Módulo 9 - Aulas 3 e 4

Módulo 9: Infraestrutura de Chaves Públicas e Blockchain

Aula 3: Gerenciamento de Infraestrutura de Chaves Públicas (PKI)

Objetivos

- [ ] Compreender os princípios e práticas do Gerenciamento de Certificados e Chaves.
- [ ] Explorar as estratégias de Recuperação de Chaves e Custódia.
- [ ] Identificar os desafios e as melhores práticas no Gerenciamento de Certificados.

Conceitos

- [ ] Gerenciamento de Certificados e Chaves.
- [ ] Recuperação de Chaves e Custódia.
- [ ] Expiração de Certificados.

Introdução

O primeiro tópico tratado é o Gerenciamento de Certificados e Chaves, que abrange a criação, emissão, renovação e revogação de certificados digitais, além do armazenamento seguro das chaves privadas associadas. Serão discutidas práticas recomendadas para garantir a integridade e a confidencialidade desses elementos cruciais para a segurança de uma infraestrutura. Outro tema relevante é

a Recuperação e Custódia de Chaves, abordando estratégias para recuperar chaves privadas perdidas ou corrompidas. Também serão apresentados métodos de armazenamento seguro das chaves, como o uso de hardware especializado.

Durante a aula, serão ainda explorados assuntos como a expiração de certificados, listas de revogação de certificados, os protocolos de resposta de status de certificado online, o conceito de *pinning* de certificados, os diferentes formatos de certificados, bem como o uso prático da ferramenta OpenSSL. Com uma compreensão aprofundada desses tópicos, os participantes estarão preparados para enfrentar desafios comuns no gerenciamento de PKI e garantir a segurança e a confiabilidade das comunicações digitais.

PKI.

Gerenciamento de chaves

O Gerenciamento de Chaves em uma PKI (Infraestrutura de Chaves Públicas) envolve a administração e o controle das chaves de criptografia utilizadas em certificados digitais. As chaves desempenham um papel essencial na segurança da comunicação e na autenticação de entidades em uma infraestrutura baseada em PKI.

Ciclo de vida das chaves

O ciclo de vida das chaves em uma PKI é composto por várias etapas, que incluem:

1. Geração das Chaves: Nessa etapa, as chaves criptográficas são geradas de forma segura. Uma chave privada é criada e associada a uma chave pública correspondente. A chave privada deve ser mantida em segredo e protegida adequadamente, enquanto a chave pública pode ser compartilhada livremente.
2. Solicitação e Emissão de Certificados: Após a geração das chaves, é feita uma solicitação de certificado digital que inclui a chave pública. A solicitação é enviada a uma Autoridade Certificadora (AC) confiável, que valida a identidade do solicitante e emite um certificado contendo a chave pública e outras informações relevantes.
3. Armazenamento e Proteção: O armazenamento seguro das chaves privadas é crucial para evitar o acesso não autorizado. Recomenda-se o uso de dispositivos de segurança, como HSMs (Módulos de Segurança de Hardware) ou smart cards, para proteger as chaves privadas. Além disso, é importante implementar controles adequados de acesso e realizar backups regulares das chaves.
4. Renovação e Atualização: Os certificados digitais têm uma validade limitada, geralmente de um a três anos. Durante esse período, é necessário acompanhar a expiração dos certificados e realizar sua renovação antes que se tornem inválidos. Isso envolve a geração de uma nova solicitação de certificado e a substituição do certificado anterior pela nova versão.
5. Revogação: Em certas situações, um certificado digital pode se tornar comprometido ou não confiável antes de sua data de expiração. Nesses casos, é necessário revogar o certificado para indicar que ele não deve mais ser considerado válido. A revogação pode ocorrer por motivos como perda da chave privada, suspeita de comprometimento ou cessação de associação com uma organização.
6. Destruição: Quando um certificado digital não é mais necessário ou quando a chave privada associada é comprometida, é fundamental garantir sua destruição adequada. Isso evita o uso indevido da chave privada e garante a segurança contínua da infraestrutura.

O Gerenciamento de Chaves em uma PKI é essencial para garantir a confidencialidade, integridade e autenticidade das comunicações e transações digitais. Ao seguir corretamente as etapas do ciclo de vida das chaves, é possível manter um ambiente seguro e confiável para o uso de certificados digitais.

Chave.

Tipos de gerenciamento de chave

O gerenciamento de chaves pode ser realizado de forma centralizada ou descentralizada:

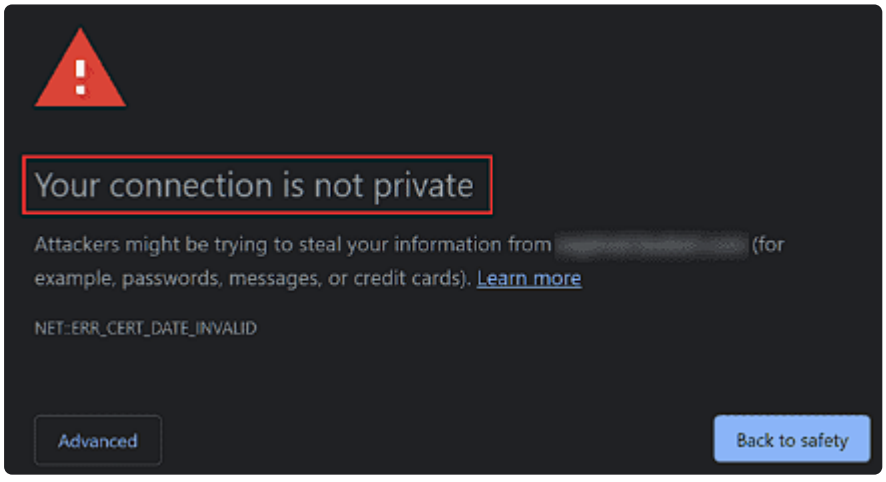
- Gerenciamento de Chaves Centralizado: Nesse modelo, todas as chaves de criptografia são armazenadas e gerenciadas em um único local centralizado. Geralmente, isso é feito por uma entidade central, como uma Autoridade Certificadora (CA) ou um servidor de chaves dedicado. Todas as solicitações de certificados e operações relacionadas às chaves são direcionadas a esse ponto central, o que permite um controle mais rigoroso e padronizado sobre as chaves e os certificados. O gerenciamento centralizado facilita a aplicação de políticas de segurança e garante a conformidade com os padrões estabelecidos.
- Gerenciamento de Chaves Descentralizado: Nesse modelo, as chaves de criptografia são distribuídas e gerenciadas em diversos locais ou sistemas independentes. Cada entidade ou sistema pode gerar suas próprias chaves e certificados, sem depender de uma autoridade central. Isso proporciona uma maior autonomia e flexibilidade, permitindo que cada entidade tenha controle

