Fundamentos de Blockchain en Algorand

Dra. Rocío A. Aldeco P.

Semestre 2023-1

Algorand
Centre of Excellence

Elementos criptográficos

Algorand
Centre of Excellence

Hash

- Una **función hash** es una función sólo de ida que se utiliza para mapear información digital de cualquier longitud a datos digitales de tamaño fijo.
- Los valores devueltos por una función hash se llaman valores hash.
- Este valor hash es único para un valor de entrada dado, así cualquier cambio en los datos de entrada cambia de manera significativa el dato de salida.

Hash 

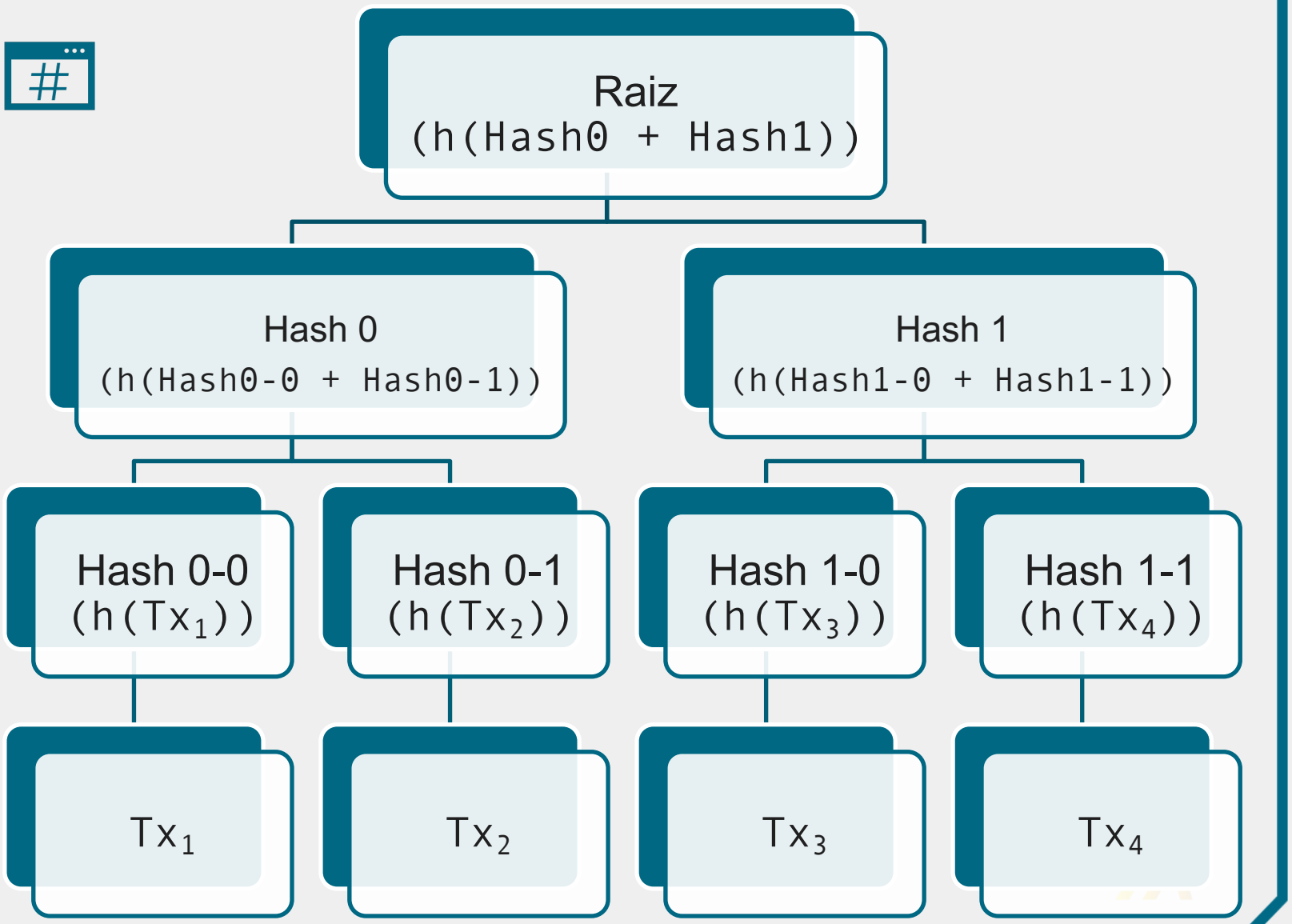
- El uso de la función hash garantiza la integridad de los datos.
- **Cadena de hash** es la aplicación sucesiva de una función hash sobre ciertos datos.

