Blockchain

¿Cómo funciona Bitcoin?

Contenidos

Una clase de estructura de datos:

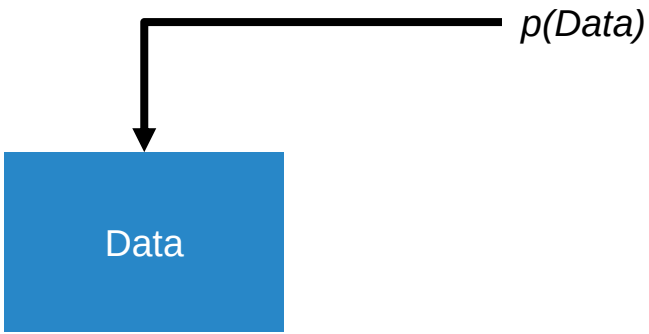
- **Hash pointers**
- Blockchain

Un puntero normal

Un puntero normal

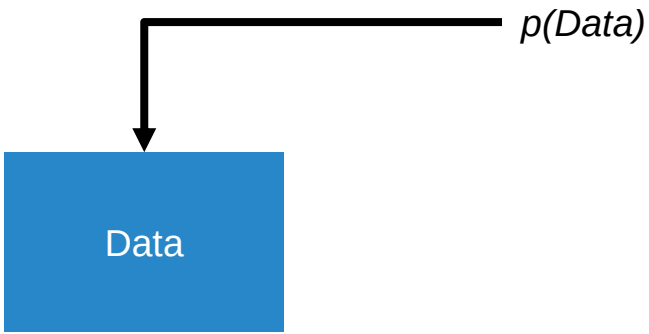
p(Data)

Un puntero normal



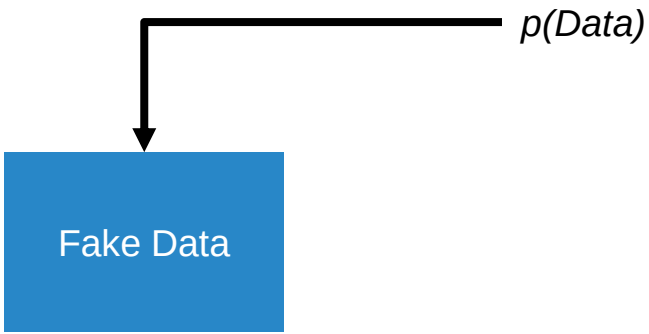
Un puntero normal

Qué pasa si cambian los datos?



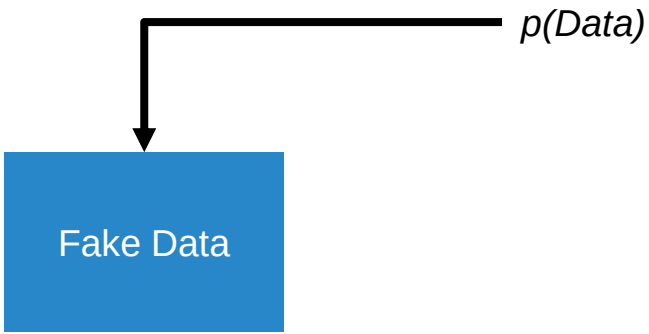
Un puntero normal

Qué pasa si cambian los datos?



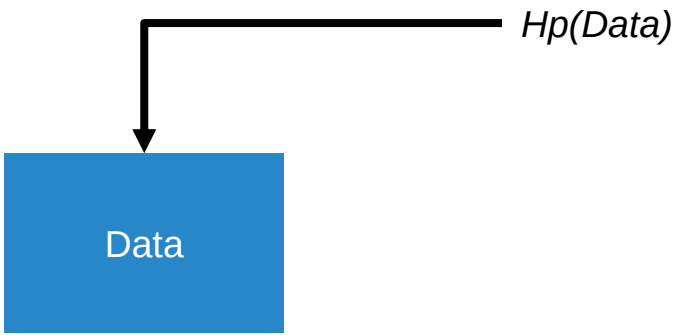
Un puntero normal

Qué pasa si cambian los datos?

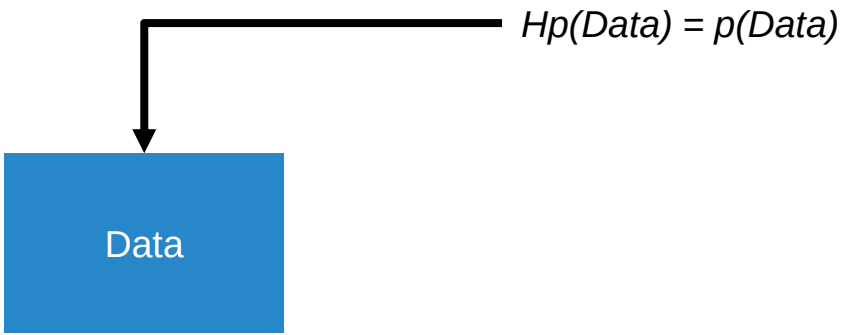


p no refleja el cambio!!!

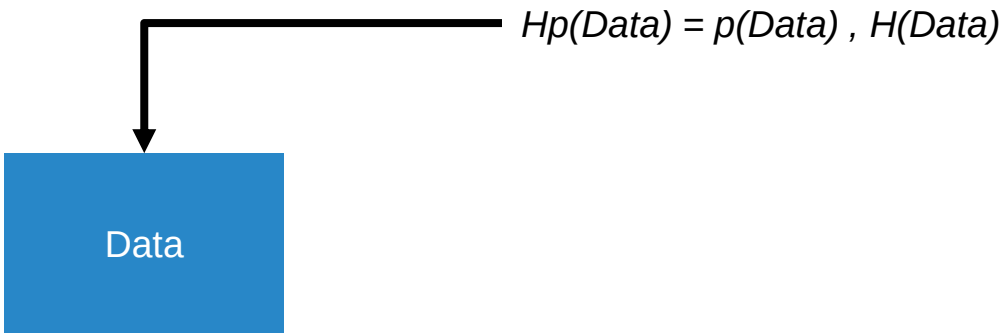
Hash pointer



Hash pointer

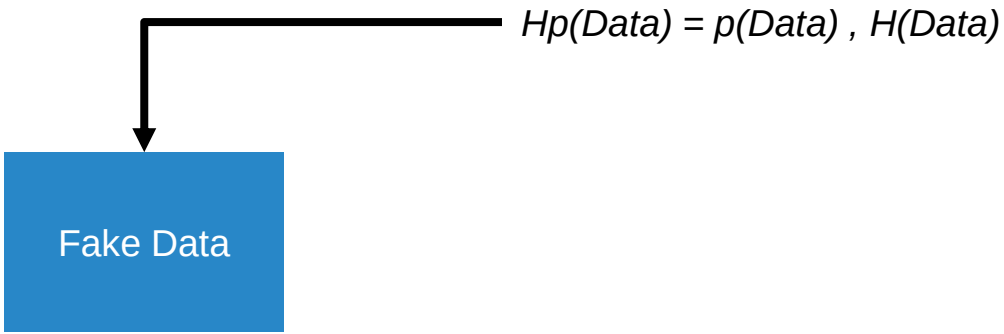


Hash pointer



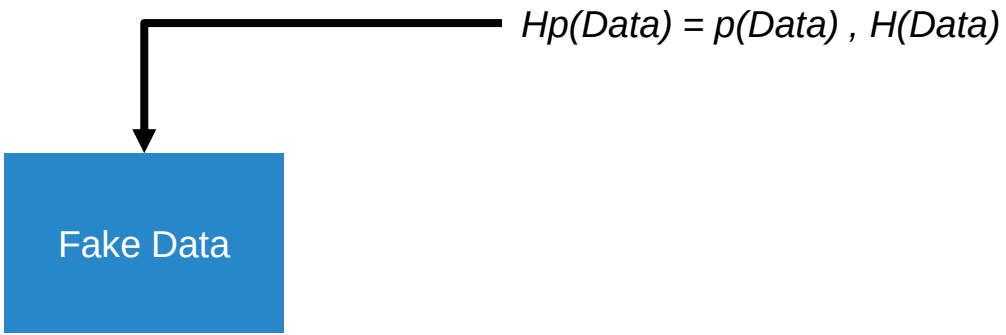
Hash pointer

Qué pasa si cambian los datos?



Hash pointer

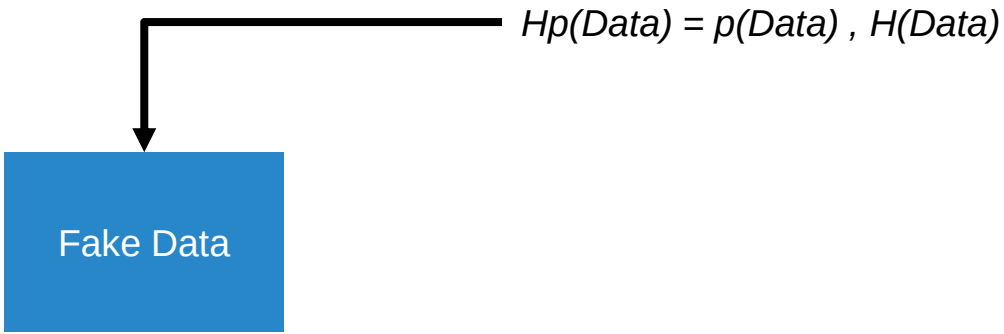
Qué pasa si cambian los datos?



Hp(Data) no apunta a Fake Data

Hash pointer

Qué pasa si cambian los datos?



Hp(Data) no apunta a Fake Data

H(Fake Data) ≠ H(Data)

Hash pointers

Ejemplos de hash pointers:

- Si tengo una variable
- Si mis datos están en un arreglo
- Si mis datos están en un mapping (key-value)

Hash pointers

Uso de hash pointers:

- En cualquier estructura de datos que usa punteros
- Listas ligadas = blockchain
- Arboles binarios = Merkle Trees

Contenidos

Una clase de estructura de datos:

