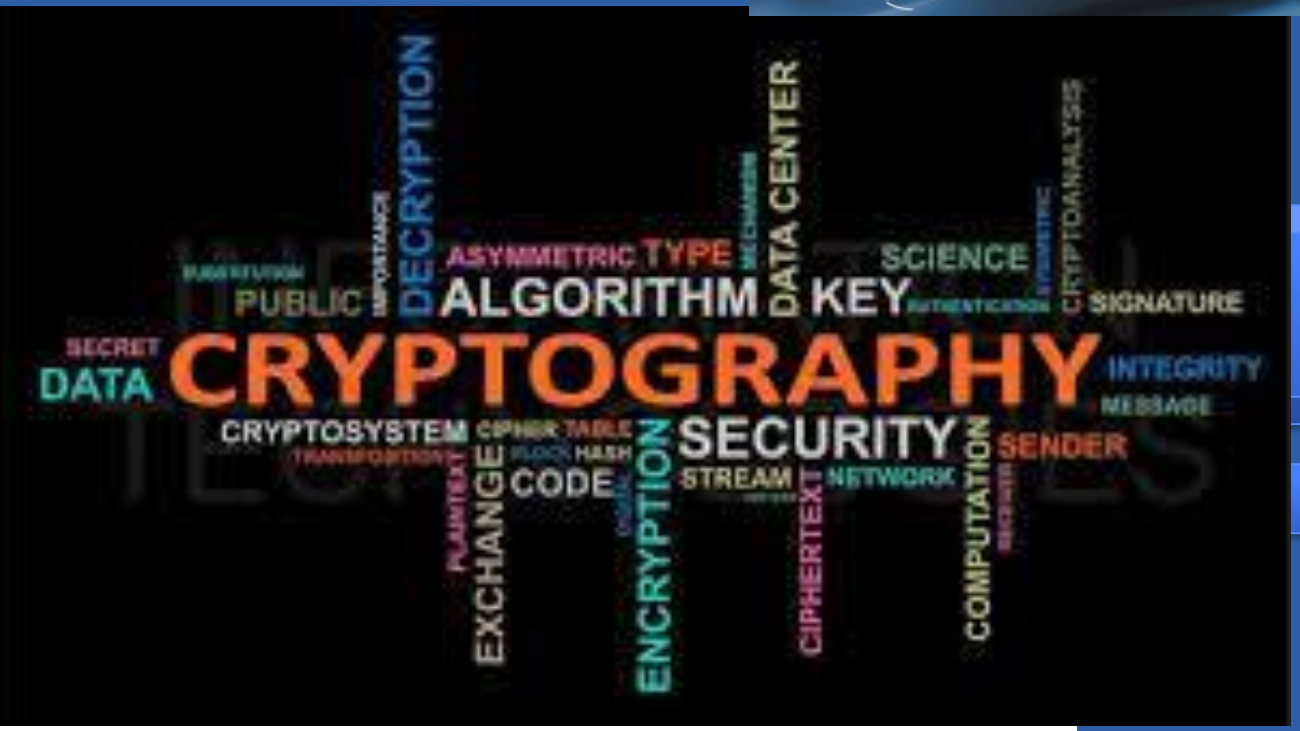
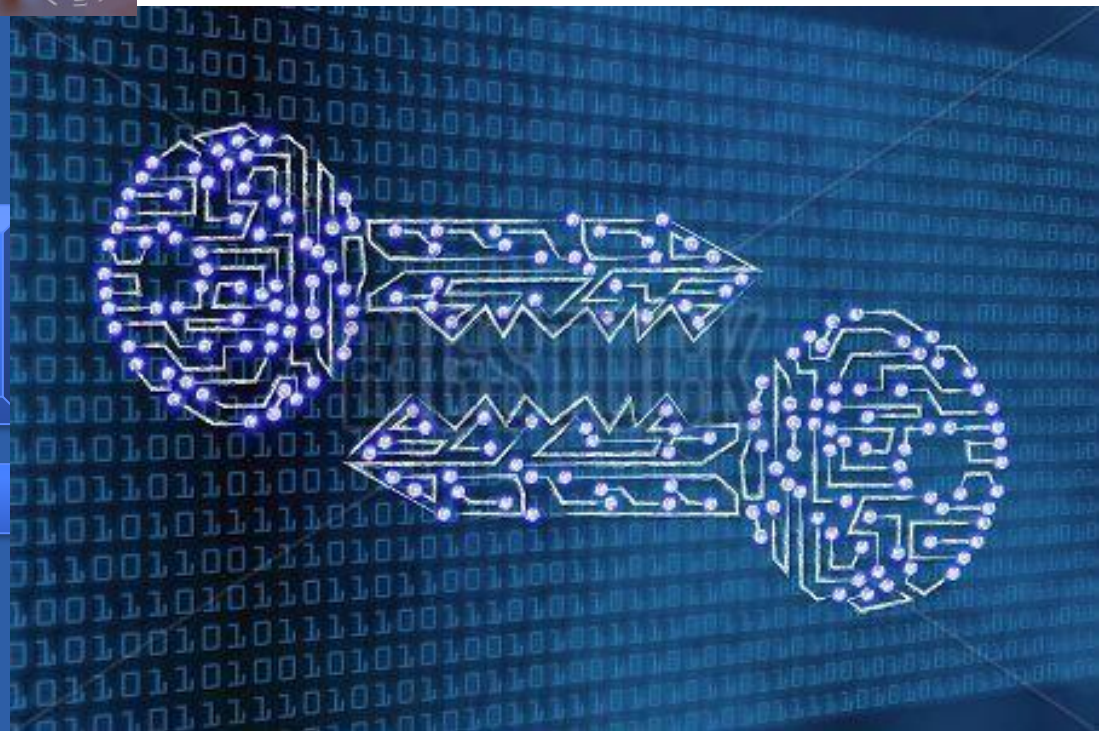
Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 5
Aplicaciones de la Criptografía





