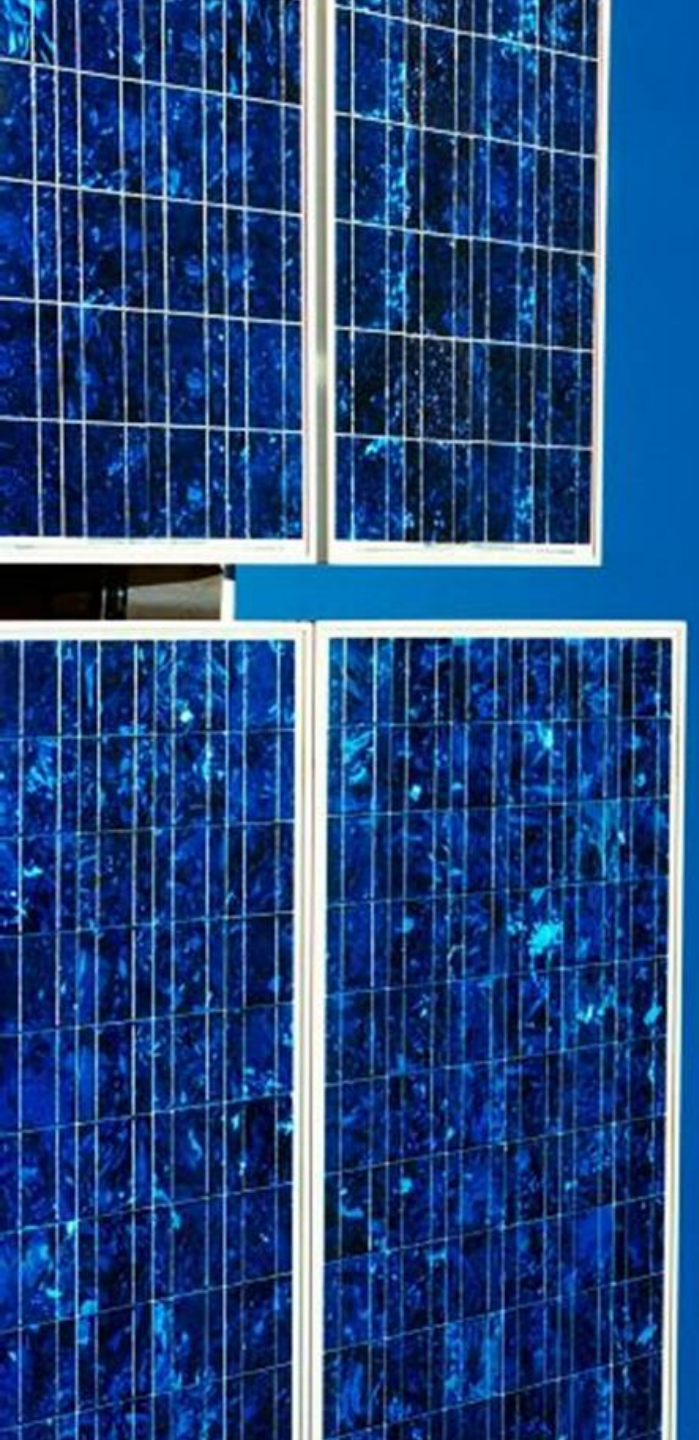


KPMG

Blockchain: Aplicaciones Prácticas

Otto Mora, KPMG Management Consulting

Febrero 2017

Con ustedes hoy

Otto Mora
Supervisor
Management Consulting
KPMG
ottomora@kpmg.com

Luis Rivera
Director
Management Consulting
KPMG
lgrivera@kpmg.com

Contenidos

¿Que tanto conoces de Blockchain?

Blockchain – ¿Que es?

Beneficios e Implicaciones

Caso de Estudio: Smart Contracts

Caso de Estudio: Identidad Digital

Preguntas

KPMG

¿Que tanto conoces de Blockchain?

Blockchain es un derivado de soluciones basadas en Bitcoin

VERDADERO o FALSO

Todas las soluciones de plataformas Blockchain utilizan solo un tipo de crypto-moneda (es decir BITCOIN)

VERDADERO o **FALSO**

Tipos de Cripto-Monedas

Año	Moneda
2009	Bitcoin
2011	Namecoin
2011	Litecoin
2013	Dogecoin
2013	Nxt
2013	Ripple –XRP [1]
2014	Auroracoin
2014	BlackCoin
2014	BitShares
2014	Dash
2014	DigitalNote

Año	Moneda
2014	MazaCoin
2014	Monero - XMR
2014	Stellar – XLM (lumens)
2015	Decred
2015	Ethereum – ETH [2]
2016	Ethereum Classic (fork de Ethereum)
2016	Steem
2016	Zcash
2016	Rootstock – RSK [2]

1) A RIPPLE TAMBIEN SE LE CONOCE COMO UN CONSENSUS BASED PAYMENT NETWORK
2) ETHEREUM Y ROOTSTOCK TAMBIEN PERMITEN CREAR SMART CONTRACTS

KPMG

Dentro de un periodo de 5 a 7 años tendremos todos nuestros sistemas internos de reconciliación y transferencias internacionales en Blochain.

VERDADERO o **FALSO**

Los costos operativos para los servicios Financieros se espera se reduzcan en un:

1. 5 – 12%
2. **20 – 40%**
3. 45 - 55%
4. 60 - 80%

En Costa Rica tenemos una empresa dedicada a “minar” Bitcoin con energía solar.