- Hash pointers
- **Blockchain**

Blockchain

Estructura de datos

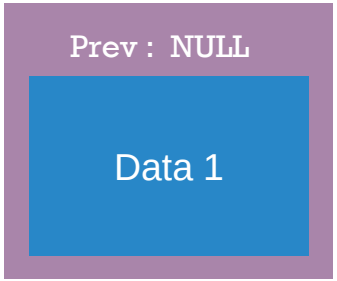
Blockchain

Estructura de datos

Prev : NULL

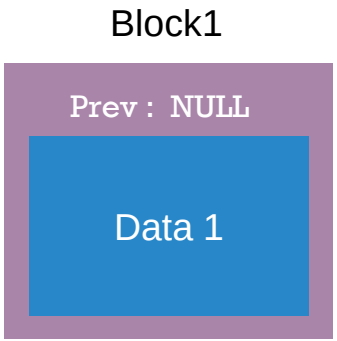
Blockchain

Estructura de datos



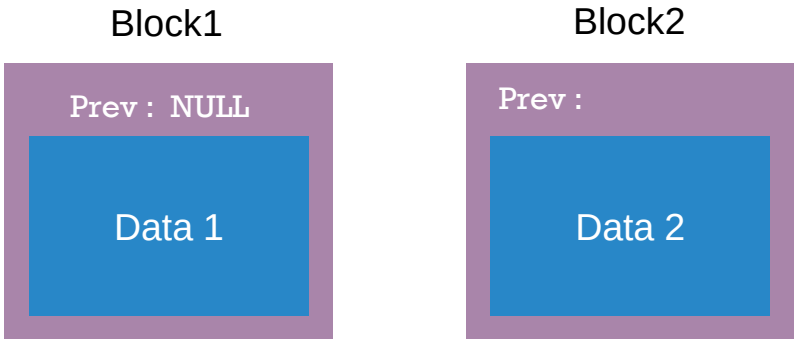
Blockchain

Estructura de datos



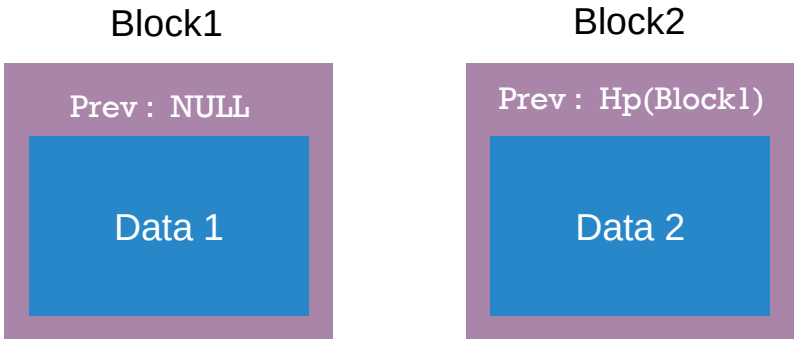
Blockchain

Estructura de datos



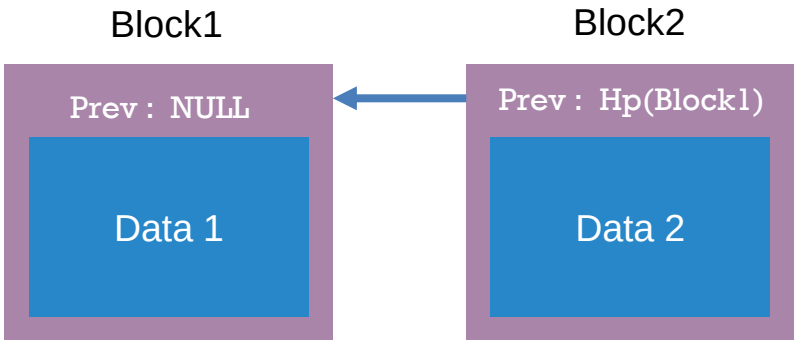
Blockchain

Estructura de datos



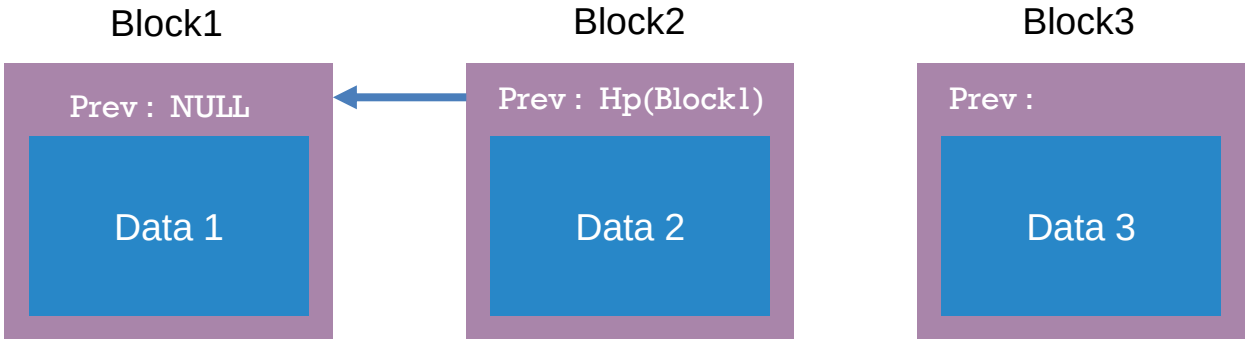
Blockchain

Estructura de datos



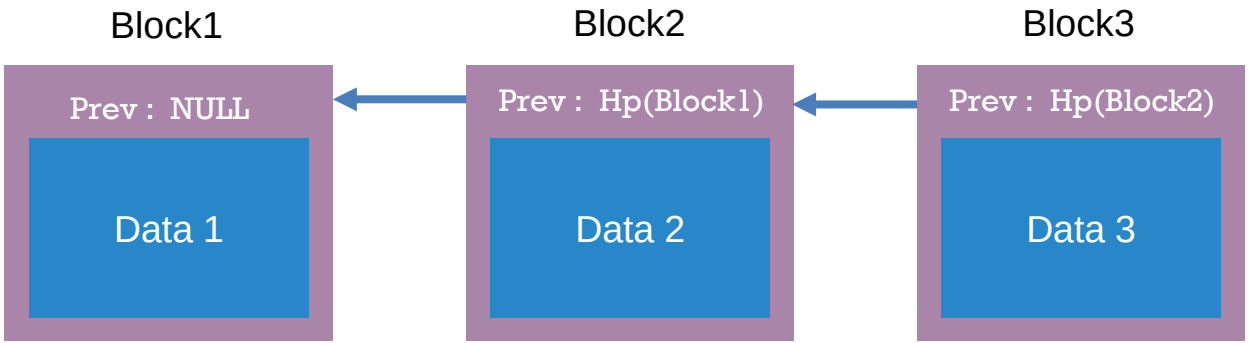
Blockchain

Estructura de datos



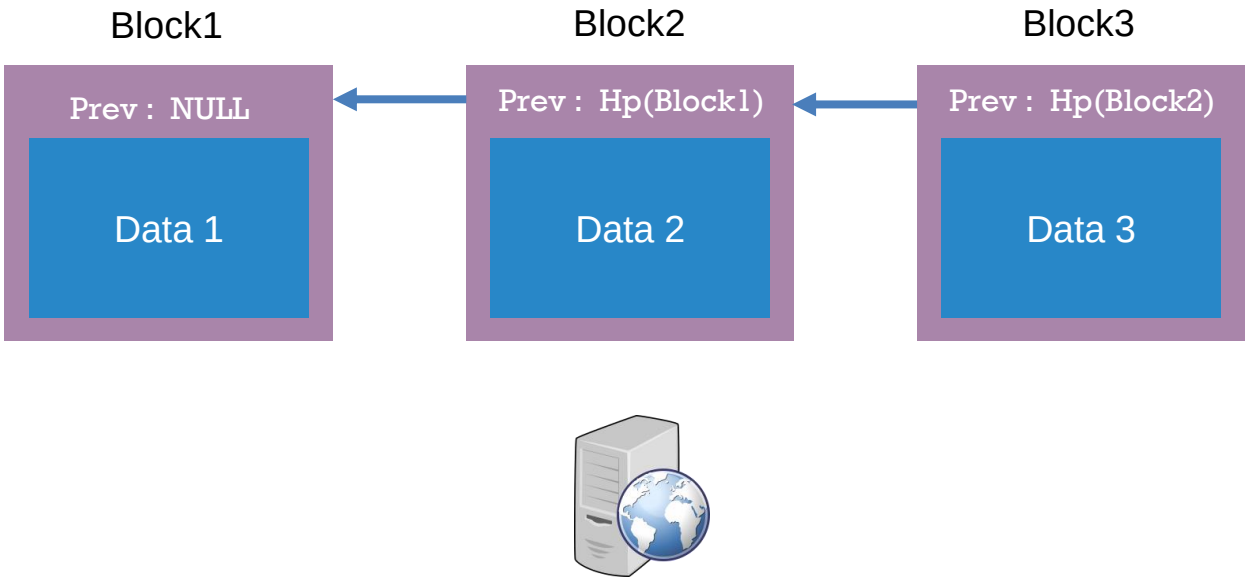
Blockchain

Estructura de datos



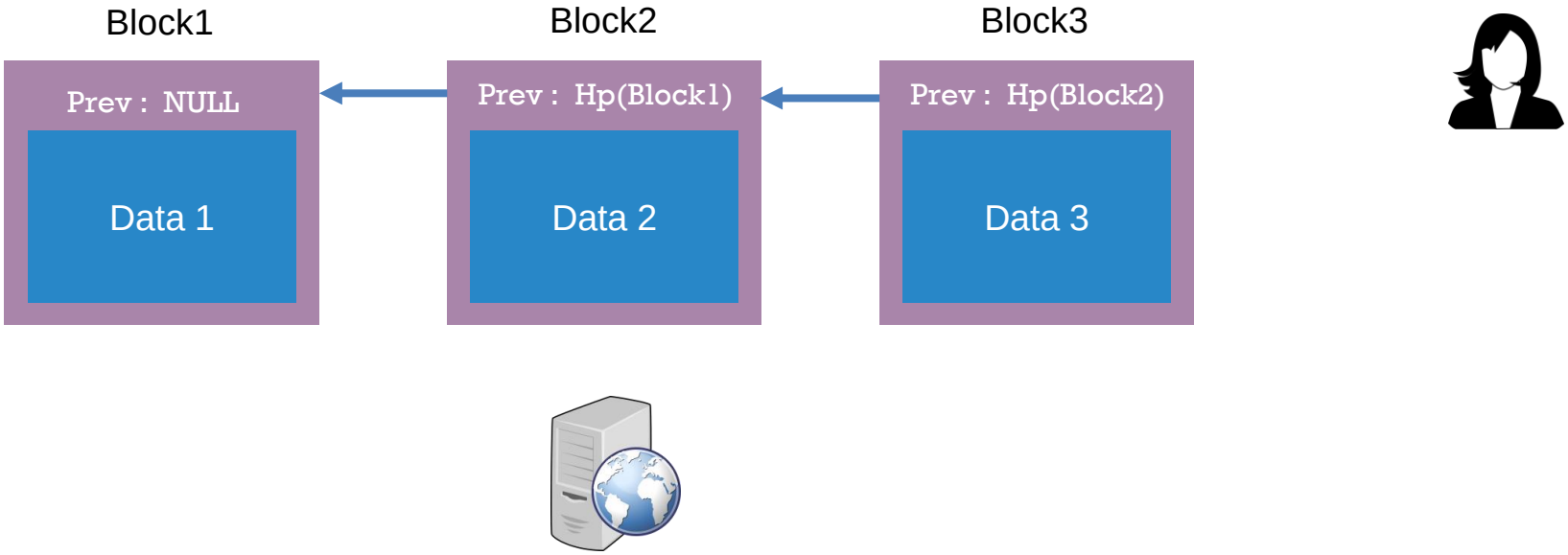
Uso de Blockchain

Tamper-evident log



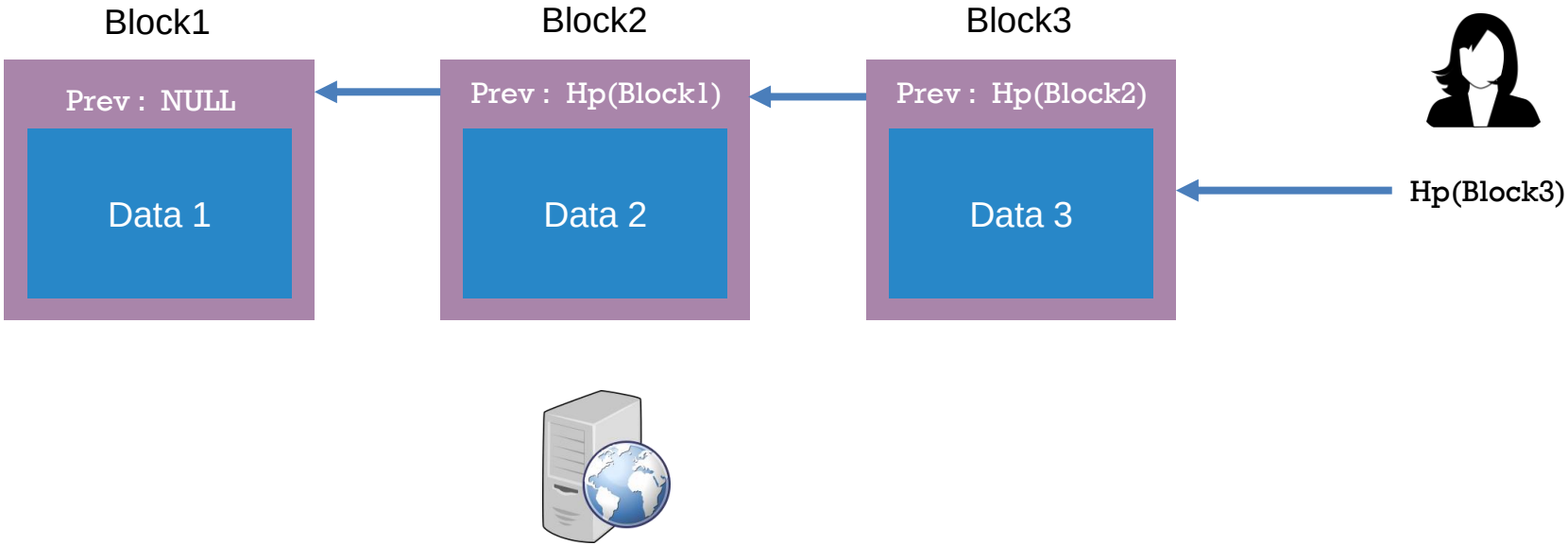
Uso de Blockchain

Tamper-evident log



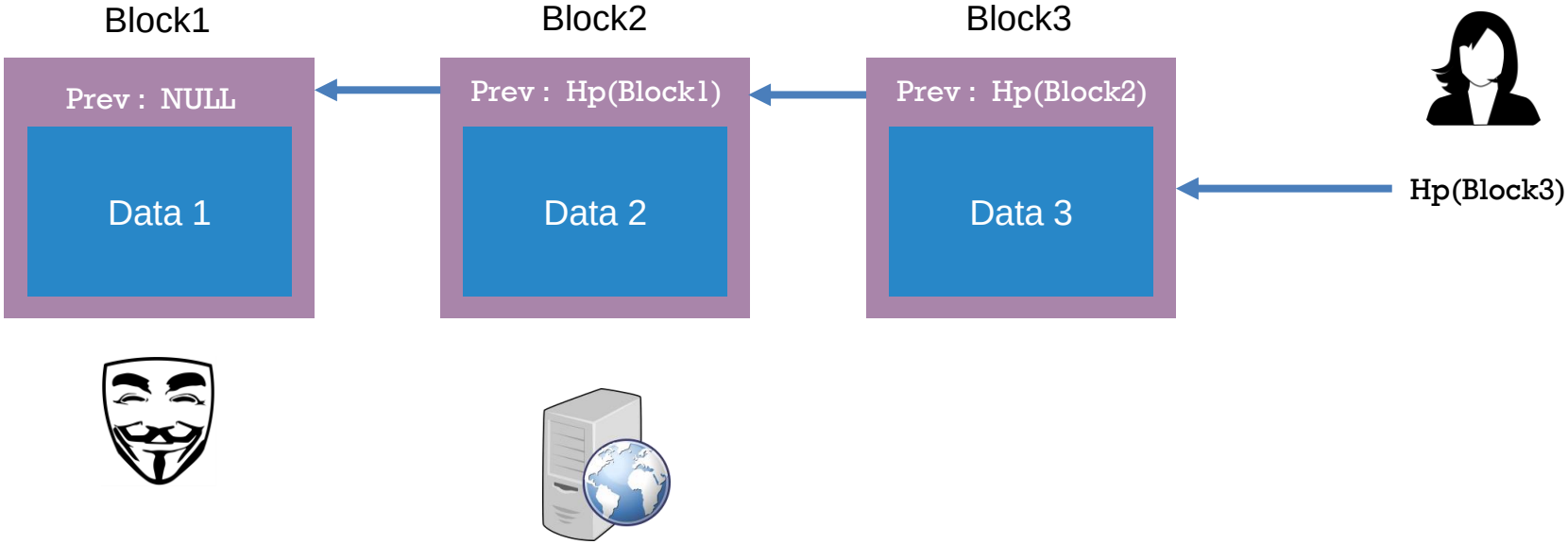
Uso de Blockchain

Tamper-evident log



