Identidad digital

¿Cómo funciona Bitcoin?

Contenidos

- ¿Cómo establecer identidad digital?

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Charlie

Libro contable

Alice paga Bob $50

Alice paga Charlie $20

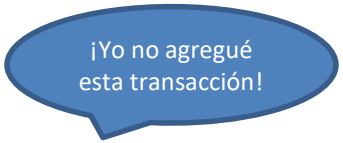
Bob paga Charlie $100

¿ Fue Alice quién me mandó los fondos?

Bob

Problema 2 de ePeso

¿Quién agrega las transacciones?



Alice

Libro contable

Alice paga Bob $50

Alice paga Charlie $20

Bob paga Charlie $100

Alice paga Bob $10000

Bob

Charlie

Identidad en el mundo digital

Alice

Bob

Identidad en el mundo digital

Alice

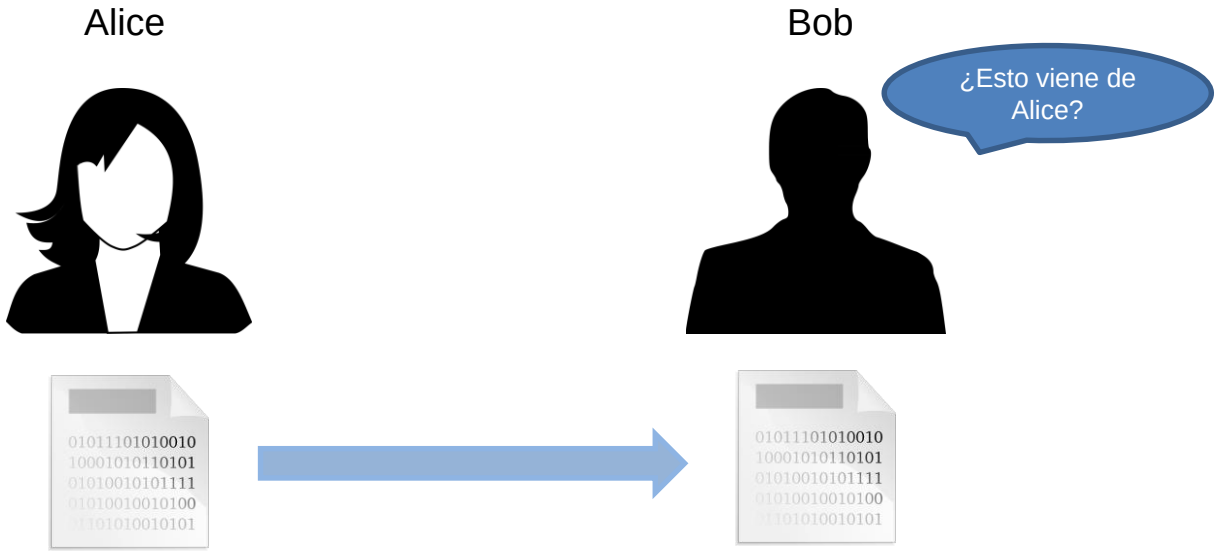
Bob

Identidad en el mundo digital

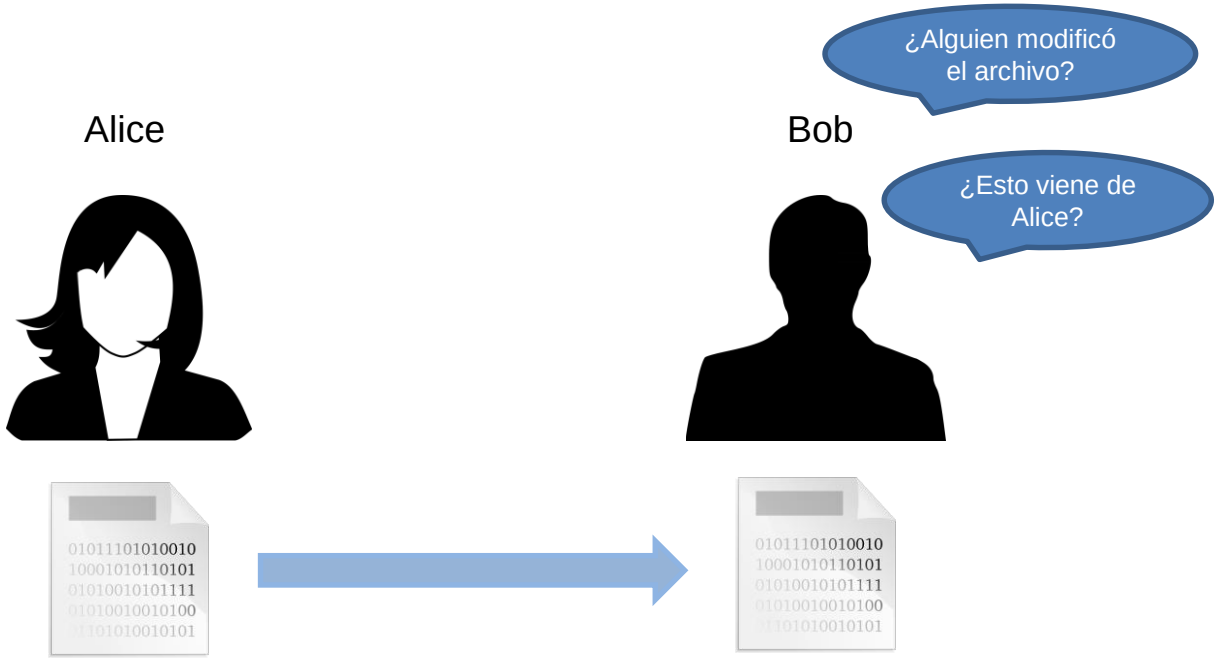
Alice

Bob

Identidad en el mundo digital



Identidad en el mundo digital



Solución en el mundo físico

Alice

Bob

Solución en el mundo físico

Alice

Alice

Bob

Solución en el mundo físico

Alice

Alice

Bob

Solución en el mundo físico

Alice

Bob

Alice

Solución digital insuficiente

Alice

Bob

Alice

Solución digital insuficiente

Alice

Alice = 110101

Bob

Solución digital insuficiente

