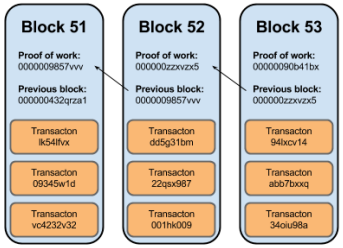


Criptomonedas y Tecnología

Alejandro Hevia, Ph.D.
Depto. Ciencias de la Computación, Universidad de Chile

Jornada Temática
"Criptomonedas, Oportunidades y Desafíos desde Tres Perspectivas",
Comisión de Hacienda, Cámara de Diputados de Chile
14 de Mayo 2018

UNIVERSIDAD DE CHILE

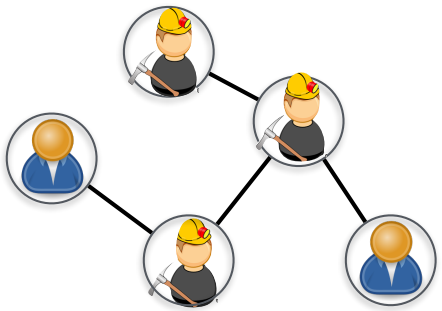

WHEN TO BUY,
WHEN TO SELL
UNDERSTANDING
BITCOIN

¿Qué es una criptomoneda?

- Ejemplo más conocido: Bitcoin 
- Propuesto el 2008 como hobby (proyecto personal de programación) por Satoshi Nakamoto
- Hoy alcance mundial, > US$ 143.000 MM
- Variantes: Ethereum, Ripple, Litecoin, Zcash

Ingredientes de Bitcoin

Bitcoin está construída sobre una red de computadores

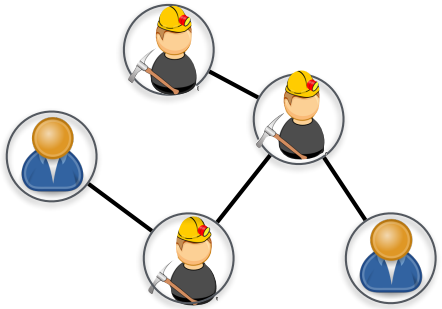


red

nodos especiales: mineros

Ingredientes de Bitcoin

Bitcoin está construída sobre una red de computadores



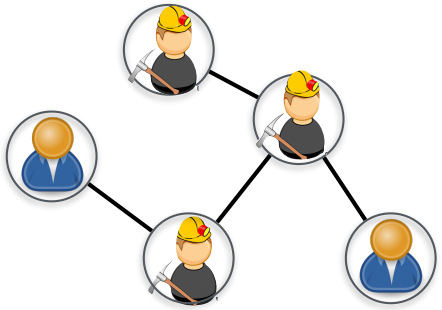
red

nodos especiales: mineros

Cualquiera puede participar

Ingredientes de Bitcoin

Bitcoin está construída sobre una red de computadores

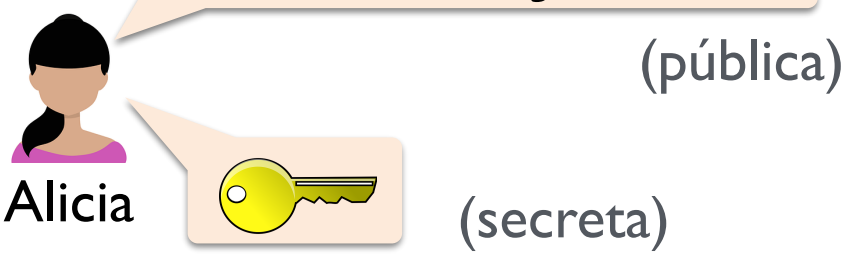


red

nodos especiales: mineros

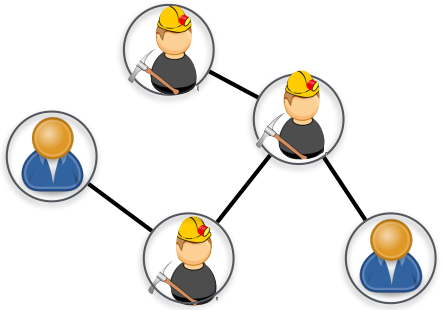
Cualquiera puede participar

Cualquiera puede crear una cuenta:



Ingredientes de Bitcoin

Bitcoin está construída sobre una red de computadores



red

nodos especiales: mineros

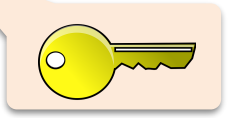
Cualquiera puede participar

Cualquiera puede crear una cuenta:

Alicia

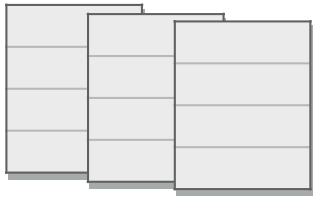
`1BvBMSEYst…g7xJaNVN2`

(pública)

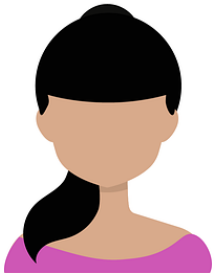


(secreta)

No hay dinero explícito. La red mantiene un libro contable virtual (distribuído): llamado *blockchain*.



Bitcoin en un ejemplo

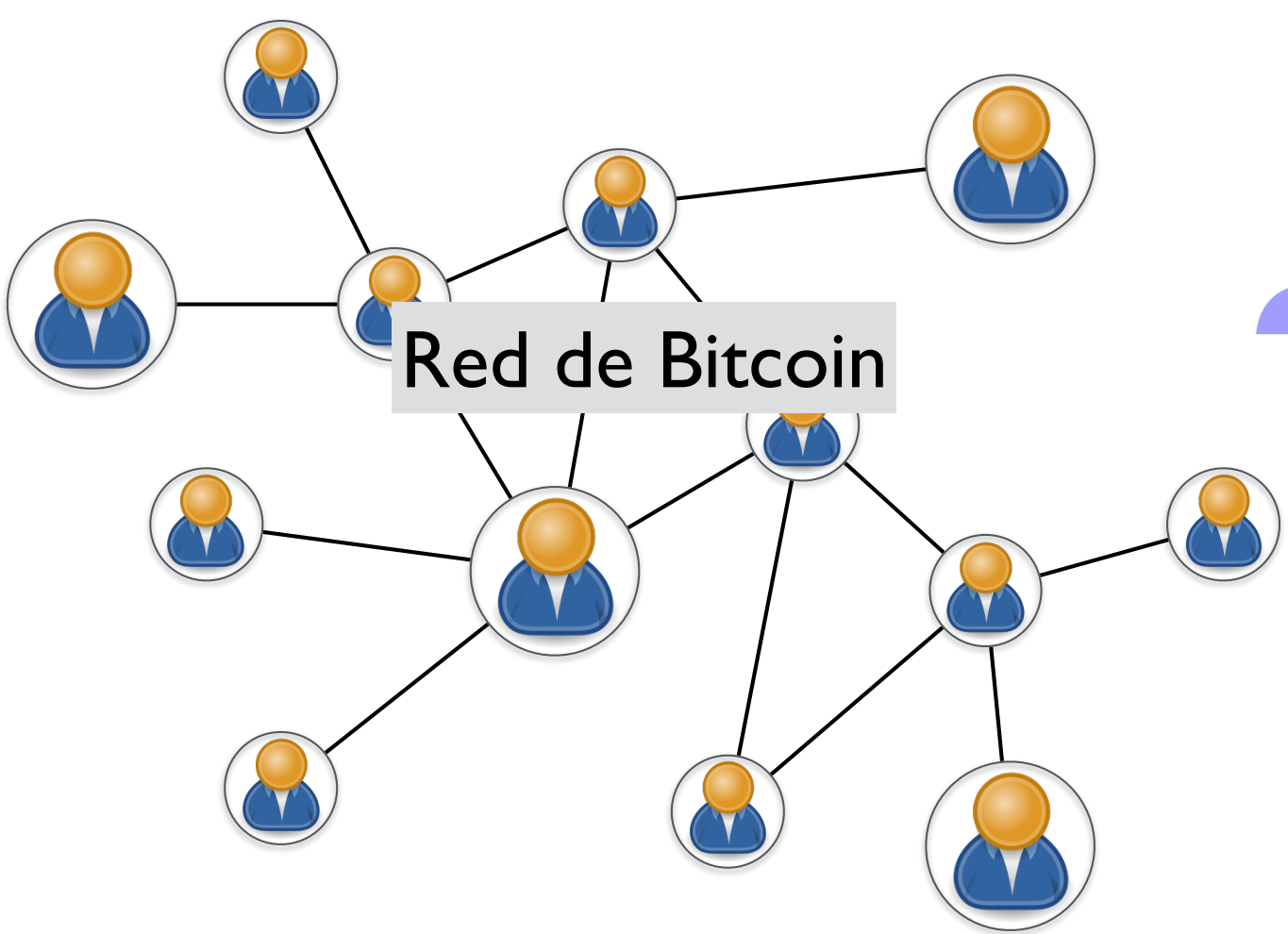
Alicia   Roberto

Alicia desea pagarle 10 monedas a Roberto

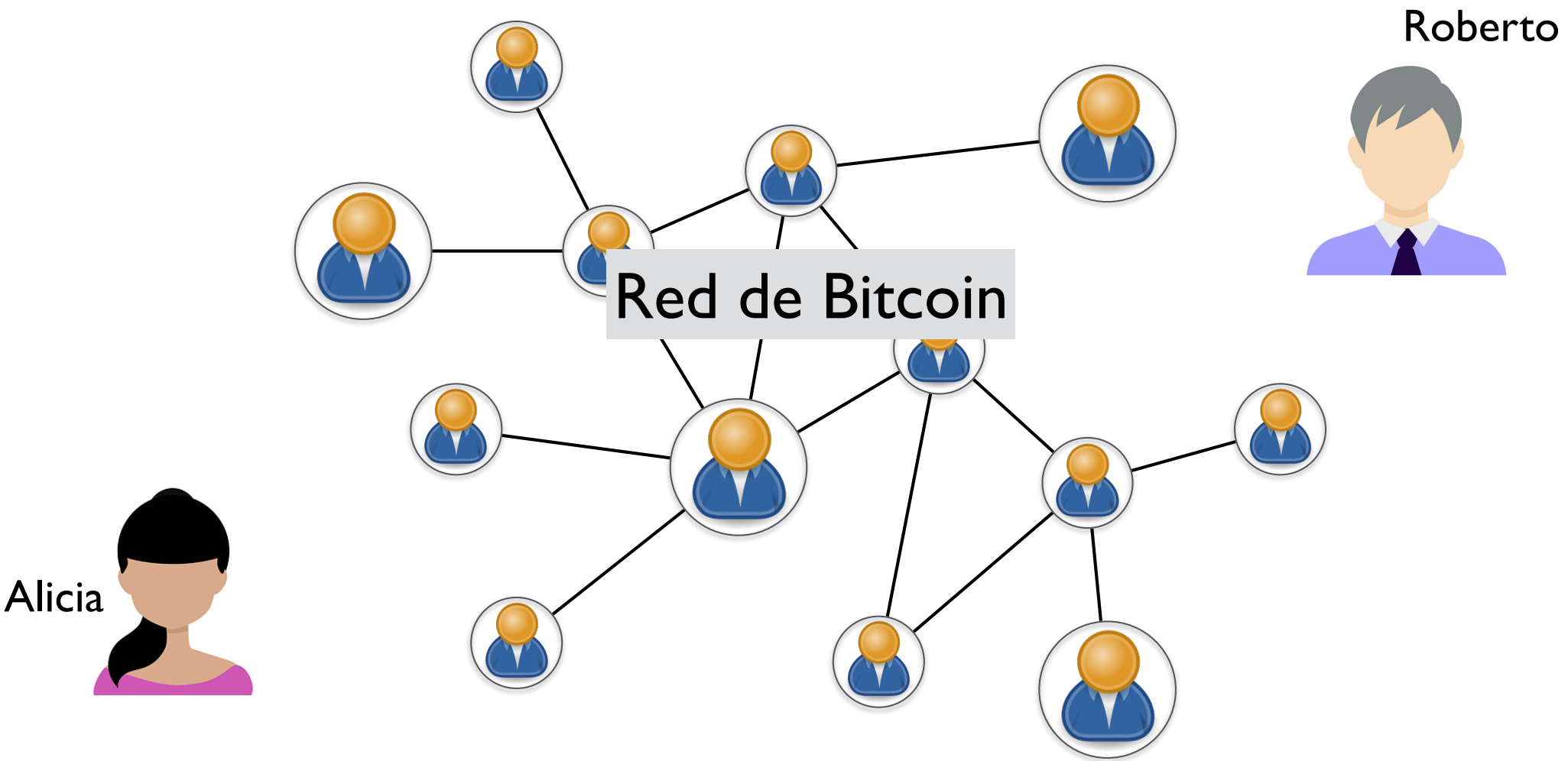
Pago en 3 pasos:

1. Crear el pago o transacción
2. Difundir a la red
3. Validar y enlazar la transacción

Bitcoin paso 1



Bitcoin paso 1

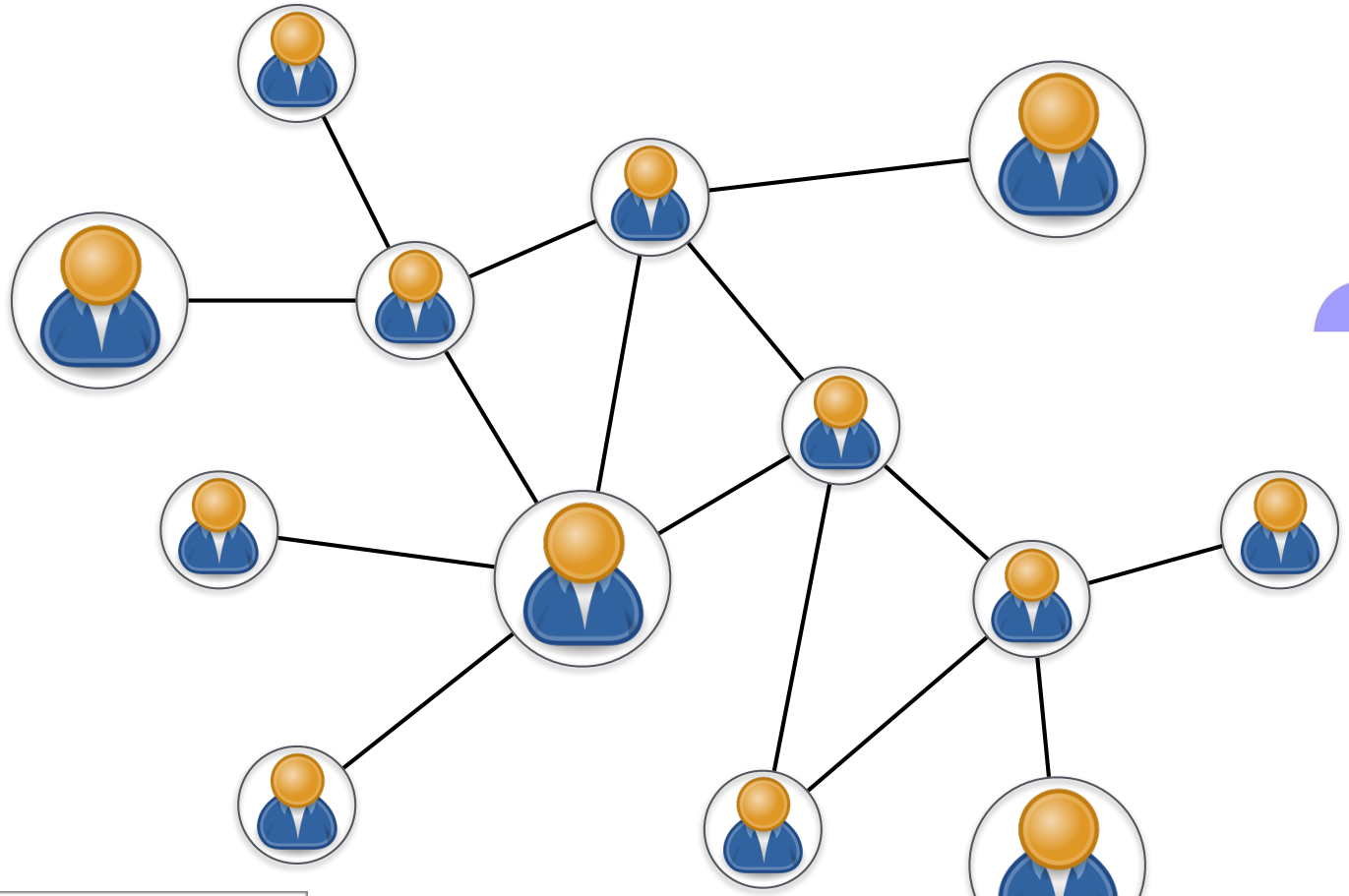


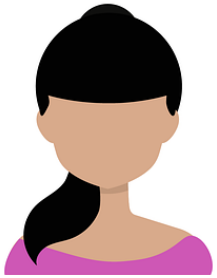
Miembros de la red recuerdan los saldos de c/u

Bitcoin paso 1

Miembros de la red recuerdan los saldos de c/u

Paso 1: Creación

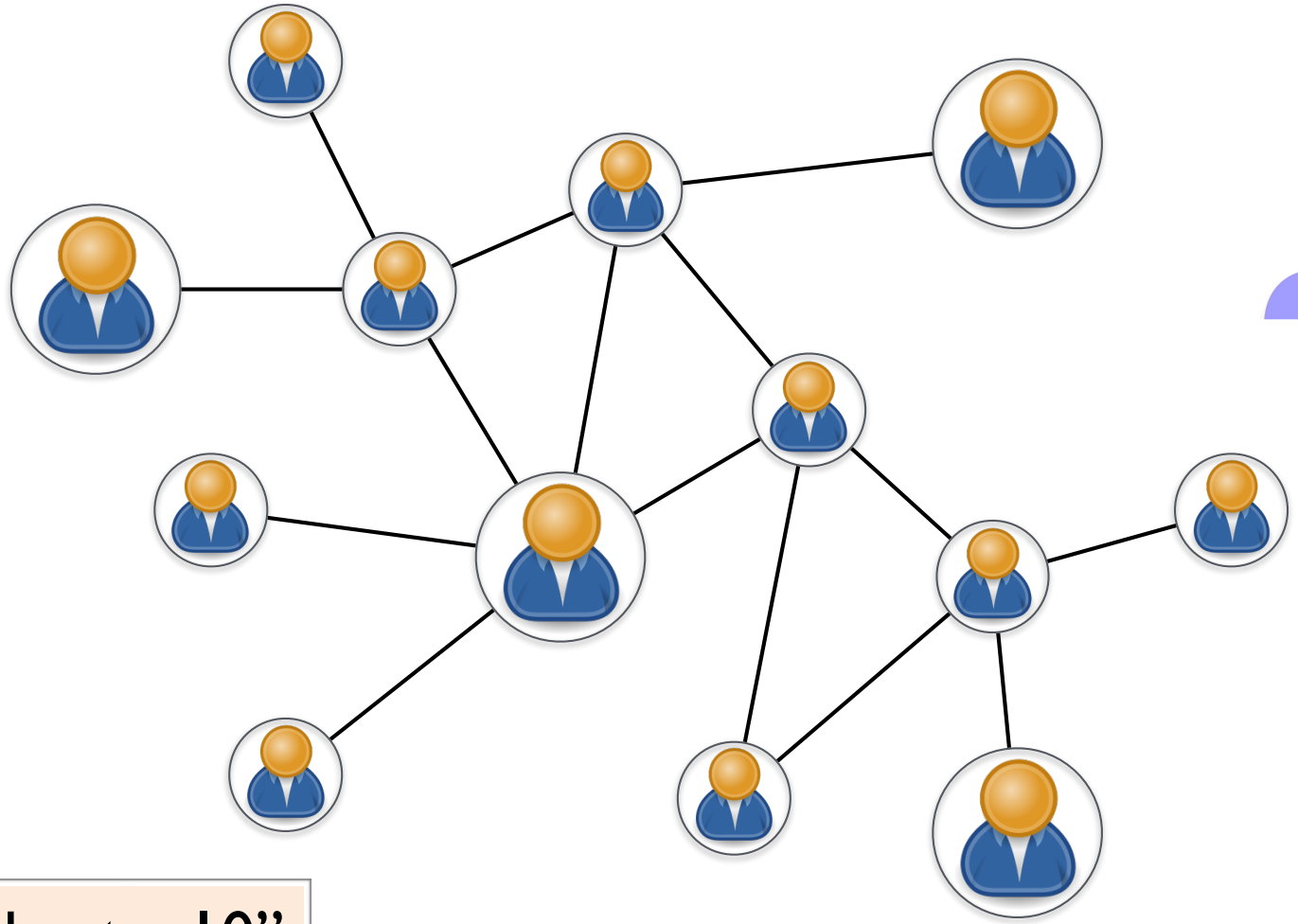


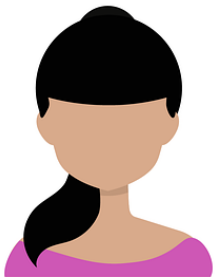


"Yo Alicia le pagaré a Roberto10 monedas"

Alicia crea una transacción (un mensaje firmado digitalmente)

