LA FUNCIÓN REGISTRAL EN UN MUNDO DE **SMART CONTRACTS Y BLOCKCHAIN**

Daniel A. Monroy
2018

Universidad Externado de Colombia

sunarp

Sunarp recibirá títulos con firma digital para operaciones inmobiliarias

Registros Públicos autoriza este mecanismo como alternativa a la presentación física de documentos.

Encriptación / menores trámites

Comunidades campesinas podrán pedir la inscripción de predios informales

El gobierno decretó la derogación de requisitos para la inscripción de terrenos ante Registros Públicos (Sunarp) por parte de comunidades campesinas.

Informalidad / capacidad de gestión

Así puedes proteger tu propiedad de un fraude inmobiliario

La mejor forma de preservar y proteger una propiedad inmueble es inscribirla en la Superintendencia Nacional de los Registros Públicos (Sunarp).

Fraude / seguridad

Bitcoin.com Notary

Prove ownership on the Bitcoin Cash (BCH) Blockchain for only 0.00005 BCH (less than 5 cents).

Select Your document

Add your file by dragging it into the browser or using the file selector below.

Fund Your Anchor

Send Bitcoin Cash (BCH) to the address provided and fund your blockchain anchor.

Sign To The Blockchain

Your file will be forever signed into the blockchain with a unique address and timestamp.

View Your Proof

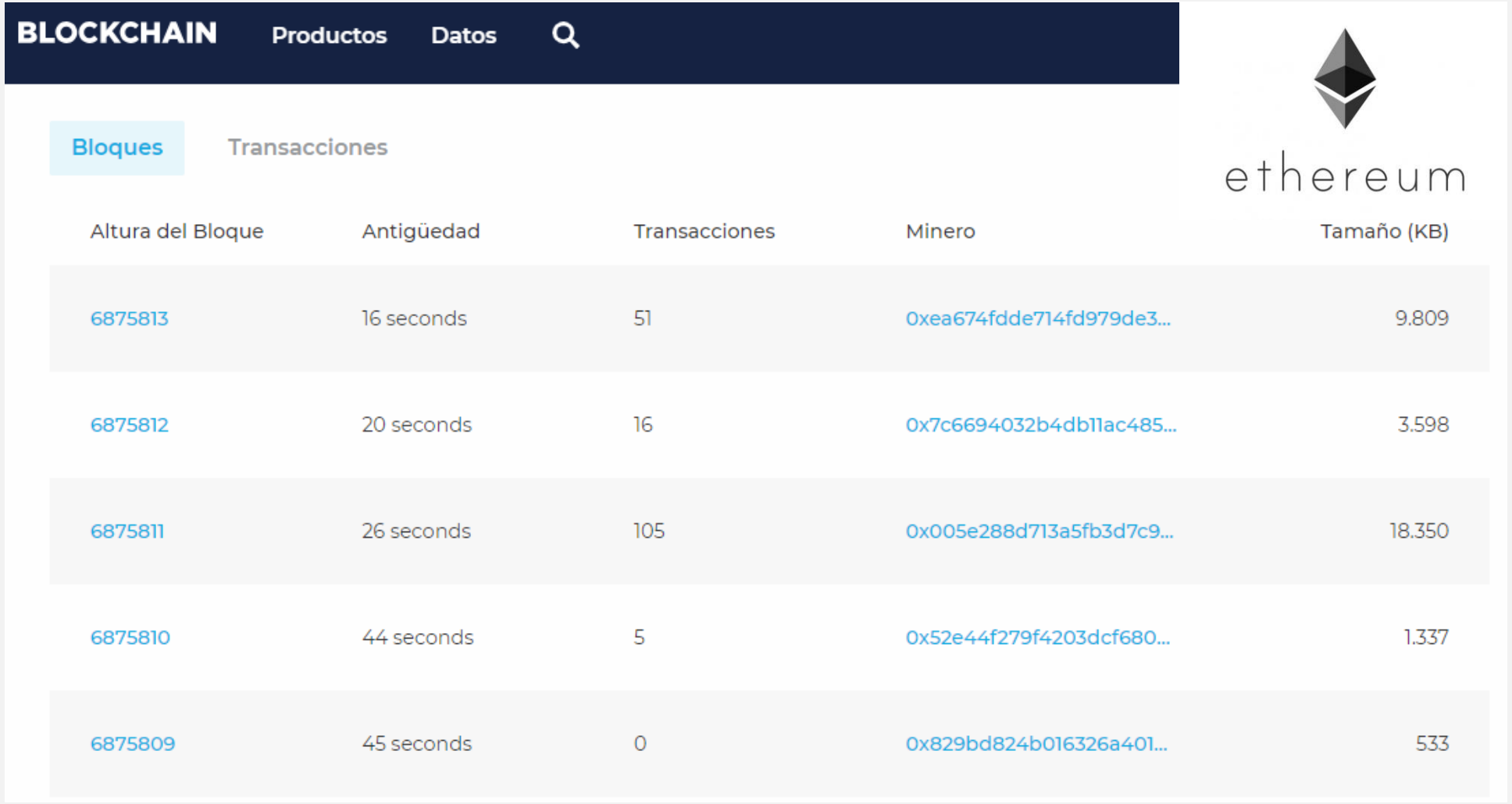
See your proof on the blockchain by checking the transaction in a block explorer.

CONTENIDO

1. **¿Qué es un 'Smart contract"?**
   - Diferencias y similitudes con contratos convencionales
2. **¿Smart contracts y blockchain?**
3. **¿Qué es blockchain y por qué todo el mundo está hablando de eso?**
   - **Registros distribuidos vs. registros centralizados**
   - El rol de la encriptación en blockchain
   - ¿Se puede hacer fraude en blockchain?
4. **Usos de blockchain en la gestión pública**
5. **Experiencias de blockchain en registros públicos**

SMART CONTRACTS EN 'TIEMPO REAL'

- https://www.blockchain.com/es/explorer?currency=ETH



Altura del Bloque	Antigüedad	Transacciones	Minero	Tamaño (KB)
6875813	16 seconds	51	0xea674fdde714fd979de3...	9.809
6875812	20 seconds	16	0x7c6694032b4db11ac485...	3.598
6875811	26 seconds	105	0x005e288d713a5fb3d7c9...	18.350
6875810	44 seconds	5	0x52e44f279f4203dcf680...	1.337
6875809	45 seconds	0	0x829bd824b016326a401...	533

¿QUÉ ES UN ‘SMART CONTRACT’?

¿CÓMO FUNCIONA UN SMART CONTRACT?

