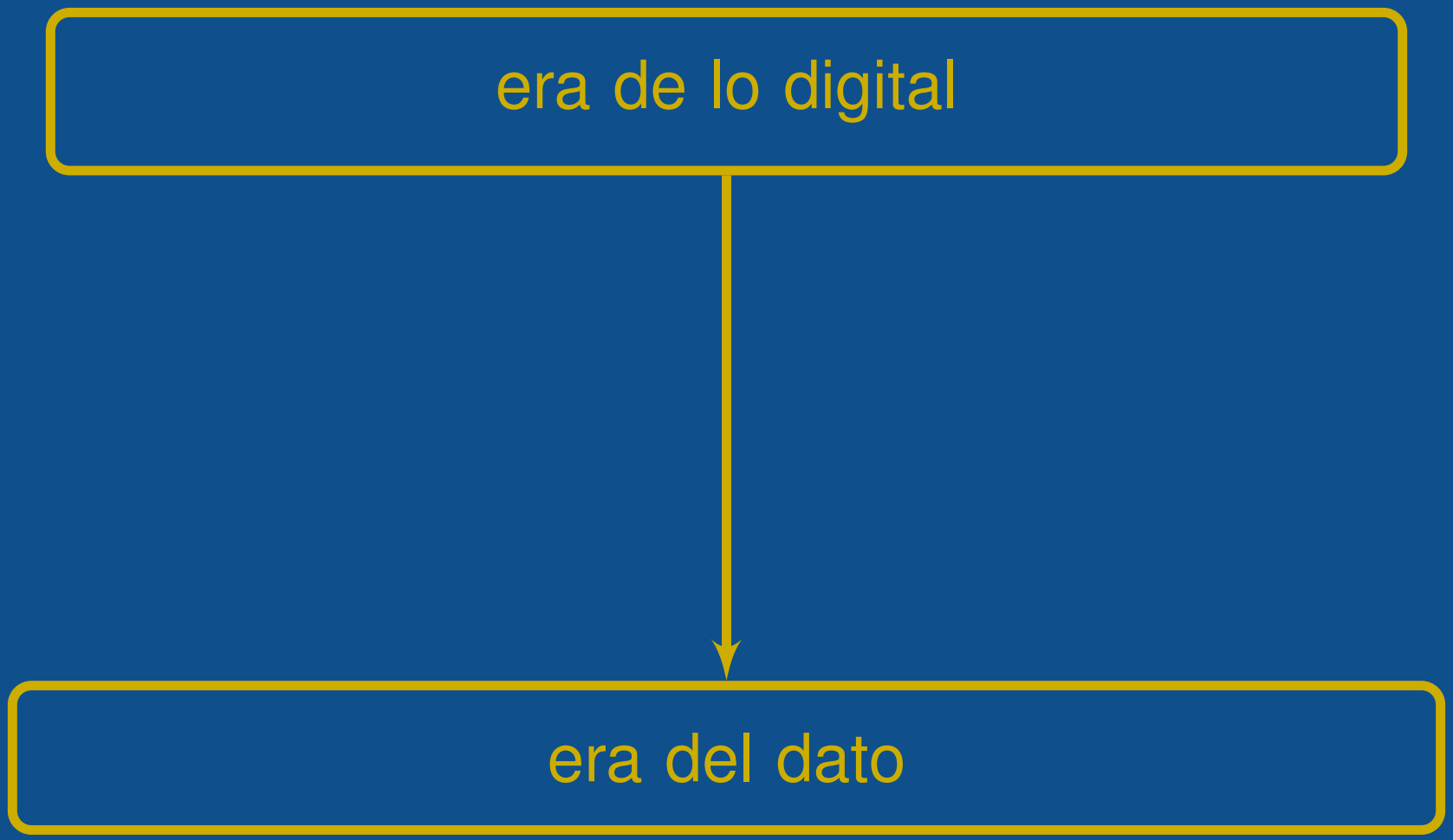
Blockchain: fundamentos técnicos y trabajo futuro

David Arroyo Guardeño

era de lo digital


era de lo digital
era del dato

Las TIC organizan nuestro día a día. . .

. . . debemos cuidar las TIC

La información tiene valor por sí misma. . .

- ¿Quién accede a la información?

La información tiene valor por sí misma. . .

- ✓ ¿Quién accede a la información?
- ✓ ¿Qué puede hacer con la información?

La información tiene valor por sí misma. . .

- ✓ ¿Quién accede a la información?
- ✓ ¿Qué puede hacer con la información?
- ✓ ¿Por cuánto tiempo puede tener acceso a la información?

La información tiene valor por sí misma…

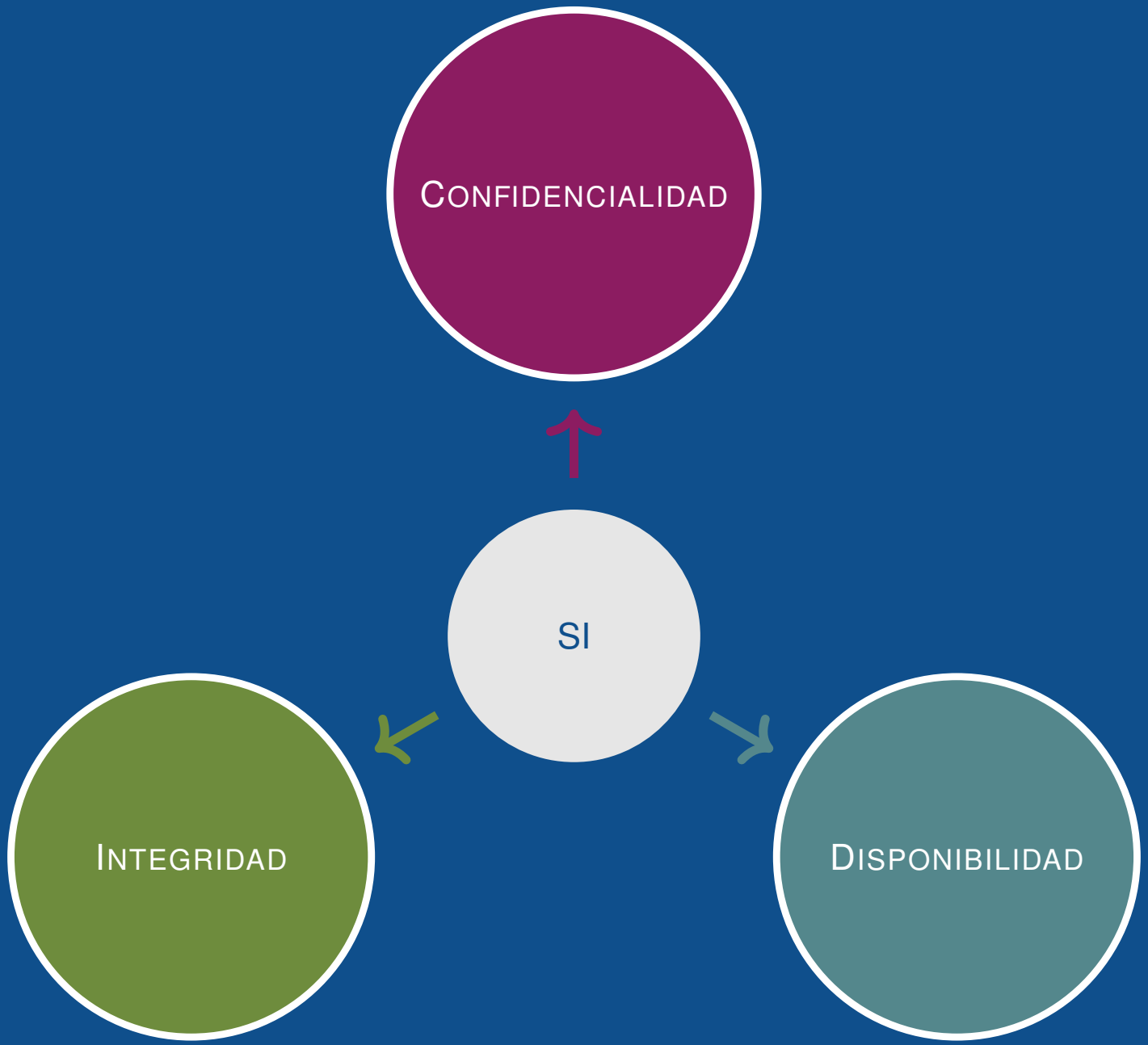
- ✓ ¿Quién accede a la información?
- ✓ ¿Qué puede hacer con la información?
- ✓ ¿Por cuánto tiempo puede tener acceso a la información?
- ✓ ¿Cómo puedo acceder a la información?

