Sistemas Computacionais e Segurança

Professor Robson Calvetti

Turma:

USJT-SINSP1AN-BUA2-SIST.COM.SEGURANÇA

Alunos:

Annely Desireé Junemann – 824217739

Alexandre

Larissa Maschio – 824221401

Ano 2.024

ATIVIDADE PRÁTICA 04

CRIPTOGRAFIA

- Citar 2 exemplos históricos do uso de criptografia:

- Criptografia de *Blockchain* (corrente de blocos):

É um mecanismo de banco de dados avançada, no qual permite o compartilhamento de informações dentro da rede. É um banco de dados interligados em forma em forma de cadeia, que originalmente foi denominada de *Timechain.* Sua funcionalidade é realizar modificação e não é tão simples, os dados são cronologicamente consistentes, pois não é possível excluir nem modificar a cadeia sem o consenso da rede. O *Blockchain é muito utilizado em sistemas financeiros, com intuito de evitar que niguémk consiga fraudar transações, para criar um ledger inalterável ou imutável para monitorar pedidos, pagamentos, contas e outras transações. Devemos destacar que a mesma por ser uma nova tecnologia, está sendo avaliada com bons olhos para diversos setores, dentre eles: energia, media e varejo.*

1. Principais componentes:

Ledger distribuído: è um banco de dados compartilhado, no qual aqueles envolvidos poderão estar acessando e editando. Também podendo saber quem foi o último ter acessado e editado. Uma das regras é seu ponto contra: ao editar, não te dá a possibilidade de exclusão.

Contratos Inteligentes:

Ele funciona sozinho e segue regras definidas de antemão. Quando as condições dessas regras são cumpridas, o contrato é executado automaticamente.

Criptografia de chave pública:

é um método de segurança usado para garantir que as informações em uma rede blockchain sejam protegidas e acessíveis apenas por quem tem permissão. Ela funciona com dois tipos de chaves: a **chave pública** e a **chave privada**.

***Chave pública**: Esta é visível para todos na rede, como um endereço de e-mail. Ela identifica os participantes de forma única e permite que outros enviem informações ou transações para você.*	***Chave privada**: Esta é secreta e pertence apenas a você. Ela funciona como uma senha, permitindo que você acesse as informações que foram enviadas para sua chave pública.*

2. Como a blockchain funciona?

Os mecanismos de blockchain são complexos, então vamos fornecer uma visão geral bastante breve nas próximas etapas. O software da blockchain pode automatizar a maioria destas etapas:

Etapa 1 – Registrar a transação

Uma transação de blockchain mostra a movimentação de ativos físicos ou digitais de uma parte para outra na rede blockchain. Ela é registrada como um bloco de dados que inclui detalhes como estes:

- Quem foram os envolvidos na transação?
- O que aconteceu durante a transação?
- Quando a transação ocorreu?
- Onde a transação ocorreu?
- Por que a transação ocorreu?
- Qual é o volume do ativo que foi trocado?
- Quantas pré-condições foram cumpridas durante a transação?

Etapa 2 – Obter consenso

A maioria dos participantes da rede blockchain distribuída precisa concordar que a transação registrada é válida. Dependendo do tipo de rede, as regras do acordo podem variar, mas elas normalmente são estabelecidas no início da rede.

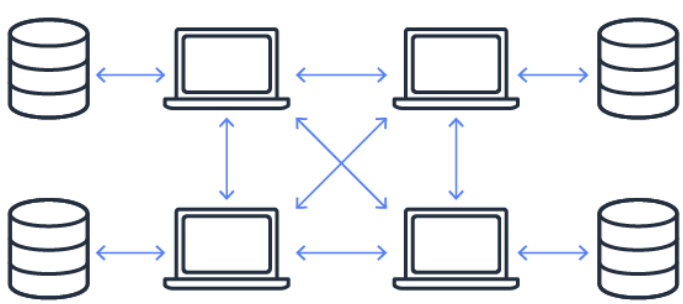
Etapa 3 – Vincular os blocos

Quando os participantes chegam a um consenso, as transações na blockchain são gravadas em blocos, equivalentes às páginas de um livro contábil. Junto com as transações, também é anexado um hash criptográfico ao novo bloco. O hash atua como uma cadeia que interliga todos os blocos. Se o conteúdo dos blocos for modificado de forma intencional ou inadvertida, o valor do hash será alterado, permitindo a detecção da violação dos dados.