- Usted y otra persona **(que no conoce)** se encuentran en un bar de la ciudad en que transmitirán un partido **Alianza Lima** contra **Universitario**.
- Los dos quieren apostar 50 soles a quién acierte el ganador del partido, pero **por la no confianza**, los dos tienen razones para suponer que una vez hecha la apuesta, el perdedor intentará escabullirse.
- **Solución 1.-** Entregar el dinero antes del partido al barman **(autoridad central)** y que este pague al ganador al final.
- **Solución 2.-** Utilizar una app de Smart Contracts para apuestas

¿QUÉ ES UN SMART CONTRACT?

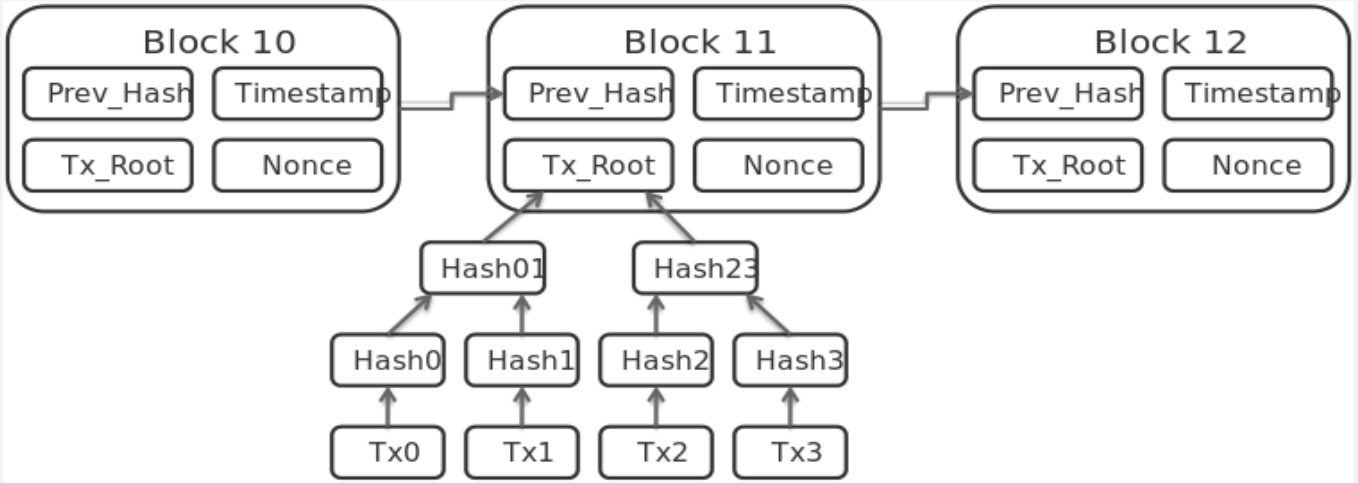
SMART CONTRACT COMO SISTEMA	SMART CONTRACT COMO 'CONTRATO'
• Agentes o nodos de software que comparten e interactúan en torno a un **registro distribuido**. (*shared ledger*) • La palabra "contrato" en este sentido supone que estos agentes-nodos de software cumplen con ciertas **obligaciones** y ejercen ciertos **derechos**, y pueden controlar ciertas acciones dentro del registro distribuido	• Contrato cuya característica principal es que se puede ejecutar de forma automática sin que sea necesaria la intervención de un tercero. • Acuerdos que pueden ejecutarse de manera consistente por una **red distribuida de nodos** que desconfían mutuamente y sin el arbitraje de una autoridad central.

‘SMART CONTRACTS VS. CONTRATOS CONVENCIONALES

CONTRATO CONVENCIONAL	‘SMART CONTRACT’
En caso de disputas las partes deben ‘conciliar’ o ir donde **una autoridad**	‘**Autoejecutable**’ no necesita de terceros, las disputas las dirime un **algoritmo**
Puede tener representación física (papel)	Tiene representación en una cadena de bloques **Blockchain**
Algunos registros legales se hacen en un **deposito centralizado** (oficina de registro)	Todas las operaciones se registran pero en un **deposito distribuido** o en red.
Se asume que partes ‘**confían**’ en el registro centralizado	Se asume que nodos-agentes **desconfían** entre sí
Seguridad del registro e información depende de protocolos de autoridad de registro	Seguridad del registro depende de **‘criptografía’**

¿BLOCKCHAIN?

Es una lista creciente de **registros distribuidos**, llamados **bloques**, que se vinculan mediante **criptografía**. Cada bloque contiene una **'huella digital'** encriptada del bloque anterior, una marca de tiempo y datos de transacción