Alice

Bob

Alice = 110101

Solución digital insuficiente

Alice

Bob

Alice = 110101

Solución digital insuficiente

Alice *Alice* = 110101

Bob

Charlie

Solución digital insuficiente

Alice

Alice = 110101

Bob

Charlie

Solución digital insuficiente

Alice

Alice = 110101

Bob

Charlie

Solución digital insuficiente

Alice *Alice* = 110101

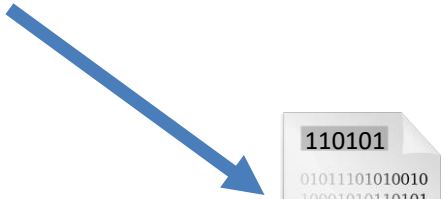
Bob

Charlie

Solución digital insuficiente

Alice

Alice = 110101



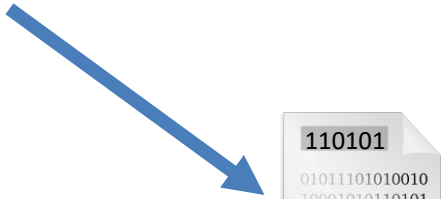
Bob

Charlie

Solución digital insuficiente

Alice

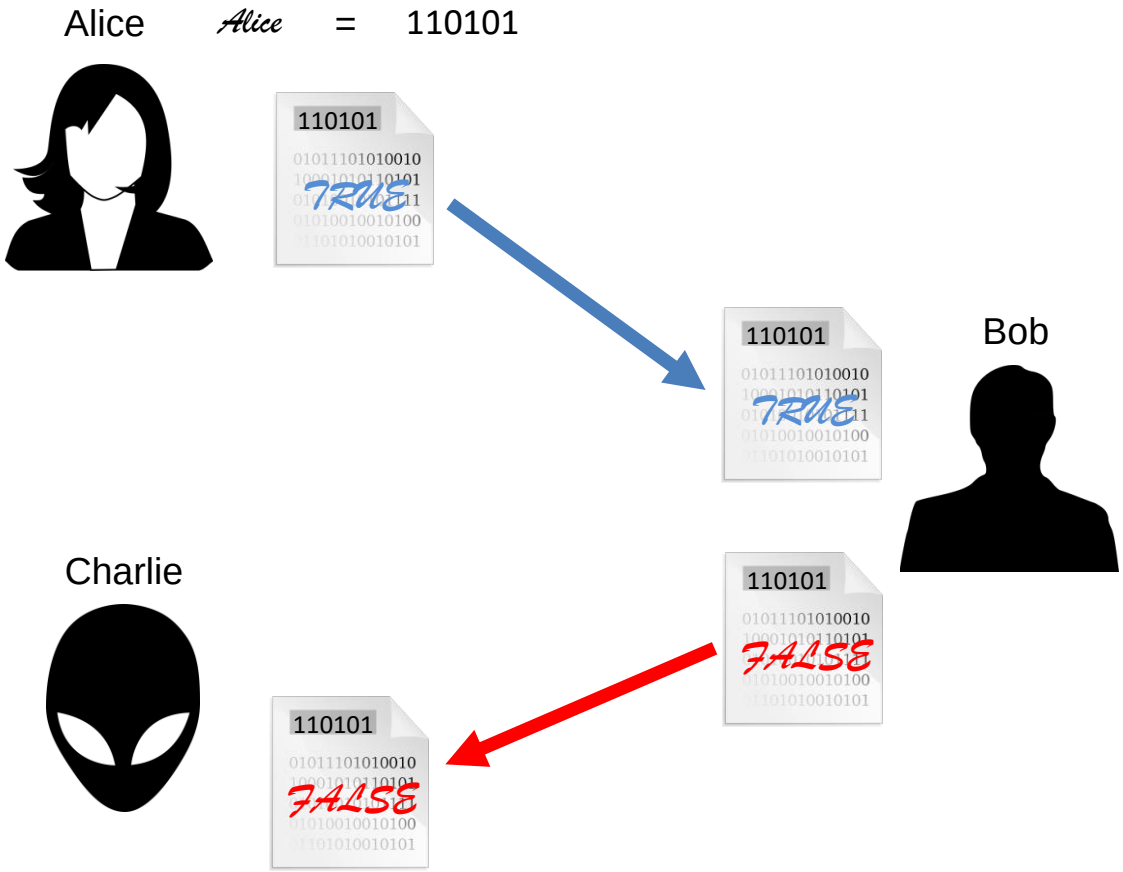
Alice = 110101



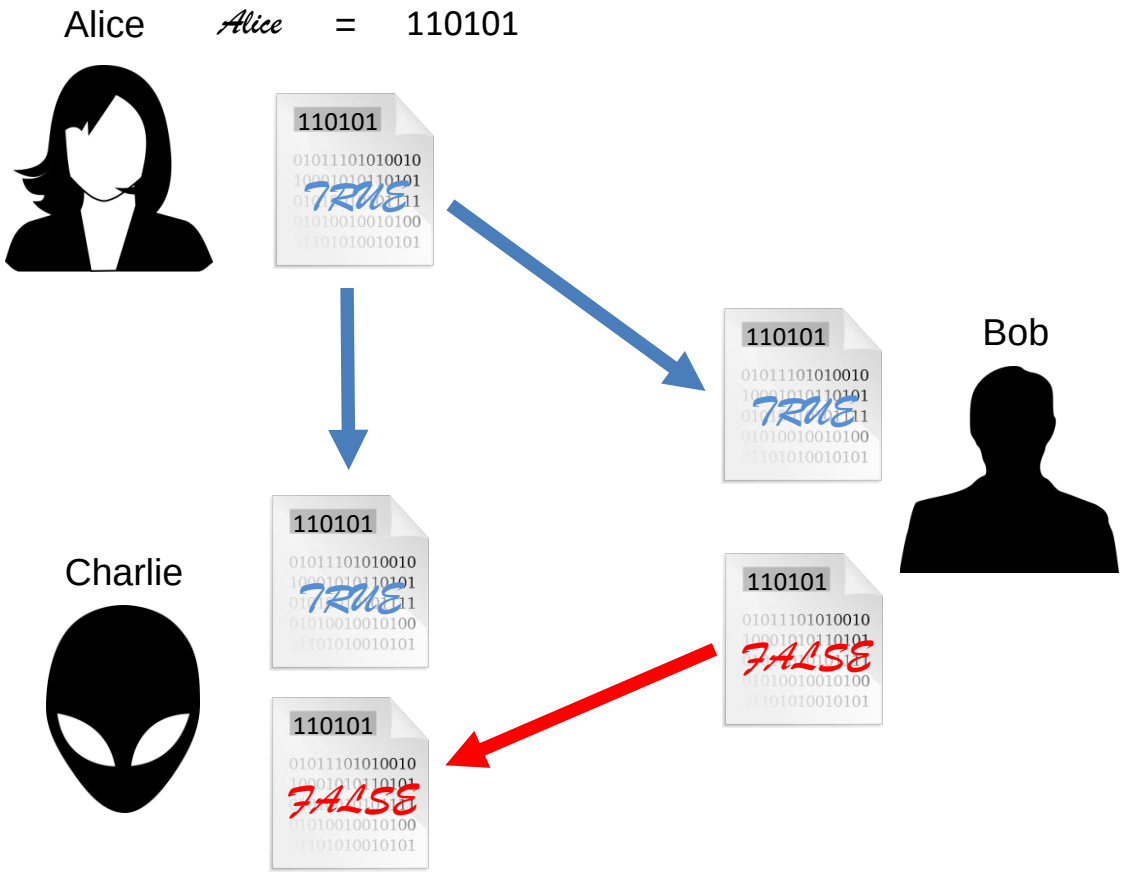
Bob

Charlie

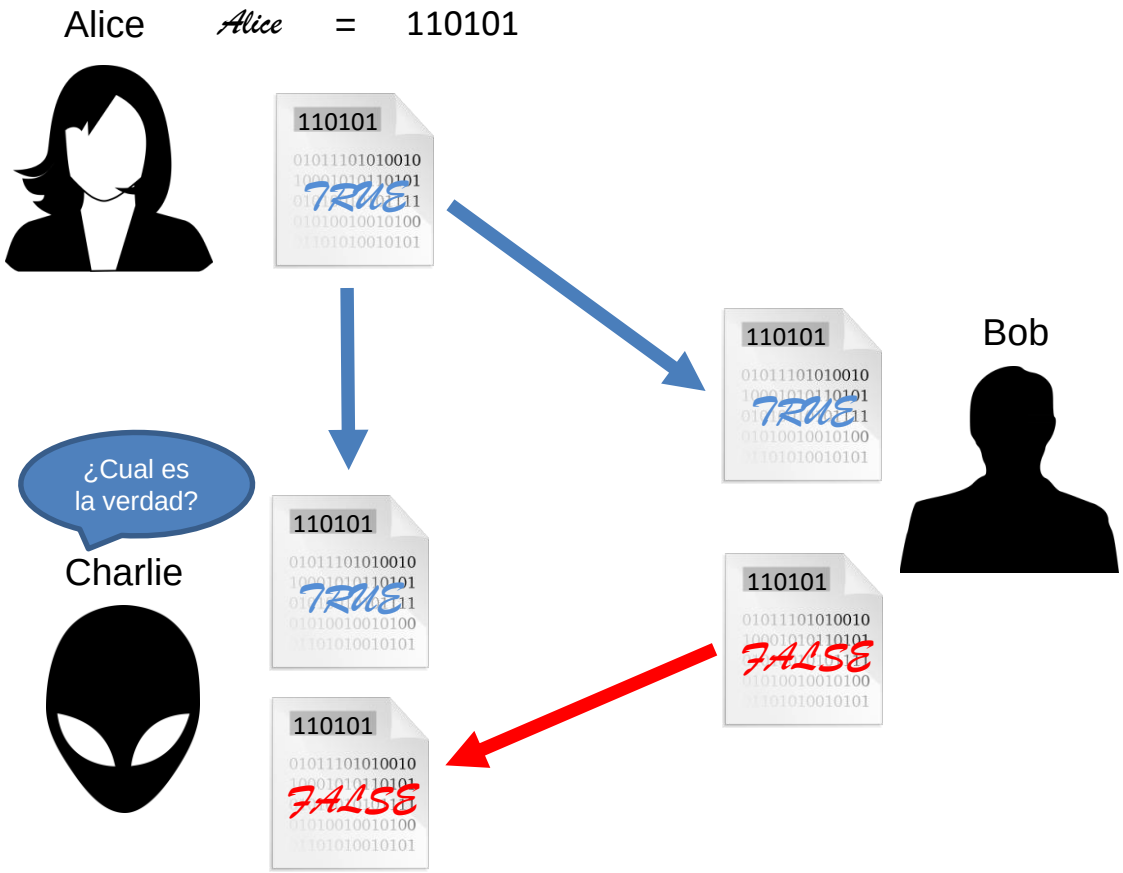
Solución digital insuficiente



Solución digital insuficiente



Solución digital insuficiente



Firmas digitales

Segunda primitiva criptográfica

Protocolo de firmas digitales:

- Sólo Alice puede firmar sus documentos
- Cada documento tiene una firma distinta
- Todos pueden confirmar que Alice firmó el documento

Firmas digitales

Segunda primitiva criptográfica

Protocolo de firmas digitales:

- Sólo Alice puede firmar sus documentos
- Cada documento tiene una firma distinta
- Todos pueden confirmar que Alice firmó el documento

Consiste de tres algoritmos:

1. Algoritmo de generación de llaves secretas y públicas
2. Algoritmo de firma de un documento
3. Algoritmo de verificar la firma de un documento

Firmas digitales

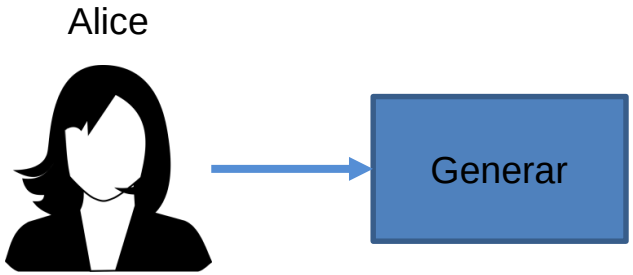
Generación de llaves

Alice

Generar

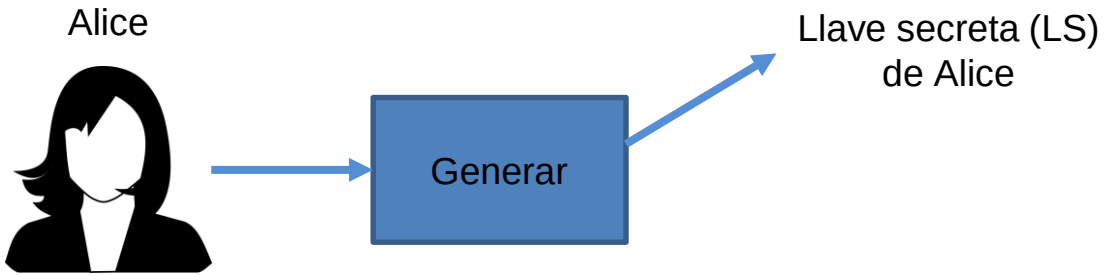
Firmas digitales

Generación de llaves



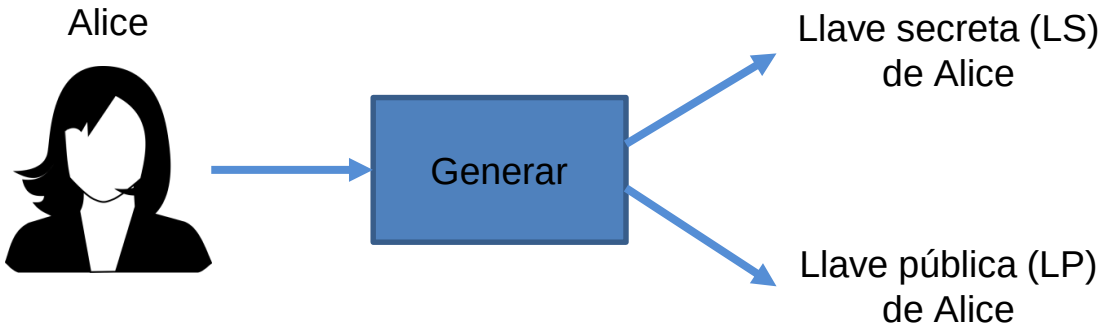
Firmas digitales

Generación de llaves



Firmas digitales

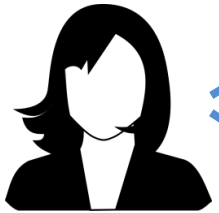
Generación de llaves



Firmas digitales

La llave secreta y la llave publica

Alice



Llave secreta (LS) de Alice = Un secreto de Alice!

Llave pública (LP) de Alice = Información pública

Identidad digital de Alice

Firmas digitales

Firma de un documento

Alice (LS,LP)

Firmas digitales

Firma de un documento

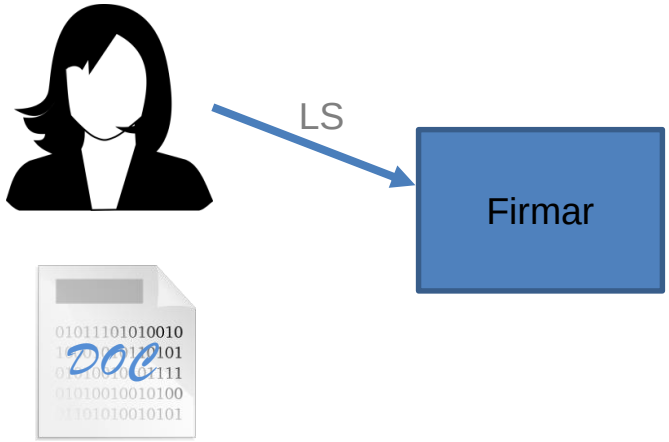
Alice (LS,LP)

Firmar

Firmas digitales

Firma de un documento

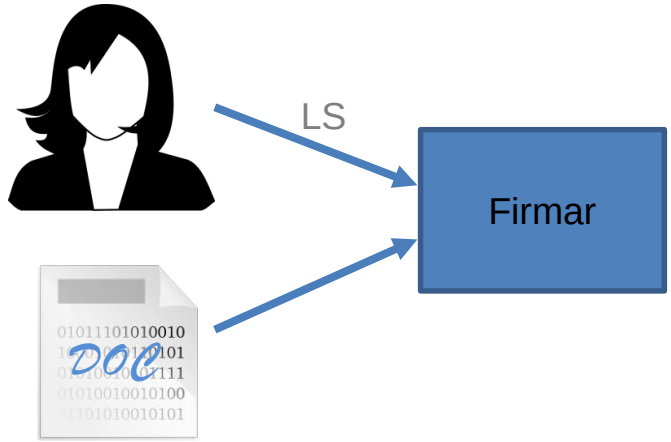
Alice (LS,LP)