$d_1 \rightarrow d_2 \rightarrow d_3 \rightarrow \ldots \rightarrow d_n$

$hash(d_1) \rightarrow hash(hash(d_1)|hash(d_2)) \rightarrow hash(hash(hash(d_1)|hash(d_2))|hash(d_3)) \rightarrow \ldots$

Árbol de Hash

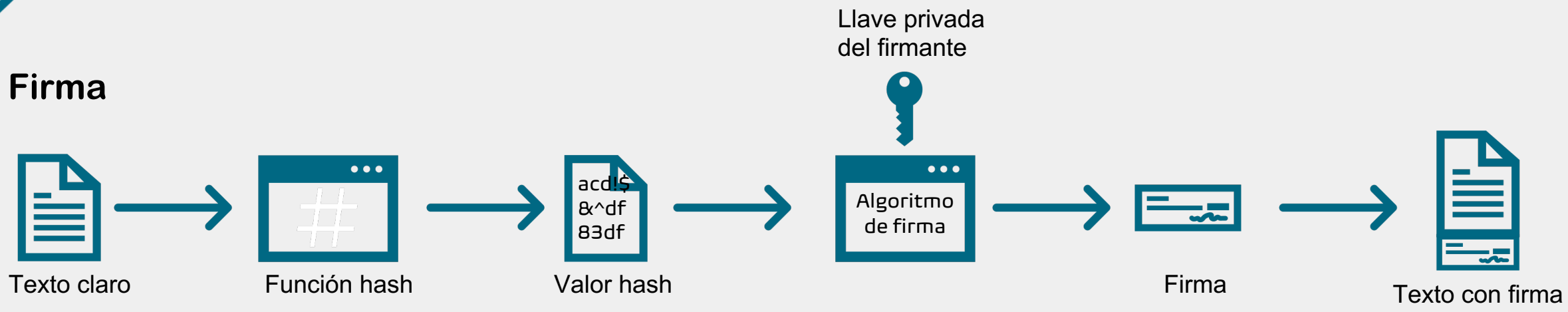
- Un **árbol de hash** o Merkle-tree es un árbol en el que cada nodo hoja está etiquetado con el hash criptográfico de un bloque de datos.
- Los nodos no hoja están etiquetado con el hash criptográfico de las etiquetas de sus nodos hijos.
- Los árboles de hash permiten una verificación eficiente y segura del contenido de grandes estructuras de datos.