total sobre suas chaves e certificados. No entanto, o gerenciamento descentralizado pode apresentar desafios em termos de coordenação e conformidade, uma vez que não há uma única autoridade central responsável pelo controle e pela aplicação de políticas de segurança.

Vulnerabilidades no gerenciamento de certificados

Se o gerenciamento de certificados e chaves não for realizado de maneira adequada, várias vulnerabilidades podem surgir, comprometendo a segurança e a confiabilidade de uma infraestrutura de chaves públicas:

- Exposição de Chaves Privadas: Se as chaves privadas forem mal protegidas ou armazenadas em locais não seguros, elas podem ser facilmente acessadas por indivíduos não autorizados. Isso pode levar à divulgação de informações sensíveis, como dados criptografados, comunicações privadas ou até mesmo a possibilidade de falsificação de identidade.
- Certificados Inválidos ou Comprometidos: Se os certificados digitais forem emitidos de forma inadequada ou se os processos de autenticação e verificação forem insuficientes, certificados inválidos ou comprometidos podem ser aceitos como válidos. Isso pode permitir que atacantes obtenham acesso não autorizado a sistemas ou dados confidenciais.



Certificado inválido.

- Falta de Revogação de Certificados: A revogação de certificados é essencial para invalidar certificados que foram comprometidos, perdidos ou não são mais confiáveis. Se os certificados não forem revogados corretamente e as listas de revogação não forem atualizadas, os sistemas podem continuar a confiar em

certificados inválidos, permitindo a ocorrência de ataques e violações de segurança.

Revogação de certificados.

- Falha na Renovação de Certificados: Se os certificados não forem renovados antes de sua expiração, sistemas e serviços dependentes desses certificados podem deixar de funcionar. A expiração de um certificado pode resultar em interrupções de serviços, negação de acesso ou até mesmo a necessidade de reimplantar toda a infraestrutura de chaves públicas.
- Uso de Algoritmos e Parâmetros Obsoletos: Se não houver uma política adequada de atualização e acompanhamento dos algoritmos e parâmetros de criptografia utilizados nos certificados e chaves, podem surgir vulnerabilidades devido a algoritmos fracos ou obsoletos. Isso pode permitir a exploração de ataques criptográficos avançados e comprometer a segurança dos sistemas.
- Falta de Monitoramento e Auditoria: A ausência de monitoramento adequado das atividades relacionadas a certificados e chaves pode dificultar a detecção de atividades suspeitas ou anômalas. A falta de auditoria pode levar a atrasos na identificação de problemas de segurança, aumentando o risco de violações de dados ou ataques cibernéticos.

Controle de acesso a chaves

O controle M de N de acesso a chaves é um mecanismo de segurança que visa garantir a proteção das chaves privadas em uma infraestrutura de chaves públicas (PKI). Esse mecanismo é projetado para impedir o acesso não autorizado às chaves privadas, exigindo a participação de várias entidades ou partes confiáveis para desbloquear o acesso às chaves. No controle M de N, "M" representa o número mínimo de entidades ou partes necessárias para desbloquear as chaves privadas, e

"N" é o número total de entidades ou partes envolvidas. Por exemplo, em um controle 2 de 3 (2 de 3), pelo menos duas das três entidades autorizadas devem concordar e participar para desbloquear as chaves privadas.

Esse mecanismo de controle é implementado dividindo a chave privada em partes e atribuindo essas partes a diferentes entidades ou partes confiáveis. Cada parte da chave privada é mantida em sigilo e protegida separadamente. Quando é necessário usar a chave privada, um procedimento de combinação é realizado, reunindo as partes mantidas pelas entidades autorizadas para desbloquear a chave e permitir seu uso. O controle M de N oferece uma camada adicional de segurança, pois requer o envolvimento e a concordância de múltiplas entidades ou partes para acessar as chaves privadas. Isso torna mais difícil para um indivíduo ou entidade mal-intencionada obter acesso não autorizado a uma chave privada, pois seria necessário comprometer várias partes mantidas por entidades diferentes.

Esse mecanismo é comumente usado em ambientes de alto risco, onde a proteção das chaves privadas é uma prioridade, como instituições financeiras, governamentais ou militares. O controle M de N ajuda a mitigar os riscos associados a uma única entidade ter acesso completo e exclusivo às chaves privadas, proporcionando uma abordagem mais robusta e distribuída para a proteção das chaves em uma PKI.

Custódia de Chaves

A Custódia de Chaves, também conhecida como Key Escrow em inglês, consiste em um mecanismo pelo qual uma cópia das chaves privadas é armazenada em um local seguro e confiável, geralmente fora da organização ou entidade que as utiliza. A ideia por trás da Custódia de Chaves é garantir que, em caso de perda, corrupção ou comprometimento das chaves privadas originais, uma cópia de segurança possa ser recuperada e utilizada para recuperar o acesso aos certificados digitais associados.