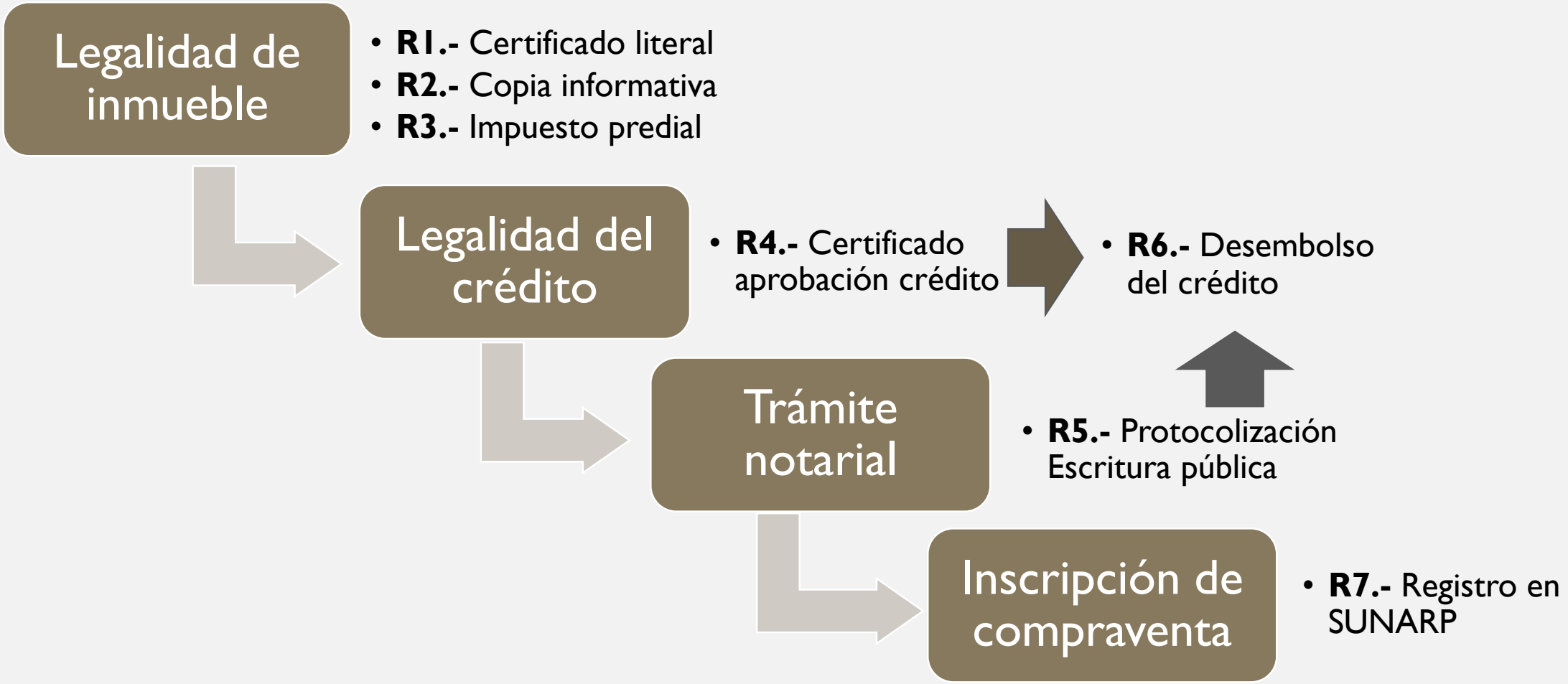


Características

1. **Replicado** todos los participantes de la red tienen una copia de todos los registros
2. **99.999% inalterable** dada su arquitectura criptográfica
3. **Accesible** en tanto que todos los participantes ven lo mismo al tiempo

CONTRATOS Y REGISTROS CENTRALIZADOS

- Suponga que A quiere vender a B un inmueble con una hipoteca de banco C



¿QUÉ SIGNIFICA QUE SEA UN **REGISTRO 'DISTRIBUIDO'**?