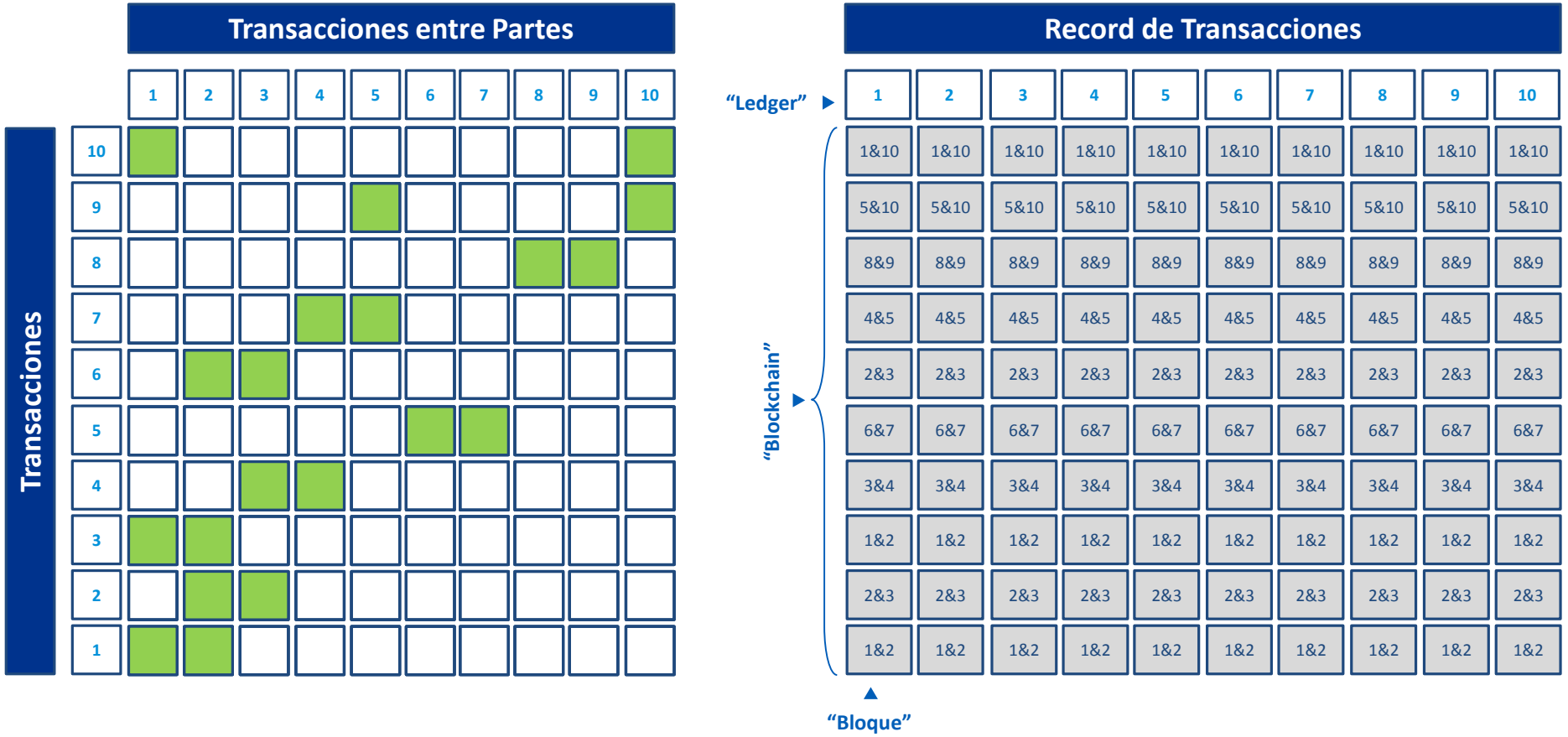
VERDADERO o FALSO

KPMG

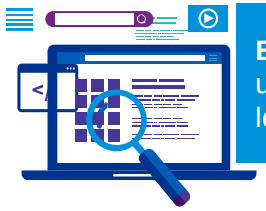
Blockchain – ¿Que es?

Que es un "Bloque", "Blockchain", y "Ledger" Distribuido?

Un *Blockchain es un record permanente de las transacciones* en una red. El sistema se protege mediante el uso de una referencia al bloque anterior ("*hash*"), el cual es encriptado. Tratar de manipular el sistema sería tan evidente que cualquier cambio ilegítimo puede ser detectado y cancelado.



