2024

CERTIFICACIÓN
BLOCKCHAIN 2.0

SEBASTIAN
ALVAREZ HERRERA

MÓDULO 1

SEBASTIAN
ALVAREZ HERRERA

HISTORIA DEL INTERNET: GRANDES HITOS

1969 Se creó ARPAnet red infromática que conectó a diversas universidades norteamericanas

A principios de los 70 Robert Kahn y Vinton Cerf desarrollaron un nuevo protocolo de comunicación conocido como TCP/IP

Nace el correo electrónico en 1971, la primera aplicación se llamó SNDMGS

En 1983 ARPAnet adoptó el protocolo TCP/IP dando como resultado la definición incipiente de internet

En 1988 nace el lenguaje de hipertexto HTML y otras especificaciones como la URL o el HTTP

World wide web (www) se presento en 1991

Se funda en 1996 Hotmail, fué uno de los primeros servicios web de email que existió en la red

Acuerdo internacional para el registro de dominios en 1996

En 1998 Larry Page y Sergey Brin crean Google

En 2005 Youtube es fundada por varios ingenieros y se convierte en la mayor red para compartir videos

En 2006 internet tiene 100.000 millones de usuarios

Facebook existe desde el año 2006, Mark zuckerberg fundó la red social que cuenata con más de 2.200 millones de usuarios

SEBASTIAN ALVAREZ HERRERA

HISTORIA Y EVOLUCIÓN DEL DINERO

Para adentrarnos en la historia y evolución del dinero, primero debemos comprender su origen y qué función tiene dentro de la sociedad. El dinero es todo activo o bien que es generalmente aceptado como medio de pago por los agentes económicos para sus intercambios. Surge en la historia para suplir la escasa eficiencia del trueque, que empezó a utilizarse en el neolítico con los primeros asentamientos humanos.

SEBASTIAN
ALVAREZ HERRERA

EVOLUCIÓN DEL DINERO

Trueque

Oro

Moneda

Papel moneda

Dinero plástico

Dinero digital

SEBASTIAN ALVAREZ HERRERA

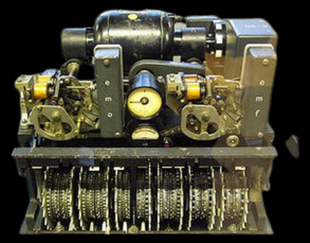
CRIPTOGRAFÍA

SEBASTIAN
ALVAREZ HERRERA

FUNDAMENTOS CRIPTOGRÁFICOS

La criptografía (del griego (kryptos), ”ocultos”, y (grafein) “escritura”, literalmente “escritura oculta” se ha definido tradicionalmente como el ámbito de la criptología, que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ilegibles a receptores no autorizados”

Escítala: Sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos.



Máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes destinados a generales de muy alto rango.

