Instituto Infnet

Segurança da Informação

FABIANO GISBERT

Etapa 05

Criptografia

Instituto Infnet

Introdução

Enviar mensagens secretas é uma tarefa muito antiga. O homem sentiu, desde muito cedo, a necessidade de guardar informações em segredo; ela nasceu com a diplomacia e com as transações militares.

Generais, reis e rainhas, durante milênios, buscavam formas eficientes de comunicação para comandar seus exércitos e governar seus países.

Criptografia

Instituto Infnet

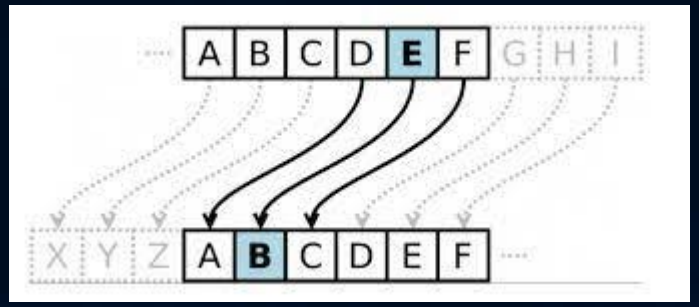
Introdução

Tendo em vista a necessidade de se criar ferramentas capazes de proteger a informação e de prover segurança aos documentos armazenados e transmitidos pelas organizações através do mundo, tem-se a motivação para o estudo da Criptografia.

Criptografia

Definição

A Criptografia é a ciência de escrever em cifra ou em código. Em outras palavras, ela abarca o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e a compreenda.



Criptografia

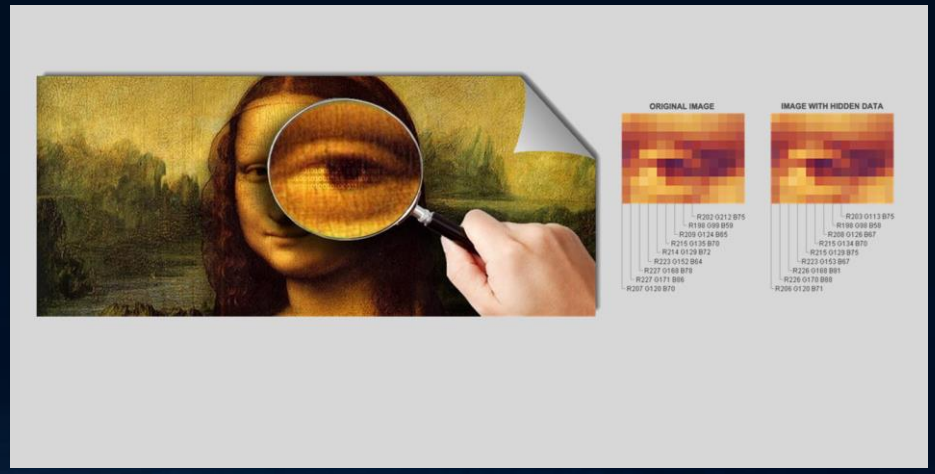
Aplicações

- Sigilo em banco de dados.
- Investigações governamentais.
- Dados hospitalares.
- Decisões estratégicas empresariais.
- Sigilo em comunicação de dados.
- Comandos militares.
- Mensagens diplomáticas.
- Operações bancárias.
- Comércio eletrônico.
- Transações por troca de documentos eletrônicos (EDI).

