Merkle trees

¿Cómo funciona Bitcoin?

Contenidos

Una clase de estructura de datos:

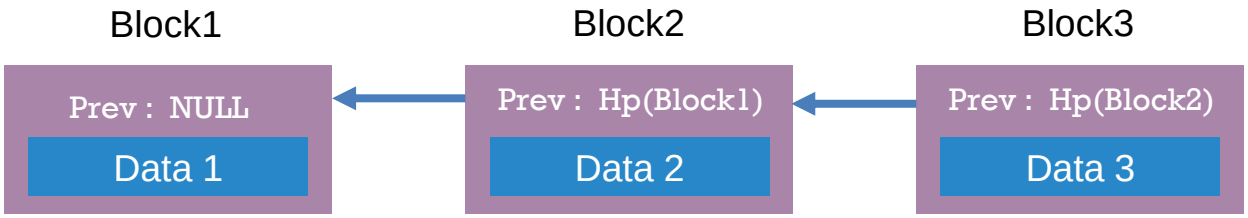
- Hash pointers
- Blockchain

Contenidos

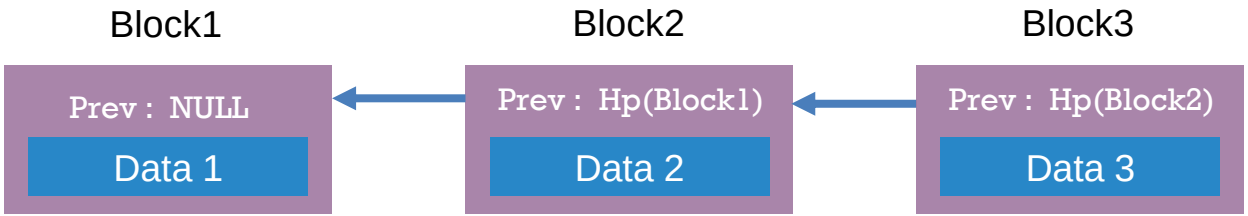
Una clase de estructura de datos:

- Hash pointers
- Blockchain
- Merkle trees

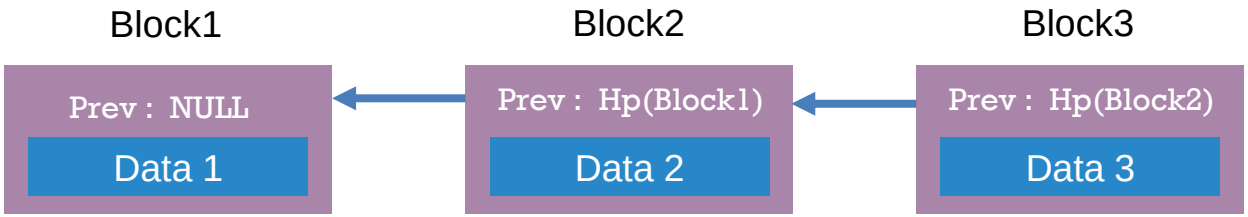
Una debilidad



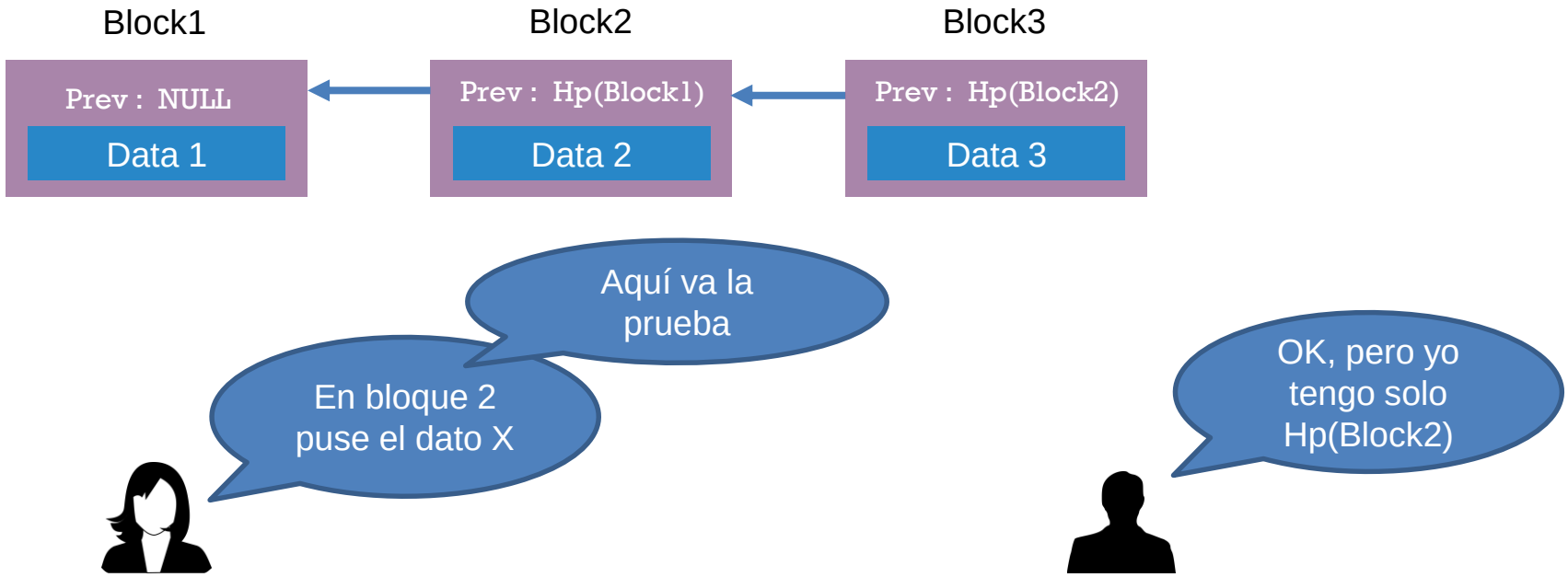
Una debilidad



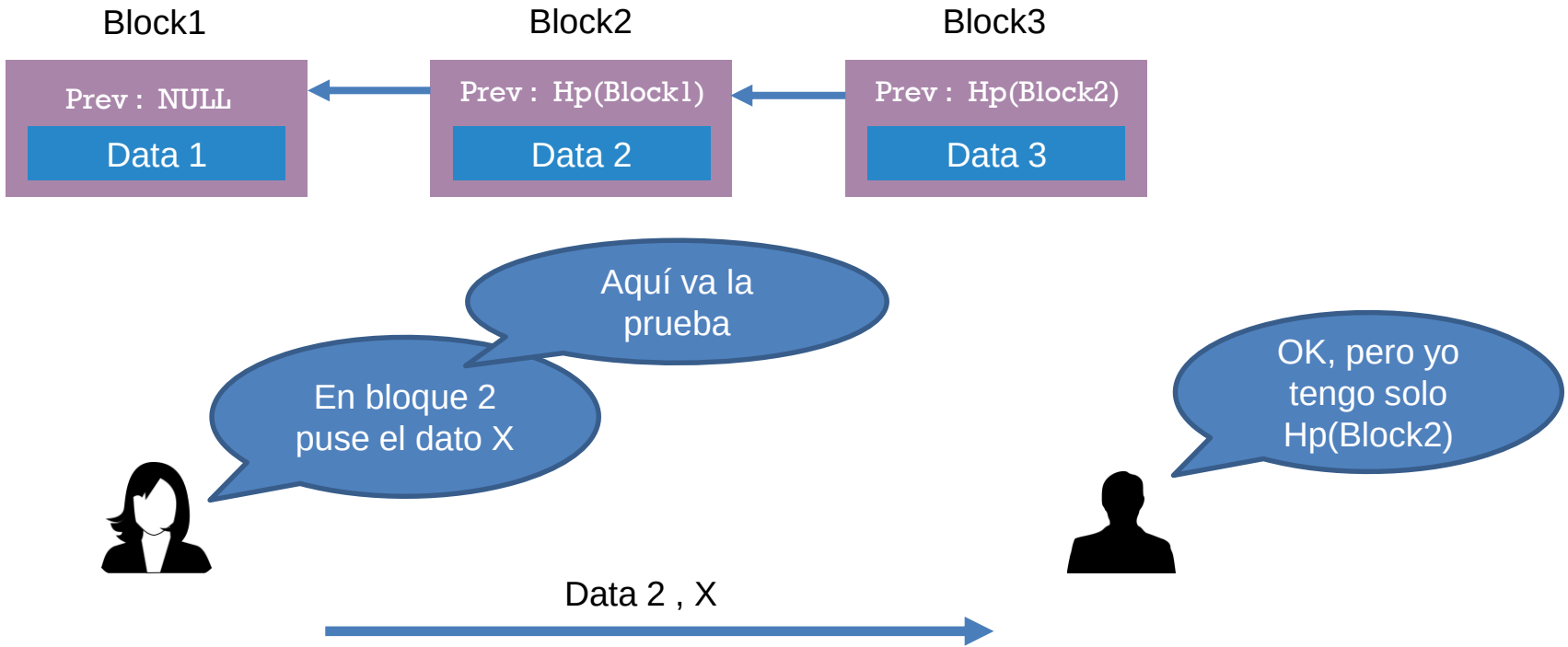
Una debilidad



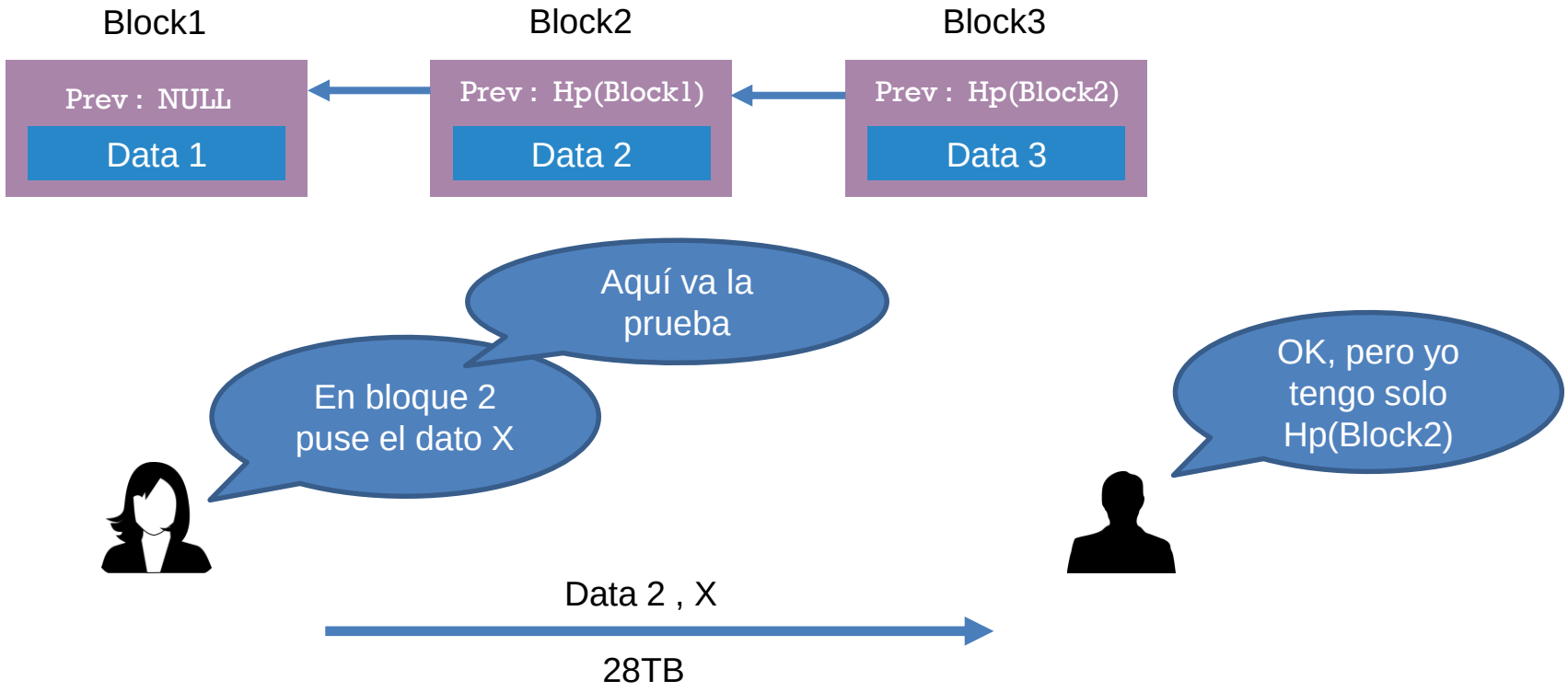
Una debilidad



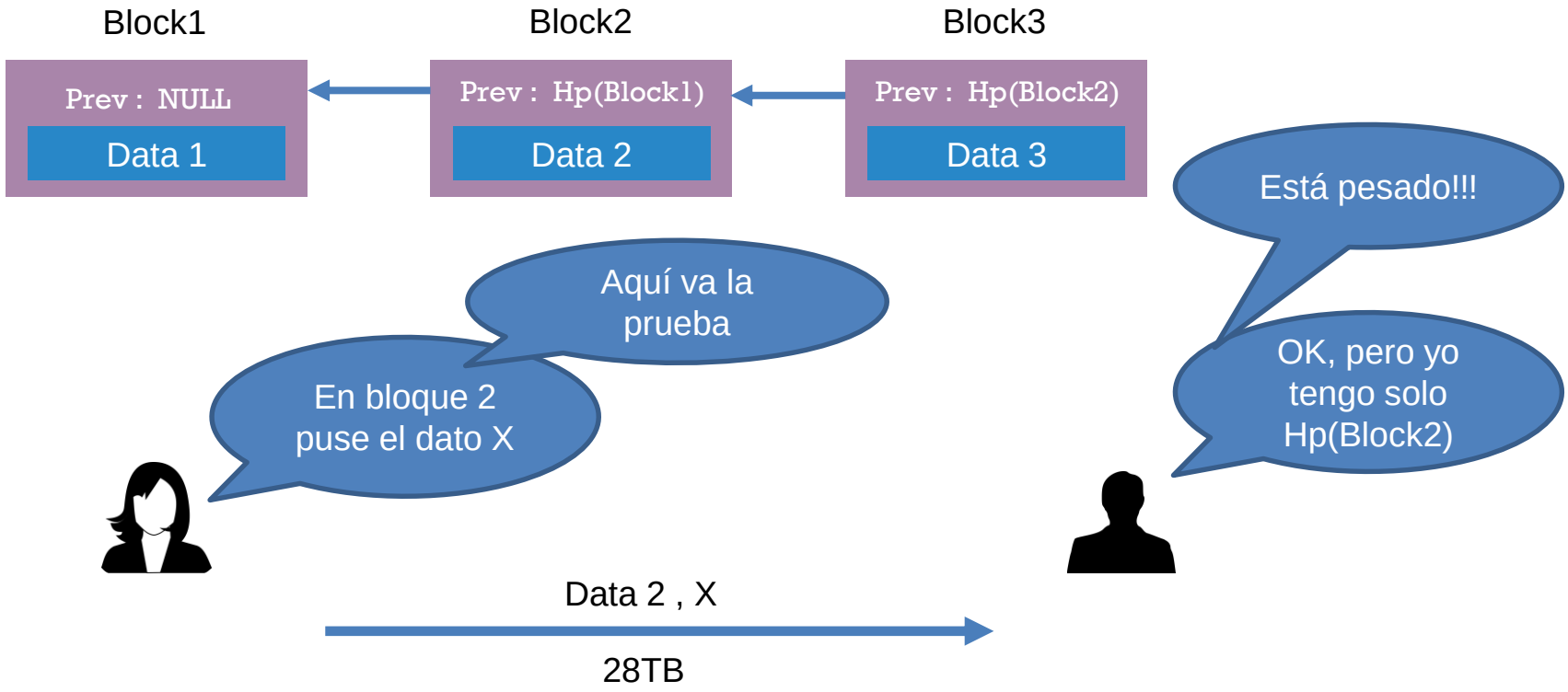
Una debilidad



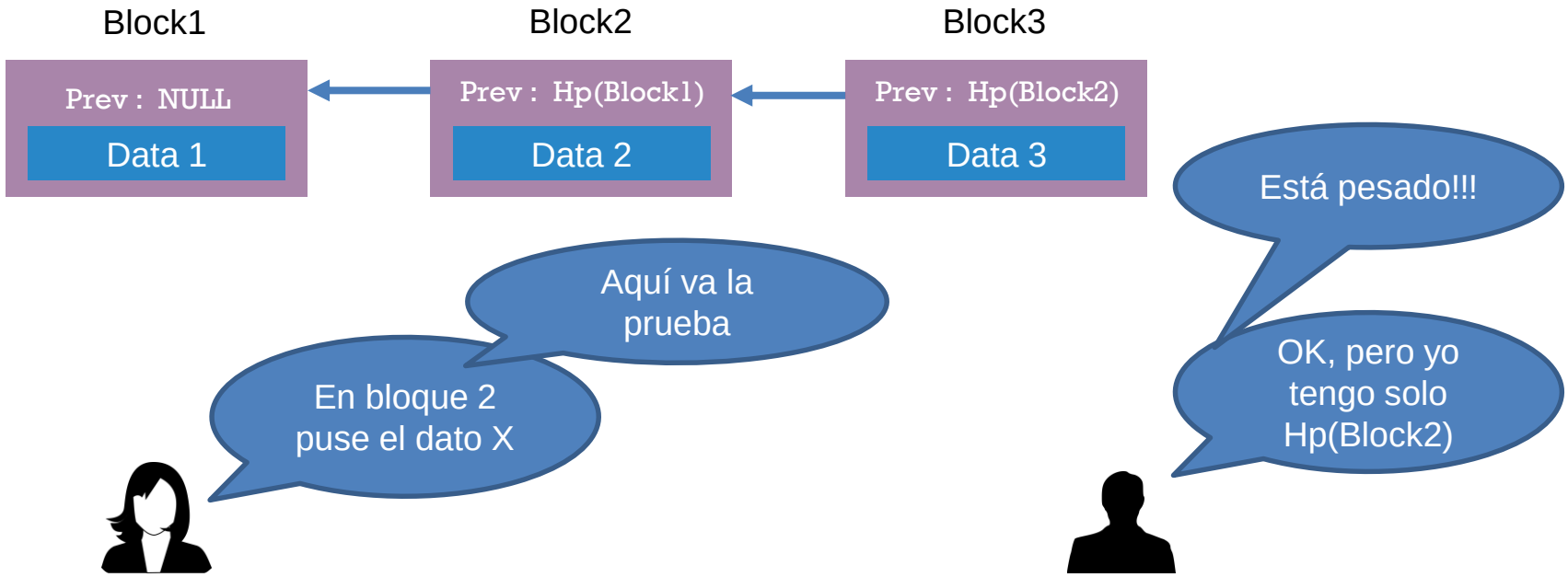
Una debilidad



Una debilidad



Una debilidad



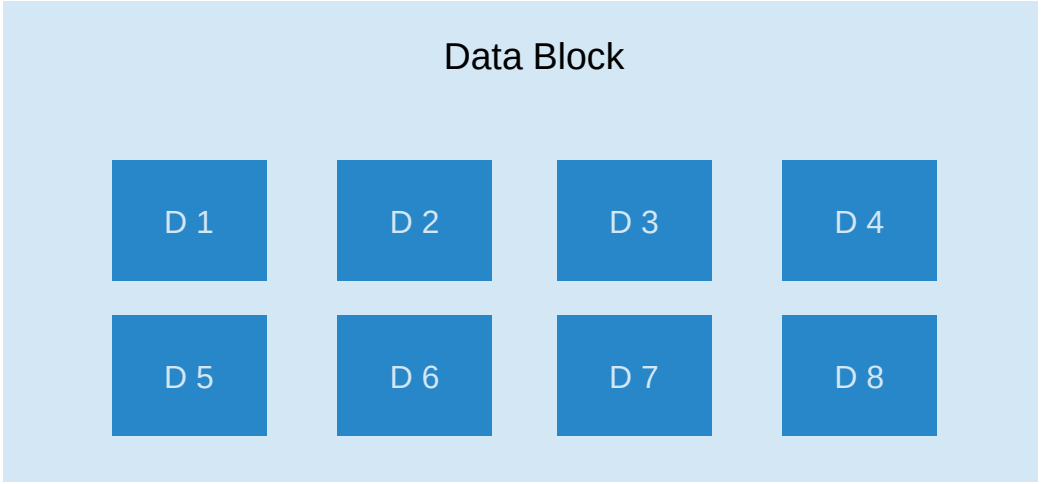
Como hacer la prueba más eficiente???

Arboles de Merkle

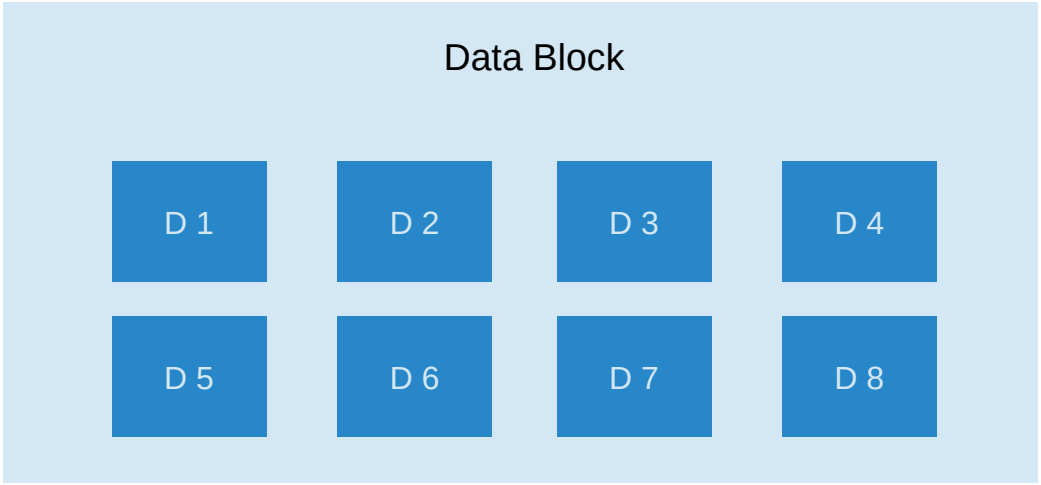
Qué queremos lograr?

D 1 | D 2 | D 3 | D 4 | D 5 | D 6 | D 7 | D 8

Qué queremos lograr?

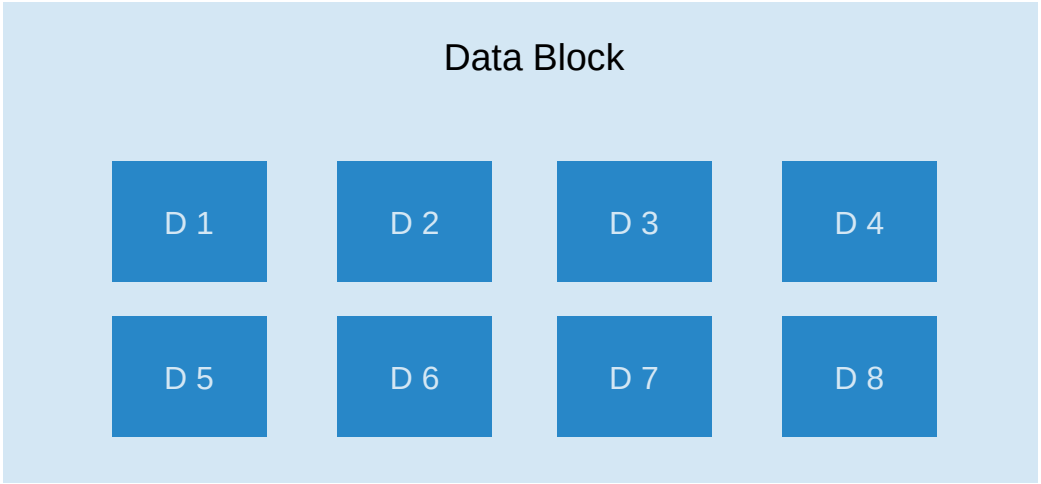


Qué queremos lograr?



H(Data Block) + Di permite verificar que Di pertenece a Data Block

Qué queremos lograr?



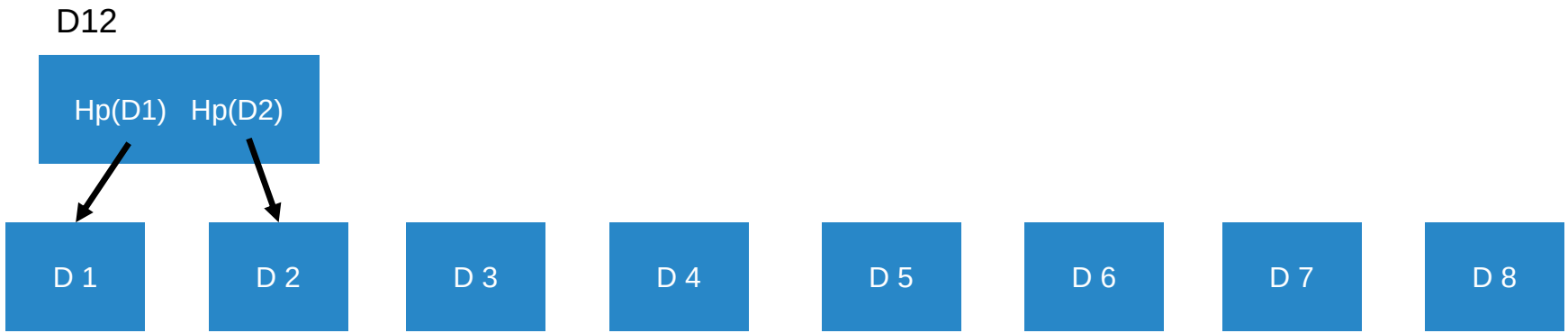
H(Data Block) + Di permite verificar que Di pertenece a Data Block

Es posible lograr esto?

