BITCOIN

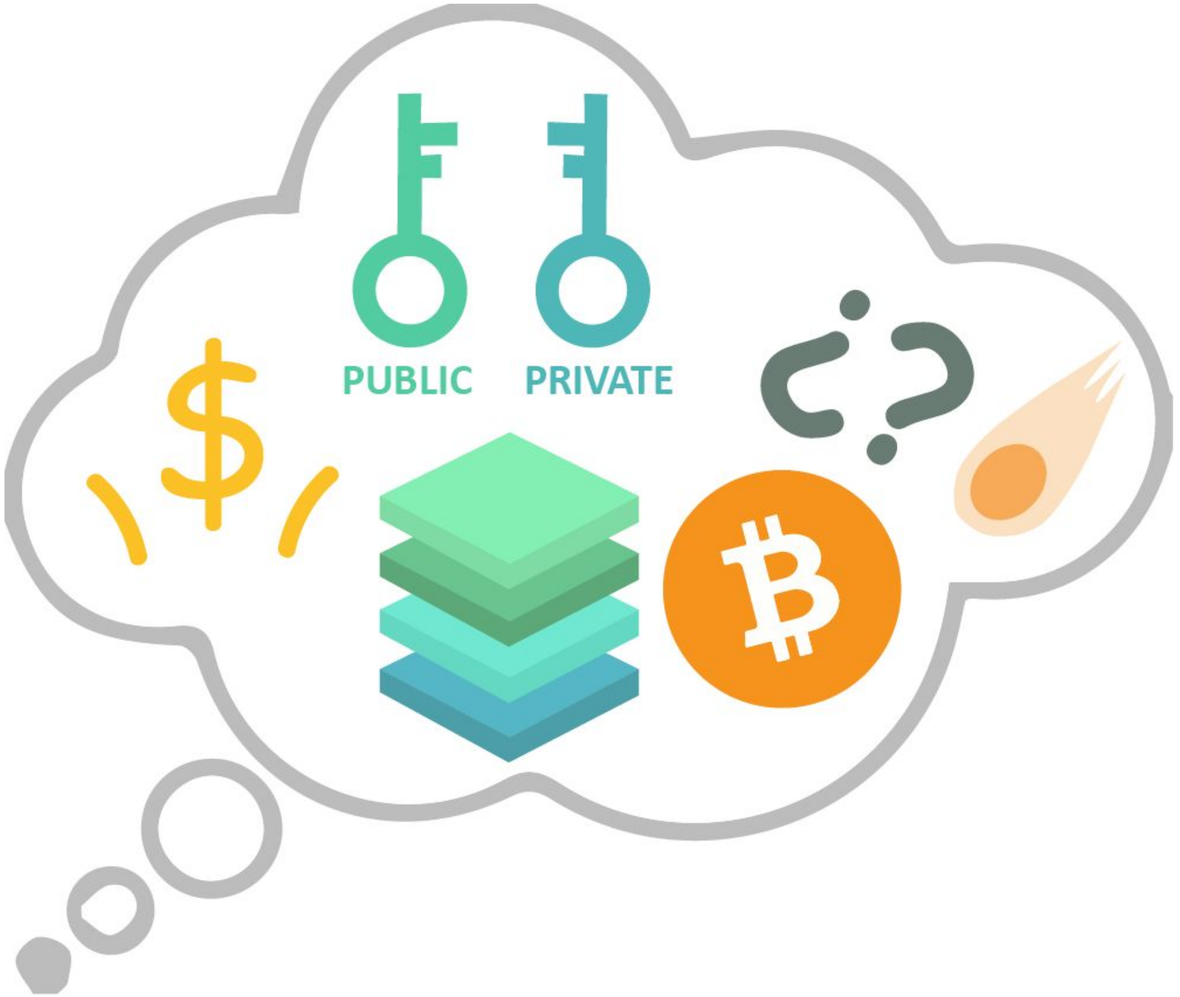
EL CAMINO DE UNA TRANSACCIÓN

Hola!

Soy **Miguel Duarte**

Menú de hoy...

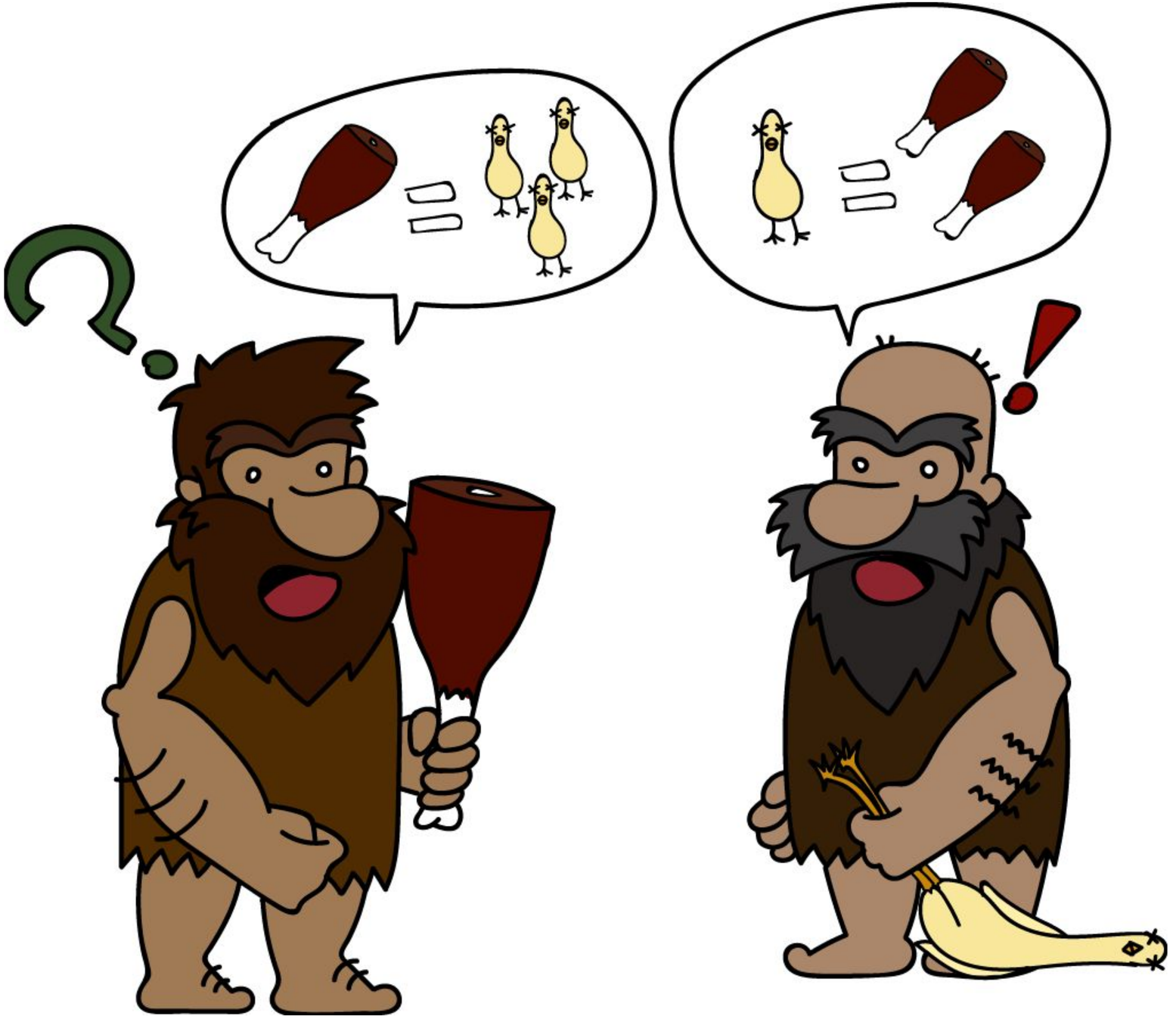
- Intro: ¿Que es una moneda?
  ¿Por qué queremos criptomonedas?
- Transacciones: ¿Que es una transacción en bitcoin?
  ¿Como funciona? ¿Como se hace? ¿Con que se come?
- Consenso en un sistema monetario distribuido: Proof of work.
- Algunas variantes a bitcoin.
- Pequeña sorpresa...
- Preguntas



INTRODUCCIÓN

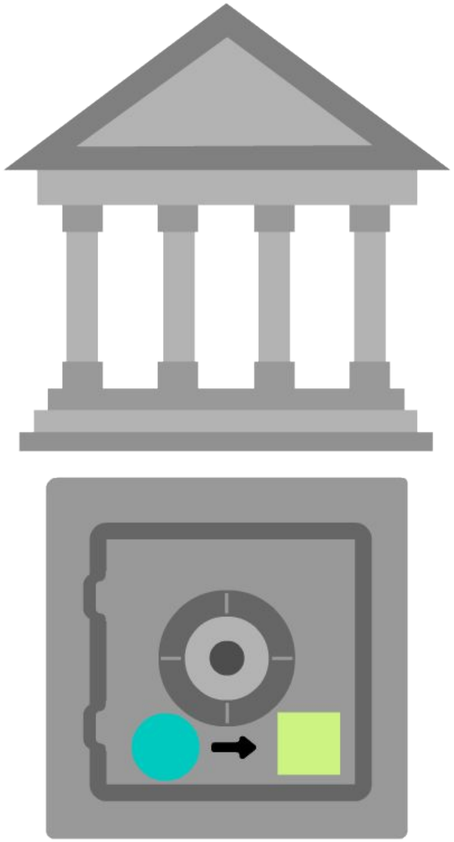
¿Que problema resuelve bitcoin?

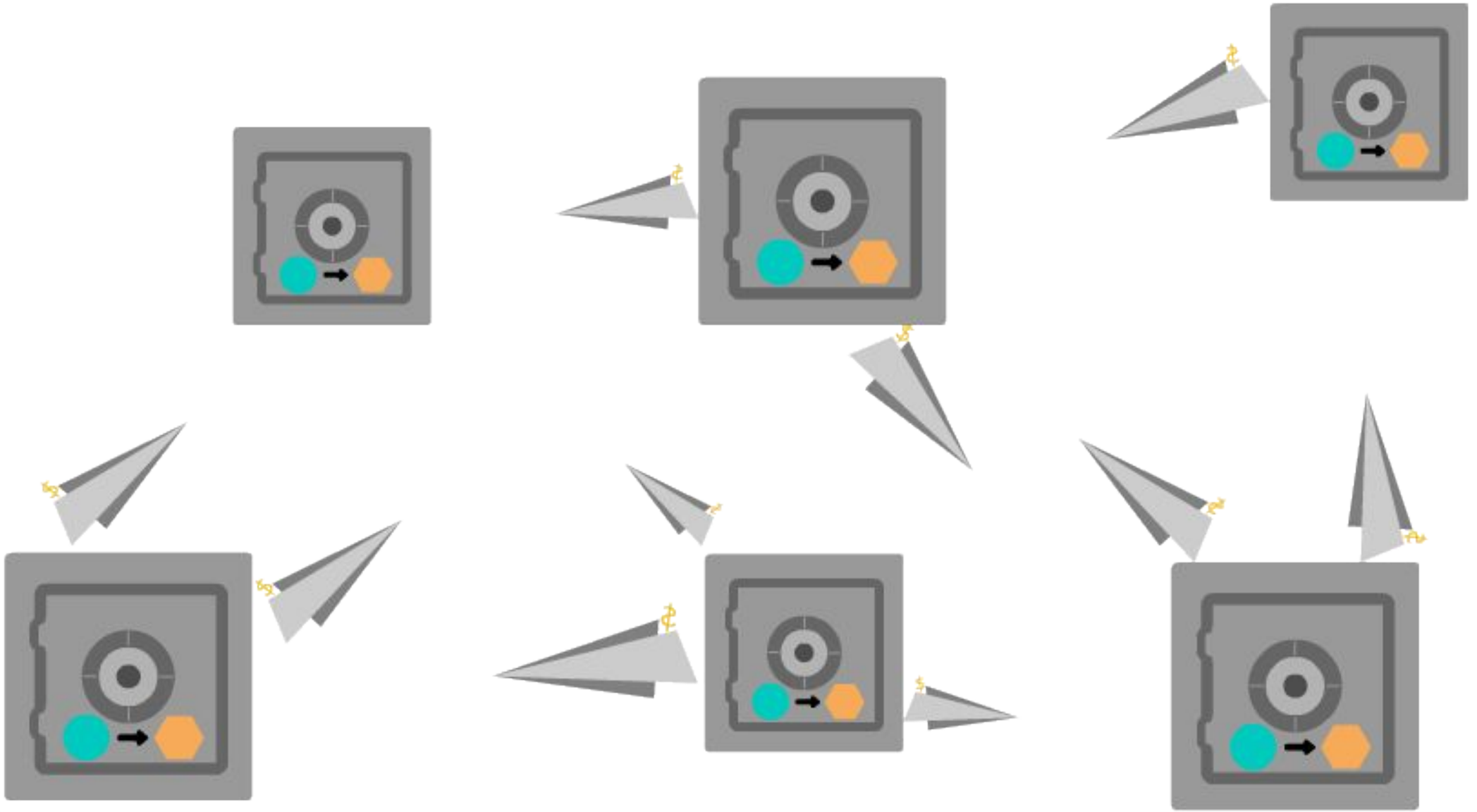
¿Qué es una moneda?