A entidade ou organização que detém a Custódia de Chaves é geralmente uma terceira parte confiável, como uma Autoridade Certificadora (AC) ou uma agência governamental. Essa entidade possui os meios e os procedimentos para proteger e armazenar as chaves privadas de forma segura. A Custódia de Chaves pode ser vista como uma medida de segurança adicional para mitigar o risco de perda

completa das chaves privadas, garantindo a disponibilidade contínua dos certificados digitais em caso de problemas. No entanto, é importante notar que a Custódia de Chaves também pode gerar preocupações em relação à privacidade e à segurança, uma vez que envolve confiar a terceiros o acesso às chaves privadas.

Custódia de chaves.

Gerenciamento de certificados

Gerenciamento de certificados refere-se ao conjunto de práticas e processos utilizados para administrar certificados digitais em uma infraestrutura de chaves públicas (PKI). Isso inclui a geração, emissão, renovação, revogação, expiração e armazenamento seguro de certificados, garantindo a autenticidade, integridade e confidencialidade das informações transmitidas por meio de criptografia de chave pública.

Geração de certificados

A geração de certificados digitais em uma Infraestrutura de Chaves Públicas (PKI) envolve várias etapas e processos:

1. Solicitação de Certificado: O primeiro passo é a solicitação de um certificado por parte de um usuário ou entidade. Essa solicitação pode ser feita por meio de um formulário online, por um software específico ou até mesmo manualmente, dependendo da implementação da PKI.
2. Criação do Par de Chaves: Após receber a solicitação de certificado, é gerado um par de chaves criptográficas, composto por uma chave privada e uma chave pública. A chave privada é mantida em sigilo e é usada para assinar e

descriptografar dados, enquanto a chave pública é incluída no certificado e pode ser distribuída para outros usuários.

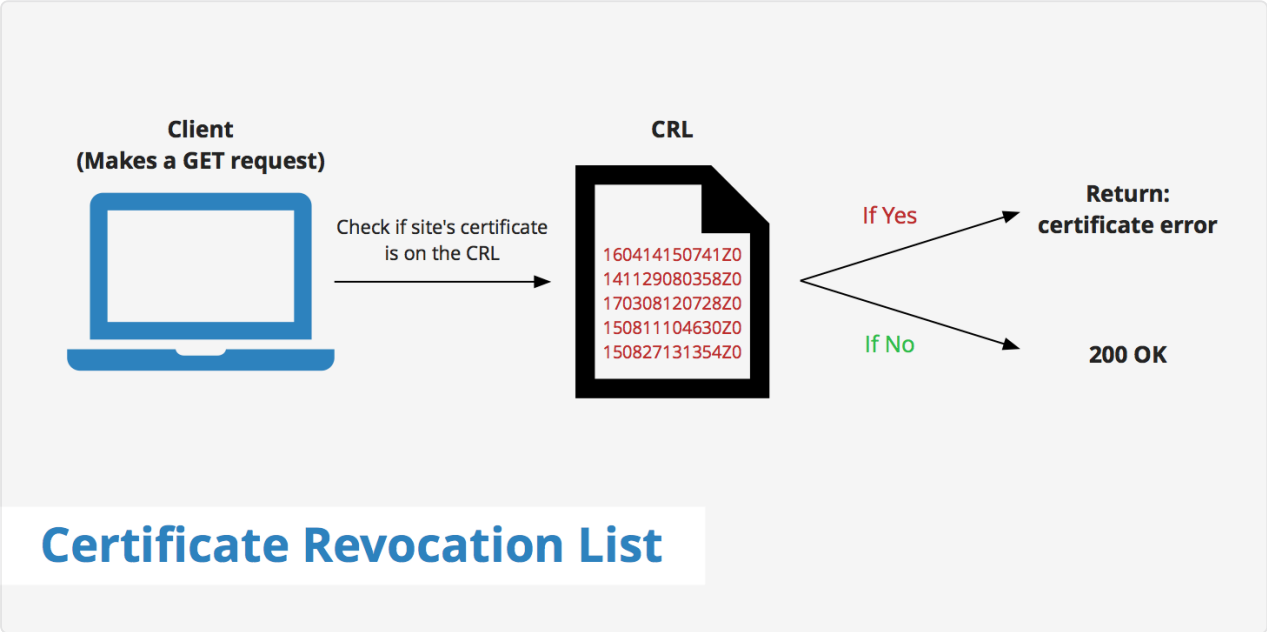
3. Preenchimento dos Dados do Certificado: Com o par de chaves criado, os dados do certificado são preenchidos. Esses dados geralmente incluem informações como o nome do titular do certificado, a entidade emissora, o período de validade, o uso pretendido do certificado e outras informações relevantes.
4. Assinatura Digital: A próxima etapa é a assinatura digital do certificado. A chave privada do emissor é usada para assinar digitalmente o certificado, garantindo a autenticidade e a integridade dos dados. Essa assinatura digital é uma prova de que o certificado foi emitido por uma entidade confiável.
5. Emissão do Certificado: Após a assinatura digital, o certificado é emitido e disponibilizado para o solicitante. O certificado contém a chave pública, os dados do titular, a assinatura digital e outras informações relevantes necessárias para validar a autenticidade do certificado.