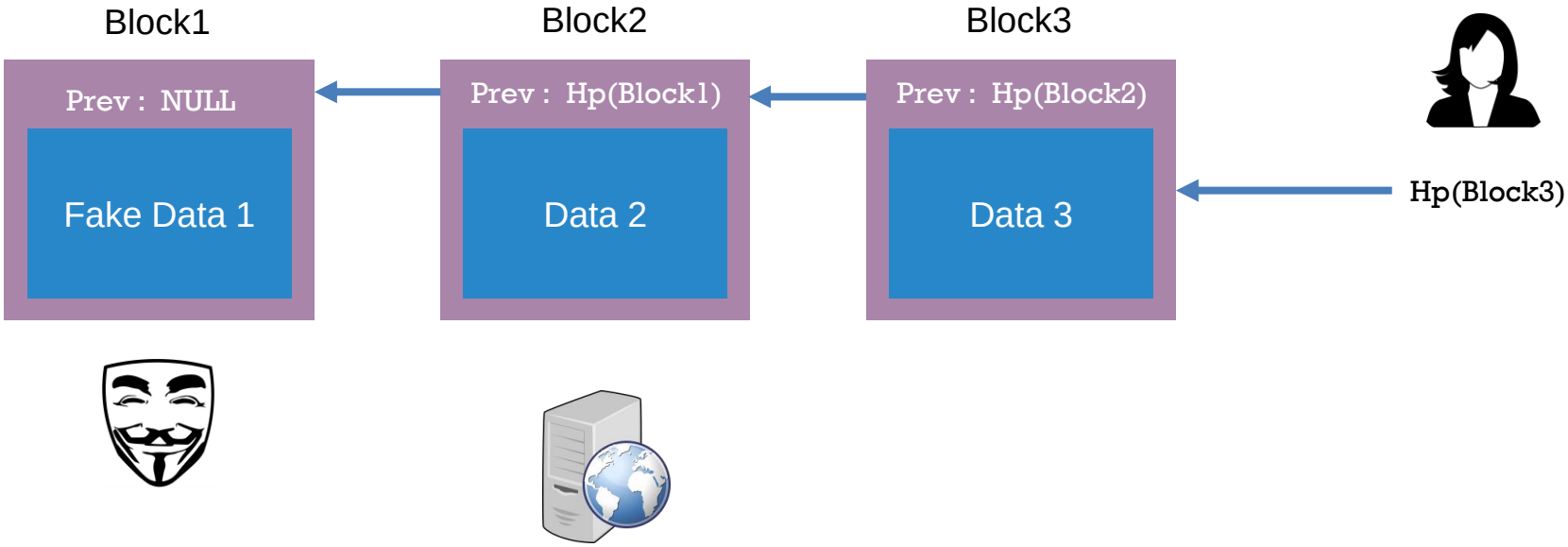
Uso de Blockchain

Tamper-evident log



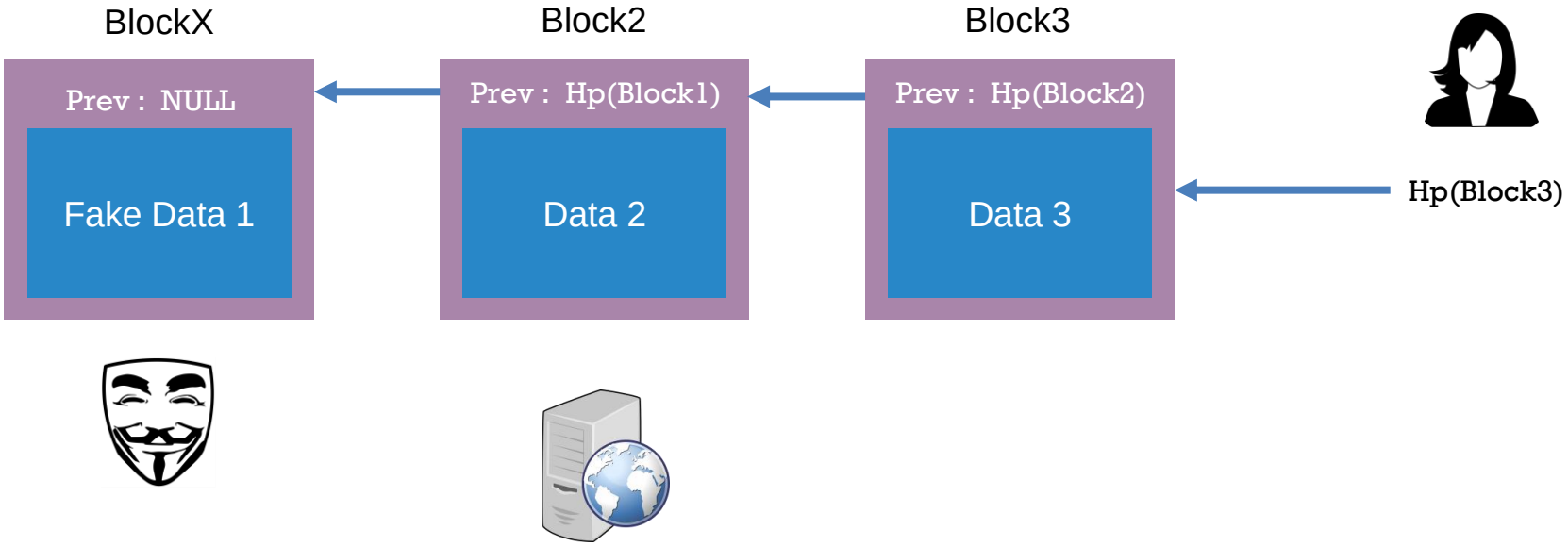
Uso de Blockchain

Tamper-evident log



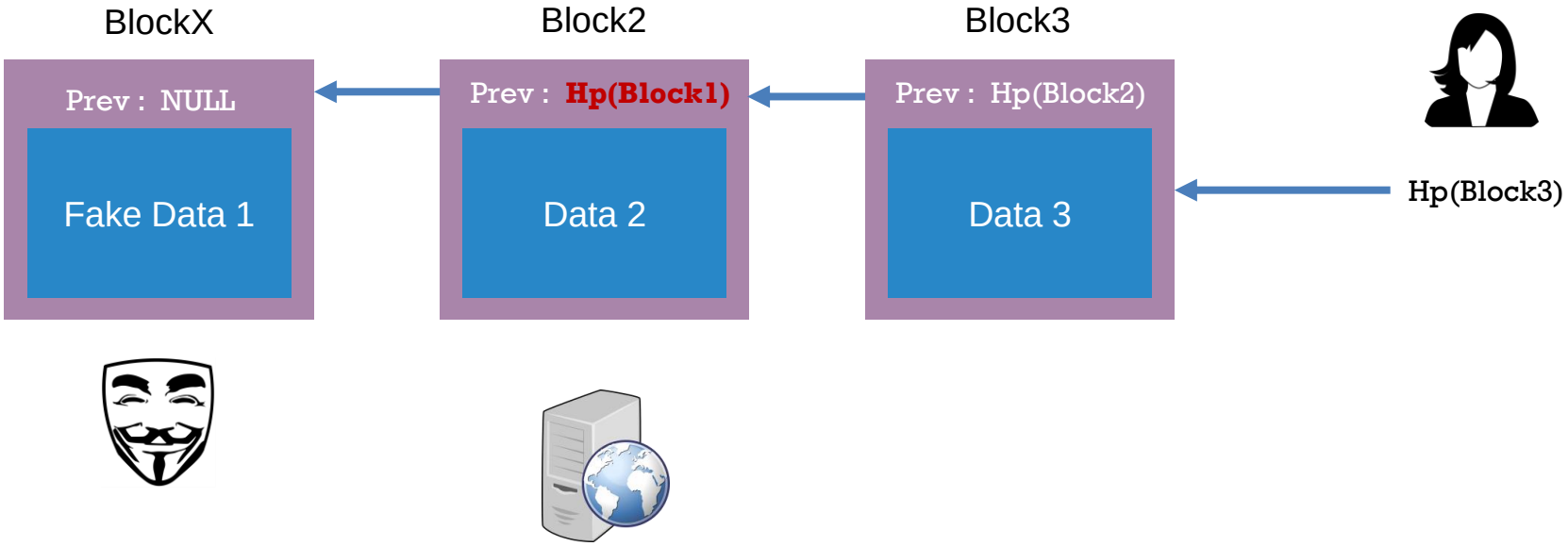
Uso de Blockchain

Tamper-evident log



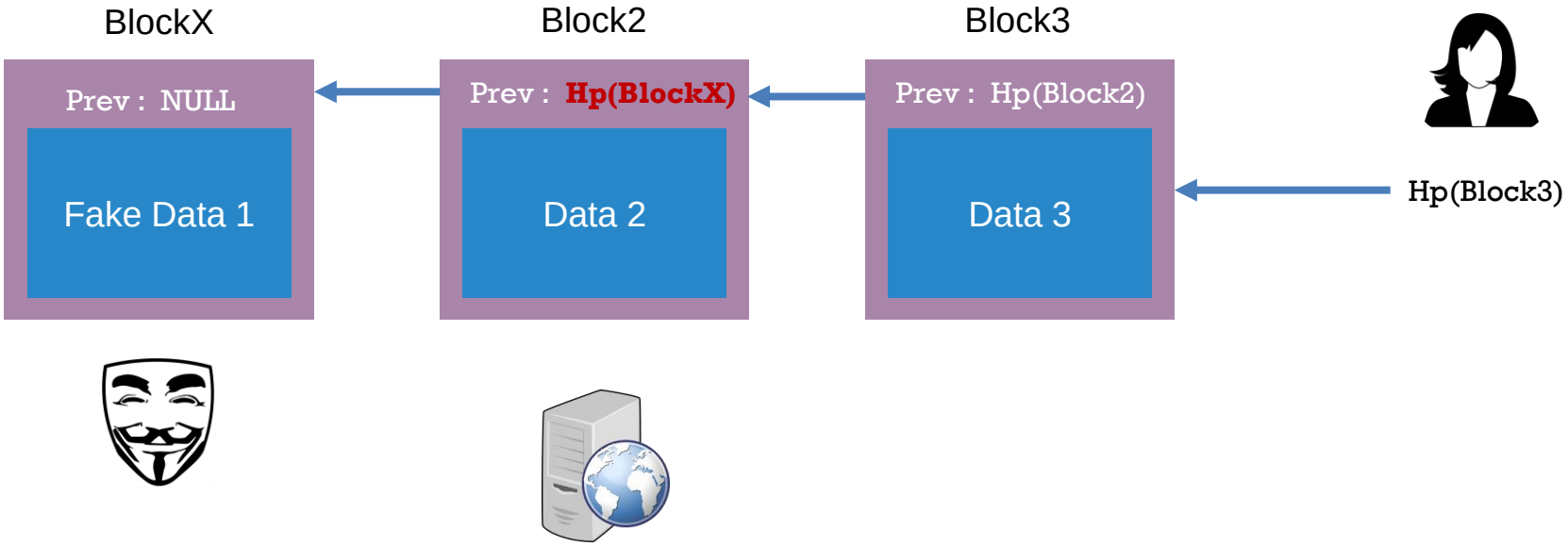
Uso de Blockchain

Tamper-evident log



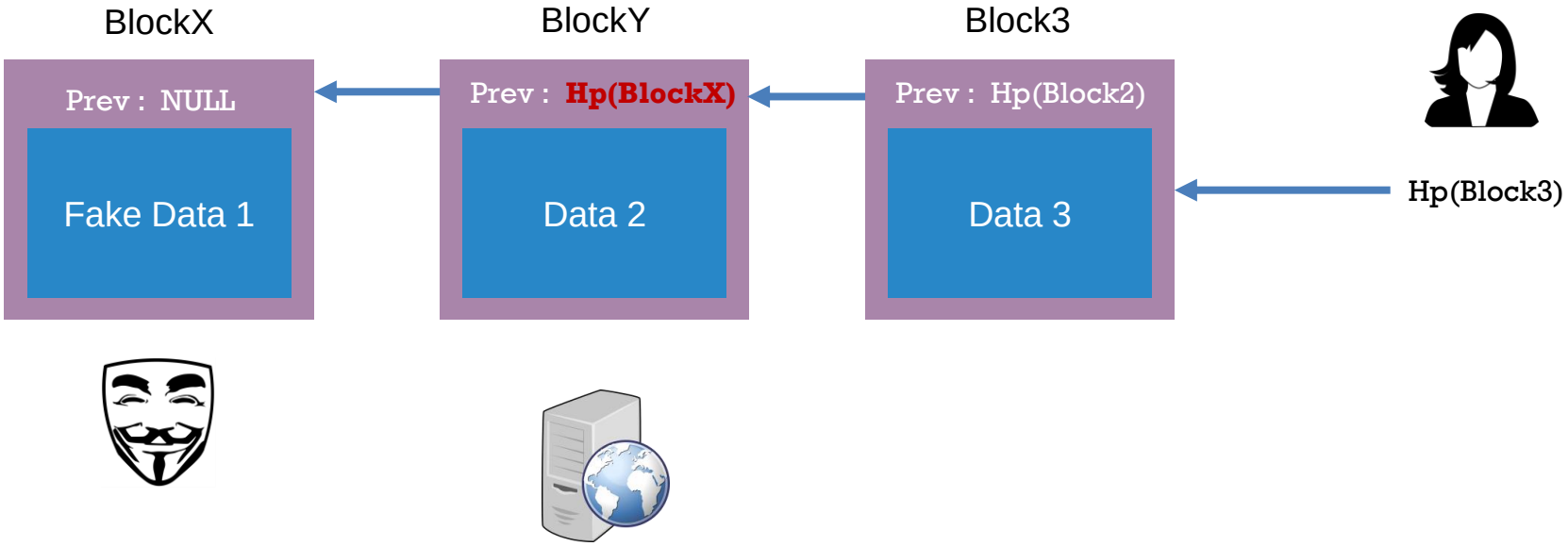
Uso de Blockchain

Tamper-evident log



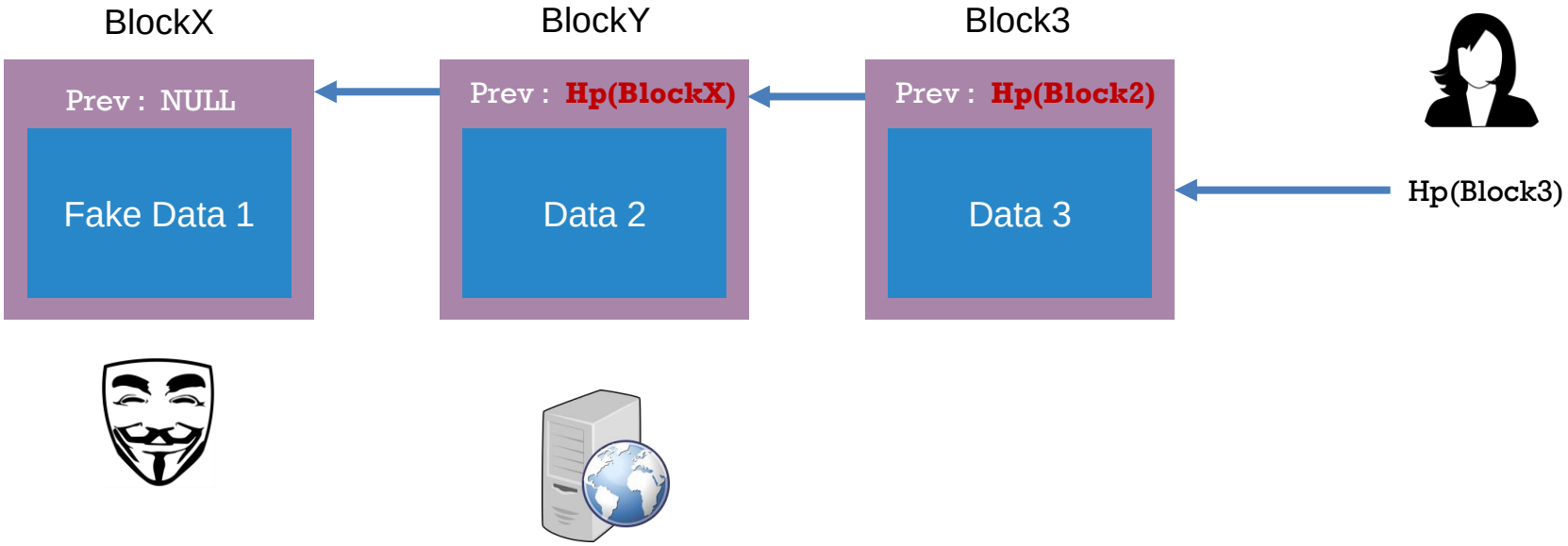
Uso de Blockchain

Tamper-evident log



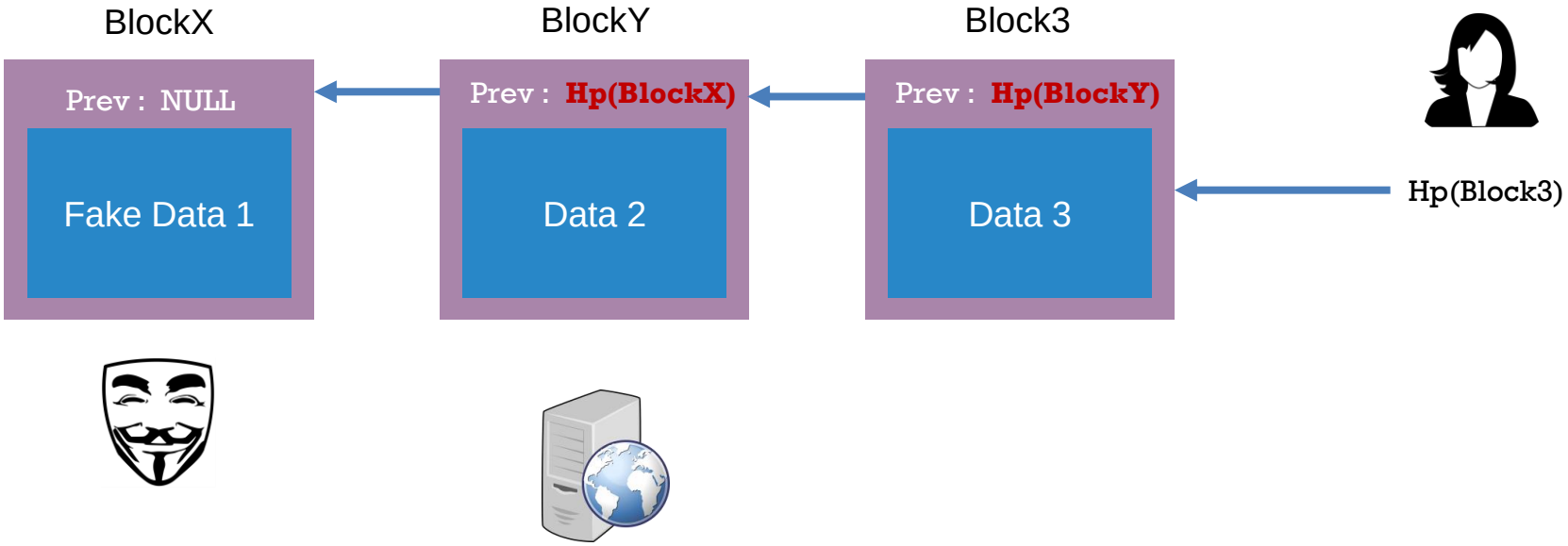
Uso de Blockchain

Tamper-evident log



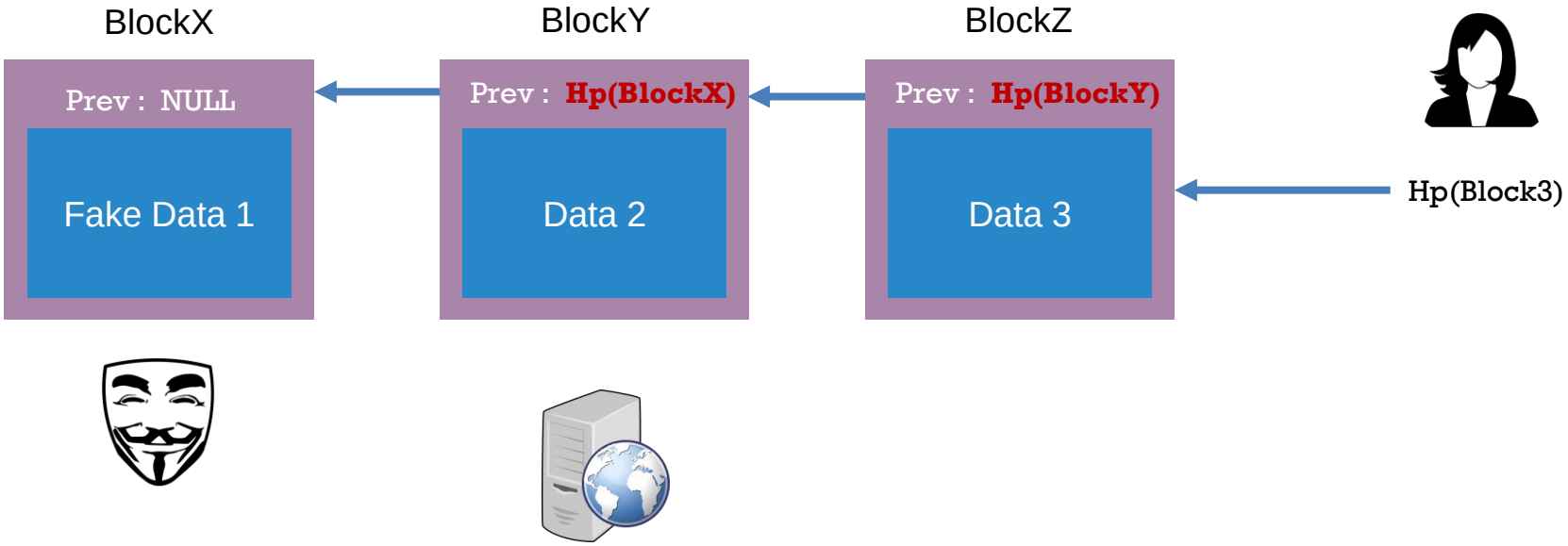
Uso de Blockchain

Tamper-evident log



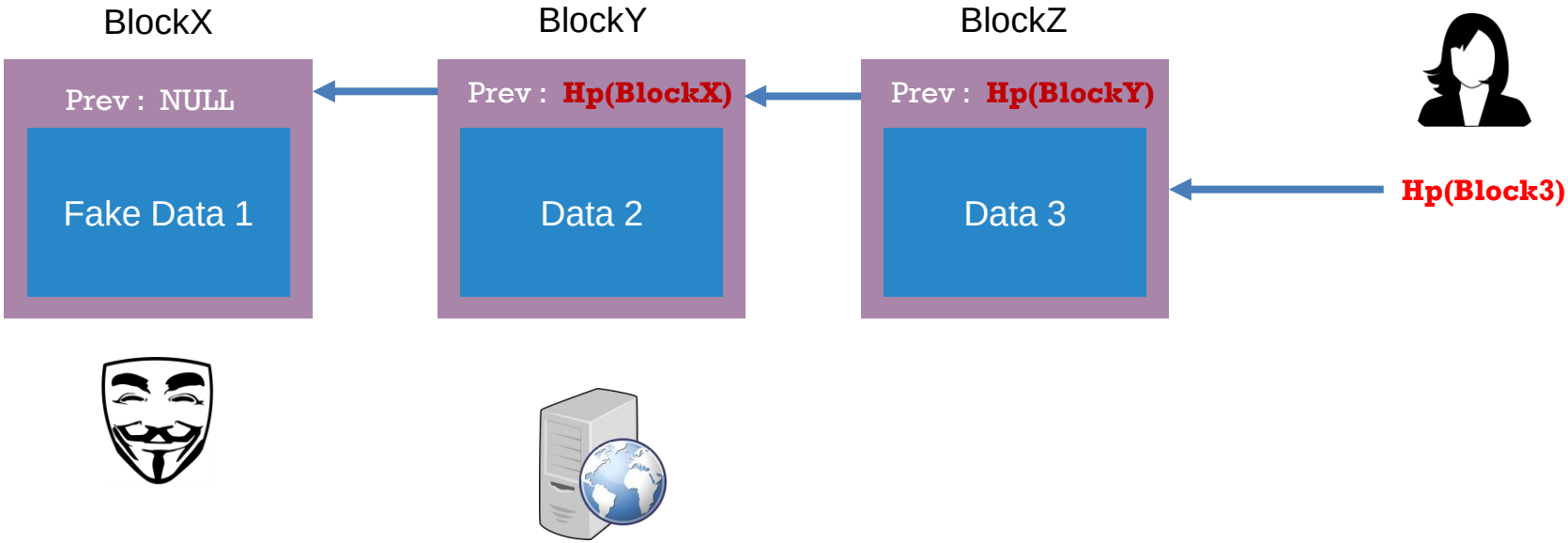
Uso de Blockchain

Tamper-evident log



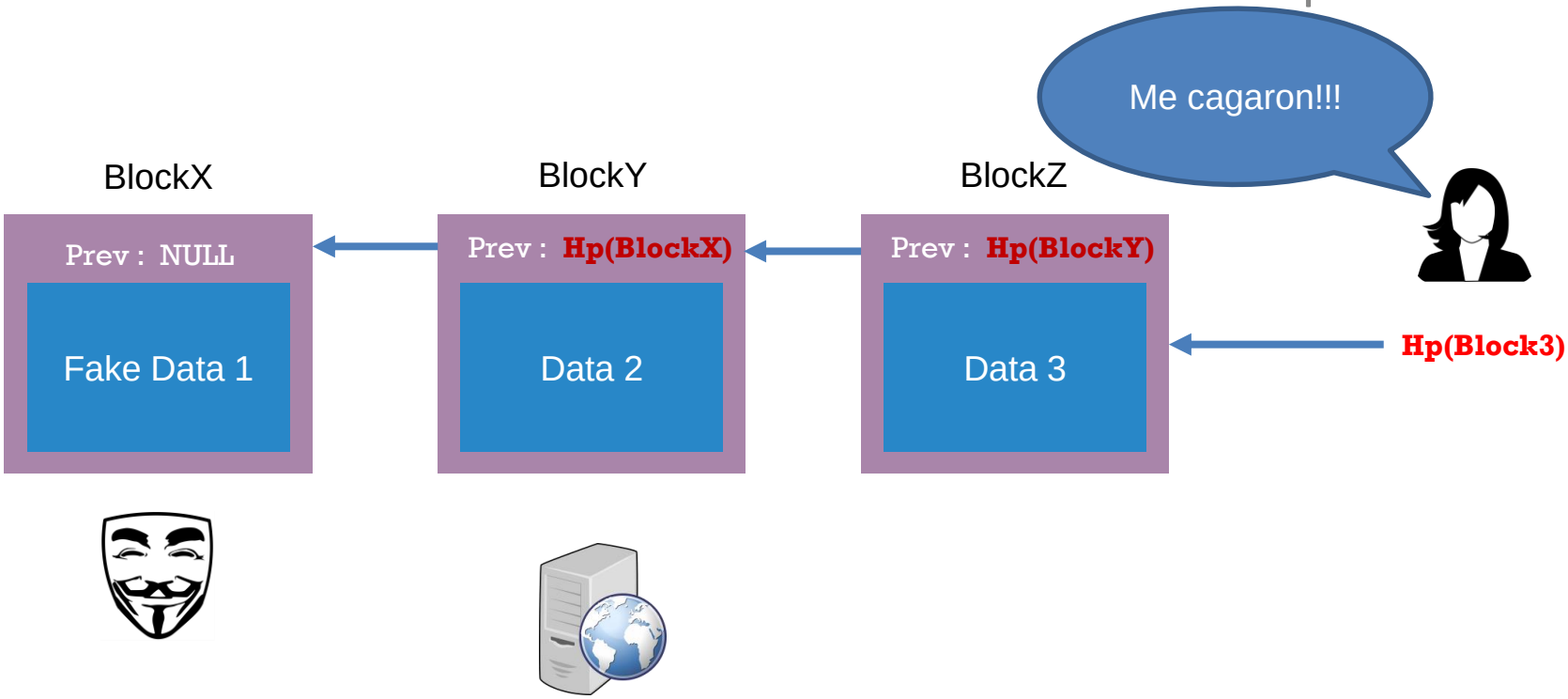
Uso de Blockchain

Tamper-evident log



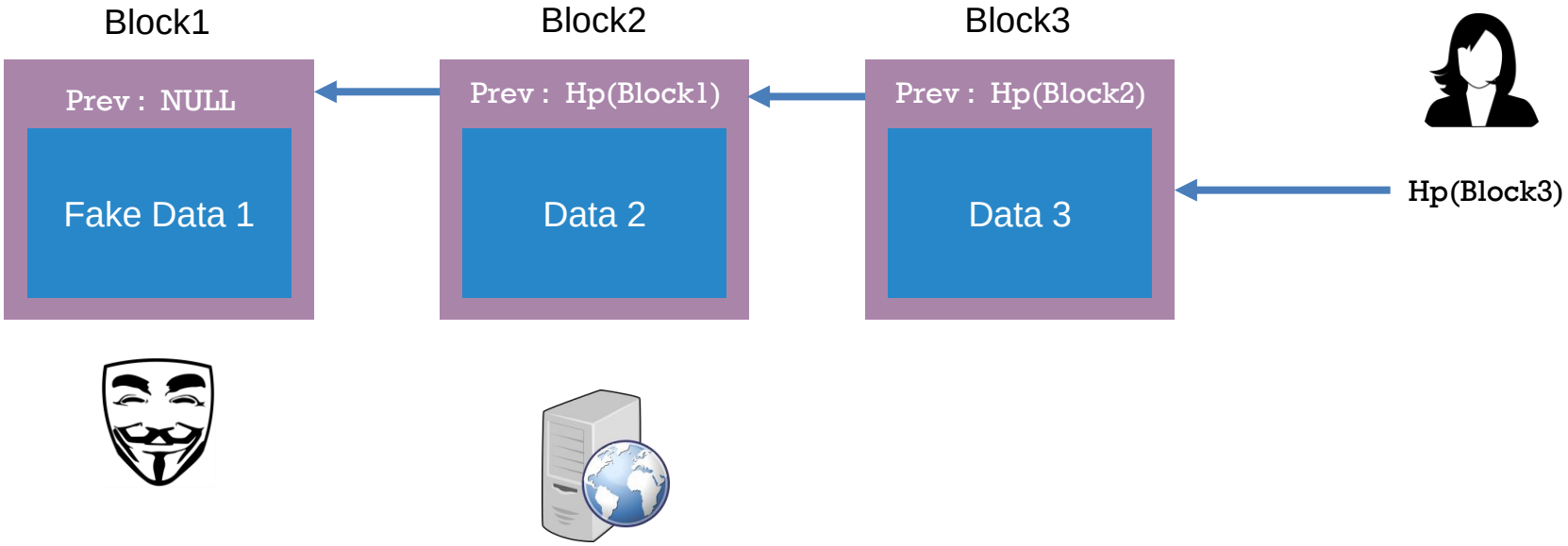
Uso de Blockchain

Tamper-evident log



Uso de Blockchain

Qué pasa si esto es el único cambio?