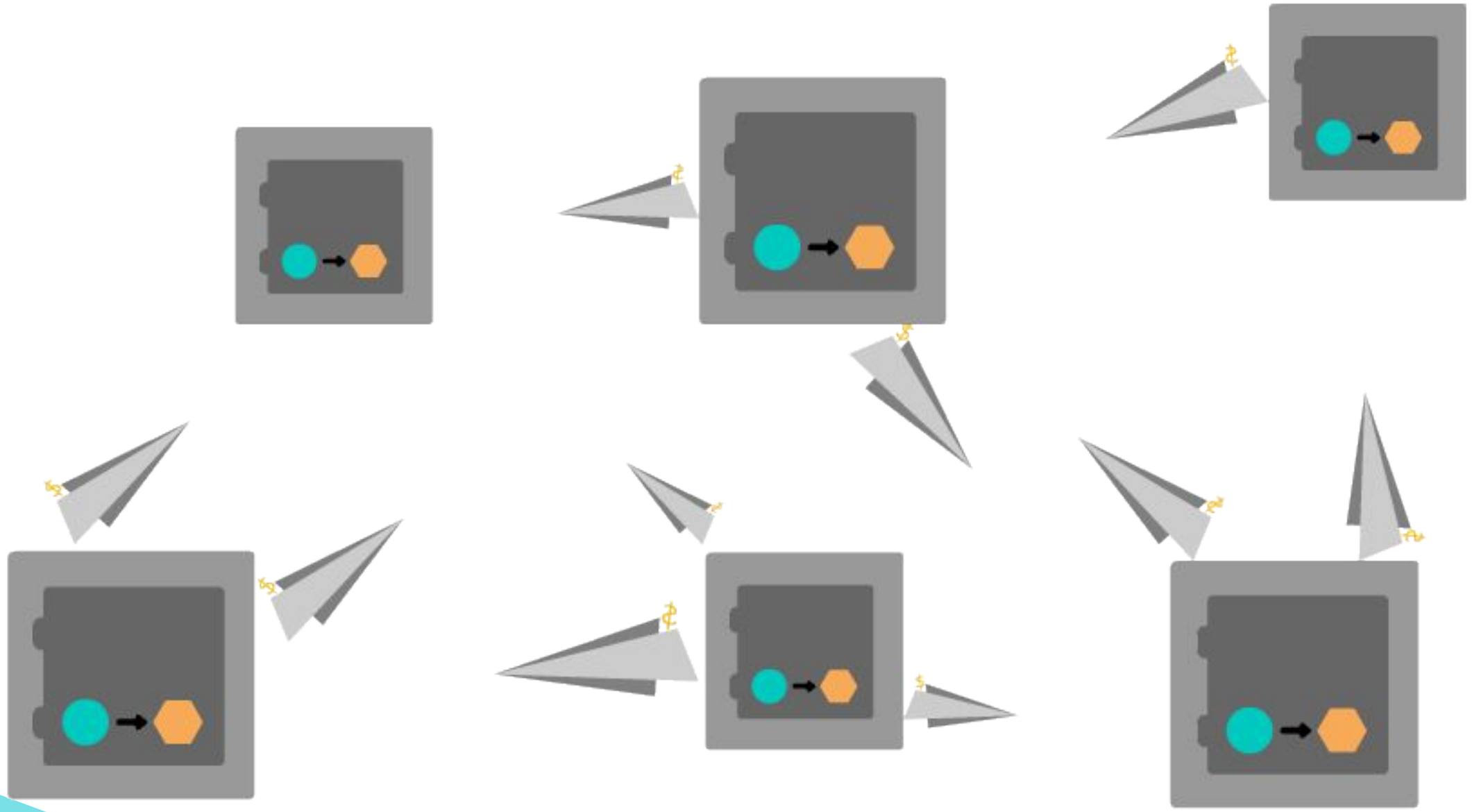


¿Qué es una moneda?

- **Escasez y fungibilidad** (se gasta)
- **Confianza** (segura, durable)
- **Convención**





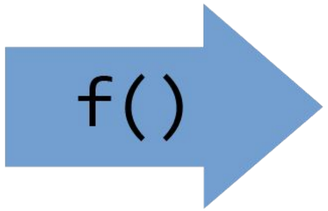


Conceptos Importantes

- Hash
- Clave Pública, Clave Privada

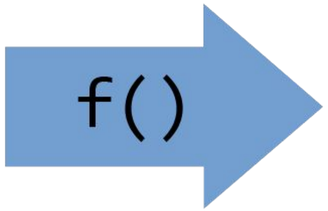
Hash

```
11111111111111111111
11111111111111111111
11111111111111111111
```




```
9117d54bb326c862cb587f86aebfafb2
```

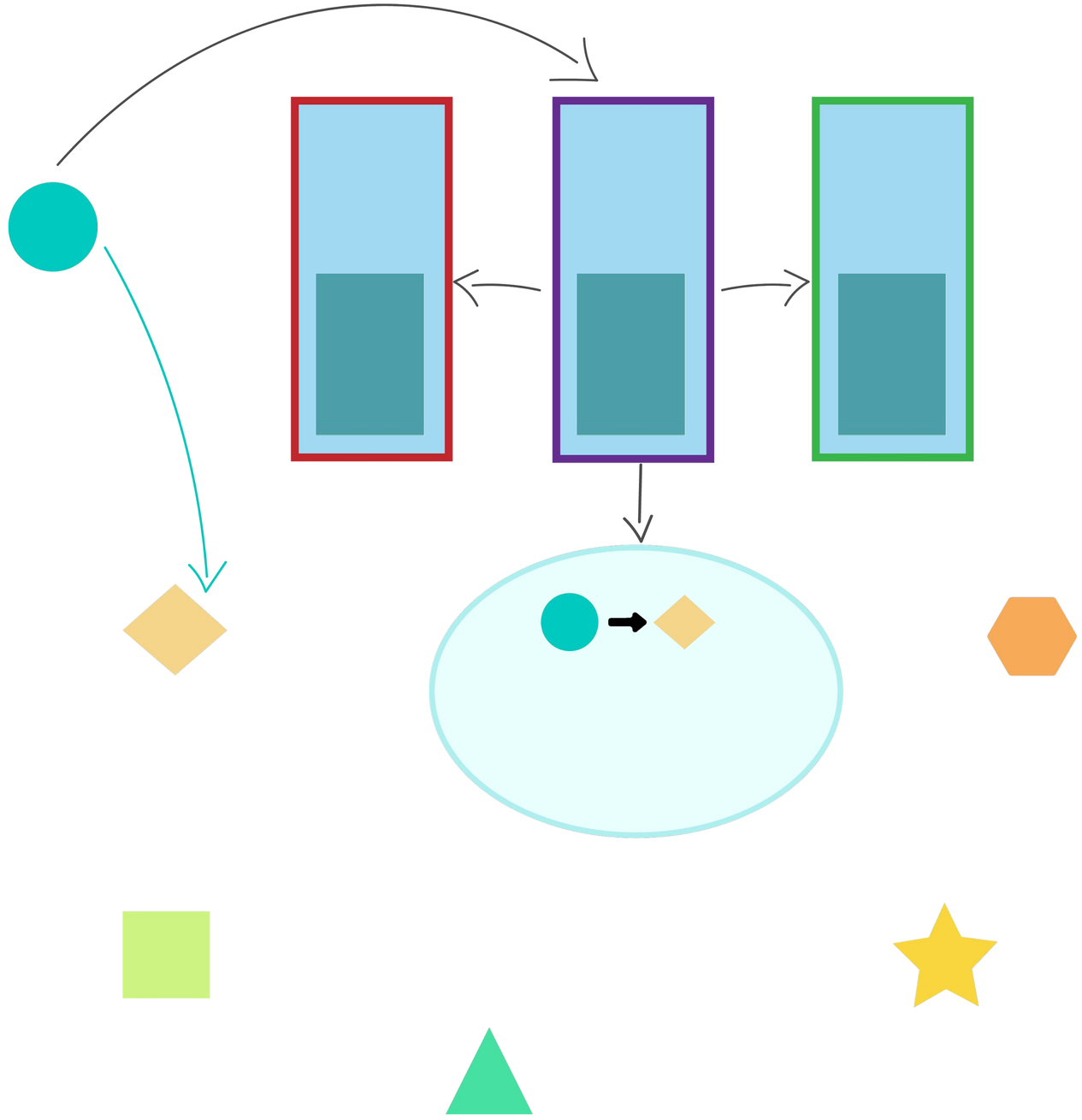
```
11111111111111111111
11111111110111111111
11111111111111111111
```

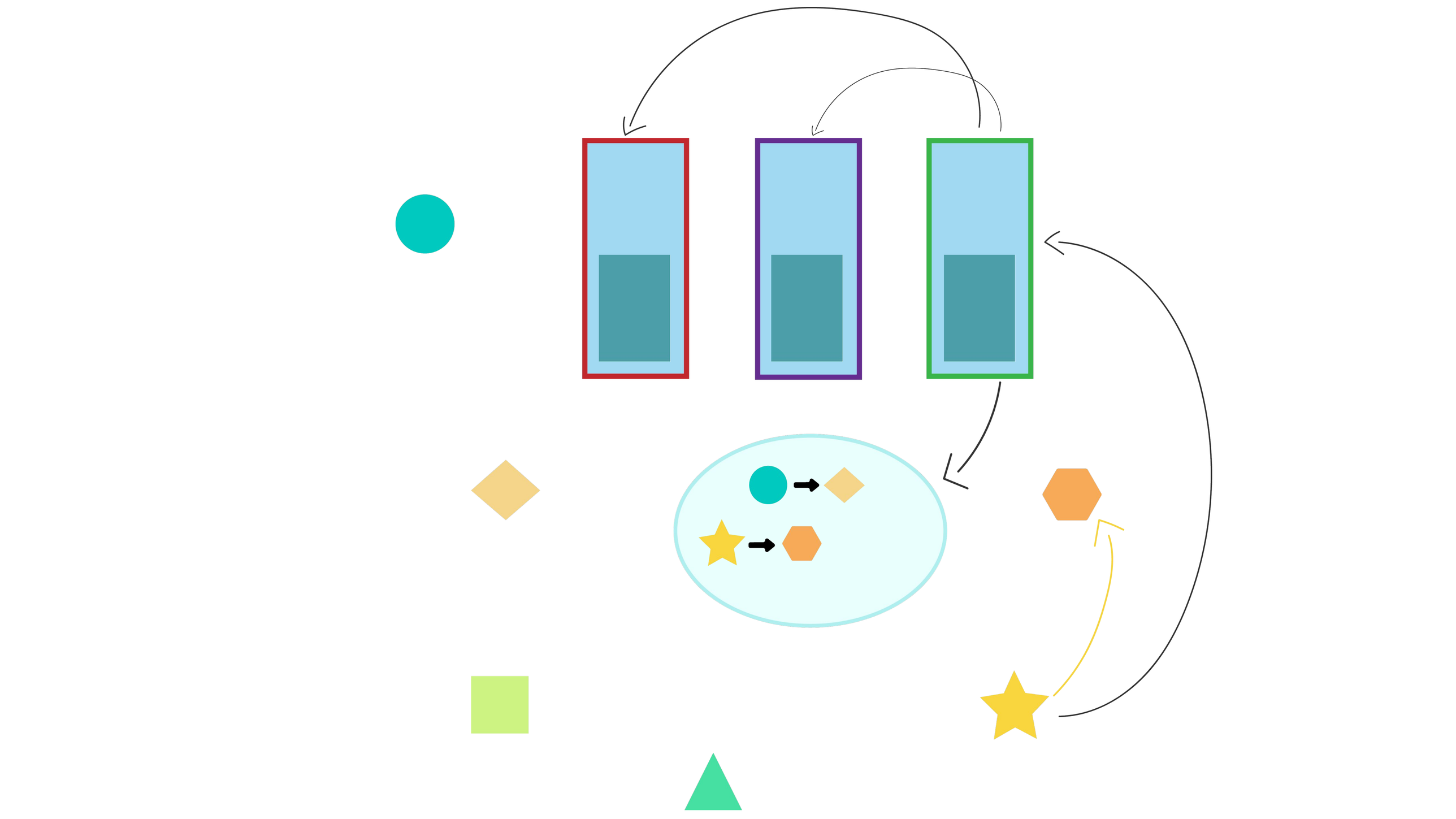


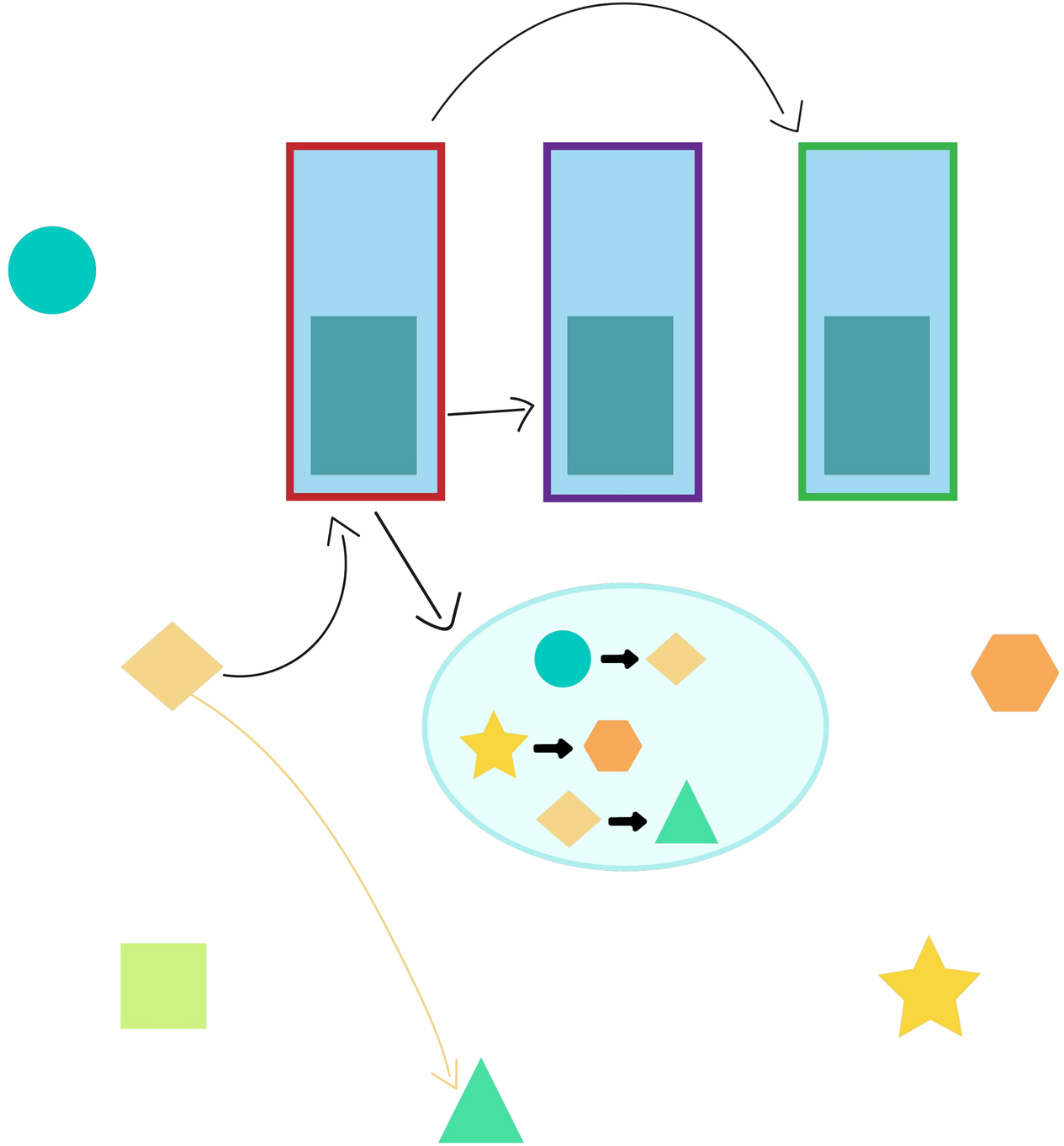

```
af249af06aff4b9a919ee57a6526abe0
```