Firmas digitales

Firma de un documento

Alice (LS,LP)



Firmas digitales

Firma de un documento

Alice (LS,LP)

LS

Firmar

F = firma del documento 

correspondiente a la
llave pública LP

(firma de Alice)

Firmas digitales

Verificación de firmas digitales

Alice (LS,LP)

Bob

LP

Firmas digitales

Verificación de firmas digitales

Alice (LS,LP)

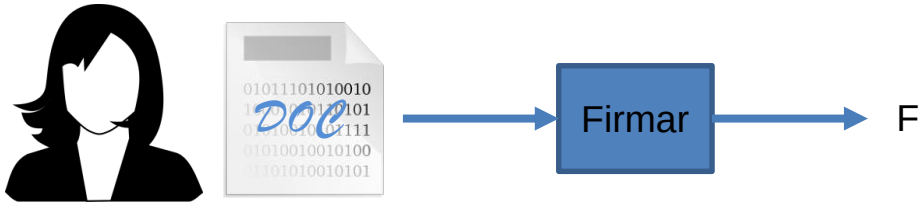
Bob

LP

Firmas digitales

Verificación de firmas digitales

Alice (LS,LP)

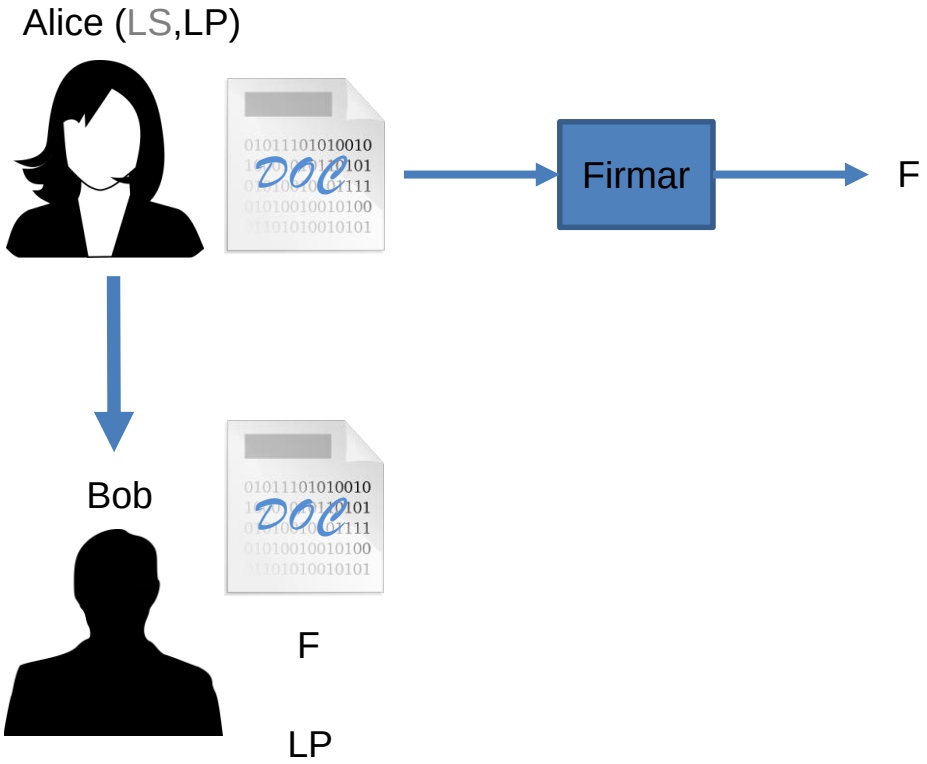


Bob

LP

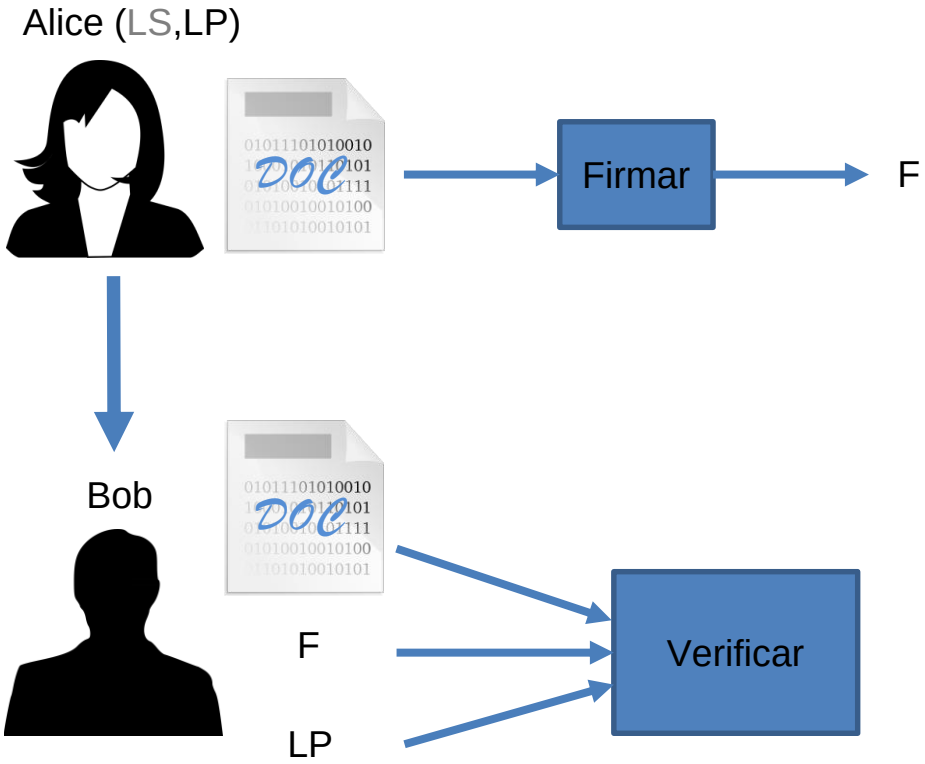
Firmas digitales

Verificación de firmas digitales



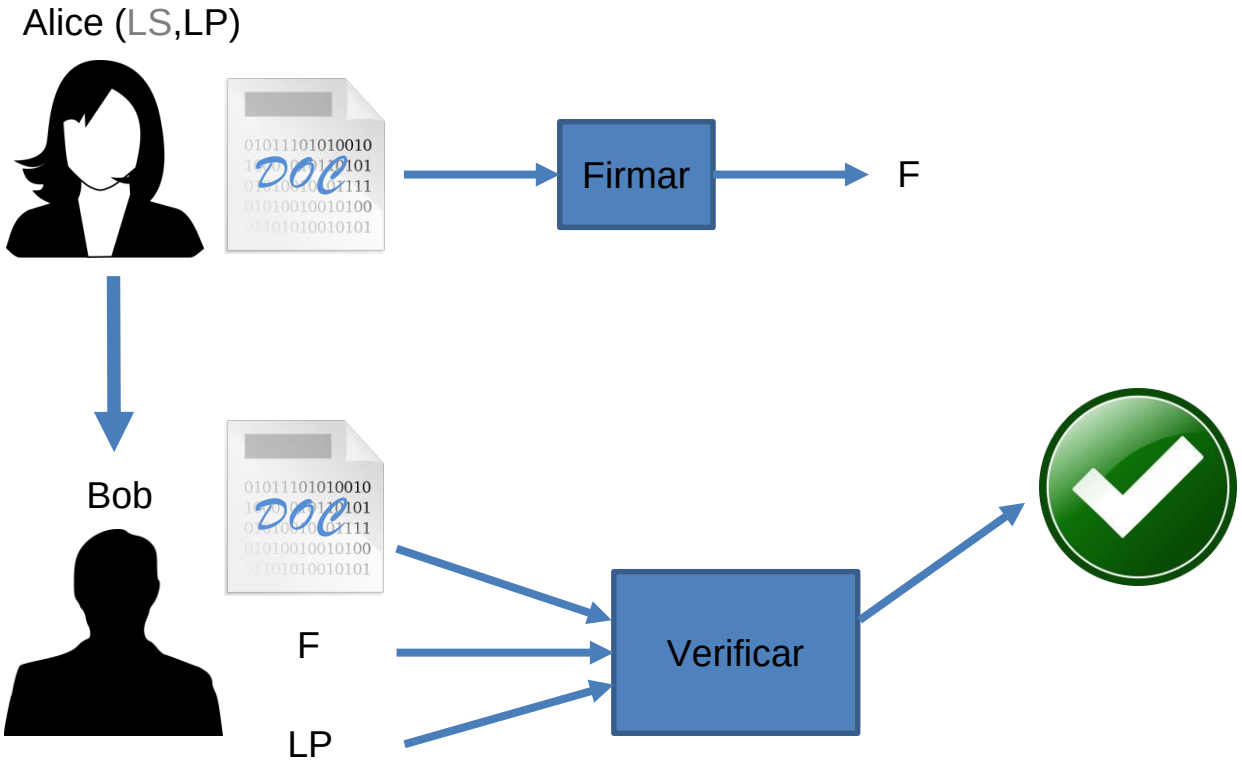
Firmas digitales

Verificación de firmas digitales



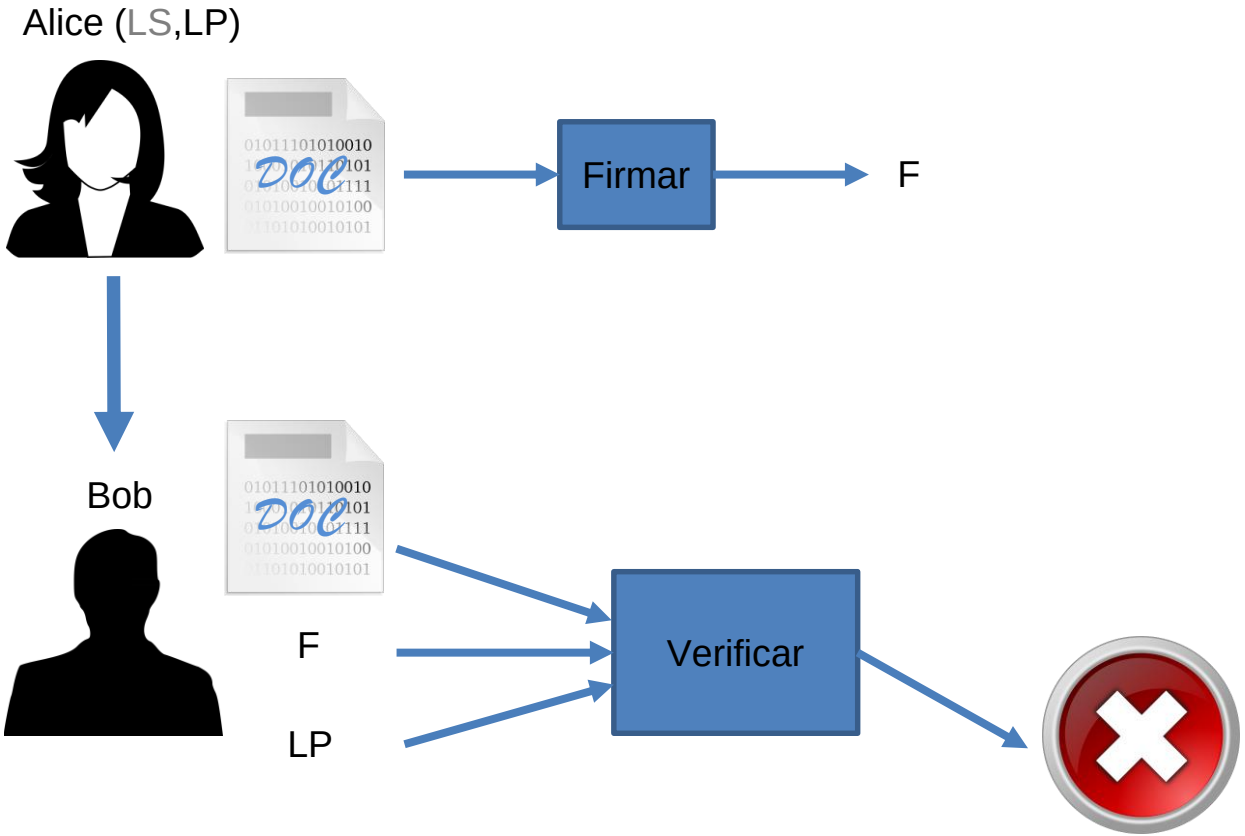
Firmas digitales

Verificación de firmas digitales



Firmas digitales

Verificación de firmas digitales



Propiedades de firmas digitales

- Los tres algoritmos son seguros:
  Imposible reconstruir LS conociendo LP
  Imposible reconstruir LS conociendo mensajes firmadas

- Firmas son infalsificables y únicas:
  Firma se puede realizar solo con LS
  Cuando cambia el documento cambia la firma

Propiedades de firmas digitales

Imposible reconstruir LS conociendo LP

Alice

(LS,LP)

Bob

LP

Propiedades de firmas digitales

Imposible reconstruir LS conociendo LP

Alice

(LS,LP)

Bob

LP

LS

Propiedades de firmas digitales

Imposible reconstruir LS conociendo mensajes de LP

Alice

(LS,LP)

Bob

LP

Propiedades de firmas digitales

Imposible reconstruir LS conociendo mensajes de LP

Alice

(LS,LP)

F1

F2

.
.
.