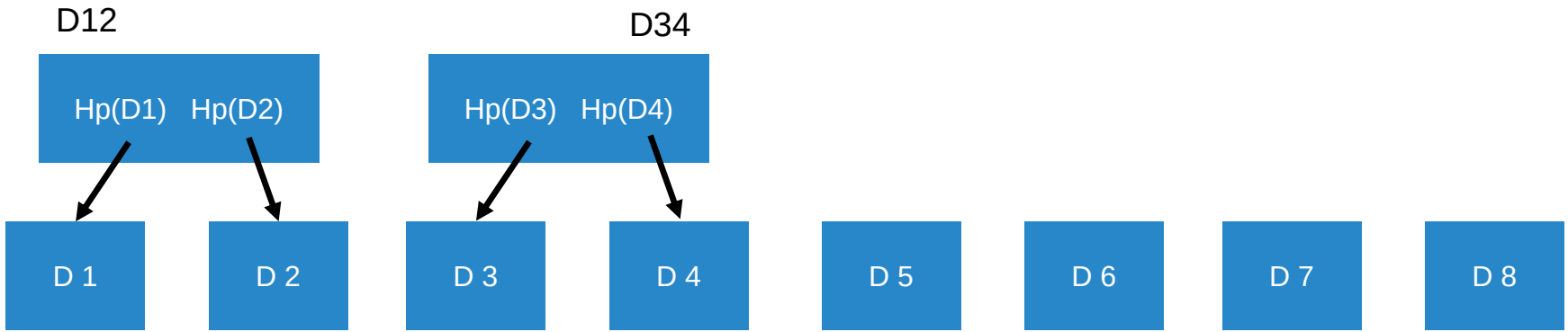
Arbol de Merkle

Arbol de Merkle

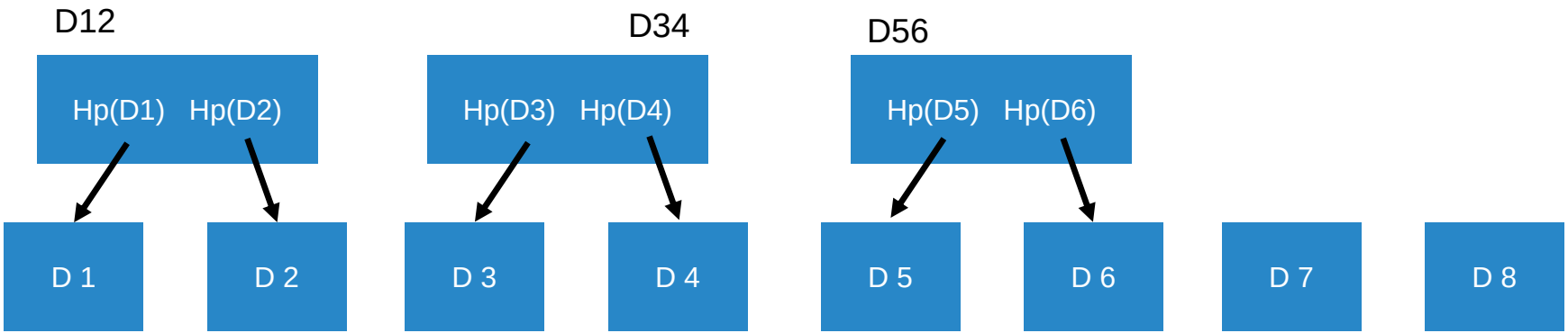
Arbol de Merkle



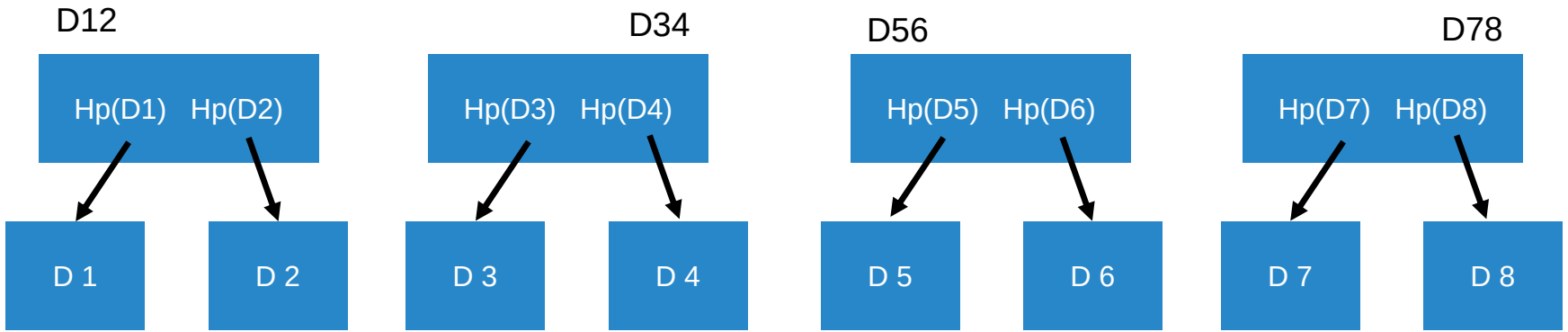
Arbol de Merkle



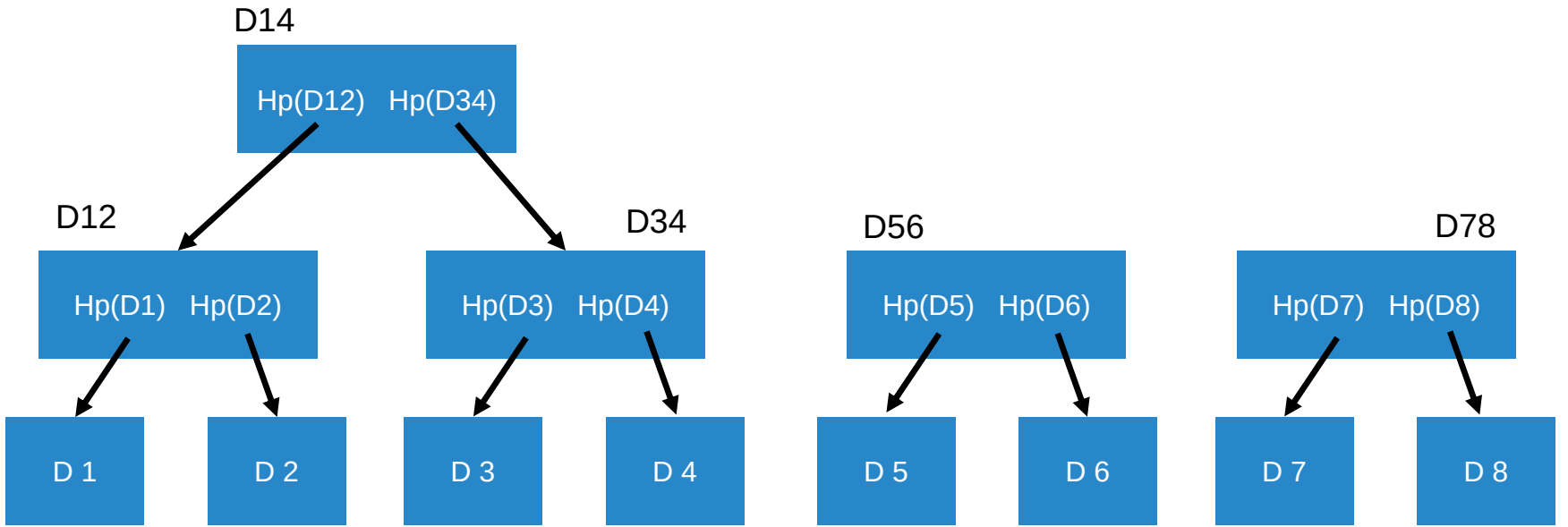
Arbol de Merkle



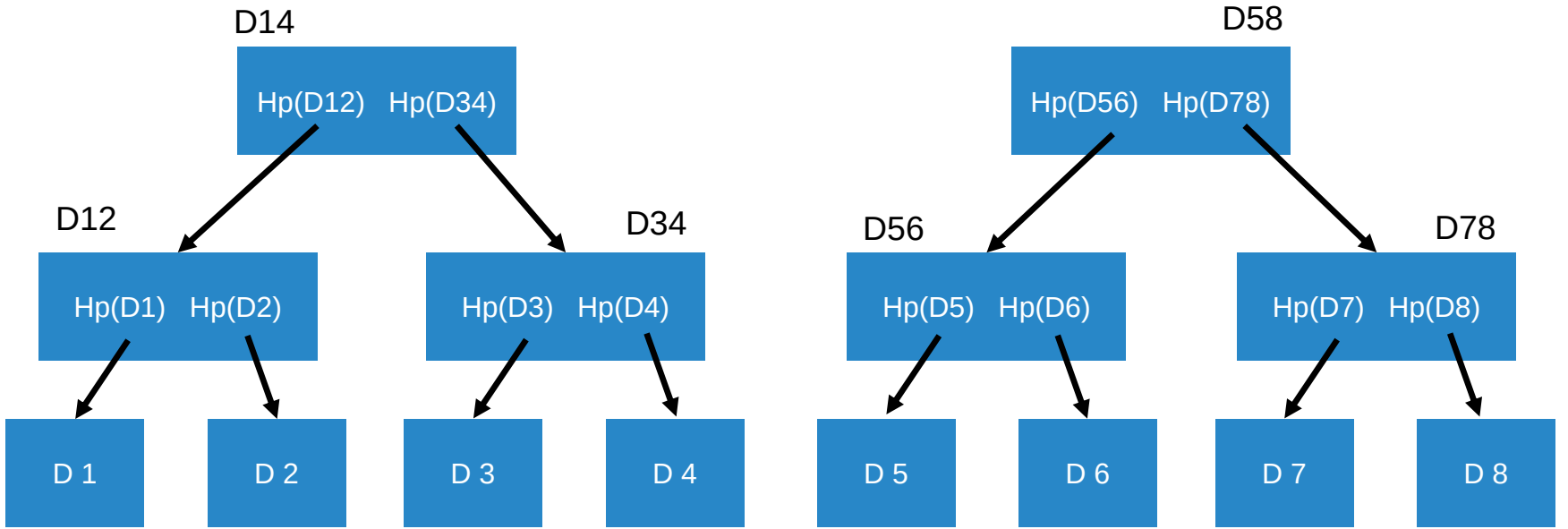
Arbol de Merkle



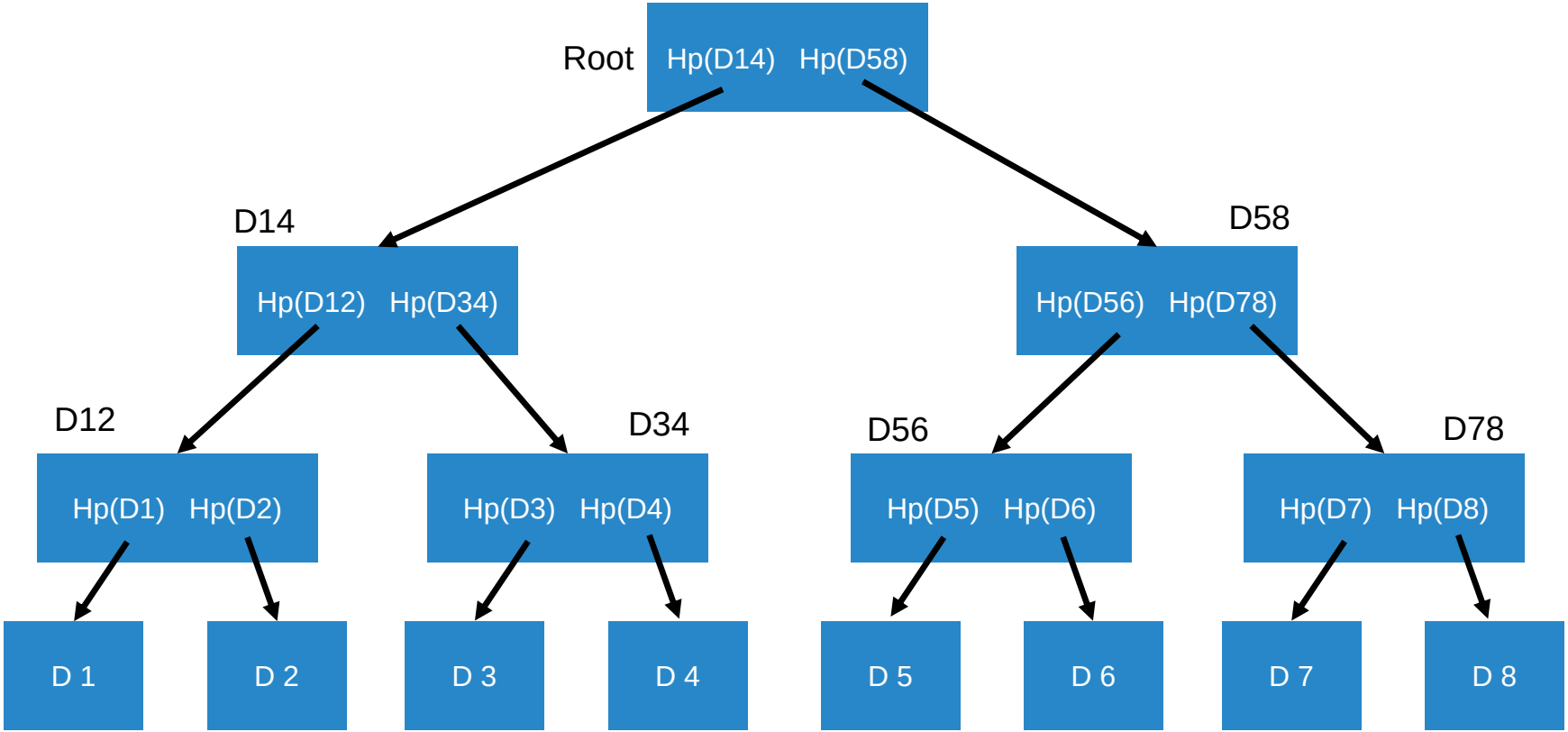
Arbol de Merkle



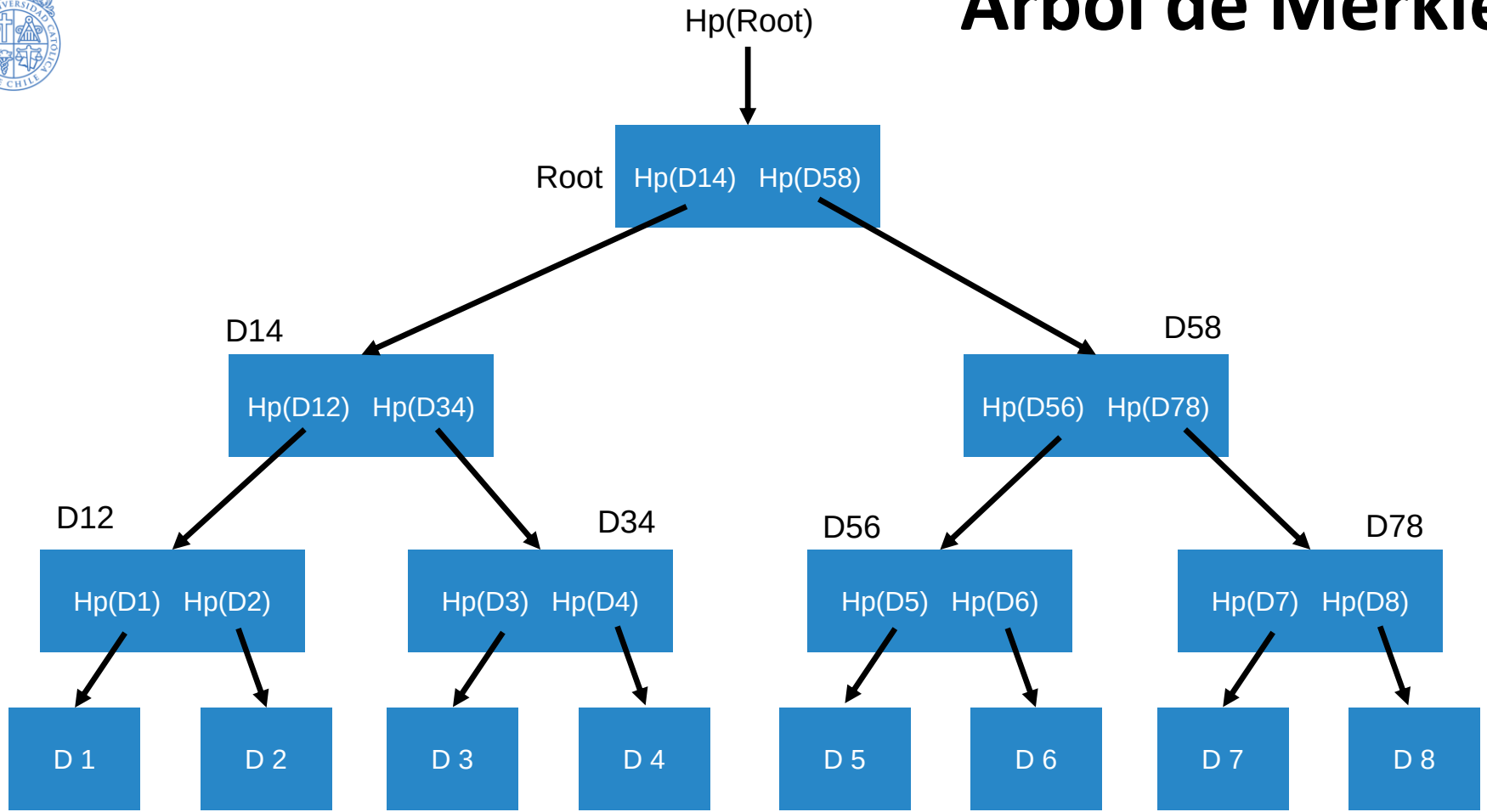
Arbol de Merkle



Arbol de Merkle



Arbol de Merkle

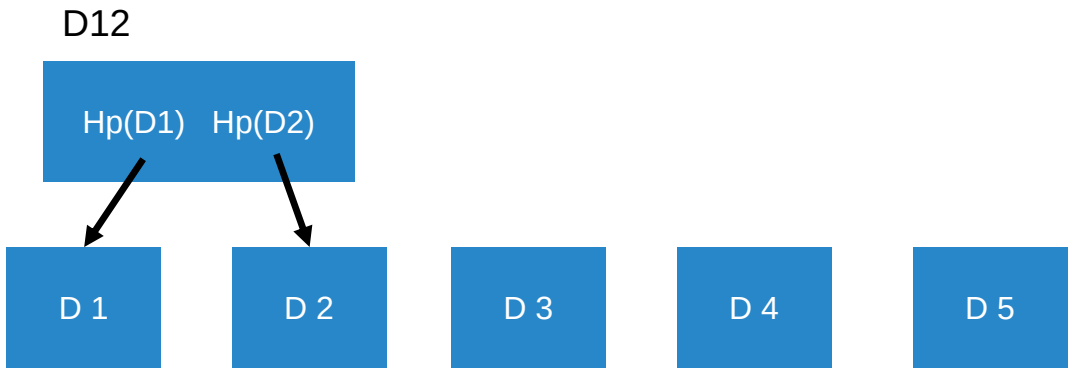


Arbol de Merkle

Si no tengo 2^n datos?