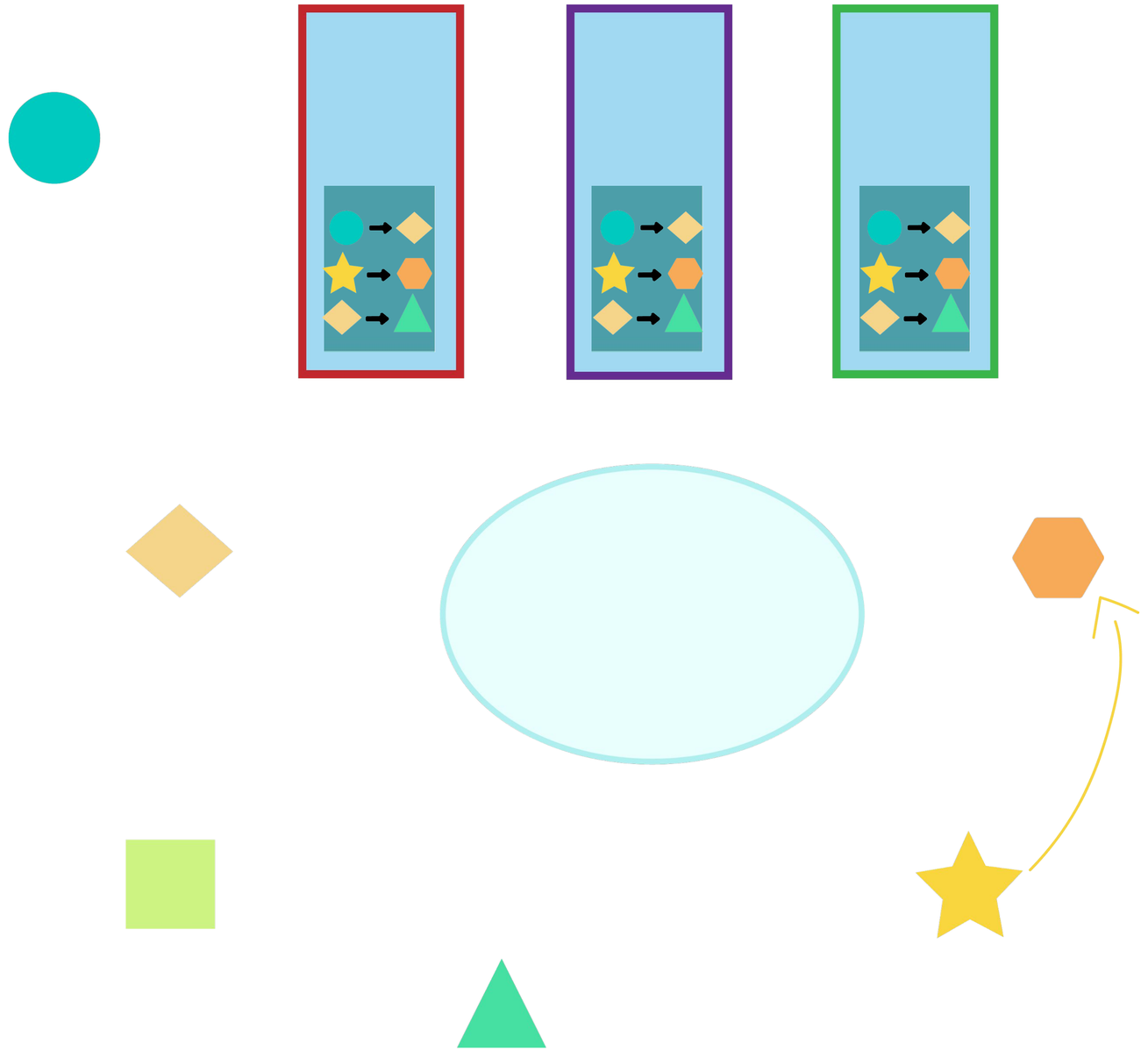

INTERNET
SENDER ENCRYPTS
RECEIVIER DECRYPTS
PUBLIC
PRIVATE

La red Bitcoin



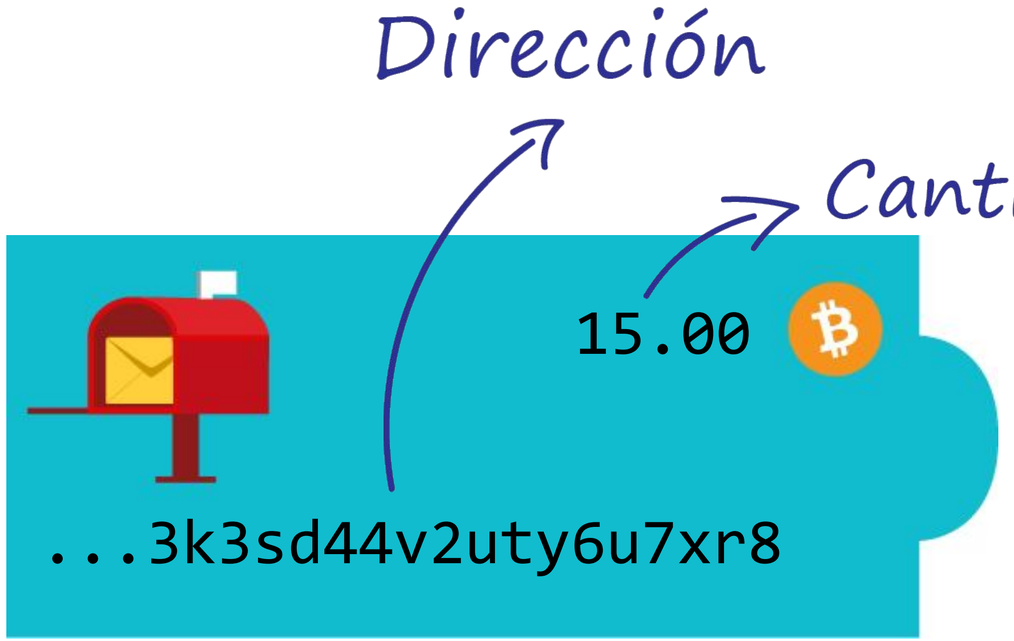


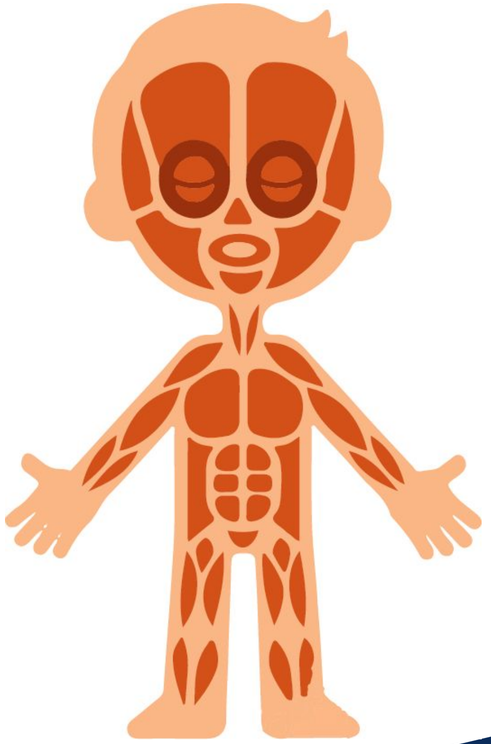




Transacciones:
Interactuando con la red

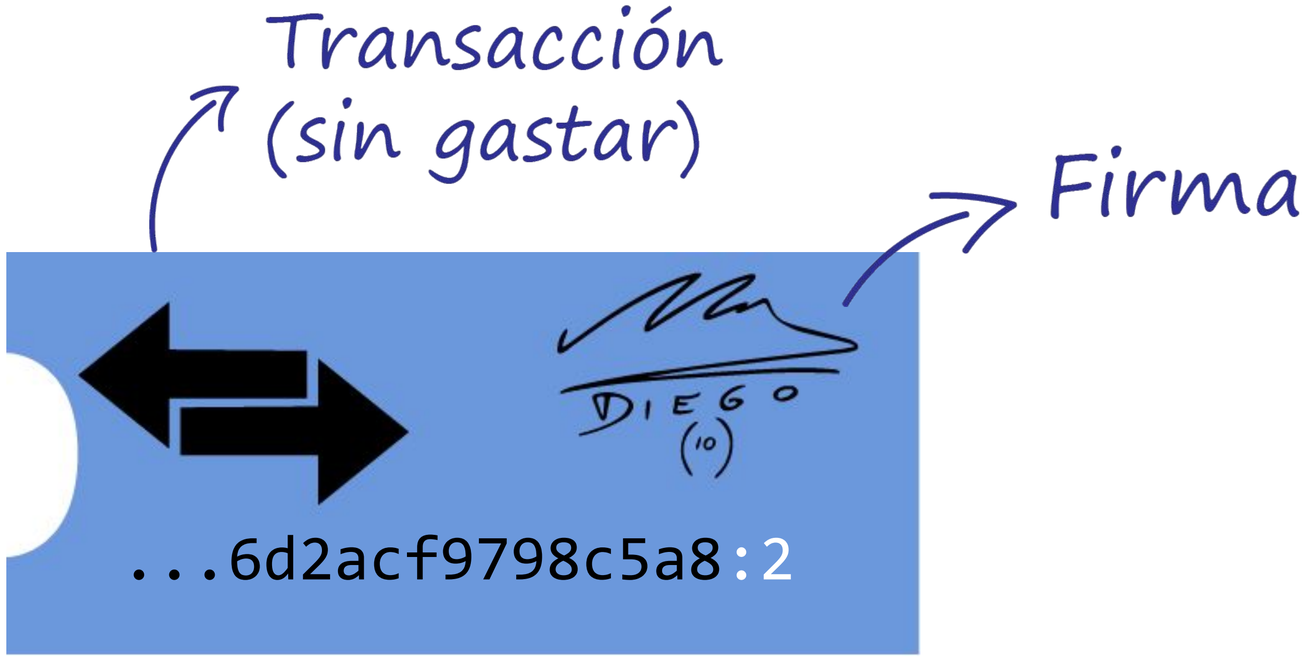
Anatomía de una transacción...

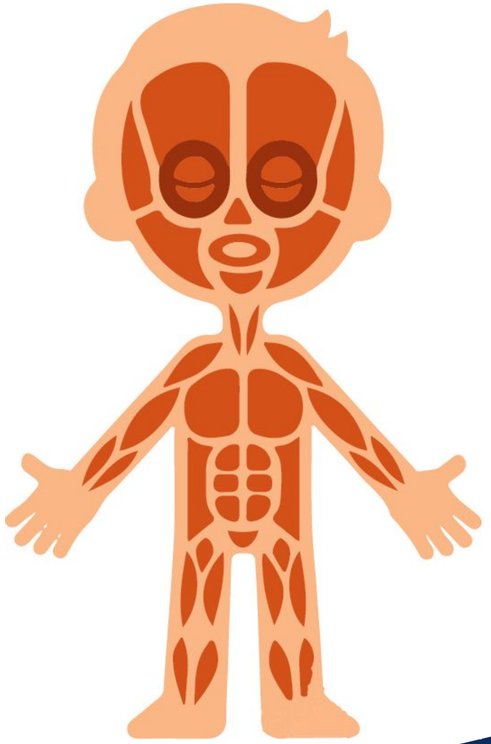




Output

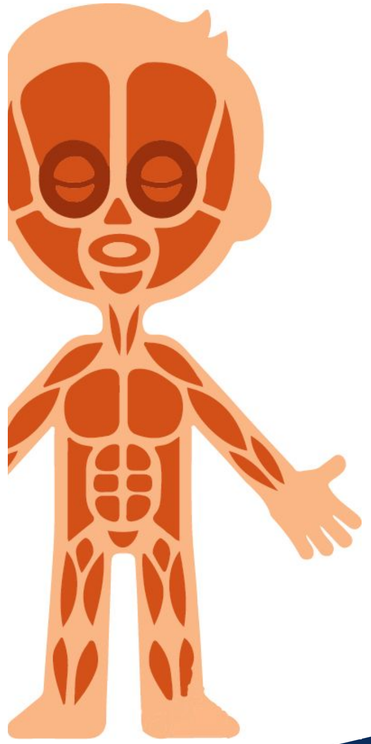
Anatomía de una transacción...