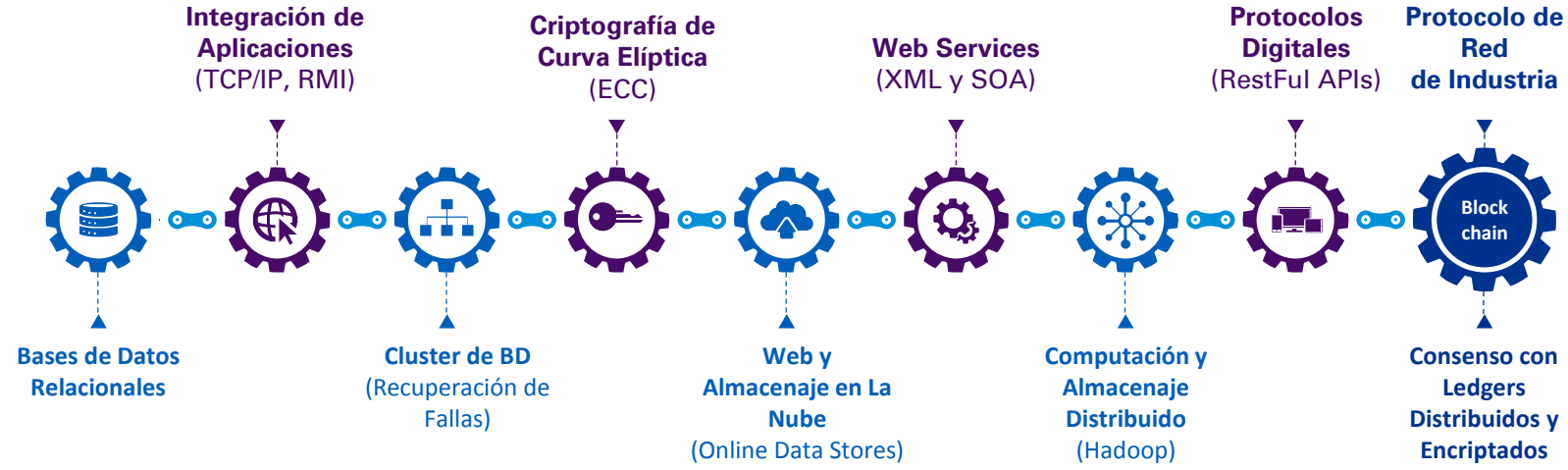
También es un concepto de Arquitectura de Sistemas



El concepto de un ledger distribuido (DLT) fue sintetizado en 1990. El Blockchain fue introducido como una plataforma de ledger distribuido para la aplicación Bitcoin en el 2009, y es la implementación de un ledger descentralizado por medio de una mecanismo de consenso anónimo.

El espectro de tecnologías de ledgers distribuidos disponibles en estos momentos tiene el objetivo de resolver los problemas de redundancia de datos y los costosos procesos de reconciliación con modelos organizacionales únicos procedimientos de consenso.

Evolución de Tecnologías pilares para permitir las DLT's



Fuente: KPMG Research

Tecnologías de Ledger Distribuido (DLTs)

LAS DLTS SON UN METODO PARA ORDENAR Y VERIFICAR TRANSACCIONES EN UN LEDGER DISTRIBUIDO

1 Iniciar Transacción

- La transacción toma lugar entre dos o mas partes
- Todas los detalles de la transacción son grabadas incluyendo detalles de fecha, hora, participantes, y monto

2 Postear y Grabar transacción en la red

- La transacción se agrega en el orden en que es recibida en un 'bloque' de la red
- Se pueden agregar registros, pero no se permite el borrado de un registro anterior
- Cada nodo en la red tiene una copia completa del ledger con los registros

3 Transmitir

- El 'bloque' es transmitido y se propaga a todos los nodos en la red
- La red de nodos de computadoras verifica y valida las transacciones en el bloque ejecutando el software que mantiene el ledger actualizado

4 Validar por medio del consenso y confirmar

- La red verifica, y valida la transacción; la confirmación se transmite a otros nodos
- El Consenso (mecanismo matemático acordado) se registra y provee una base para asegurar la confiabilidad

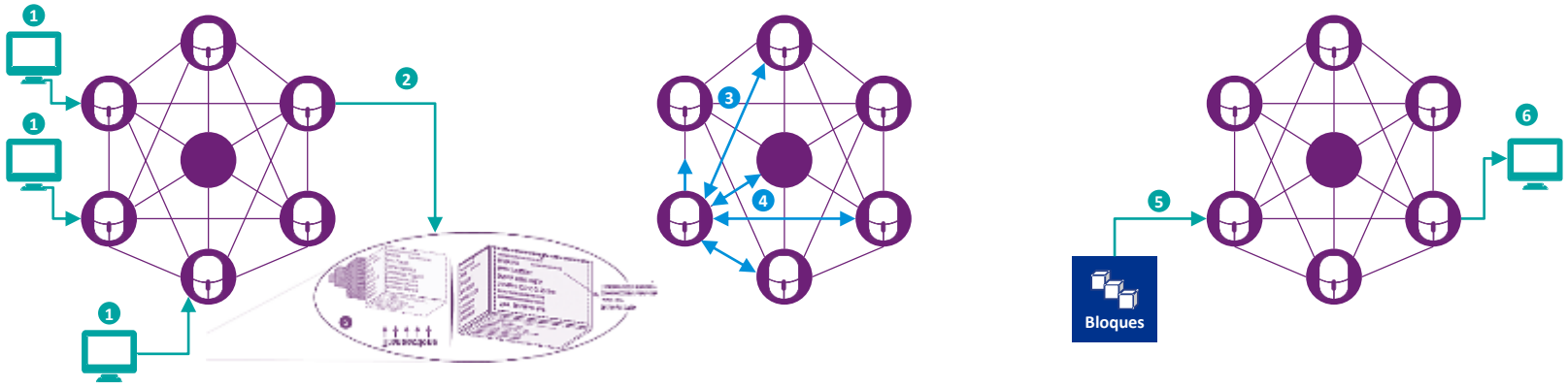
5 Bloque encriptado e inmutable

- El bloque confirmado es agregado de manera cronológica a la cadena
- Esto provee un registro transparente de todas las transacciones y puede funcionar como una pista de auditoría digital
- Los datos son persistentes y esto resulta en un registro confiable de las transacciones