Criptografia

Esteganografia

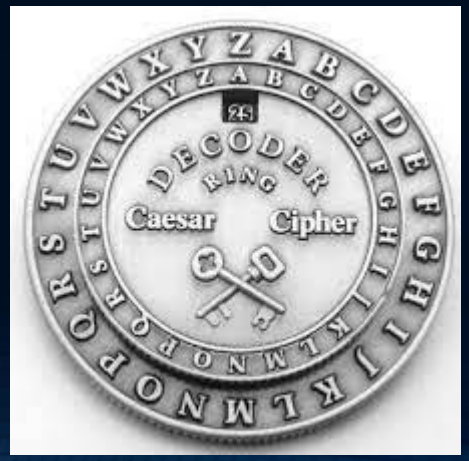
A esteganografia estuda meios e métodos para se esconder a existência da mensagem. É bastante utilizada na área de segurança monetária, na autenticação de documentos, em imagens e nas gravações em geral (música,filmes, etc)



Criptografia

Cifras

No estudo das cifras, o fundamental é o ocultamento da informação; há uma unidade básica de substituição formada por letras ou símbolos, isolados ou agrupados, e os métodos de cifragem são divididos segundo sua natureza: métodos de substituição (quando uma letra é trocada por outra, em geral diferente dela), cifragem de transposição (em que as letras da mensagem são apenas permutadas, mas não substituídas) e cifragem mista



Criptografia

Instituto Infnet

Cifras

Método de Ciframento por Transposição

Neste método os conteúdos das mensagens original e criptografada são os mesmos, porém com as letras são postas em ordem diferente (permutadas).

Z	E	B	R	A	S
V	A	M	O	S	E
M	B	O	R	A	F
O	M	O	S	D	E
S	C	O	B	E	R
T	O	S	J	E	U

Criptografia

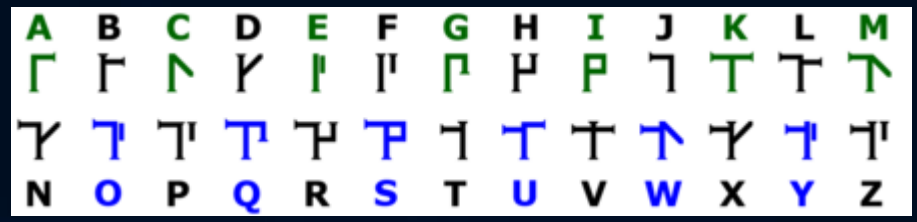
Cifras

Método de Ciframento por Substituição

Neste procedimento troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição. No método da substituição simples (monoalfabética) substitui-se cada caractere do texto por outro, de acordo com uma tabela pré-estabelecida

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C



Criptografia

Instituto Infnet

Cifras

Método de Ciframento por Chaves

Na criptografia contemporânea, com o uso de computadores, substitui-se caracteres por blocos de bits. Esses bits são "embaralhados" de acordo com uma função matemática a partir de uma chave numérica secreta.

Essa chave é uma sequência de caracteres usada em um algoritmo de criptografia para alterar os dados de forma que pareçam aleatórios. Como uma chave física, ele bloqueia (criptografa) os dados para que apenas alguém com a chave certa possa desbloqueá-los (descriptografá-los).

Criptografia

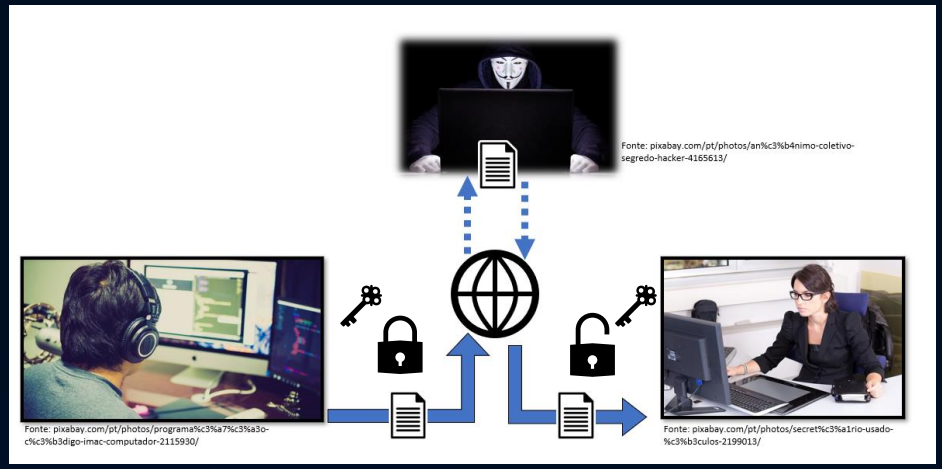
Criptografia na Computação

Método de Ciframento por Chaves Simétricas

A criptografia simétrica, também conhecida como criptografia de chave secreta, usa uma única chave para criptografar e descriptografar dados. É preciso compartilhar essa chave com o destinatário.