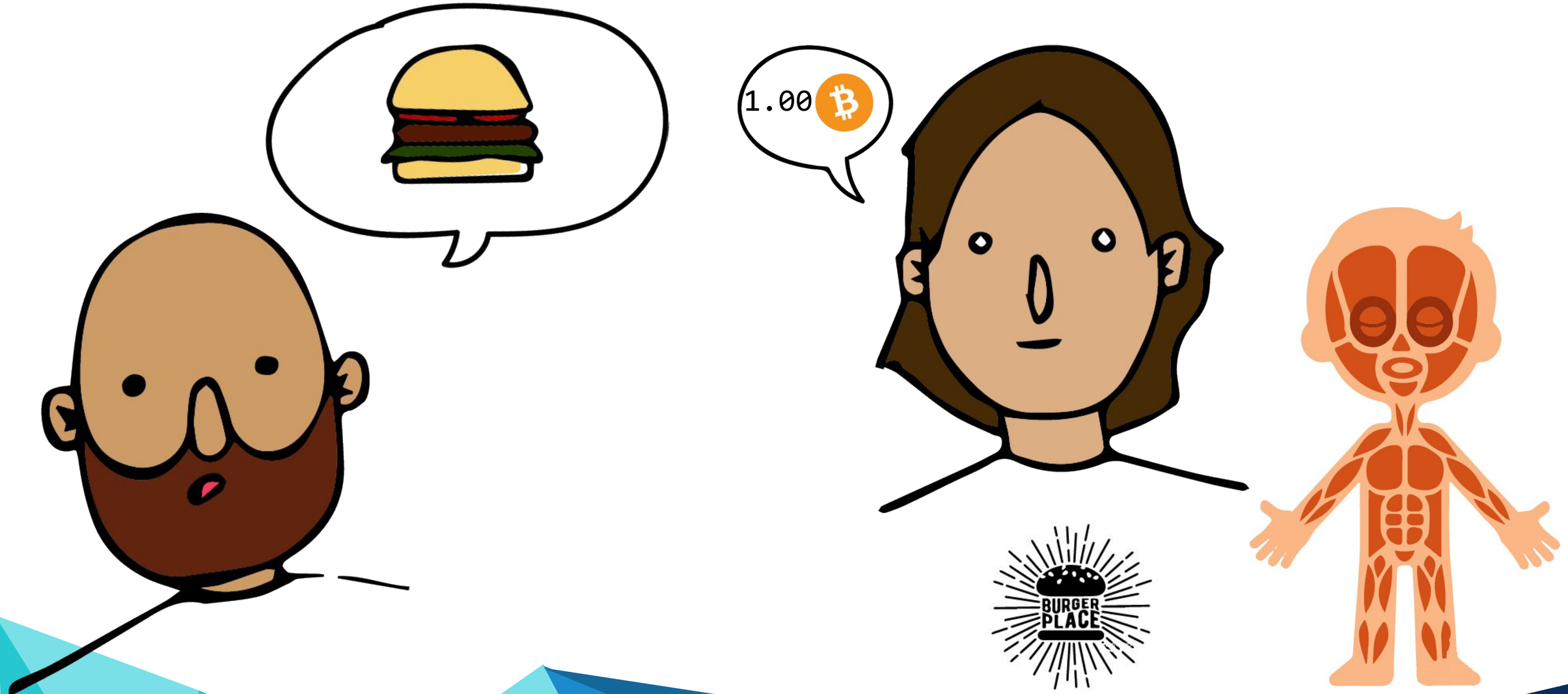


Input

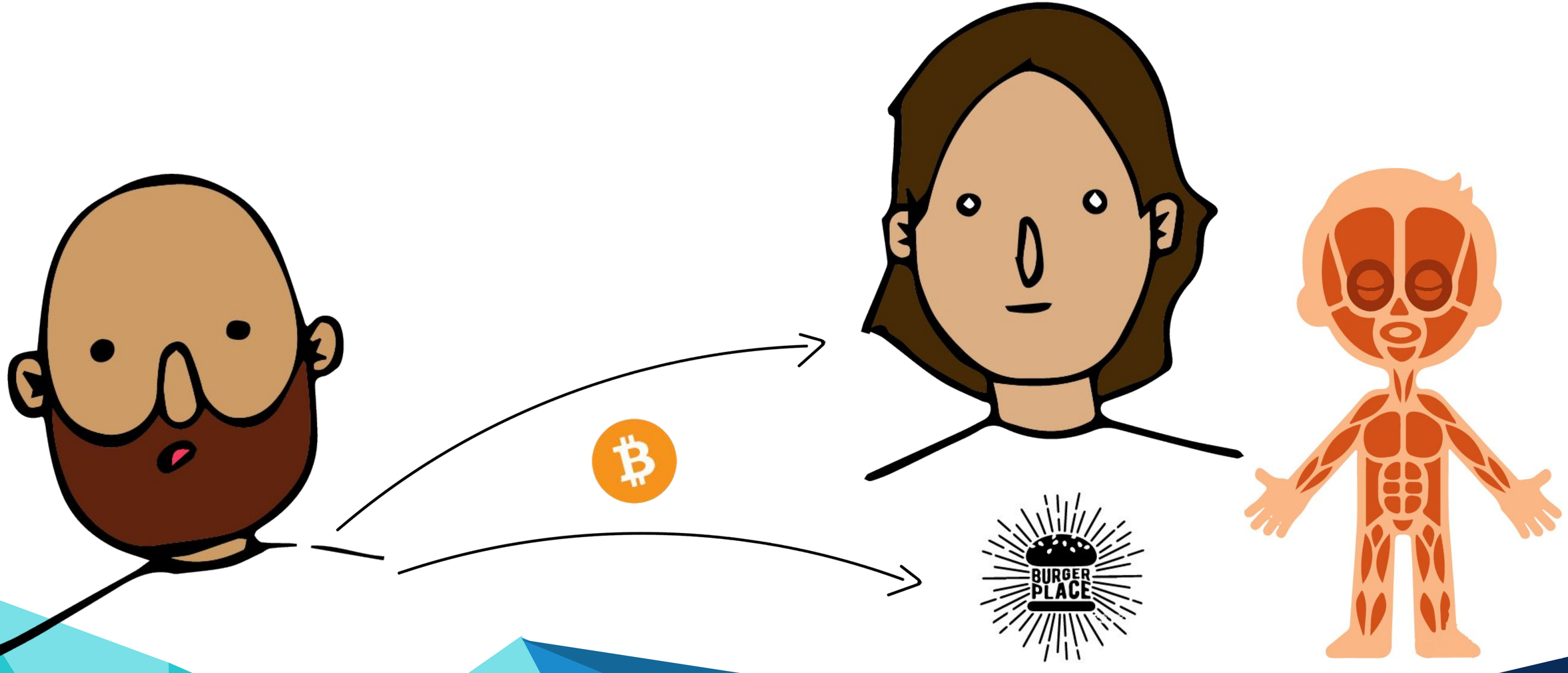
Anatomía de una transacción...



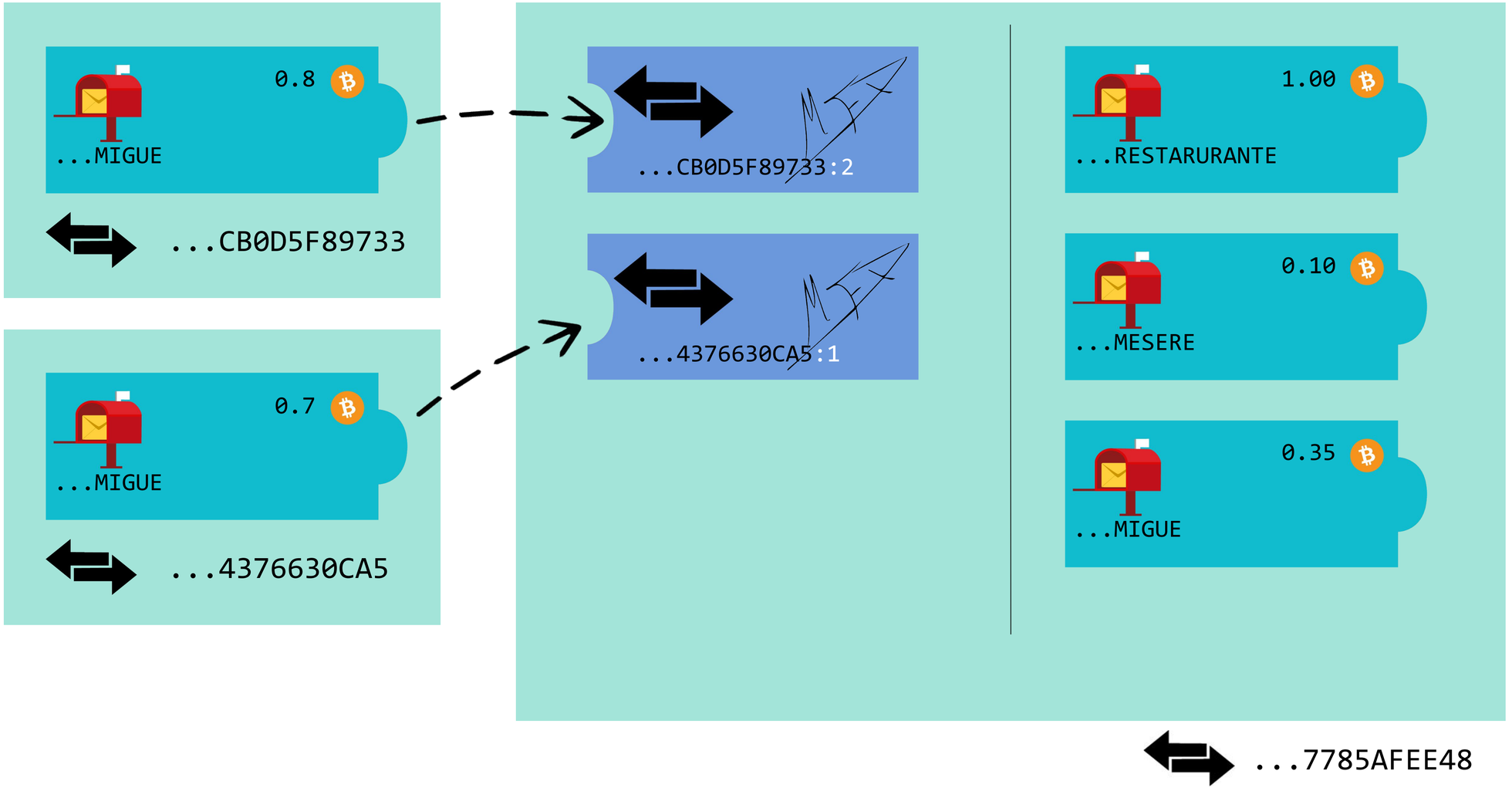
Anatomía de una transacción...

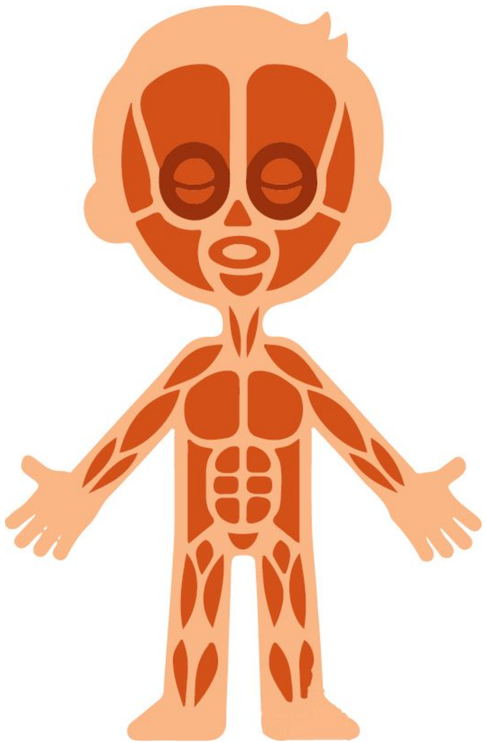


Anatomía de una transacción...

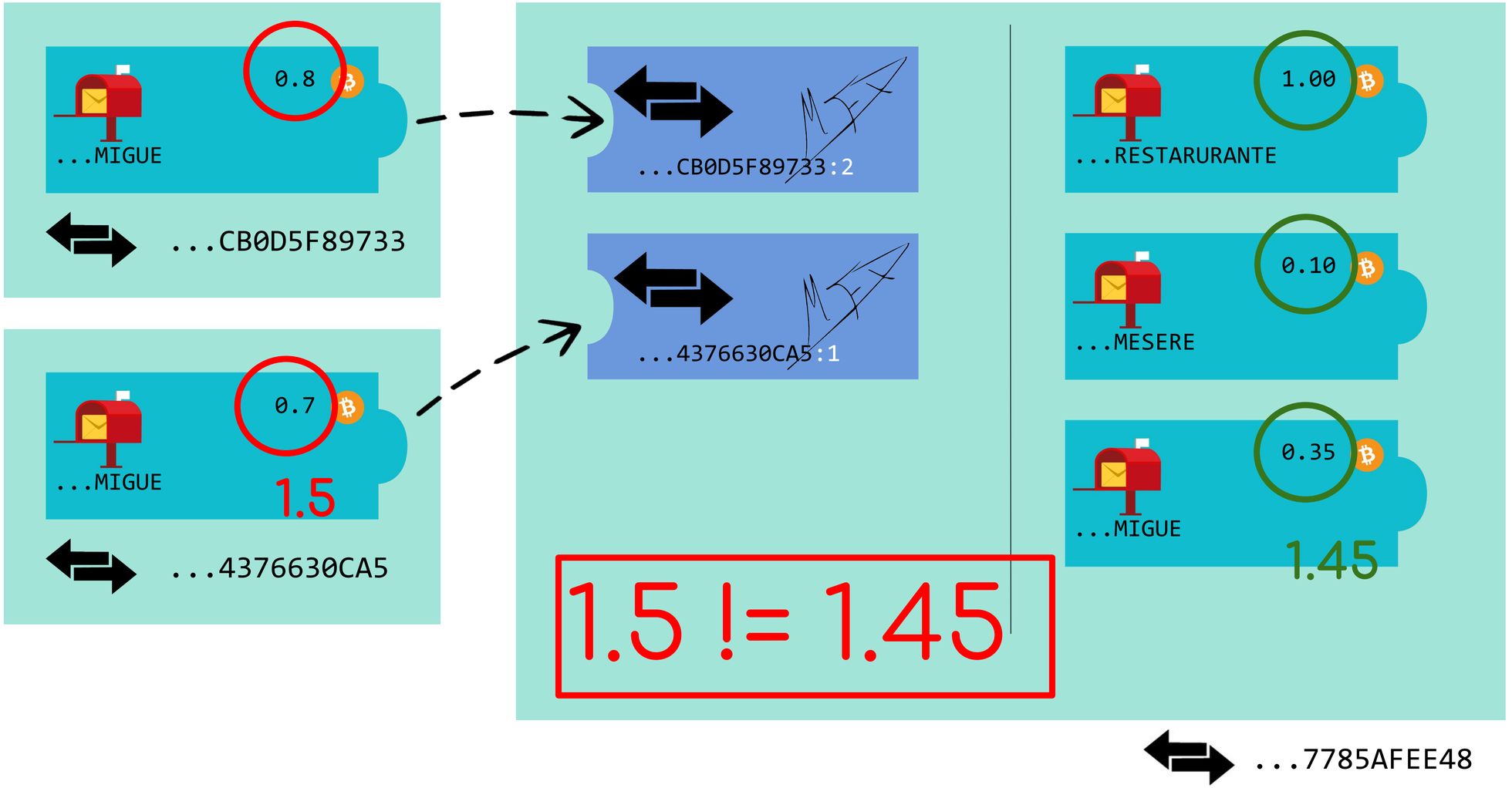


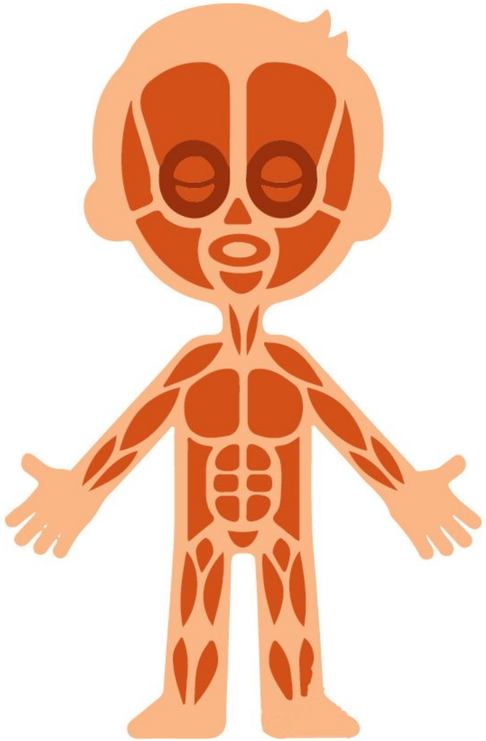
Anatomía de una transacción...





Anatomía de una transacción...