6 Transacción completada

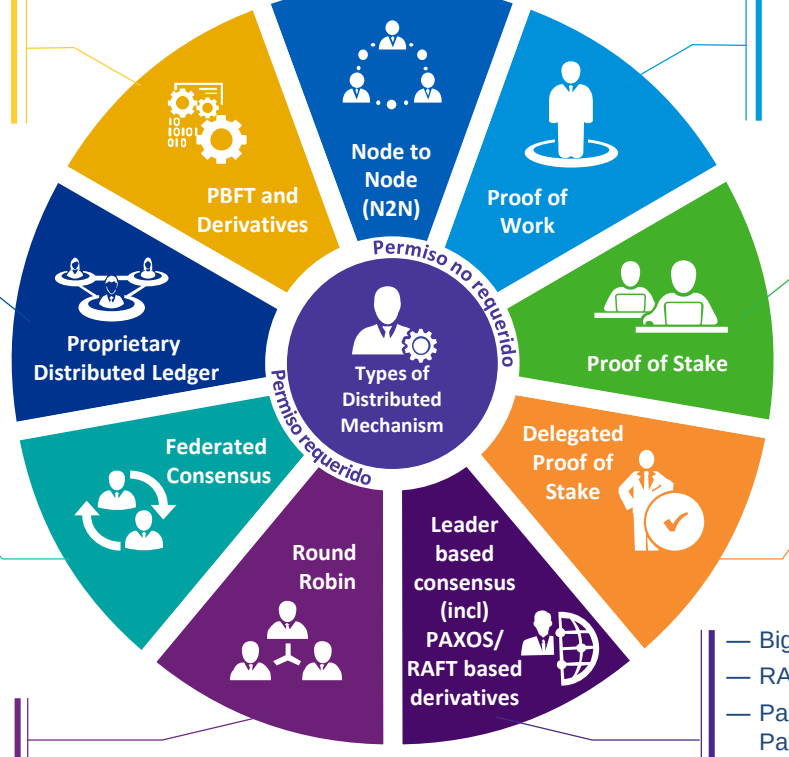
- Los Nodos tienen acceso a una única fuente compartida de la verdad
- Un bloque completado da paso al próximo bloque en el blockchain

Aplicación del Mecanismo de Consenso



Fuente: KPMG Research

Mecanismos de Consenso



— Concurrencia Distribuida
— Corda (R3 CEV)

— PBFT (Practical Byzantine Fault Tolerance)
— Derived PBFT (Hyperledger project)
— RBFT (Redundant Byzantine Fault Tolerance, e.g., Evernym)
— SBFT (Simplified Byzantine Fault Tolerance e.g., Chain)

— Bitcoin
— Colored Coins
— Metacoins Propietarias
— DAG (Directed Acyclic Graphs)
— Factom
— Coinprism

— Openchain
— PoET (Proof of Elapsed Time) by Intel (Sawtooth Lake Project)

— CASPER
— Ethereum (moving to PoS)

— Ripple (evolucionando hacia el protocolo Inter-Ledger)
— Stellar (fork de Ripple)

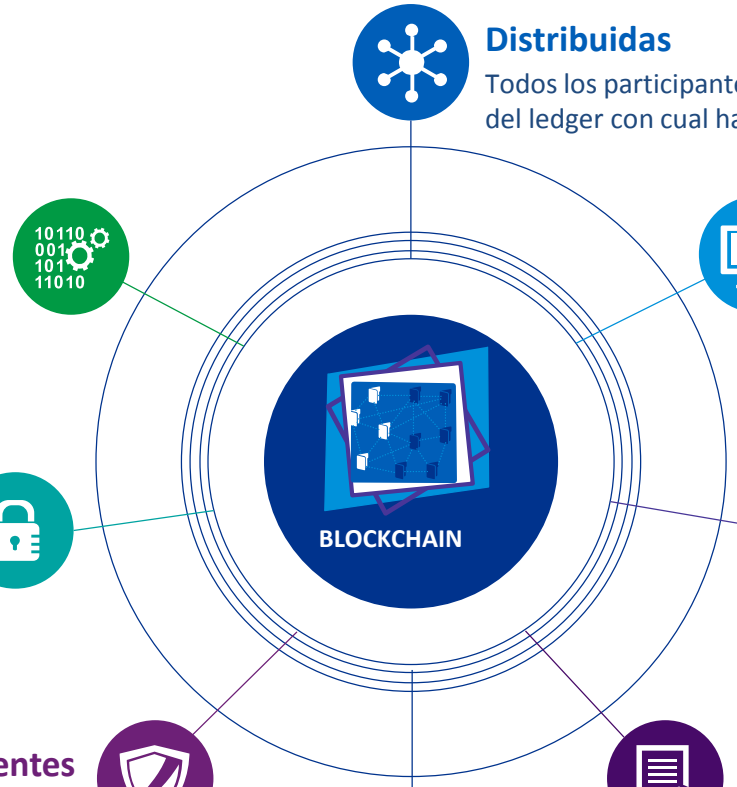
— Graphene
— Steem
— BitShares

— MultiChain
— Tendermint

— BigChainDB
— RAFT
— Paxos (incluyendo variantes como Fast Paxos, Egalitarian Paxos etc.)
— Juno (Raft-Hardened Tangaroa; JP Project)
— Tangaroa
— Mencius
— Veiwstamped Replication
— ZAB