Revogação de certificados e Lista de Revogação de Certificados (CRL)

A revogação de certificados digitais ocorre quando um certificado é comprometido, suspeito de ter sido comprometido, possui informações incorretas ou quando o titular do certificado deixa de ser autorizado a utilizá-lo. O processo de revogação de certificados na PKI envolve os seguintes passos:

1. Identificação da necessidade de revogação: A entidade emissora ou uma autoridade competente identifica que um certificado precisa ser revogado. Isso pode ocorrer em casos de comprometimento da chave privada, violação de políticas de segurança, cessação de emprego de um titular de certificado, entre outros motivos.
2. Publicação da Lista de Revogação de Certificados (CRL): A entidade emissora gera uma Lista de Revogação de Certificados (CRL), que é um arquivo ou uma publicação online que contém informações sobre os certificados revogados. A CRL lista os números de série dos certificados revogados, juntamente com outras informações relevantes, como a data e o motivo da revogação.
3. Distribuição e Atualização da CRL: A CRL é então distribuída e disponibilizada para os usuários e entidades que dependem da PKI para verificação de certificados. Os usuários devem periodicamente consultar a CRL para verificar se o certificado que estão utilizando foi revogado. A CRL também deve ser atualizada regularmente para incluir novos certificados revogados e remover certificados que tenham expirado.

4. Verificação da Revogação: Os usuários que dependem de certificados digitais devem verificar a revogação de um certificado antes de confiar nele. Eles consultam a CRL para verificar se o número de série do certificado que estão utilizando consta na lista de certificados revogados. Caso o certificado esteja presente na CRL, o usuário deve considerá-lo inválido e tomar as medidas apropriadas.



CRL.

Online Certificate Status Protocol (OCSP)

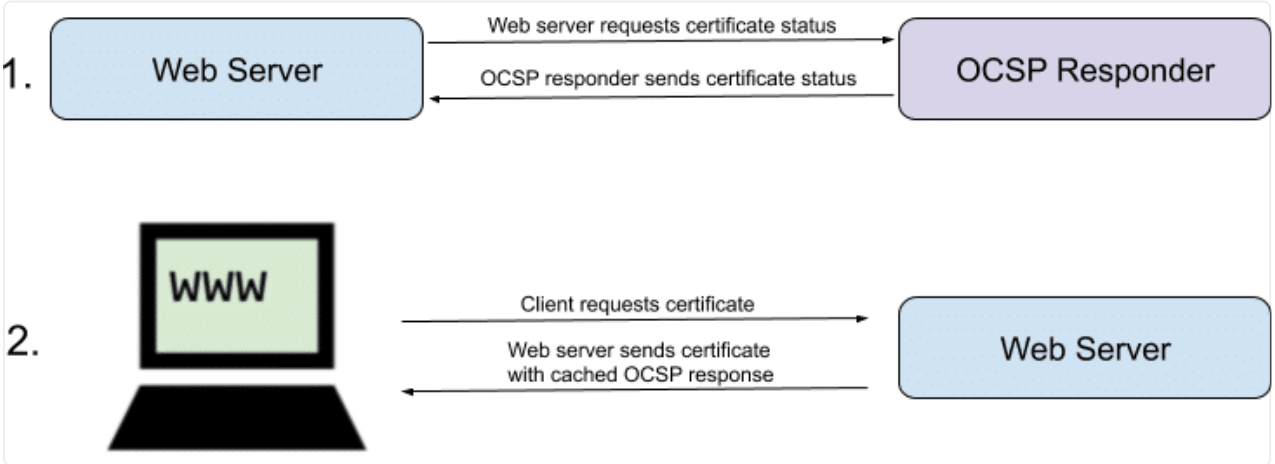
É um protocolo utilizado em uma Infraestrutura de Chaves Públicas (PKI) para verificar em tempo quase real o status de revogação de um certificado digital. Em vez de depender de uma Lista de Revogação de Certificados (CRL) estática, o OCSP permite uma verificação mais dinâmica e eficiente. O funcionamento do OCSP envolve os seguintes passos:

- Solicitação OCSP: Quando um usuário precisa verificar o status de revogação de um certificado, ele envia uma solicitação OCSP para um servidor OCSP. Essa solicitação contém informações sobre o certificado que está sendo verificado, como seu número de série.
- Resposta OCSP: O servidor OCSP recebe a solicitação e consulta sua base de dados para verificar se o certificado está revogado ou válido. Em seguida, ele emite uma resposta OCSP ao solicitante.
-

Resposta OCSP ao Solicitante: A resposta OCSP pode ter diferentes resultados. Se o certificado estiver revogado, a resposta OCSP indicará o status de revogação, juntamente com informações adicionais, como a data e o motivo da revogação. Se o certificado estiver válido, a resposta indicará que o certificado não está revogado.

- Validação do Certificado: Com base na resposta OCSP, o solicitante pode validar o certificado. Se a resposta indicar que o certificado está revogado, o solicitante deve considerá-lo inválido e tomar as medidas apropriadas. Se a resposta indicar que o certificado está válido, o solicitante pode confiar nele para estabelecer uma comunicação segura.

Vale a pena ressaltar que o OCSP oferece vantagens em relação às CRLs tradicionais, pois permite uma verificação em tempo real do status de revogação. Isso é particularmente útil em ambientes onde a revogação de certificados ocorre com frequência, pois evita a necessidade de baixar e verificar CRLs grandes e frequentemente atualizadas.



OCSP.

Fixação de Certificado (Certificate Pinning)

É uma medida de segurança utilizada para garantir a autenticidade e a integridade dos certificados digitais durante uma comunicação segura. Ela impede que certificados não autorizados ou falsificados sejam aceitos, reduzindo o risco de ataques de intermediário mal-intencionado (man-in-the-middle) e outros tipos de ataques. Funciona da seguinte maneira:

1. Seleção de Certificados: Durante o processo de desenvolvimento de um aplicativo ou configuração de um servidor, são selecionados um ou mais certificados confiáveis para estabelecer a comunicação segura. Esses certificados são escolhidos com base em sua autenticidade, validade e confiabilidade.
2. Armazenamento de Informações de Identificação: As informações de identificação dos certificados selecionados são armazenadas no aplicativo ou no servidor. Isso pode incluir o número de série do certificado, seu hash criptográfico ou outras informações que permitam identificar de forma exclusiva o certificado.
3. Verificação de Certificados: Durante a comunicação segura, quando uma conexão é estabelecida com o servidor remoto, o cliente verifica o certificado apresentado pelo servidor. Em vez de confiar apenas nas autoridades de certificação (CAs) padrão do sistema, o cliente compara o certificado apresentado com as informações de identificação armazenadas.
4. Comparação e Validação: O cliente compara as informações de identificação do certificado apresentado com as informações de identificação armazenadas. Se houver uma correspondência, significa que o certificado é considerado válido e confiável. Caso contrário, se não houver uma correspondência, o certificado é considerado não confiável e a conexão pode ser interrompida.