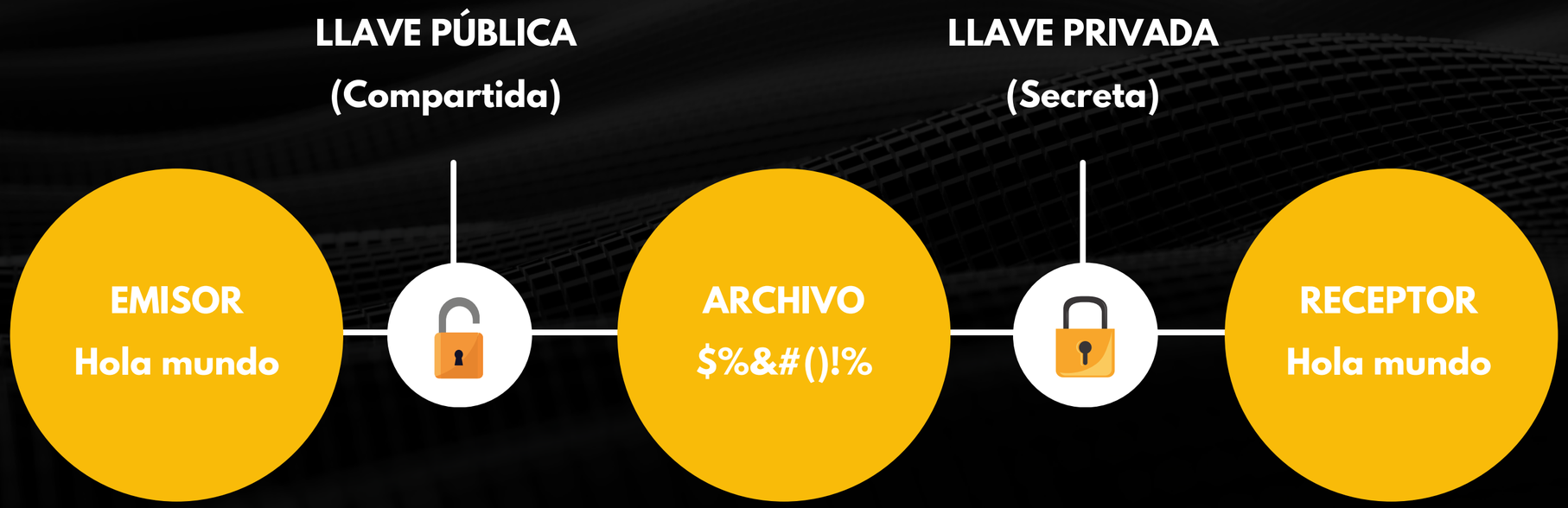
SEBASTIAN
ALVAREZ HERRERA

CRIPTOGRAFÍA SIMÉTRICA

Misma llave de cifrado y descifrado.