Problema 3 de ePeso

Consistencia en la historia

Libro contable
Alice paga Bob $50
Alice paga Charlie $20

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Libro contable 2

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Libro contable 2
Bob paga Charlie $250

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Libro contable 2
Bob paga Charlie $250
Bob paga Alice $120

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Libro contable 2
Bob paga Charlie $250
Bob paga Alice $120
Charlie paga Alice $80
Alice paga Bob $20
Alice paga Charlie $10

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
. . .

Libro contable 2
Bob paga Charlie $250
Bob paga Alice $120
Charlie paga Alice $80
Alice paga Bob $20
Alice paga Charlie $10

Libro contable 3

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1	Libro contable 2	Libro contable 3
Alice paga Bob $50	Bob paga Charlie $250	Alice paga Bob $20
Alice paga Charlie $20	Bob paga Alice $120	Alice paga Charlie $10
Bob paga Charlie $100	Charlie paga Alice $80	Bob paga Charlie $100
Charlie paga Alice $40	Alice paga Bob $20	Charlie paga Alice $40
. . .	Alice paga Charlie $10	

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

Libro contable 1	Libro contable 2	Libro contable 3
Alice paga Bob $50	Bob paga Charlie $250	Alice paga Bob $20
Alice paga Charlie $20	Bob paga Alice $120	Alice paga Charlie $10
Bob paga Charlie $100	Charlie paga Alice $80	Bob paga Charlie $100
Charlie paga Alice $40	Alice paga Bob $20	Charlie paga Alice $40
. . .	Alice paga Charlie $10	

Alice

Bob

Charlie

Problema 3 de ePeso

Consistencia en la historia

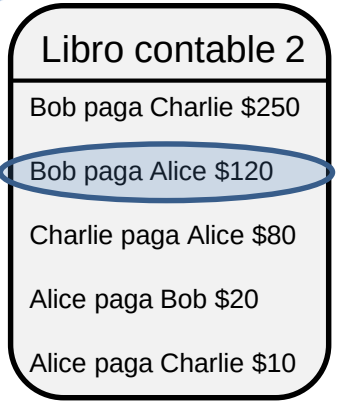
Libro contable 1	Libro contable 2	Libro contable 3
Alice paga Bob $50	Bob paga Charlie $250	Alice paga Bob $20
Alice paga Charlie $20	Bob paga Alice $20	Alice paga Charlie $10
Bob paga Charlie $100	Charlie paga Alice $80	Bob paga Charlie $100
Charlie paga Alice $40	Alice paga Bob $20	Charlie paga Alice $40
. . .	Alice paga Charlie $10	

Alice

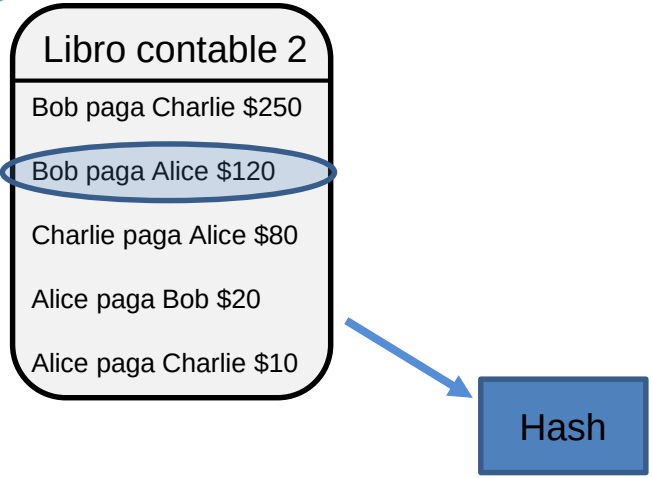
Bob

Charlie

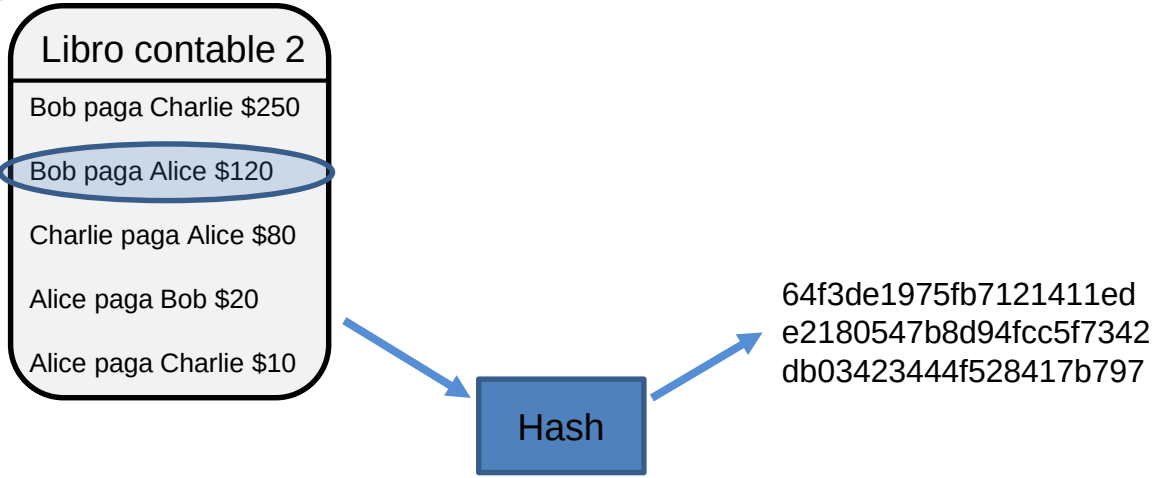
Propiedad de función de hash



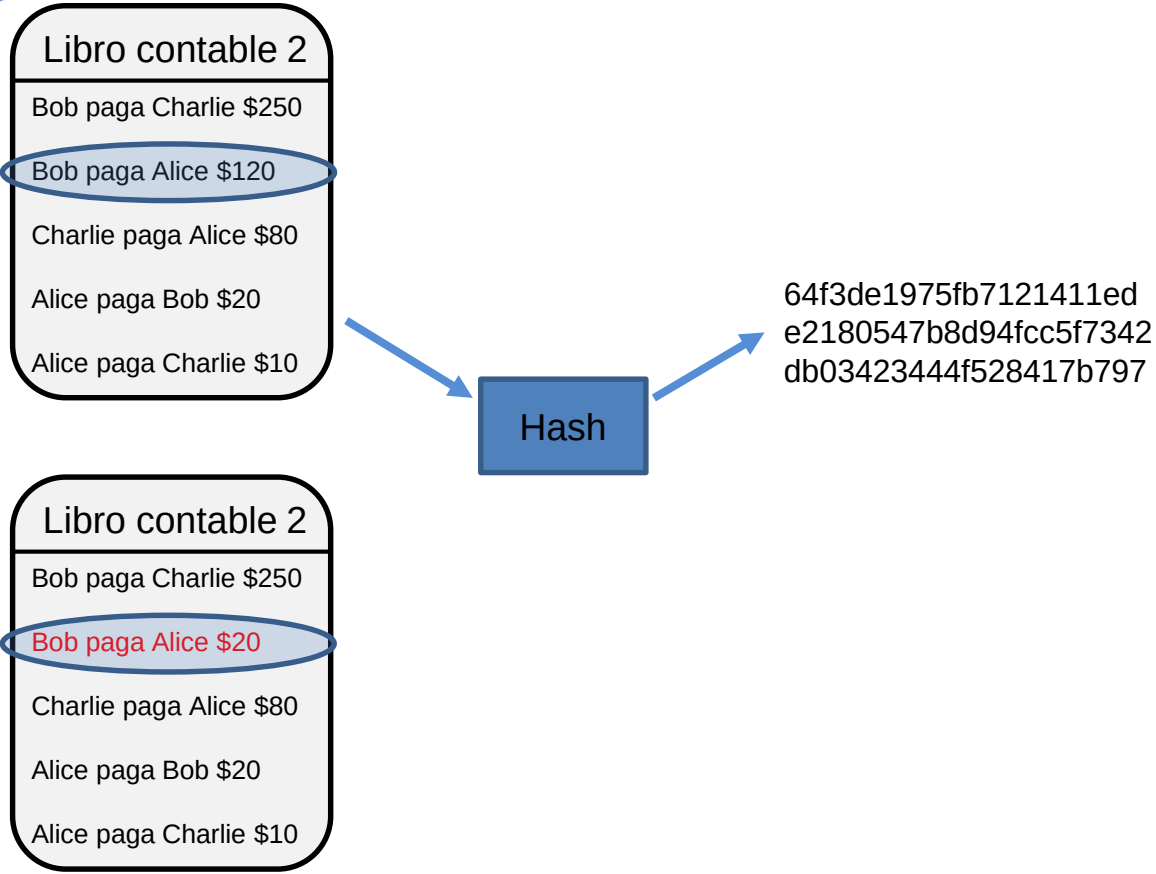
Propiedad de función de hash



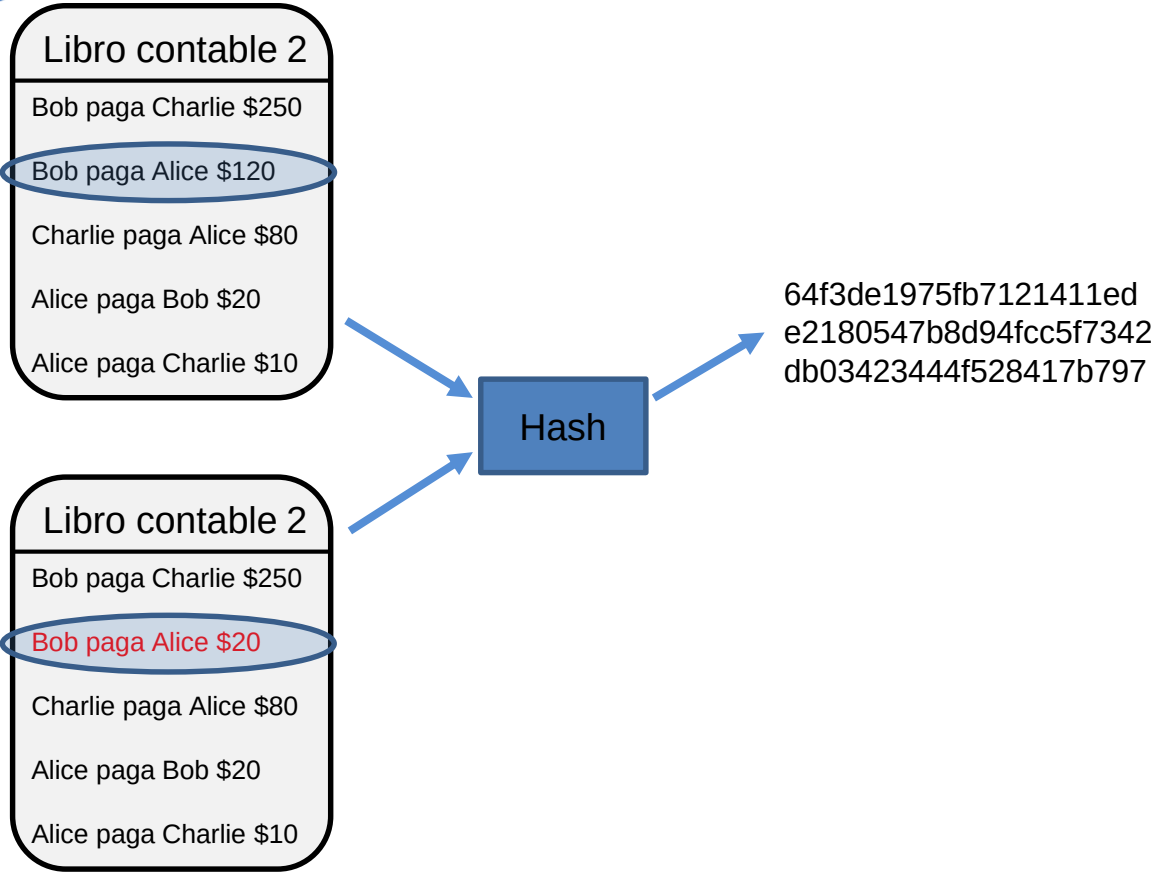
Propiedad de función de hash



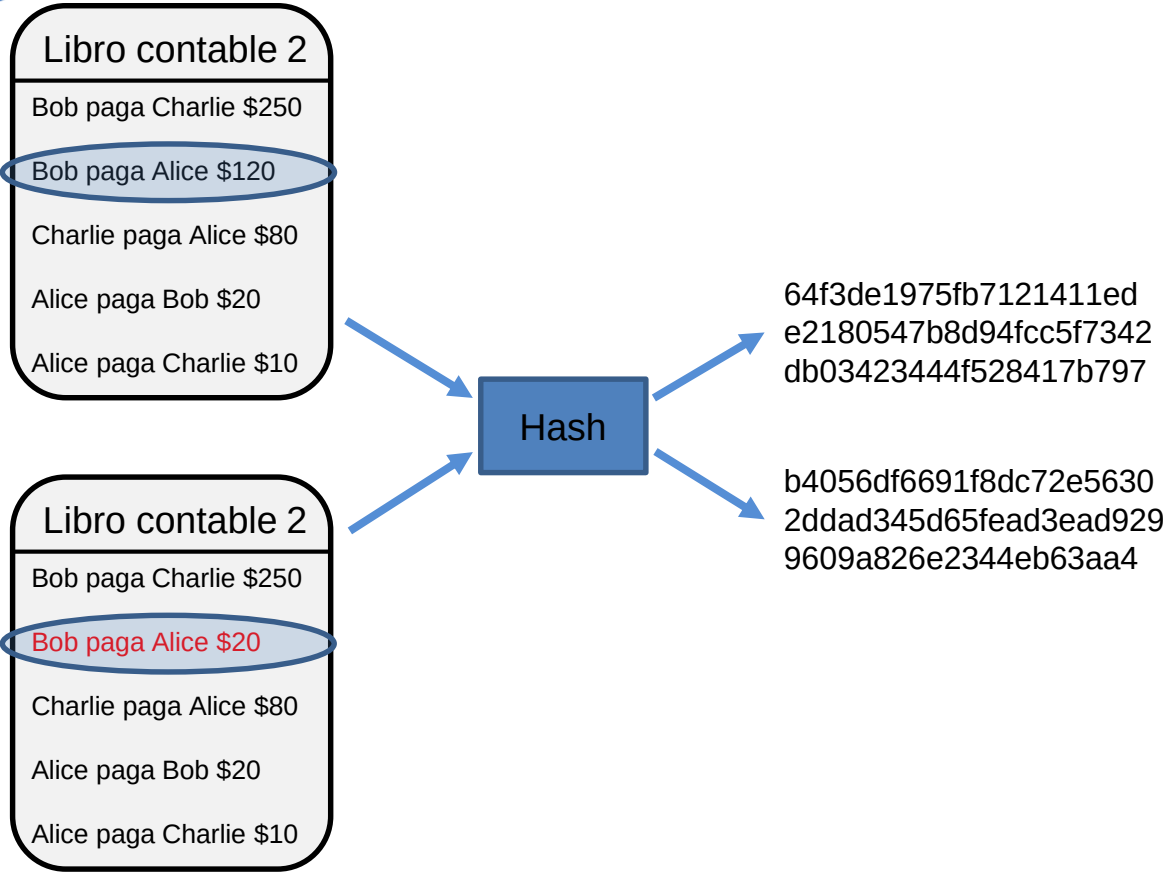
Propiedad de función de hash



Propiedad de función de hash

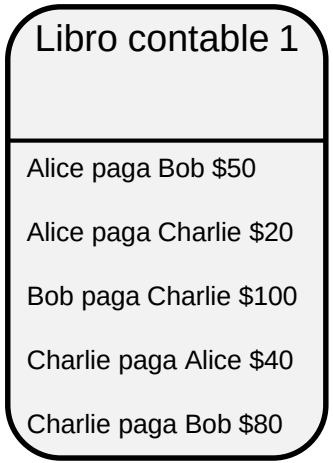


Propiedad de función de hash



Blockchain

Consistencia en la historia



Blockchain

Consistencia en la historia

Libro contable 1

Prev hash: NULL

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

Charlie paga Alice $40

Charlie paga Bob $80

Blockchain

Consistencia en la historia

L1

Libro contable 1

Prev hash: NULL

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

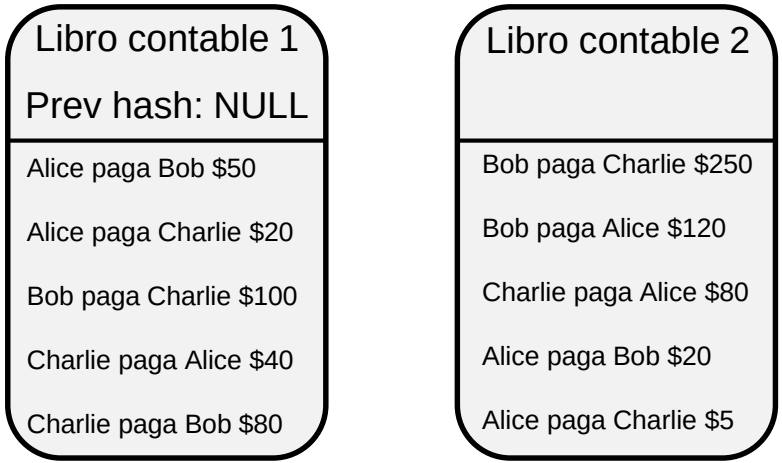
Charlie paga Alice $40

Charlie paga Bob $80

Blockchain

Consistencia en la historia

L1



Blockchain

Consistencia en la historia

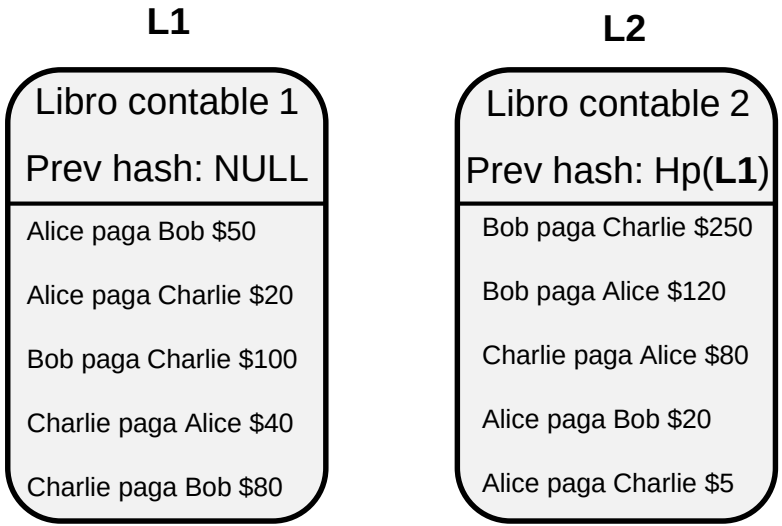
L1

Libro contable 1
Prev hash: NULL
Alice paga Bob $50
Alice paga Charlie $20
Bob paga Charlie $100
Charlie paga Alice $40
Charlie paga Bob $80

Libro contable 2
Prev hash: Hp(**L1**)
Bob paga Charlie $250
Bob paga Alice $120
Charlie paga Alice $80
Alice paga Bob $20
Alice paga Charlie $5