Fuente: KPMG Research

Algunas propiedades de las DLTs



Distribuidas
Todos los participantes en la red tienen una copia completa del ledger con cual hay transparencia

Anónimas / Pseudoanónimas
Las identidades de los participantes es pseudonanónima o anónima dependiendo del la plataforma

Registros con Fecha y Hora
El *timestamp* de las transacciones se registra en los bloques

Unánimes
Todos los participantes en la red se ponen de acuerdo con respecto a la validez de las transacciones

Confiables
No se necesitan intermediarios para poder garantizar la confiabilidad de los otros participantes

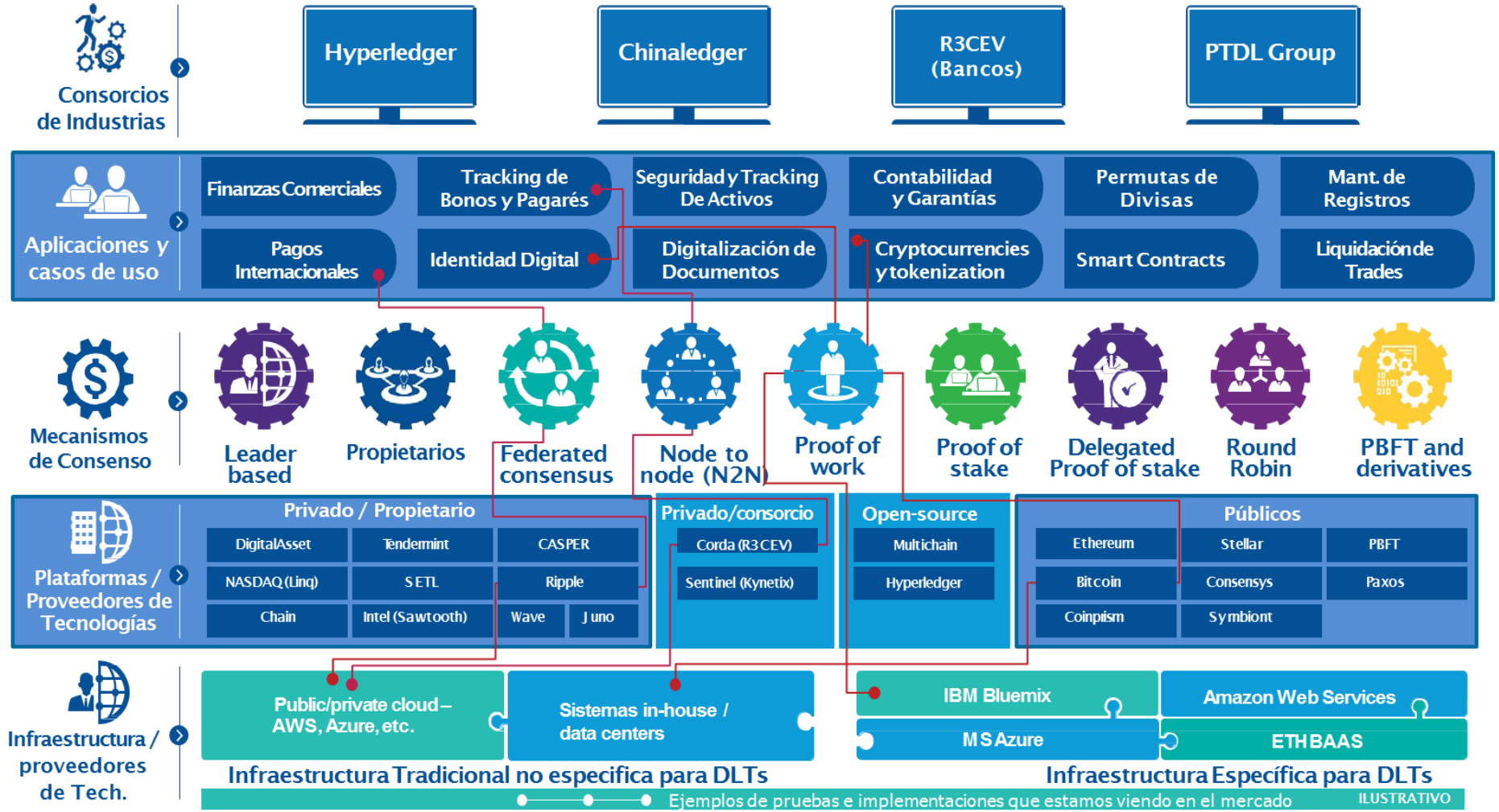
Inmutables / Persistentes
Cualquier registro que se validado es irreversible y no puede ser cambiado

Seguras
Todos los registros son encriptados individualmente

Programables
Un blockchain puede ser programable específicamente en el caso de los “Smart Contracts”