La información tiene valor por sí misma. . .

- ✓ ¿Quién accede a la información?
- ✓ ¿Qué puede hacer con la información?
- ✓ ¿Por cuánto tiempo puede tener acceso a la información?
- ✓ ¿Cómo puedo acceder a la información?
- ✓ ¿Cuándo una fuente de información puede ser considerada como confiable?

La información tiene valor por sí misma. . .

- ✓ ¿Quién accede a la información?
- ✓ ¿Qué puede hacer con la información?
- ✓ ¿Por cuánto tiempo puede tener acceso a la información?
- ✓ ¿Cómo puedo acceder a la información?
- ✓ ¿Cuándo una fuente de información puede ser considerada como confiable?


CONFIDENCIALIDAD
SI
INTEGRIDAD
DISPONIBILIDAD

Criptografía

Criptografía

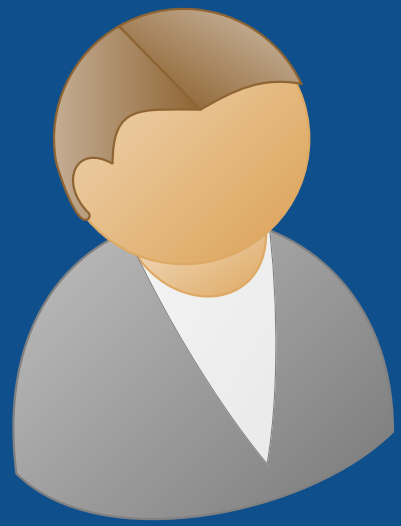
Simétrica o de clave secreta

Criptografía

Simétrica o de clave secreta

Asimétrica o de clave pública

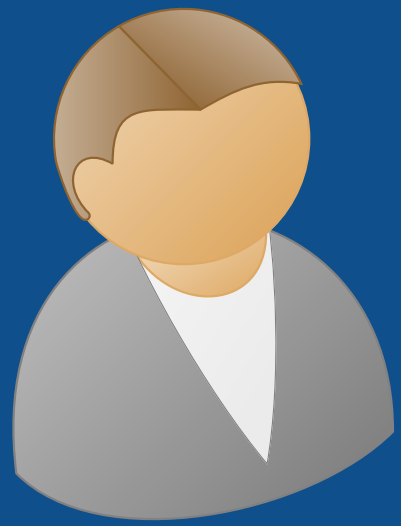
Criptografía simétrica (e.g., AES)



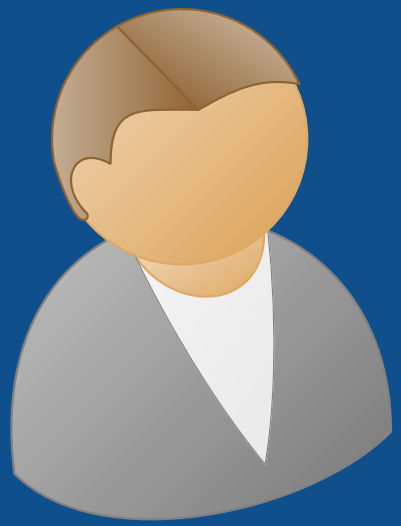
Clave secreta

de sesión

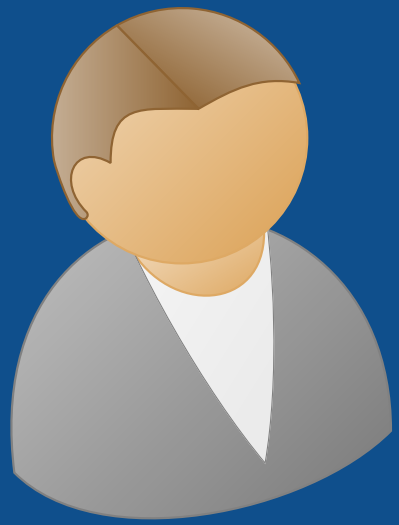
Criptografía simétrica (e.g., AES)



Criptografía asimétrica (e.g., RSA)

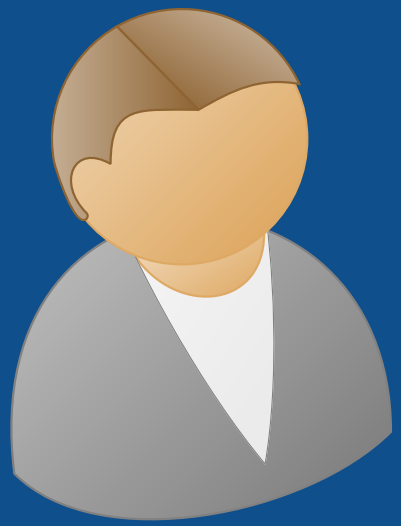


Criptografía asimétrica (e.g., RSA)

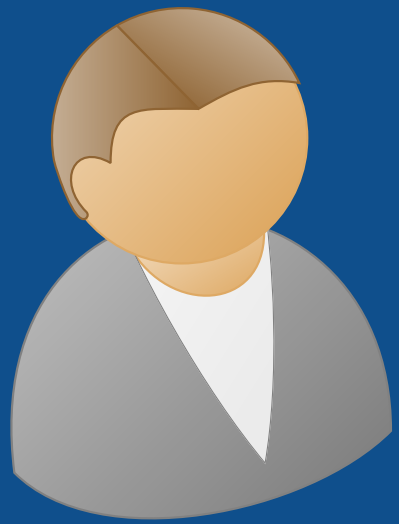


Criptografía asimétrica (e.g., RSA)