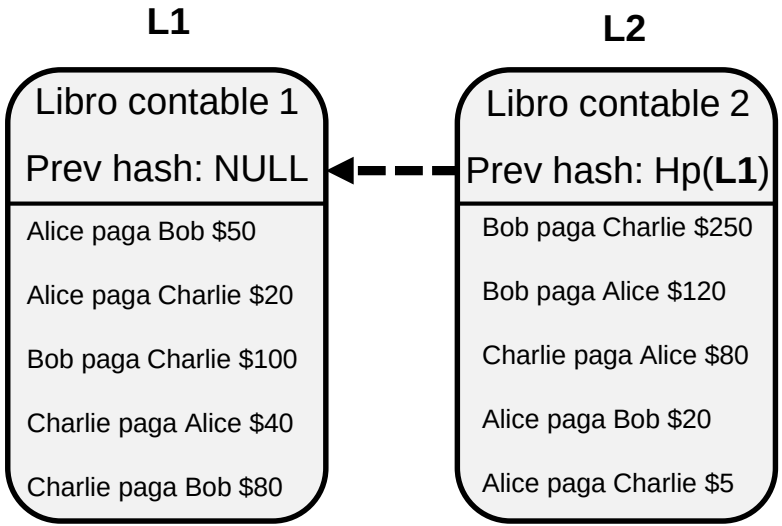
Blockchain

Consistencia en la historia



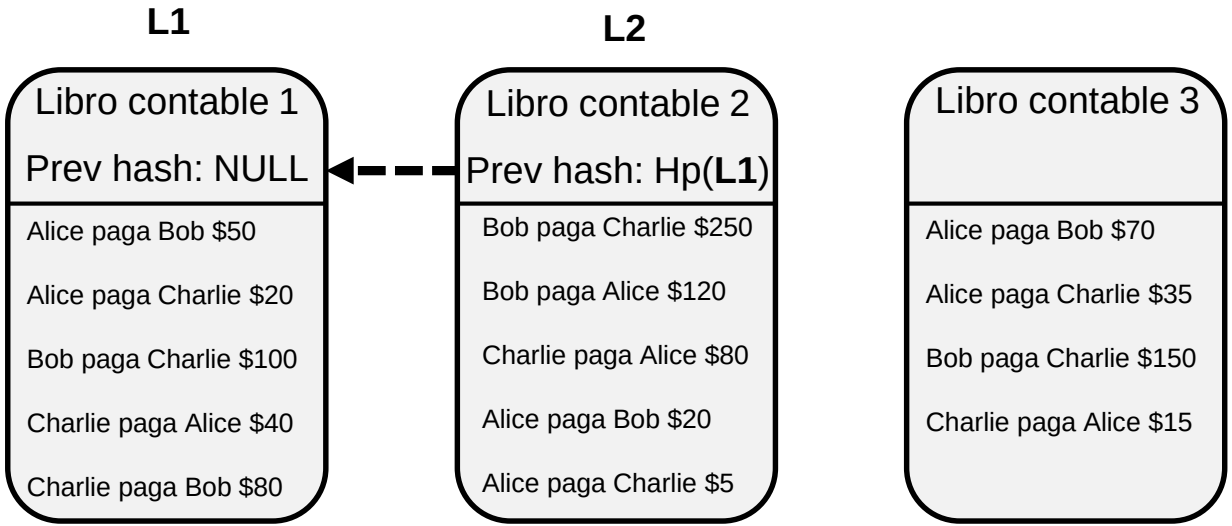
Blockchain

Consistencia en la historia



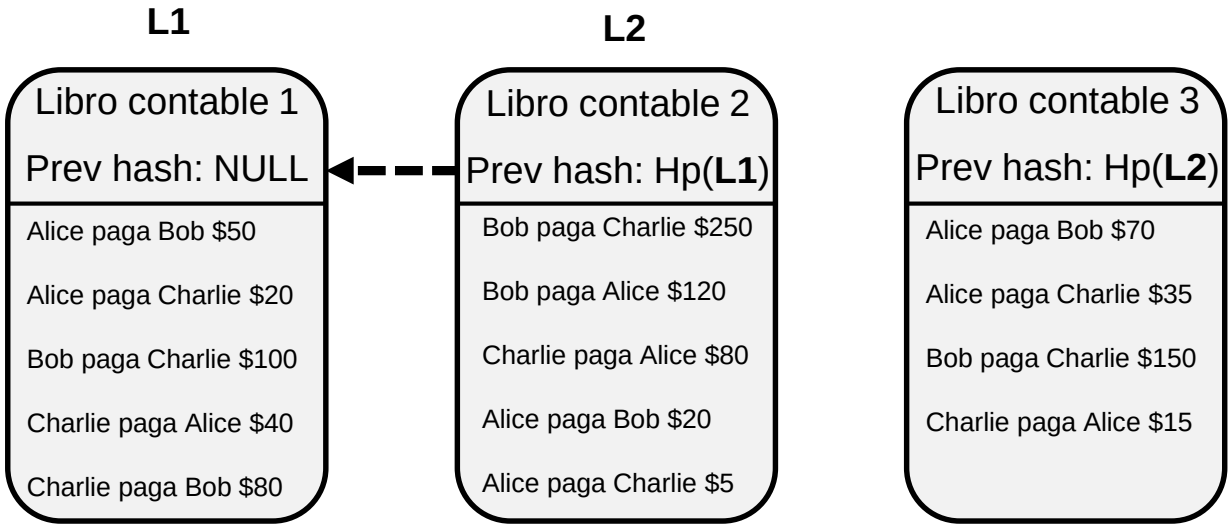
Blockchain

Consistencia en la historia



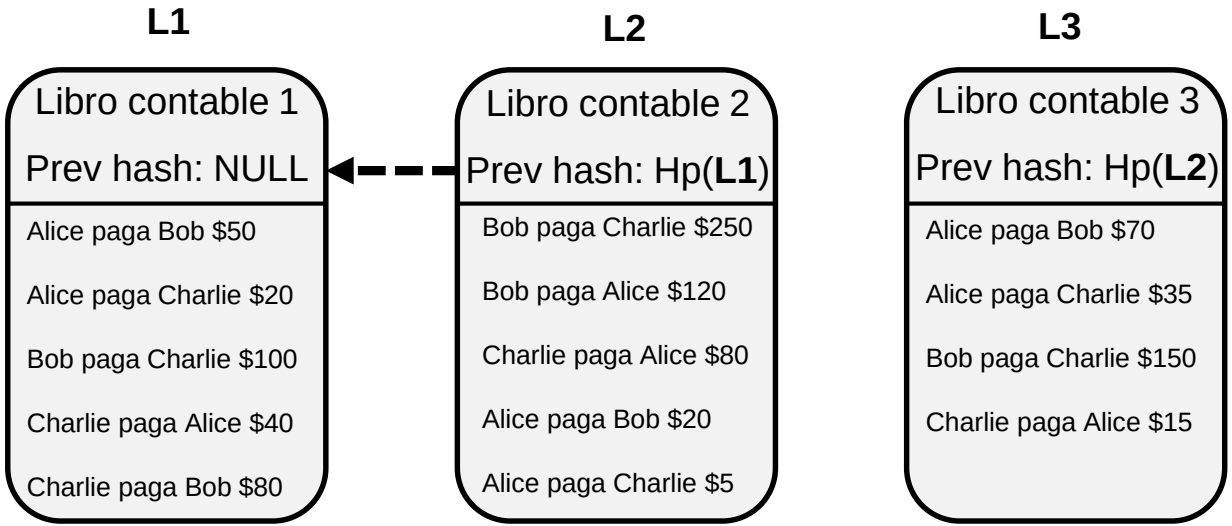
Blockchain

Consistencia en la historia



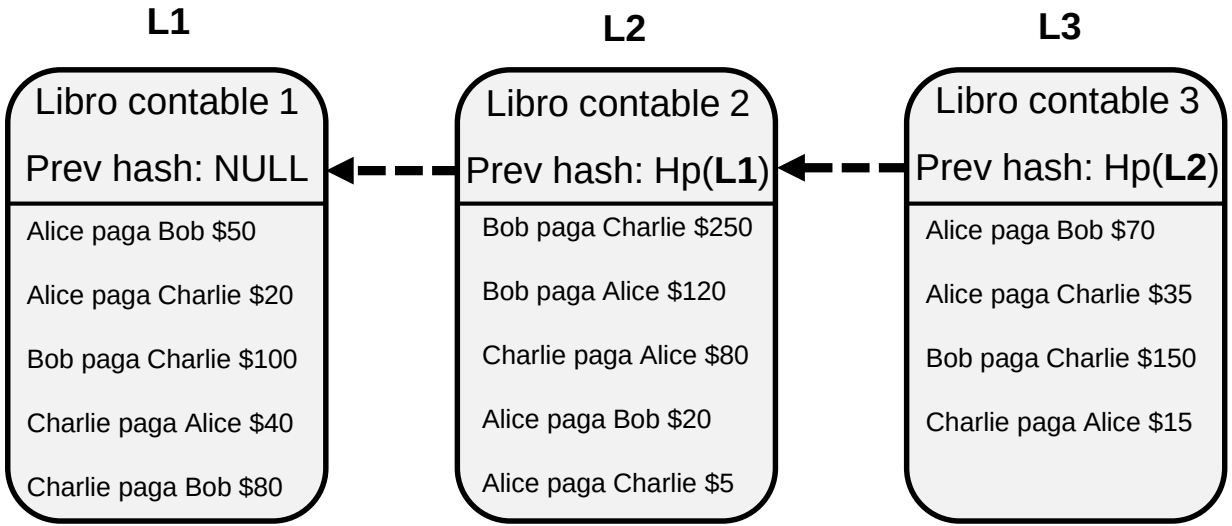
Blockchain

Consistencia en la historia



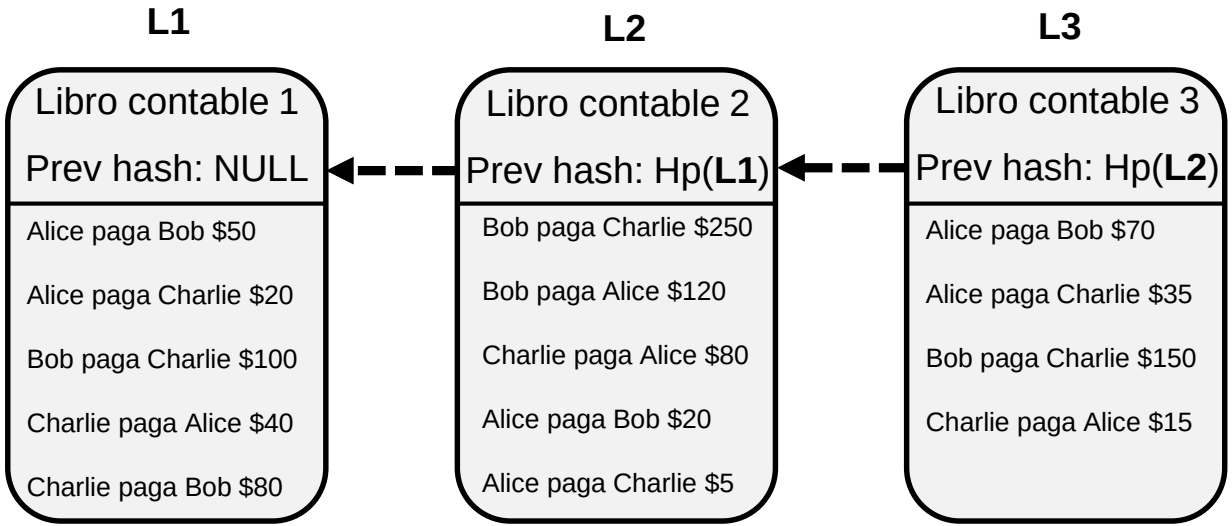
Blockchain

Consistencia en la historia



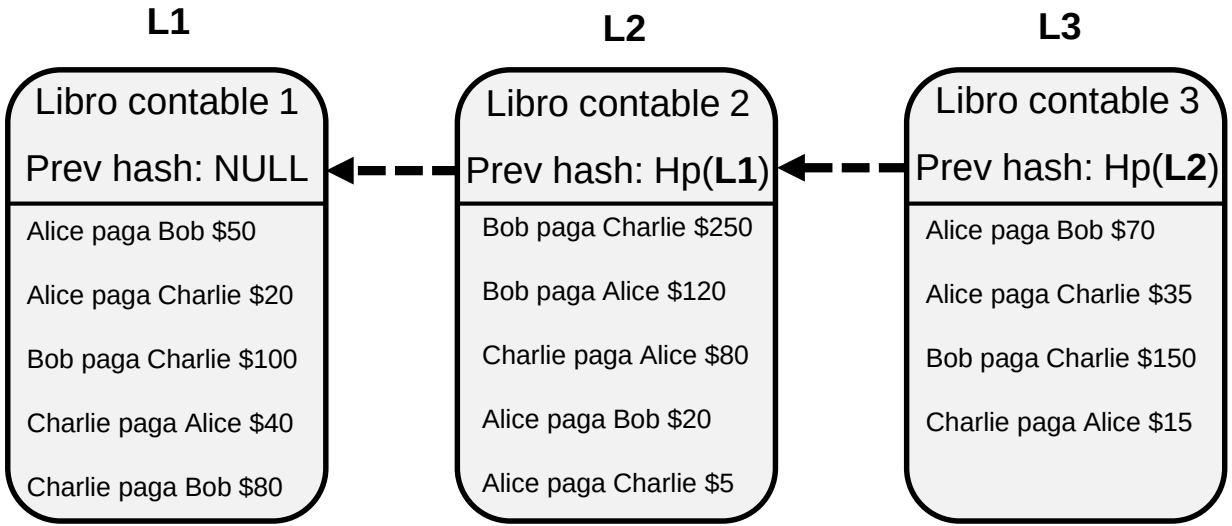
Blockchain

Consistencia en la historia

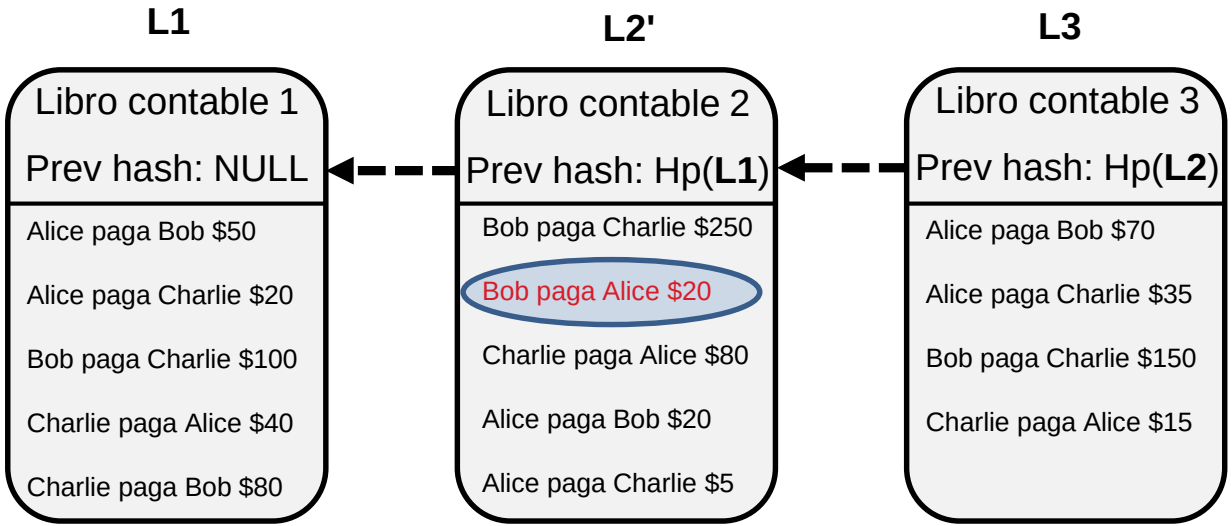


Blockchain

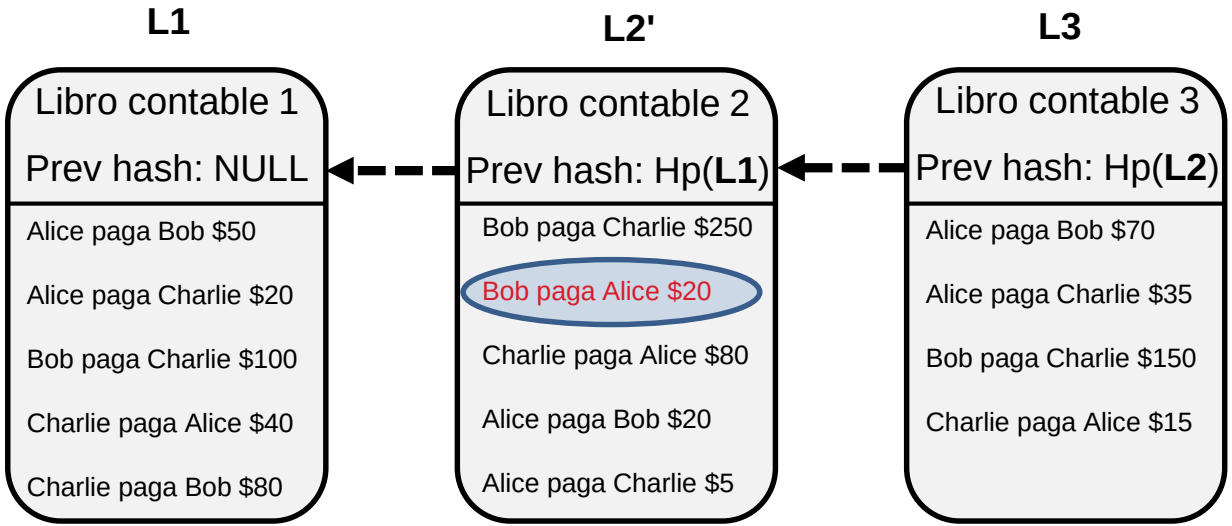
Inmutabilidad



Inmutabilidad

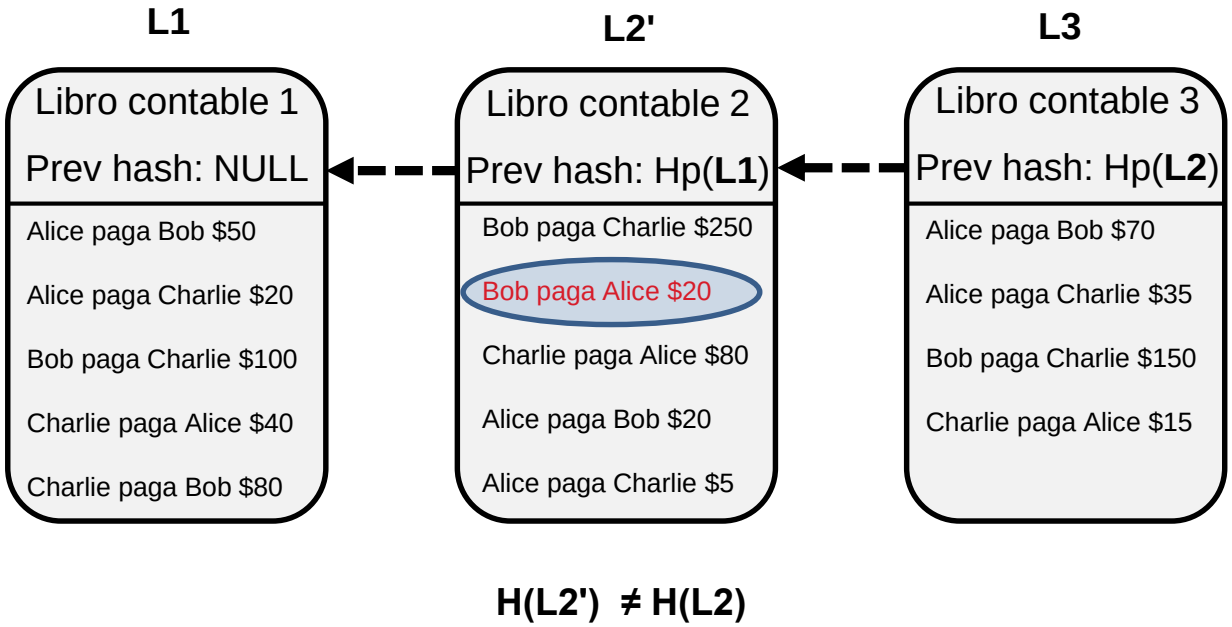


Inmutabilidad



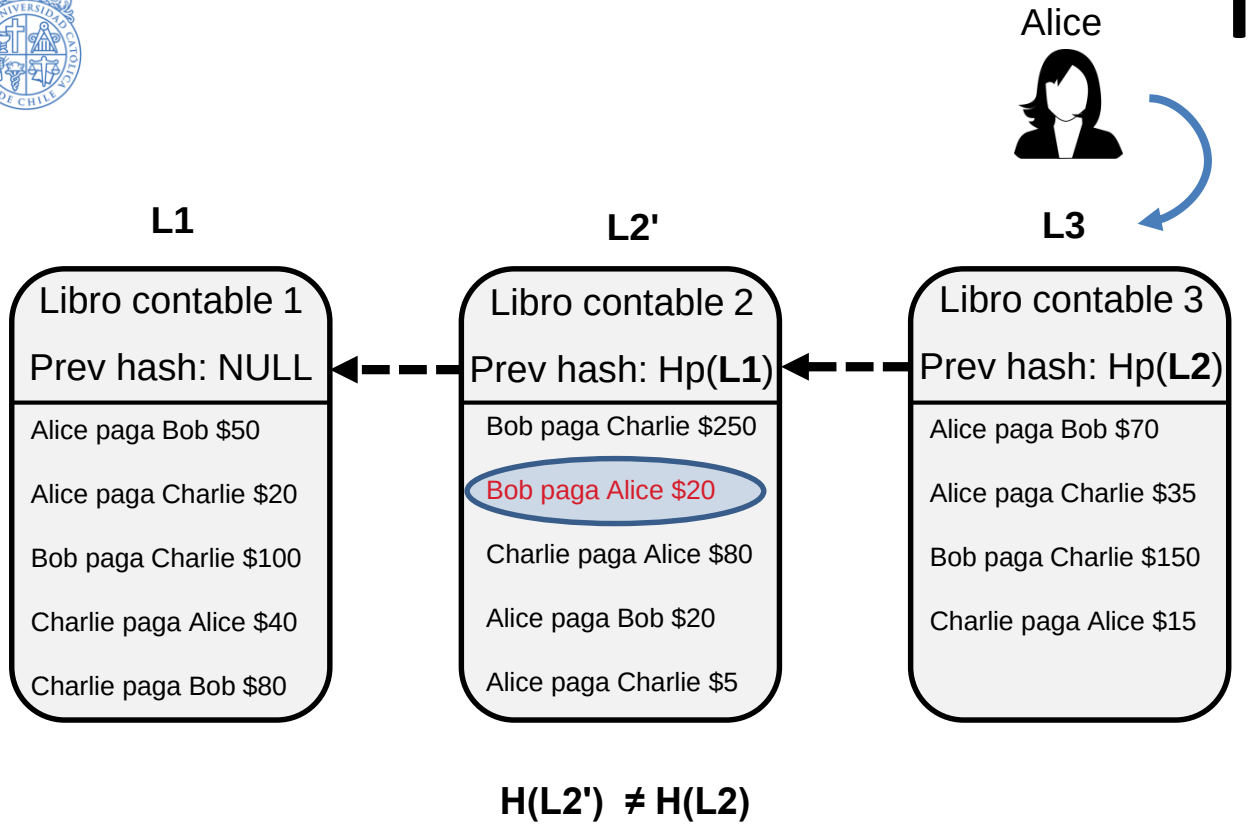
H(L2') ≠ H(L2)

Inmutabilidad



H(L2') ≠ H(L2)

Inmutabilidad



Inmutabilidad

Alice

L1

Libro contable 1

Prev hash: NULL