Fuente: KPMG Research

Ecosistema de Tecnologías DLT



Fuente : KPMG Research, Sigrid Seibold

KPMG

Implicaciones y Beneficios

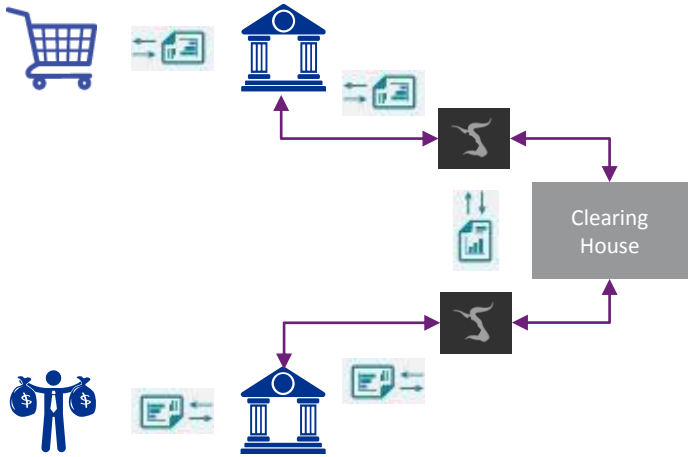
¿Porque son disruptivas?

El paradigma de descentralización de las plataformas blockchain permite tener ledger distribuidos en tiempo casi real con un mecanismo de consenso para facilitar las transacciones entre participantes

Transferencias – Hoy

La estructura tradicional de transferencias, especialmente las transferencias internacionales depende de terceros para poder transferir dineros:

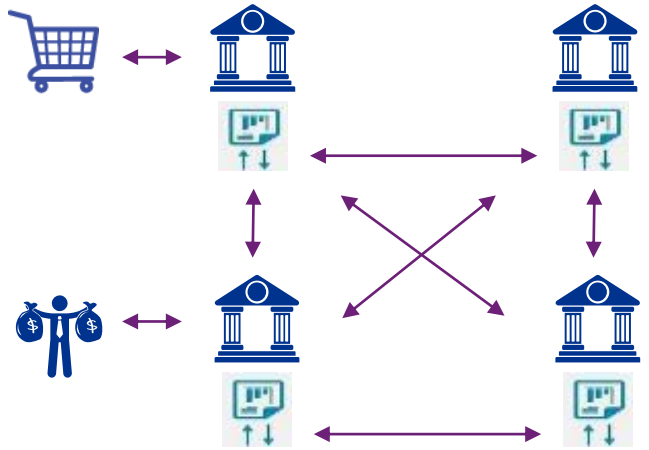
- Infraestructura legada
- Liquidación lenta T+n
- Trabajo manual intensivo
- Probabilidad de errores



Transferencias – mediante Blockchains

La transferencia de los dineros se realiza a través de una red soportada por una plataforma blockchain:

- Infraestructura compartida
- Procesamiento automatizado
- Seguridad criptográfica



Simbología

Institución Financiera | Custodio | Transacción | Custodio | Origen | Destinatario

Ambiente Competitivo

Clientes	Casos de uso	Inversión Realizada
Goldman Sachs	Securities Settlement Leveraged Loan Trading AML and KYC Compliance Cross Border Payments	• Invirtió en el **Consorcio R3CEV** • Invirtió en **Digital Asset Holdings** • Miembro de la **Linux Foundation**
JP Morgan	Smart Contracts for Credit Default Swaps Cross Border Payments Syndicated Loans	• Lanzó **Project Juno** un "distributed cryptoledger“ y mantiene una alianza con la Linux Foundation en Hyperledger • Invirtió en el **Consorcio R3CEV** • Invirtió en **Digital Asset Holdings** • Miembro de la **Linux Foundation**
Bank of America	Smart Contracts for Credit Default Swaps Trade Finance	• Invirtió en el **Consorcio R3CEV** • Invirtió en **Digital Asset Holdings**
Citi	Cross Border Payments Smart Contracts for Credit Default Swaps	• Invirtió en el **Consorcio R3CEV** • Invirtió $30m en **Chain.com**, es el primer cliente en utilizar la nueva plataforma Linq de Nasdaq, para explorar usos de los ledgers distribuidos en la arquitectura de las transacciones financieras • Invirtió en **Digital Asset Holdings**
Barclays	Trade Finance	• Invirtió en el **Consorcio R3CEV** • Alianza con Safello un exchange de bitcoin
Santander	Securities Settlement Cross Border Payments Derivatives Trading and Settlement	• Invirtió en el **Consorcio R3CEV** • Invirtió $100m en **Innoventure,** un fondo de inversión Fintech en 2014 empezando con $100M y incrementándolo año con año para hacer inversiones en startups de fintech y blockchain • Invirtió en **Digital Asset Holdings**

KPMG

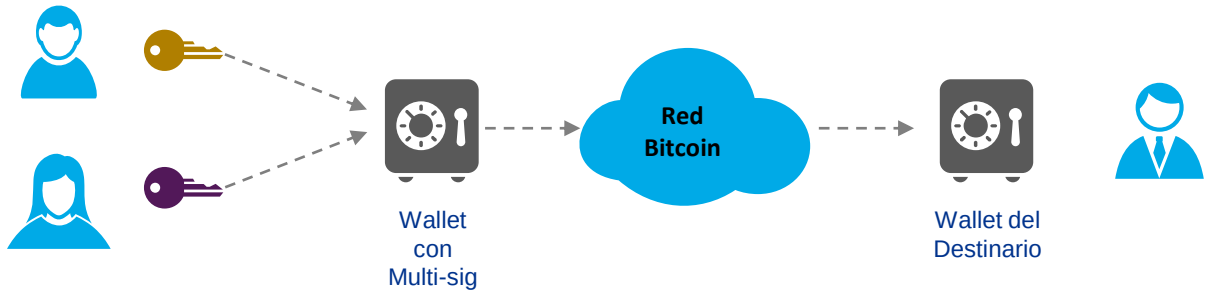
Caso de Estudio: Smart Contracts

¿Qué es un Smart Contract?