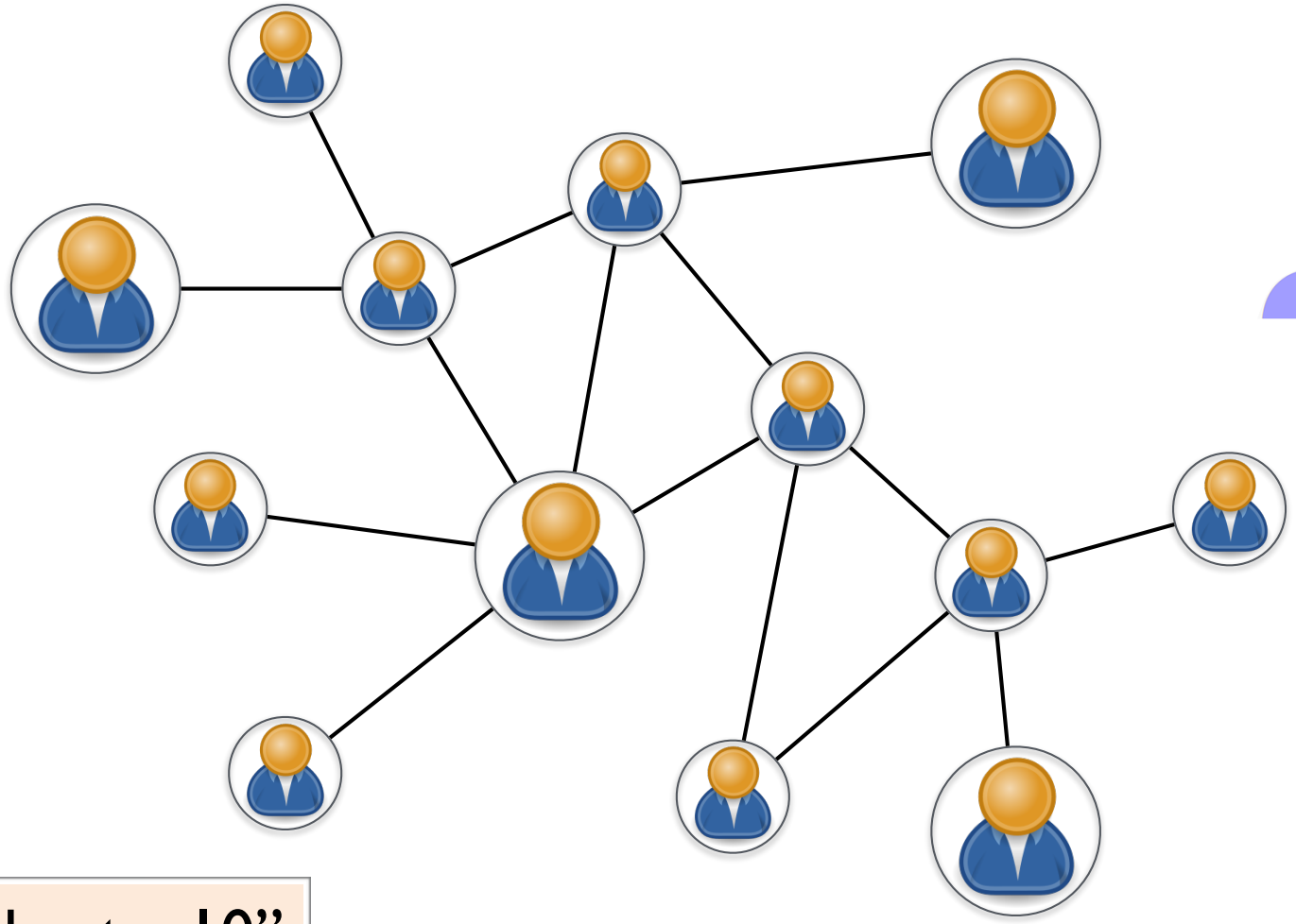
Paso 2: Difusión

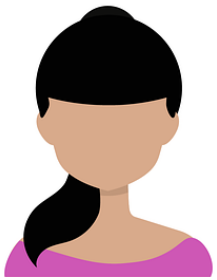




"Alicia a Roberto: 10"

Paso 2: Difusión

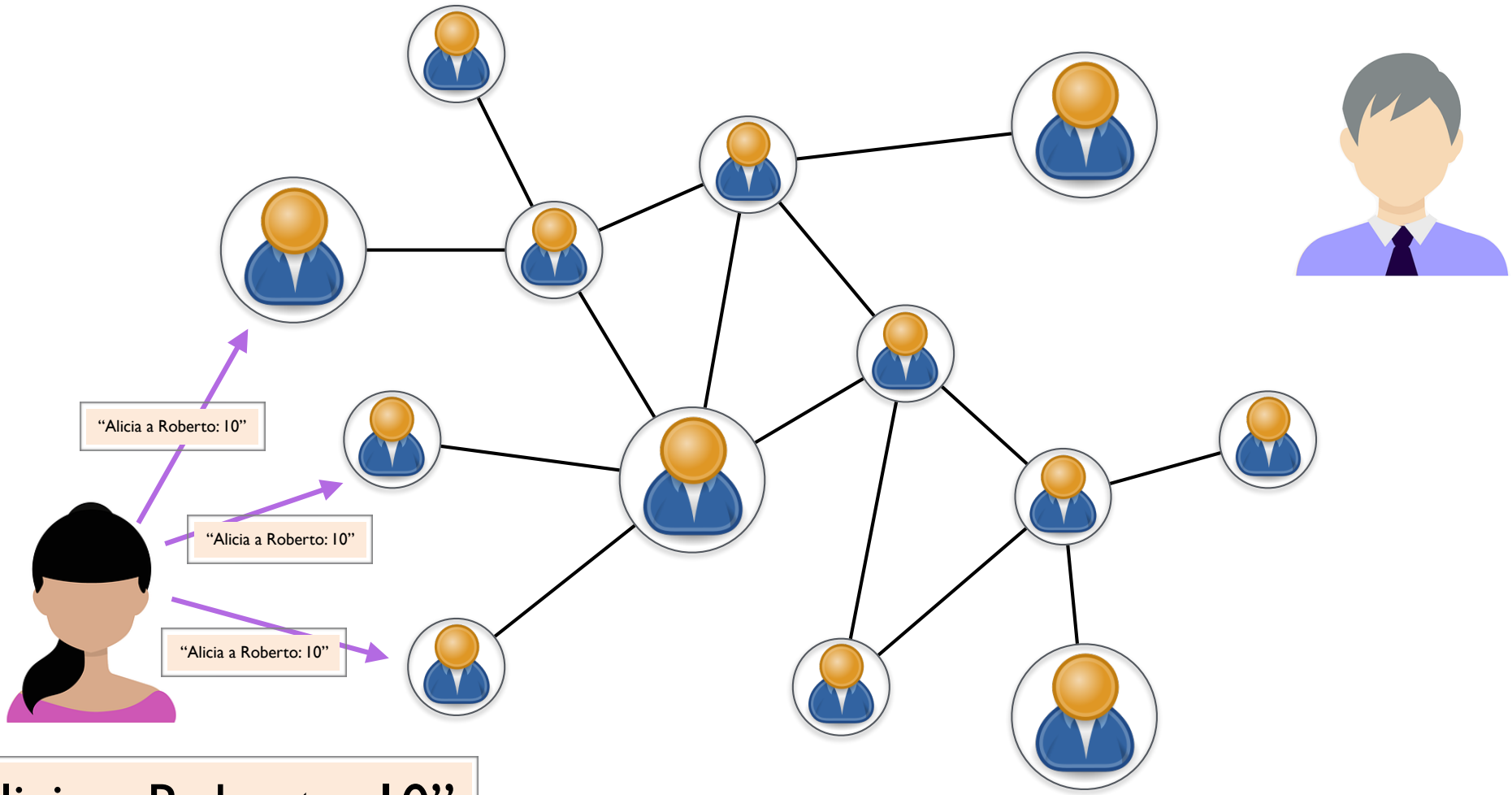




"Alicia a Roberto: 10"

Alicia envía su transacción a la red…

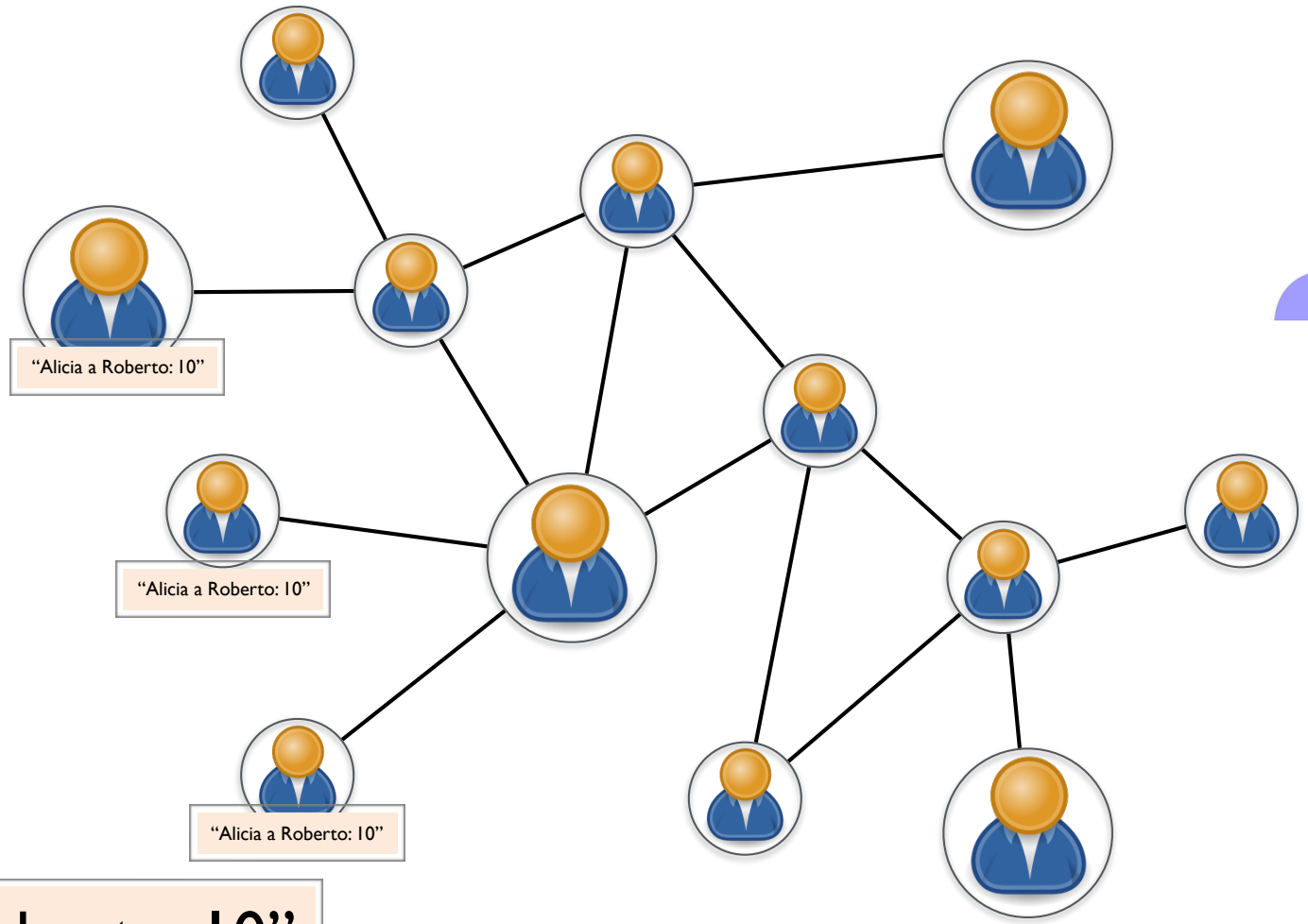
Paso 2: Difusión



"Alicia a Roberto: 10"