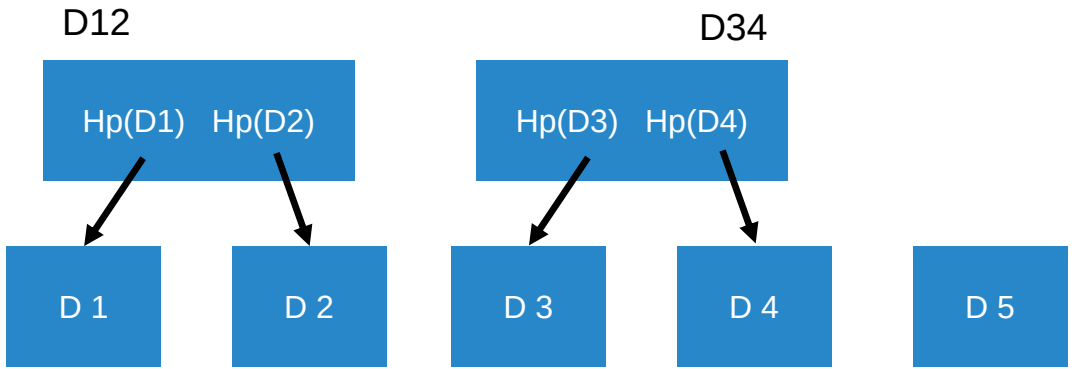
Arbol de Merkle

Si no tengo 2^n datos?



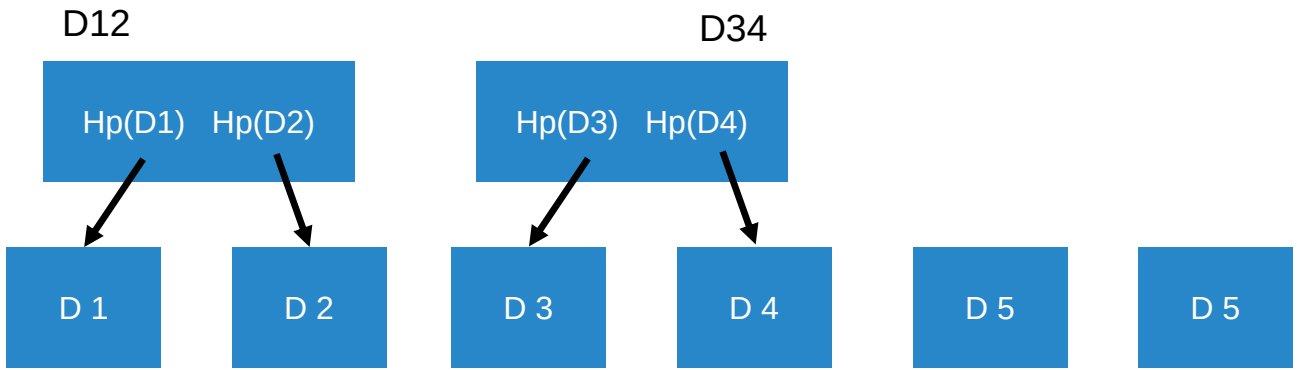
Arbol de Merkle

Si no tengo 2^n datos?



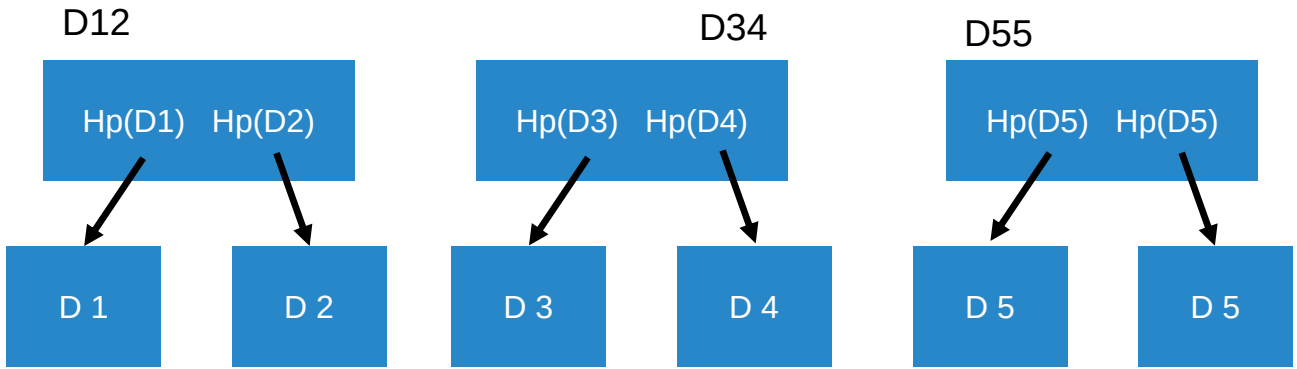
Arbol de Merkle

Si no tengo 2^n datos?



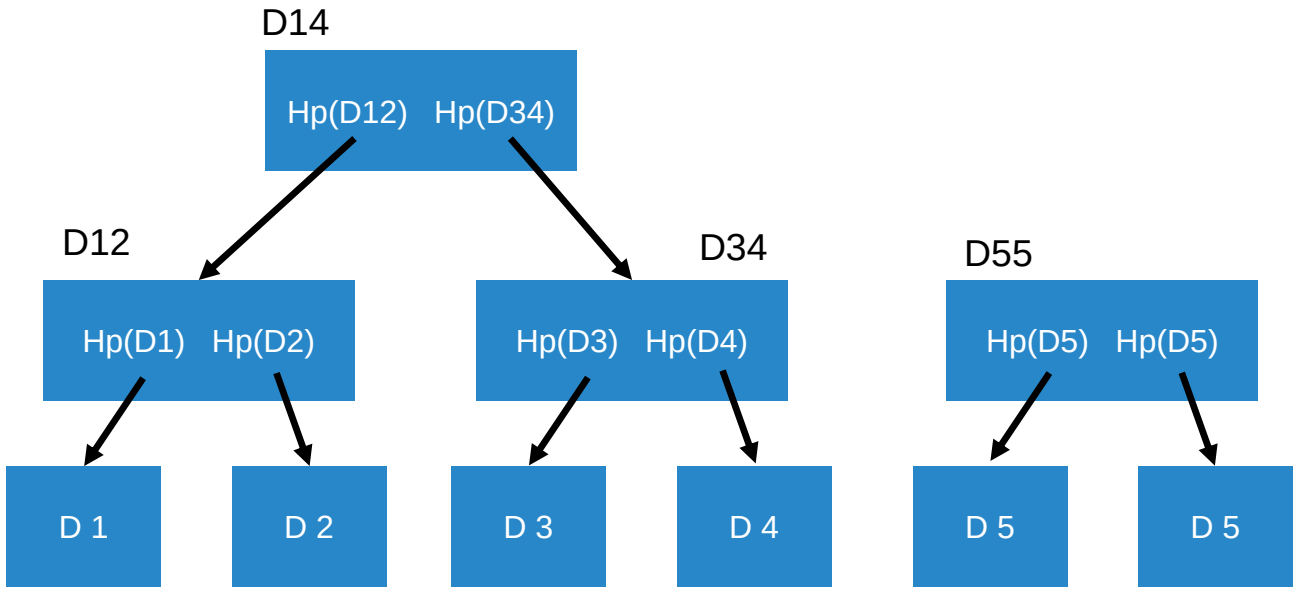
Arbol de Merkle

Si no tengo 2^n datos?



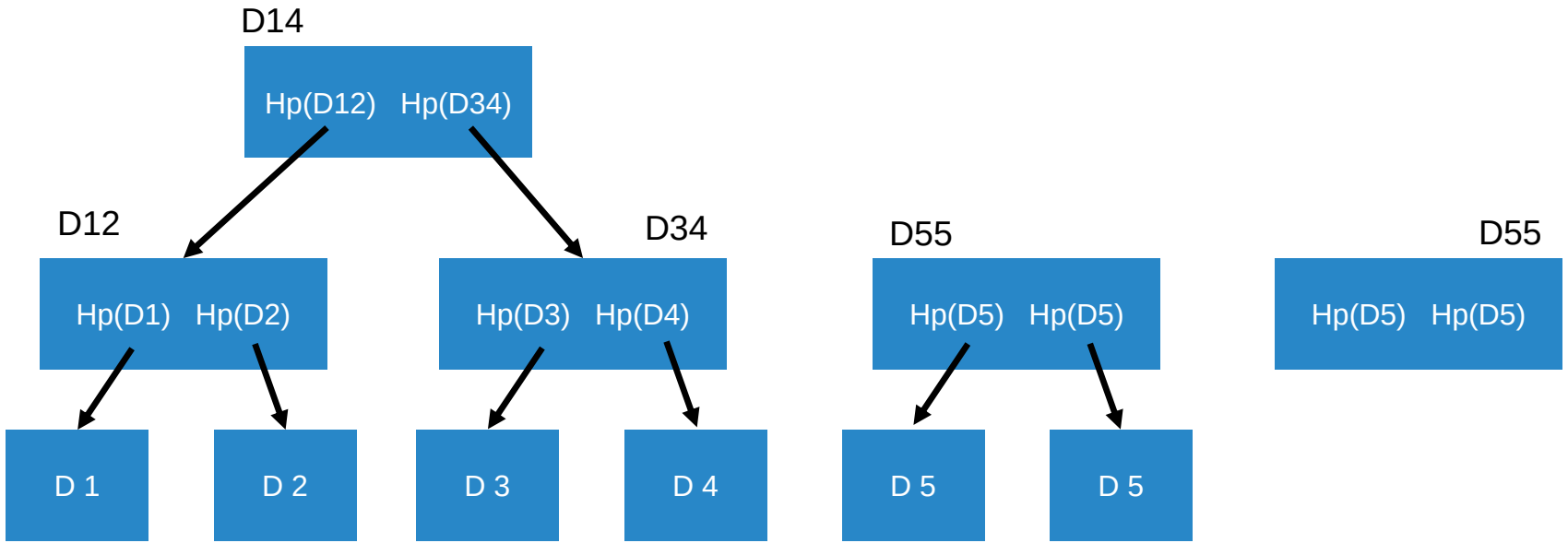
Arbol de Merkle

Si no tengo 2^n datos?



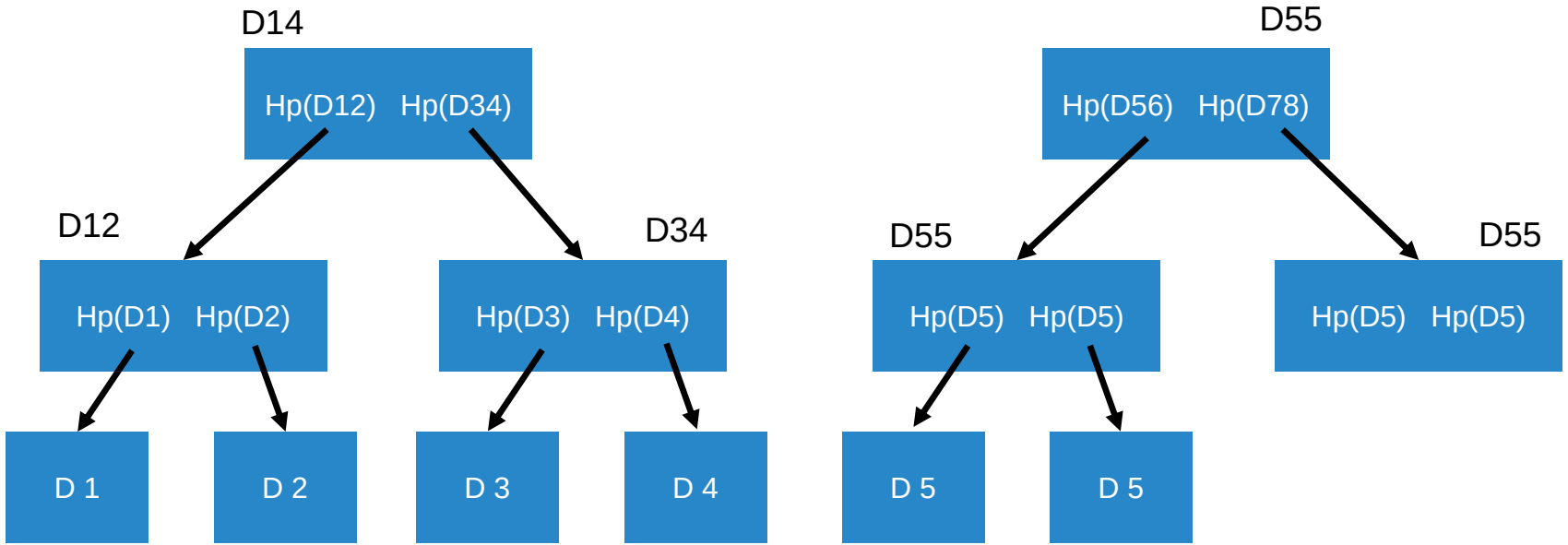
Arbol de Merkle

Si no tengo 2^n datos?



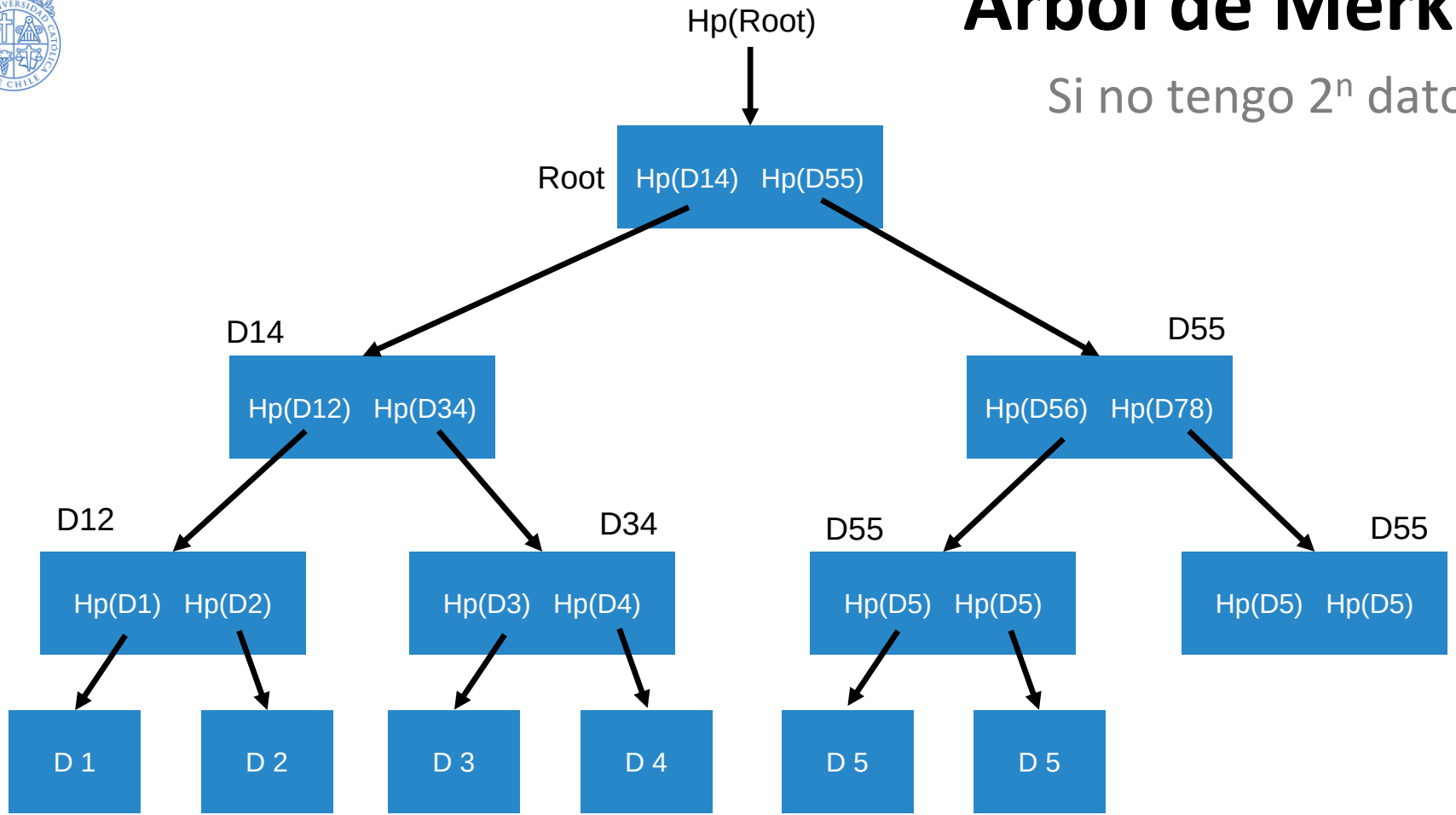
Arbol de Merkle

Si no tengo 2^n datos?