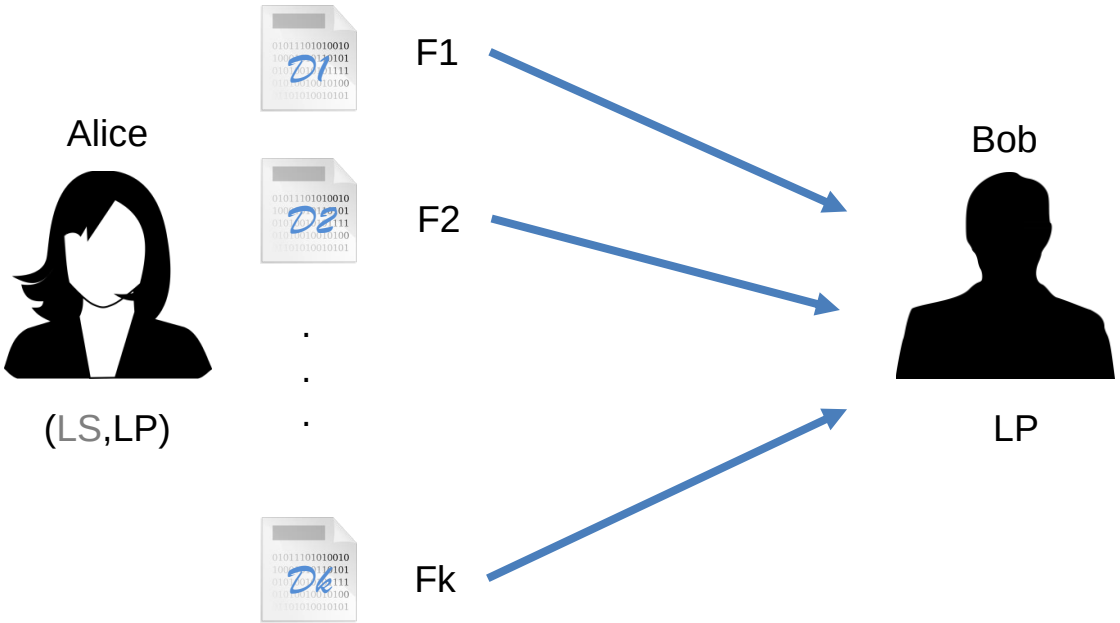
Fk

Bob

LP

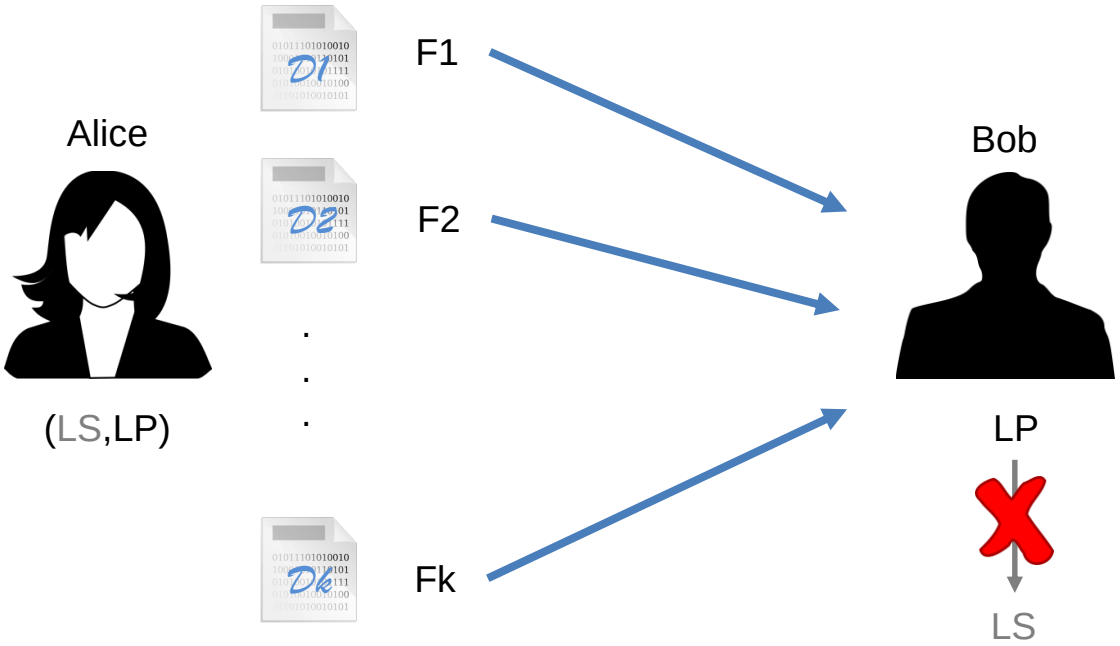
Propiedades de firmas digitales

Imposible reconstruir LS conociendo mensajes de LP



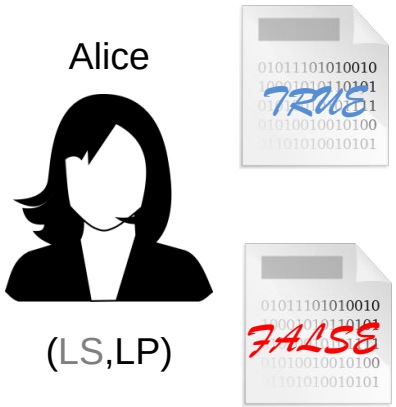
Propiedades de firmas digitales

Imposible reconstruir LS conociendo mensajes de LP



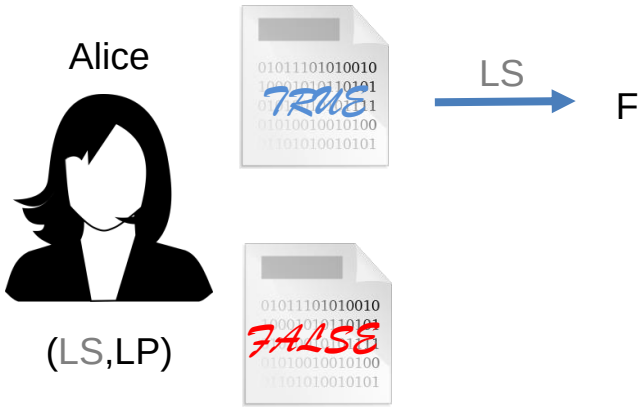
Propiedades de firmas digitales

La firma es única para cada documento



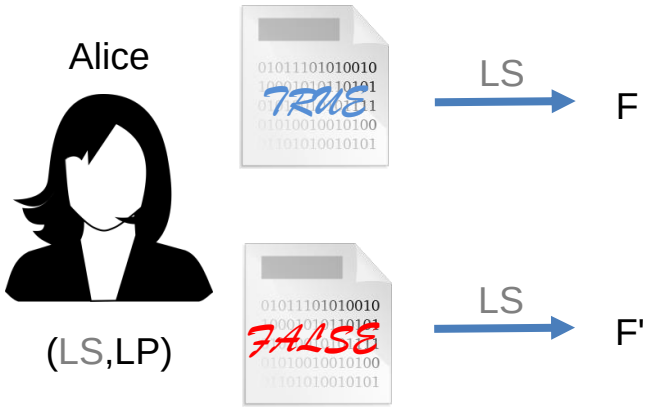
Propiedades de firmas digitales

La firma es única para cada documento



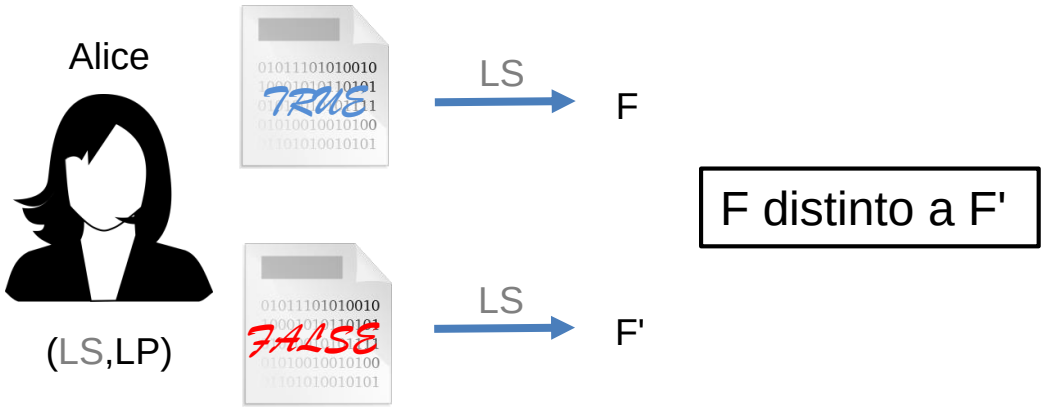
Propiedades de firmas digitales

La firma es única para cada documento



Propiedades de firmas digitales

La firma es única para cada documento



Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

Charlie

Bob (LS',LP')

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

Charlie

Bob (LS',LP')

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

Charlie

Bob (LS',LP')

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

Charlie

Bob (LS',LP')

LS' → F'

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

Charlie

F ≠ F'

Bob (LS',LP')

LS' → F'

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

Charlie

F ≠ F'

F'

Bob (LS',LP')

LS' → F'

Propiedades de firmas digitales

La firma se puede realizar solo con LS

Alice (LS,LP)

LS → F

F ≠ F'

