envolve um grupo de organizações que estabelecem uma parceria para operar a rede. Cada organização no consórcio possui um ou mais nós na Blockchain e compartilha a responsabilidade pela governança e operação da rede. Essas organizações podem ser instituições financeiras, empresas de tecnologia, organizações governamentais ou qualquer outro conjunto de empresas com interesses comuns.

- **Permissões de acesso:** Diferentemente de uma Blockchain pública, a Blockchain de Consórcio ou Federada restringe o acesso à rede. A participação é limitada aos membros do consórcio que foram autorizados e concedidos permissões para acessar e interagir com a rede. Isso permite um controle maior sobre a segurança e a privacidade dos dados, uma vez que apenas participantes confiáveis têm acesso à rede.
- **Governança:** É estabelecido um modelo de governança que define as regras, os protocolos e os processos de operação da rede. Os membros do consórcio colaboram na tomada de decisões relacionadas à governança da Blockchain, como a definição de políticas de atualização, adição de novos participantes e resolução de conflitos. Esse modelo de governança é acordado entre os participantes do consórcio.
- **Consenso:** Para chegar a um consenso sobre as transações e a validade dos blocos na Blockchain de Consórcio, diferentes algoritmos de consenso podem ser utilizados. Alguns dos algoritmos de consenso comuns incluem o Proof of Authority (PoA), onde um conjunto predefinido de nós confiáveis é responsável por validar as transações, e o Practical Byzantine Fault Tolerance (PBFT), que envolve um processo de votação entre os nós participantes.
- **Confiança interorganizacional:** Visa estabelecer confiança e colaboração entre as organizações participantes. Por meio da tecnologia Blockchain, as transações são registradas de forma imutável e transparente, permitindo que todas as partes confiem nos registros compartilhados. Isso pode facilitar a redução de intermediários, o compartilhamento eficiente de informações e a automação de processos entre as organizações do consórcio.
- **Privacidade dos dados:** Embora os dados da transação sejam compartilhados entre os membros do consórcio, mecanismos de criptografia e compartimentalização podem ser implementados para garantir que determinadas informações permaneçam privadas e sejam acessíveis apenas por partes autorizadas.
- **Benefícios da colaboração:** Ao unir forças em um consórcio Blockchain, as organizações participantes podem aproveitar os benefícios da colaboração, como a redução de custos, a melhoria da eficiência operacional, a otimização de processos e a criação de novos modelos de negócios. Permite que as organizações compartilhem dados e recursos de forma confiável e segura, criando oportunidades para inovação e parcerias estratégicas.

8.Carteira de criptomoedas

Uma carteira digital de criptomoedas é um software ou um serviço que permite aos usuários armazenar, gerenciar e interagir com suas criptomoedas. Ela funciona

com base em um par de chaves criptográficas: uma chave privada e uma chave pública.

Explorando em detalhes como uma carteira digital de criptomoedas funciona:

- **Chave privada:** É uma sequência alfanumérica criptograficamente segura que serve como a identidade e a assinatura digital do proprietário da carteira. Essa chave é gerada aleatoriamente e deve ser mantida em sigilo absoluto, pois é a única forma de acesso e controle dos ativos na carteira.
- **Chave pública:** A chave pública é derivada da chave privada por meio de algoritmos criptográficos. Ela é compartilhada publicamente e serve como o endereço da carteira, permitindo que outras pessoas enviem criptomoedas para a carteira do usuário.
- **Carteiras de software:** Aplicativos ou programas instalados em dispositivos como computadores, smartphones ou tablets. Elas permitem ao usuário armazenar e acessar suas criptomoedas por meio de uma interface amigável.
- **Carteiras de hardware:** Dispositivos físicos especialmente projetados para armazenar chaves privadas offline, oferecendo maior segurança contra ataques cibernéticos. Essas carteiras geralmente possuem recursos adicionais de autenticação e criptografia para proteger as chaves privadas.
- **Carteiras online:** Serviços baseados na nuvem que armazenam as chaves privadas em servidores controlados por terceiros. Embora sejam convenientes para acessar as criptomoedas de qualquer dispositivo conectado à internet, as carteiras online podem ser vulneráveis a riscos de segurança associados a terceiros.
- **Carteiras de papel:** Representações físicas das chaves privadas impressas em papel. Essas carteiras são altamente seguras, pois não estão conectadas à internet, mas requerem precauções adicionais para proteger o papel físico de danos e acesso não autorizado.
- **Recebimento e envio de criptomoedas:** Com uma carteira digital, os usuários podem receber criptomoedas enviando sua chave pública para o remetente. A transação é registrada na Blockchain e os fundos são adicionados ao saldo da carteira. Da mesma forma, para enviar criptomoedas, o usuário insere o endereço de destino e assina a transação com sua chave privada. Essa assinatura garante a autenticidade da transação e permite que ela seja registrada na Blockchain.
- **Segurança:** A segurança é uma consideração crítica ao utilizar uma carteira digital de criptomoedas. Os usuários devem manter sua chave privada segura e protegida, evitando compartilhá-la com outras pessoas ou armazená-la em

dispositivos comprometidos. Recomenda-se utilizar autenticação de dois fatores (2FA) e criptografia de dispositivo para proteger a carteira digital contra acesso não autorizado.