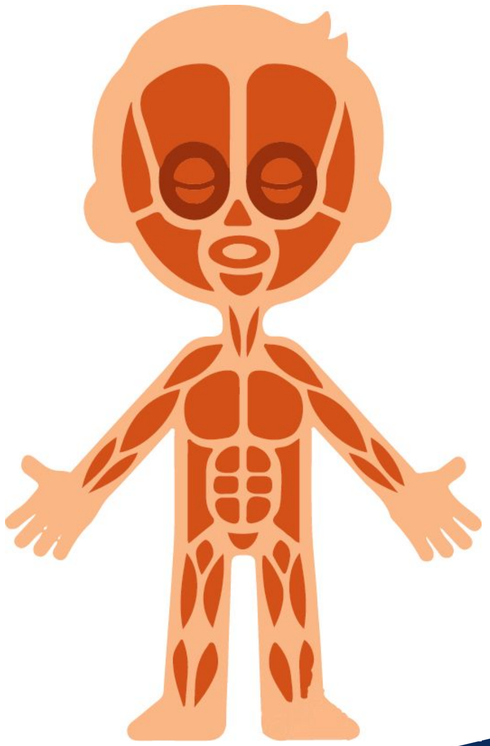




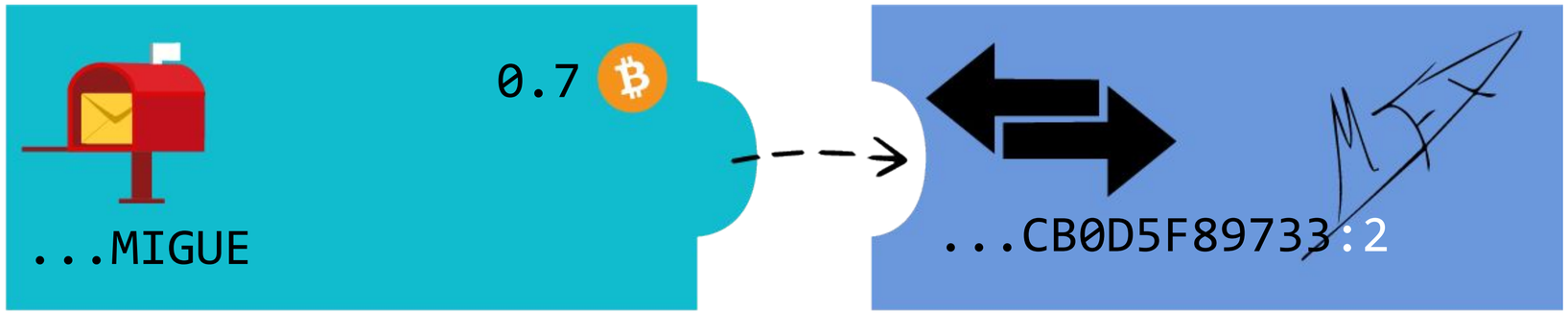
Tal vez con código se entiende mejor...

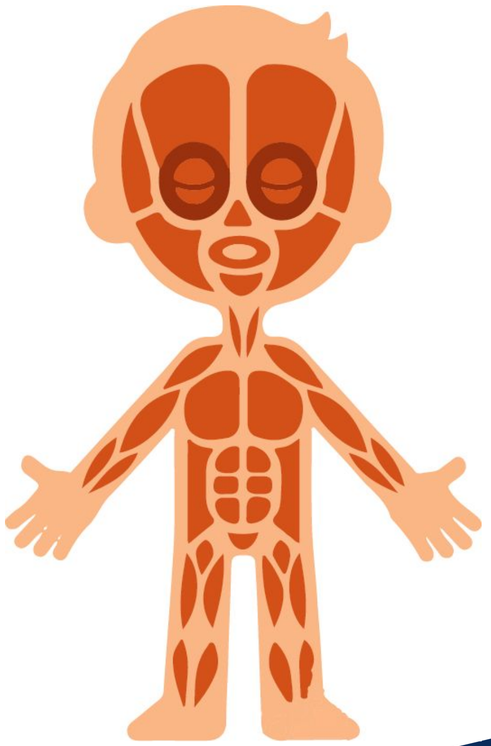
bitcore

```
import Bitcore from ‘bitcore-lib-cash’

var transaction = new Bitcore.Transaction()
  .to(direccionBurgerPlace, 1.0)
  .to(direccionMesere, 0.1)
  .change(direccionMigue)
  .from(outputSinGastar1)
  .from(outputSinGastar2)
  .sign(listaDeClavesPrivadas)

var txSerializada = tranaction.checkedSerialized()
bitcoinRpc.broadcast(txSerializada)
```



Cada input gasta un output

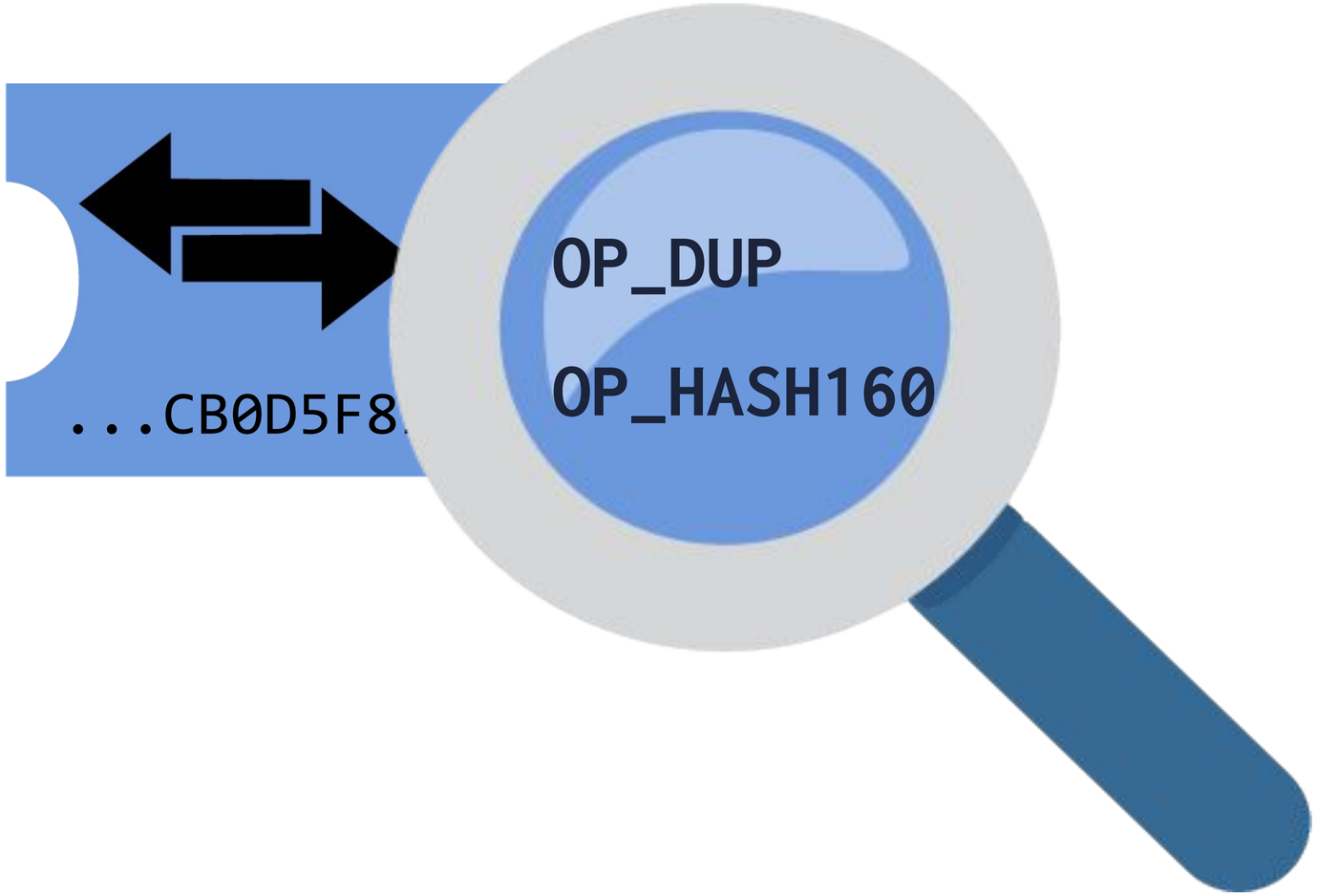


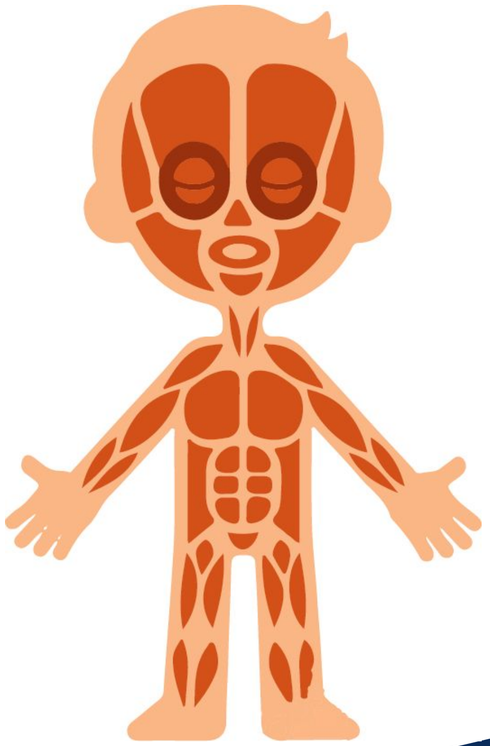


¿Qué hace que los criptos sean una moneda?

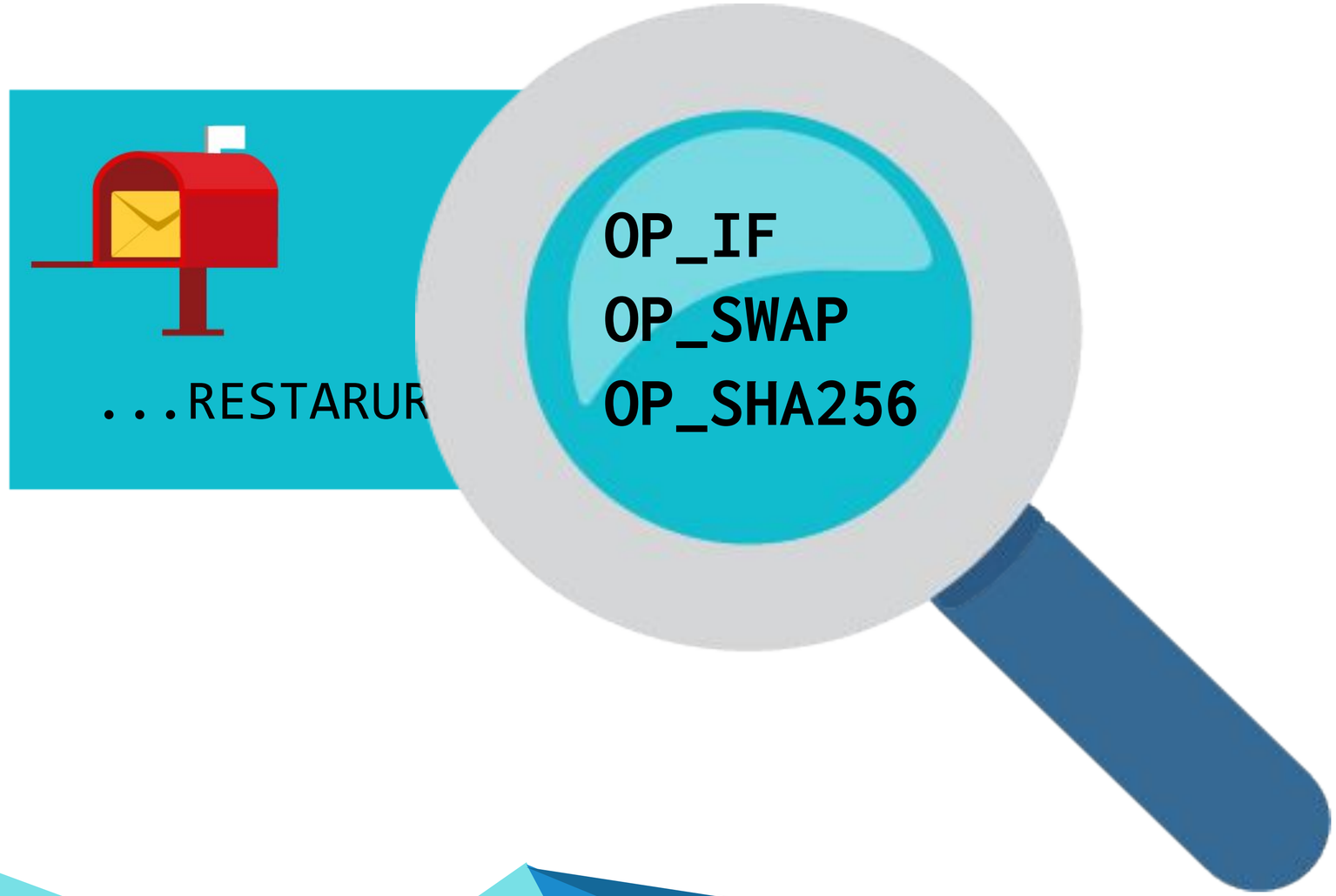
- **fungibilidad** (se gasta)

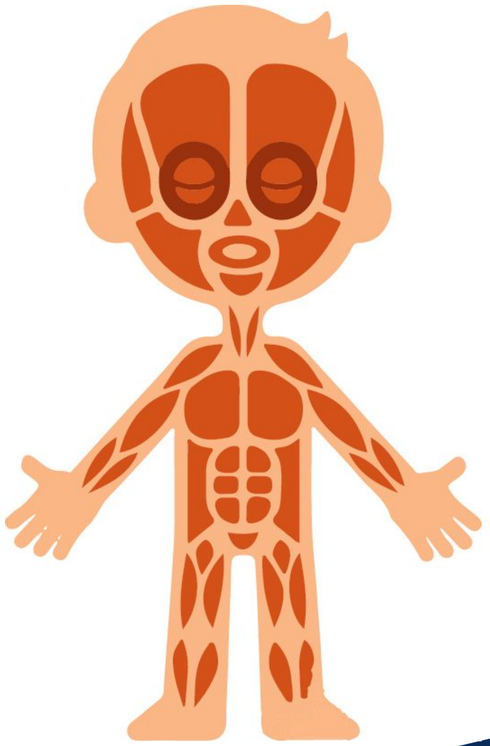
Anatomía de una transacción...





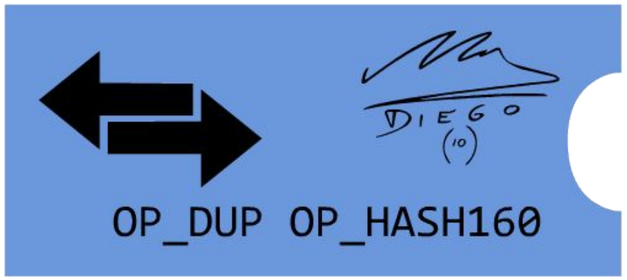
Anatomía de una transacción...





Y como quién no quiere la cosa...

Y como quién no quiere la cosa...