Assim, os blocos e as cadeias são interligados de forma segura, e você não pode editá-los. Cada bloco adicional fortalece a verificação do bloco anterior e, portanto, toda a blockchain. Esse processo é semelhante ao empilhamento de blocos para construir uma torre. Você só pode empilhar blocos no topo e, se remover um bloco do meio da torre, tudo cairá.

Etapa 4 – Compartilhar o ledger

O sistema distribui a cópia mais recente do ledger central para todos os participantes.



Quais são os protocolos da blockchain?

O termo protocolo da blockchain refere-se a diferentes tipos de plataformas de blockchain, que estão disponíveis para o desenvolvimento de aplicações. Cada protocolo da blockchain se adapta aos princípios básicos da blockchain, de acordo com aplicações ou setores específicos. Alguns exemplos de protocolos da blockchain são fornecidos nas subseções abaixo:

- *Hyperledger Fabric*

O *Hyperledger Fabric* é um projeto de código aberto com um conjunto de ferramentas e bibliotecas. As empresas podem usá-lo para criar aplicações de blockchain privada de forma rápida e eficiente. Esse protocolo é um framework para fins gerais que oferece gerenciamento de identidades exclusivo e acesso a recursos de controle. Esses recursos o tornam adequados para várias aplicações, como rastreamento e monitoramento de cadeias de suprimento, finanças comerciais, programas de fidelidade e lealdade e liquidação de ativos financeiros.

- *Ethereum*

O *Ethereum* é uma plataforma de blockchain descentralizada de código aberto que pode ser usada para criar aplicações de blockchain pública. A Ethereum Enterprise foi criada para casos de uso comerciais.

- Corda

A Corda é um projeto de blockchain de código aberto criado para empresas. Com a Corda, você pode criar redes blockchain interoperacionais que fazem transações com privacidade rigorosa. As empresas podem usar a tecnologia de contratos inteligentes da Corda para fazer transações diretas com valor. Instituições financeiras são os principais usuários da Corda.

- *Quorum*

A *Quorum* é um protocolo de blockchain de código aberto, derivado da Ethereum. Ela foi criada especialmente para uso em uma rede blockchain privada, na qual somente um único membro tem propriedade de todos os nós, ou em uma rede blockchain consórcio, na qual cada membro da rede tem a propriedade de uma parte dela.

Quais são os benefícios da tecnologia blockchain?

A tecnologia blockchain oferece vários benefícios para o gerenciamento de transações de ativos. Nas subseções abaixo, listamos alguns deles:

- Segurança avançada

Os sistemas de blockchain oferecem o alto nível de segurança e confiança que as transações digitais modernas exigem. O medo de que alguém manipule o software subjacente para gerar dinheiro falso para eles próprios é uma constante. Porém, a blockchain utiliza os três princípios de criptografia, descentralização e consenso para criar um sistema de software subjacente altamente seguro, que é quase impossível de ser violado. Não há um único ponto de falha, e um único usuário não é capaz de alterar os registros de transações.

- Eficiência aprimorada

As transações B2B (“de empresa para empresa”) podem ser demoradas e criar gargalos operacionais, principalmente quando a conformidade e organismos reguladores terceiros estiverem envolvidos. A transparência e os contratos inteligentes tornam essas transações mais rápidas e eficientes.

- Auditorias mais rápidas

As empresas devem poder gerar, fazer o câmbio, arquivar e reconstruir transações eletrônicas de forma auditável. Os registros de blockchain são cronologicamente imutáveis, o que significa que todos os registros são sempre ordenados de acordo com a cronologia. A transparência dos dados acelera muito o processo de auditoria.

- A criptografia de *hash* é um processo que transforma dados de qualquer tamanho (como um texto ou um arquivo) em um valor fixo, chamado de *hash*. Esse valor é gerado por uma função matemática e é único para cada conjunto específico de dados, ou seja, se os dados forem alterados, mesmo que ligeiramente, o *hash* também mudará completamente.

Como funciona?

1. Entrada de dados: Você insere qualquer tipo de dado, seja uma senha, uma mensagem, ou um arquivo.
2. Função de *hash*: Uma função matemática é aplicada ao dado, gerando um código único e de tamanho fixo (por exemplo, 64 caracteres).
3. Saída (*hash*): O resultado é o *hash*, que parece uma sequência aleatória de números e letras, mas que corresponde exclusivamente àqueles dados originais.