Uma das vantagens do método de criptografia simétrica é que o processo é mais rápido de processar, e muito fácil de configurar.

A desvantagem é que a chave secreta precisa ser compartilhada com o destinatário.



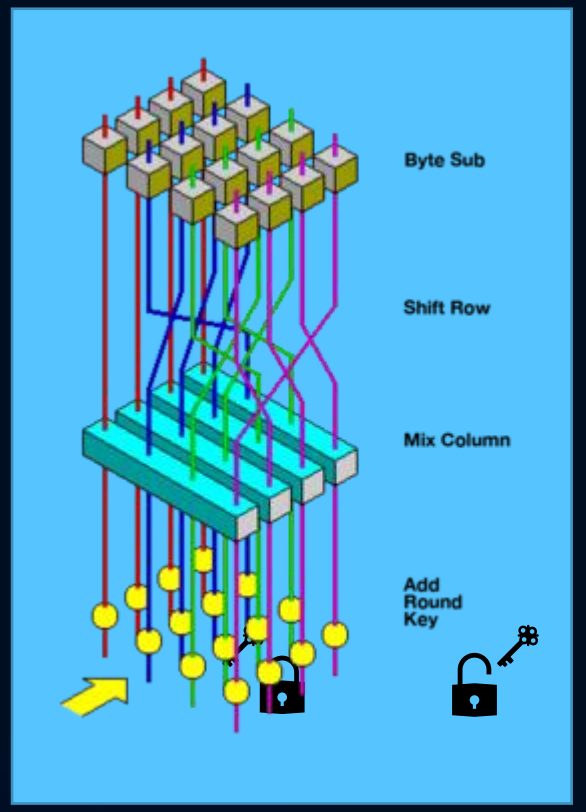
Criptografia

Criptografia na Computação

Método de Ciframento por Chaves Simétricas

Um dos padrões de cifra simétrica mais utilizada atualmente é o AES 256 . O AES é baseado em um princípio de design conhecido como rede de substituição-permutação, e é eficiente tanto em software quanto em hardware. O AES possui um tamanho de bloco fixo de 128 bits e um tamanho de chave de 256 bits, que define 14 rodadas de transformação.

Cada rodada consiste em várias etapas de processamento, incluindo uma que depende da própria chave de criptografia. Um conjunto de rodadas reversas é aplicado para transformar o texto cifrado de volta ao texto plano original usando a mesma chave de criptografia.