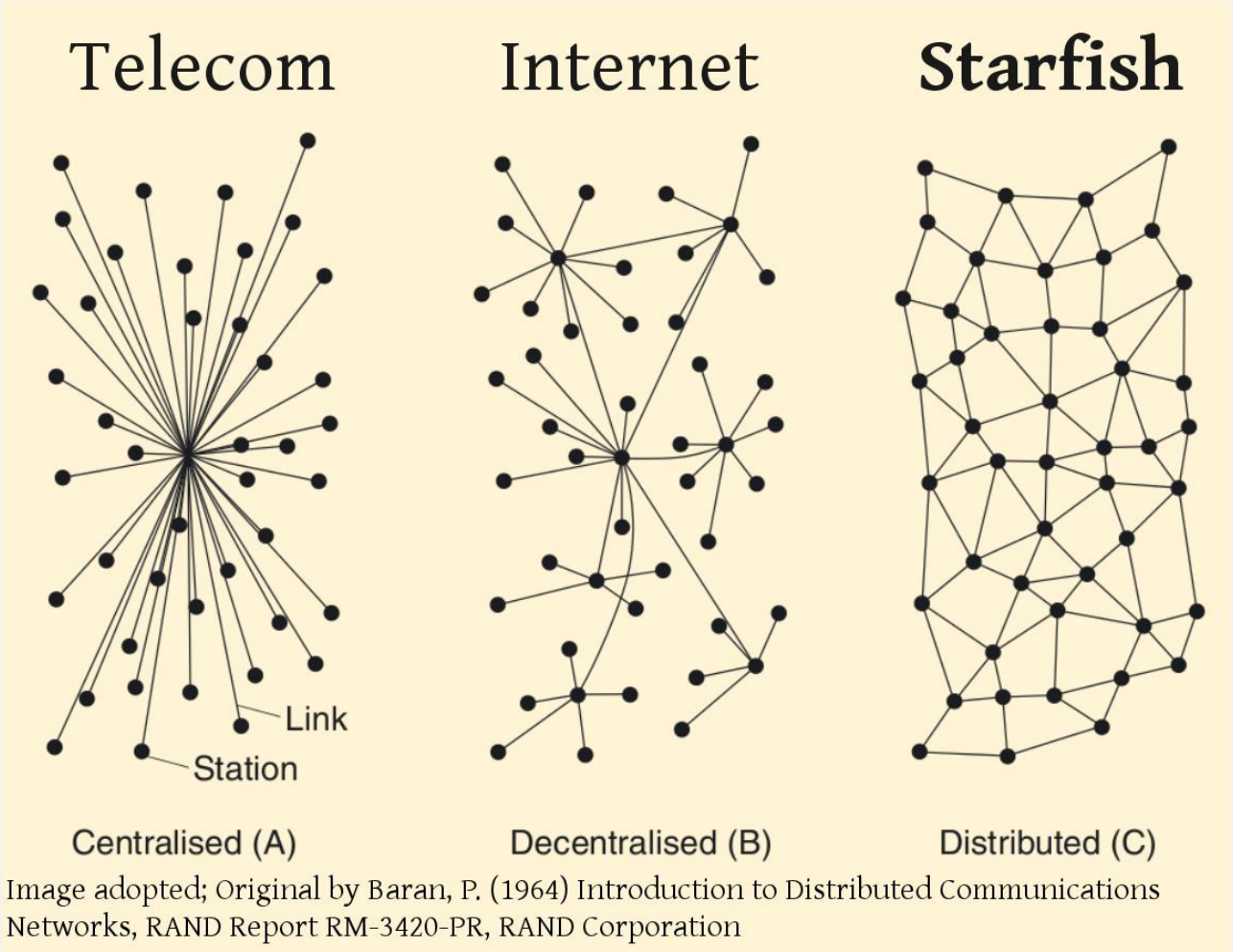


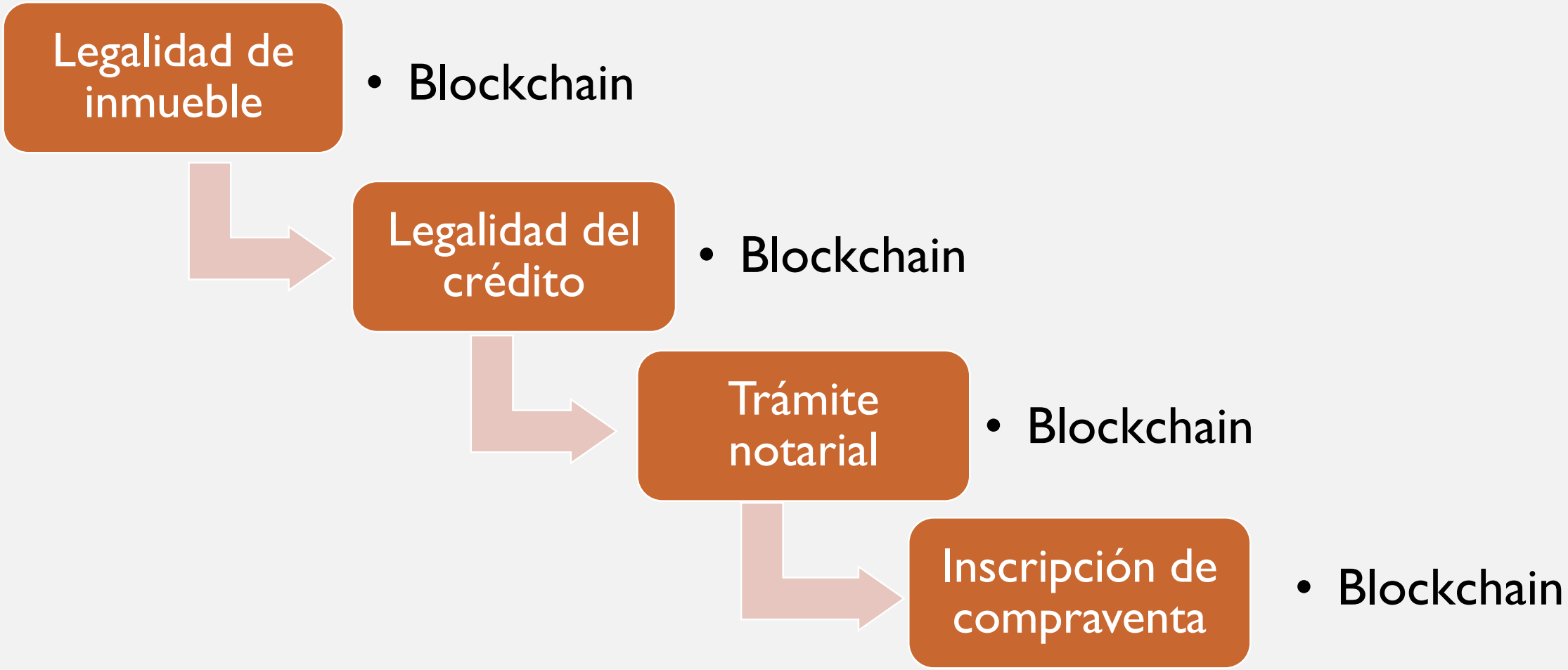
Image adopted; Original by Baran, P. (1964) Introduction to Distributed Communications Networks, RAND Report RM-3420-PR, RAND Corporation

Registro distribuido

- **Replicado:** Cuando se produce información todos los nodos reciben una copia.
- **Ausencia de centro** individual (Banco central) o colectivo (Internet)
- **Horizontal** Ningún nodo controla ninguna parte de la red
- **Transparente** La información no se puede filtrar (todos ven lo mismo)

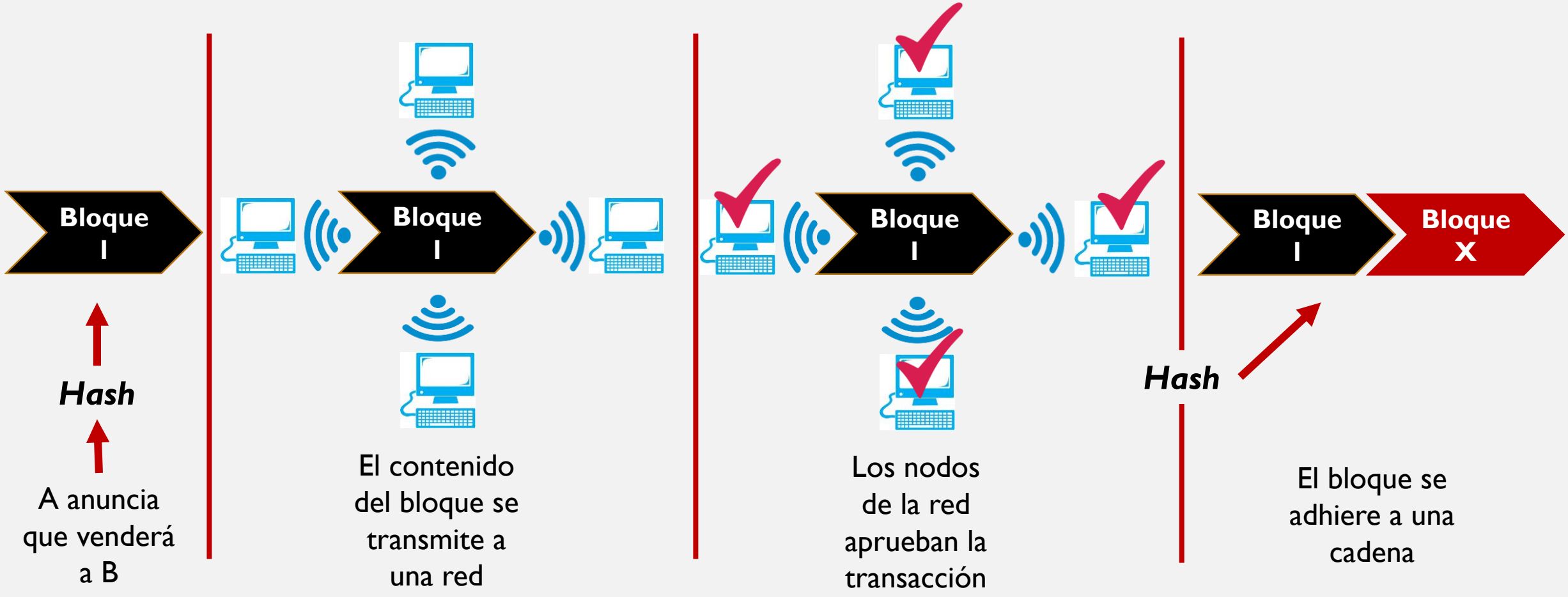
‘CONTRATOS’ Y REGISTROS EN BLOCKCHAIN’