SEBASTIAN
ALVAREZ HERRERA

CRIPTOGRAFÍA ASIMÉTRICA



Llaves de cifrado y descifrado son distintas

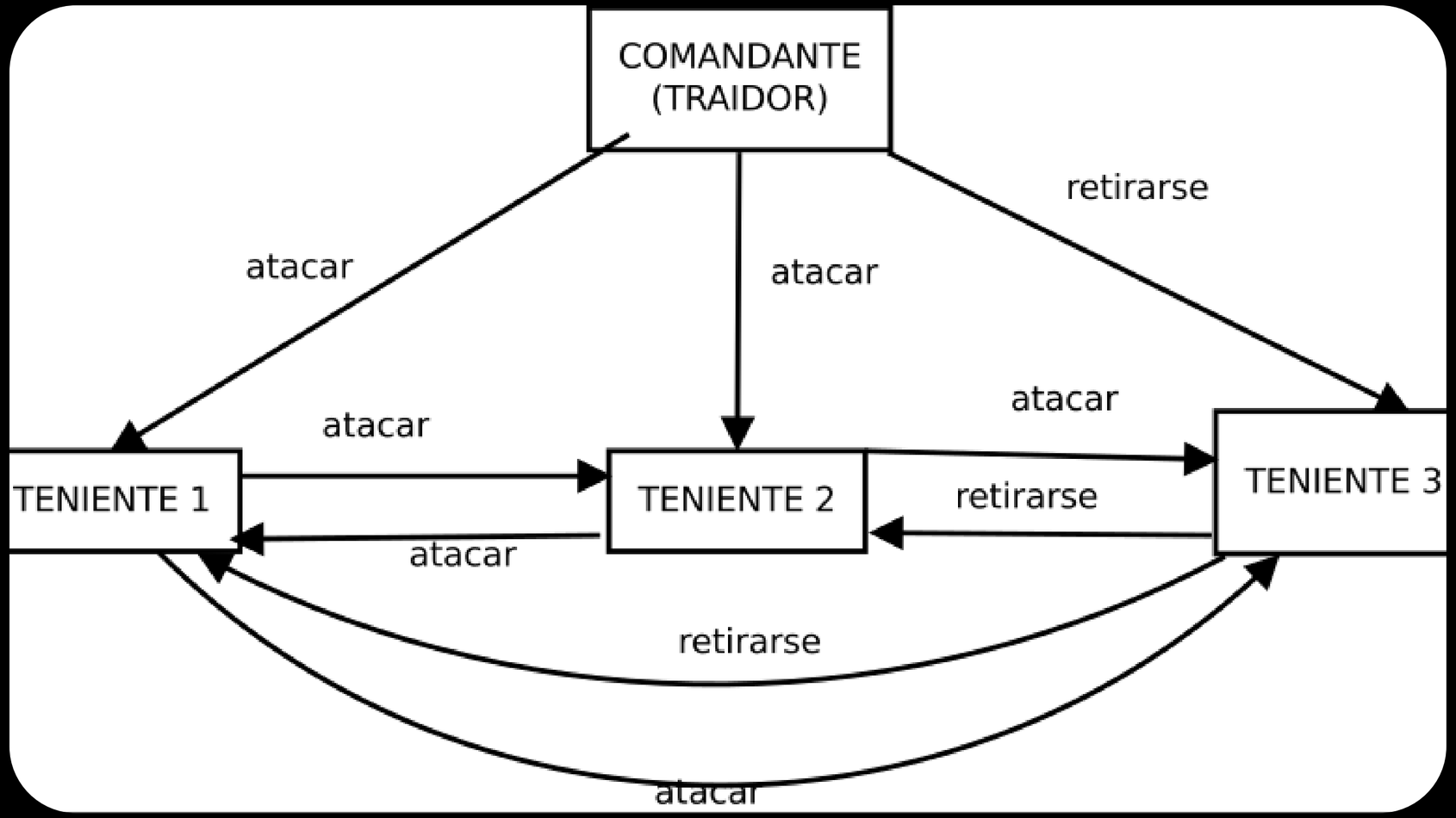
SEBASTIAN
ALVAREZ HERRERA

CRIPTOGRAFÍA HÍBRIDA

SEBASTIAN
ALVAREZ HERRERA

EL PROBLEMA DE LOS GENERALES BIZANTINOS.

SEBASTIAN
ALVAREZ HERRERA



ALGORITMOS DE CONSENSO.

SEBASTIAN
ALVAREZ HERRERA

ESTOS MODELOS DE CONSENSO DE BLOCKCHAIN CONSISTEN EN ALGUNOS OBJETIVOS PARTICULARES TALES COMO:

- Llegar a un acuerdo: El mecanismo reúne todos los acuerdos del grupo tanto como puede.
- Colaboración: Cada uno en el grupo apunta a un mejor acuerdo que resulte en los intereses colectivos del grupo.
- Cooperación: Cada miembro trabajará en equipo y dejará de lado sus propios intereses.
- Igualdad de derechos: Cada uno de los participantes tiene el mismo valor en la votación. Esto significa que el voto de cada persona es importante.
- Participación: Todos los que están dentro de la red, deben participar en la votación. Nadie se puede quedar por fuera de la votación.
- Actividad: Cada miembro del grupo es igualmente activo. No hay miembros con más responsabilidades que otros en el grupo

SEBASTIAN
ALVAREZ HERRERA

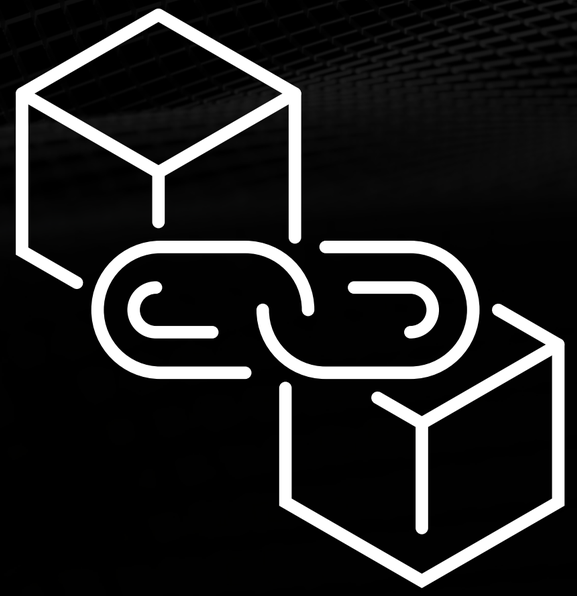
¿POR QUÉ NECESITAMOS ALGORITMOS DE CONSENSO?