El concepto de Smart Contracts fue propuesto por primera vez por el criptógrafo Nick Szabo en 1994.
La definición mas común es la siguiente:

> *"Los Smart Contracts son programas de computación que permiten asegurar y hacer cumplir la ejecución de acuerdos previamente registrados entre personas y organizaciones. Como tales, permiten asistir en la negociación y definición de estos acuerdos"*

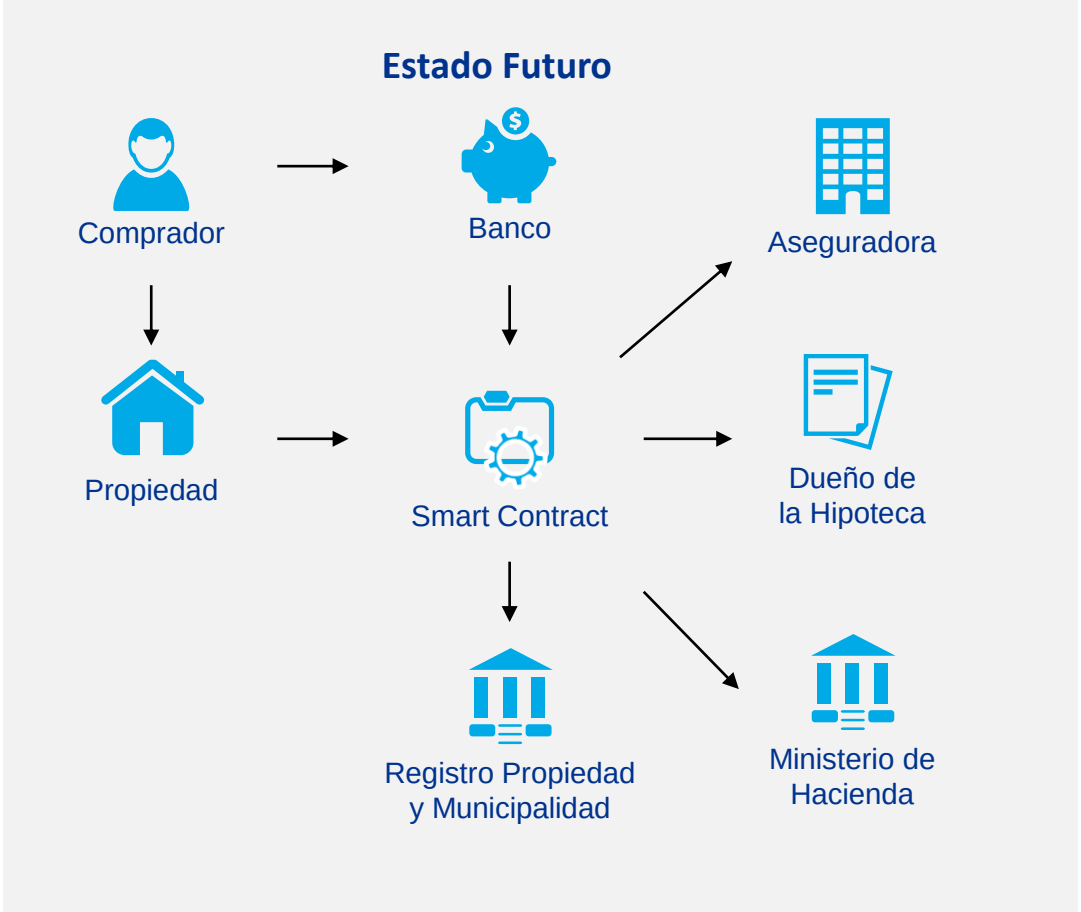
El ejemplo mas sencillo de Smart Contracts en uso en la actualidad son las cuentas multi-signature en Bitcoin. Estas son un tipo de cuentas mancomunadas que establece que dos o más individuos deben firmar una transacción antes de autorizar el envío de bitcoins hacia otra cuenta.



La definición es un poco más complicada porque se permite definir también que *M de N* firmas estén de acuerdo, por ejemplo que con 3 firmas de las 5 registradas se ejecute una transacción.

Smart Contracts para Préstamos Hipotecarios

Los préstamos hipotecarios habilitados con Smart Contracts permiten el procesamiento automático de los pagos y la liberación de las retenciones sobre la propiedad.