Alicia envía su transacción a la red…

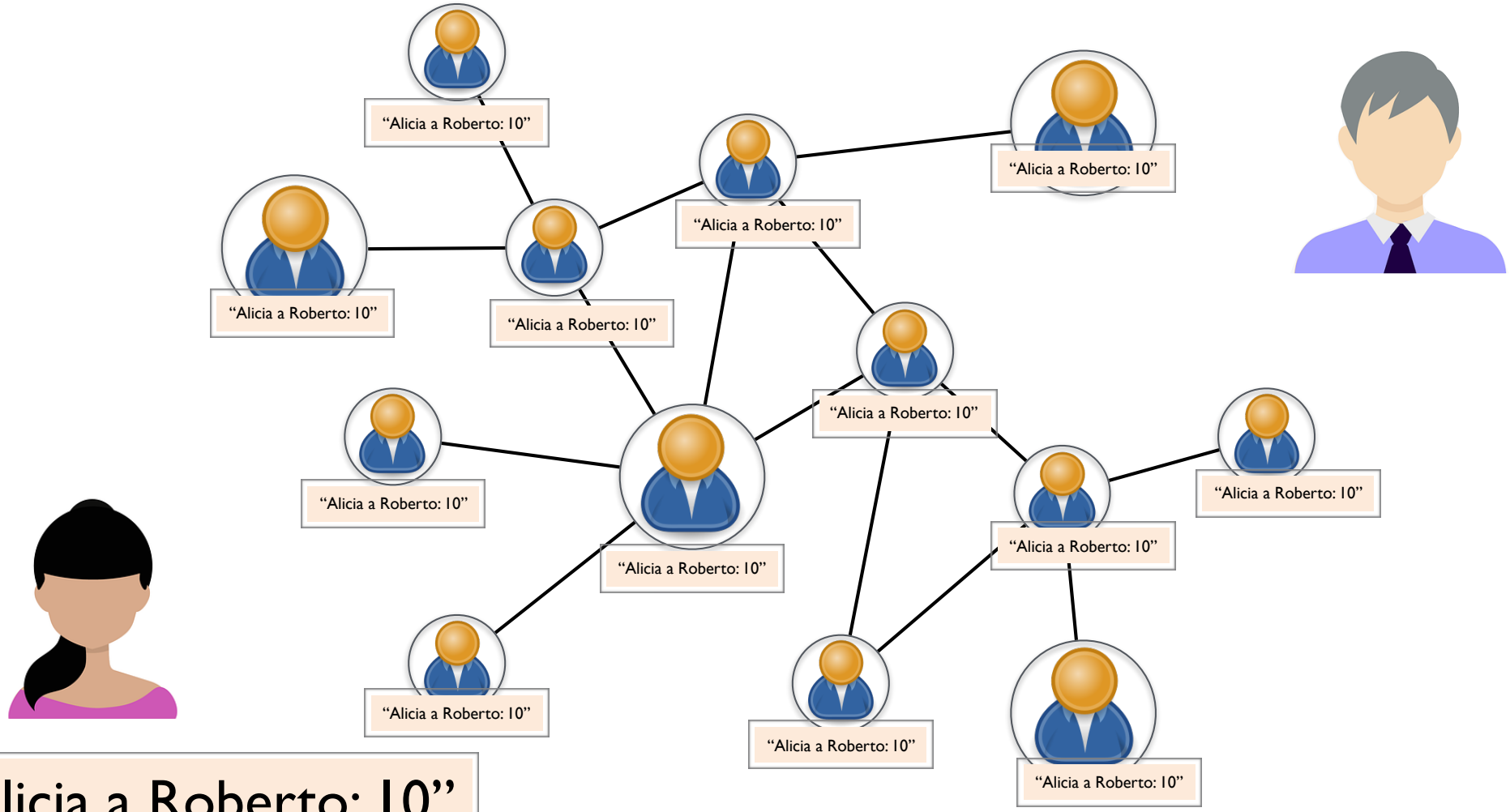
Paso 2: Difusión



"Alicia a Roberto: 10"

…y la red difunde la transacción

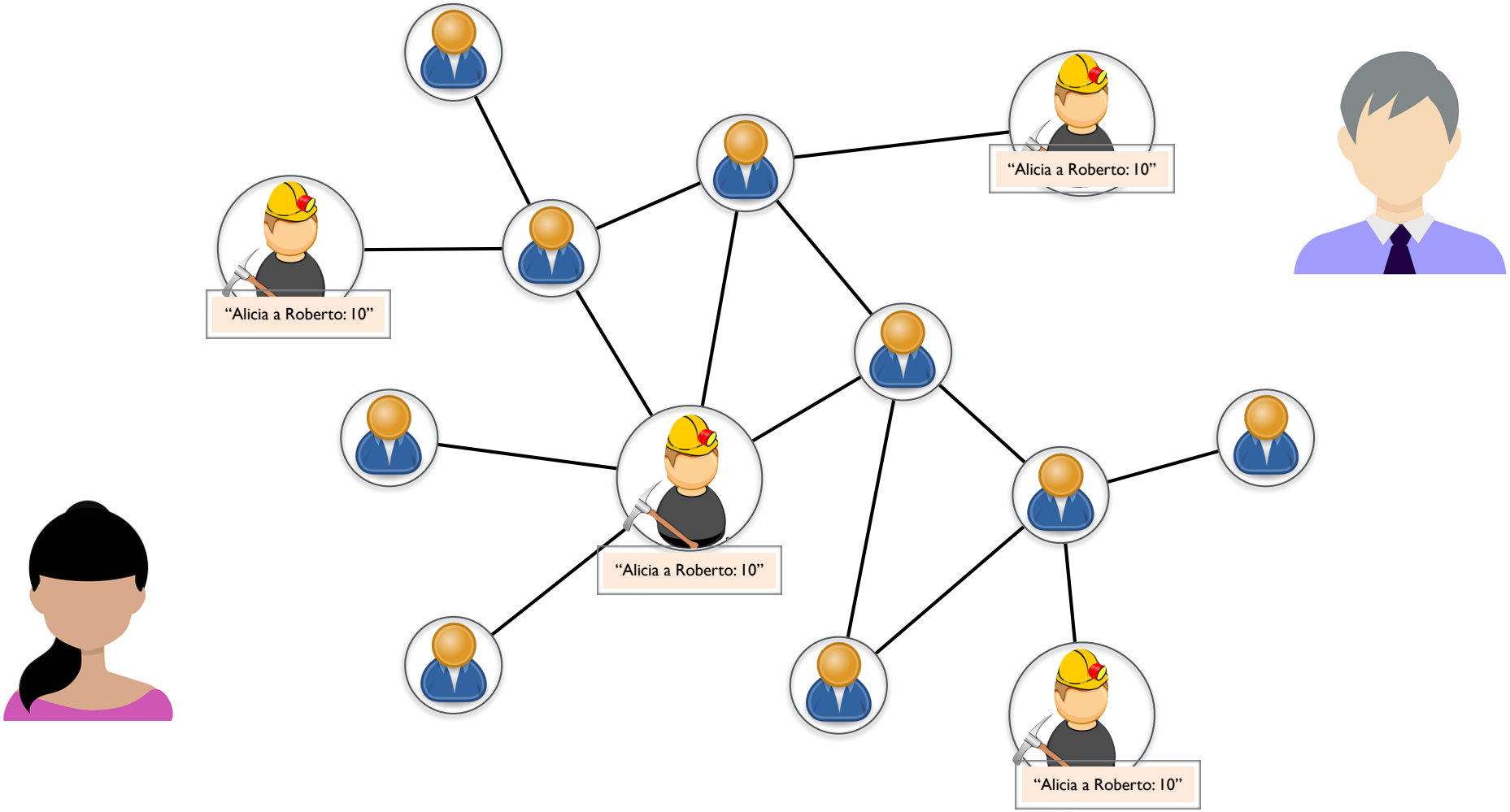
Paso 2: Difusión



"Alicia a Roberto: 10"