Certificate Pinning.

OpenSSL

O OpenSSL é uma biblioteca de código aberto amplamente utilizada para implementação de criptografia, incluindo o gerenciamento de certificados digitais em uma Infraestrutura de Chaves Públicas (PKI). O OpenSSL oferece diversas

funcionalidades que podem ser usadas no gerenciamento de certificados digitais, como geração de chaves, criação e assinatura de certificados, criação e verificação de assinaturas digitais, entre outras:

- Geração de chaves: O OpenSSL permite a geração de pares de chaves criptográficas, compostos por uma chave privada e uma chave pública. Com o OpenSSL, é possível gerar chaves RSA, DSA, ECDSA e outros algoritmos suportados. Essas chaves podem ser usadas para criar certificados digitais.
- Criação e assinatura de certificados: O OpenSSL possui ferramentas que permitem a criação de certificados digitais, como o comando "openssl req". Com esse comando, é possível gerar uma solicitação de certificado (CSR) contendo informações sobre o solicitante. Em seguida, o OpenSSL também permite assinar digitalmente essa solicitação para gerar um certificado válido.
- Criação e verificação de assinaturas digitais: O OpenSSL oferece suporte a diferentes algoritmos de assinatura digital, como RSA e ECDSA. Com o OpenSSL, é possível criar assinaturas digitais de arquivos ou dados usando uma chave privada. Além disso, o OpenSSL permite verificar a autenticidade e a integridade de assinaturas digitais usando a chave pública correspondente.
- Verificação de certificados: O OpenSSL também fornece ferramentas para verificar a validade e a integridade de certificados digitais. Por exemplo, o comando "openssl verify" permite verificar se um certificado é confiável e se foi assinado por uma autoridade de certificação (CA) confiável.
- Gerenciamento de CRLs: O OpenSSL suporta a criação, verificação e atualização de Listas de Revogação de Certificados (CRLs). Com o OpenSSL, é possível gerar CRLs contendo informações sobre certificados revogados, bem como verificar a validade e a integridade dessas CRLs.
- Implementação de OCSP Responders: O OpenSSL pode ser usado para implementar servidores OCSP (Online Certificate Status Protocol) Responders. Esses servidores permitem que os usuários consultem o status de revogação de um certificado em tempo real, fornecendo uma resposta direta sobre o status de revogação do certificado solicitado.

OpenSSL.

Conclusão

O gerenciamento adequado de certificados e chaves é fundamental para evitar vulnerabilidades, como a exposição de informações sensíveis e o uso indevido de certificados inválidos ou revogados. O conhecimento sobre os tópicos abordados nesta aula, como o gerenciamento de chaves, a revogação de certificados, o uso do OCSP e a fixação de certificados, é fundamental para implementar práticas de segurança eficazes e proteger as comunicações e transações online.

> Parabéns pela conclusão da aula de Gerenciamento de PKI! Você adquiriu um conhecimento valioso sobre as práticas e os desafios envolvidos no gerenciamento de certificados digitais em uma Infraestrutura de Chaves Públicas.

Aula 4: Blockchain

Objetivos

- [x] Explorar a estrutura de dados em Blockchain.
- [x] [] Entender os algoritmos de consenso utilizados para garantir a segurança e a integridade da Blockchain.
- [x] Familiarizar-se com os conceitos de criptografia e segurança no contexto da tecnologia Blockchain.

Conceitos

- [x] Estrutura de Dados em Blockchain.
- [x] Criptografia e Segurança em Blockchain.
- [x] Blockchain Pública, Privada e Consórcio.