Charlie

LP

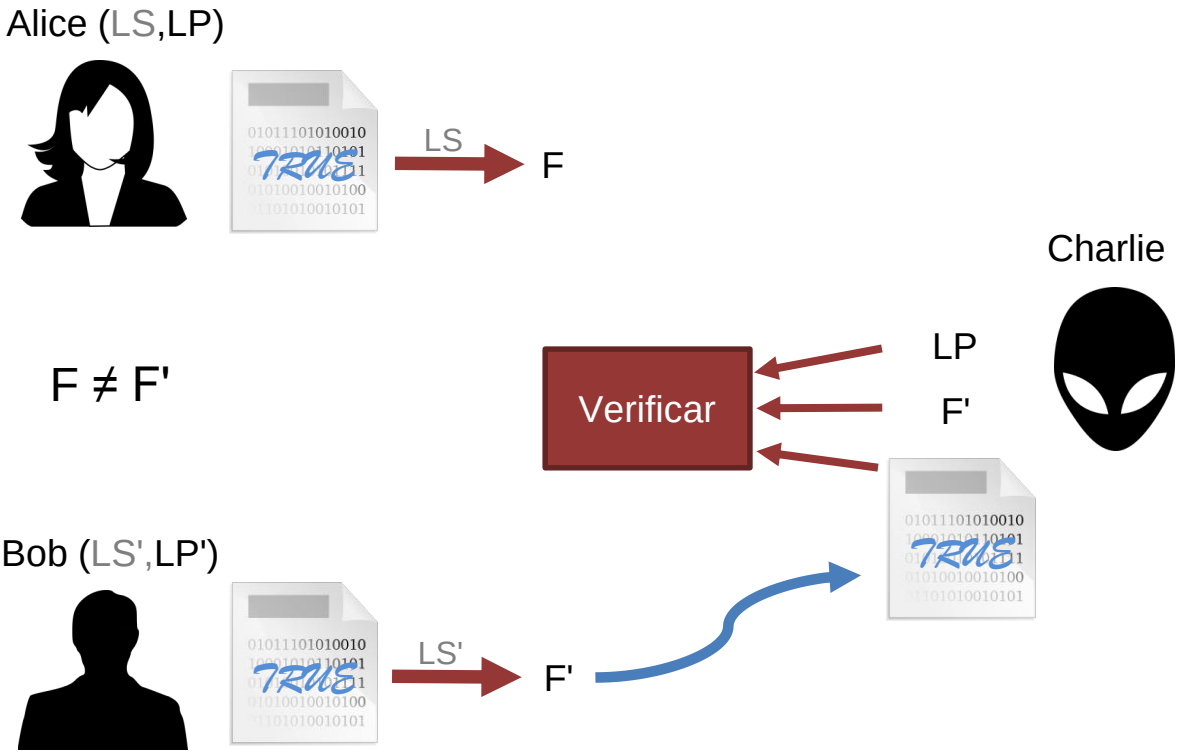
F'

Bob (LS',LP')

LS' → F'

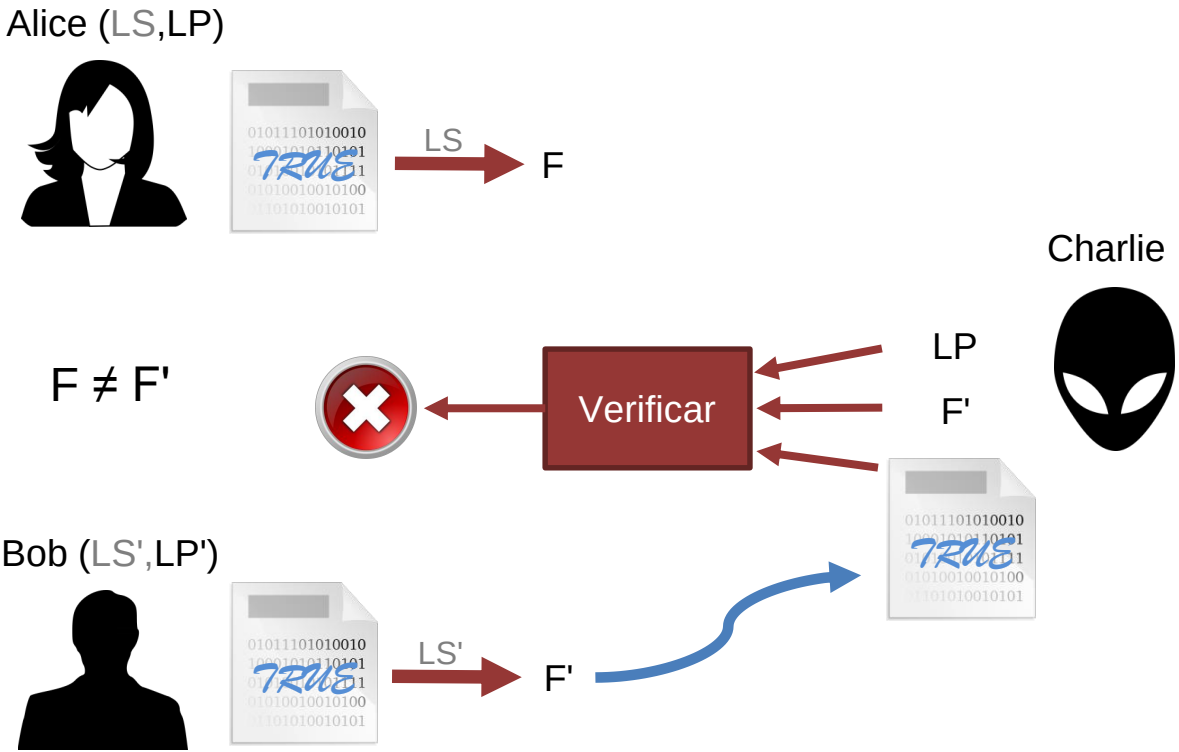
Propiedades de firmas digitales

La firma se puede realizar solo con LS



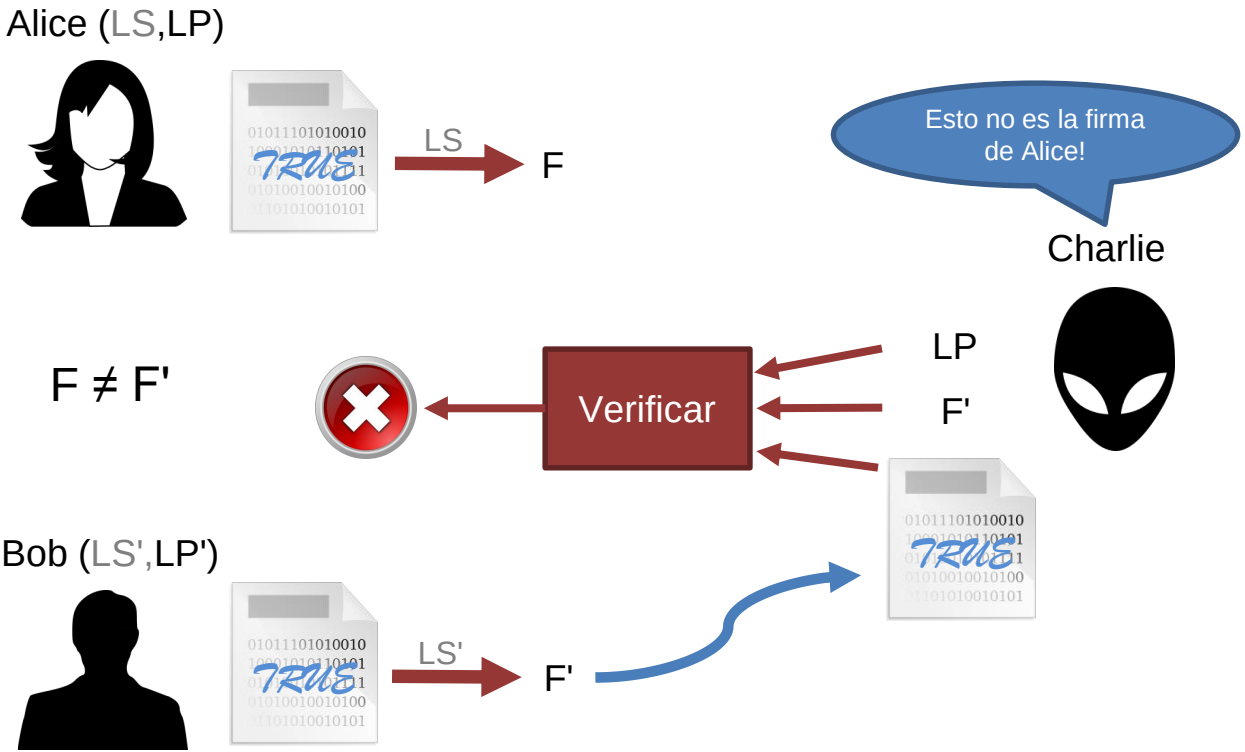
Propiedades de firmas digitales

La firma se puede realizar solo con LS



Propiedades de firmas digitales

La firma se puede realizar solo con LS



Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50 F-A

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50 F-A

¡Alice me pagó $50!