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

Charlie paga Alice $40

Charlie paga Bob $80

L2'

Libro contable 2

Prev hash: Hp(**L1**)

Bob paga Charlie $250

Bob paga Alice $20

Charlie paga Alice $80

Alice paga Bob $20

Alice paga Charlie $5

L3

Libro contable 3

Prev hash: Hp(**L2**)

Alice paga Bob $70

Alice paga Charlie $35

Bob paga Charlie $150

Charlie paga Alice $15

H(L2') ≠ H(L2)

Inmutabilidad

Alice

L1

Libro contable 1

Prev hash: NULL

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

Charlie paga Alice $40

Charlie paga Bob $80

L2'

Libro contable 2

Prev hash: Hp(**L1**)

Bob paga Charlie $250

Bob paga Alice $20

Charlie paga Alice $80

Alice paga Bob $20

Alice paga Charlie $5

L3

Libro contable 3

Prev hash: Hp(**L2**)

Alice paga Bob $70

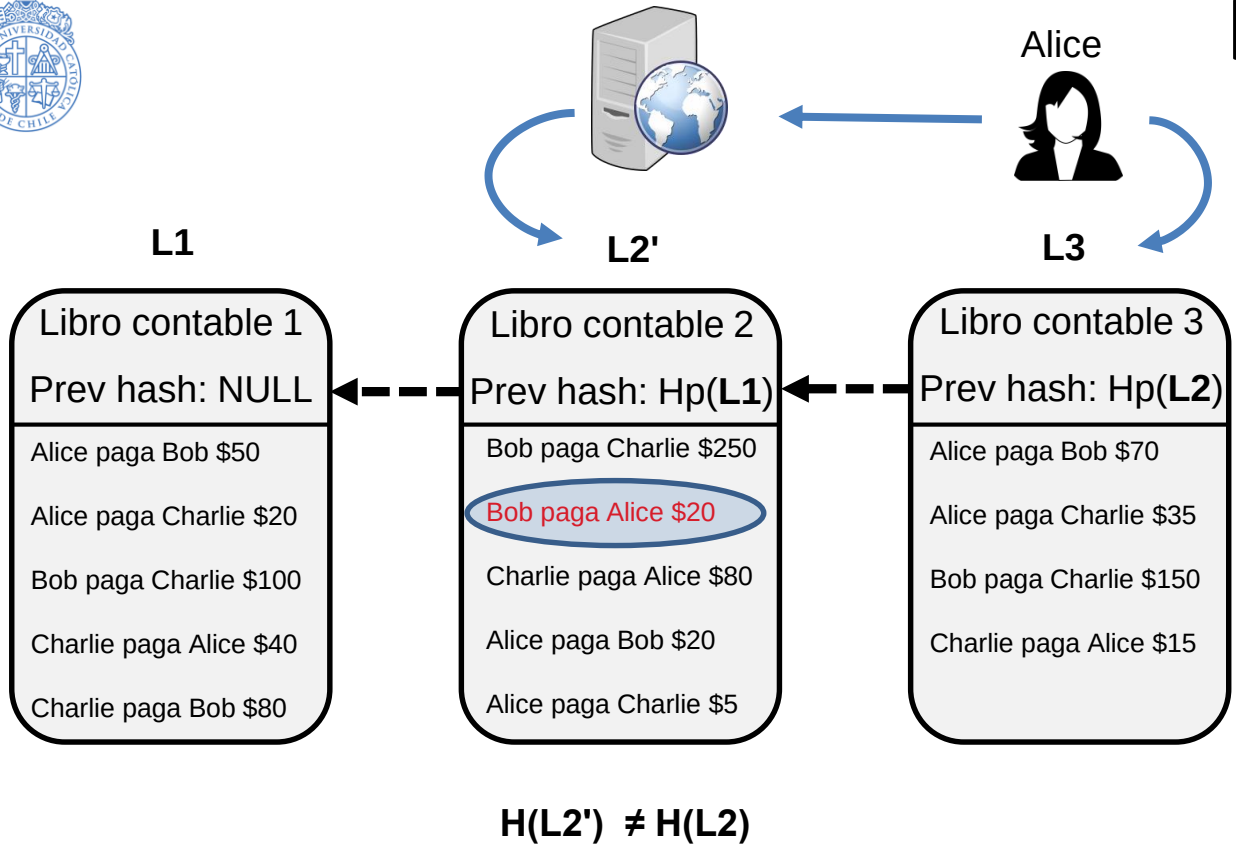
Alice paga Charlie $35

Bob paga Charlie $150

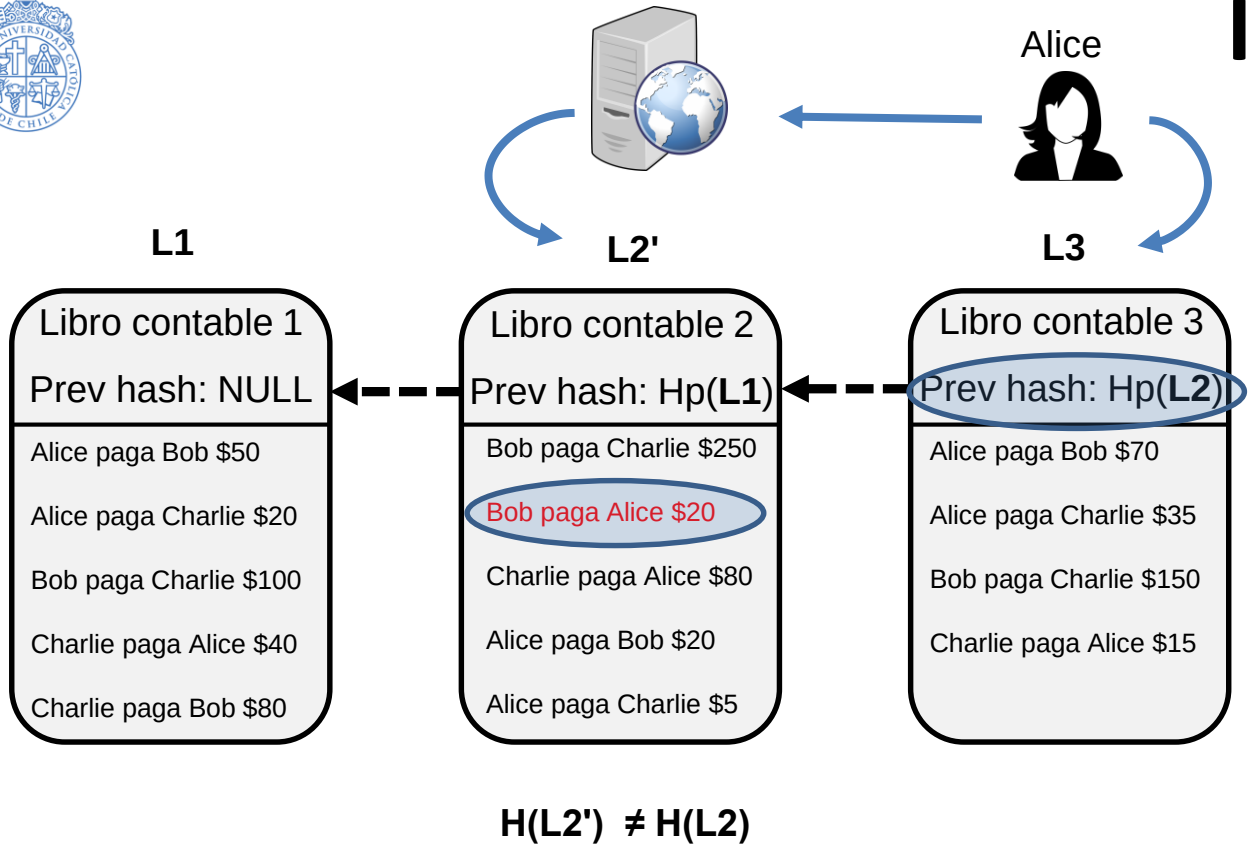
Charlie paga Alice $15

H(L2') ≠ H(L2)