Comunicaciones Seguras

- ***SSH***
- ***HTTPS***
- ***IPSEC***
- ***VPN***

Comunicaciones Seguras: SSH

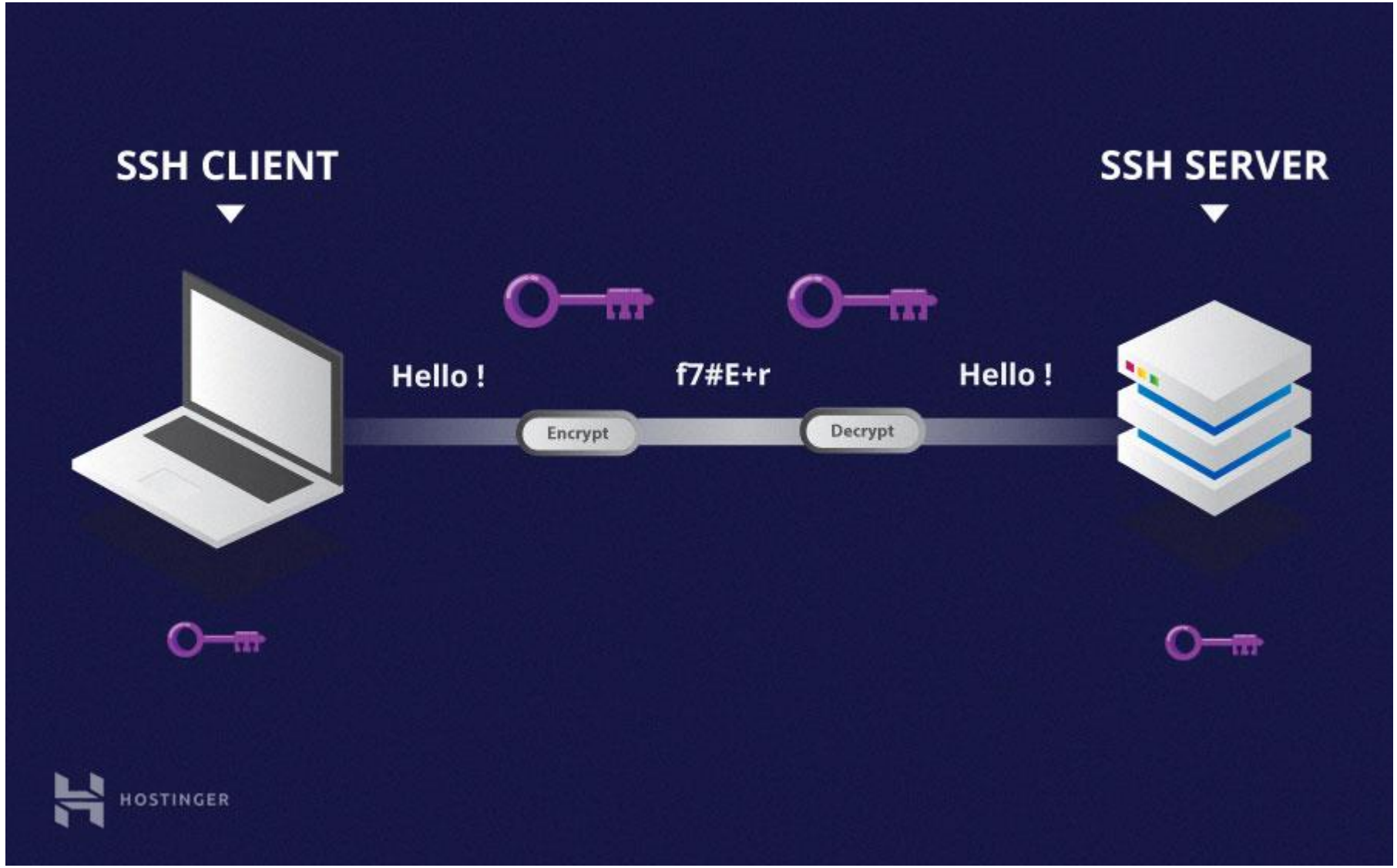
- **SSH™** (o Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios **conectarse a un host remotamente**.

- A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, **SSH encripta la sesión de conexión**, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

- SSH está diseñado para **reemplazar** los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como **telnet o rsh**.

- El uso de métodos seguros para registrarse remotamente a otros sistemas **reduce los riesgos** de seguridad tanto para el sistema cliente como para el sistema remoto.

Comunicaciones Seguras: SSH



Comunicaciones Seguras: SSH

- El protocolo SSH proporciona los siguientes tipos de protección:
  - Después de la conexión inicial, el cliente puede **verificar** que se está conectando al mismo servidor al que se conectó anteriormente.
  - El cliente transmite su **información de autenticación** al servidor usando una **encriptación** robusta de 128 bits.
  - Todos los **datos enviados y recibidos** durante la sesión se transfieren por medio de **encriptación** de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.
- Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para **asegurar protocolos inseguros**. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada **reenvío por puerto**, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

Comunicaciones Seguras: SSL, TLS y HTTPS

- **SSL** es el acrónimo de **Secure Sockets Layer** (capa de sockets seguros), la tecnología estándar para mantener segura una **conexión** a Internet, así como para proteger cualquier **información confidencial** que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.

- Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

- Esto lo lleva a cabo asegurándose de que todos los datos que se transfieren entre usuarios y sitios web o entre dos sistemas sean imposibles de leer. Utiliza algoritmos de **cifrado** para codificar los datos que se transmiten.