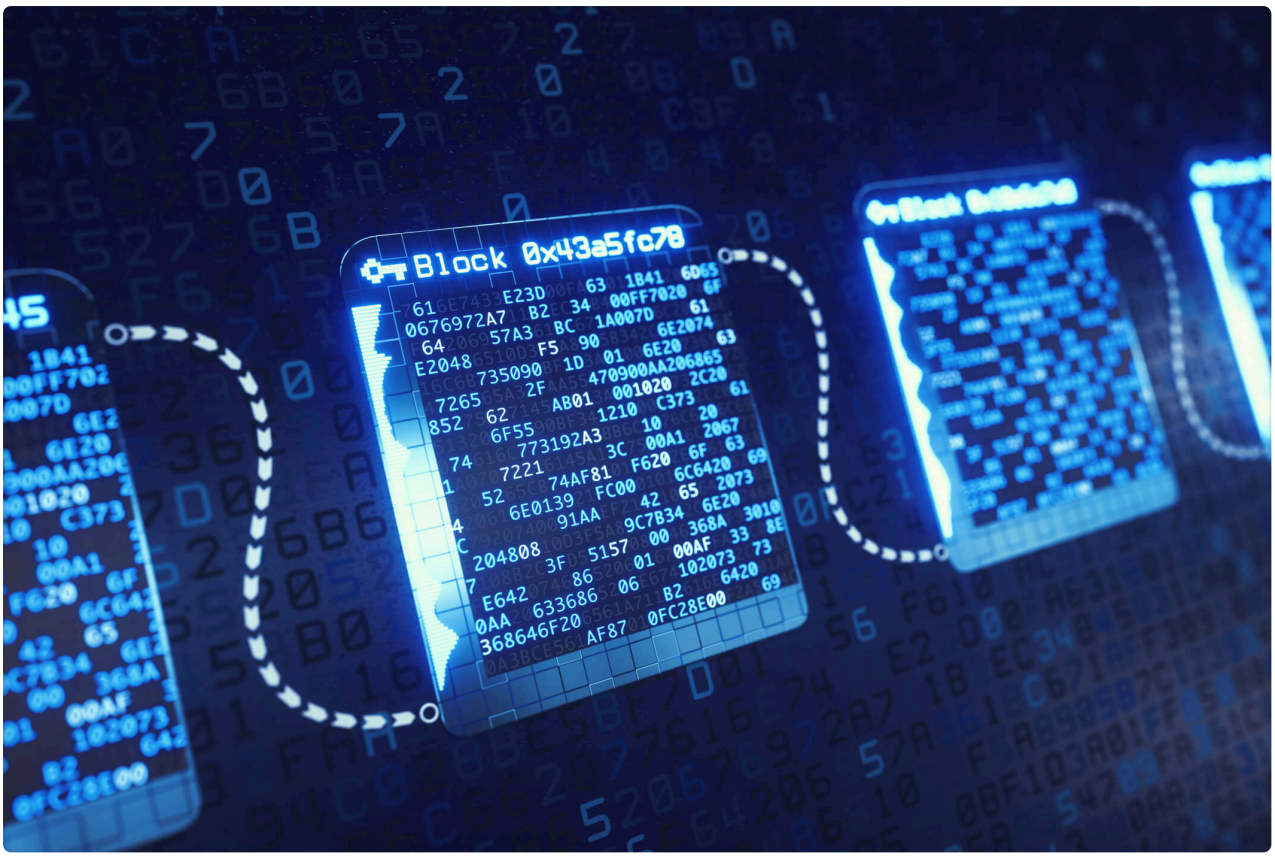
Introdução

Bem-vindos à aula de Blockchain, uma tecnologia revolucionária que está mudando a forma como interagimos, realizamos transações e garantimos a segurança da informação na era digital. Blockchain pode ser definida como um registro digital descentralizado, transparente e imutável de transações ou eventos. É uma estrutura de dados que armazena informações de forma sequencial em blocos, que estão interligados através de criptografia, formando uma cadeia de blocos.

A beleza da Blockchain reside na sua natureza descentralizada. Diferente dos sistemas tradicionais, onde uma entidade central controla e valida as transações, a Blockchain é mantida por uma rede de computadores distribuídos, chamados de nós, que trabalham em conjunto para verificar e validar as transações. Isso significa que não há uma autoridade central que detém o controle absoluto sobre o sistema, o que confere maior segurança e transparência às operações realizadas na Blockchain.

Outro elemento fundamental da Blockchain é a criptografia. Ela desempenha um papel crucial na segurança da tecnologia, garantindo a autenticidade, integridade e confidencialidade das transações. A criptografia de chave pública e privada permite a criação de identidades digitais e assinaturas digitais, tornando possível a verificação da autenticidade dos participantes e a comprovação de que uma transação foi realizada por uma parte específica.

A Blockchain começou a ganhar destaque com a popularização das criptomoedas, como o Bitcoin, mas suas aplicações vão muito além disso. Ela pode ser utilizada em cadeias de suprimentos, sistemas de votação eletrônica, registros médicos, gestão de direitos autorais e uma infinidade de outras áreas. Sua capacidade de criar contratos inteligentes, que são acordos digitais autoexecutáveis e autoverificáveis, torna a tecnologia ainda mais poderosa e disruptiva.



Blockchain.

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.

Blocos e cadeia de blocos

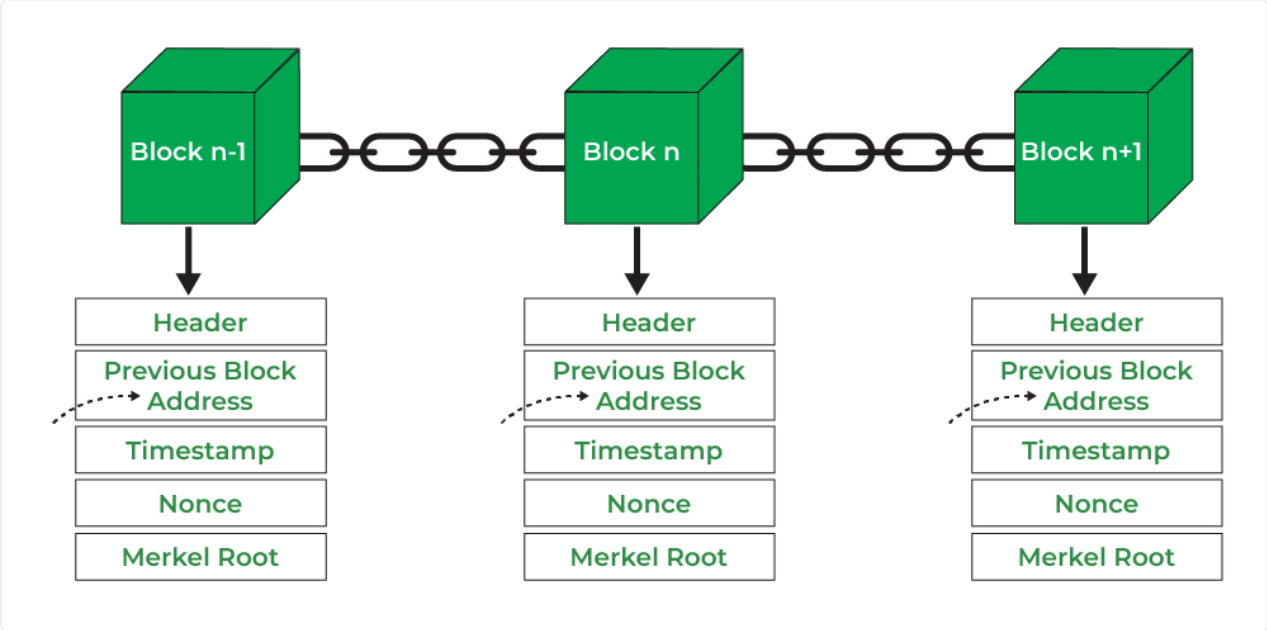
Na tecnologia Blockchain, os blocos são unidades fundamentais que compõem a estrutura de dados. Eles são responsáveis por armazenar informações sobre transações e eventos ocorridos na rede. Cada bloco contém um conjunto de dados, como transações, timestamps e outras informações relevantes, que são registradas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