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50 F-A

Alice paga Bob $1000

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50 F-A

Alice paga Bob $1000 ???

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?

Alice

Libro contable

Alice paga Bob $50 F-A

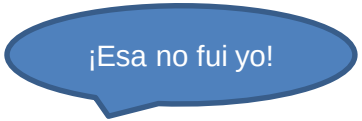
Alice paga Bob $1000 F-B

Bob

Charlie

Problema 2 de ePeso

¿Quién agrega las transacciones?



Alice

Libro contable

Alice paga Bob $50 F-A

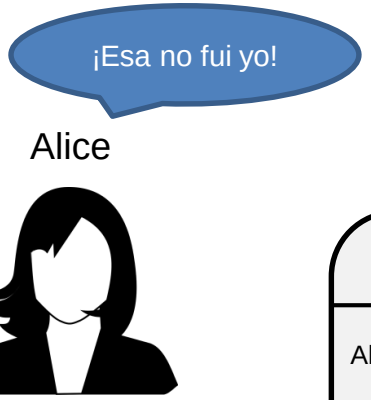
Alice paga Bob $1000 F-B

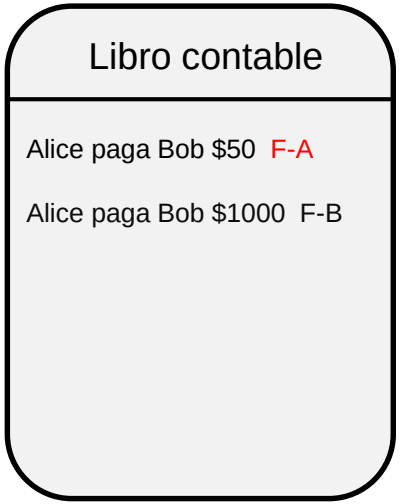
Bob

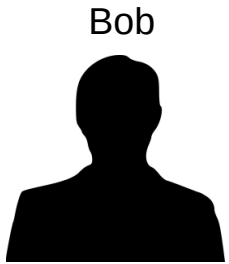
Charlie

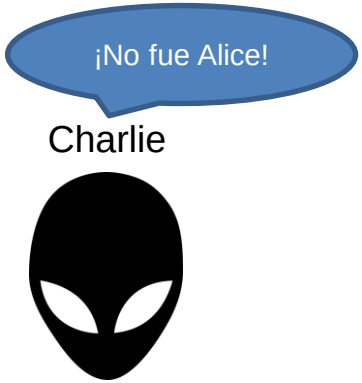
Problema 2 de ePeso

¿Quién agrega las transacciones?









Consideraciones practicas

Aleatoriedad:

- Se requiere una buena fuente de aleatoriedad
- Para generar llaves
- Para generar la firma (cada firma!!!)

Consideraciones practicas

Tamaño de la firma:

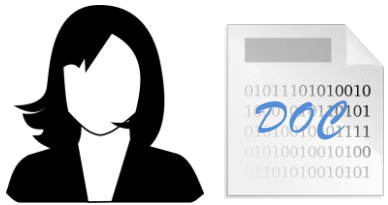
- En algoritmos clásicos depende del documento
- Solución que se usa es firmar el hash

Consideraciones practicas

Tamaño de la firma:

- En algoritmos clásicos depende del documento
- Solución que se usa es firmar el hash

Alice (LS,LP)

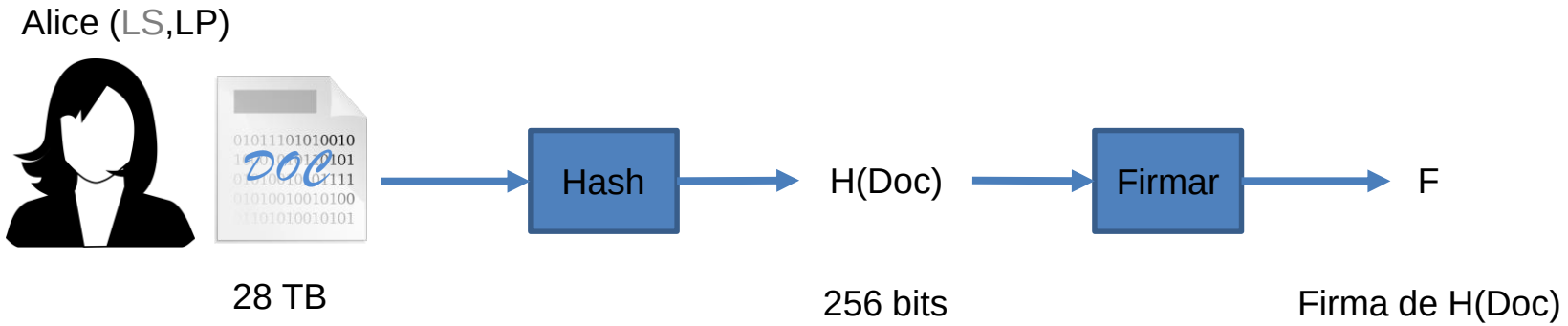


28 TB

Consideraciones practicas

Tamaño de la firma:

- En algoritmos clásicos depende del documento
- Solución que se usa es firmar el hash



Firma digital de BitCoin

Elliptic curve digital signature algorithm (ECDSA)

- NIST/NSA standard
- Curva secp256k1
- 2^{128} bits de seguridad (número de operaciones para romper el esquema)

Tamaños relevantes:

- LS = 256 bits
- LP = 512 bits (257 bits comprimido)
- Tamaño de mensaje = 256 bits (well, that's convenient)
- Tamaño de firma = 512 bits

Usuario en BitCoin

LP nos permite:

- Vincular firmas a una entidad (la cual controla la correspondiente LS)

Usuario en BitCoin

LP nos permite:

- Vincular firmas a una entidad (la cual controla la correspondiente LS)

Usuario de un sistema descentralizado:

- Una LP (o la persona que controla la LS de esta LP)

Peculiaridades

De los usuarios de un sistema descentralizado

Necesito más de un usuario:

- Usa el algoritmo de generación de las llaves
- Puedes tener cualquier cantidad de usuarios (puede ser problemático)

Es seguro?

- Como nadie controla los LPs de los usuarios alguien puede generar el mío?
- En teoría sí, pero la probabilidad es efectivamente 0 (dado una buena fuente de aleatoriedad)

Peculiaridades

De los usuarios de un sistema descentralizado

Es seguro? (2)

- 100%
- Si uno maneja bien su LS (y las firmas -- aleatoriedad)

Qué pasa si pierdo mi LS?

- 0% posibilidad de recuperarla
- Un gran beneficio de los bancos es permitir recuperación de usuario/transacción
- BitCoin es 100% seguro criptográficamente, pero no permite esto

Referencias

Todas las imagenes de esta clase eran recuperadas en:

https://pixabay.com/