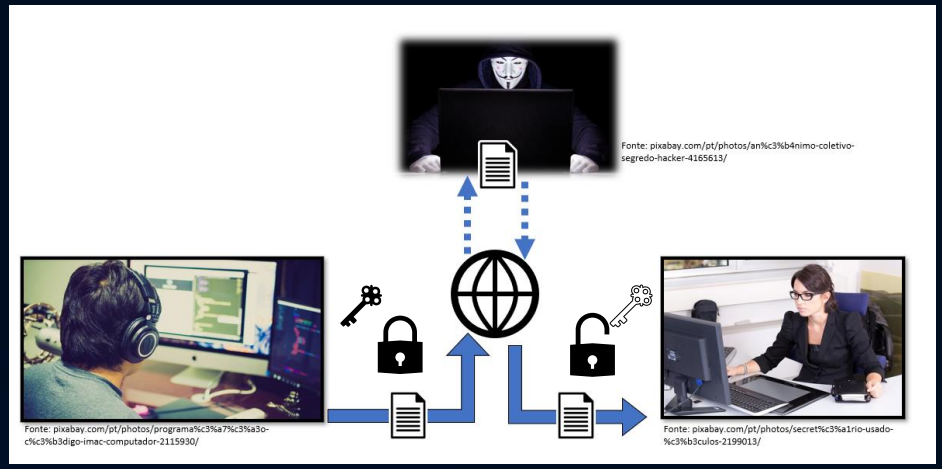
Criptografia

Criptografia na Computação

Método de Ciframento por Chaves Assimétricas

A criptografia assimétrica anterior requer duas chaves para funcionar: uma chave pública deve ser tornada pública e uma chave privada usada apenas pelo detentor do par criptográfico.

A chave usada para criptografar (seja a publica ou privada) não serve para descriptografar, necessitando do par equivalente para que o texto seja convertido em texto livre.



Criptografia

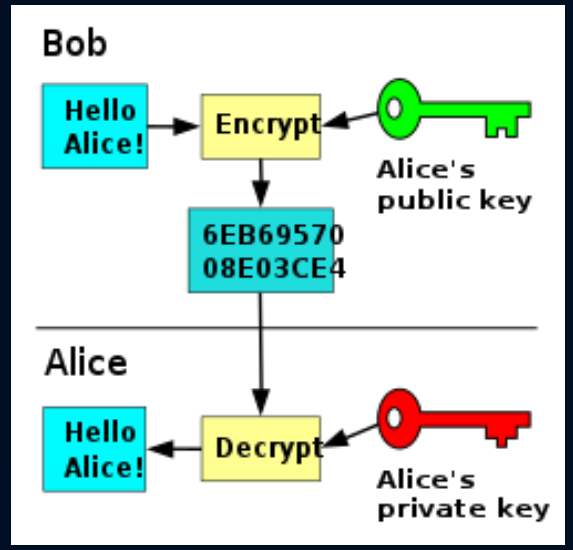
Instituto Infnet

Criptografia na Computação

Método de Ciframento por Chaves Assimétricas

Ambas chaves são geradas pelo mesmo algoritmo criptográfico e são baseados num par de números primos relativamente grande ao ponto de não ser descoberto. Um algoritmo muito utilizado e reconhecido internancionalmente é o RSA (Rivest-Shamir-Adleman).

A vantagem da Criptografia assimétrica é que ela não força o usuário a compartilhar chaves (secretas) como a criptografia simétrica, removendo, portanto, a necessidade de distribuição de chaves. A Desvantagem é que o algoritmo de encriptação é mais pesado para encriptação de muitos dados.



Criptografia

Instituto Infnet

RSA

No RSA as chaves são geradas desta maneira:

1. Escolha de forma aleatória dois números primos grandes p e q, da ordem de 10^{100} no mínimo.
2. Calcule $n = pq$
3. Calcule a função Função totiente de Euler em n: $\phi(n) = (p-1)(q-1)$.[2]
4. Escolha um inteiro e tal que $1 < e < \phi(n)$, de forma que e e $\phi(n)$ sejam relativamente primos entre si.
5. Calcule d de forma que $de \equiv 1 \pmod{\phi(n)}$, ou seja, d seja o inverso multiplicativo de e em $\pmod{\phi(n)}$.

- No passo 1 os números podem ser testados probabilisticamente para primalidade
- No passo 5 é usado o algoritmo de Euclides estendido, e o conceito de inverso multiplicativo que vem da aritmética modular

Por final temos:

A chave pública: o par (n, e).

A chave privada: a tripla (p, q, d). (De fato, para desencriptar, basta guardar d como chave privada, mas os primos p e q são usados para acelerar os cálculos)

Criptografia

Aplicação

O Protocolo HTTP/HTTPS

HTTP (Hypertext Transfer Protocol). Esse é um protocolo para transferência de textos e endereços de objetos (como fotos e vídeos). Qualquer informação tramitada por ele será feita como texto simples, inclusive seus dados pessoais!