- El problema principal de una falla bizantina es el poder llegar a un acuerdo. Si se produce un solo fallo, los nodos no podrán llegar a un acuerdo o tendrán un valor de dificultad mayor.
- Por otro lado, los algoritmos de consenso no se enfrentan a este tipo de problema. Su objetivo principal es el de alcanzar una meta específica por cualquier medio.
- Por eso, cuando podría haber resultados contradictorios en un sistema distribuido; es mejor usar algoritmos de consenso para una mejor salida.

SEBASTIAN
ALVAREZ HERRERA

TIPOS DE ALGORITMOS DE CONSENSO

1. Proof of Work.
2. Proof of Stake.
3. Delegated Proof of Stake.
4. Proof of Elapsed Time.
5. Byzantine Fault Tolerance.
6. Enjambre.
7. Proof of Authority.



SEBASTIAN
ALVAREZ HERRERA

PROOF OF WORK

La generación de una cadena de bloques válida tiene que ser un proceso relativamente costoso

- Ideal, tan costoso que no lo pueda hacer ningún individuo o grupo
- Si no, cualquiera podría reescribir las transacciones registradas
- El concepto de “Prueba de Trabajo” se creó como una medida para combatir el spam
- Encontrar una solución a un puzzle criptográfico relacionado al mensaje o transacción enviada, mediante muchas pruebas aleatorias.

SEBASTIAN
ALVAREZ HERRERA

VENTAJAS

- Muy descentralizado
- Fácil de implementar
- Muy seguro
- Resiste hasta un 51% de nodos deshonestos
- Usado en las dos cadenas más importantes

PROBLEMAS

- Mucho consumo eléctrico
- Poco escalable
- Necesita muchos nodos para mantenerse seguro

SEBASTIAN
ALVAREZ HERRERA

ALTERNATIVAS AL PROOF OF WORK

Objetivos

- Mejorar la escalabilidad
- Reducir el consumo energético

Consideraciones de diseño

- Tolerancia a nodos deshonestos
- Cantidad de transacciones por segundo
- Tiempo de generación del bloque
- Finalidad de las transacciones
- Grado de descentralización

SEBASTIAN
ALVAREZ HERRERA

PROOF OF STAKE

En lugar de entregar la solución a un puzzle, debo dejar un depósito en garantía a cambio del derecho a generar bloques

- Se hacen verificaciones cruzadas de las transacciones aceptadas
- Si intento ser deshonesto, se quema el depósito en garantía
- Muchos ven en esto el futuro de los blockchains

SEBASTIAN
ALVAREZ HERRERA

VENTAJAS

- Menor consumo energético
- Más seguro con menos “masa”
- Permitiría dividir la cadena en cadenas más pequeñas
- Sharding
- Más rápido

PROBLEMAS

- Ha costado generar un algoritmo que impida la concentración extrema del control de la red
- Atenta contra los intereses de los actuales mineros

SEBASTIAN
ALVAREZ HERRERA

ALGORITMOS DE CONSENSO

¿Por qué es importante entender la base de los algoritmos?

1. Nos permitirá elegir que tipo de protocolo podemos usar.

2. Entender las complejidades y puntos débiles.

3. Comprender posibles vulneraciones que se puedan desarrollar.

4. Modelo de gobernanza a implementar.

SEBASTIAN
ALVAREZ HERRERA