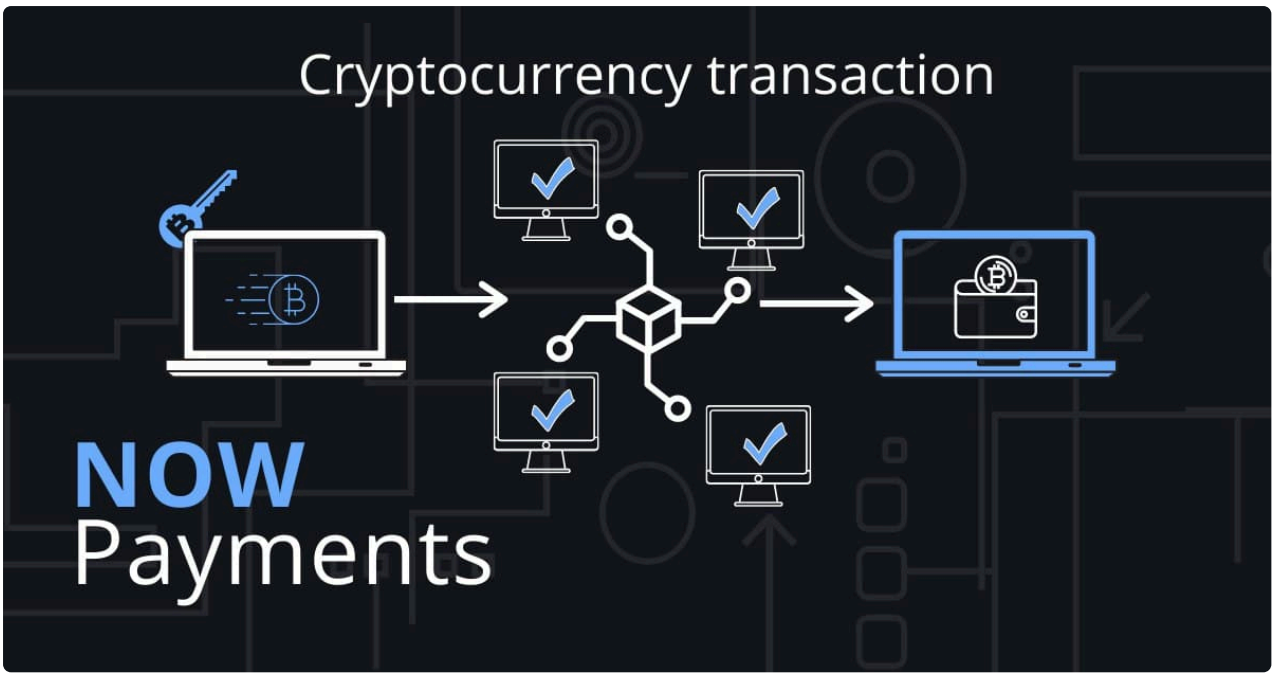
Cadeia de blocos.

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.



Transações de criptomoedas.

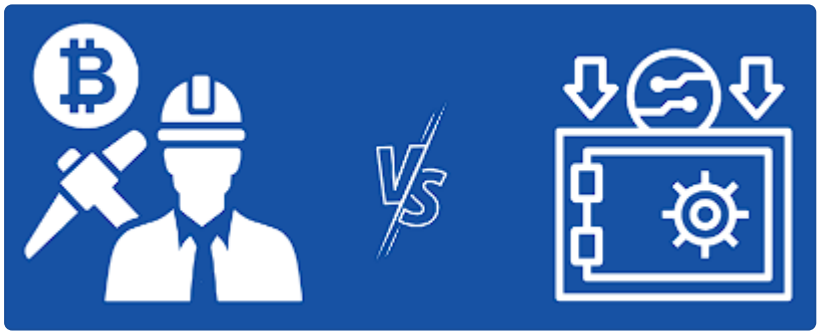
Algoritmos de consenso

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:

1. Proof of Work (Prova de Trabalho): 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.

2. Proof of Stake (Prova de Participação): 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.



Proof of Work x Proof of Stake.

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:

- 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.

- 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.
- 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.
- 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.
- 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.
- 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.

Criptografia em Blockchain.

Tipos de Blockchain

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

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.

Blockchain pública.

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.

Blockchain privada.