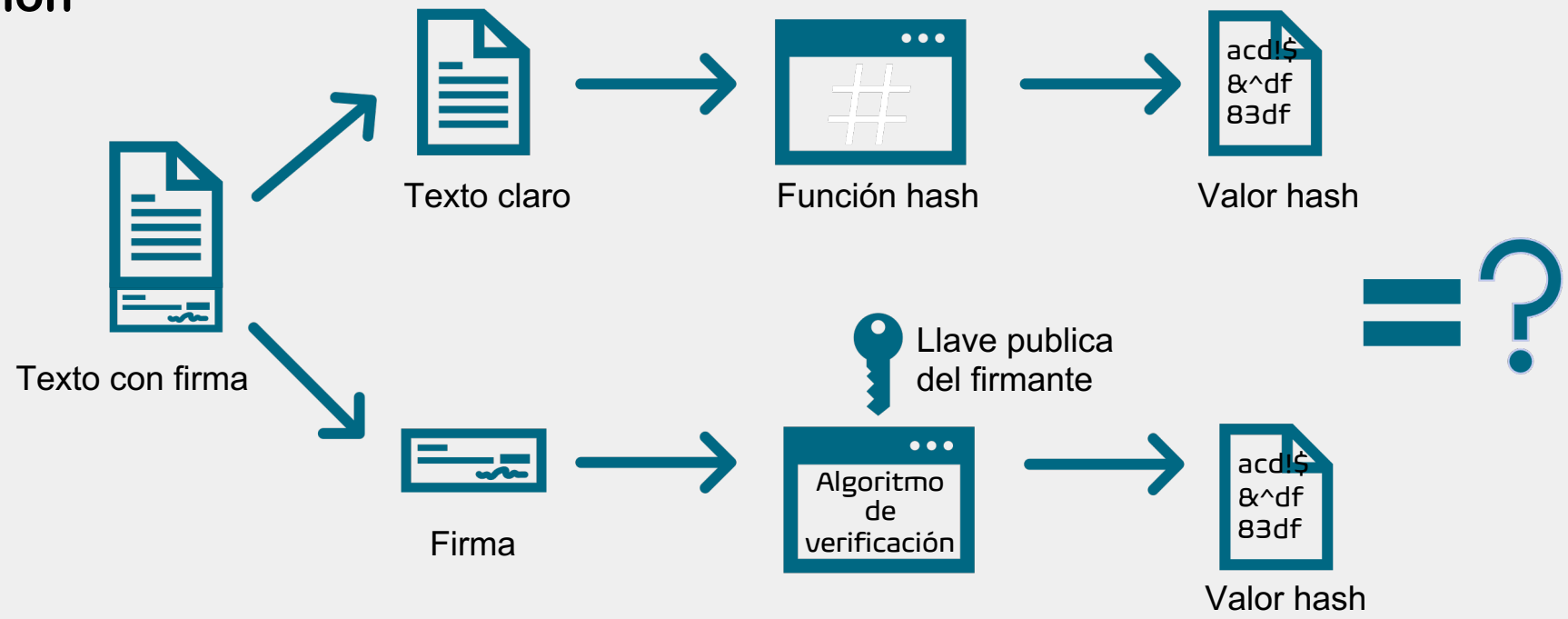
Firma digital

- La **firma digital** es un esquema que sirve para verificar la autenticidad de mensajes.
- Una firma digital válida ofrece al receptor razones para creer que el mensaje fue creado por un remitente conocido (autenticación), y que el mensaje no fue alterado en tránsito (integridad).

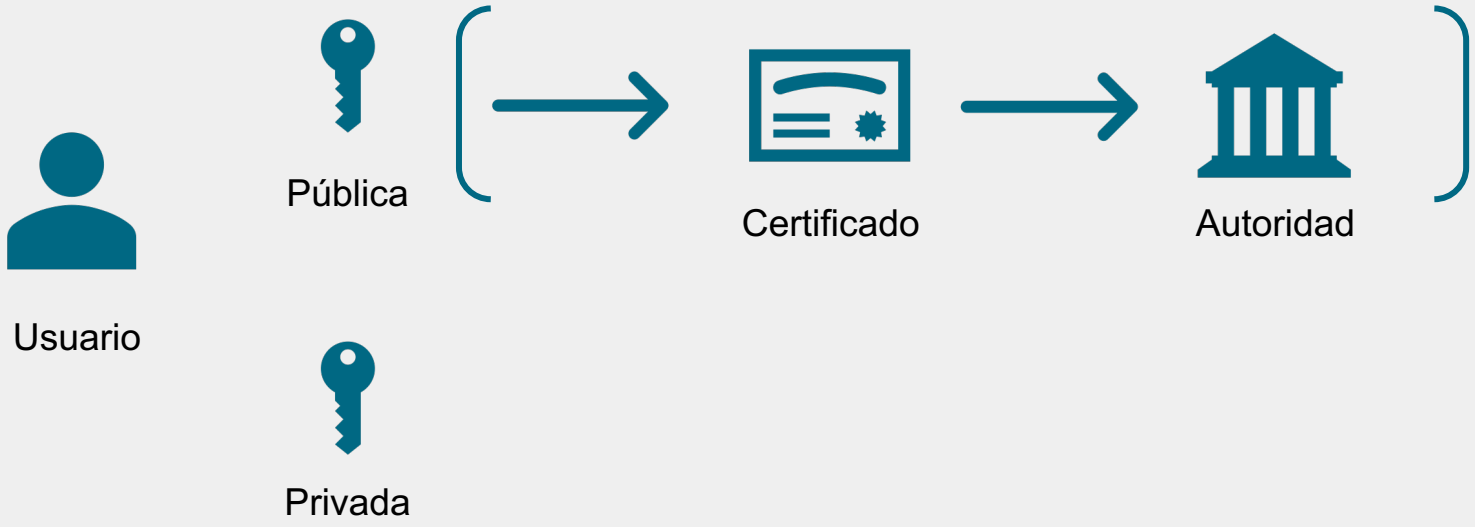
Firma



Verificación



Autenticación



PROPUESTAS DE MEJORA

- Nuevos protocolos de consenso: PoS, PoH, VRF, VDF…
- *Sharding*. Dividir una red en una serie de bloques de base de datos separados ("shards") haciendo a la blockchain más manejable.

Ethereum	Algorand	Solana	Cardano	Polkadot	Avalanche
2015	2019	2020	2017	2020	2020
PoW	PPoS	PoS	PoS (Ouroboros)	NPoS	PoS
ETH 2.0	VRF	PoH (VDF)	Hydra	Parachains	Probabilistic Leaderless BFT