Criptografia

Aplicação

O Protocolo HTTP/HTTPS

HTTPS (Hyper Text Transfer Protocol Secure). Acrescenta uma camada de segurança na transferência de informações, garantindo que, caso sejam interceptadas, seu conteúdo não poderá ser compreendido.
Inclui um protocolo denominado SSL (Secure Sockets Layer) e nas versões mais recentes o TLS (Transport Layer Security) .

O segredo do TSL é o uso de Certificado Digital e troca de Chave Criptográfica.

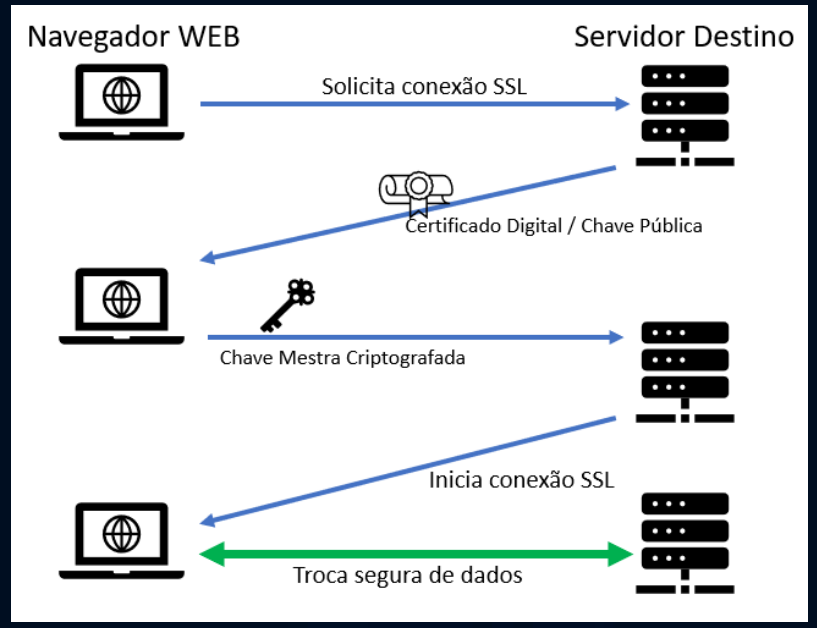
Criptografia

Aplicação

O Protocolo HTTP/HTTPS

As três fases de uma sessão SSL são:

- Apresentação,
- Criação da chave mestra;
- Transferência segura de dados



Criptografia

Aplicação

O Protocolo TLS

Substituiu o SSL em função de uma vulnerabilidade descoberta em 2014, que poderia ser explorada por ameaças.

Protocolo para inicializar a conexão entre navegador e Servidor: Handshaking. Possui chaves criptográficas mais fortes que o SSL.

Função Hash

Instituto Infnet

Conceito

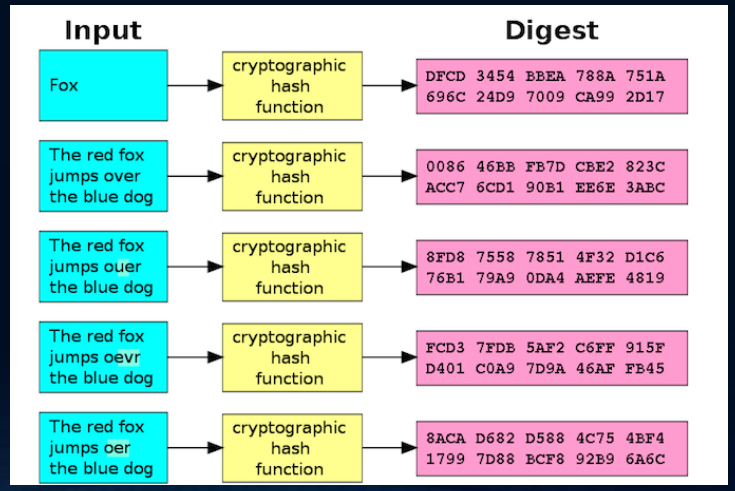
Uma função de hash criptográfico, muitas vezes é conhecida simplesmente como hash – é um algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo. Independentemente do comprimento dos dados de entrada, o mesmo tipo de hash de saída será sempre um valor do mesmo comprimento.