Comunicaciones Seguras: SSL, TLS y HTTPS

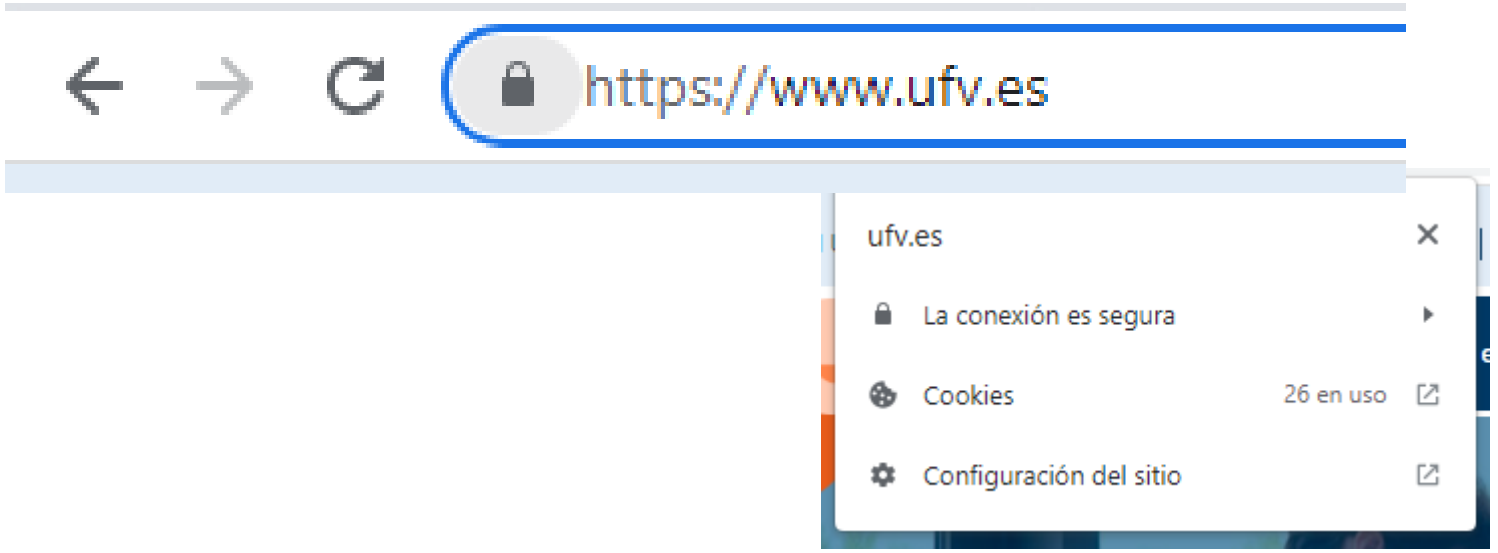
- El protocolo **TLS** (***Transport Layer Security***, seguridad de la capa de transporte) es solo una versión **actualizada y más segura de SSL**.

- Si bien aún denominamos a algunos certificados de seguridad SSL porque es un término más común, al comprar certificados SSL, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

Comunicaciones Seguras: SSL, TLS y HTTPS

- **HTTPS** (Hyper Text Transfer Protocol Secure o protocolo seguro de transferencia de hipertexto) aparece en la dirección URL cuando un sitio web está protegido por un certificado SSL.

