COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

LECCIÓN 3
Ataque del 51%

Ataque al 51%

Tiempo de ejecución: 4 horas

Planteamiento de la sesión:

En la tercera sesión se profundizará en el concepto de participación total en la red que se expuso anteriormente, y cómo debe haber una regulación para no recibir posibles ataques en una blockchain. Al finalizar el desarrollo teórico se propone un cuestionario para evaluar los conceptos aprendidos.

Desarrollo de la sesión: 2 horas

Vulnerabilidades en blockchain

La tecnología blockchain genera una estructura de datos con características de seguridad incorporadas, fundamentada en principios de criptografía, descentralización y consenso, asegura la confiabilidad en las transacciones. En sistemas blockchain, los datos se organizan en bloques, siendo cada bloque portador de una transacción o un conjunto de transacciones.

Cada nuevo bloque se enlaza a todos los bloques anteriores mediante una cadena criptográfica, prácticamente inalterable. Todas las transacciones dentro de los bloques se validan y acuerdan a través de un mecanismo de consenso, garantizando la veracidad y corrección de cada transacción.

La descentralización se logra mediante la participación de los miembros en una red distribuida en la tecnología blockchain. No existe un punto único de fallo y ningún usuario individual puede modificar el registro de transacciones. A pesar de esto, existen variaciones en aspectos importantes de seguridad entre distintas tecnologías blockchain.

Tipos de blockchain (públicas y privadas):

Las blockchains tienen variaciones en cuanto a quiénes pueden participar y quiénes tienen acceso a los datos. Por lo general, se clasifican como públicas o privadas, lo que indica quién puede unirse, y con o sin permiso, describiendo cómo los participantes acceden a la red.

En el caso de las blockchains públicas, suelen permitir la participación de cualquier individuo y mantener el anonimato de los participantes. Estas blockchains utilizan computadoras conectadas a Internet para validar transacciones y alcanzar consenso. Estas redes carecen de controles de identidad significativos, salvo por las claves públicas.

En cambio, las blockchains privadas emplean la identidad para confirmar la membresía y los privilegios de acceso, generalmente permitiendo la participación sólo de organizaciones conocidas. Estas organizaciones forman una red comercial privada y exclusiva para sus miembros.

El consenso en una blockchain privada se logra a través del respaldo selectivo, donde usuarios conocidos verifican transacciones. Solo aquellos con acceso y permisos especiales pueden mantener el registro de transacciones. Este tipo de red requiere controles más estrictos de identidad y acceso.

Las redes privadas y autorizadas ofrecen un control estricto y son preferibles para cumplir con normativas y regulaciones. Sin embargo, las redes públicas y sin permiso pueden lograr una mayor descentralización y distribución.

Aunque la blockchain crea un registro de transacciones resistente a manipulaciones, las redes blockchain no son invulnerables a ciberataques y fraudes. Personas con intenciones maliciosas pueden aprovechar vulnerabilidades conocidas en la infraestructura de blockchain, habiendo logrado éxito en diversos ataques y fraudes a lo largo del tiempo. Algunos ejemplos incluyen:

1. Explotación de código:

Se refiere a la identificación y aprovechamiento de vulnerabilidades en el código de software para realizar acciones no autorizadas. Los contratos inteligentes, programas autónomos ejecutados en la cadena de bloques, pueden contener vulnerabilidades que podrían ser explotadas para realizar acciones por los atacantes.

2. Robo de claves:

El robo de claves en blockchain es especialmente crítico, ya que las claves privadas son esenciales para acceder y controlar los activos almacenados en una billetera criptográfica. Los ataques dirigidos a la obtención no autorizada de claves privadas pueden ocurrir a través de malware, phishing u otras tácticas.

