CRIPTOGRAFíA

I Funciones de Hash

- Funciones de Hash: SHA256; SHA512; RIPEMD160, etc — SHA256 paso a paso
- Base 58 para calcular direcciones

II Aritmética Modular

- Criptografía Matemática o Aritmética Modular.

III TIPOS de criptografía. Cifrado y Descifrado

- CRIPTOGRAFÍA SIMÉTRICA: Cifrado Julio César, AES
- CRIPTOGRAFÍA ASIMÉTRICA. Cifrado el Gamal, RSA y ECC
- CRIPTOGRAFÍA HÍBRIDA: Algoritmo de Diffie Hellman

IV PROPIEDADES A CUMPLIR o NO Va a DEPENDER

- La CONFIDENCIALIDAD
- La INTEGRIDAD
- La AUTENTICIDAD
- El NO REPUDIO

V ECC o Curvas Elípticas

- Es un tipo especial de Criptografía Modular con una función Eliptic Curve Cryptografy o Curvas Elípticas. Se hace el Módulo y por eso tenemos pares de puntos (x,y) de enteros. Bitcoin, Ethereum y muchas criptomonedas las utilizan. — Curva de Bitcoin — Explicación extra

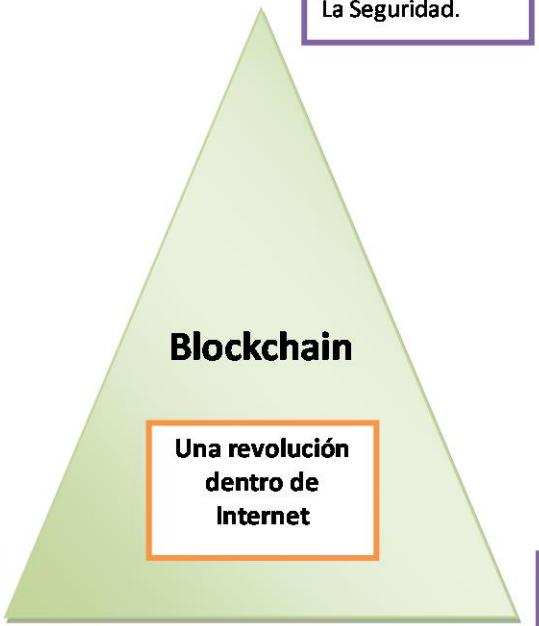
VI PRESENTE Y FUTURO

- Otras formas utilizando Matrices o Algebras con Espacios Vectoriales.
- El futuro pasa por la Criptografía POST-CUÁNTICA
- Tranquilos porque ya hay muchos avances.

La Blockchain-Esquema I

Los tres PILARES de la Blockchain

1) La Seguridad
2) Redes Distribuidas
3) Incentivos



Criptografía
La Seguridad.

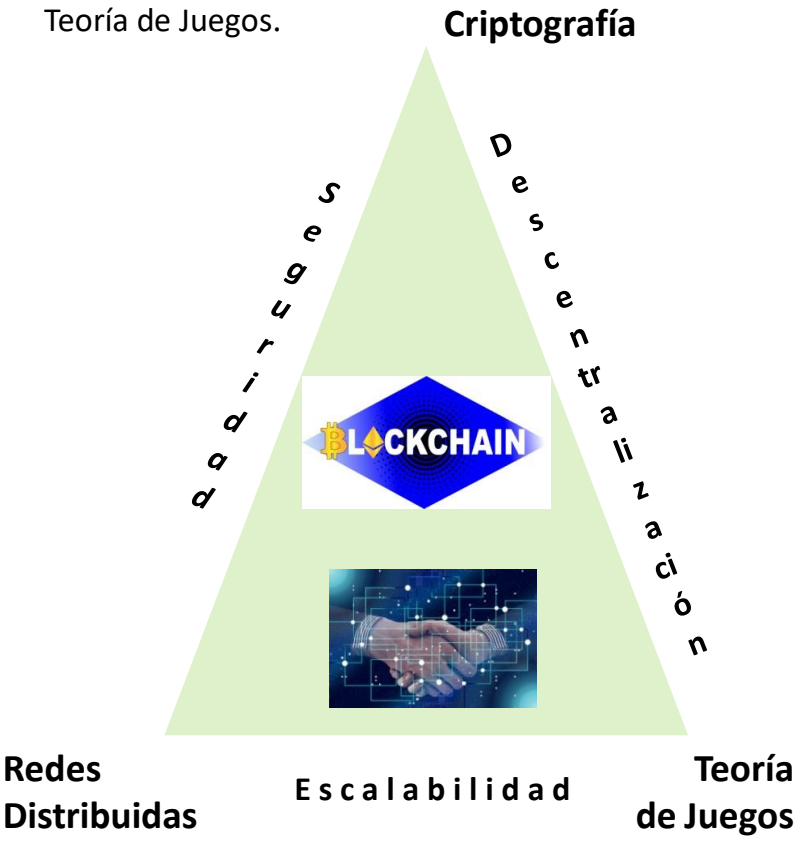
PROPIEDADES
1) Descentralizada
2) Incorruptible
3) Transparente
4) Información perdurable
5) Tx seguras y confiables
6) Posibilidad de ESCALAR

Redes distribuidas
Consenso: RAFT, PBFT, PoW, PoS
el consenso es fundamental en esta red descentralizada.