- Suponga que A quiere vender a B un inmueble con una hipoteca de C



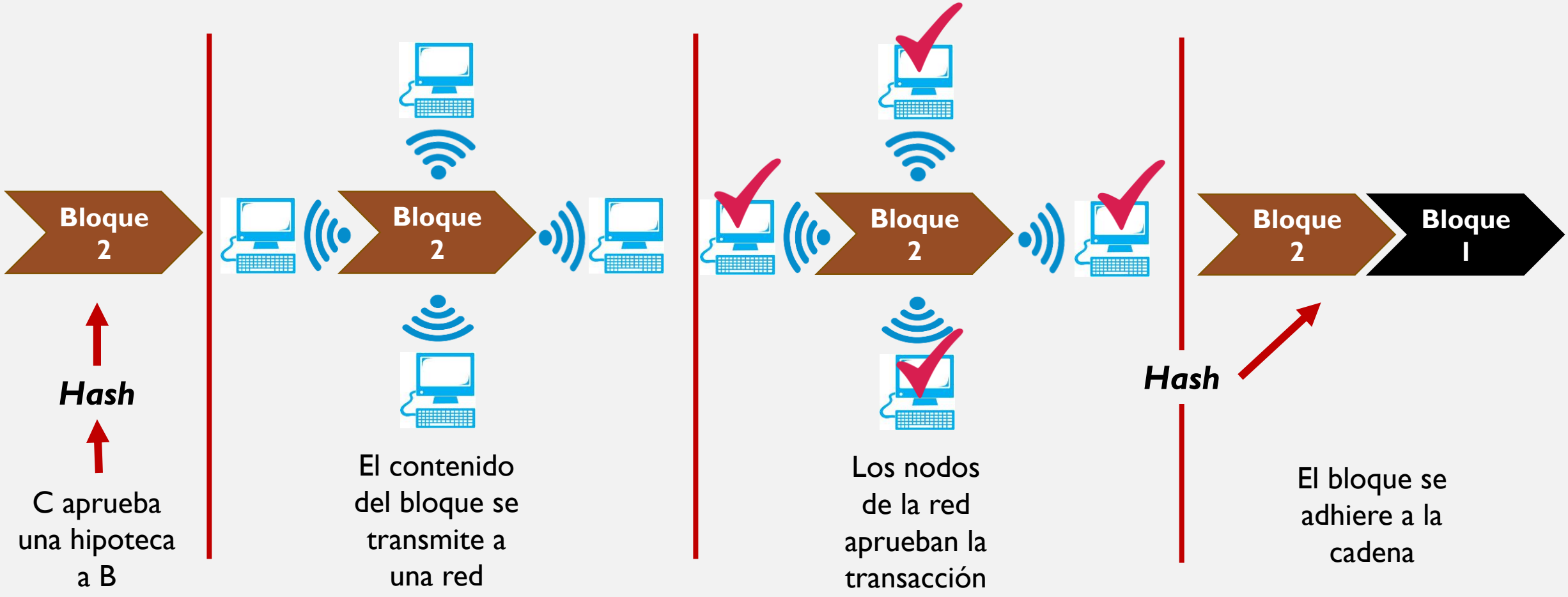
BLOCKCHAIN

- Suponga que **A quiere vender a B** un inmueble con una hipoteca de C



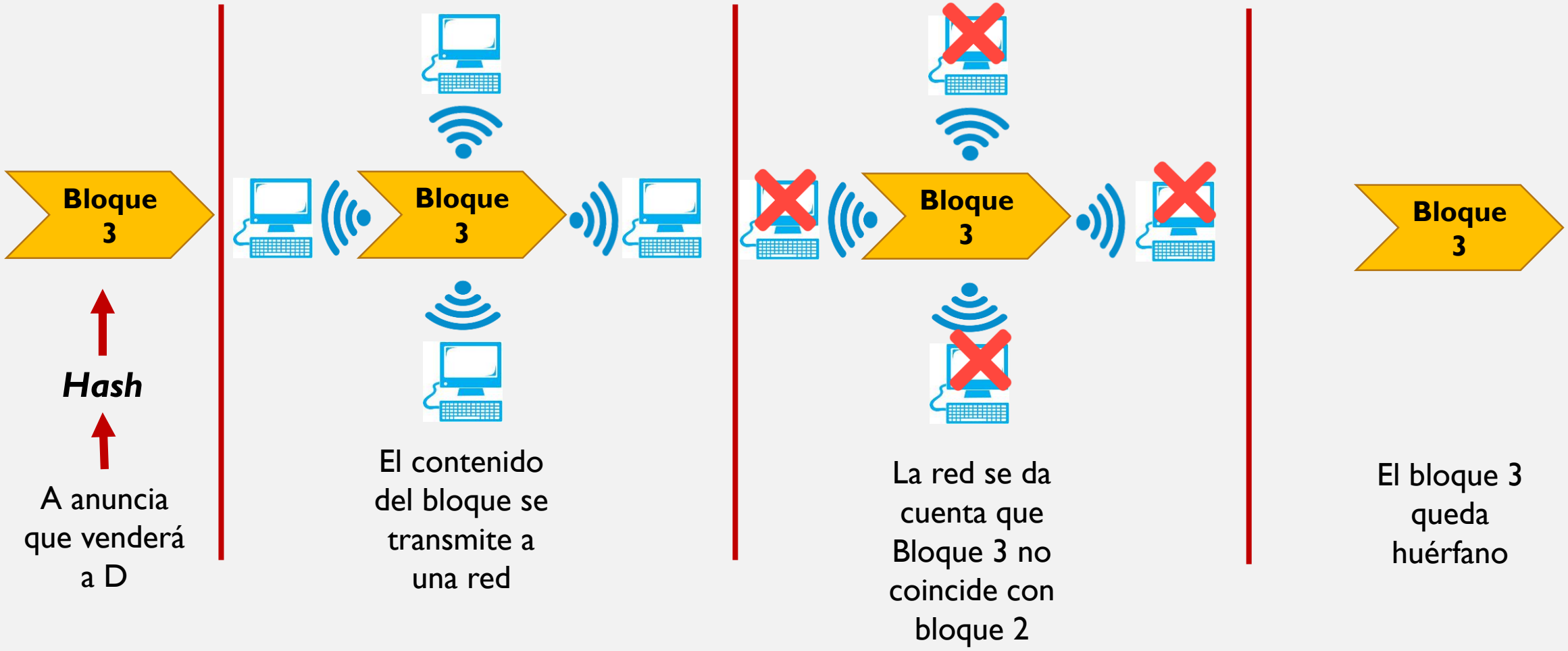
BLOCKCHAIN

- Suponga que A quiere vender a B un inmueble **con una hipoteca de C**



¿SE PUEDE DEFRAUDAR A BLOCKCHAIN?

- **Caso 1.-** Suponga que A quiere volver a vender lo mismo a D



¿DE QUE ESTÁ HECHO UN BLOQUE?