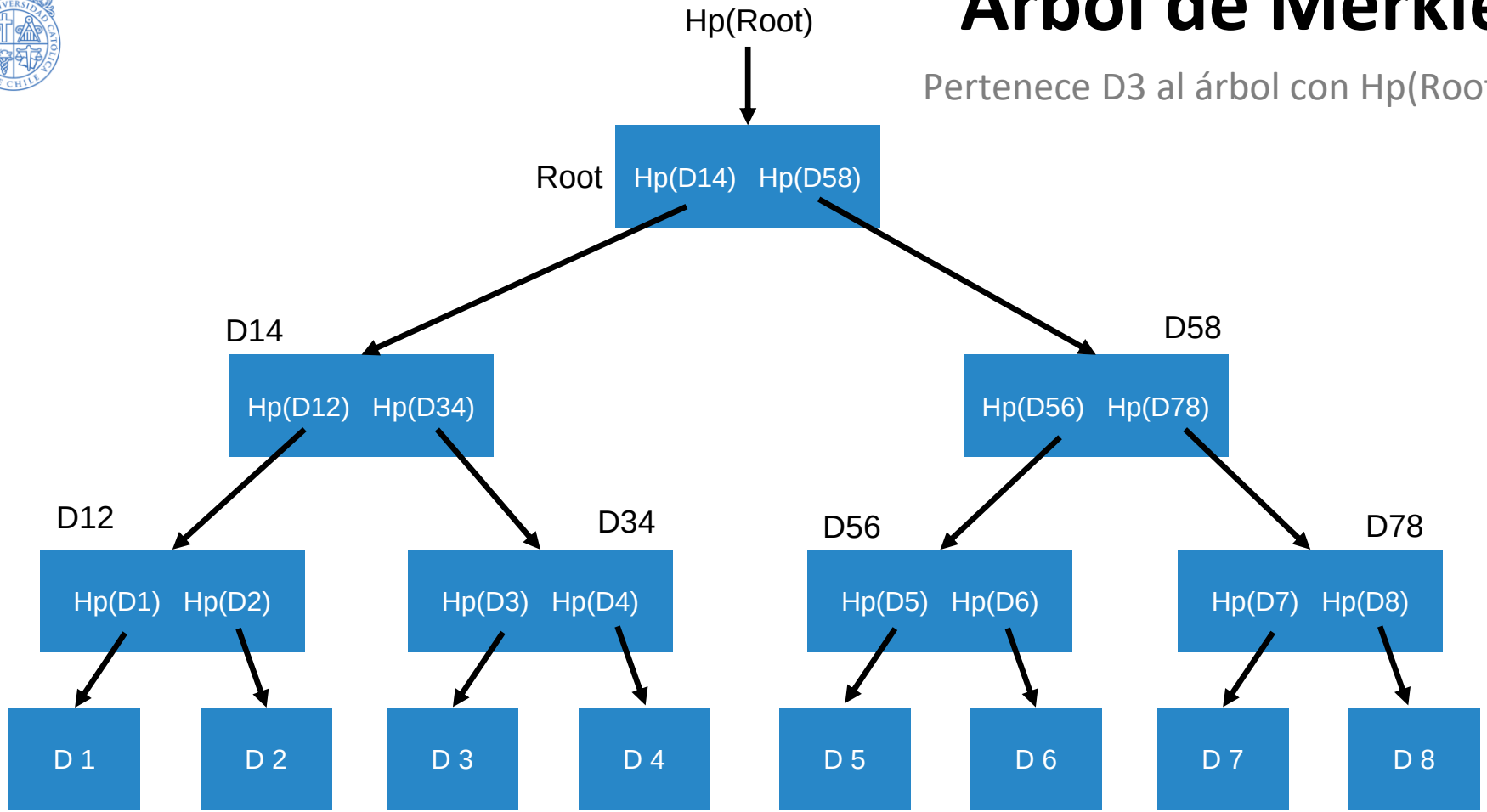
Arbol de Merkle

Si no tengo 2^n datos?



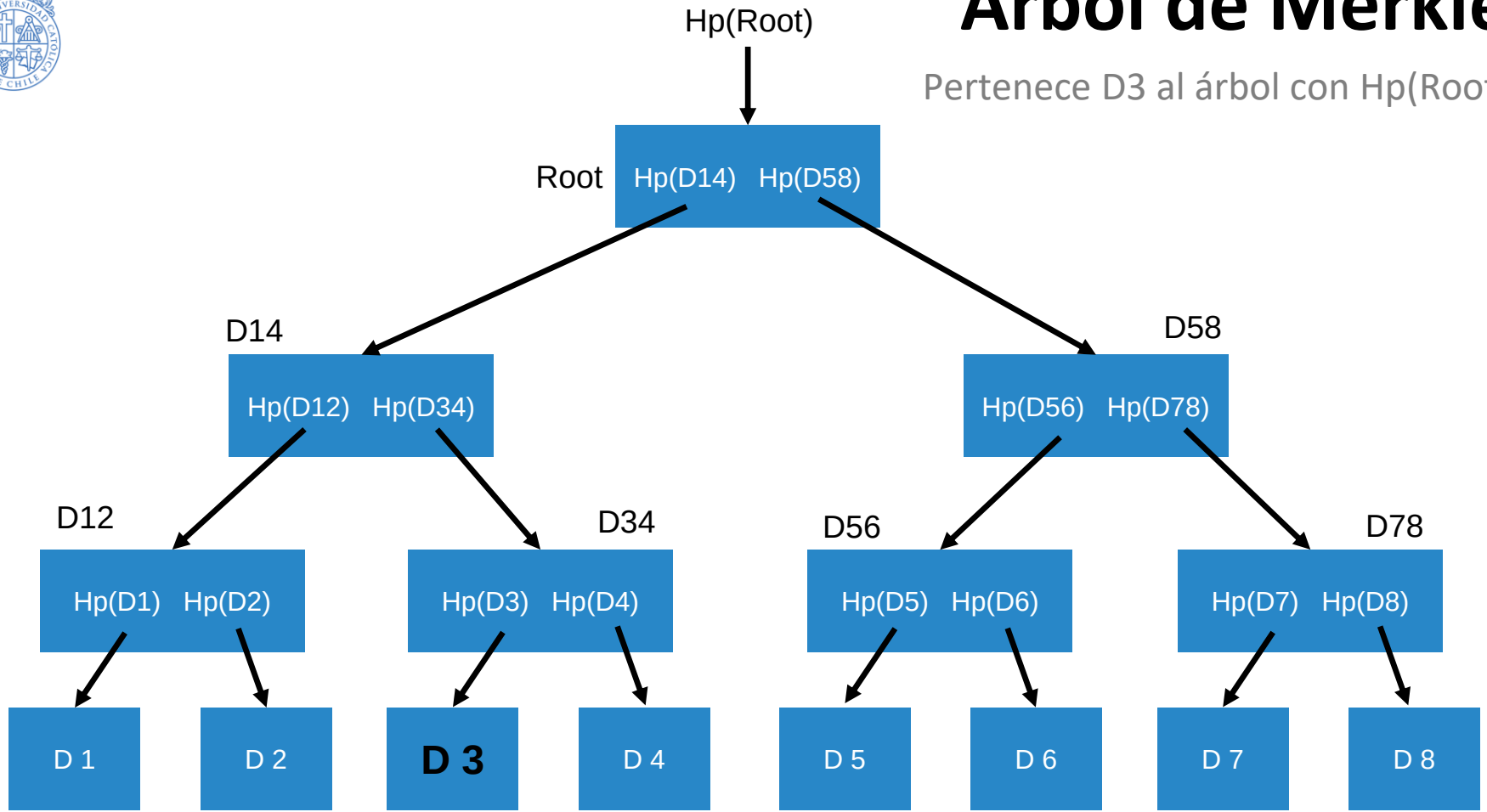
Arbol de Merkle

Pertenece D3 al árbol con Hp(Root)



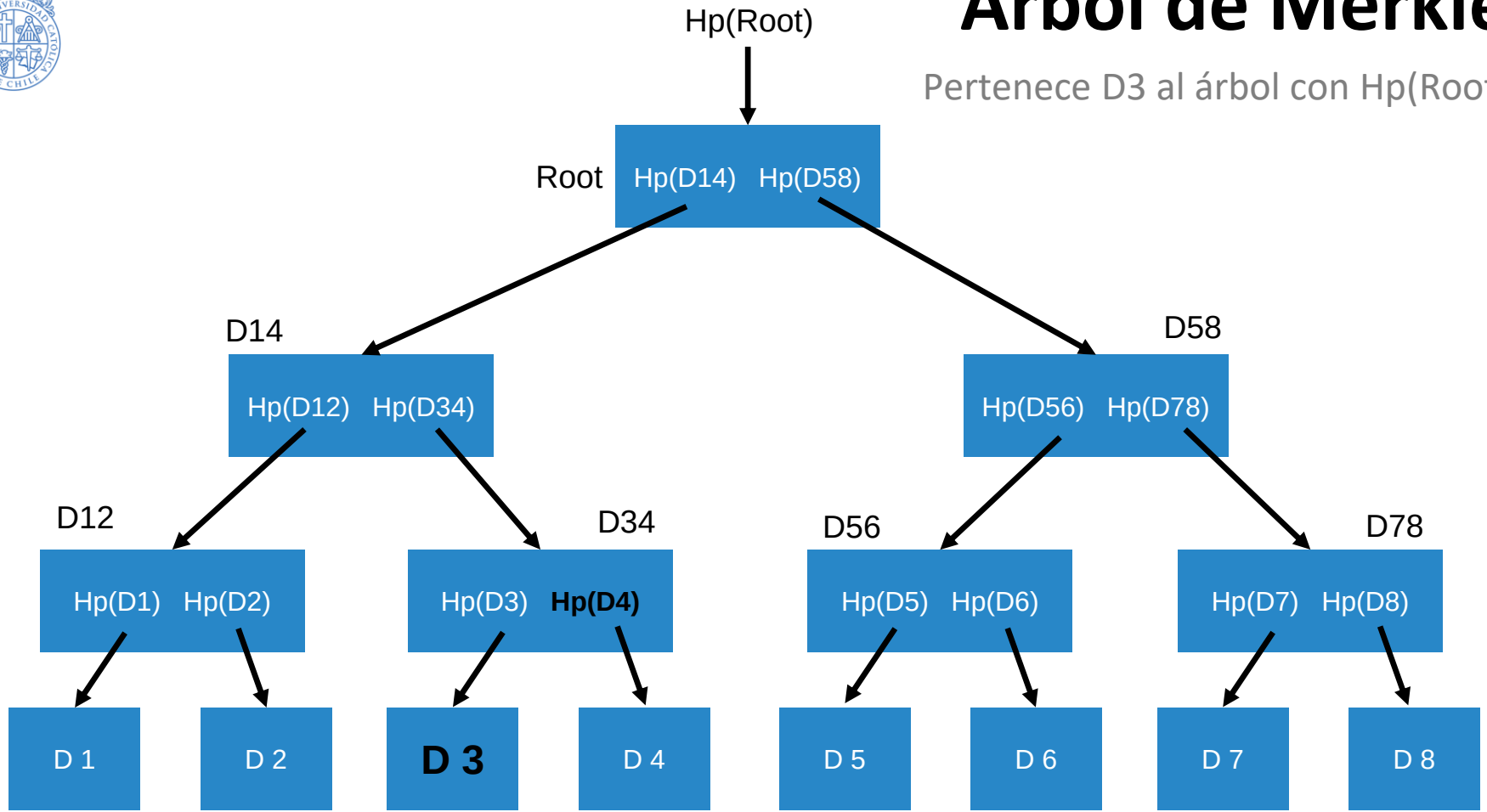
Arbol de Merkle

Pertenece D3 al árbol con Hp(Root)



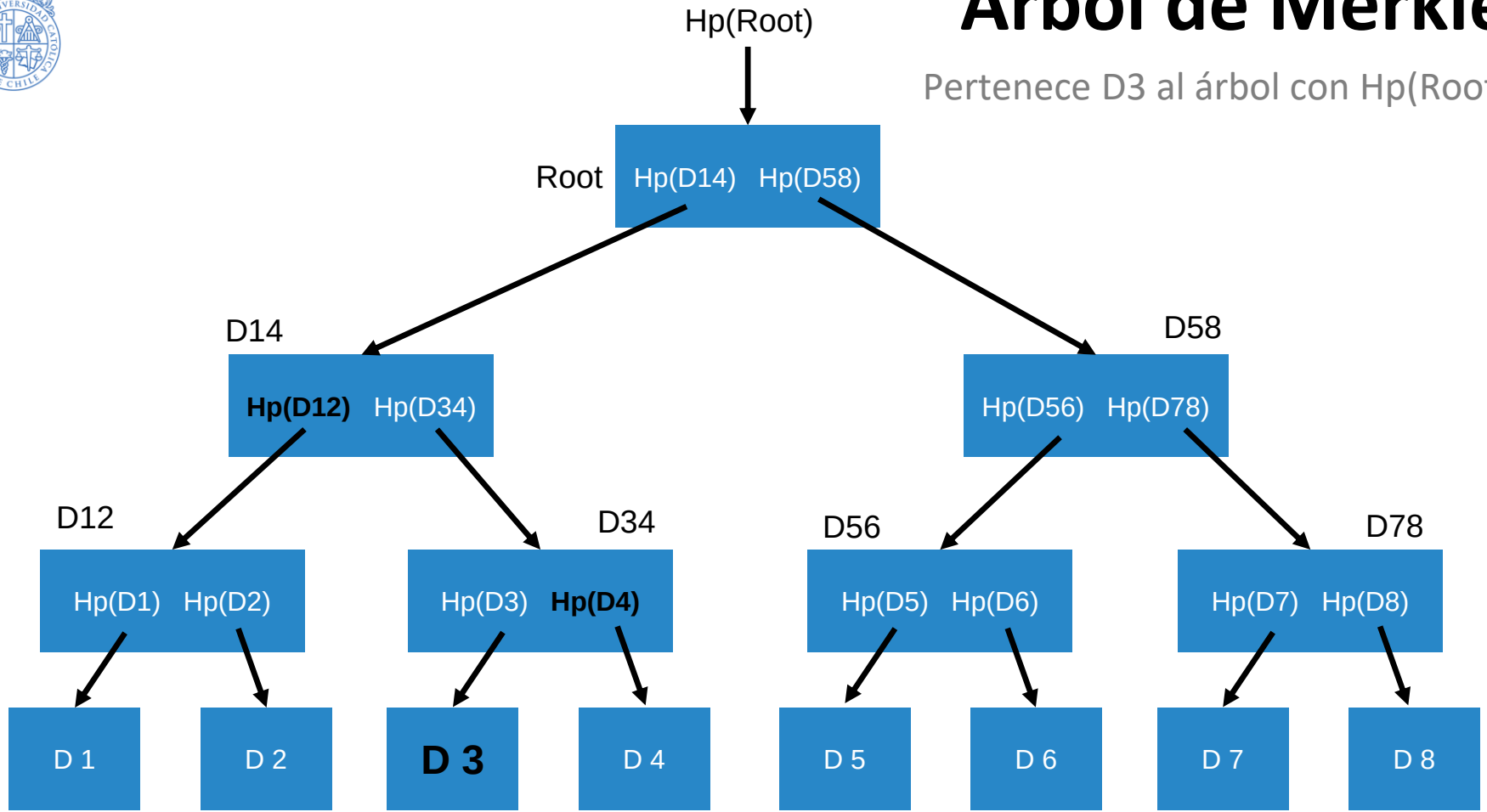
Arbol de Merkle

Pertenece D3 al árbol con Hp(Root)