Scripts de Bitcoin

- Máquina virtual basada en una pila
- Opcodes standard
- NO son turing compatibles
- No hay bucles

Scripts de Bitcoin

pay-to-pubkey-hash

pay-to-pubkey-hash

OUTPUT: OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

INPUT: **<firma>** <clavePublica>

pay-to-pubkey-hash

Vacía.| **<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

Vacía.	**<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma>	**<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_	**OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_ _<clavePublica>_	**OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> _<clavePublicaHashada>_	**<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_	**OP_EQUALVERIFY** OP_CHECKSIG
<firma> <clavePublica>	**OP_CHECKSIG** +
true	_Termina con éxito_

pay-to-pubkey-hash

<firma>|**<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

Vacía.	**<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma>	**<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_	**OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_ _<clavePublica>_	**OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> _<clavePublicaHashada>_	**<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_	**OP_EQUALVERIFY** OP_CHECKSIG
<firma> <clavePublica>	**OP_CHECKSIG** +
true	_Termina con éxito_

pay-to-pubkey-hash

<firma> _<clavePublica>_ | **OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

Vacía. | **<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> | **<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ | **OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ _<clavePublica>_ | **OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> _<clavePublicaHashada>_ | **<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_ | **OP_EQUALVERIFY** OP_CHECKSIG

<firma> <clavePublica> | **OP_CHECKSIG** +

true | _Termina con éxito_

pay-to-pubkey-hash

<firma> <clavePublica> _<clavePublica>_ | **OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

Vacía. | **<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> | **<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ | **OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> _<clavePublica>_ | **OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> _<clavePublicaHashada>_ | **<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_ | **OP_EQUALVERIFY** OP_CHECKSIG

<firma> <clavePublica> | **OP_CHECKSIG** +

true | _Termina con éxito_

pay-to-pubkey-hash

<firma> <clavePublica> _<clavePublicaHashada>_ | **<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG

Vacía.	**<firma>** <clavePublica> OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma>	**<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_	**OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_ _<clavePublica>_	**OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> _<clavePublicaHashada>_	**<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_	**OP_EQUALVERIFY** OP_CHECKSIG
<firma> <clavePublica>	**OP_CHECKSIG** +
true	_Termina con éxito_

pay-to-pubkey-hash

<firma> <clavePublica> _<clavePublicaHashada>_ _<clavePublicaHashada>_ | **OP_EQUALVERIFY** OP_CHECKSIG

Vacía. | **<firma>** <clavePublica> OP DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> | **<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ | **OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ _<clavePublica>_ | **OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> _<clavePublicaHashada>_ | **<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG

<firma> <clavePublica> _<clavePublicaHashada>_ _<clavePublicaHashada>_ | **OP_EQUALVERIFY** OP_CHECKSIG

<firma> <clavePublica> | **OP_CHECKSIG** +

true | _Termina con éxito_

pay-to-pubkey-hash

<firma> _<clavePublica>_| **OP_CHECKSIG**

Vacía.	**<firma>** <clavePublica> OP DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma>	**<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_	**OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> _<clavePublica>_ _<clavePublica>_	**OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> _<clavePublicaHashada>_	**<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG
<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_	**OP_EQUALVERIFY** OP_CHECKSIG
<firma> _<clavePublica>_	**OP_CHECKSIG**
true	Termina con éxito_

pay-to-pubkey-hash

true | **Termina con éxito**

Vacía. | **<firma>** <clavePublica> OP DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> | **<clavePublica>** OP_DUP OP_HASH160 <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ | **OP_DUP** OP_HASH160 <clave PublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

<firma> _<clavePublica>_ _<clavePublica>_ | **OP_HASH160** <clavePublicaHashada> OP_EQUALVERIFY OP_CHECKSIG

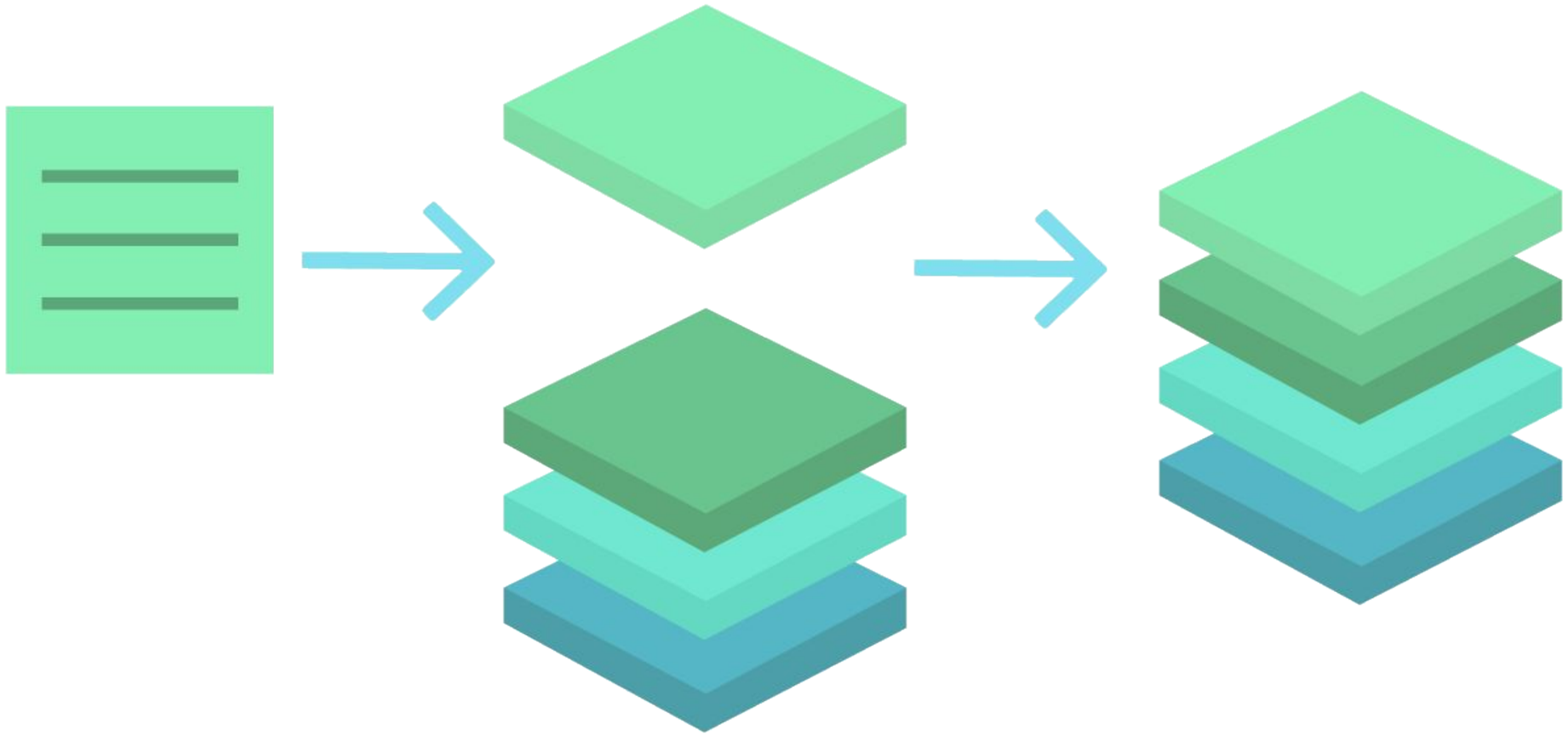
<firma> <clavePublica> _<clavePublicaHashada>_ | **<clavePublicaHashada>** OP_EQUALVERIFY OP_CHECKSIG

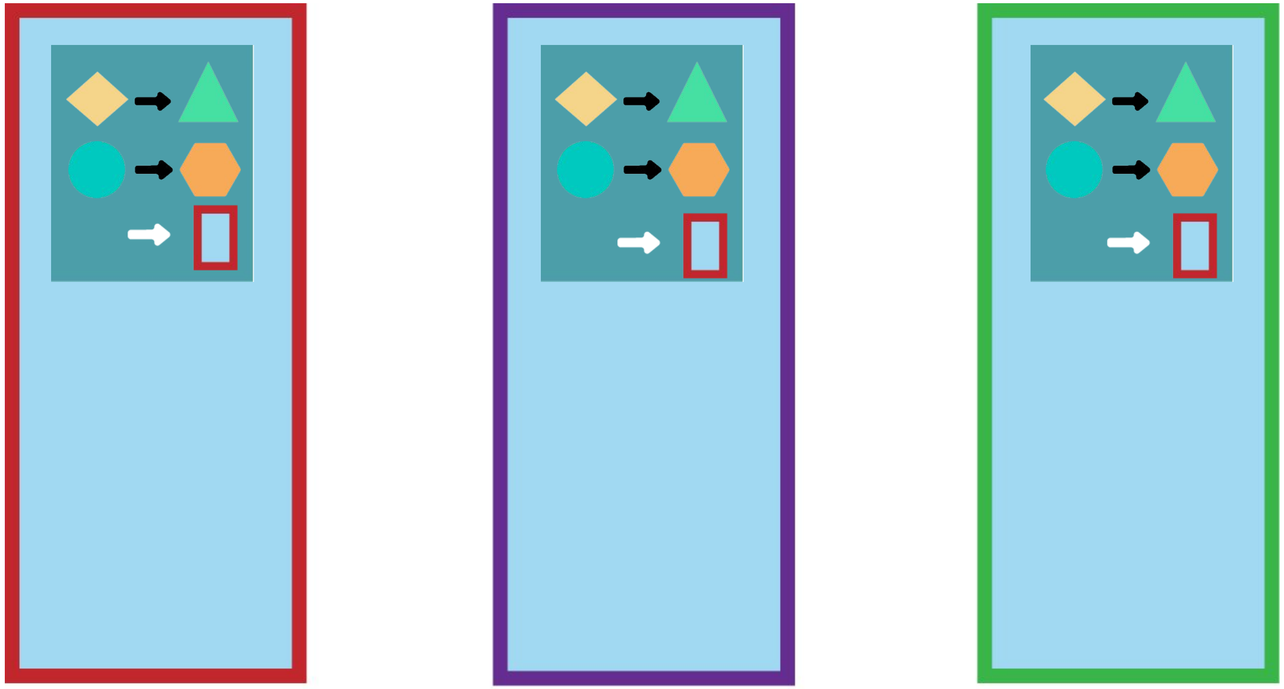
<firma> <clavePublica> | <clavePublicaHashada> _<clavePublicaHashada>_ | **OP_EQUALVERIFY** OP_CHECKSIG

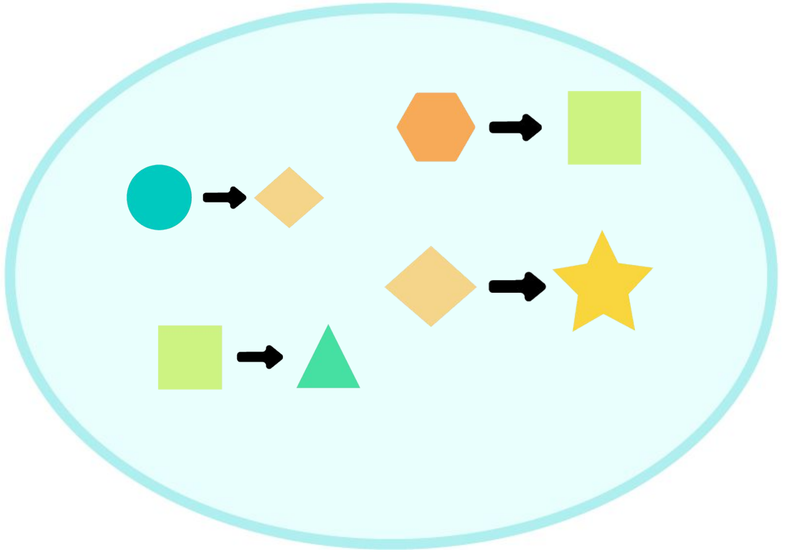
<firma> <clavePublica> | **OP_CHECKSIG**