- ¿Qué es un **hash**? https://www.md5hashgenerator.com/
  - Es un algoritmo matemático que encripta cualquier contenido de datos y lo convierte en una serie de caracteres irrepetible y con una longitud fija
  - Independientemente de la cantidad de datos de entrada, el valor del hash de salida siempre tendrá la misma longitud.
  - Si se cambia una sola letra al dato de entrada, cambia completamente el hash
  - Comprobar que un dato de entrada genera cierto hash es muy fácil, pero deducir el dato de entrada de un hash necesita gigantescas capacidades de computación
  - La frase *'A vende a B'* puede *hashearse* y registrarse igual de fácil que una escritura pública de incluso de cientos de páginas.

¿DE QUE ESTÁ HECHO UN BLOQUE?

Daniel → Función Hash → 262031397020fd8df478ec13b4b096c5 

Daniela → Función Hash → 826acedae5686466ac4b3ccfec725ac0 

(Preambulo Constitución) → Función Hash → ed6bc3b3925d81a40b6958b9eaaefe41 

Función Hash → 7e4d32acdb26ae7764d7fc6c87e11843

¿DE QUE ESTÁ HECHO UN BLOQUE?

262031397020fd8df478ec13b4b096c5
826acedae5686466ac4b3ccfec725ac0
ed6bc3b3925d81a40b6958b9eaaefe41

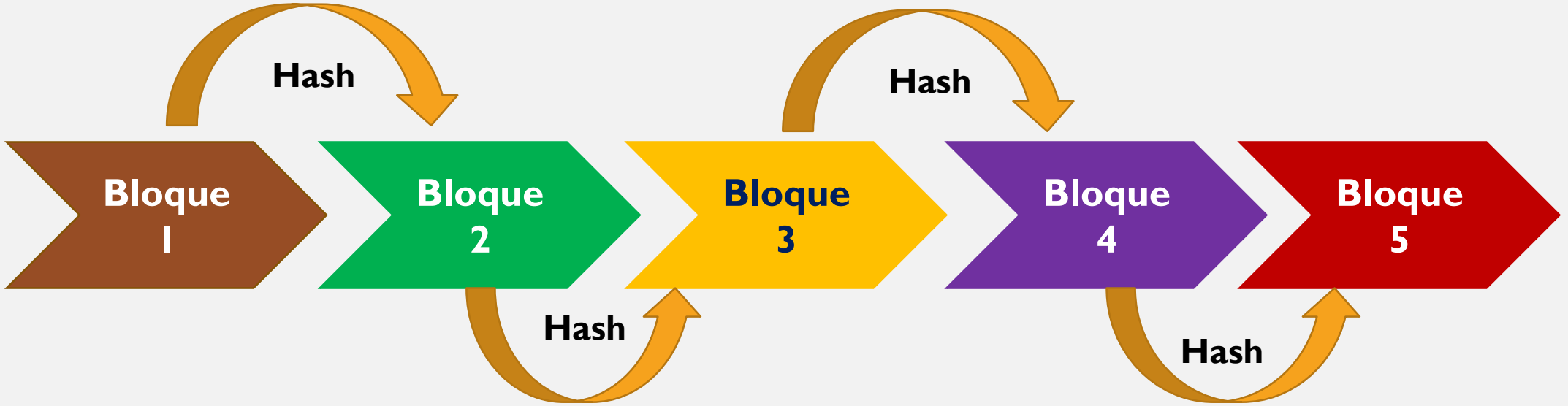
7e4d32acdb26ae7764d7fc6c87e11843

¿Qué bloque de información genera este hash?

"Prueba de trabajo" (PoW)

Hipoteca = 138a395b38564257b7f1ed677545fd17

Embargo = 34668aea00cecc152cadc65aa483a1f9


Hash
Hash
Hash
Hash
Bloque 1
Bloque 2
Bloque 3
Bloque 4
Bloque 5

¿SE PUEDE DEFRAUDAR A BLOCKCHAIN?

Caso 2.- Suponga que A quiere **modificar el bloque I** para volver a vender

Suponga que alguien quiere manipular el registro para su propio provecho (**corrupción**)

Esto es imposible

1.- Debe saber en qué **nodos** hay una copia del bloque I en el registro distribuido

2.- Debe convencer o ofrecer dadivas ($$$) a cada uno de los **nodos** que tiene el bloque I para que lo modifique

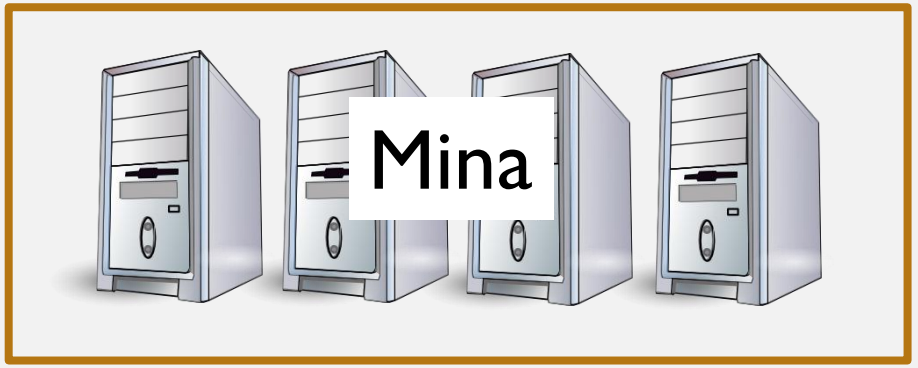
3.- Debe ser mas rápido y con mayor capacidad de computo que todos los **mineros de bloques.**