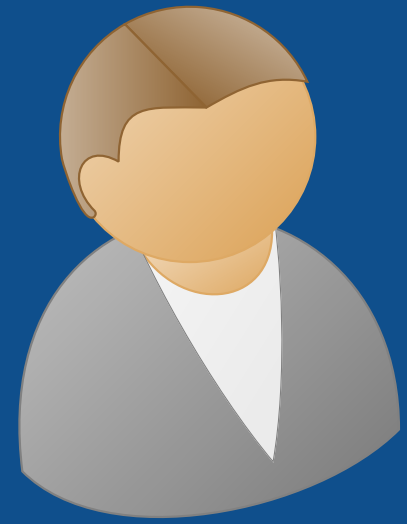
Criptografía asimétrica (e.g., RSA)



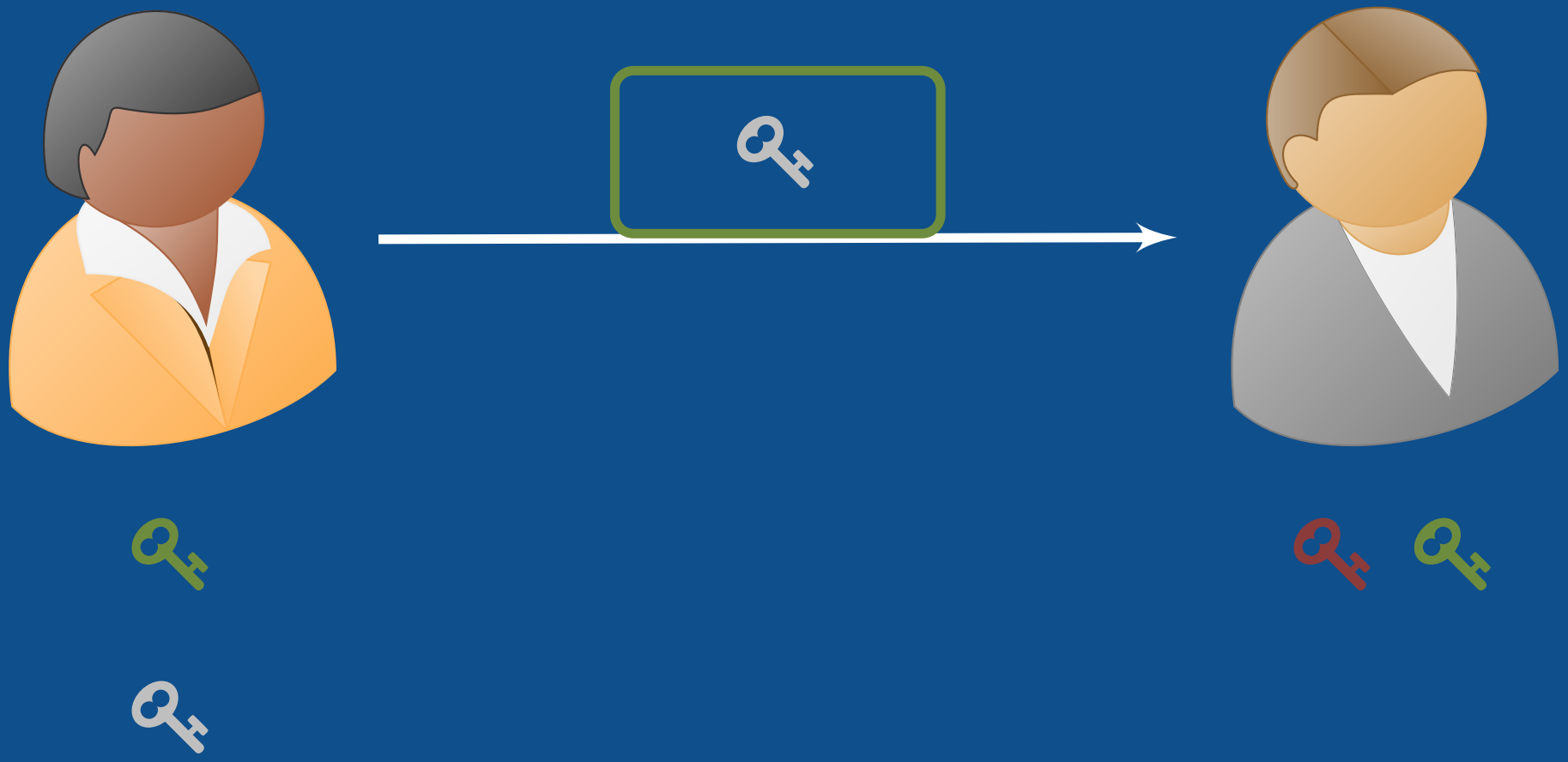
Criptografía asimétrica (e.g., RSA)



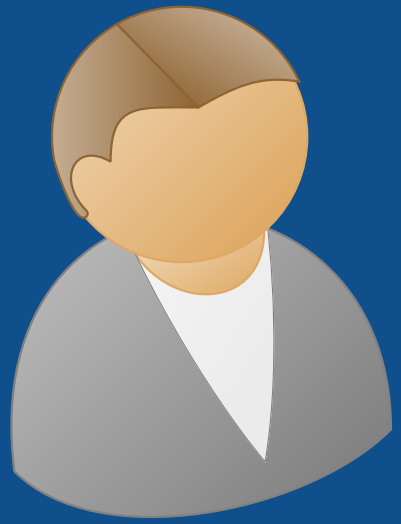
Criptografía asimétrica: intercambio de clave de sesión



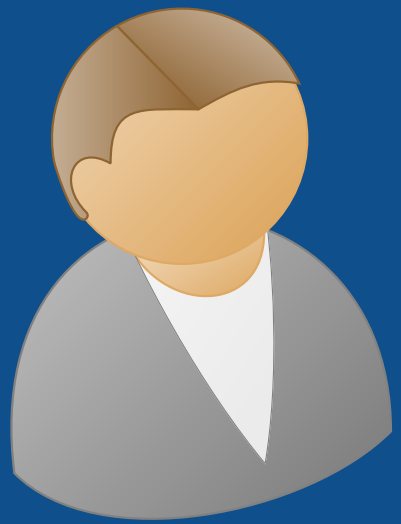
Criptografía asimétrica: intercambio de clave de sesión