Um hash é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um conjunto cada. O conceito teórico diz que "hash é a transformação de uma grande quantidade de dados em uma pequena quantidade de informações".

Função Hash

Conceito

Essa sequência busca identificar um arquivo ou informação unicamente. Por exemplo, uma mensagem de correio eletrônico, uma senha, uma chave criptográfica ou mesmo um arquivo. É um método para transformar dados de tal forma que o resultado seja exclusivo. Além disso, funções usadas em criptografia garantem que não é possível a partir de um valor de hash retornar à informação original.



Função Hash

Principais Algorítmos

MD4: Desenvolvido em 1990/91 por Ron Rivest, vários ataques foram detectados, o que fez com que o algoritmo fosse considerado frágil.
MD5: O MD5 (Message-Digest algorithm 5) é um algoritmo de hash de 128 bits unidirecional desenvolvido pela RSA Data Security, Inc., descrito na RFC 1321, e muito utilizado por softwares com protocolo par a par (P2P, ou Peer-to-Peer, em inglês), verificação de integridade e logins. Existem alguns métodos de ataque divulgados para o MD5.
SHA (Secure Hash Algorithm): Desenvolvido pelo NIST e NSA. Já foram exploradas falhas no SHA.
WHIRLPOOL: função criptográfica de hash desenvolvida por Paulo S. L. M. Barreto e por Vincent Rijmen (coautor do AES). A função foi recomendada pelo projeto NESSIE (Europeu). Foi também adotado pelo ISO e IEC como parte do padrão internacional ISO 10118-3.
SHA-256 e SHA-512 são funções hash inovadoras computadas com palavras de 32 e 64 bytes, respectivamente. Eles usam quantidades de deslocamento e constantes aditivas diferentes, mas as suas estruturas são praticamente idênticas, diferindo apenas no número de rodadas.

Função Hash

Aplicação

https://md5file.com/calculator - Gerar HASH

https://akad.com.br/verifica_hash.php - Verificar HASH

Certificado Digital

Instituto Infnet

Conceito

O Certificado digital é uma espécie de identificação eletrônica emitida por uma entidade reconhecida e idônea, para comprovar a identidade do emissor em meios eletrônicos.

Seu objetivo principal é proporcionar uma forma segura de assinar digitalmente conteúdos disponibilizados na Internet.

Certificado Digital

Instituto Infnet

Aplicação

$ openssl req -x509 -sha256 -newkey rsa:2048 -keyout certificate.key -out certificate.crt -days 1024 -nodes

Win64 OpenSSL

sudo apt-get install openssl
sudo yum install openssl

Blockchain

Instituto Infnet

Conceito

Blockchain pode ser traduzida como corrente de blocos. De uma forma simples, trata-se de uma tecnologia que agrupa um conjunto de informações que se conectam por meio de criptografia. Assim, transações financeiras e outras operações podem ser feitas de forma segura.