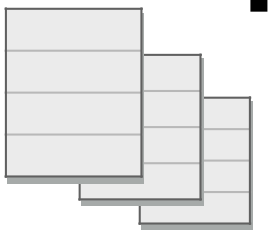
…y la red difunde la transacción

Paso 3: Validación

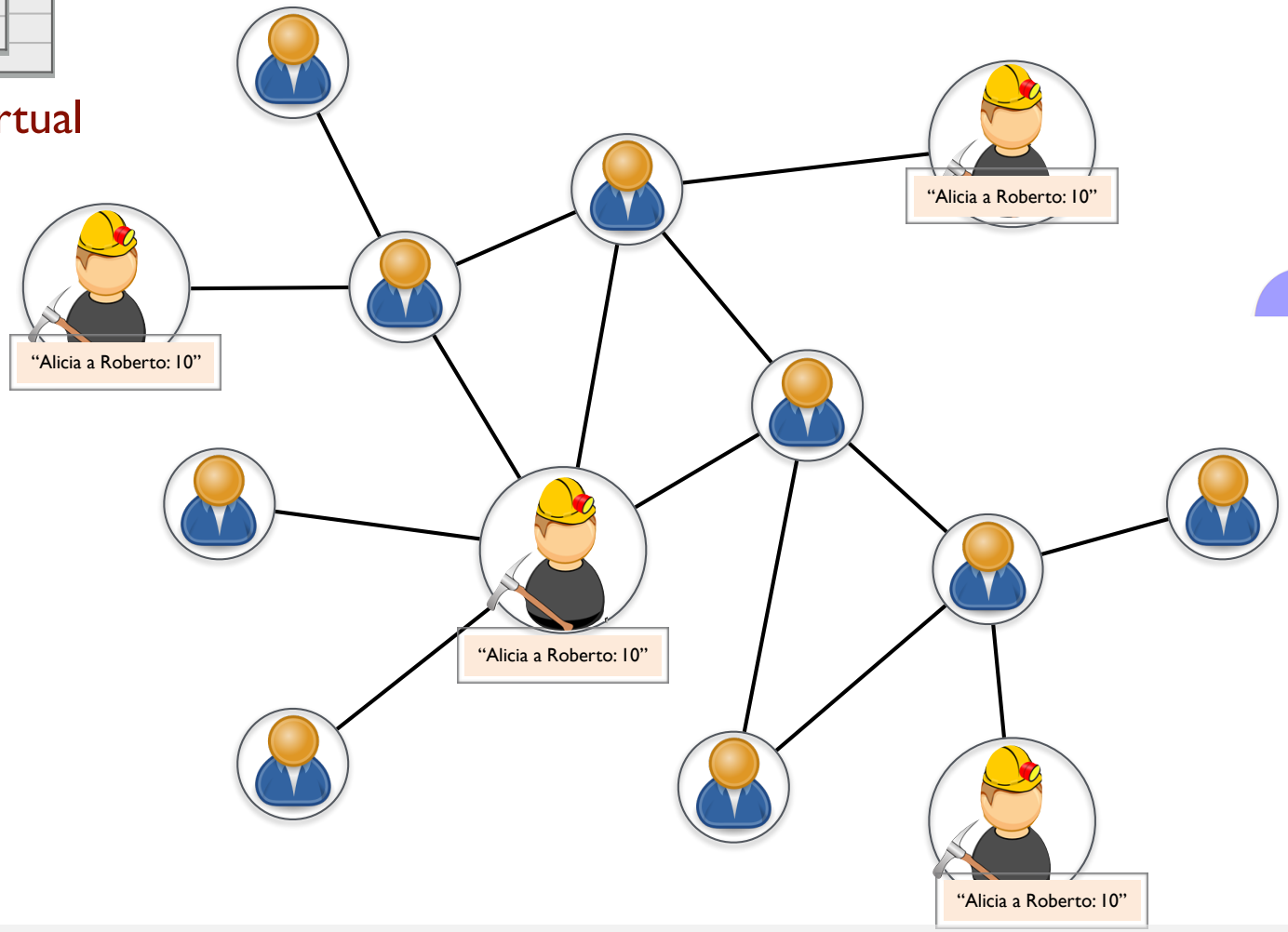


Los nodos mineros validan la transacción…

Paso 3: Validación



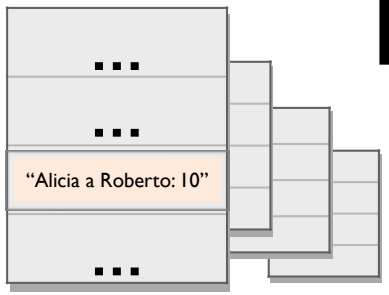
Libro contable virtual



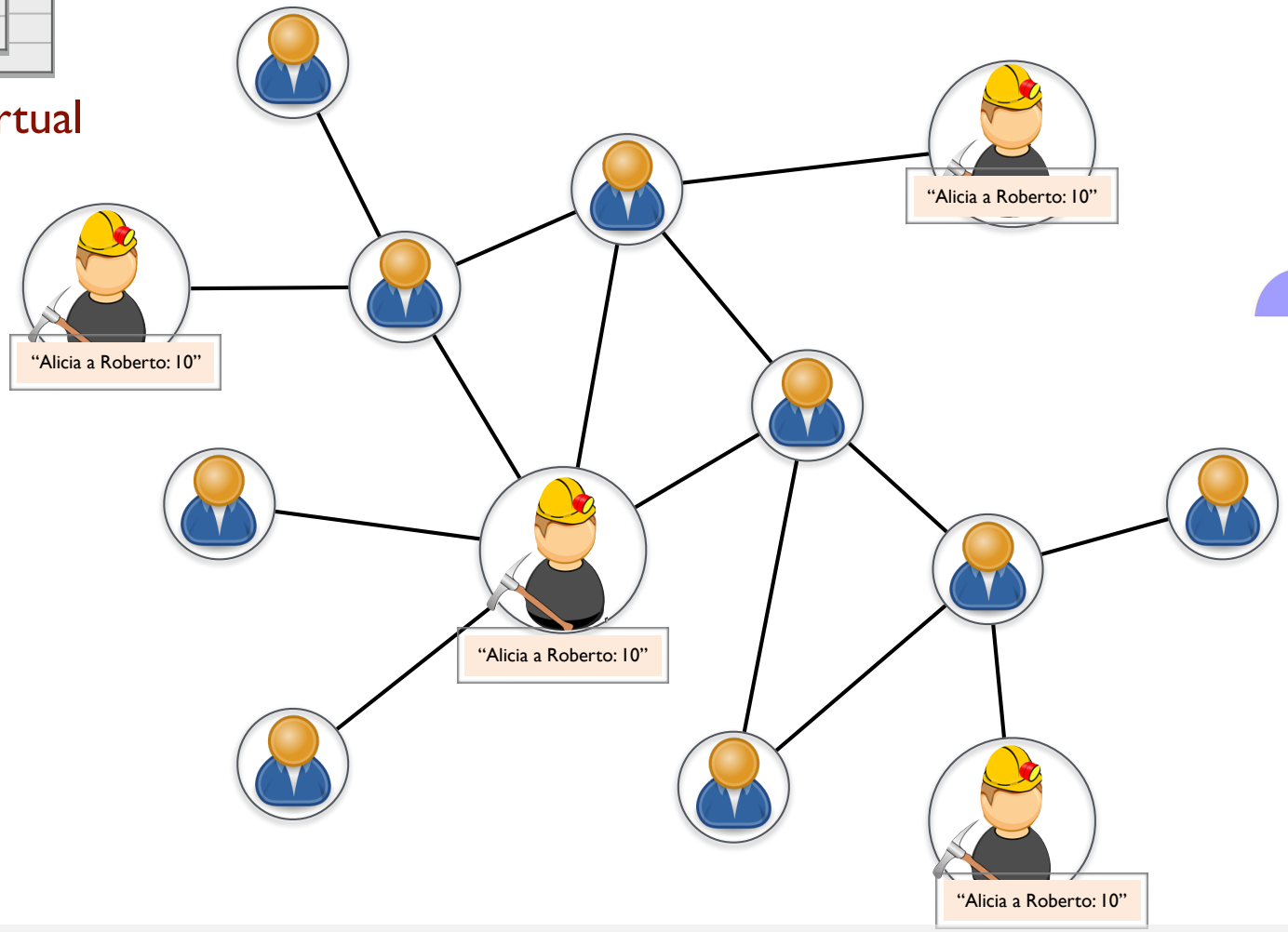
… y la incluyen en una página nueva del libro contable virtual.

Paso 3: Validación

Nueva página



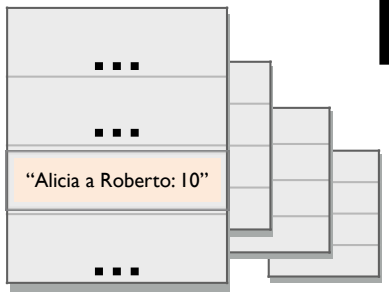
Libro contable virtual



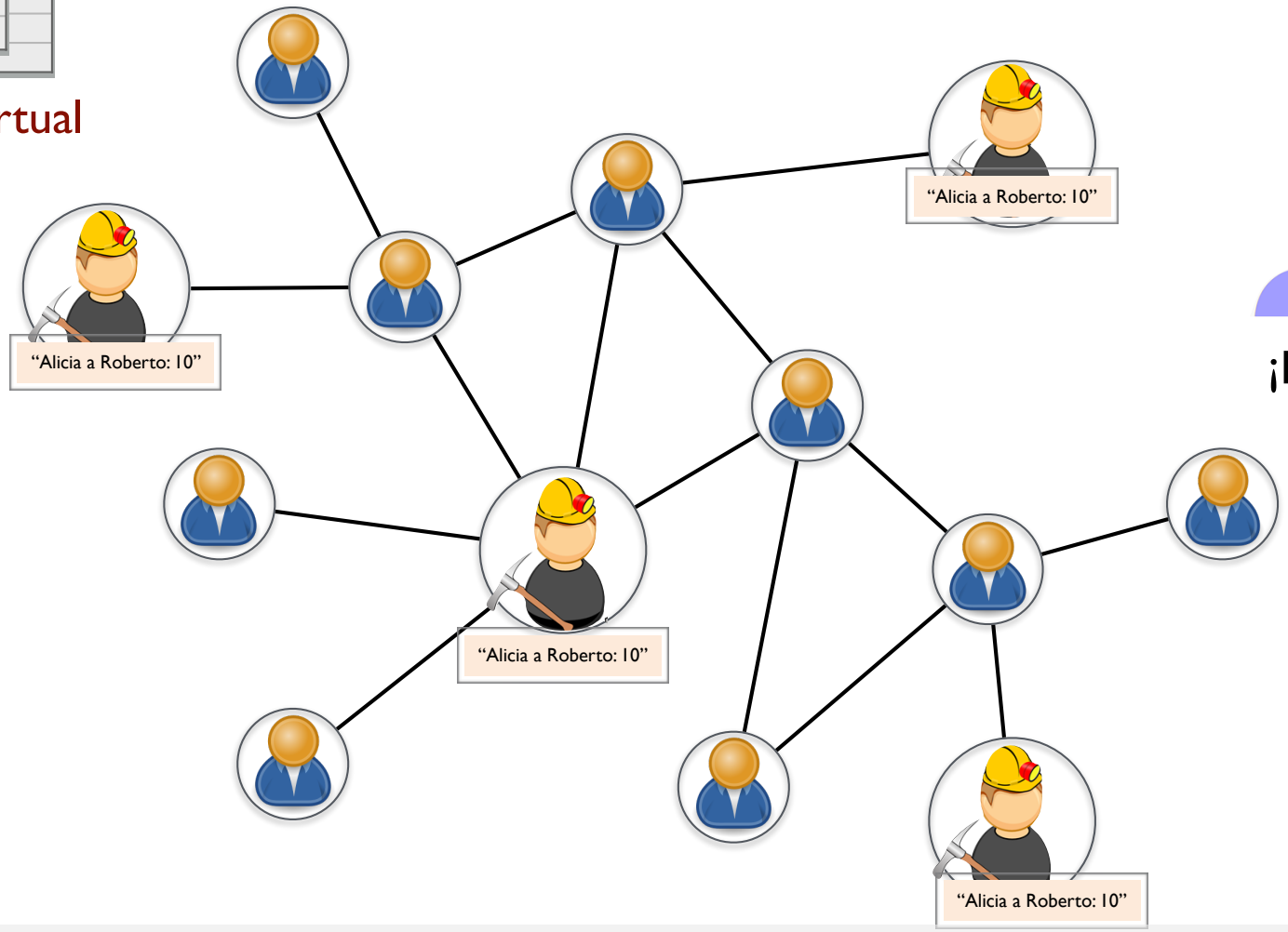
… y la incluyen en una página nueva del libro contable virtual.

Paso 3: Validación

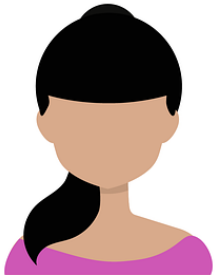
Nueva página



Libro contable virtual

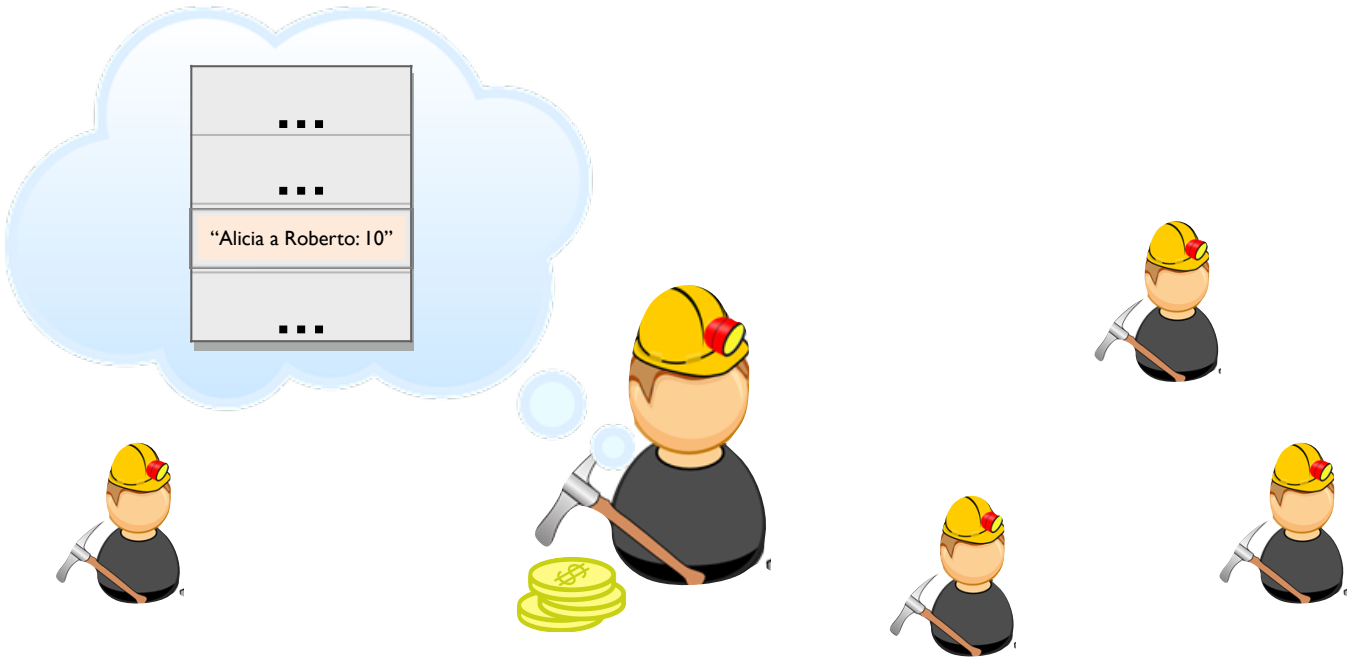


¡Excelente!