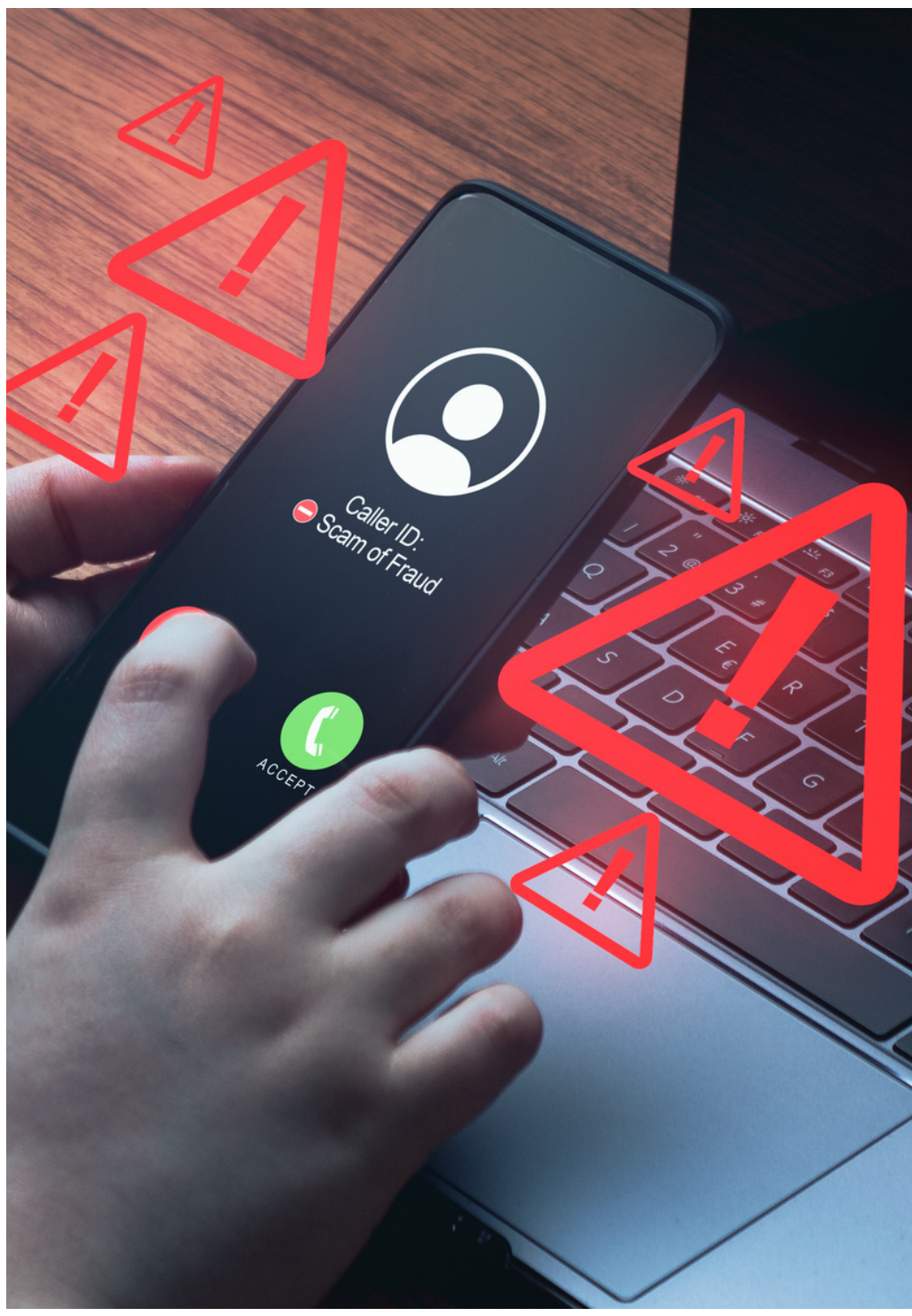
3.Hackeo de computadoras de usuarios:

Puede implicar el compromiso de los sistemas utilizados para interactuar con la cadena de bloques, como billeteras y aplicaciones descentralizadas (dApps). Los atacantes podrían buscar acceder a las claves privadas, manipular transacciones o realizar todo tipo de acciones.