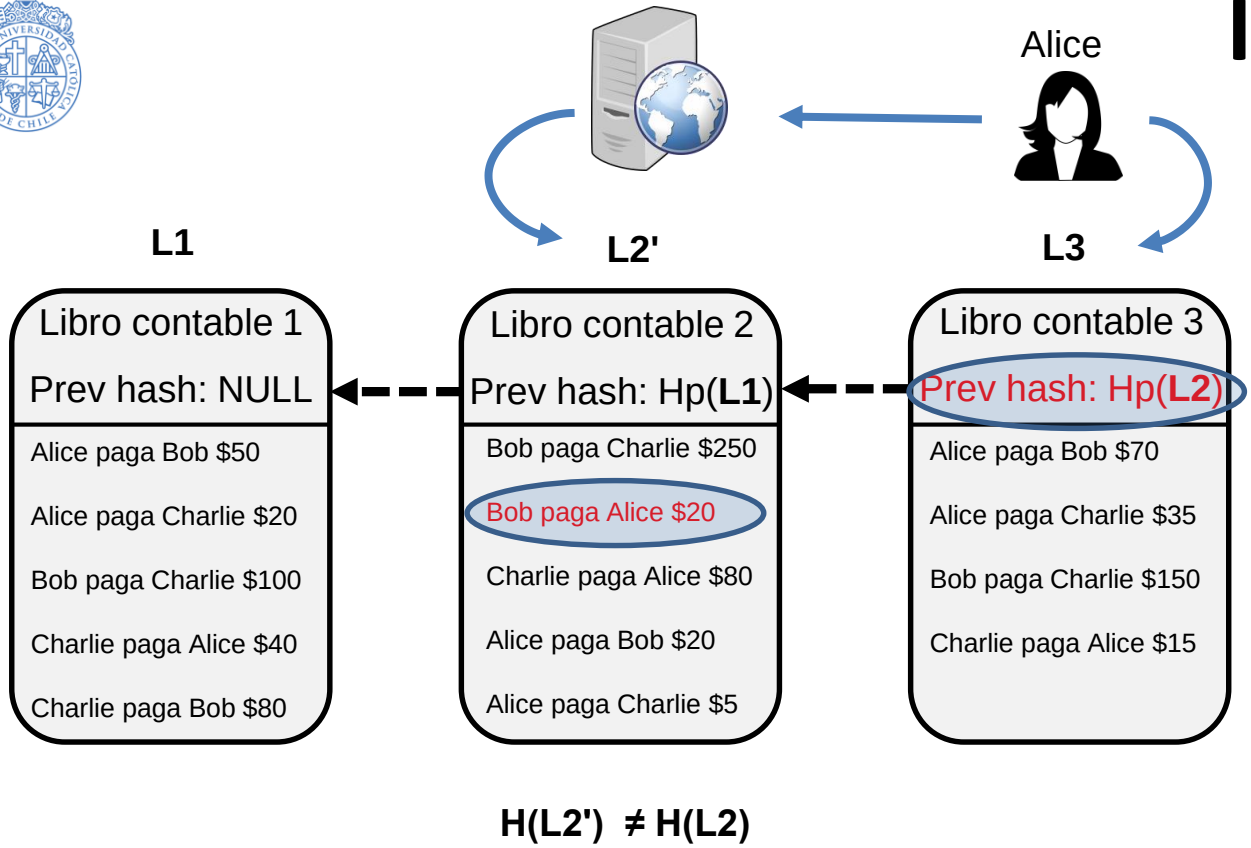
Inmutabilidad



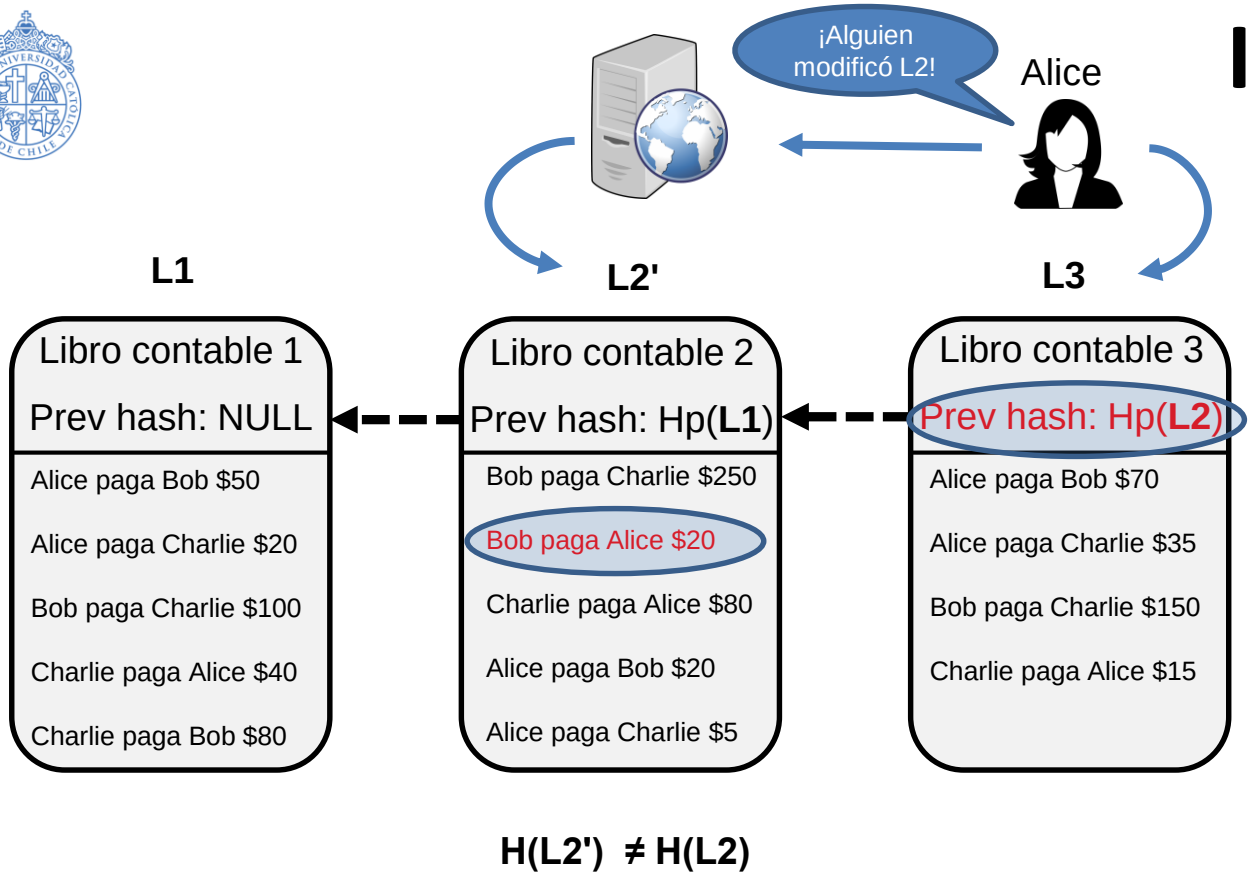
Inmutabilidad



Inmutabilidad

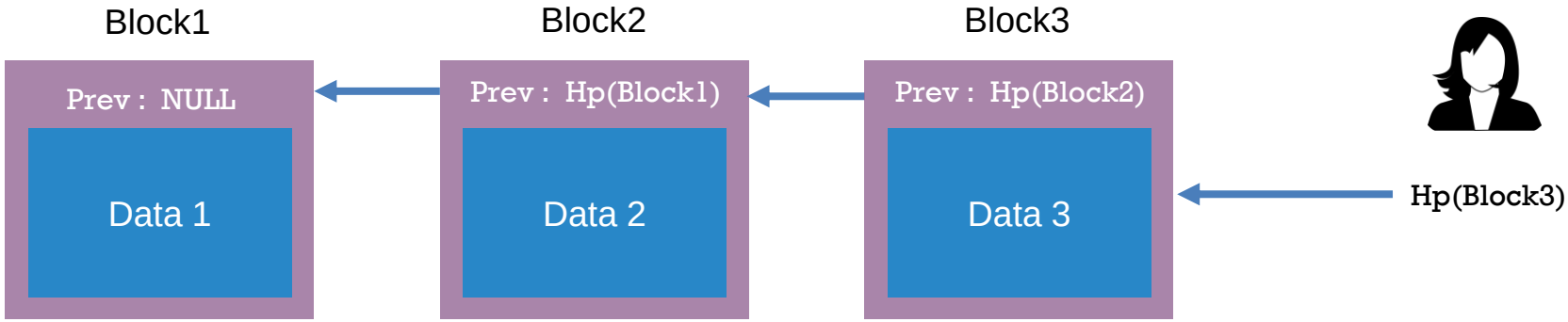


Inmutabilidad



Uso de Blockchain

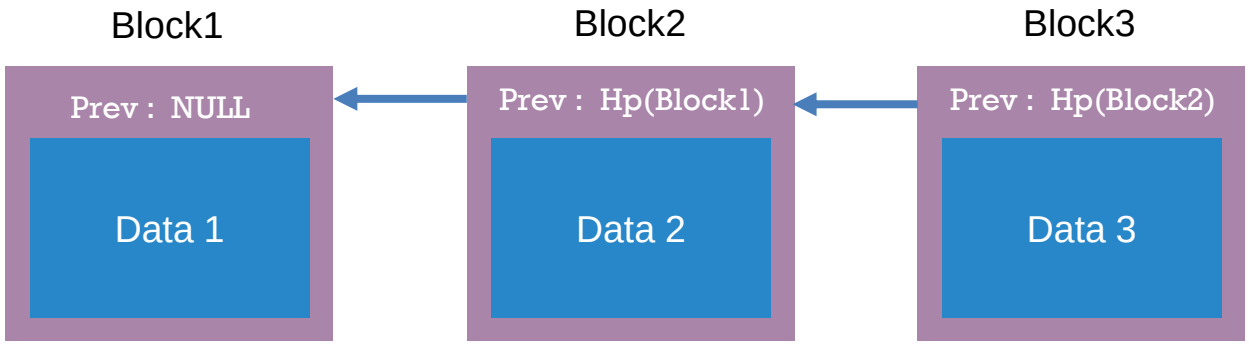
Como detectar donde ocurrió el cambio?



Si tenemos solo la cabeza

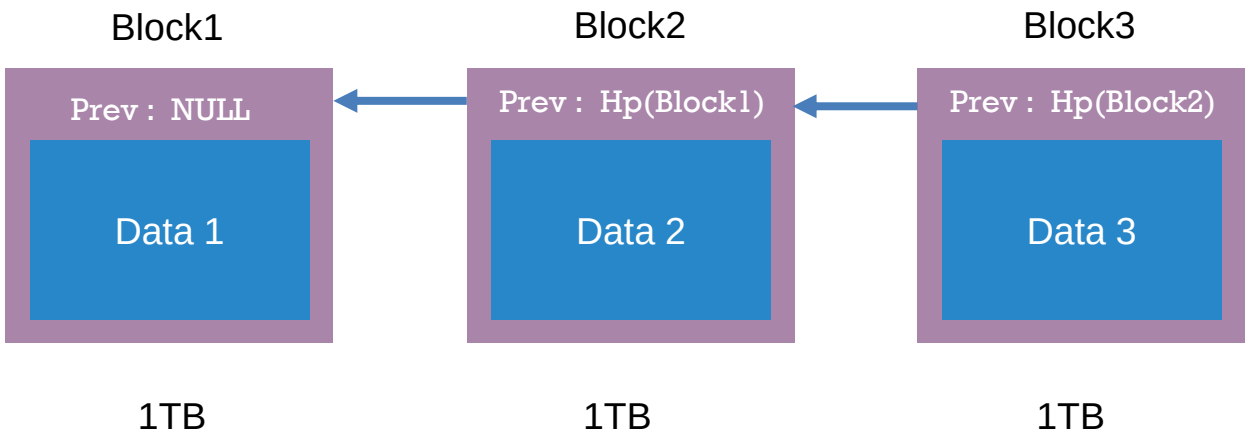
Uso de Blockchain

Como detectar donde ocurrió el cambio?



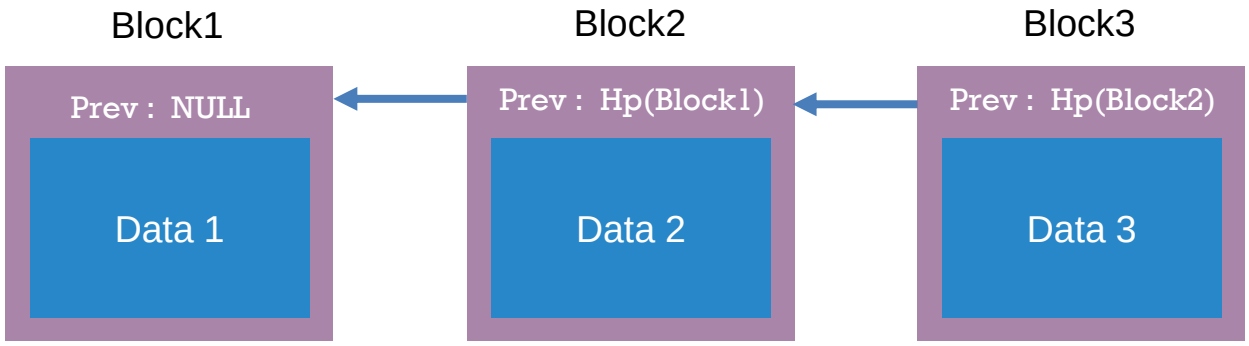
Uso de Blockchain

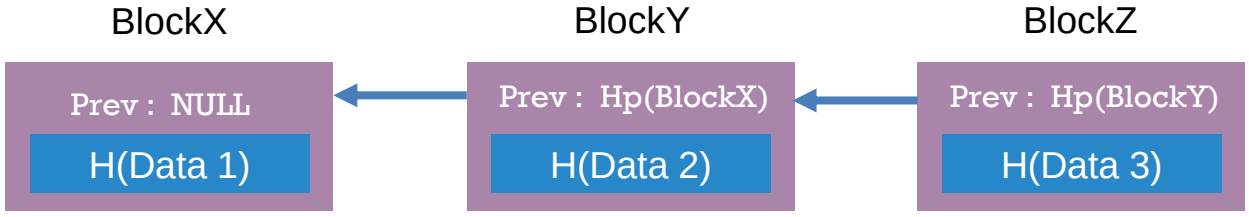
Como detectar donde ocurrió el cambio?



Uso de Blockchain

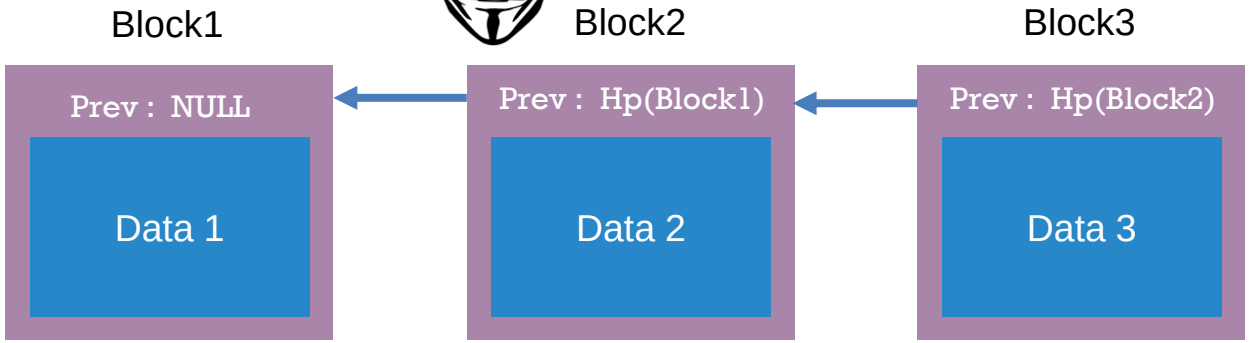
Como detectar donde ocurrió el cambio?

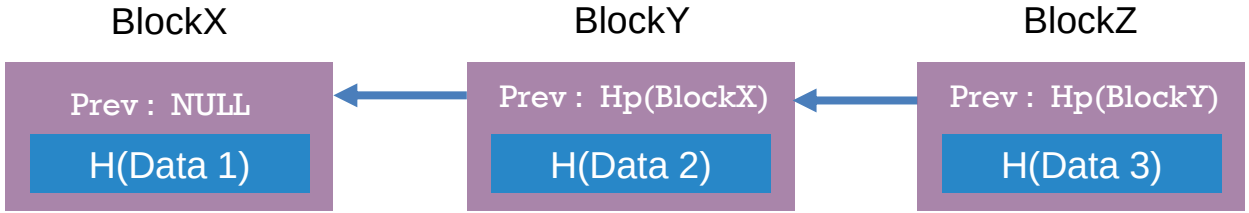




Uso de Blockchain

Como detectar donde ocurrió el cambio?





Uso de Blockchain

Como detectar donde ocurrió el cambio?

Block1

Prev : NULL

Data 1

Block2

Prev : Hp(Block1)

Fake Data 2

Block3

Prev : Hp(Block2)

Data 3

BlockX

Prev : NULL

H(Data 1)

BlockY

Prev : Hp(BlockX)

H(Data 2)

BlockZ

Prev : Hp(BlockY)

H(Data 3)

Uso de Blockchain

Como detectar donde ocurrió el cambio?

Block1

Prev : NULL

Data 1

Block2

Prev : Hp(Block1)

Fake Data 2

Block3

Prev : Hp(Block2)

Data 3

BlockX

Prev : NULL

H(Data 1)

BlockY

Prev : Hp(BlockX)

H(Data 2)

BlockZ

Prev : Hp(BlockY)

H(Data 3)

Blockchain y commitments

Blockchain y commitments

Day1

Data Alice

Data Bob

Blockchain y commitments

Day1

Data 1

Data Alice

Data Bob

Blockchain y commitments

Day1

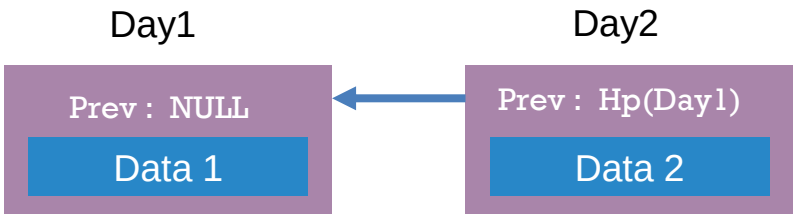
Prev : NULL

Data 1

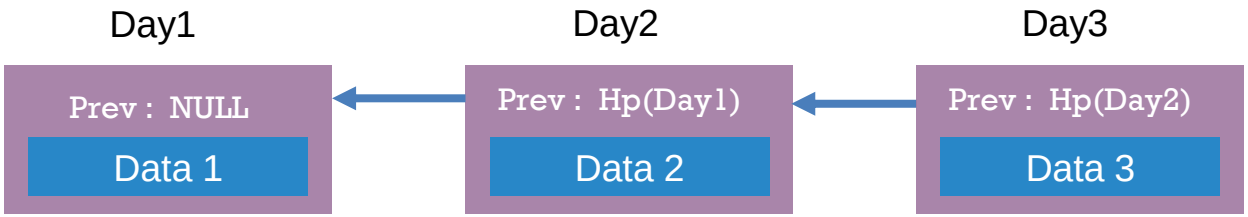
Data Alice

Data Bob

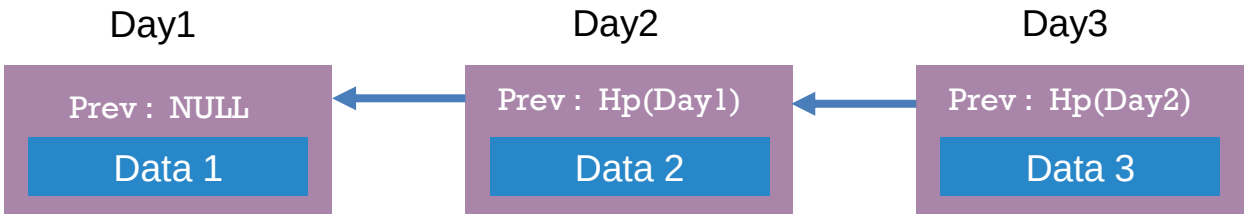
Blockchain y commitments

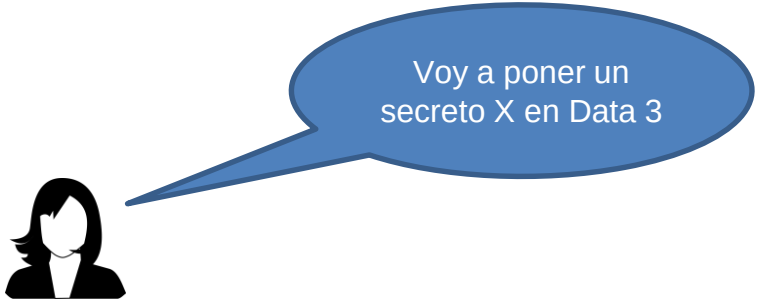


Blockchain y commitments

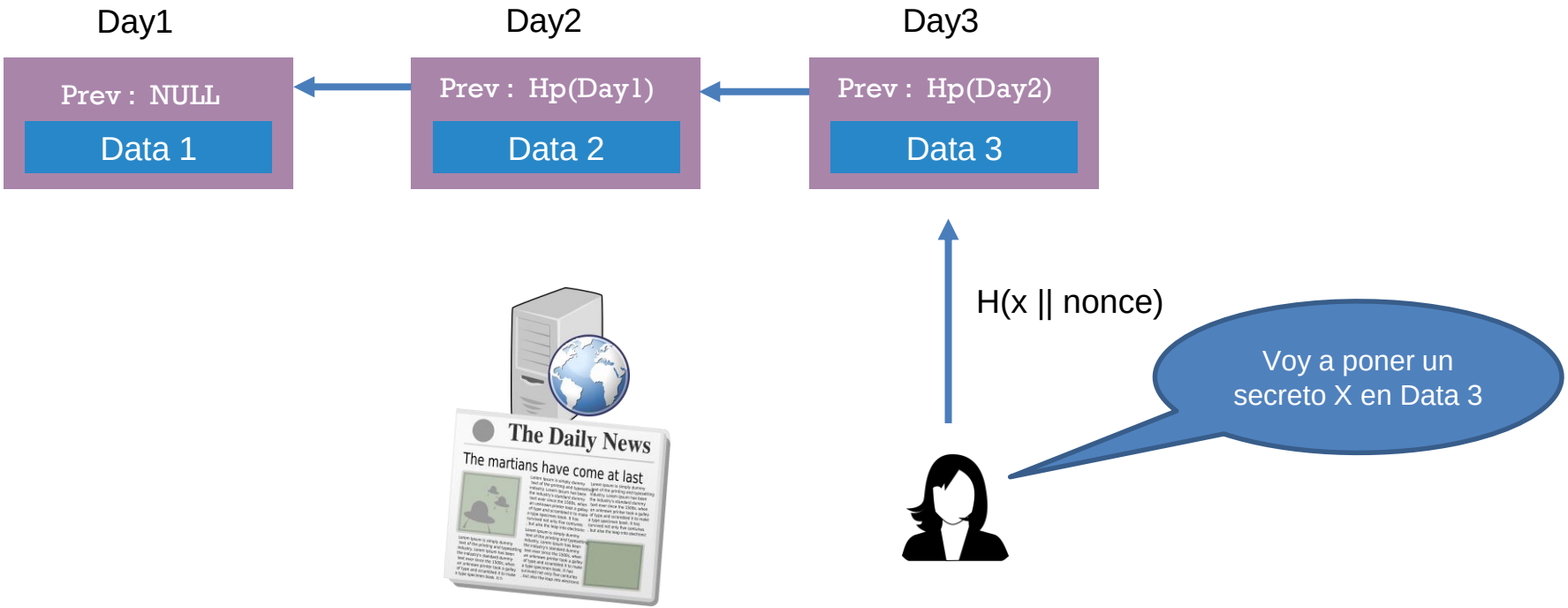


Blockchain y commitments

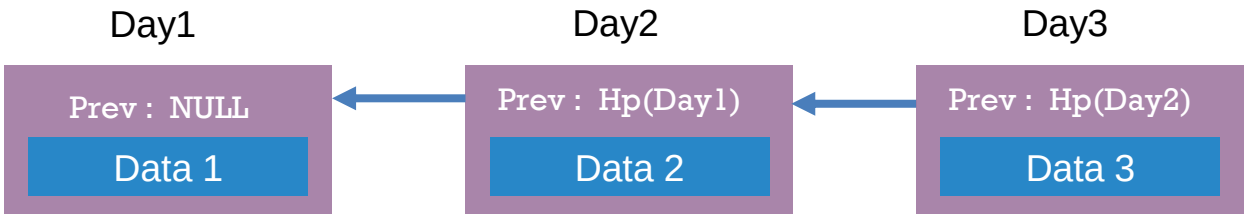




Blockchain y commitments



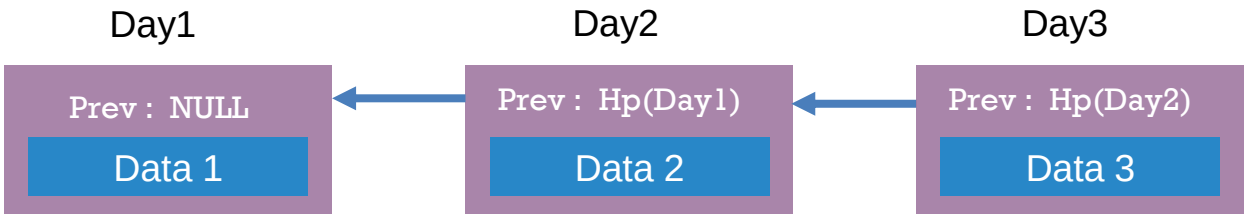
Blockchain y commitments



H(x || nonce)

El día 183 voy a mostrar que ya conocía X el día 3

Blockchain y commitments

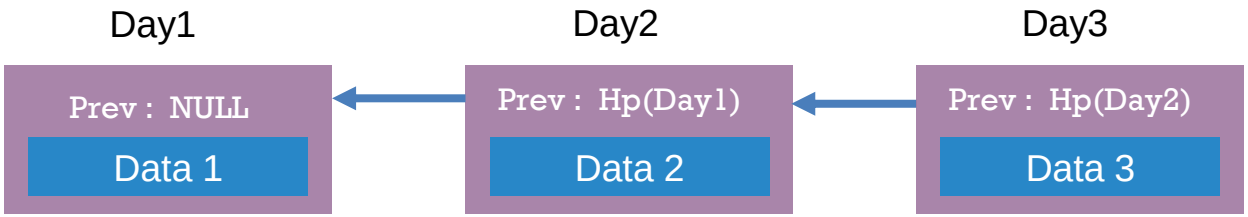


H(x || nonce)