Por exemplo, se você usa a função hash em uma palavra, digamos "blockchain", ela será transformada em um código único. Se você mudar a palavra para "blockchaim" (apenas trocando uma letra), o hash resultante será completamente diferente.

Benefícios da criptografia de hash:

1. Integridade dos dados: O hash ajuda a verificar se os dados foram alterados. Se alguém tentar modificar um arquivo ou uma transação, o hash será diferente do original, mostrando que houve uma alteração.
2. Segurança: Mesmo que o hash seja público, é impossível reverter o processo e descobrir os dados originais a partir do hash (ou seja, o processo de hash é "unidirecional").
3. Velocidade: Funções de hash são rápidas e eficientes, permitindo processar grandes quantidades de dados em pouco tempo.
4. Autenticidade: Hashes podem ser usados para assinar digitalmente documentos, verificando se um arquivo ou uma mensagem foi criada por uma pessoa específica e não foi alterada.
5. Aplicações na blockchain: Nas redes blockchain, o hash é usado para criar blocos de dados e garantir que cada bloco dependa do anterior, protegendo a cadeia contra adulterações.

- Criptografia Simétrica: É o tipo em que só existe apenas uma única chave secreta que é usada para ambas as partes do processo, na criptografia e na descriptografia. Exemplos

    1. Data *Encryption Standart*(DES): é um algoritmo de criptografia simétrica que foi desenvolvido por volta da década de 1970. O DES realiza apenas duas operações sobre sua entrada, o chamado deslocamento de bits e substituição de bits. Ao repetir essas operações inúmeras vezes e de uma forma não-linear, chega-se a um resultado que não pode ser revertido sem o uso da chave, esse algoritmo trabalha com 64 bits. Ele foi desenvolvido há mais de 20 anos e até hoje não se sabe o caminho para quebrá-lo, exceto por força bruta.
    2. *Blowfish*: esse algoritmo foi desenvolvido por Bruce Schneier em 1993. Esse tipo de criptografia é muito conhecido na área de negócios de e-commerce, devido a garantia de segurança ao lidar com métodos de pagamento. Ele foi criado para substituir o DES, ele utiliza chaves de 32 a 446 bits, segmentando as informações em blocos de 64 bits e criptografando cada um deles individualmente. O *blowfish* é conhecido pela sua velocidade de encriptação e confiabilidade, muitos especialistas afirmam que o código é virtualmente inquebrável, ainda se destaca por estar na lista de algoritmos não patenteados e licença livre.

- Criptografia Assimétrica: É o tipo que existe duas chaves secretas, uma para cada parte do processo, sendo uma chave para criptografar e a outra para descriptografar. Exemplos:

    1. *Rivest Shamir Adleman* (RSA) atualmente é a base da maioria das aplicações de usam criptografia assimétrica, surgindo por volta de 1977. É um algoritmo de chave pública, a criptografia de RSA permite que os usuários criptografem mensagens com um código chamado chave pública que podem ser compartilhadas abertamente. Devido às propriedades matemáticas específicas do algoritmo RSA, uma vez que um usuário criptografa uma mensagem com uma chave pública, somente uma chave privada pode descriptografá-la. Os usuários têm um par de chaves públicas e privadas e este último são mantidos em segredo. Geralmente esse tipo é indicado usar em conjunto com outros sistemas de criptografia, a fim de comprovar a integridade e autenticidade das mensagem, geralmente, os usuários criptografam um arquivo com um algoritmo de chave assimétrica e utilizam a criptografia RSA para criptografar a chave simétrica. Assim, apenas uma chave privada RSA pode descriptografar a chave simétrica usada e sem ela, não é possível decifrar a mensagem.

    2. ElGamal: Foi fundado pelo egípcio Taher Elgamal, em 1984. É um algoritmo de chave pública, esse, diferente do RSA, envolve a manipulação de grandes quantidades numéricas. A segurança consiste em um algoritmo matemático discreto e de corpo finito simular a uma fatoração.

Sites de pesquisa:

https://www.veritas.com/pt/br/information-center/rsa-encryption

https://www.mjvinnovation.com/pt-br/blog/tipos-de-criptografia/

https://www.gta.ufrj.br/grad/99_2/marcos/des.htm

https://medium.com/prognosys/criptografia-sim%C3%A9trica-6b4271ff697c

https://aws.amazon.com/pt/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

https://www.clicksign.com/blog/tipos-de-criptografia-como-funcionam

https://academiatech.blog.br/exemplos-de-criptografia/