Teoría de Juegos
para calcular los incentivos para los actores de esta gran red.

Propiedades de la Blockchain (IV)

Los 3 pilares de la Blockchain:
Criptografía.
Redes Distribuidas.
Teoría de Juegos.



.- Las **Transacciones son seguras** y confiables, gracias a la criptografía.

.- **Descentralización**. No hay un ordenador central tomando las decisiones, estas se hacen de forma **consensuada** por muchos nodos.

.- **Escalabilidad** o capacidad de crecer. Los developers de ahora mismo están investigando y desarrollando en la capa 2 para ganar velocidad en las Transacciones. Ejemplo: la zkEVM de Polygon.

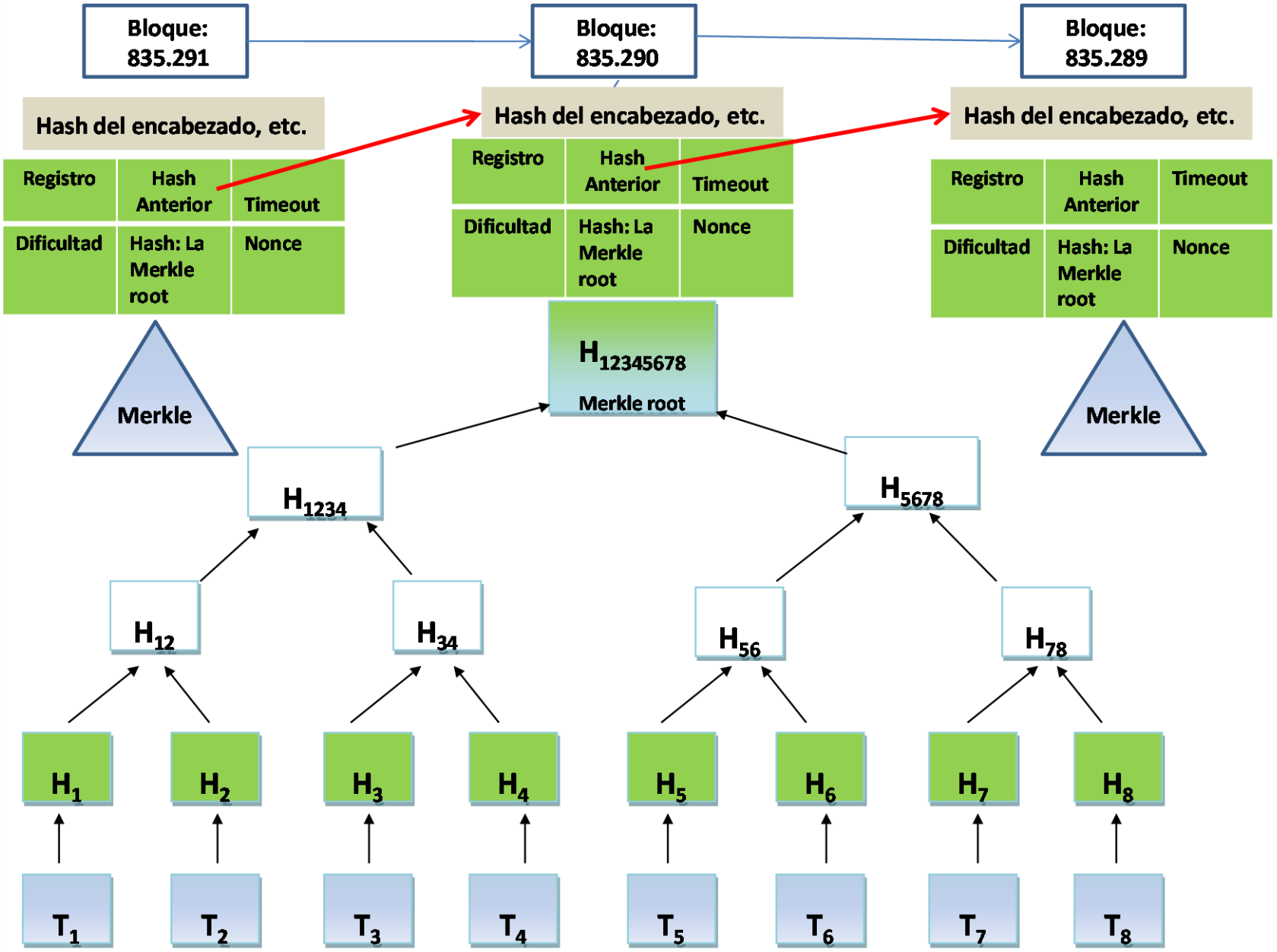
.- La información es **PÚBLICA** y por tanto **Transparente**. Podemos ver los datos menos el nombre de la persona.