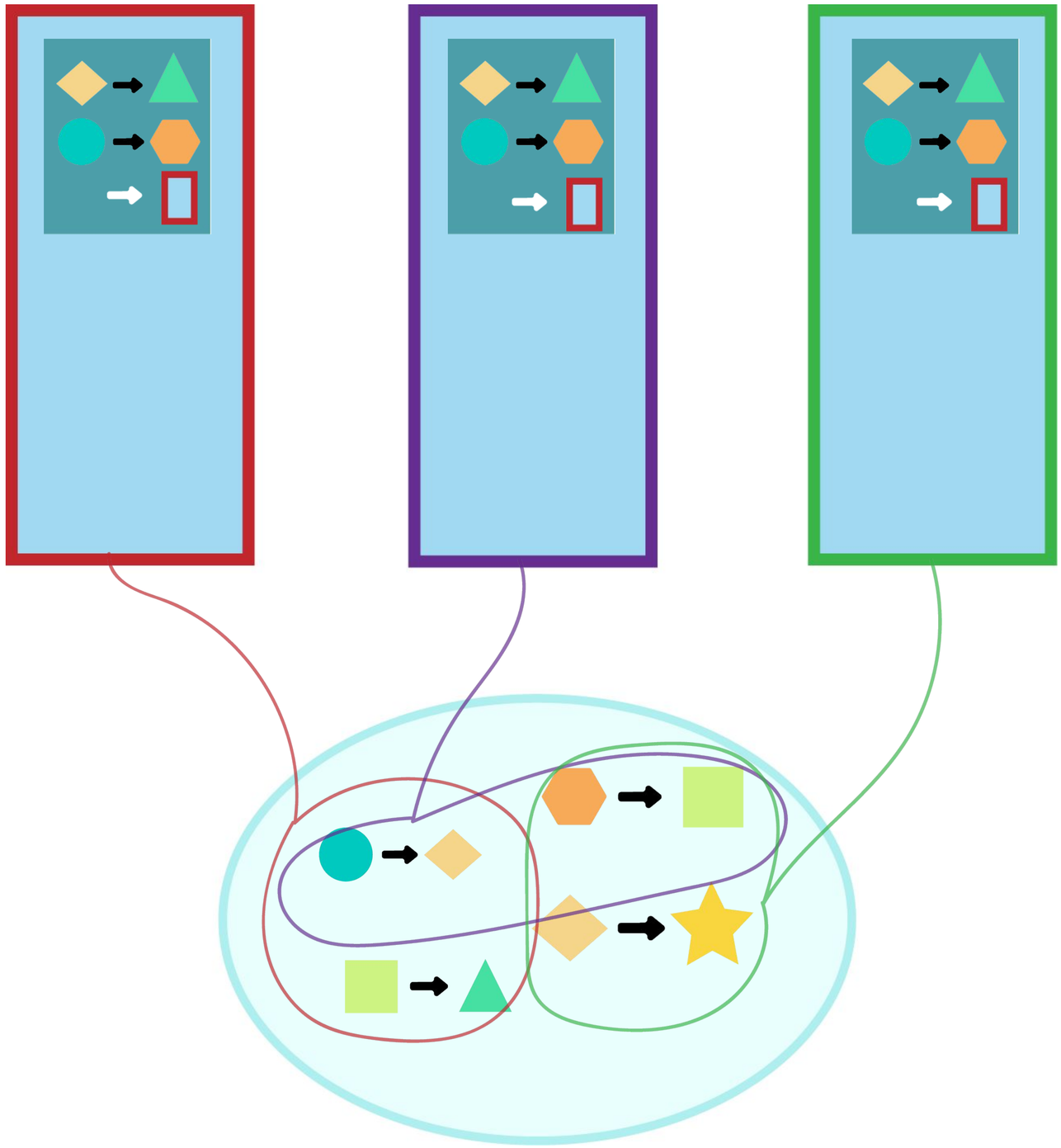
true | **Termina con éxito**

Consenso en un sistema distribuido

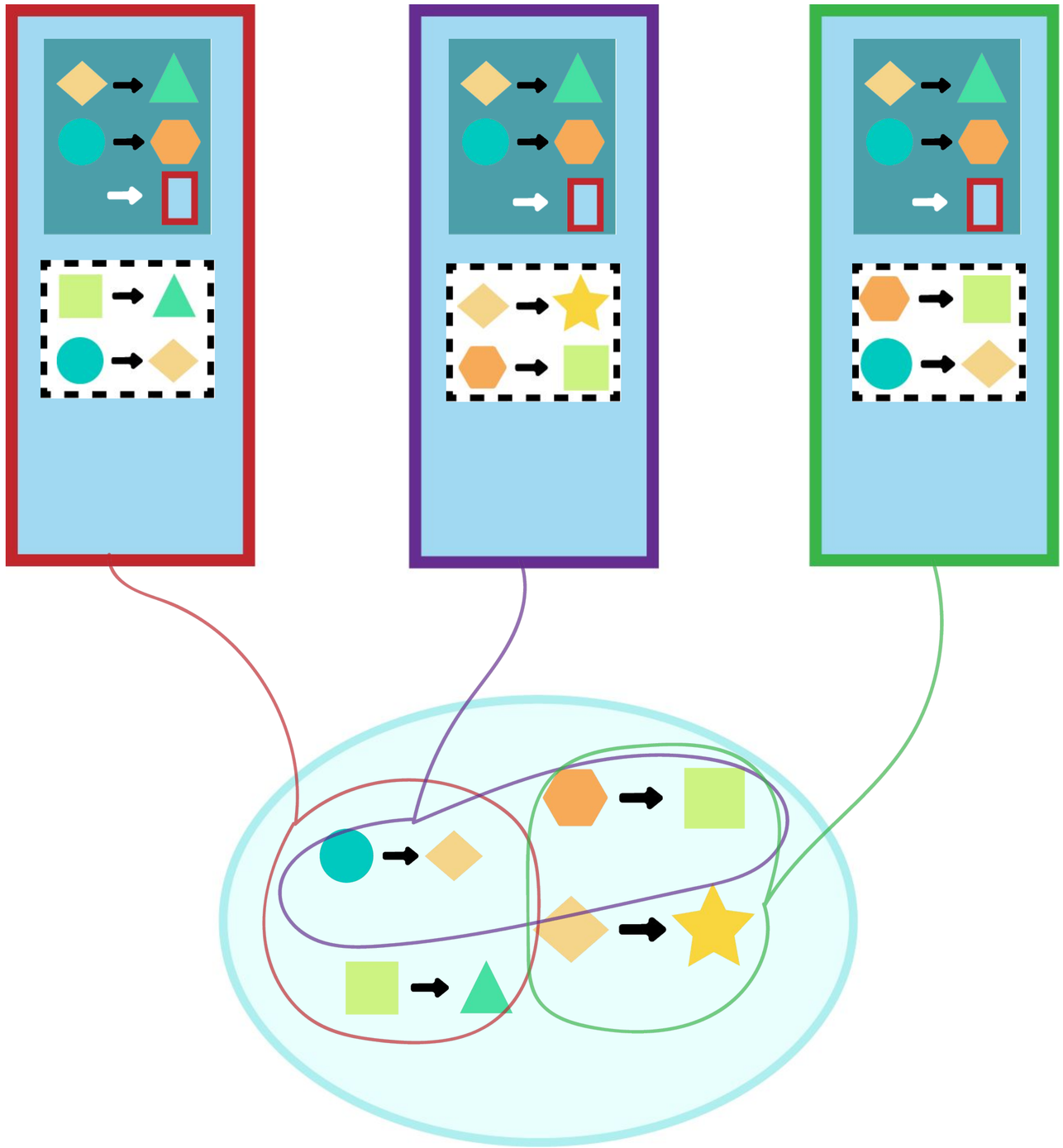






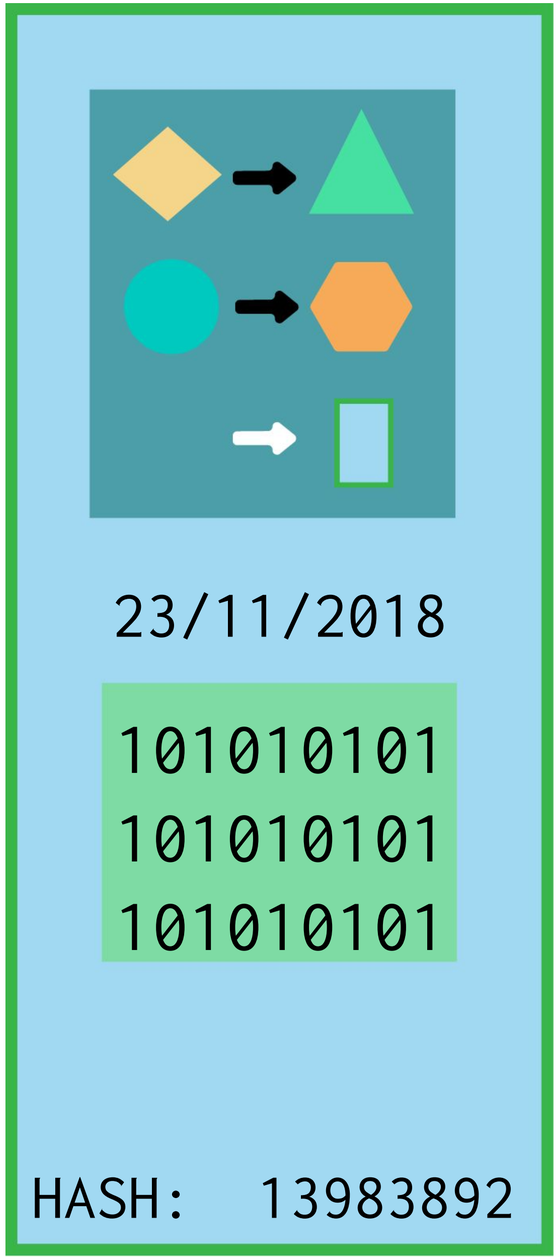


1MB



1MB

10101010110101010110
1010101



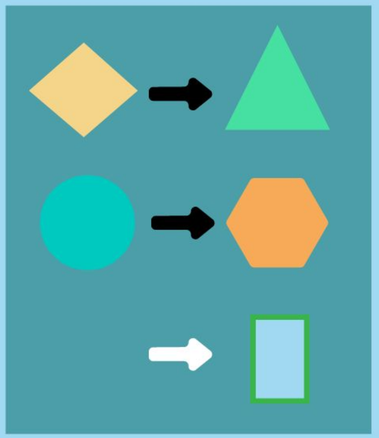
23/11/2018

101010101
101010101
101010101

HASH: 13983892

HASH<100000

~~10101010110101010110~~
~~1010101~~
11110000000001111111
1100000



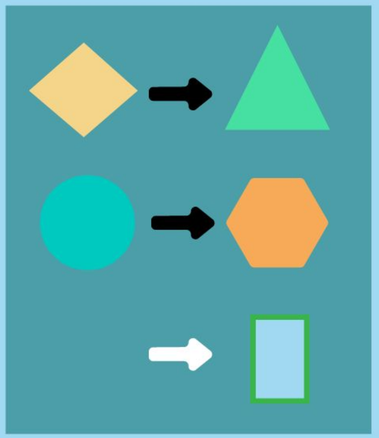
23/11/2018

111100000
000011111
111100000

HASH: 902949123

HASH<100000

~~10101010110101010110~~
~~1010101~~
~~11110000000001111111~~
~~1100000~~
00011100011100011100
0111000



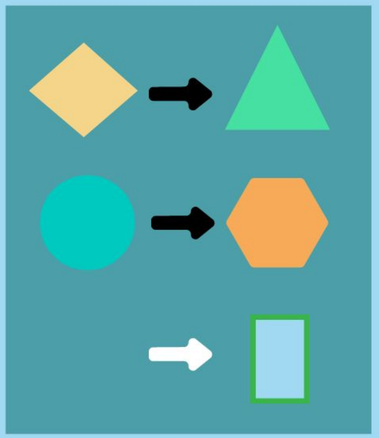
23/11/2018

000111000
111000111
000111000

HASH: 922959156

HASH<100000

~~10101010110101010110~~
~~1010101~~
~~11110000000001111111~~
~~1100000~~
~~00011100011100011100~~
~~0111000~~
11111111100000000011
1111111



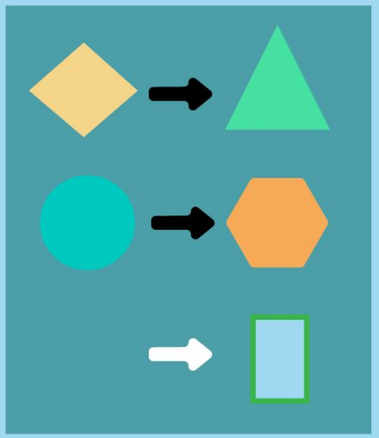
23/11/2018

111111111
000000000
111111111

HASH: 41912891

HASH<100000

~~10101010110101010110~~
~~1010101~~
~~11110000000001111111~~
~~1100000~~
~~00011100011100011100~~
~~0111000~~
~~11111111100000000011~~
~~1111111~~
00000000011111111100
0000000



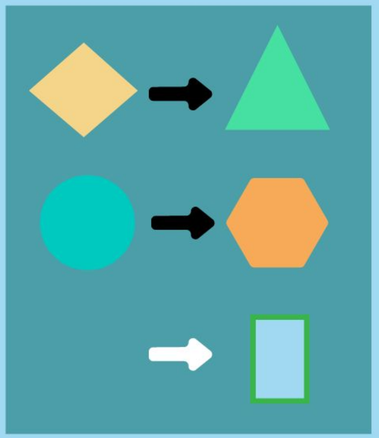
23/11/2018

000000000
111111111
000000000

HASH: 48292184

HASH<100000

~~10101010110101010110~~
~~1010101~~
~~11110000000001111111~~
~~1100000~~
~~00011100011100011100~~
~~0111000~~
~~11111111100000000011~~
~~1111111~~
~~00000000011111111100~~
~~0000000~~
10101010101010101010
1010101



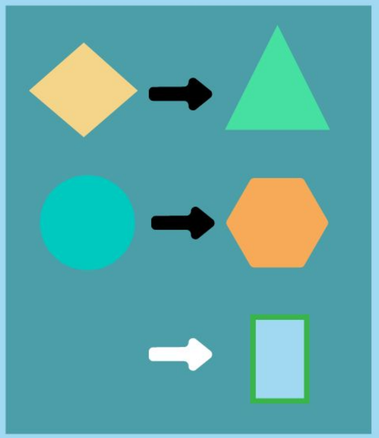
23/11/2018

101010101
010101010
101010101

HASH: 77770707

HASH<100000

~~10101010110101010110~~
~~1010101~~
~~11110000000001111111~~
~~1100000~~
~~00011100011100011100~~
~~0111000~~
~~11111111100000000011~~
~~1111111~~
~~00000000011111111100~~
~~0000000~~
~~10101010101010101010~~
~~1010101~~
0111010=ID050000✓