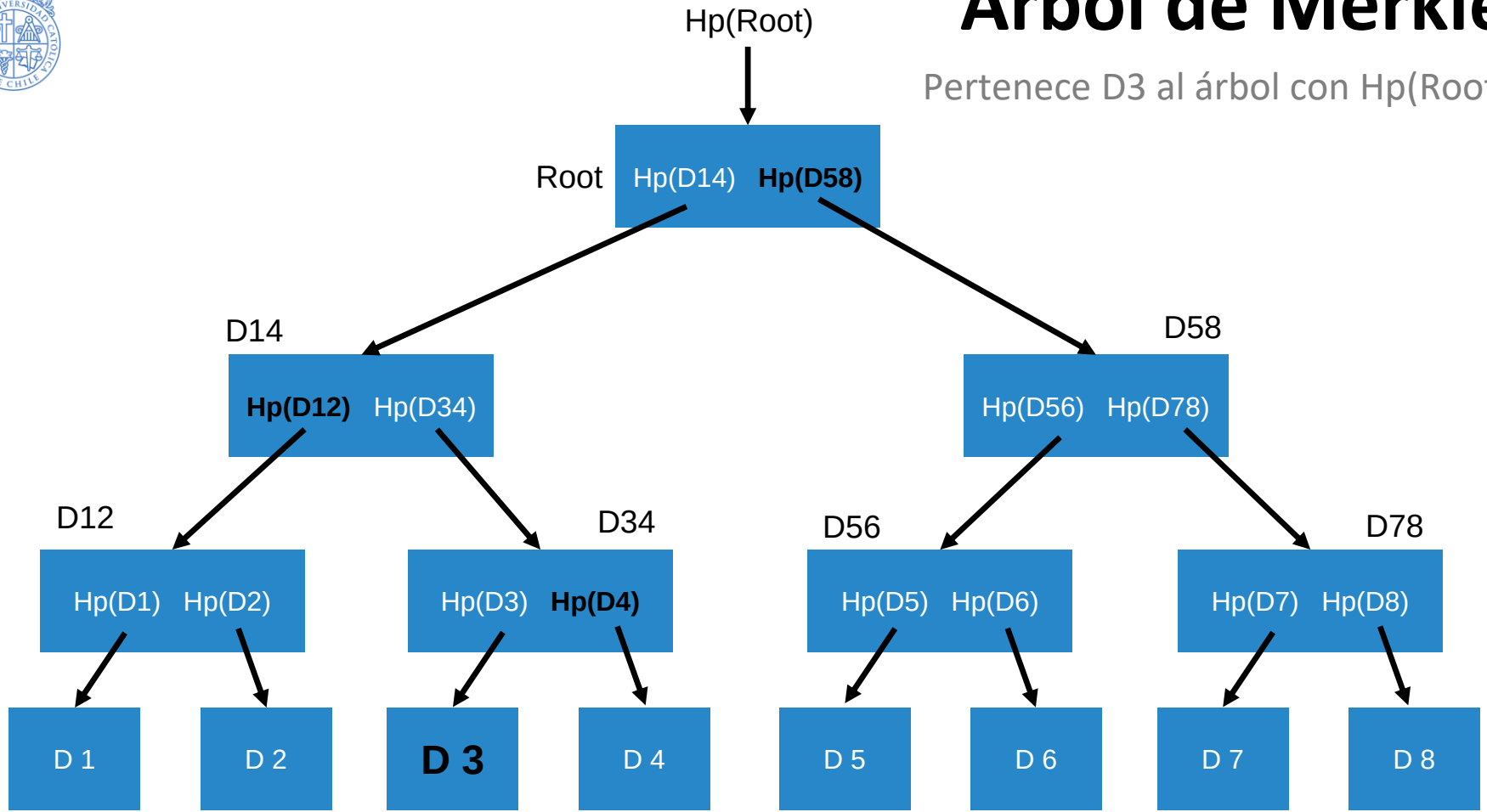
Arbol de Merkle

Pertenece D3 al árbol con Hp(Root)



Arbol de Merkle

Pertenece D3 al árbol con Hp(Root)



Proof of membership

Para mostrar que Di pertenece al árbol con raíz Hp(Root):

- D_i
- Hp(vecinos en el camino hasta el raíz)

Total de $\log_2(n)$ hashes para verificar que D_i pertenece al árbol

Ejemplo: 1024 D_i cada con 1GB = Data Block de 1TB:

- Muestra de D_i pesa -- 1GB (D_i) + $\log_2(1024)$ = 10 hashes (2560 bits)
- Un orden de magnitud menos que el peso de Data Block

Proof of non-membership

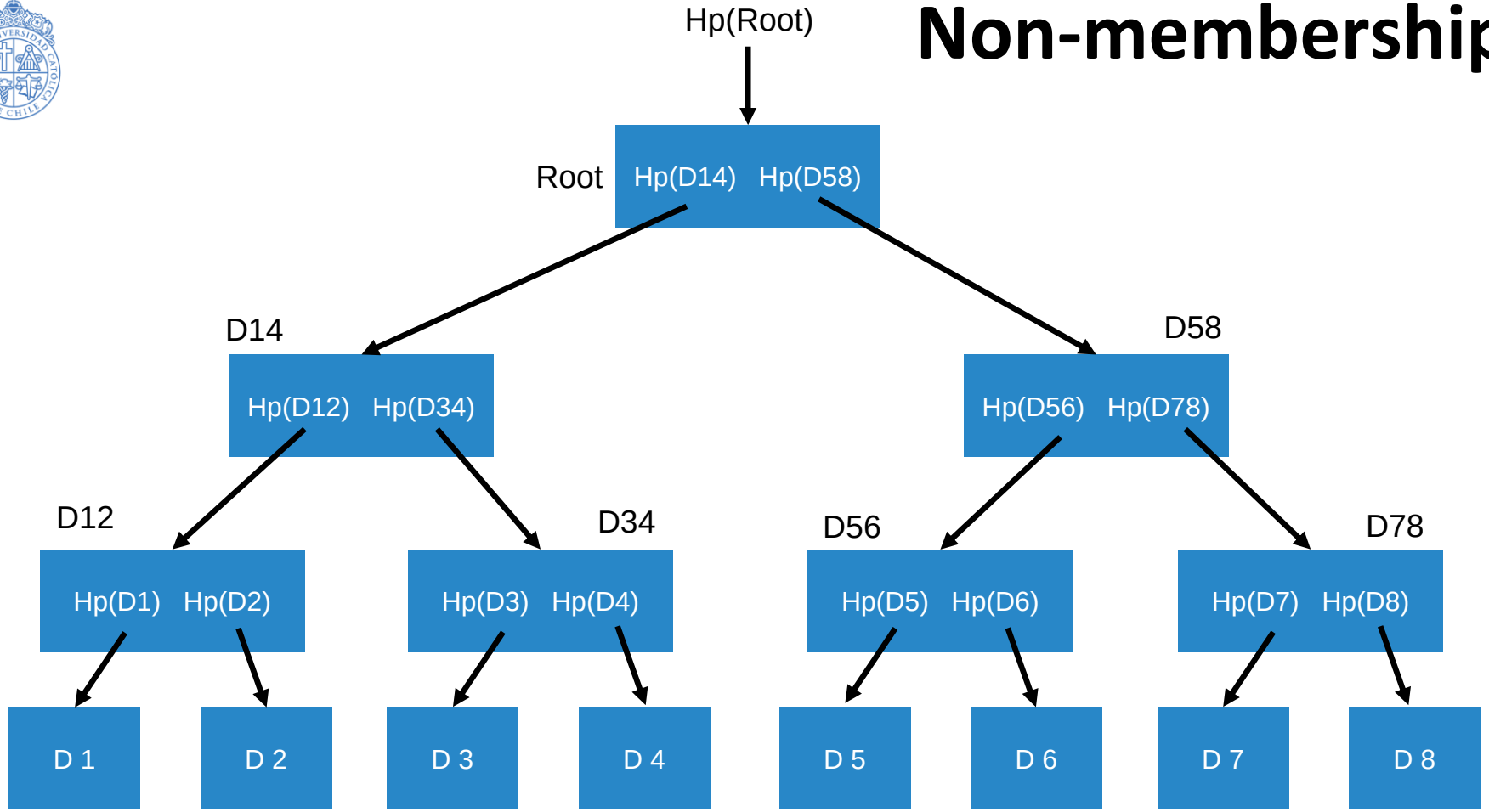
Como mostrar qué un dato D no pertenece al árbol con raíz Hp(Root)?

Proof of non-membership

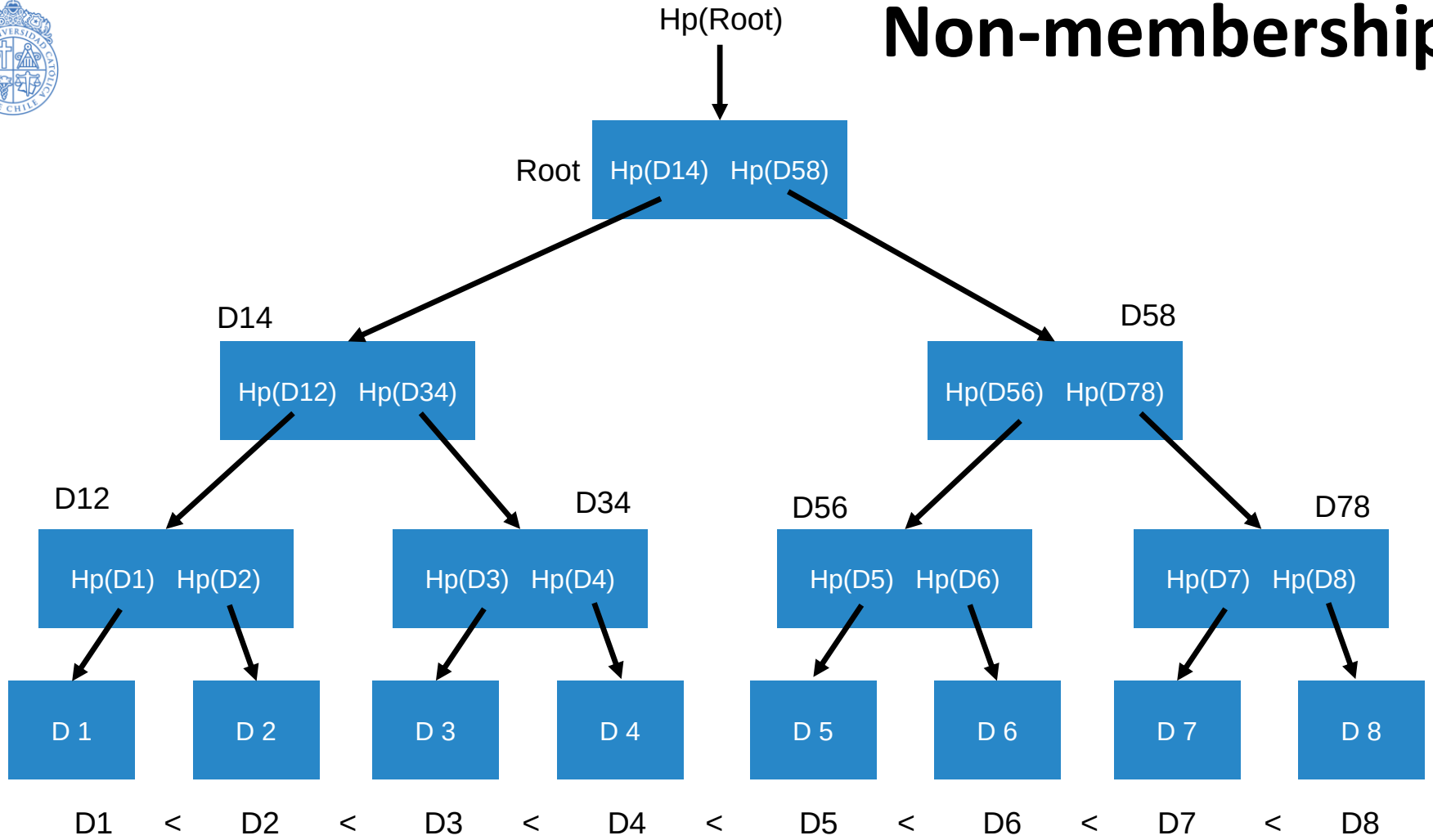
Como mostrar qué un dato D no pertenece al árbol con raíz Hp(Root)?

Ordenemos nuestros datos en las hojas!!!