Los ataques a las redes blockchain son muy comunes debido a las grandes cantidades de dinero que estas contienen y hay varios métodos usados para este propósito.

Ataques de Phishing:

El phishing representa un intento de estafa dirigido a obtener las credenciales de un usuario. En estos casos, los estafadores envían correos electrónicos a los titulares de claves de billetera, simulando ser fuentes legítimas.



Estos correos electrónicos solicitan a los usuarios que proporcionen sus credenciales a través de enlaces falsos. Obtener acceso a estas credenciales y otra información confidencial puede ocasionar pérdidas tanto para el usuario individual como para la red blockchain dependiendo de lo que el atacante decida hacer con los accesos.

Ataques de Enrutamiento:

Dado que las blockchains dependen de grandes transferencias de datos en tiempo real, los hackers pueden interceptar estos datos durante su transferencia a proveedores de servicios de Internet.

En un ataque de enrutamiento, los participantes de la blockchain generalmente no pueden detectar la amenaza, ya que todo parece normal en la superficie. Sin embargo, en segundo plano, los estafadores han extraído datos confidenciales o incluso monedas.

Ataques de Sybil:

En un ataque de Sybil, los hackers crean y utilizan múltiples identidades de red falsas para inundar la red y comprometer el sistema. El término "Sybil" hace referencia a un personaje famoso de un libro diagnosticado con trastorno de identidad múltiple.

Ataques del 51%

La minería en blockchain requiere una gran potencia informática, especialmente en blockchains públicas a gran escala. Sin embargo, si un minero o grupo de mineros logra reunir suficientes recursos, podrían alcanzar más del 50% de la potencia de minería en una red blockchain, esto implica tener control sobre el registro de transacciones y la capacidad de manipularlo según sus intereses. Es importante destacar que los blockchains privados no son vulnerables a los ataques del 51%.

En otras palabras, tendrían más capacidad de cálculo que todos los demás mineros y más influencia en las "votaciones" que todos los demás participantes combinados.