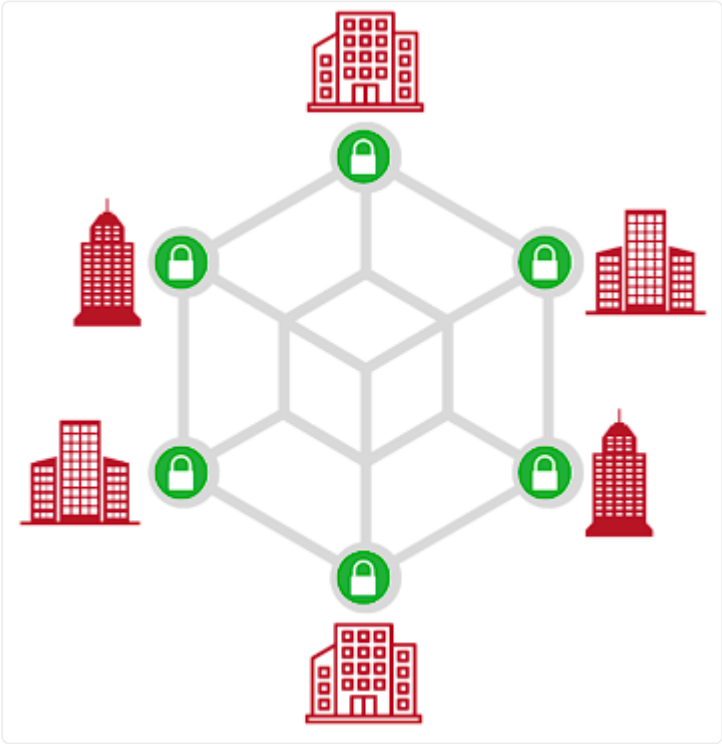
Blockchain de Consórcio ou Federada

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. Vamos entender 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.



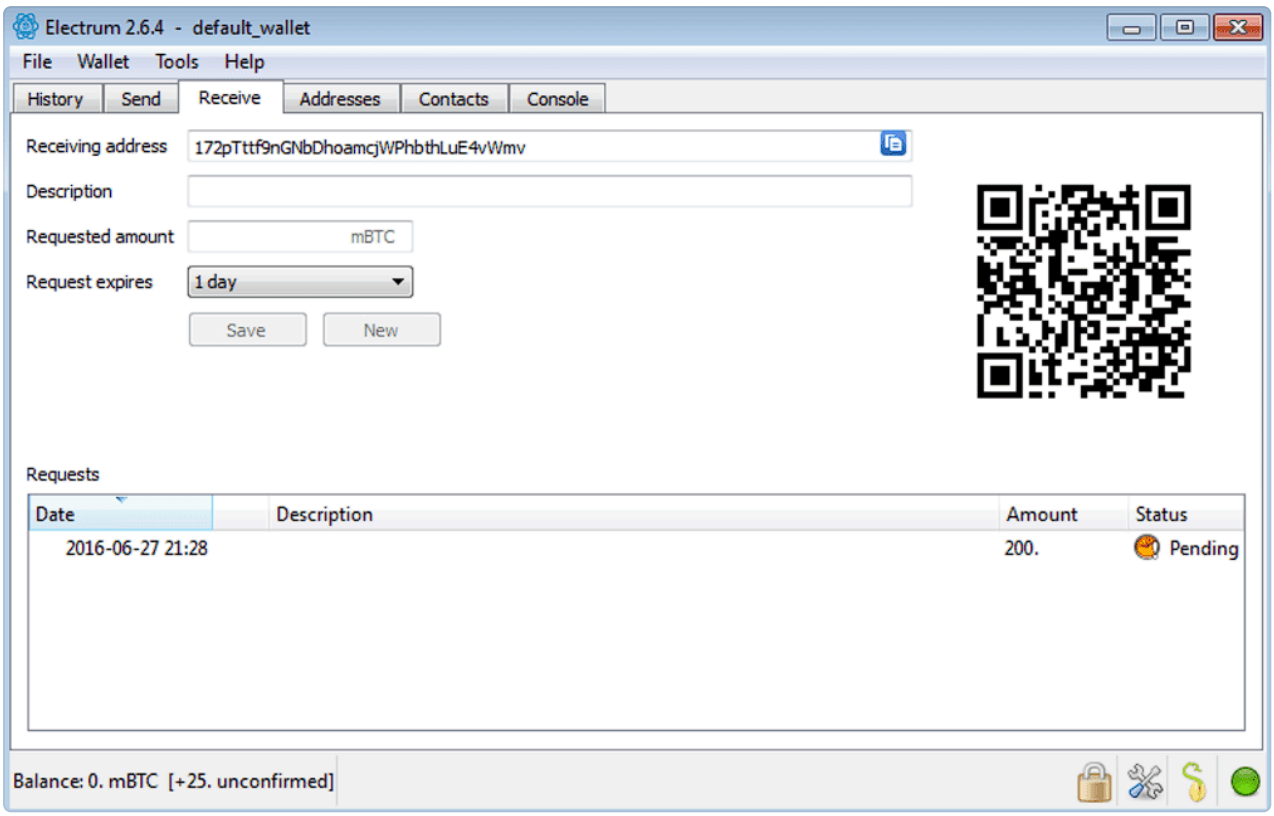
Blockchain de consórcio ou federada.

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. Vamos explorar 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.



Software de Bitcoin Etherum.

Conclusão

Nesta aula aprendemos que a Blockchain é uma estrutura de dados descentralizada e imutável, composta por blocos interligados e distribuídos em uma rede de participantes. Ela oferece segurança, transparência e confiança nas transações, eliminando a necessidade de intermediários e abrindo caminho para inúmeras aplicações em diversos setores.

Na aula também exploramos diferentes tipos de Blockchains, como a Pública, de Consórcio e Federada, cada uma com suas características e casos de uso específicos. Compreendemos os principais elementos da tecnologia Blockchain, como transações, registros distribuídos, algoritmos de consenso e criptografia de chave pública e privada. Esses conceitos são fundamentais para entendermos o potencial transformador da Blockchain em áreas como finanças, cadeia de suprimentos, saúde, governança e muito mais.

> Parabéns por concluir a aula de Blockchain com sucesso! Nesta aula você adquiriu conhecimentos sobre essa tecnologia inovadora. Continue a explorar e

> aplicar esses conhecimentos, contribuindo para o avanço e a adoção da tecnologia Blockchain em um mundo cada vez mais digital e conectado.