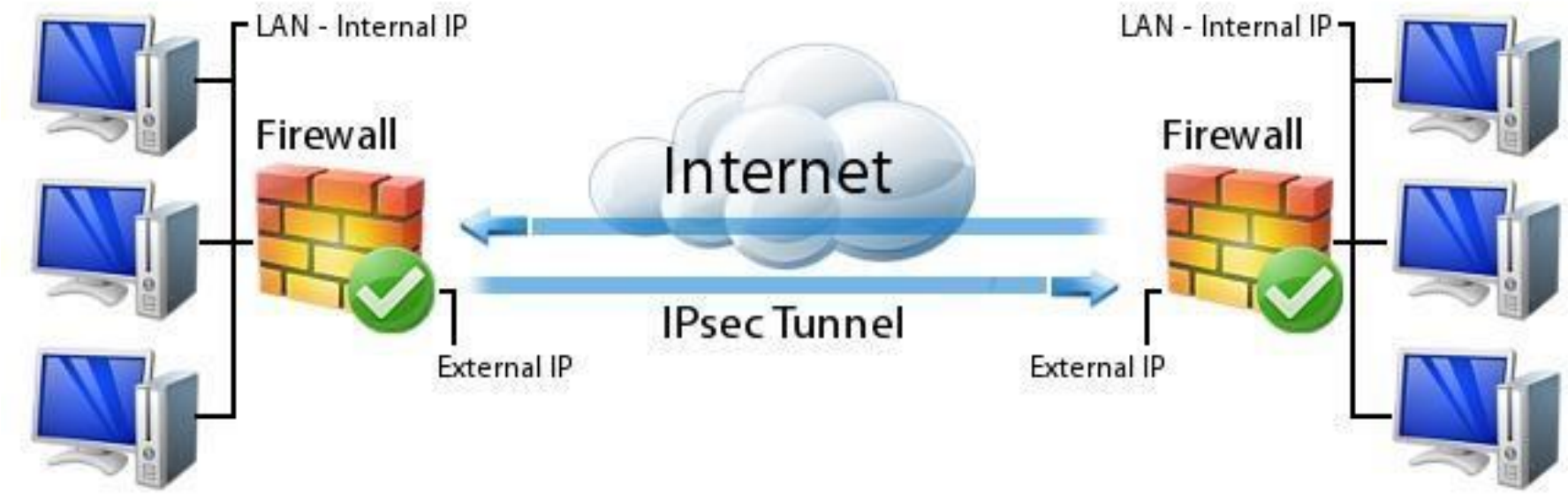
- Los detalles del certificado, por ejemplo la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado de la barra del navegador.



Comunicaciones Seguras: IPSEC

- **IPsec** (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

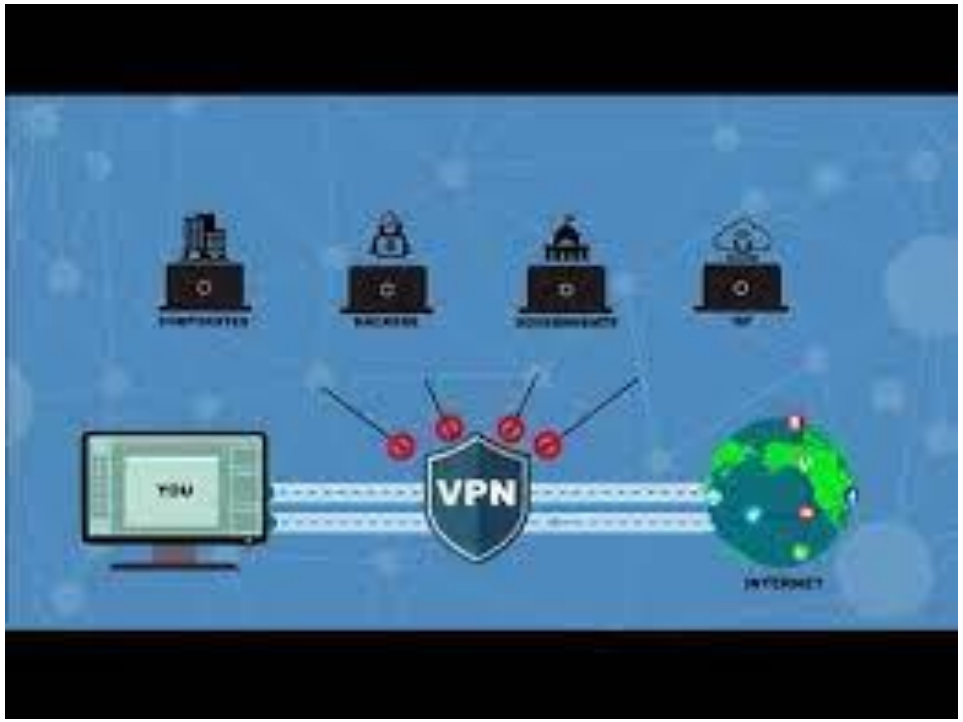
- IPsec también incluye protocolos para el establecimiento de claves de **cifrado**.