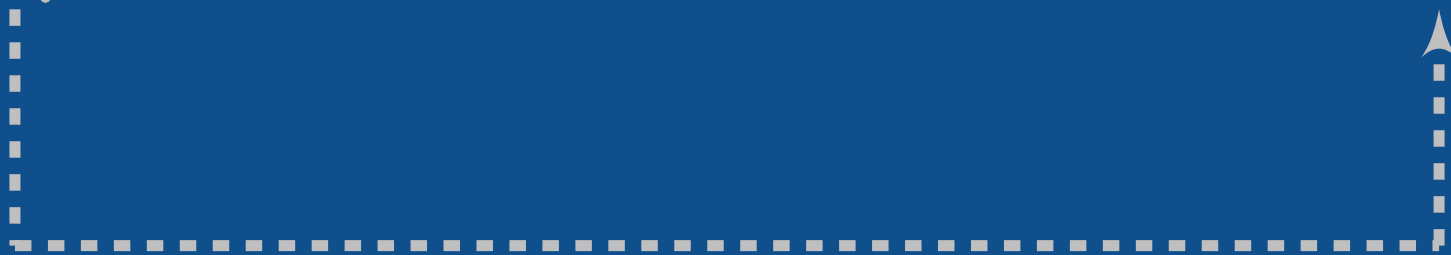


Criptografía asimétrica: intercambio de clave de sesión

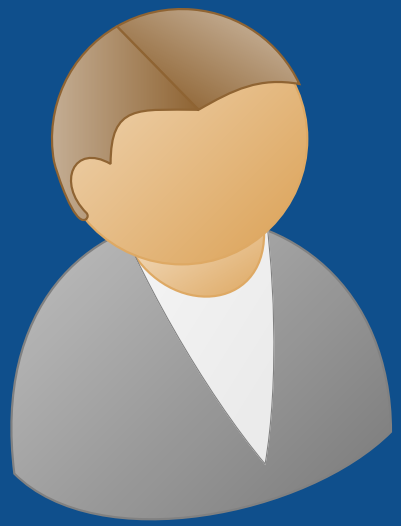


Criptografía asimétrica: intercambio de clave de sesión

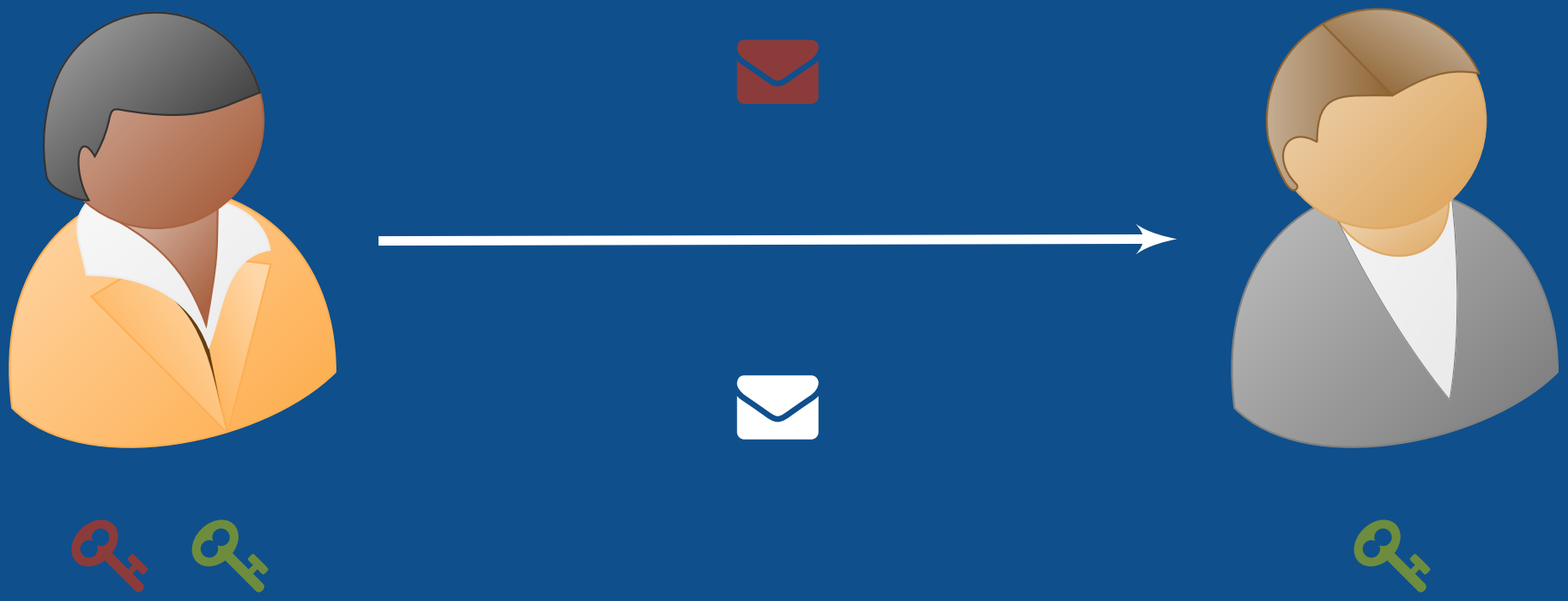




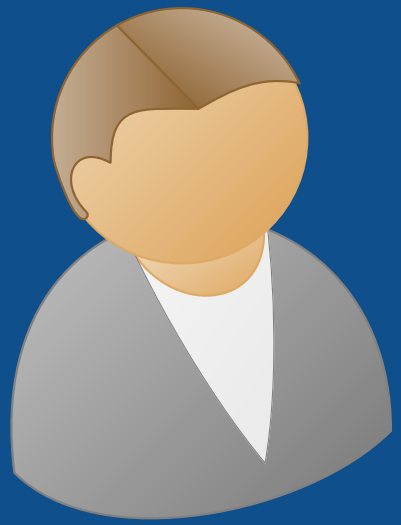
Firma digital convencional



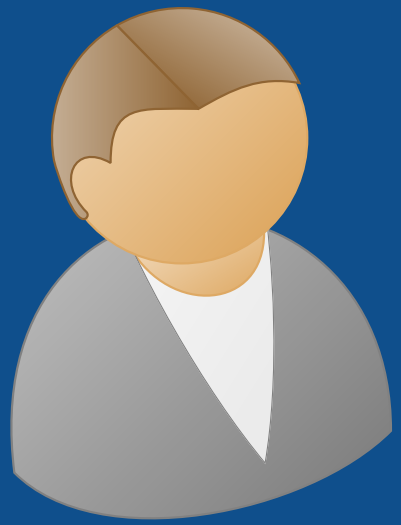
Firma digital convencional

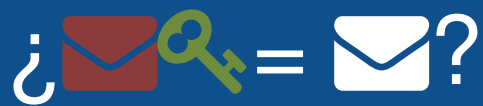


Firma digital convencional



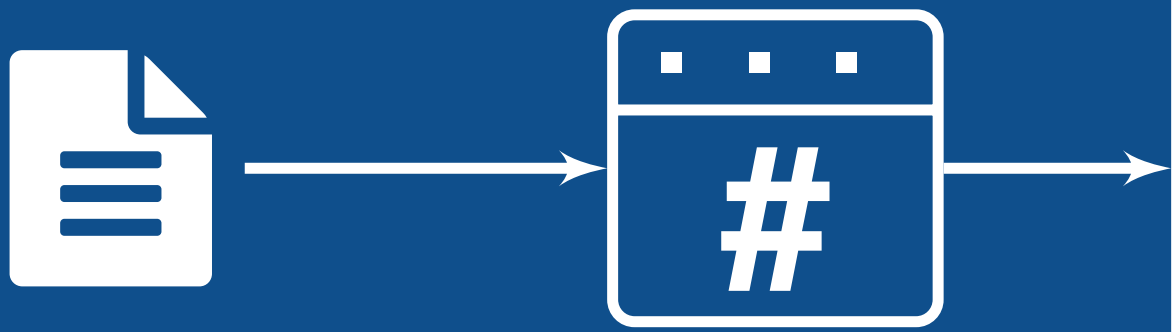
Firma digital convencional





Funciones hash

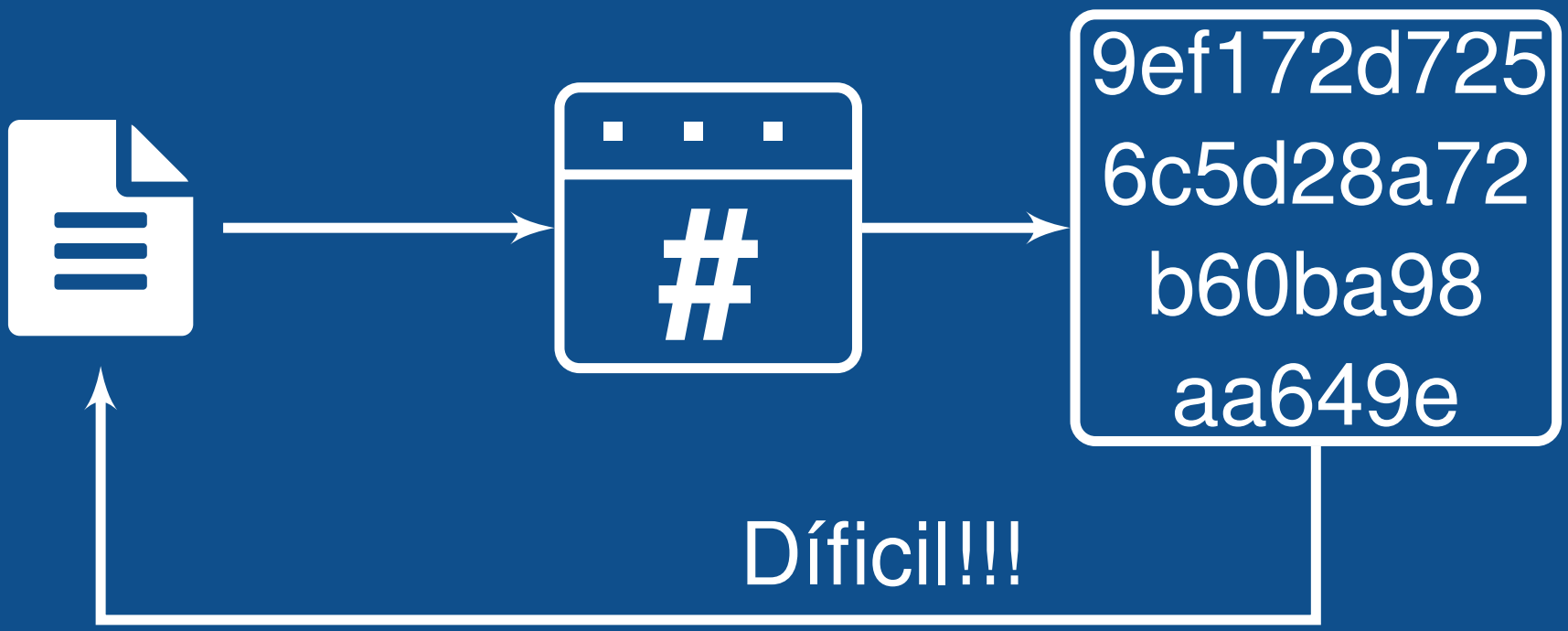
Tamaño variable



Tamaño fijo

9ef172d725
6c5d28a72
b60ba98
aa649e

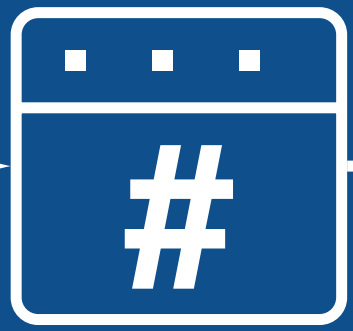
Funciones hash



Funciones hash

Conocido

Conocido



9ef172d725
6c5d28a72
b60ba98
aa649e

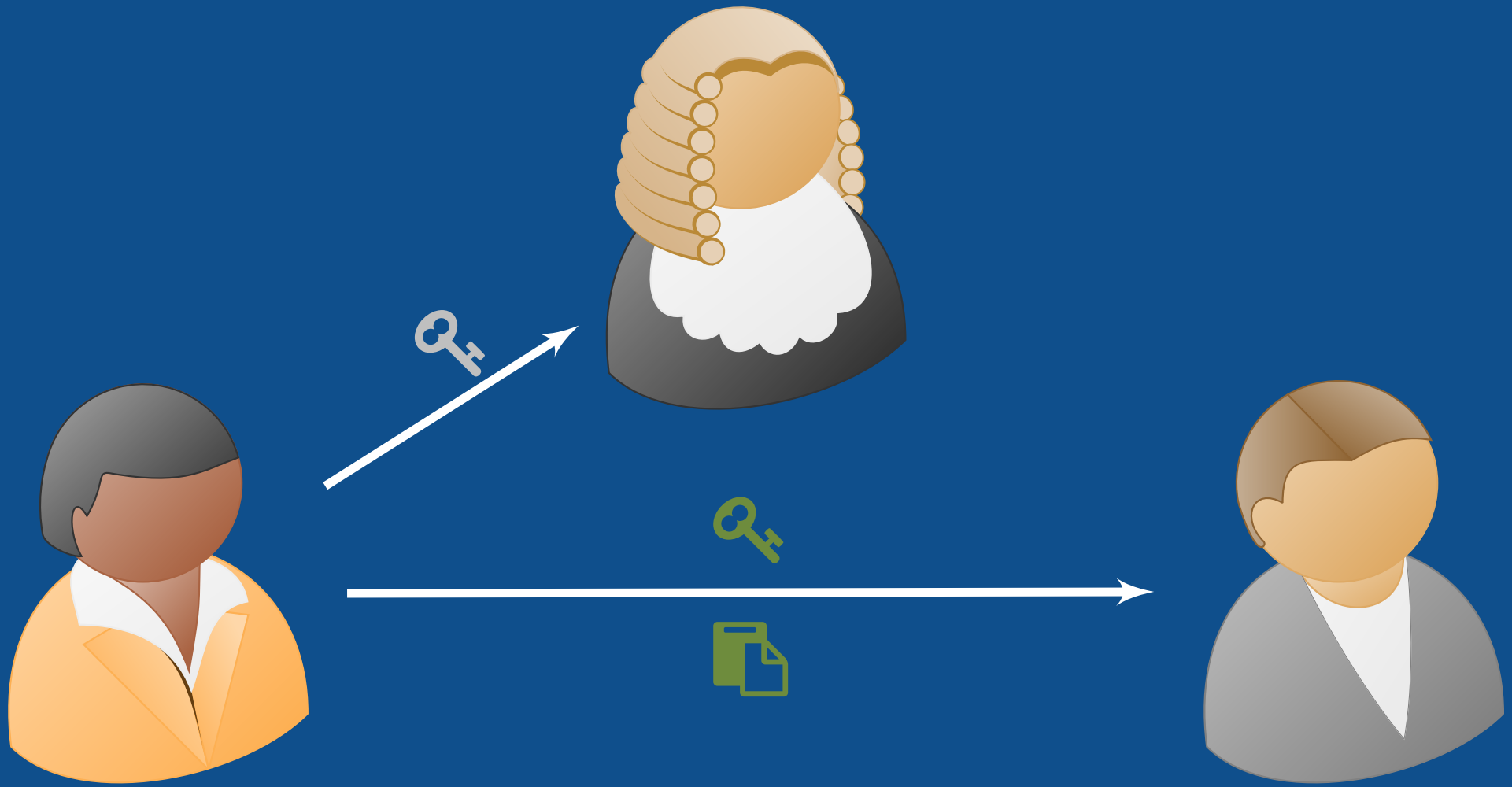
Buscar otro texto

Difícil

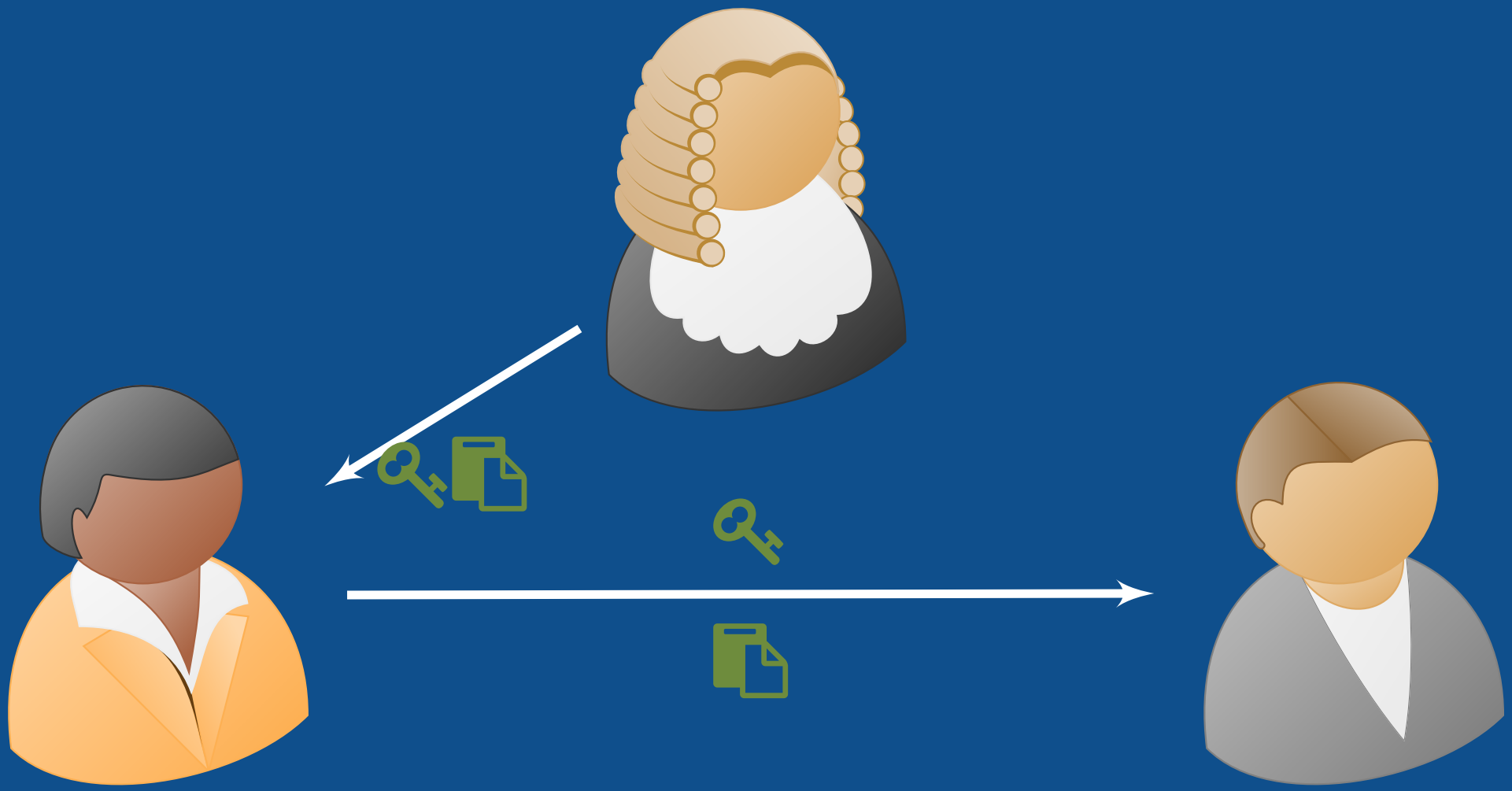
Verificación de integridad

- ✓ De contenido: funciones hash
- ✓ De origen de contenido (autoría): firmas digitales

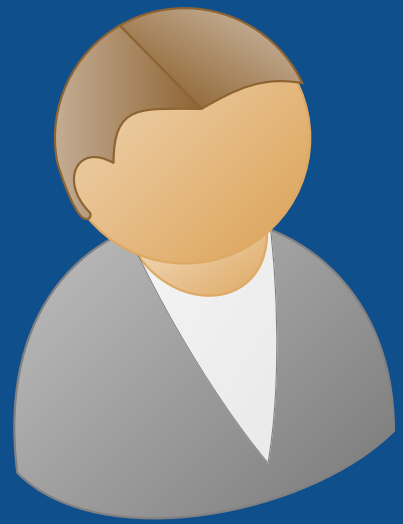
¿Quién me asegura que la clave pública es válida?