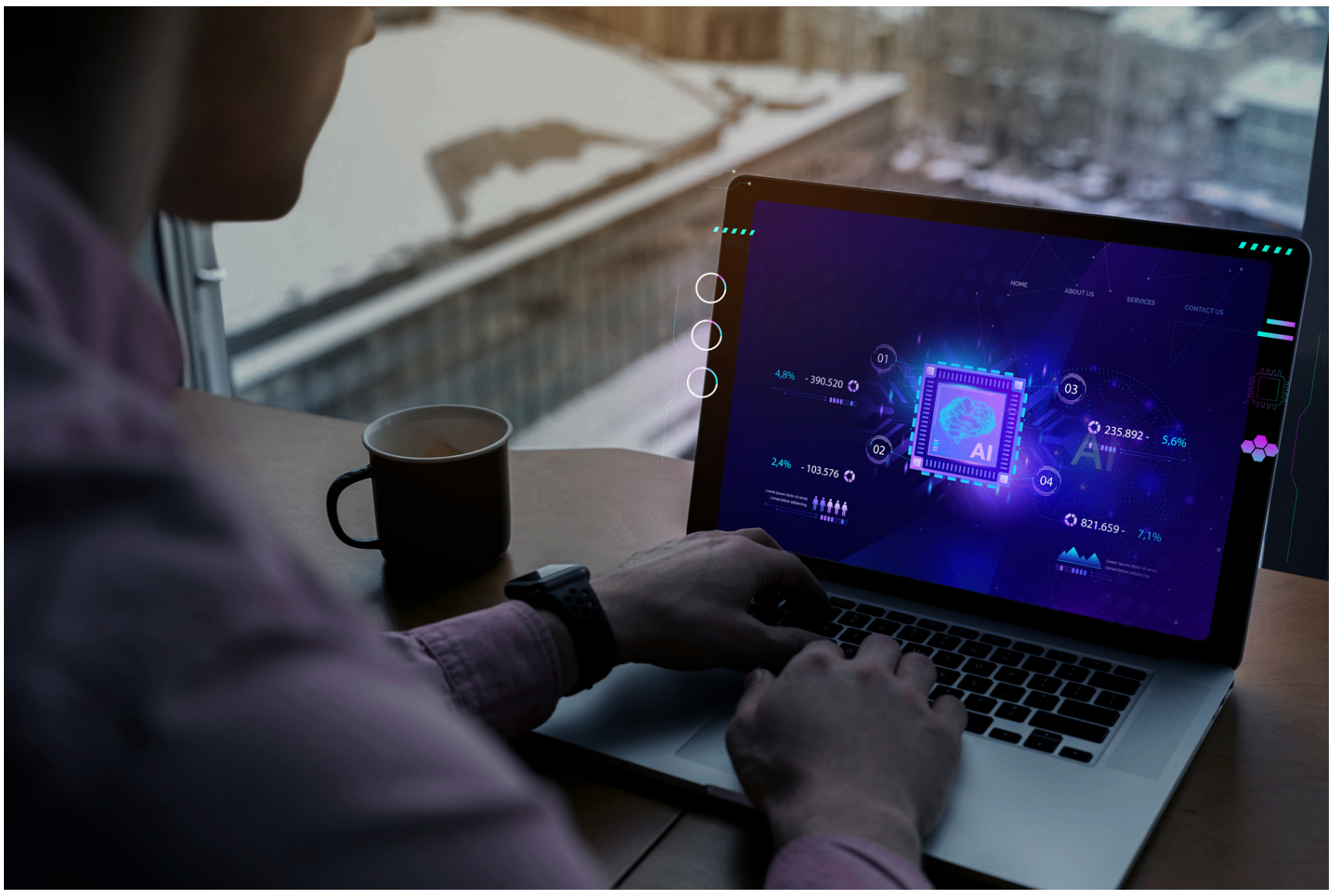
Esta situación tiene el potencial de afectar negativamente el funcionamiento de la red de forma temporal, según la teoría.
Incluso el whitepaper de Bitcoin aborda directamente el escenario de un ataque del 51%, reconociéndose como un desafío que debe ser considerado en este tipo de infraestructuras distribuidas.

Históricamente, estas preocupaciones no son exclusivas del presente. En el pasado, se vivieron períodos de incertidumbre relacionados con el "fantasma" del ataque del 51% en Bitcoin. A principios de 2014, la empresa de minería en la nube Ghash.IO se aproximaba peligrosamente al 50% del total de la potencia de hash de la red Bitcoin.

Esta situación generó inseguridades entre los usuarios recién llegados a Bitcoin. Sin embargo, en la actualidad, la empresa ya no está operativa, y el poder de hash de Bitcoin se distribuye de manera más amplia.

Es importante señalar que, debido al entorno competitivo, un atacante malintencionado estaría obligado a ejecutar su ataque de manera constante y en cuestión de segundos, lo cual resulta prácticamente imposible ya que cada bloque se mina en un intervalo de 10 minutos. Incluso si lograra llevar a cabo el ataque en otro momento o contexto, el escenario cambiaría.

En caso de éxito, se tendría un control aparente sobre la red, pero a un costo significativo. ¿Con qué propósito? Por ejemplo, podría intentar realizar doble gastos, aunque esto eventualmente sería detectado por la red, que respondería con una bifurcación para eliminar la amenaza.



Vale la pena destacar que muchas entidades financieras que inicialmente expresaron preocupaciones sobre la vulnerabilidad de Bitcoin han tenido que rectificar sus afirmaciones. Después de un análisis más profundo de cómo funciona, Bitcoin emitió un estudio que asegura que actualmente es prácticamente imposible comprometer la seguridad de la red mediante un exitoso ataque del 51%.