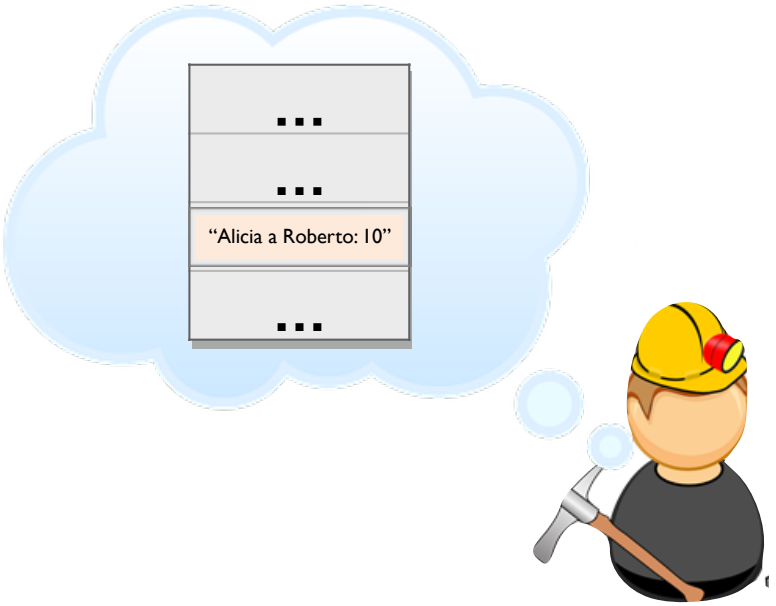
… y la incluyen en una página nueva del libro contable virtual.

Validación y Enlace



1. Un minero es **seleccionado cada vez** para crear la nueva página del libro.
2. Quién resuelve primero un puzzle matemático (PoW) es seleccionado.
3. **Ganar monedas** por ello.

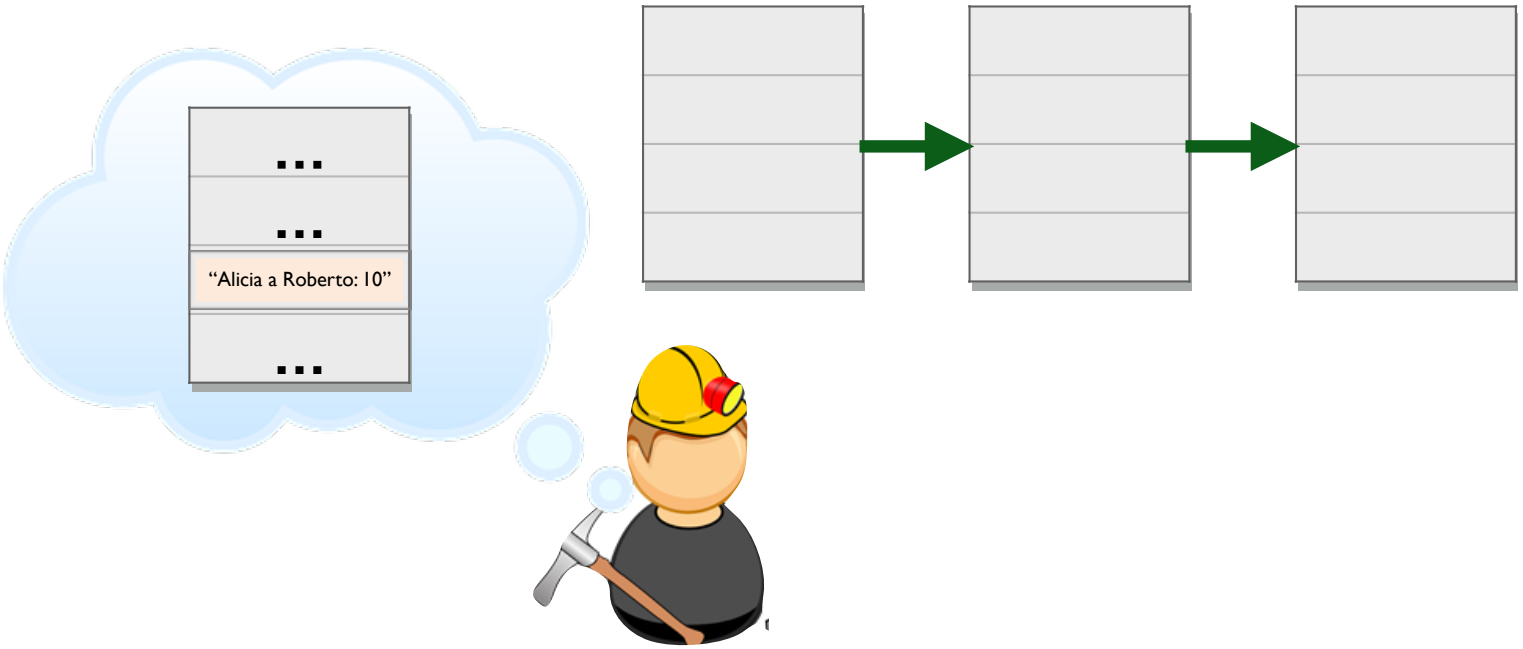
Enlace: donde se crea la Blockchain



4. Minero debe **enlazar** la nueva página a las páginas anteriores.

Mecanismo matemático de enlace hace imposible cambiar las páginas anteriores una vez difundido el bloque

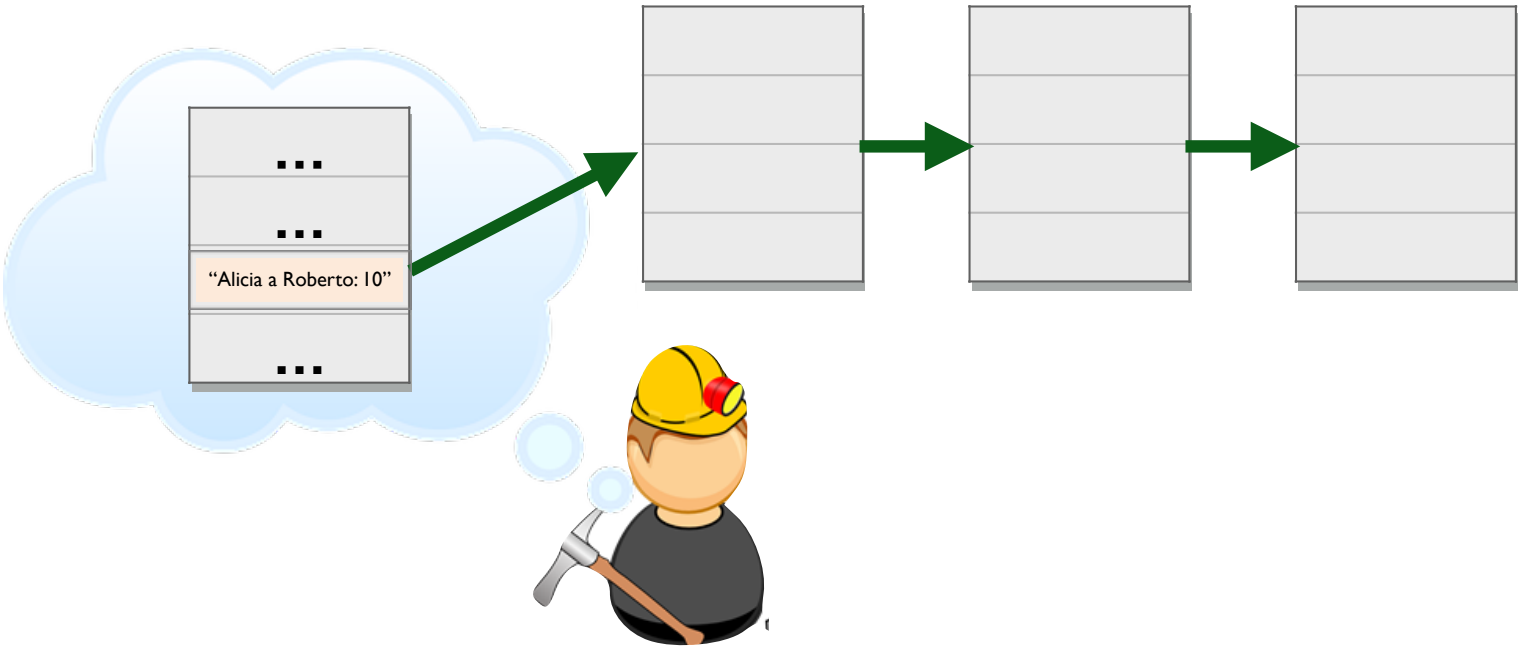
Enlace: donde se crea la Blockchain



4. Minero debe **enlazar** la nueva página a las páginas anteriores.

Mecanismo matemático de enlace hace imposible cambiar las páginas anteriores una vez difundido el bloque

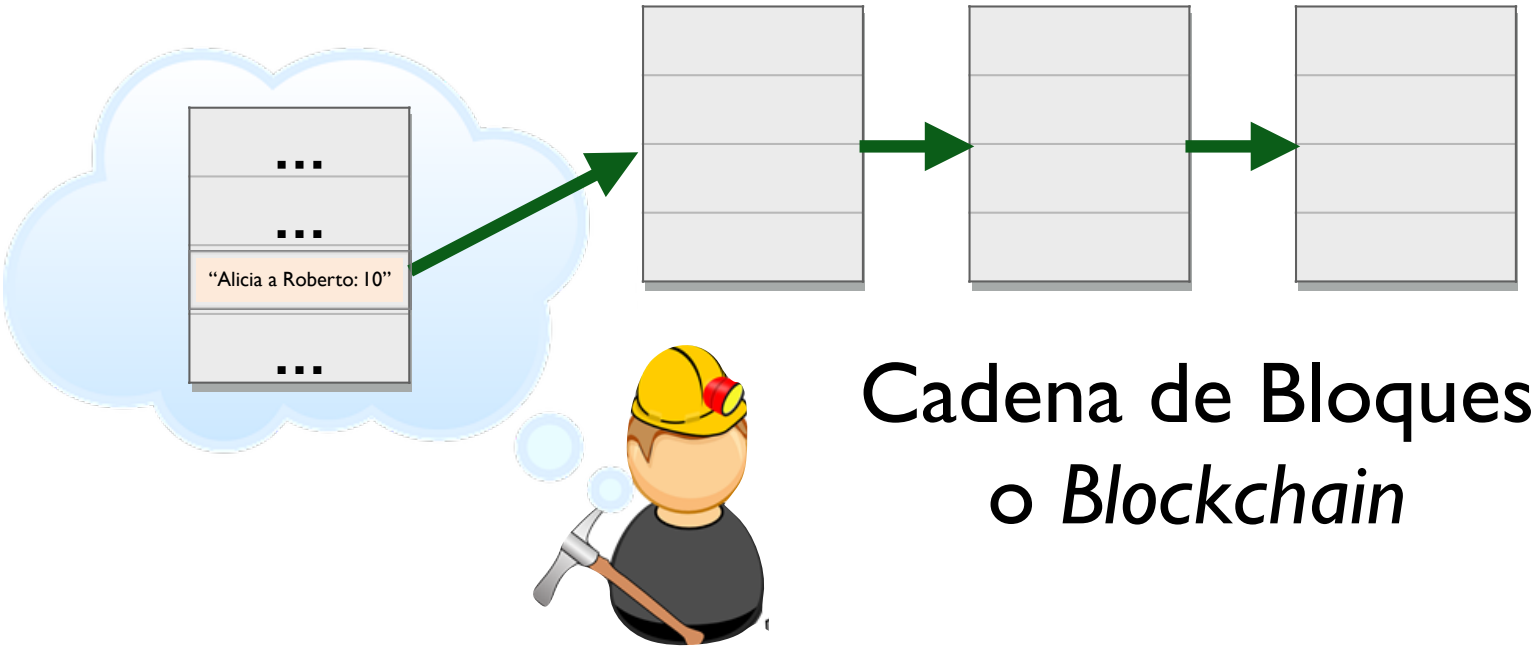
Enlace: donde se crea la Blockchain



4. Minero debe **enlazar** la nueva página a las páginas anteriores.

Mecanismo matemático de enlace hace imposible cambiar las páginas anteriores una vez difundido el bloque