4.- Debe hacerlo antes de que se cree el siguiente bloque

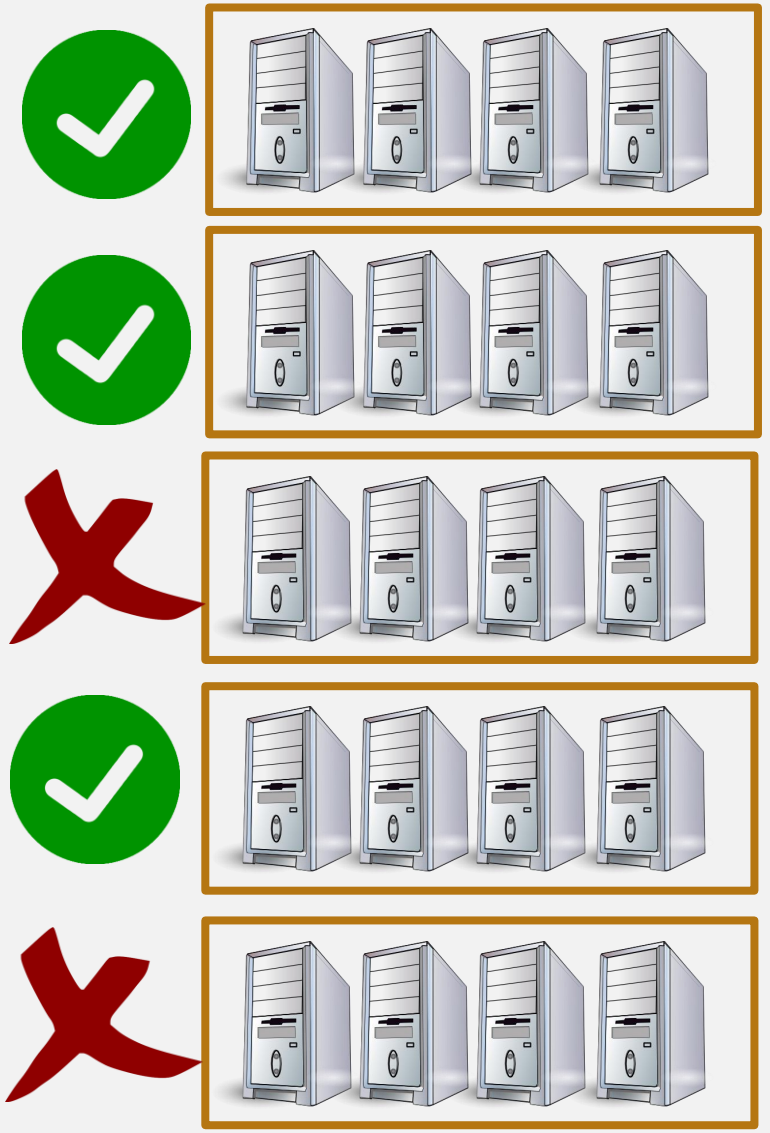
¿CÓMO SE APRUEBA UNA TRANSACCIÓN ES REAL?
EL CONSENSO EN BLOCKCHAIN

7e4d32acdb26ae7764d7fc6c87e11843

¿Qué bloque de información genera este hash?



"Prueba de trabajo" (PoW)



60%

Valida la *PoW*

Puede crearse otro bloque

Bloque X

¿SE PUEDE DEFRAUDAR A BLOCKCHAIN?

Suponga que A quiere **modificar el bloque I** para volver a vender (**Fraude**)

Esto es imposible

1.- Debe saber quiénes tienen copia del bloque I en el registro distribuido	Plataforma Ethereum tiene 30.000 nodos
2.- Debe convencer a cada uno de los que tienen bloque I que lo modifique	
3.- Debe ser mas rápido y con mayor capacidad que todos los demás mineros	Nadie tiene esta capacidad de computación en el mundo
4.- Debe hacerlo antes de que se cree el siguiente bloque	

Bitmain Ordos
(Mongolia)
25.000 computadores minando

BLOCKCHAIN VS. SISTEMAS CENTRALIZADOS DE REGISTRO

Característica	Sistema centralizado	Blockchain
Administración de la información	Existe un administrador de la información.	La información se encuentra **distribuida**.
Sistema de seguridad	El administrador debe implementar un sistema de seguridad con la finalidad de proteger la información.	Existe un sistema **criptográfico**, el cual puede variar a través de algoritmos de encriptación.
Transparencia	El administrador puede opacar los procesos de seguridad y nivel de acceso a la información	Los participantes del sistema tienen la posibilidad de acceder a la información y verificarla a través de la cadena de bloques.
Protección de información sensible	El administrador decide cómo protege información sensible	Es posible tanto hacer totalmente abierta la infomación hasta mantenerla 100% oculta a través de **encriptación**

BLOCKCHAIN VS. SISTEMAS CENTRALIZADOS DE REGISTRO

Característica	Sistema centralizado	Blockchain
Costos De administración	Se materializan costos por razón de la infraestructura tecnológica y en materia de la ciberseguridad que requiere el administrador central en el manejo de la información.	Hay una reducción de costos ya que el manejo de la información es reemplazado por códigos algorítmicos, los cuales, a través de nodos, procesan y verifican la información de forma independiente de cada transacción.
Alterabilidad de la información	Depende de los sistemas tecnológicos de ciberseguridad con que cuenta el administrador, los cuales no son inmunes a ataques cibernéticos.	Al existir una distribución de la información, la cual está organizada en bloques por medio de procesos algorítmicos, la manipulación y alteración de dicha información **es fácticamente imposible de realizar.**

FORMAS DE LA TECNOLOGÍA BLOCKCHAIN

Característica	Sistema público	Sistema privado
Definición	En este sistema, cualquier parte está en la posibilidad de participar en el proceso sin ningún tipo de verificación (Deloitte, 2017b, p. 4).	Existe un administrador que evalúa la participación de un agente dentro del sistema.
Riesgos	**Sistema rígido:** Una vez la administración está en manos de los mineros, es muy difícil controlar el sistema. No existen criterios para verificar los antecedentes de los participantes del proceso.	**Sistema flexible:** Se pueden modificar los protocolos iniciales para fijar reglas de quienes pueden o no participar en el sistema Mayor protección de la información de los participantes

VENTAJAS DE BLOCKCHAIN

- **99.999% inmune al fraude o a los hackers.**
- **Es imposible que la información se pierda.**
- **¡Nueva era de la función de registro!:**
  - Todo el proceso de certificación, autenticación y registro de documentos la pueden hacer maquinas conectadas a blockchain.
  - Ahora se puede registrar transacciones que antes era impensable (*vgr.* tener acceso a todas las transacciones que haga cualquier persona)

VENTAJAS DE BLOCKCHAIN

- **Completamente 'customizable' para las necesidades**
  - En Internet se pueden conseguir apps 'blockchain'
  - www.stateofthedapps.com registra 1899 apps 'blockchain' para igual número de necesidades.

ALGUNOS USOS DE 'BLOCKCHAIN' EN SECTOR PRIVADO

Microsoft Azure

Almacenamiento en la nube

Seguimiento de carga y logística marítima

IBM

MAERSK

Prevención de fraudes, manejo de coberturas y pago de indemnizaciones

'Smart Contracts'