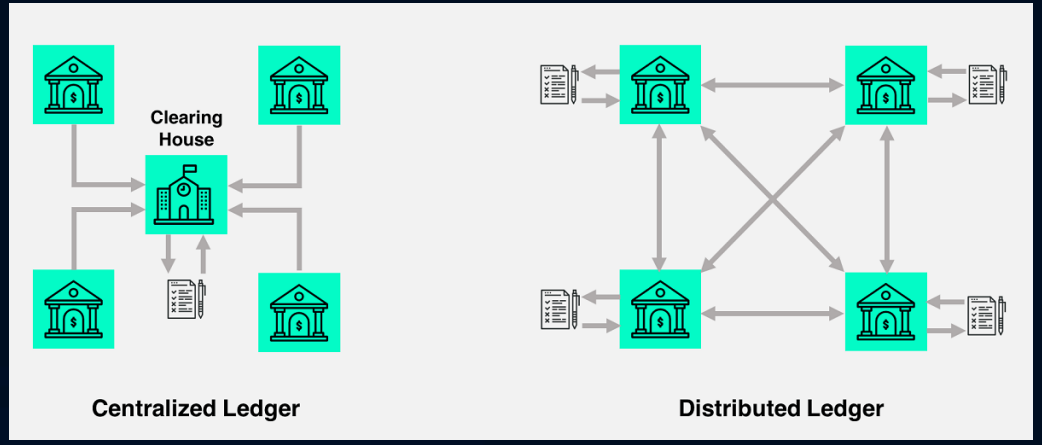
A grande inovação da Blockchain foi armazenar os dados de forma sequencial, porém sem a necessidade de uma entidade coordenando o processo. Os próprios usuários da rede conseguem verificar de forma simples e praticamente sem custo se as regras estão sendo cumpridas.

Blockchain

Conceito

A Blockchain ordena blocos de informação em cadeia sequencial, e originalmente foi denominada de Timechain, ou cadeia temporal. Ela é importante para garantir que ninguém consiga fraudar transações, já que os saldos de cada endereço dependem das movimentações passadas.

Ao contrário de uma conta bancária, em que um banco de dados armazena os saldos, podendo inclusive apagar o histórico de períodos mais longos, a Blockchain registra apenas as movimentações. Para calcular o saldo, deve-se percorrer todo o histórico da rede, acompanhando as transações desde a emissão de cada moeda.