Enlace: donde se crea la Blockchain



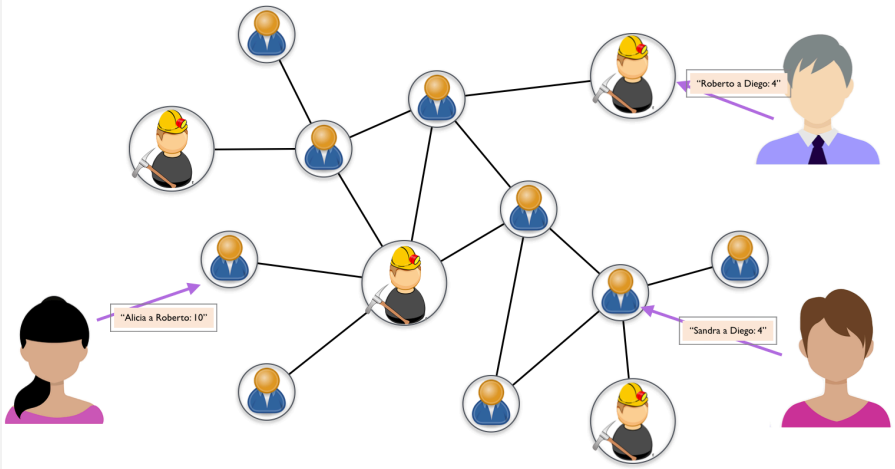
Cadena de Bloques
o *Blockchain*

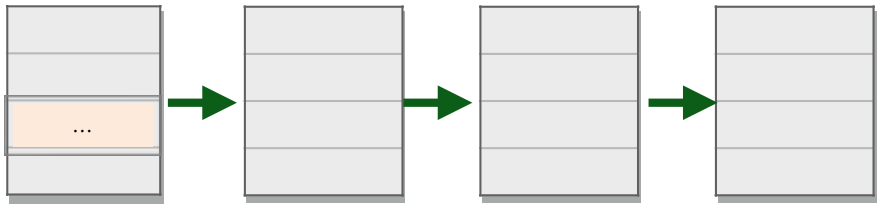
4. Minero debe **enlazar** la nueva página a las páginas anteriores.

Mecanismo matemático de enlace hace imposible cambiar las páginas anteriores una vez difundido el bloque

Bitcoin en resumen

1. *Usuarios crean transacciones*
2. *Red las distribuye*
3. *Mineros las incluyen en un nuevo bloque*
4. *Bloque es enlazado a la cadena de bloques (blockchain)*
5. *Todos tienen copia de la cadena*

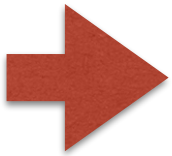




Nada es tan simple

No existen nombres, sólo números de cuenta

"Yo Alicia le pagaré a Roberto10 monedas"

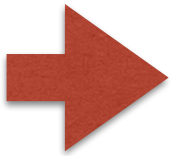


"Yo `1aEYst…g7xJaNVN2` le pagaré a `bc1qar0s...wf5mdq` 10 monedas"

Nada es tan simple

No existen nombres, sólo números de cuenta

"Yo Alicia le pagaré a Roberto10 monedas"



"Yo `1aEYst…g7xJaNVN2` le pagaré a `bc1qar0s...wf5mdq` 10 monedas"

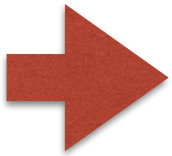
Costo por Tx:

"Yo Alicia le pagaré a Roberto10 monedas, y le daré una **propina** de 0.01 al minero que incluya mi transacción"

Nada es tan simple

No existen nombres, sólo números de cuenta

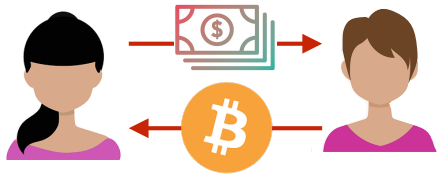
"Yo Alicia le pagaré a Roberto10 monedas"



"Yo `1aEYst…g7xJaNVN2` le pagaré a `bc1qar0s...wf5mdq` 10 monedas"

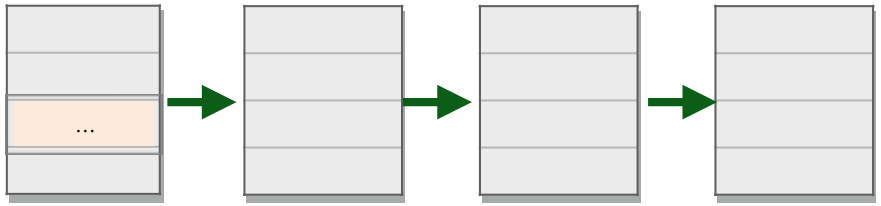
Costo por Tx:

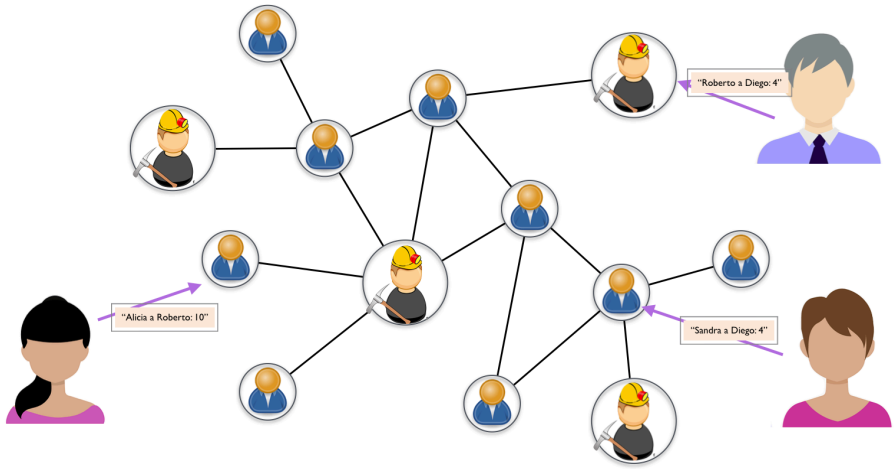
"Yo Alicia le pagaré a Roberto10 monedas, y le daré una **propina** de 0.01 al minero que incluya mi transacción"



Alicia puede comprar monedas de alguien que quiera vender usualmente vía una casa de cambio

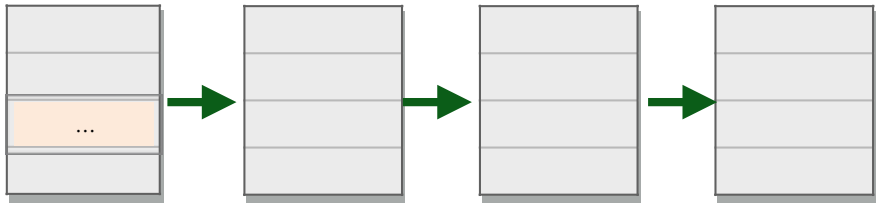
Propiedades

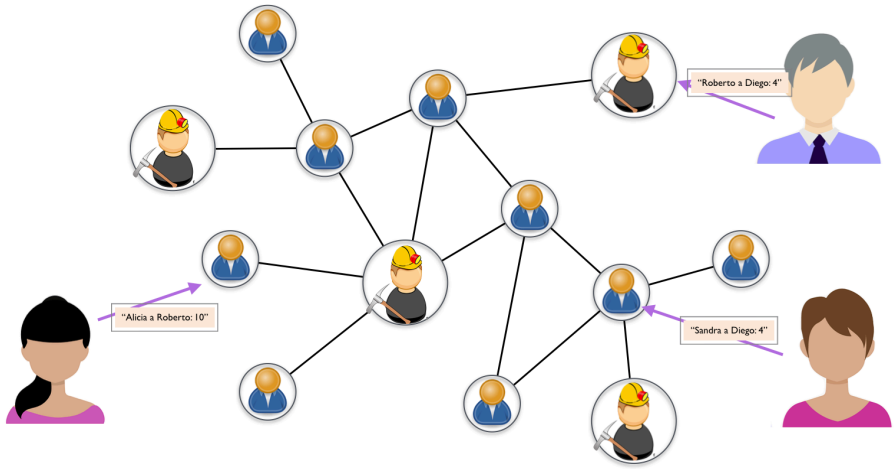




1. *Transacciones son **irreversibles** y **públicas** (en gral.)*
2. *Participantes son pseudo-anónimos (conozco cuenta pero no identidad)*
3. *Mineros son fundamentales para la solidez del sistema*
4. *Reglas de operación definidas por el creador*
5. *Cualquiera puede crear su propia moneda, pero ¿convencerá a mineros de participar?*

Usos interesantes

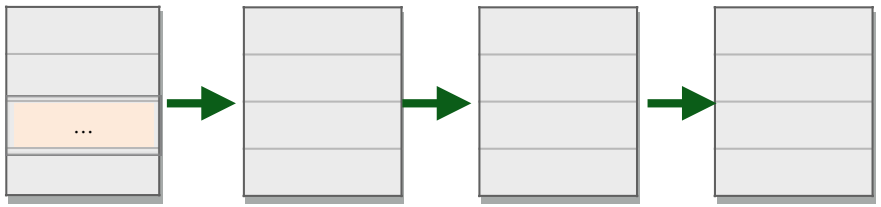




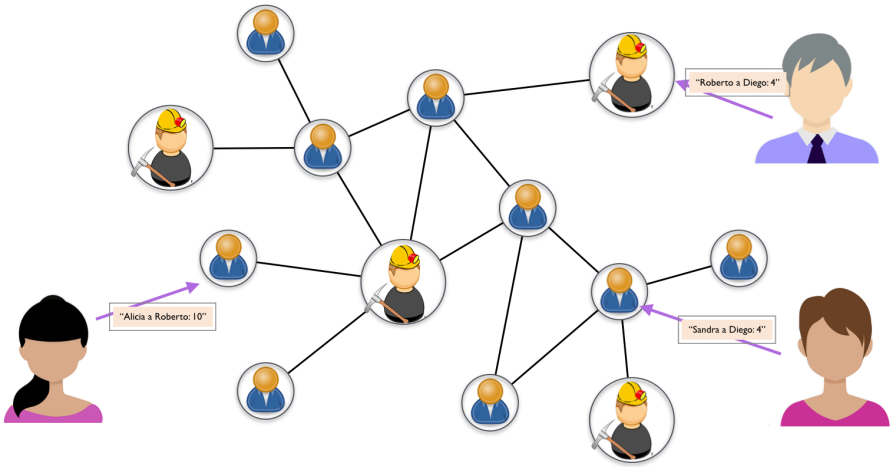
1. *Permite pagos "a fecha" y pagos con "fideicomiso"*
2. *Almacenar información pública en forma robusta y distribuida:*
   - *Registros de propiedades*
   - *Certificados*
   - *Datos médicos*