Día 183 Alice publica:

x, nonce

Blockchain y commitments

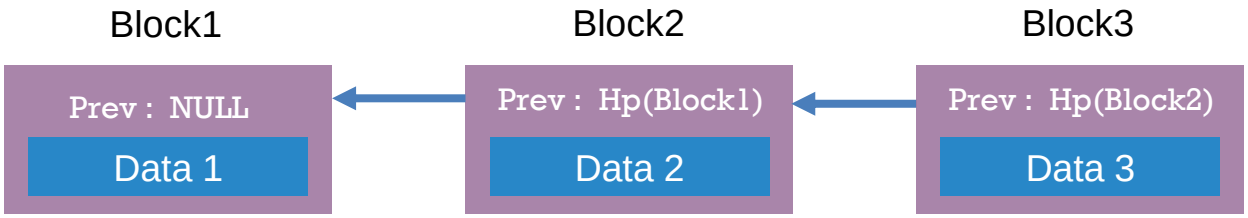


H(x || nonce)

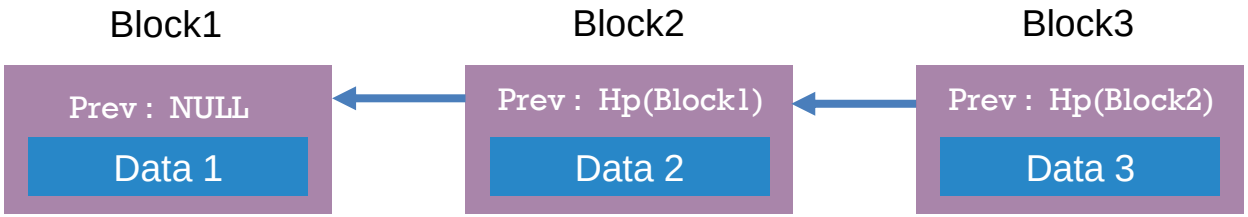
Ejemplos de x:

1) Schema de un patente
2) Codigo de Bob
3) …

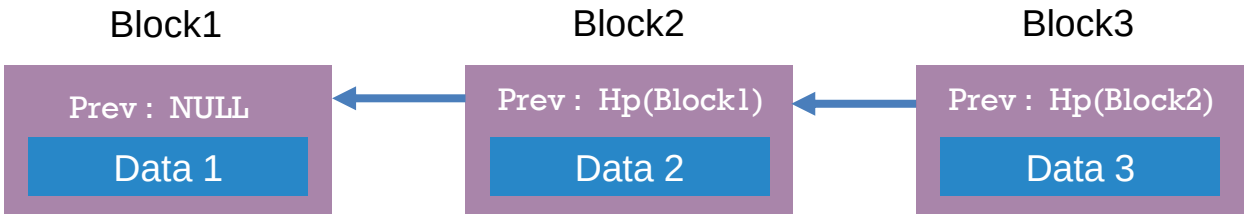
Una debilidad



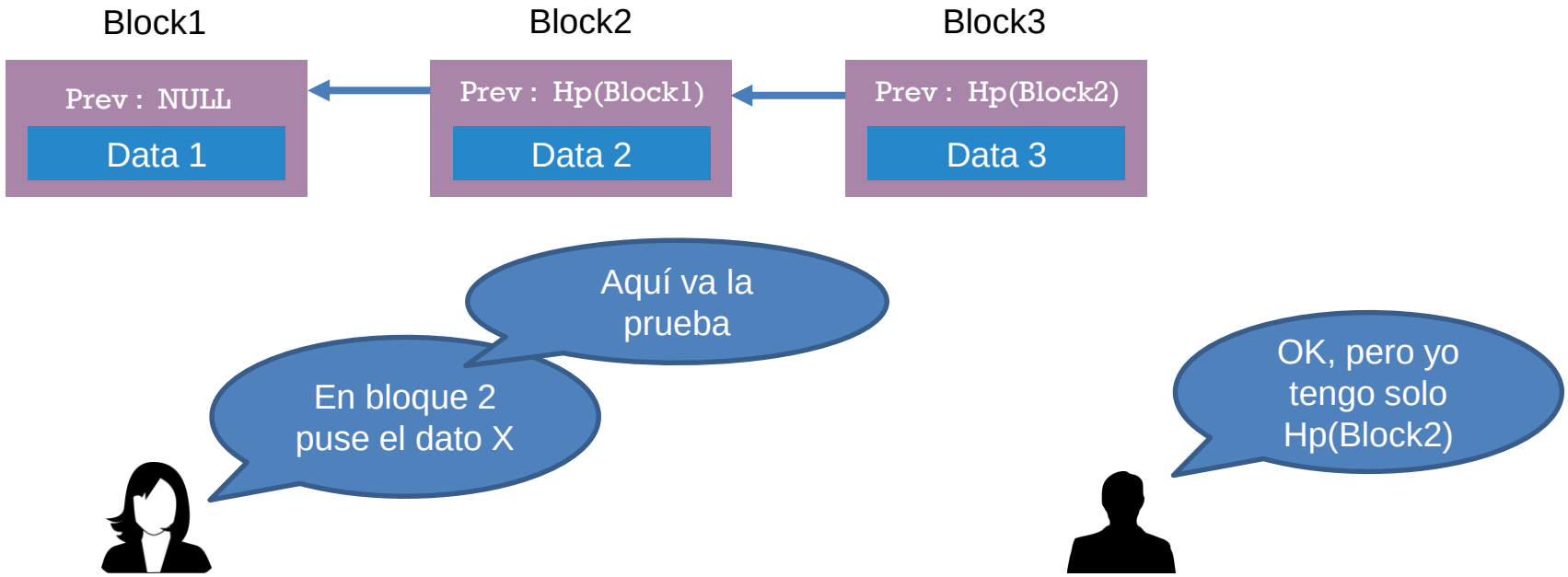
Una debilidad



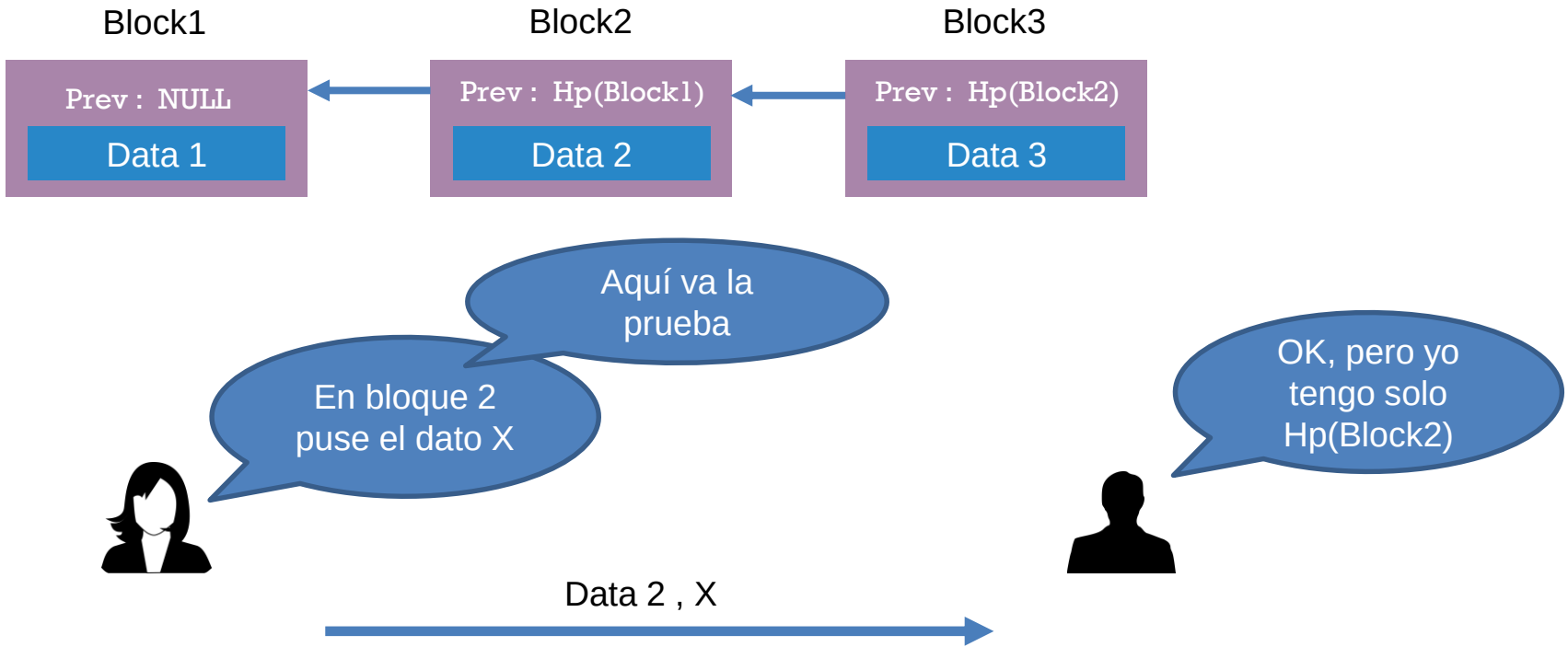
Una debilidad



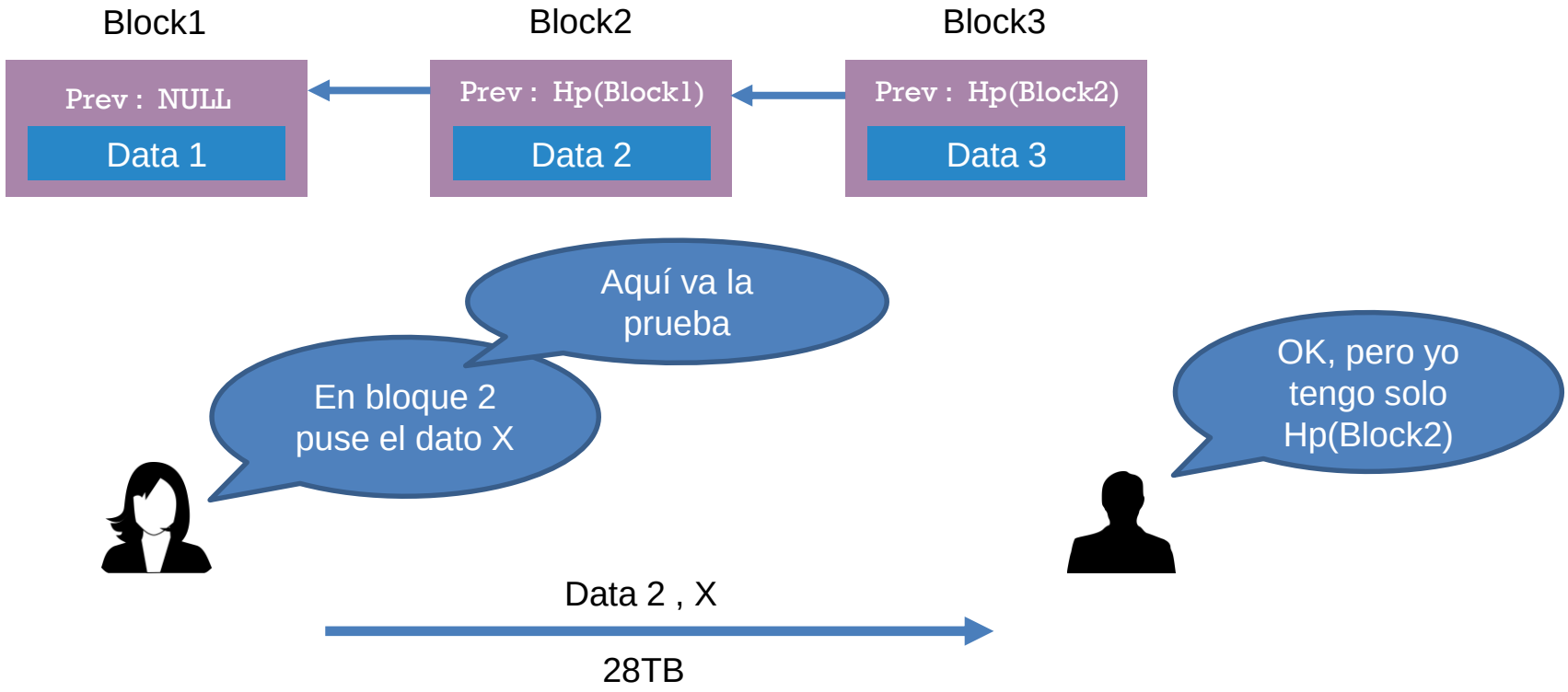
Una debilidad



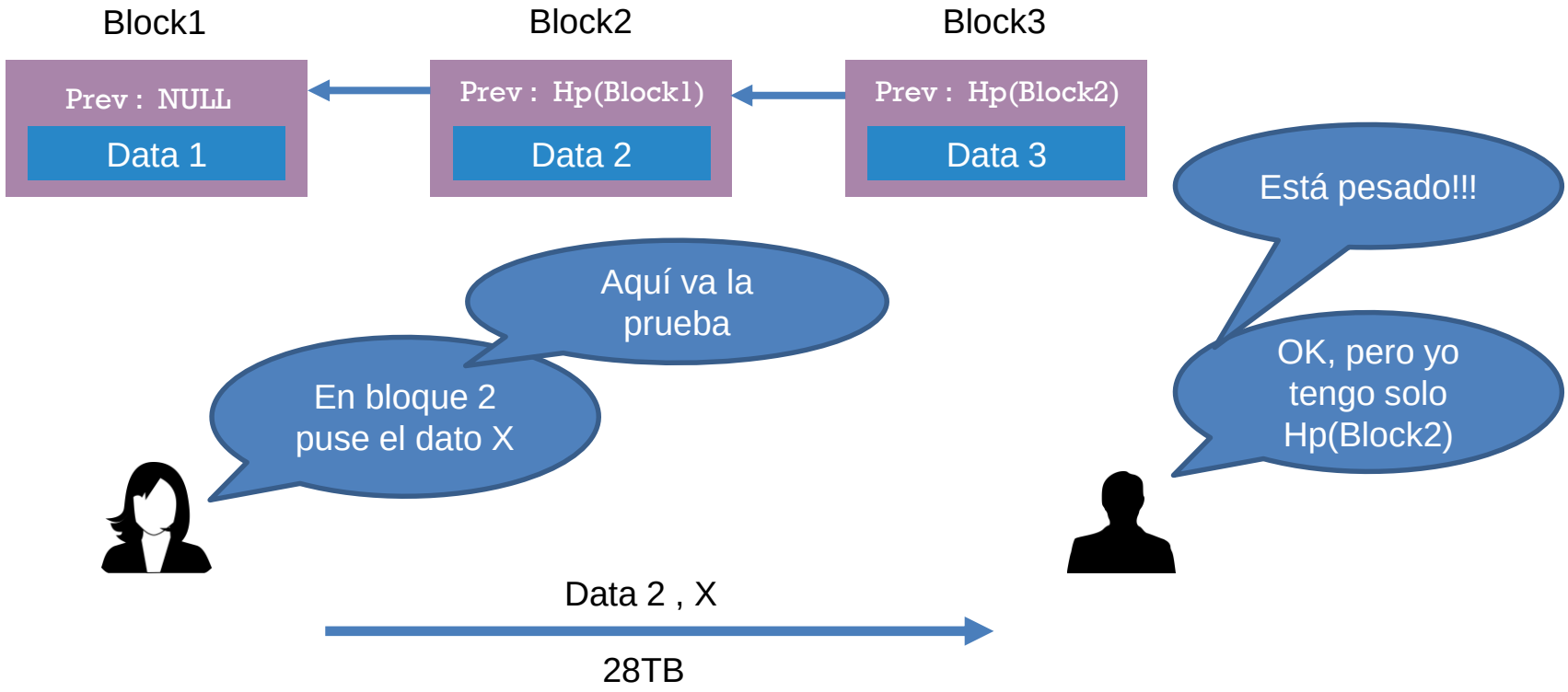
Una debilidad



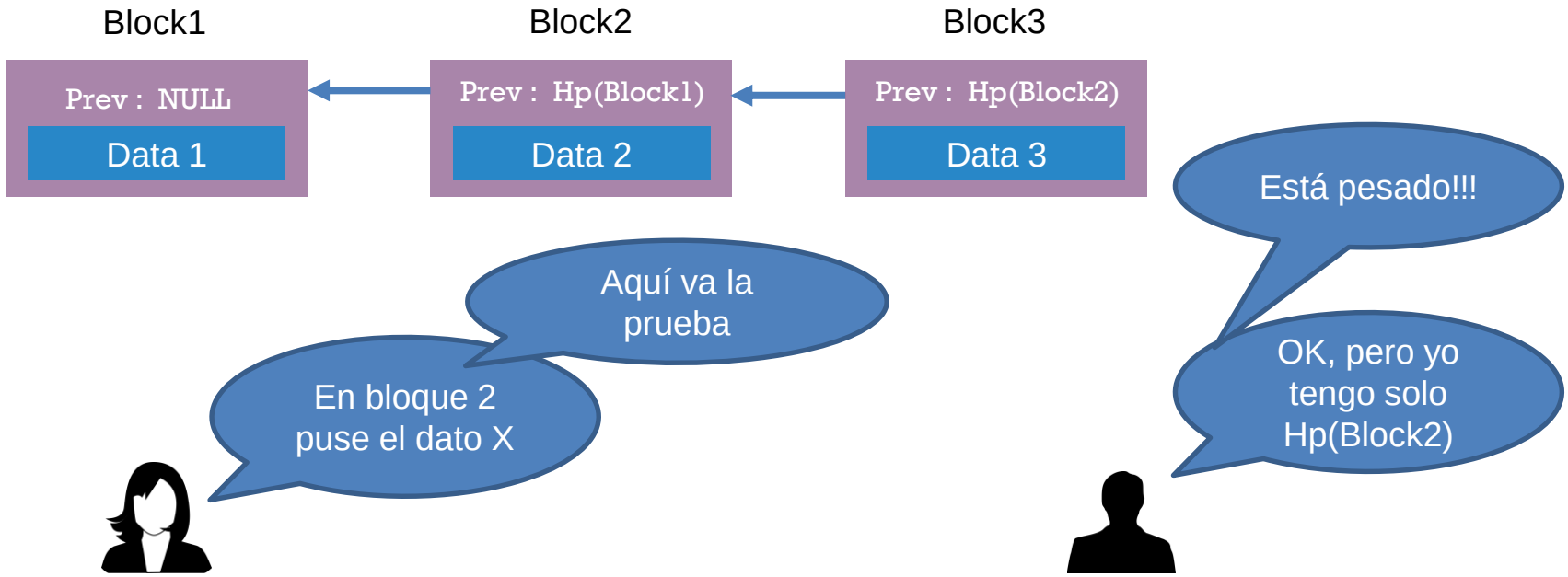
Una debilidad



Una debilidad



Una debilidad



Como hacer la prueba más eficiente???

Lectura

Materiale proveniente de Narayanan et. Al:

- Capitulo 1.2
- Capitulo 9.1

Practice time!!!

Ejercicios!!!

- Implementar blockchain
- Correr contra datos de prueba
- Maneras de implementar

Discutir los métodos de las dos clases en pizarra!!!

Referencias

Todas las imagenes de esta clase eran recuperadas en:

https://pixabay.com/