¿Quién me asegura que la clave pública es válida?



¿Quién me asegura que la clave pública es válida?



Estándar X.509


DOCUMENTO NACIONAL DE IDENTIDAD
ESPAÑA
PRIMER APELLIDO
APELLIDO1
SEGUNDO APELLIDO
APELLIDO2
NOMBRE
NOMBRE
SEXO
M
NACIONALIDAD
ESP
FECHA DE NACIMIENTO
01 05 1972
DESP
AAA-000000
VALIDO HASTA
01 01 2016
DNI NUM.
99999999-R
dni
electrónico


https://

Centralización de la confianza

*William Mougayar. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, 2016

TI ($\rightarrow$ 1994)	Era de Internet($\rightarrow$ 2015)	Blockchain promise
Computación	Interacciones sociales	Descentralización de la confianza
Aplicaciones de bases datos	comercio electrónico	
Procesamiento de transacciones	Auto-publicación	Flujo de *valor* sin intermediarios
Inteligencia de negocio	Comunicaciones personales	

¿Qué es la BlockChain (BC)?

- ✓ Mecanismo P2P para generación de consenso

¿Qué es la BlockChain (BC)?

- ✓ Mecanismo P2P para generación de consenso
- ✓ Actividad colaborativa

¿Qué es la BlockChain (BC)?

- ✓ Mecanismo P2P para generación de consenso
- ✓ Actividad colaborativa
- ✓ No existe una Autoridad Central