Otras monedas: Temas comunes

A todas las criptomonedas



Blockchain



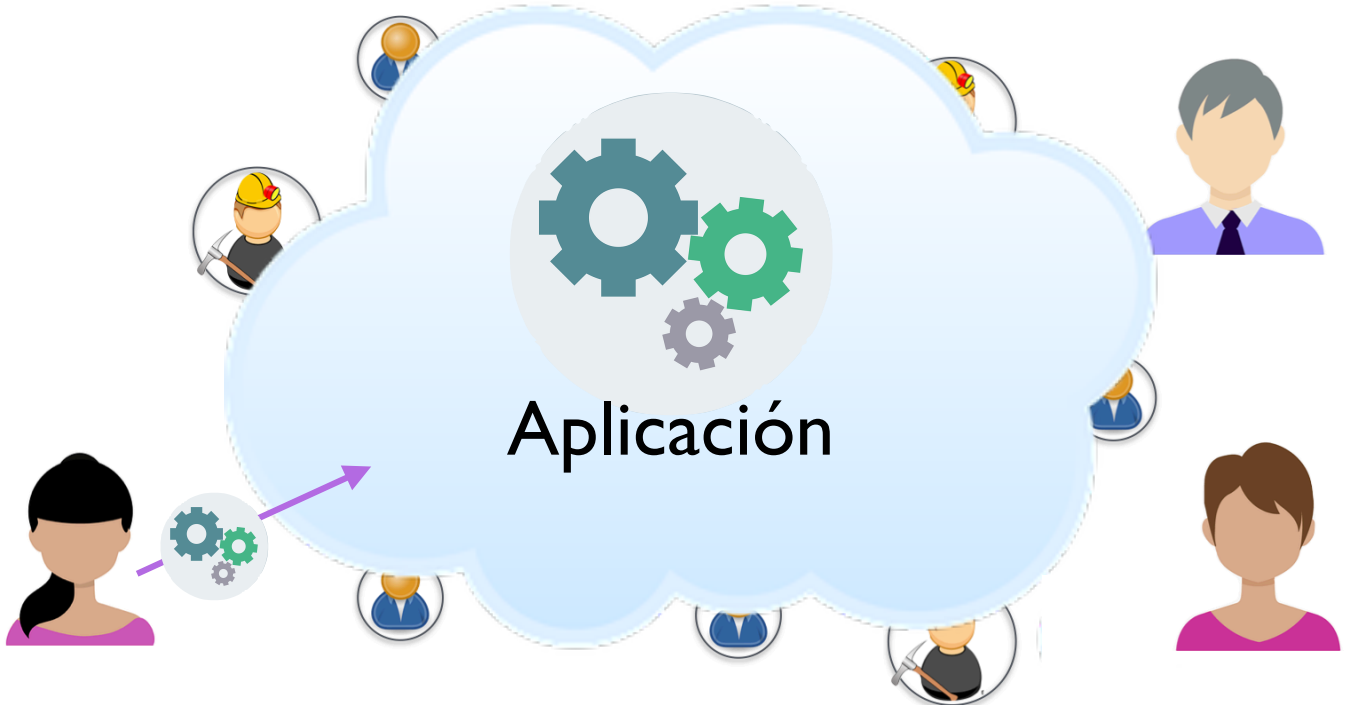
Participantes distribuidos

10 minutos

15 segundos

Variante: Ethereum

No sólo pagos.
Cualquiera puede crear aplicaciones que se ejecuten en forma distribuida, sin confiar en nadie.



Ejemplos de usos

- Empresa de seguros virtual
- Logística
- Préstamos totalmente distribuidos
- Hotelería distribuida

Contratos Inteligentes

"Un computador mundial"

Otras variantes

Bitcoin Cash

Litecoin

Derivados de Bitcoin, motivadas por eficiencia

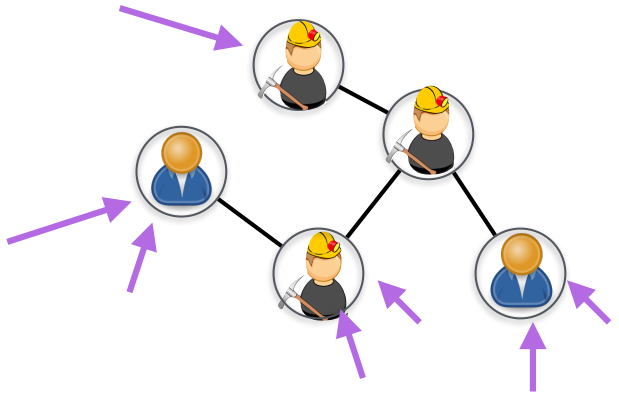
Ripple: Orientación financiera, no completamente descentralizada

Zcash: Transacciones son privadas (origen, destino, monto)

Tokens: bono/acción creados sobre otras monedas (típicamente Ethereum): EOS, NEM, etc.

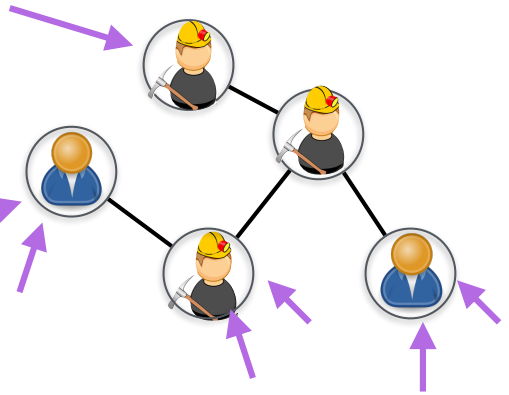
Desafíos

Escalabilidad: incrementar el número de transacciones por segundo

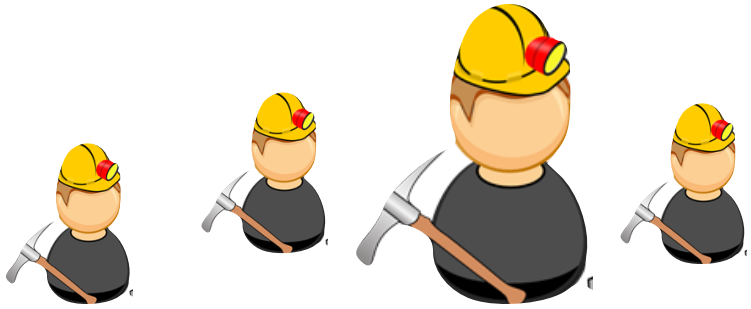


Desafíos

Escalabilidad: incrementar el número de transacciones por segundo

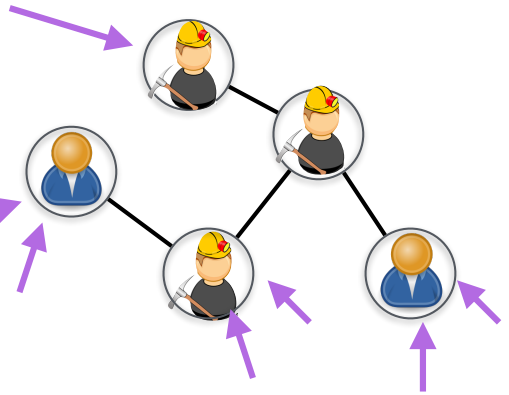


Descentralización

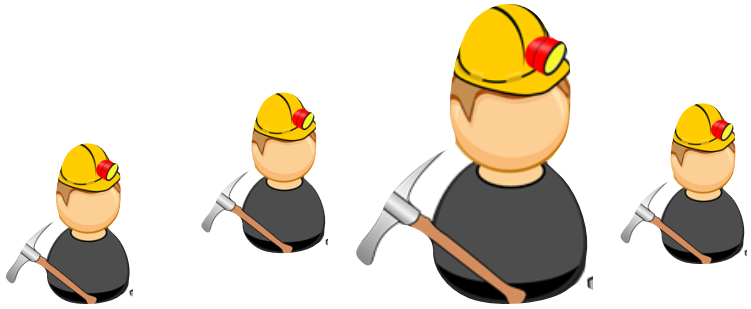


Desafíos

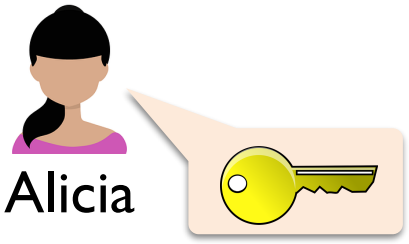
Escalabilidad: incrementar el número de transacciones por segundo



Descentralización



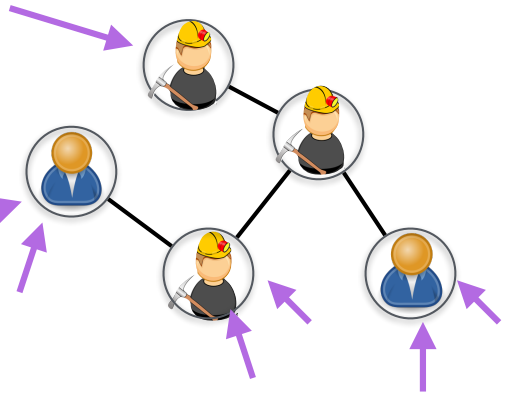
Seguridad de la billetera



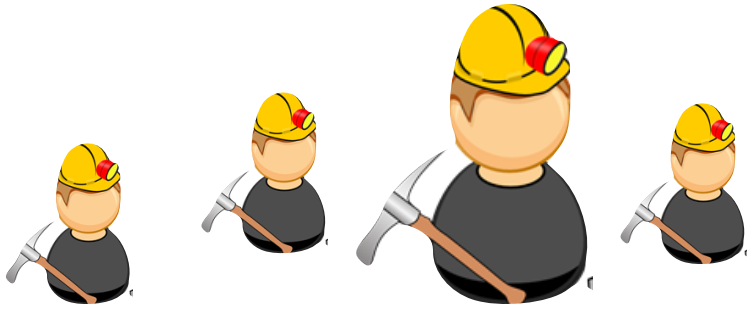
(secreta)

Desafíos

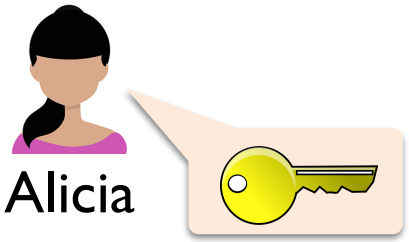
Escalabilidad: incrementar el número de transacciones por segundo



Descentralización



Seguridad de la billetera

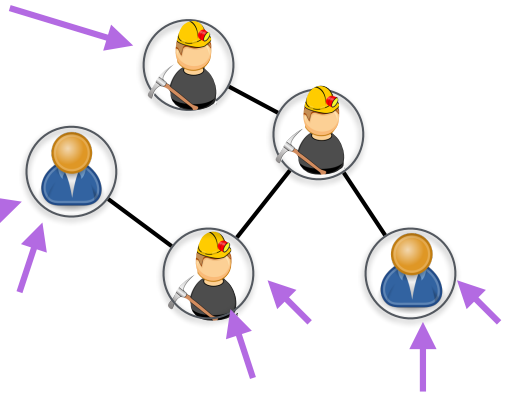


(secreta)

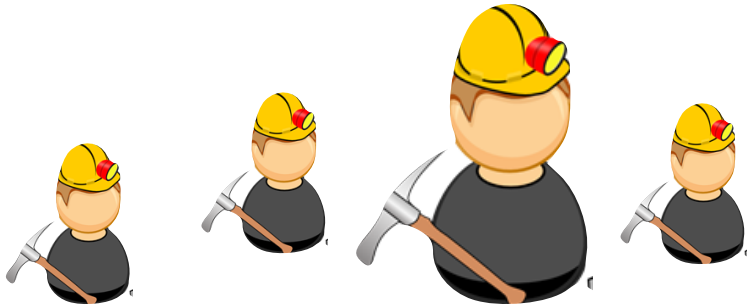
Seguridad del software (contratos)

Desafíos

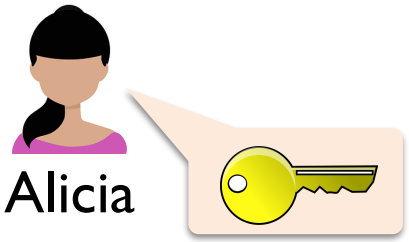
Escalabilidad: incrementar el número de transacciones por segundo



Descentralización



Seguridad de la billetera



(secreta)

Seguridad del software (contratos)

Definición de **Interfaces** con el mundo

¡Gracias!

ahevia@dcc.uchile.cl