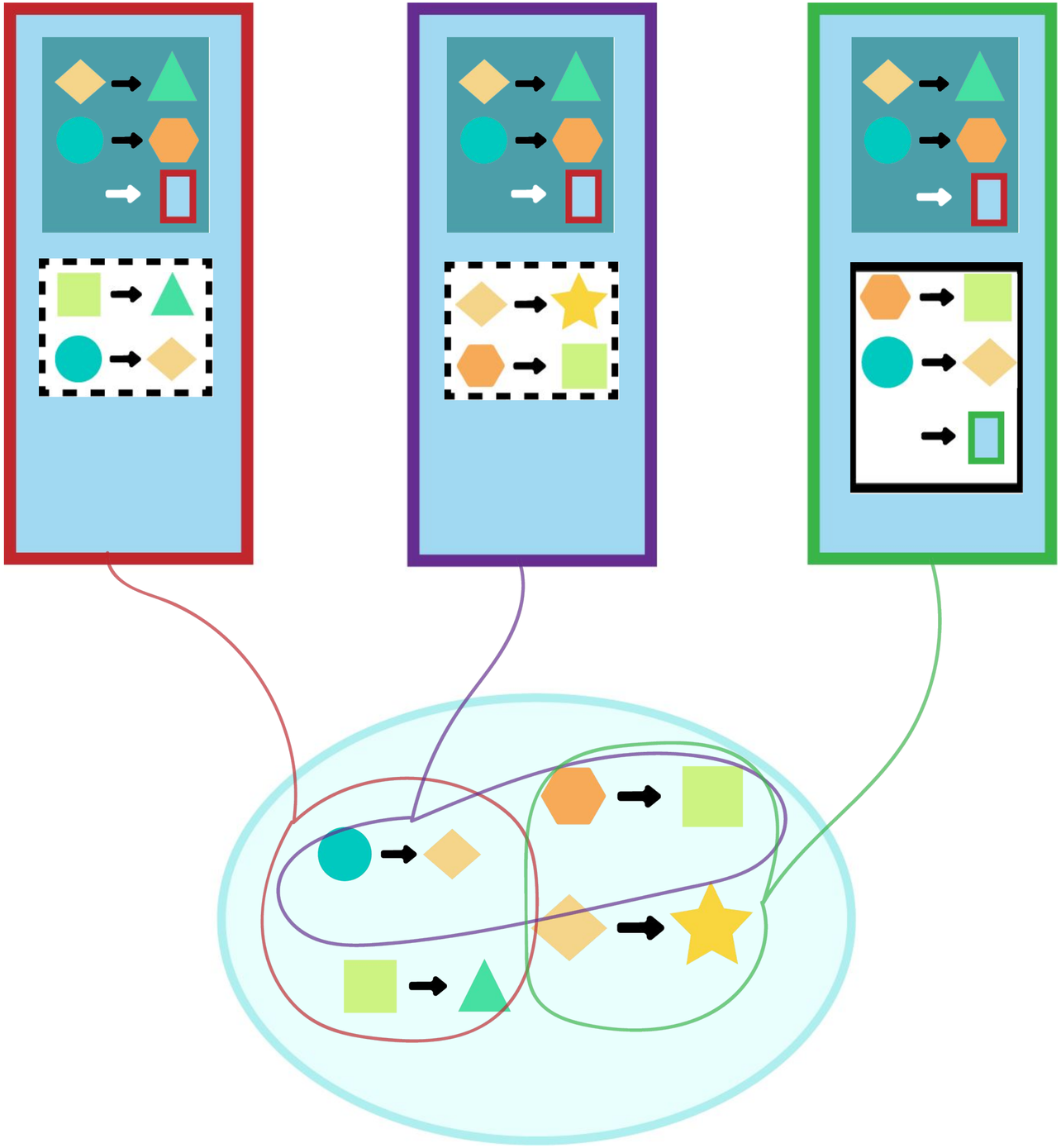
23/11/2018

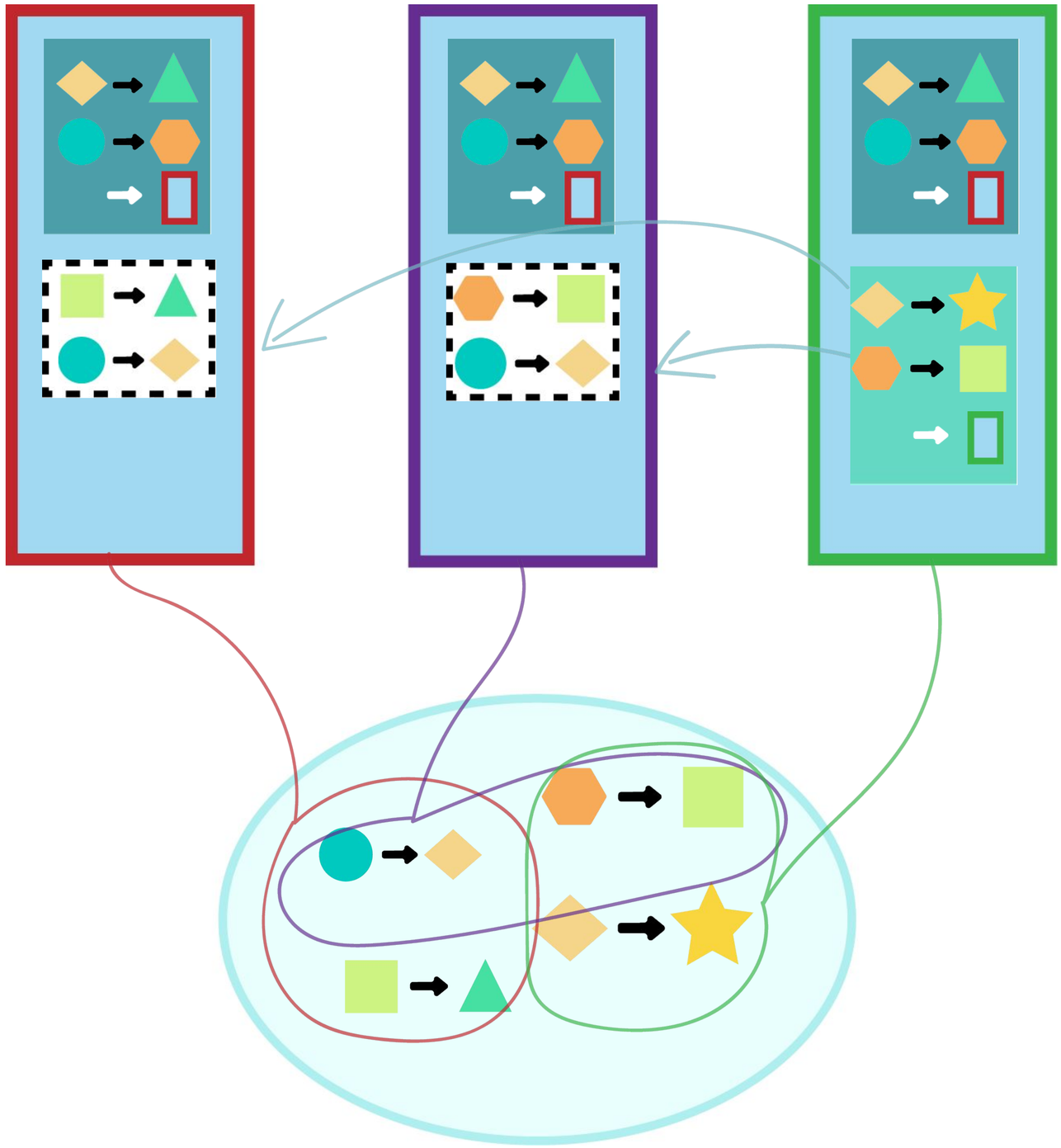
110011001
001100110
110011001

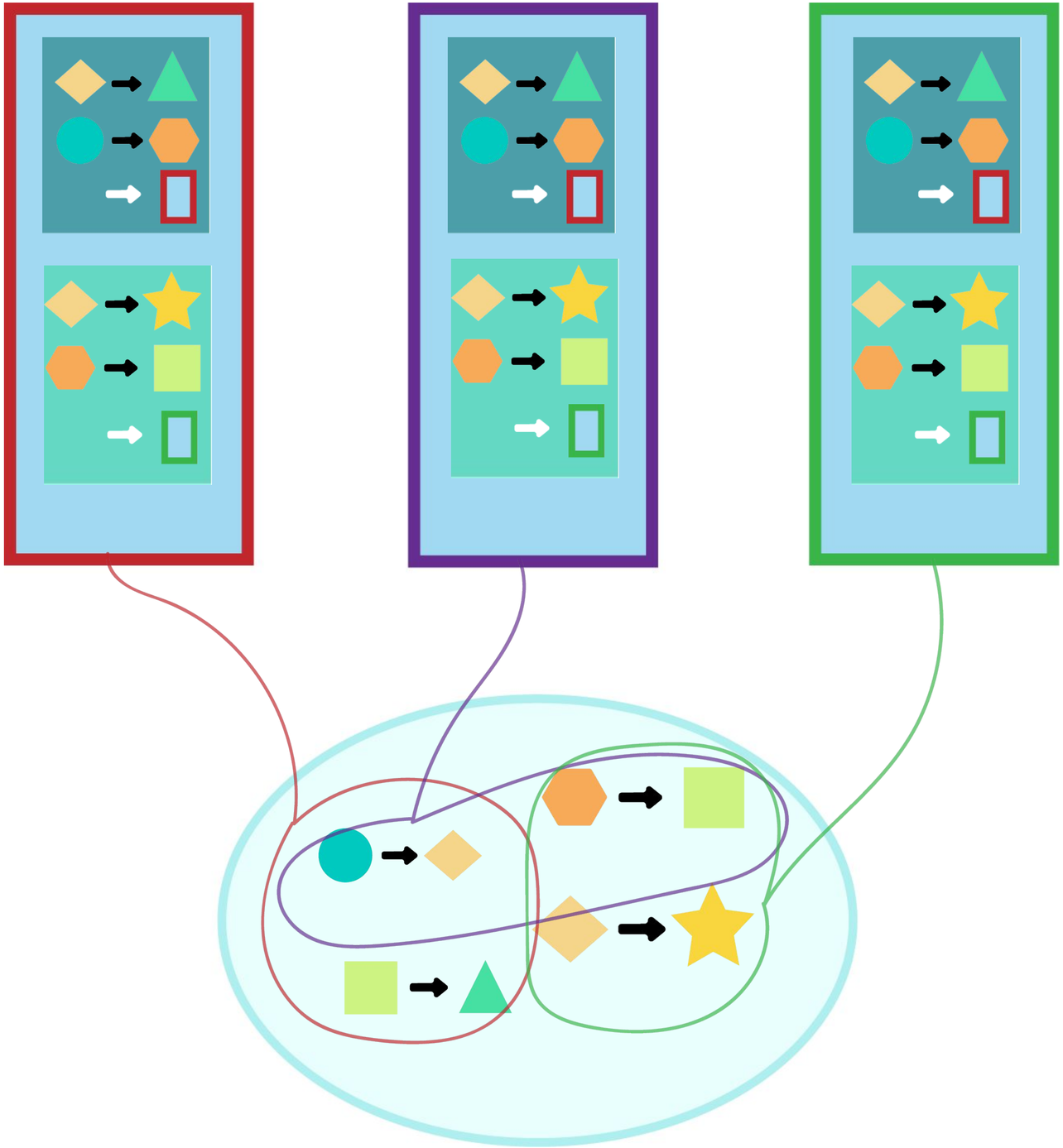
HASH: 0005211

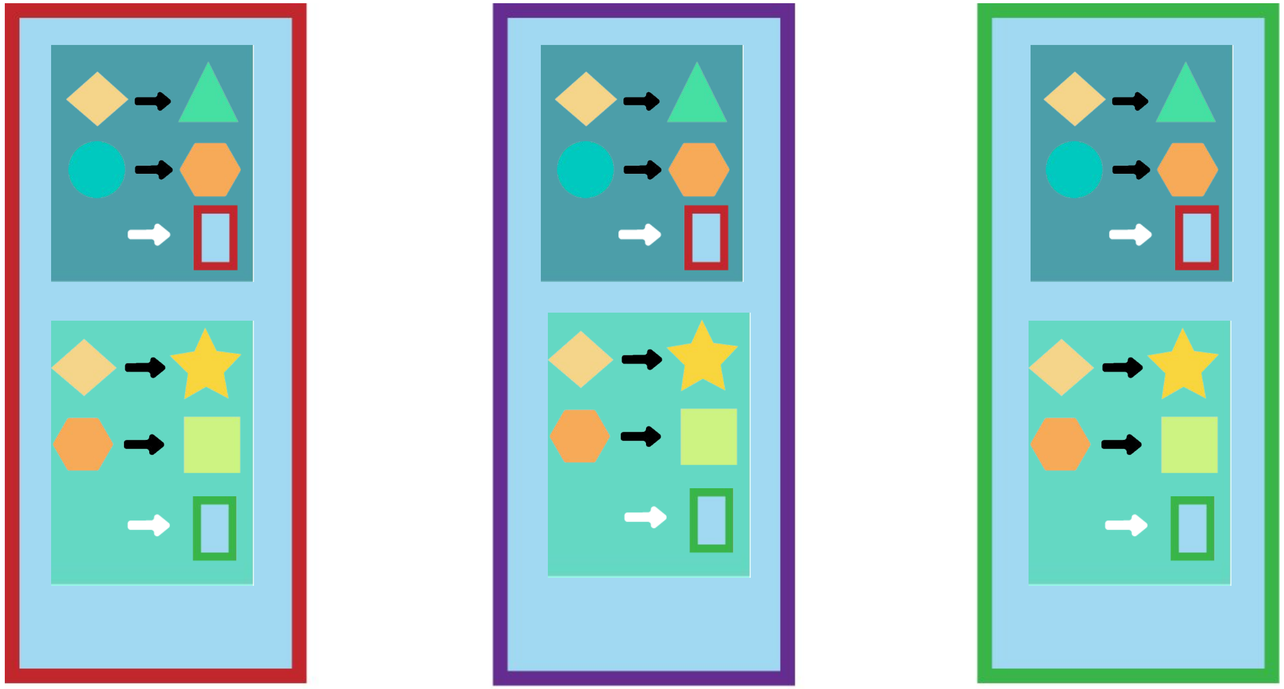
HASH<100000

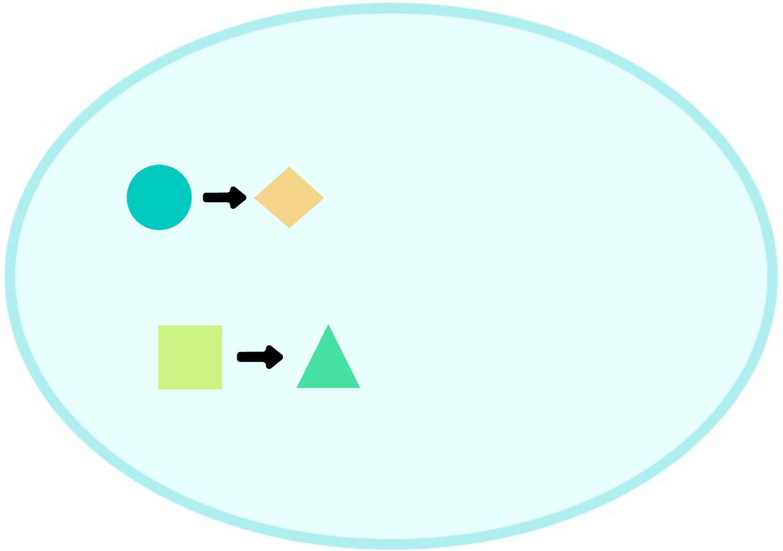
✓











¿Qué hace que los criptos sean una moneda?

- ✓ fungibile
- ✓ segura
- ✓ Escasa
- ✓ Durable
- ? ¿Convención?

- ✗ Transacciones lentas (~1h)
- ✗ Transacciones caras (a veces)
- ✗ Dificil de entender

Hagamos de unos pequeños ajustes...

Bloques MUY GRANDES

BitcoinCash

¿Qué hace que los criptos sean una moneda?

- ✓ fungibile
- ✓ segura
- ✓ Escasa
- ✓ Durable
- ? ¿Convención?

- ✗ Transacciones lentas (~1h)
- ✗ Transacciones caras (a veces)
- ✗ Dificil de entender

¿Qué hace que los criptos sean una moneda?

- fungibile
- segura
- Escasa
- Durable
- ¿Convención?
- Transacciones instantáneas
- Transacciones baratas
- Dificil de entender

money button

UX para la **Blockchain**

Demo

¿Qué hace que los criptos sean una moneda?

- fungibile
- segura
- Escasa
- Durable
- ¿Convención?
- Transacciones instantaneas
- Transacciones baratas
- Dificil de entender

¿Qué hace que los criptos sean una moneda?

- fungibile
- segura
- Escasa
- Durable
- ¿Convención?
- Transacciones instantáneas
- Transacciones baratas
- ¡Fácil de entender!

“

“Sound digital money for the entire world”

“*Dinero sólido y digital para todo el mundo*”

CREDITOS

Agradecimiento especial a la gente que hace y comporte estos increíbles recursos multimedia de manera libre y gratuita

- Presentación diseñada por Slidesmash
- Diseño por unsplash.com, pexels.com y Carla Belatti
- Ilustraciones por Carla Belatti

Gracias!

Contacto: @hojarasca miguel@moneybutton.com