¿Qué es la BlockChain (BC)?

- ✓ Mecanismo P2P para generación de consenso
- ✓ Actividad colaborativa
- ✓ No existe una Autoridad Central
- ✓ Como resultado del acuerdo, se guarda información en un registro (*distributed ledger*)

¿Qué es la BlockChain (BC)?

- ✓ Mecanismo P2P para generación de consenso
- ✓ Actividad colaborativa
- ✓ No existe una Autoridad Central
- ✓ Como resultado del acuerdo, se guarda información en un registro (*distributed ledger*)
- ✓ Es un registro inmutable

Orígenes de la blockchain

- ✓ Hashcash de Adam Back (1997): mecanismo para evitar el correo spam
- ✓ Primera aplicación de *éxito* en criptomonedas: Bitcoin ₿(2009)
- ✓ Se han ido desarrollando alternativas
  - ✗ Política de control de acceso
  - ✗ Variantes del procedimiento para alcanzar consenso distribuido

Blockchain ₿

- ✓ Creación de un registro de transacciones no centralizado
- ✓ Las transacciones se escriben en bloques
- ✓ Integridad mediante punteros hash (*hash pointers*) y firmas digitales
- ✓ Las identidades de los usuarios son los hashes de claves públicas generadas por cada uno de ellos (no hay autoridad central!!!)