Comunicaciones Seguras: VPN

- Una **VPN** significa 'red privada virtual' (***virtual private network***). Es una herramienta digital que redirige tu tráfico de internet a través de un túnel seguro, **ocultando tu dirección IP y encriptando tus datos**.

Así es como una VPN mantiene tus datos privados y te protege frente a potenciales. ciberataques



Blockchain

Blockchain es un libro mayor (**ledger**) compartido e inmutable que facilita el proceso de registro de **transacciones** y de seguimiento de **activos** en una red de negocios.

Un *activo* puede ser tangible (una casa, un auto, dinero en efectivo, terrenos) o intangible (propiedad intelectual, patentes, derechos de autor, marcas).

Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de blockchain, reduciendo el riesgo y los costos para todos los involucrados.

Blockchain: Elementos Clave

- Tecnología de libro mayor distribuido

Todos los participantes de la red tienen acceso al libro mayor distribuido y a su registro inmutable de transacciones. Con este libro mayor compartido, las transacciones se registran solo una vez, eliminando la duplicación del esfuerzo que es típico de las redes de negocios tradicionales.

- Registros inalterables

Ningún participante puede cambiar o falsificar una transacción una vez grabada en el libro mayor compartido. Si el registro de una transacción incluye un error, se debe añadir una nueva transacción para revertir el error, pero ambas transacciones serán visibles.

- Contratos inteligentes

Para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente, se almacena en el blockchain y se ejecuta automáticamente. Un contrato inteligente puede definir las condiciones para las transferencias de bonos corporativos, incluir los términos de un seguro de viaje que se pagará y mucho más.

Blockchain: Cómo funciona

- A medida que se produce una transacción, se registra como un "**bloque**" de datos

Estas transacciones muestran el **movimiento de un activo**, el cual puede ser tangible (un producto) o intangible (intelectual). El bloque de datos puede registrar la información de su elección: quién, qué, cuándo, dónde, cuánto e incluso la condición, como la temperatura de un envío de alimentos.

- Cada bloque está **conectado** al bloque anterior y al bloque posterior

Estos bloques forman una cadena de datos a medida que un activo se mueve de un lugar a otro o cambia de dueño. Los bloques confirman tanto el tiempo exacto como la secuencia de las transacciones y se unen de forma segura para evitar que se alteren o se inserten entre dos bloques existentes.

- Las transacciones se unen y forman una **cadena irreversible**: un blockchain

Cada bloque adicional refuerza la verificación del bloque anterior y, por lo tanto, de todo el blockchain. Esto hace que dicha cadena sea a prueba de manipulaciones, lo que constituye la ventaja principal de la inalterabilidad. Esto evita que alguien malintencionado modifique la cadena y crea un libro mayor distribuido de transacciones en la que usted y otros miembros de la red pueden confiar.

Seguridad en mensajería: WhatsApp

https://www.whatsapp.com/security/?lang=es

https://scontent.whatsapp.net/v/t39.8562-34/271639644_1080641699441889_2201546141855802968_n.pdf/WhatsApp_Security_Whitepaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=dNoryuSeF6EAX_MZ5Mt&_nc_ht=scontent.whatsapp.net&oh=01_AVyE-kzuWoSZoMb5hnSJVqm0sYWlZ1MmbWSOKhsyEElu-A&oe=624F363E

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 5
Aplicaciones de la Criptografía