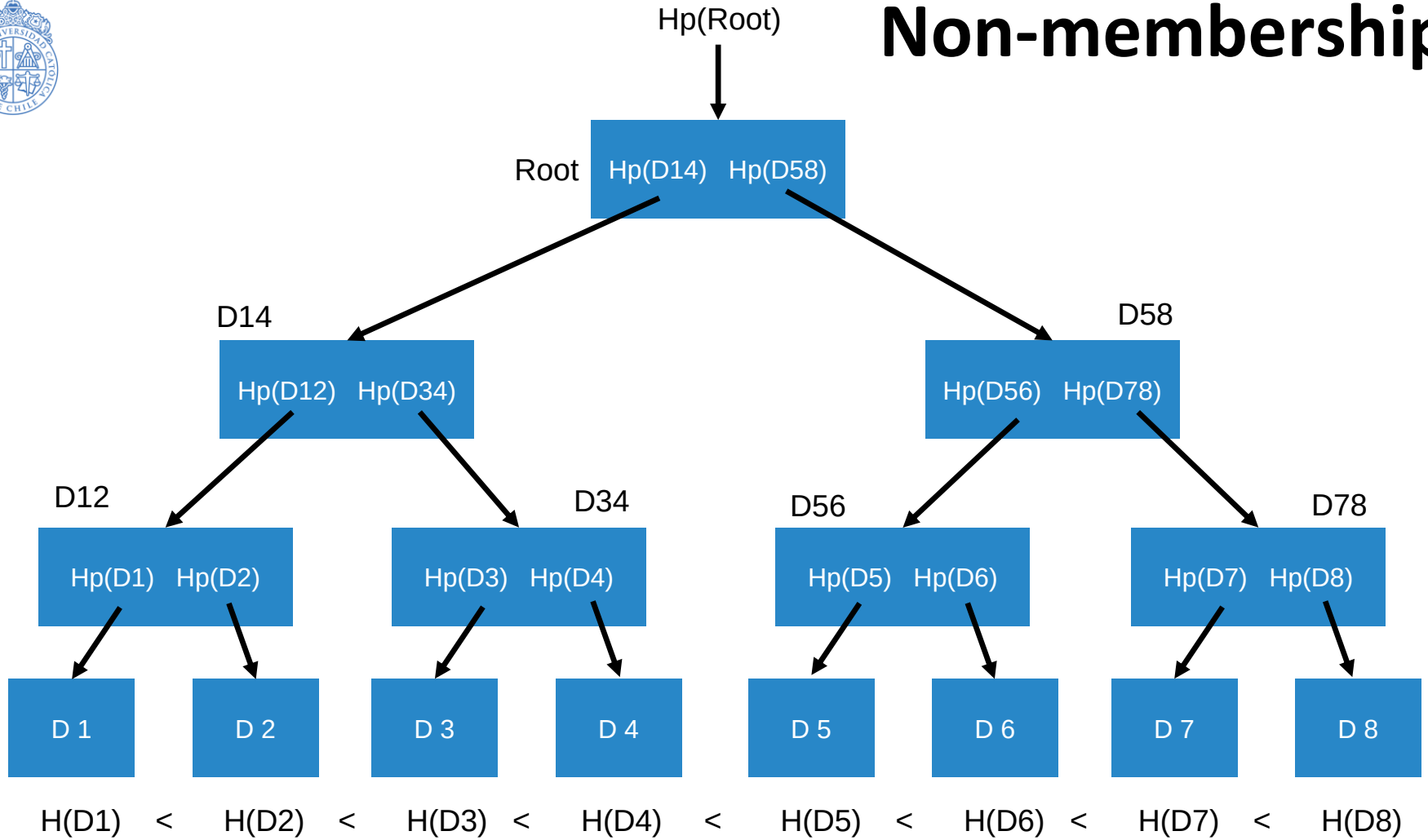
Non-membership



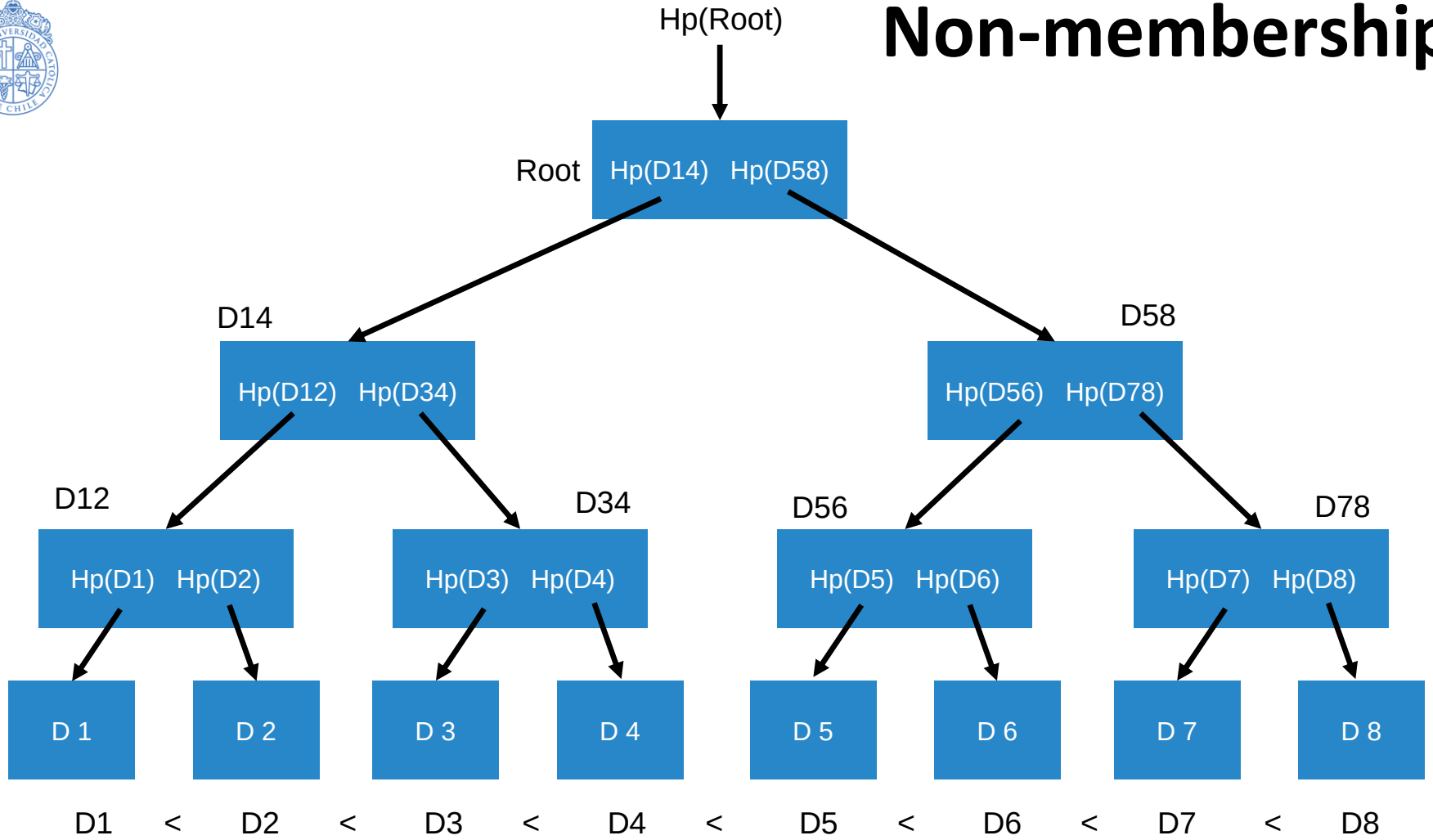
Non-membership



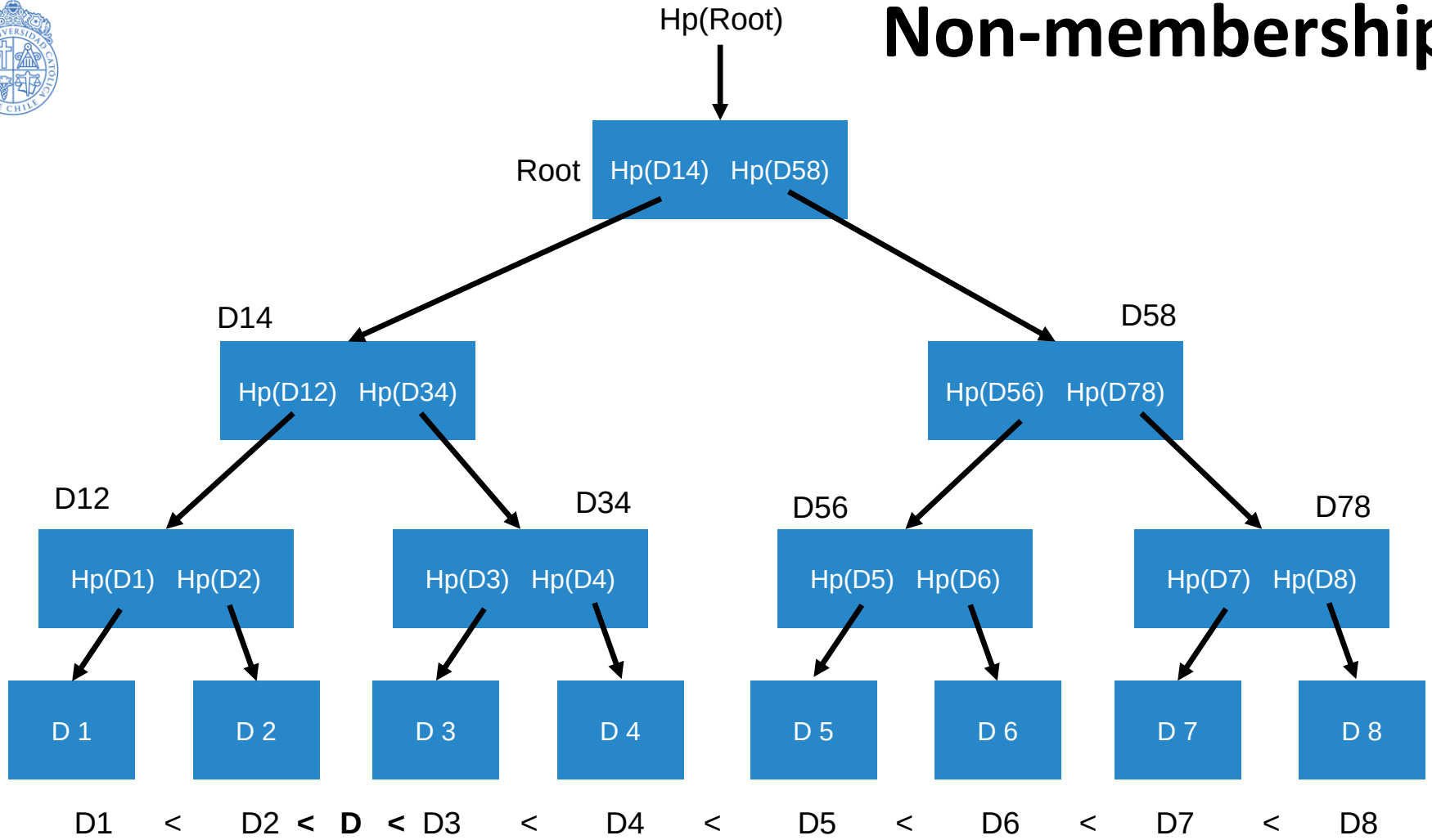
Non-membership



Non-membership



Non-membership



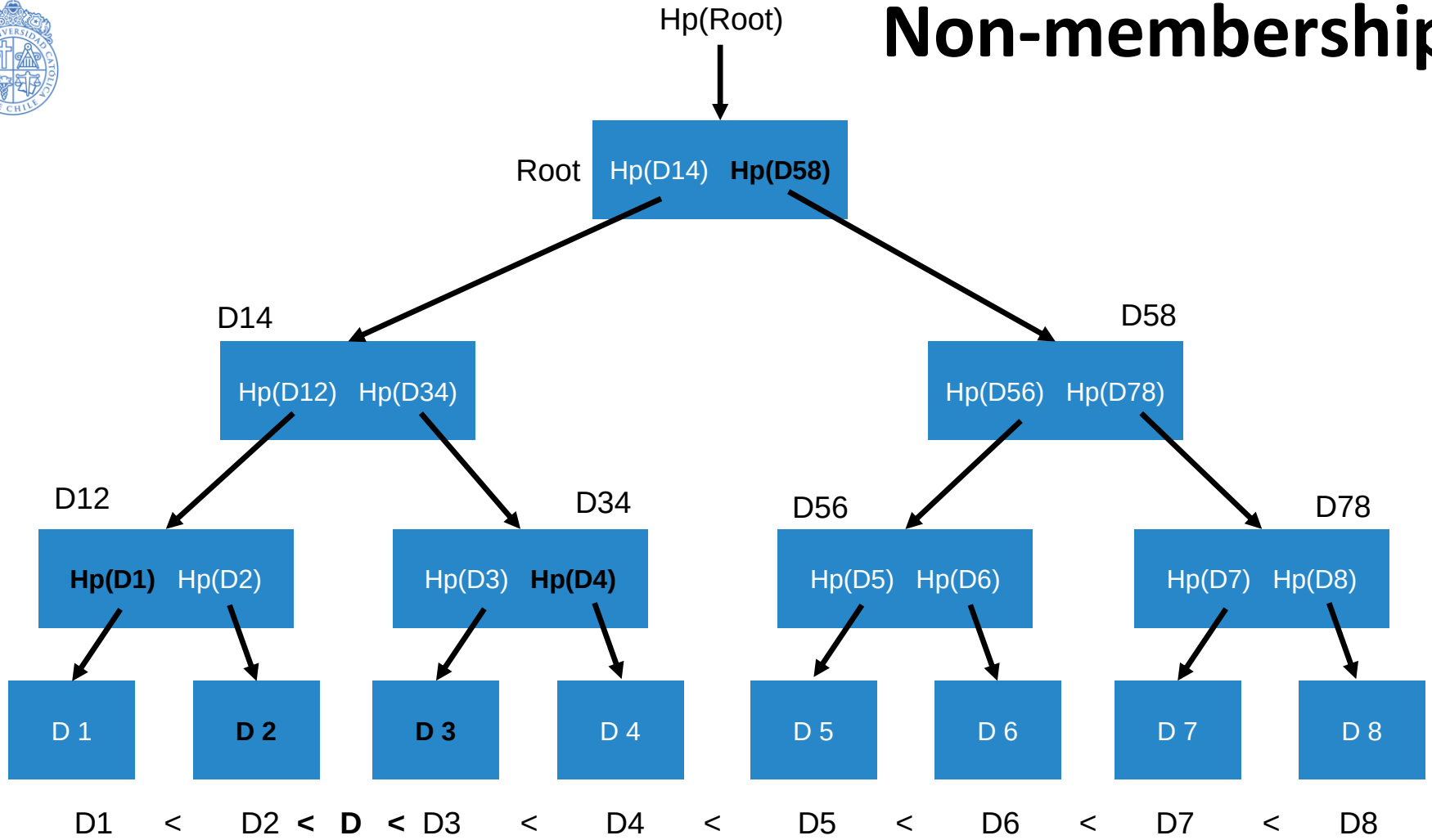
Proof of non-membership

Para mostrar que D ***no*** *pertenece* al árbol con raíz Hp(Root):