ALGUNOS USOS DE 'BLOCKCHAIN' EN SECTOR PÚBLICO

Crypto Valley

Proyecto de gobierno Suizo para identificar residentes y votaciones en línea

---

Certificar calidad y no alteración de información y precios de energía en Chile

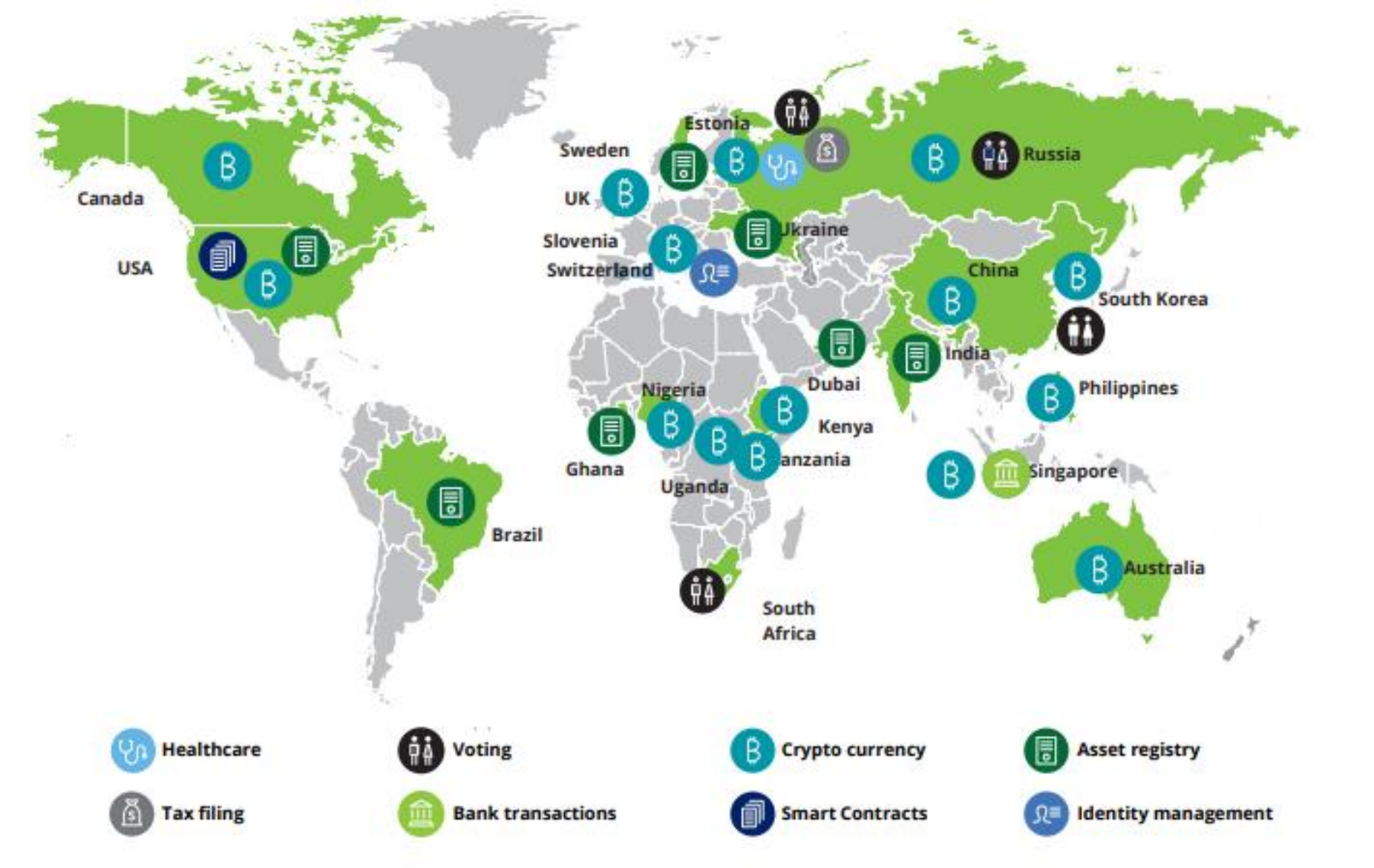
CNE | COMISIÓN NACIONAL DE ENERGÍA

---

essentia.one
INTEROPERATIONS AND DATA FOR THE NEW INTERNET

Aplicación de gobierno holandés para el control de acceso en las fronteras

Experiencias de gestión pública basada en blockchain (2017)



Brasil
Ucrania
Georgia
Estonia
India
EE.UU.
Suecia

BLOCKCHAIN Y FUNCIÓN REGISTRAL

Registering property (rank)	4
Score for registering property (0–100)	92.86
Procedures (number)	1
Time (days)	1
Cost (% of property value)	0.0
Quality of land administration index (0–30)	21.5

Georgia

Registering property (rank)	45
Score for registering property (0–100)	74.89
Procedures (number)	5
Time (days)	7.5
Cost (% of property value)	3.3
Quality of land administration index (0–30)	17.5

Perú

Registering property (rank)	59
Score for registering property (0–100)	71.22
Procedures (number)	7
Time (days)	15
Cost (% of property value)	2.0
Quality of land administration index (0–30)	16.5

Colombia

BLOCKCHAIN Y FUNCIÓN REGISTRAL

National Agency of Public Registry Georgia (NAPR)

Primer país del mundo en que todos los registros de propiedad inmueble y copias de escrituras públicas están guardados y respaldados en **blockchain**.

Balance

- A Junio de 2018 había cargadas 1'5 millones de documentos en el registro
- El sistema ha permitido que función registral sea mas transparente para ciudadanos.
- Ha permitido reducir la alta informalidad en la propiedad (75% para su independencia en 1991) y la alta incidencia del fraude en el registro.
- Gobierno ha iniciado proyecto para incorporar modulo de 'Smart Contracts' para transferencias de propiedad.

LOS RETOS FUTUROS DE BLOCKCHAIN

1. **Solucionar el problema energético:** La capacidad de computo que exige 'blockchain' supone un elevado consumo energético y despliegue de infraestructura de computo, lo cual hoy día no está medido su impacto.
2. **Avanzar hacia un estándar universal en registros:** Existe una competencia hoy entre programadores por desarrollar el mejor 'estándar'. La no estandarización afecta la masificación de la tecnología (economía de redes)
3. **Cambio en paradigma y mentalidad:**
    - Los registros centralizados probablemente desaparezcan en menos 5 años.
    - Las certificaciones y autenticaciones por 'humanos' desaparecerán

LOS RETOS FUTUROS DE BLOCKCHAIN

3. **Cambio en paradigma y mentalidad:**
    - La idea de 'fe pública notarial' va a ser modificada por la confianza en la infalibilidad de blockchain
    - Blockchain habla de una 'verdad registrada', pero blockchain no puede controlar la verdad fuera del registro, es decir, la causa de las transacciones que están en los bloques.
    - Los notarios ni los registradores van a desaparecer, porque son ellos los que controlan la 'verdad' fuera de blockchain
    - Abogados y funcionarios deben entrenarse para comprender conceptos como 'encriptación', 'programación', 'algoritmos'.

LA FUNCIÓN REGISTRAL EN UN MUNDO DE **SMART CONTRACTS Y BLOCKCHAIN**

Daniel A. Monroy
2018

Universidad Externado de Colombia

sunarp