.- **Inmutable**. No se puede borrar ni modificar una vez que el bloque es minado. La información queda definitivamente para la historia.

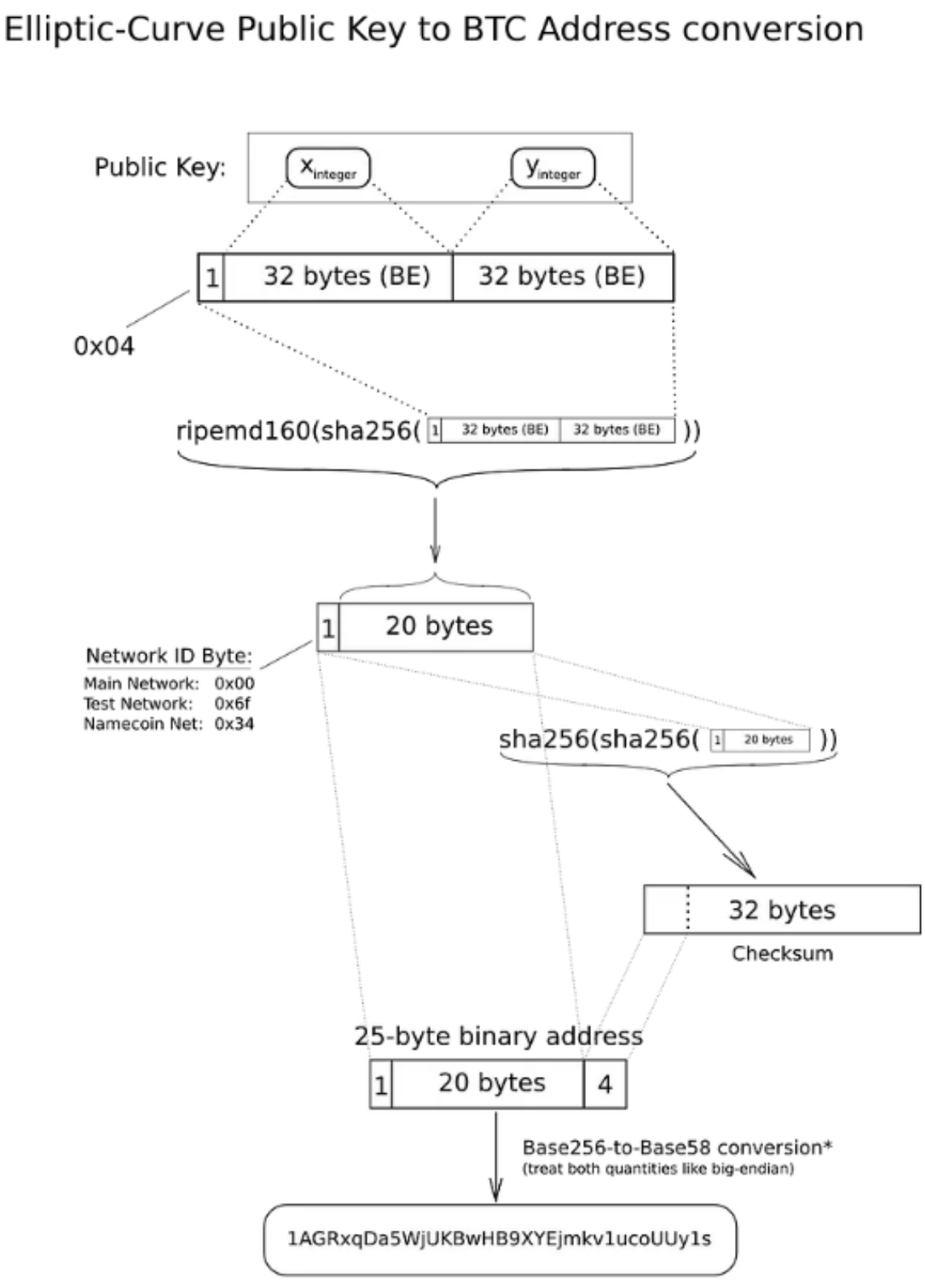
.- La información es **Perdurable** en el tiempo. Nunca se pierde. Tenemos la historia completa.

.- La Blockchain es esencial para **Internet de las cosas** o **IOT**. La criptomoneda IOTA NO utiliza la tecnología Blockchain. Lo hace con la tecnología Tangle, que en lugar de la cadena de bloques, existe un DAG (= grafo acíclico dirigido) que llamamos «tangle» o «enredo»
https://cutt.ly/B8xjH9e

¿Qué se guarda en un Bloque?: Las Tx (en texto plano) y lo de color verde y gris. La mayoría en SHA256 y otros códigos como el Timeout, Dificultad, Registro, Nonce. Los 6 datos del rectángulo verde forman el encabezado del bloque que ocupa 80 bytes fijos siempre.



Ejemplo ¿Qué hace Bitcoin?



*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'