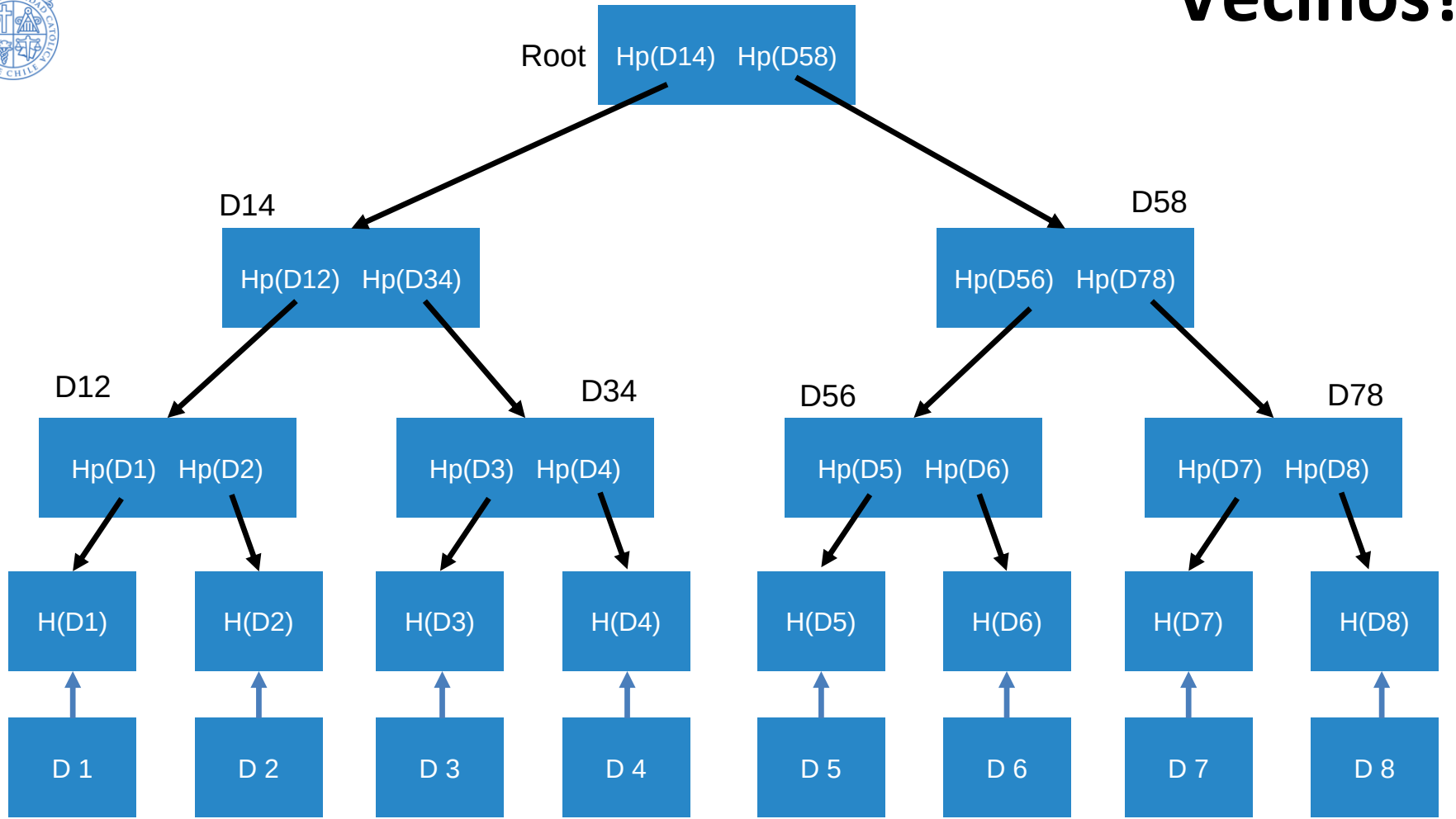
- Mínimo *i* t.q. $D_i < D$
- Muestra de pertenencia de D_i y D_{i+1}
- Muestra que D_i y D_{i+1} son vecinos en el árbol (**como lograr esto???**)

Como D_i y D_{i+1} son vecinos en el árbol, D no cabe

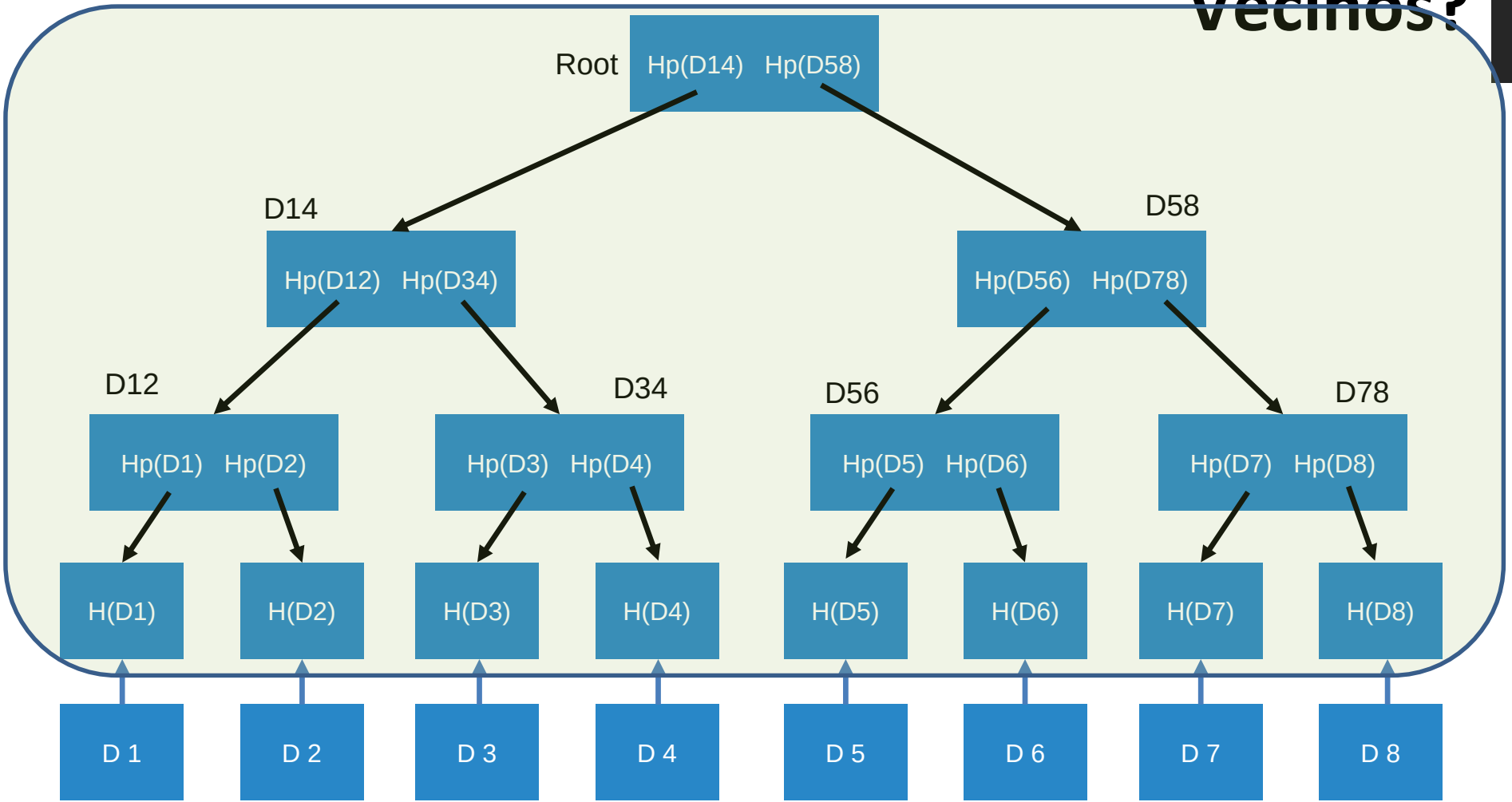
Non-membership



Vecinos?


Root
Hp(D14) Hp(D58)
D14
Hp(D12) Hp(D34)
D58
Hp(D56) Hp(D78)
D12
Hp(D1) Hp(D2)
D34
Hp(D3) Hp(D4)
D56
Hp(D5) Hp(D6)
D78
Hp(D7) Hp(D8)
H(D1)
H(D2)
H(D3)
H(D4)
H(D5)
H(D6)
H(D7)
H(D8)
D 1
D 2
D 3
D 4
D 5
D 6
D 7
D 8

Vecinos?


Root
Hp(D14) Hp(D58)
D14
Hp(D12) Hp(D34)
D58
Hp(D56) Hp(D78)
D12
Hp(D1) Hp(D2)
D34
Hp(D3) Hp(D4)
D56
Hp(D5) Hp(D6)
D78
Hp(D7) Hp(D8)
H(D1)
H(D2)
H(D3)
H(D4)
H(D5)
H(D6)
H(D7)
H(D8)
D 1
D 2
D 3
D 4
D 5
D 6
D 7
D 8

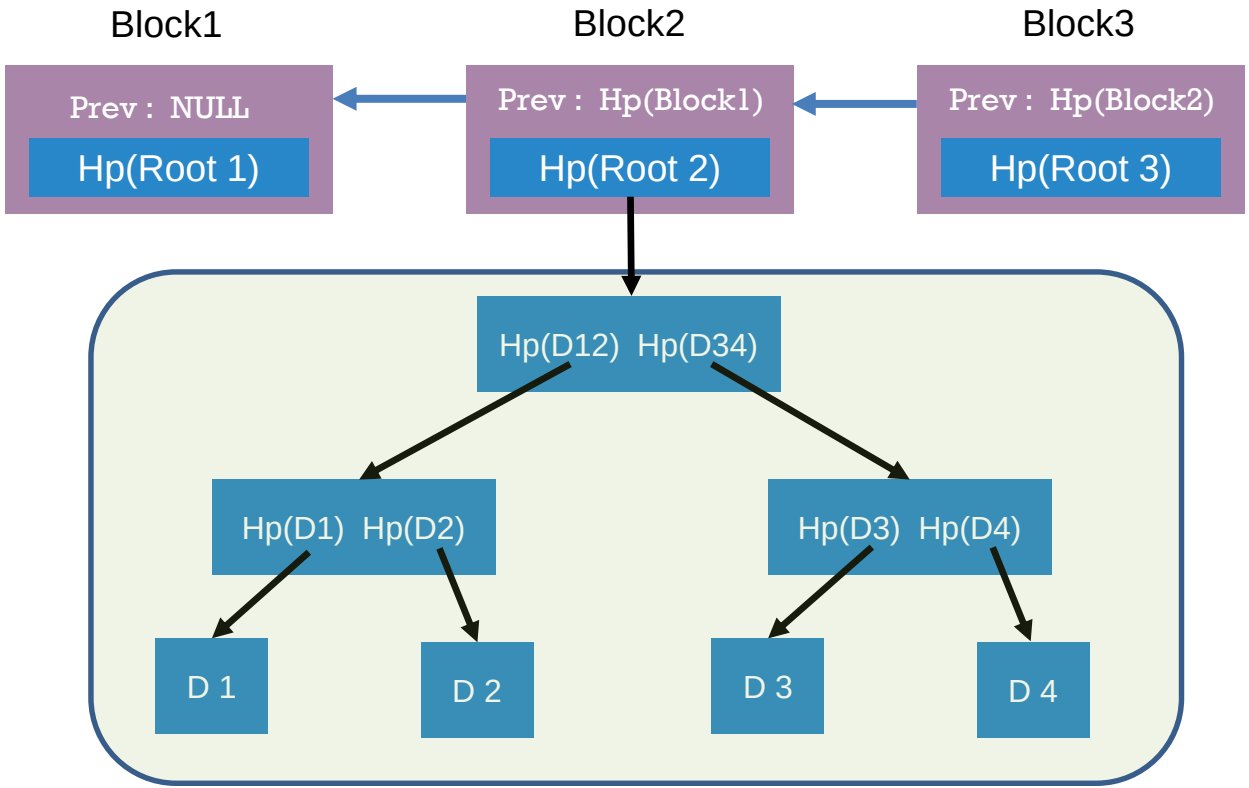
Qué pasa en BitCoin?

Puedo usar arboles para tener tamper-evident log?

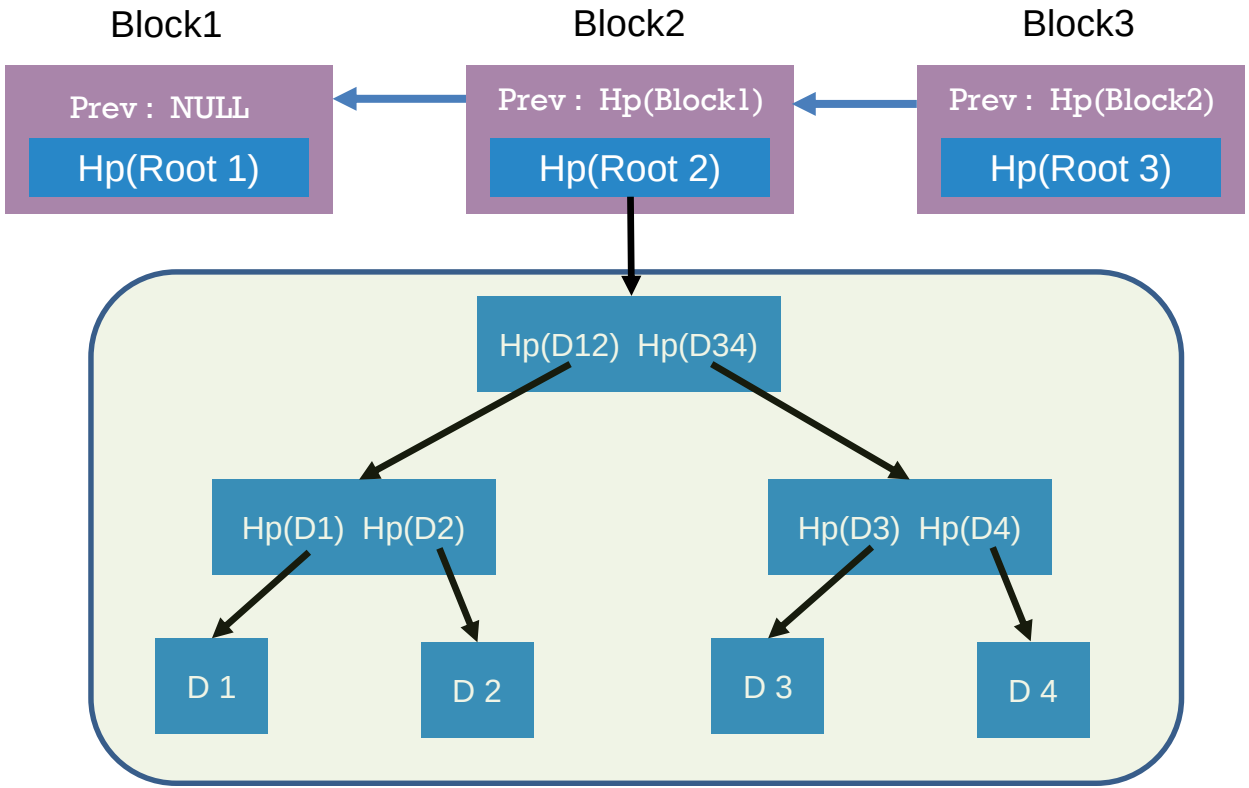
BlockChain:

- Datos en un bloque = árbol de Merkle
- Bloques forman un blockchain

Qué pasa en BitCoin?



Qué pasa en BitCoin?



En BitCoin:

D_i es una transacción

Referencias

Lectura:

- Capitulo 1.3 en el libro azul
- Capitulo 11 de Programming Bitcoin (Jimmy Song)

Referencias

Todas las imagenes de esta clase eran recuperadas en:

https://pixabay.com/