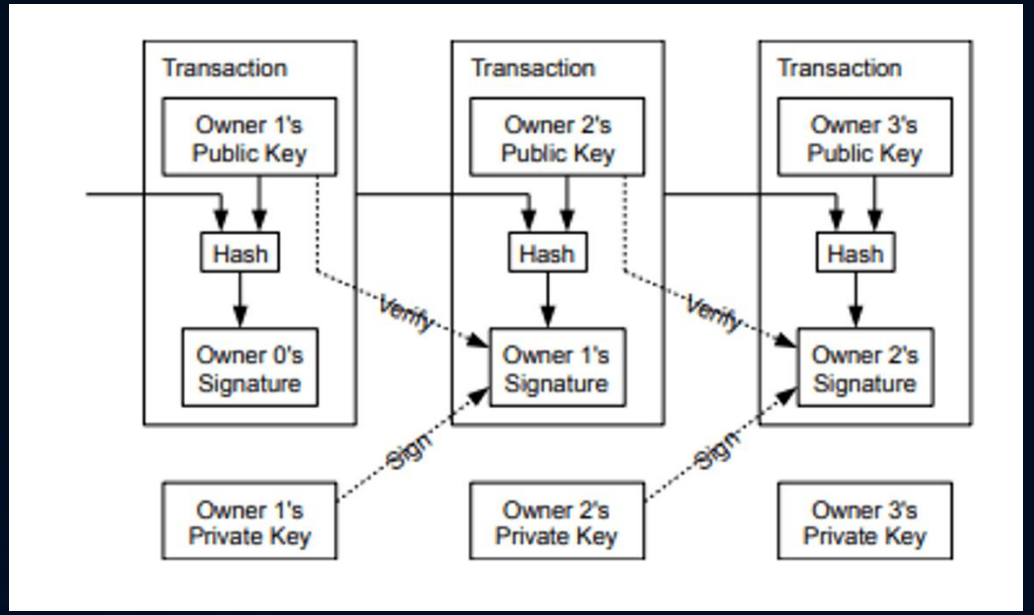


Blockchain

Instituto Infnet

Blocos

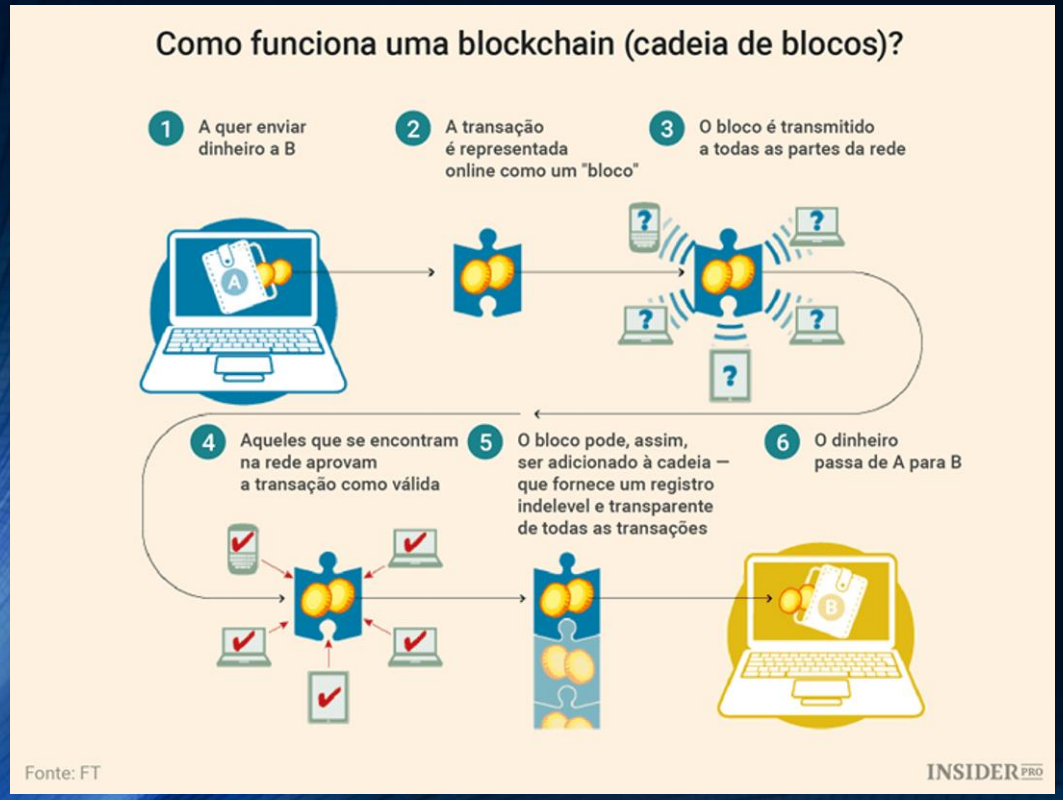
- Um bloco possui um cabeçalho que inclui o conjunto de regras para a validação que o bloco deve seguir.
- versão;
- Valor do hash de 256 bits que indica qual o bloco anterior, chamado Parent block hash;
- Valor de hash que se refere a todas as transações daquele bloco, denominado merkle root hash;
- Timestamp;
- Um alvo de hash compacto – nBits;
- Nonce um campo de 4 bytes e aumenta para cada hash.

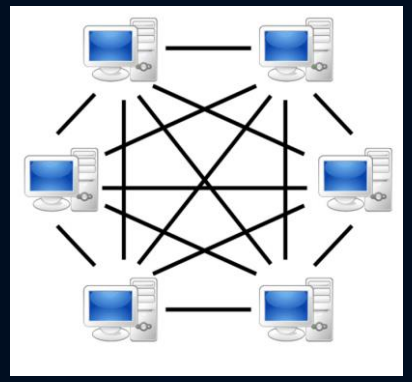


Blockchain

Instituto Infnet

Aplicação





A rede peer-to-peer é estrutura de computadores ou redes que compartilham eventos ou arquivos entre pares, denominados peers, sendo que todos possuem as mesmas prerrogativas e privilégios no ambiente da Blockchain, o que não ocorre em outras plataformas. Em uma rede peer-to-peer casa usuário é denominado "nó

Fim da Etapa 05