Bloques de la BC ₿

Cabecera

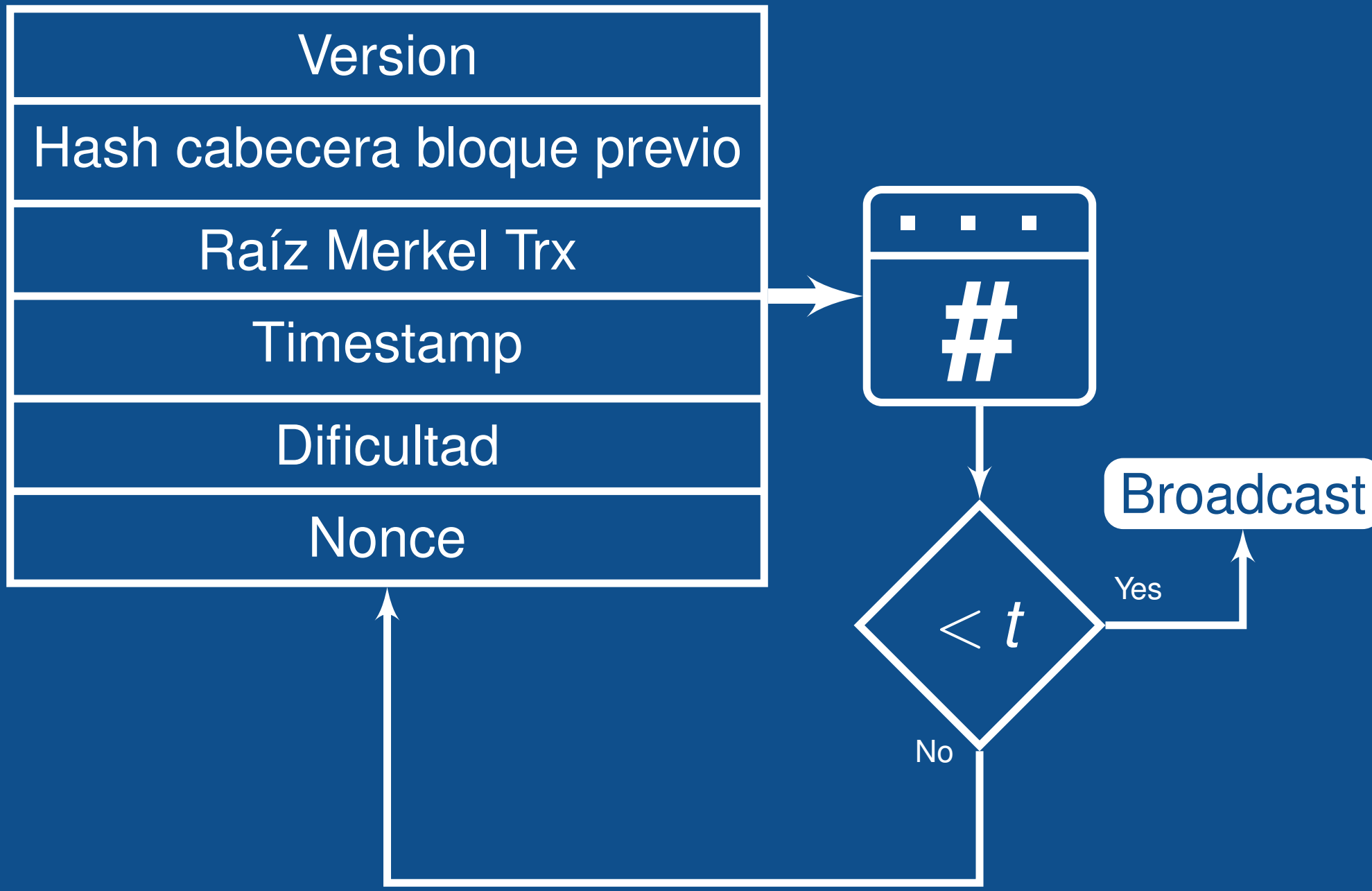
Hash de la cabecera del bloque previo

Raíz del árbol de Merkle

Transacciones (árbol Merkle)

Creación de un bloque (minado, Proof of Work)

- ✓ Cuando un nodo crea un bloque lo envía por *broadcast* a la red
- ✓ La creación del nodo es un proceso costoso: asegura selección aleatoria de nodos y evita ataques por duplicación de identidades (*sybil attacks*)
- ✓ Recompensa por creación del nodo: 12.5 BTC (se reduce a la mitad cada $21 \cdot 10^5$ bloques)


Version
Hash cabecera bloque previo
Raíz Merkel Trx
Timestamp
Dificultad
Nonce
#
< t
Yes
No
Broadcast

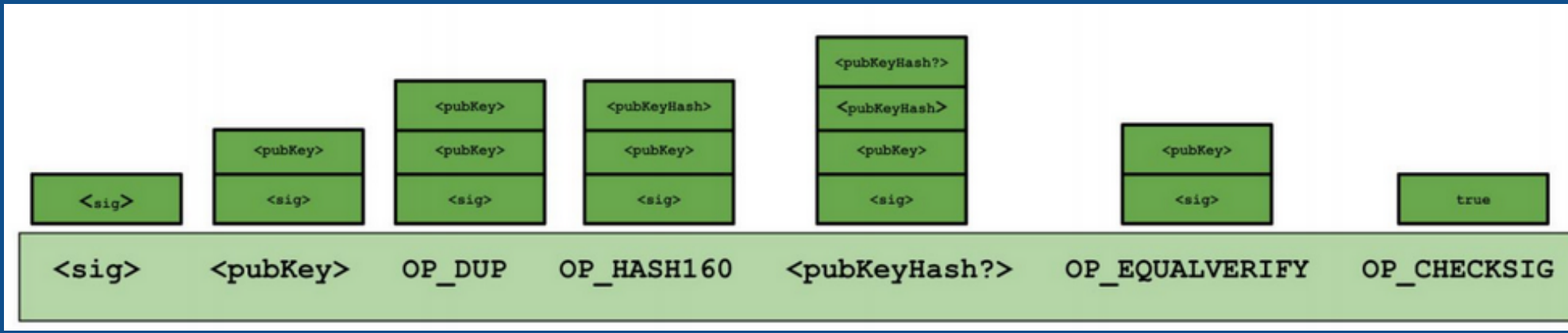
Formato de las transacciones[1]

Transaction always spends money from previous transaction


```
{
  "hash":"b8ddb8d91f18c9ad80727c2f05f96d1c0db0ba204f0233f3725ae39bcd074ffd",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":191,
  "in":[
    {
      "prev_out":{
        "hash":"09173d4cb8cc71e1cfcdb0446c9886b7cc1e0875290b1e1566be1fa1a4df0f4a",
        "n":14
      },
      "scriptSig":"304402202d42afd73aec0fb7d91db750b1be61ad2103378d9fe39cde24f8b12351b3
            08ad02200cad5e7c3a0e0fc98dbfe0bfb820c85ea317896e44c9b4a3a2d2bdfecdc2ecf201
            031eac46e3a4e001f2c1e937e0b2c5027fa3f2d405c59df5a2b2233fdc6b671c53"
    }
  ],
  "out":[
    {
      "value":"0.03400000",
      "scriptPubKey":"OP_DUP OP_HASH160 e936205ce69349818cd510ca982c2e76a03ec967
                      OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```


[1] https://en.bitcoin.it/wiki/Transaction

Verificación de una transacción [Nar+16]

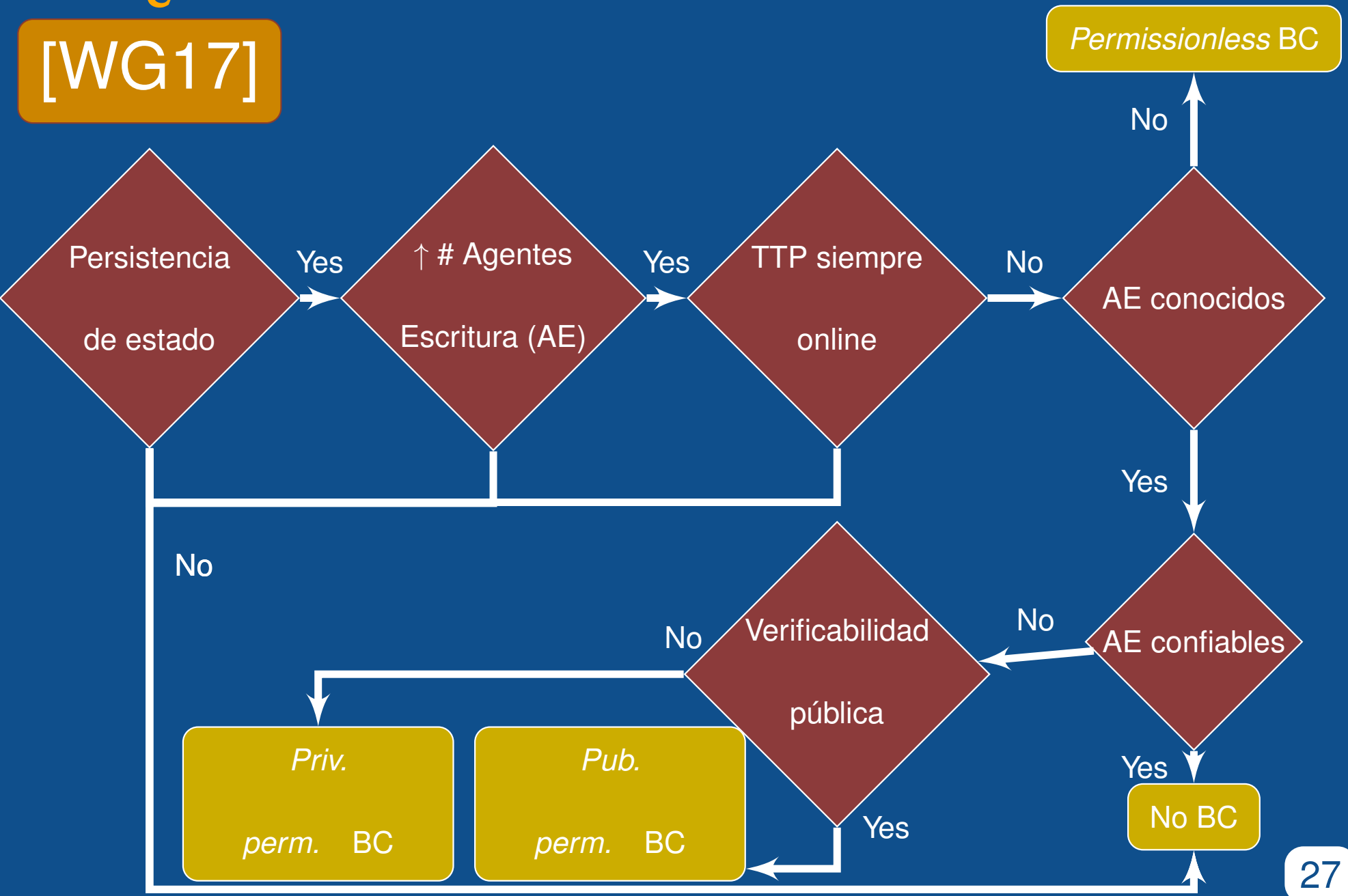


Scripts ฿

- ✓ La composición de los campos **in** y **out** generan scripts
- ✓ Repertorio de OP_CODES
- ✓ Posibilidad de incluir metadatos en BC ฿(e.g., haciendo uso de **OP_RETURN**)
  - ✗ Blockchain As a Service
  - ✗ EverLedger, MaidSafe, Stampery, Guardtime, EverLedger, La'ZooZ, . . .
  - ✗ OJO: los metadatos son públicamente accesibles y no se pueden borrar

Y, ¿de verdad necesitas una blockchain?

[WG17]



Problemas de blockchain

- ✓ Escalabilidad
- ✓ Regulación
- ✓ Gestión de la identidad: privacidad
- ✓ Protocolos M2M: *smart contracts*
- ✓ Seguridad
  - ✗ Ataque del 51%
  - ✗ Minado egoista
  - ✗ Computación cuántica (Grover, Schor)

Investigación específica sobre blockchain

- ✓ Casos de uso
- ✓ Gestión de identidad en blockchain
  - ✗ Anonimato criptográfico
  - ✗ Evaluación estadística de la privacidad: k-anonymity, privacidad diferencial
- ✓ Limitaciones de blockchain: diagnóstico y soluciones
  - ✗ Alternativas al minado
  - ✗ Análisis del dilema “tragedy of the commons”

MUCHAS GRACIAS

http://davidarroyoguardeno.blogspot.com.es/

- Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.
- Jesus Diaz, David Arroyo, and Francisco B Rodriguez. "Fair anonymity for the Tor network". In: *The 14th International Conference on Security and Cryptography (SECRYPT 2017)*. 2017, Accepted as Position Paper. In Press.
- Jesus Diaz, David Arroyo, and FranciscoB. Rodriguez. "Anonymity Revocation through Standard Infrastructures". In: *Public Key Infrastructures, Services and Applications*. Ed. by Sabrina Capitani di Vimercati and Chris Mitchell. Vol. 7868. LNCS. Springer Berlin Heidelberg, 2013, pp. 112–127. ISBN: 978-3-642-40011-7.
- Pedro Franco. *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.
- Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". In: *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE. 2016, pp. 839–858.
- William Mougayar. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, 2016.
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

- Alejandro Sanchez-Gomez, Jesus Diaz, Luis Hernández Encinas, and David Arroyo. “Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers”. In: *Computer and Network Security Essentials*. Ed. by K. Daimi. Vol. In Press. Studies in Computational Intelligence. Springer Berlin Heidelberg, 2017.

- Karl Wüst and Arthur Gervais. “Do you need a Blockchain?” In: *IACR Cryptology ePrint Archive* 2017 (2017), p. 375.

- Guy Zyskind, Oz Nathan, and Alex Pentland. “Enigma: Decentralized computation platform with guaranteed privacy”. In: *arXiv preprint arXiv:1506.03471* (2015).