Casos de Uso de los Smart Contracts y Plataformas Blockchain

Hay muchas aplicaciones para los Smart Contracts pero veamos algunos usos para industria de servicios financieros:

Mercados de Capital y Investment Banking	Banca Comercial y de Consumo	Seguros

• Finanzas Corporativas:
  • Oferta Públicas Iniciales (IPOs)
  • Capital Privado
• Transacciones Financieras Estructuradas: Créditos sindicados, prestamos apalancados
• Infraestructura de mercados bursátiles
	• Finanzas Comerciales: documentación de cadena de suministros, facturación, pagos
	• Préstamos hipotecarios
	• Prestamos y crowfunding para empresas nuevas y PYMES
		• Procesamiento automatizado de reclamos en seguros de automóviles, seguros agrarios, etc.
		• Prevención del fraude en los bienes de lujo
		• Productos nuevos: seguros para el sharing economy, vehículos autónomos, seguros persona-a-persona, cyber-seguros

Principales Plataformas: ethereum RSK ROOTSTOCK SMART CONTRACTS

Implicaciones de los Smart Contracts

¿Que cosas implican los Smart Contracts?

- Procesos donde tengamos tres o mas partes interesadas pueden ser descentralizados y automatizados, los acuerdos legales de los contratos de papel tradicionales pueden ser codificados en Smart Contracts sobre plataformas blockchain
- Posibilidad de abaratar costos y agilizar procesos manuales
- Disrupción a muchos modelos de negocios tradicionales con intermediarios (agentes de seguros, prestamistas, abogados notariales y registrales) y nuevos modelos de negocio con organizaciones descentralizadas y autónomas (*DAOs*)
- En cierta manera el código de computadoras puede llegar a ser ley (*code is law*), en el tanto las legislaciones empiecen a reconocer este tipo de instrumentos

¿Qué cosas NO IMPLICAN los Smart Contracts?

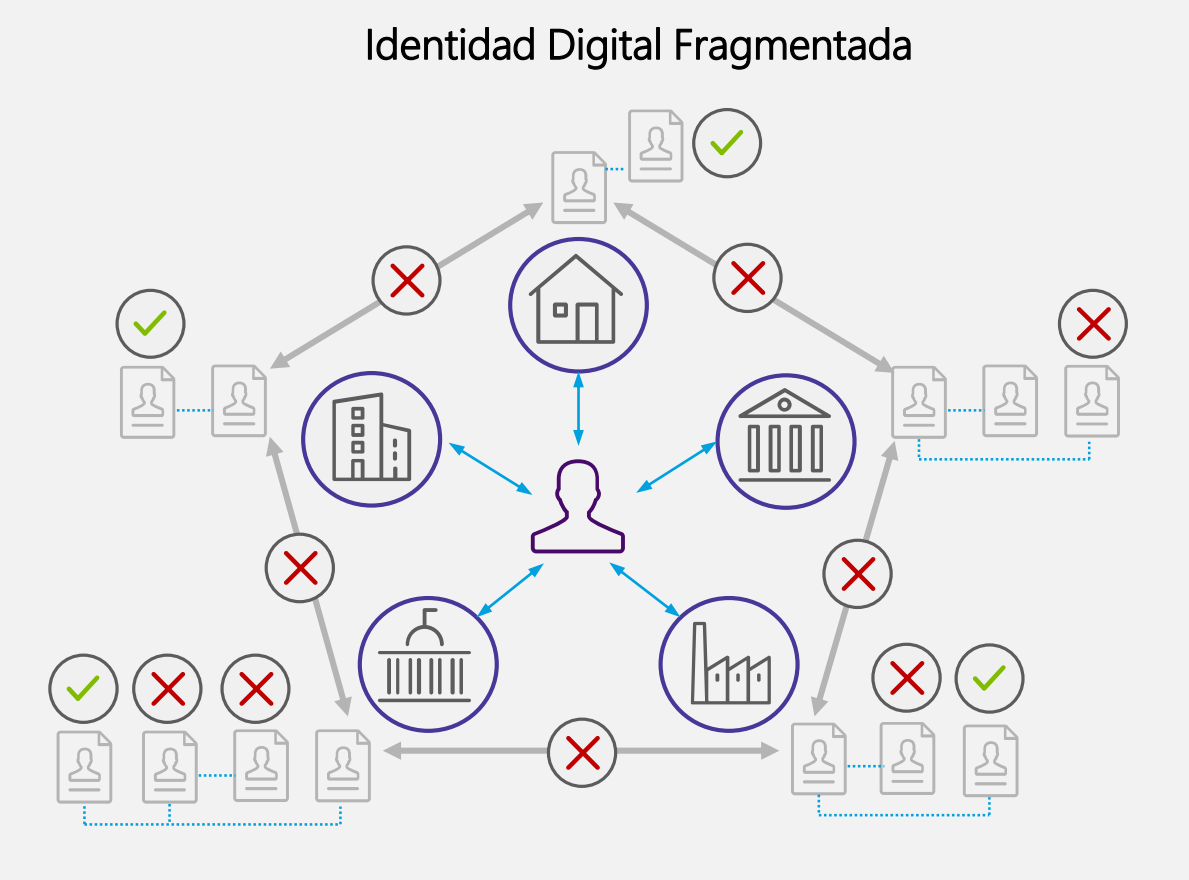
- No es el fin de la profesión legal! La codificación de los contratos y resolución de diferencias contractuales seguirán siendo importantes
- La automatización no puede ser total, el riesgo de efectos no deseados del código debe balancearse con puntos de intervención humana. El incidente de la DAO en Junio del 2016 en Ethereum puso en riesgo $50 millones, debido a un smart contract mal codificado y tuvo que resolverse mediante un *hard-fork*

KPMG

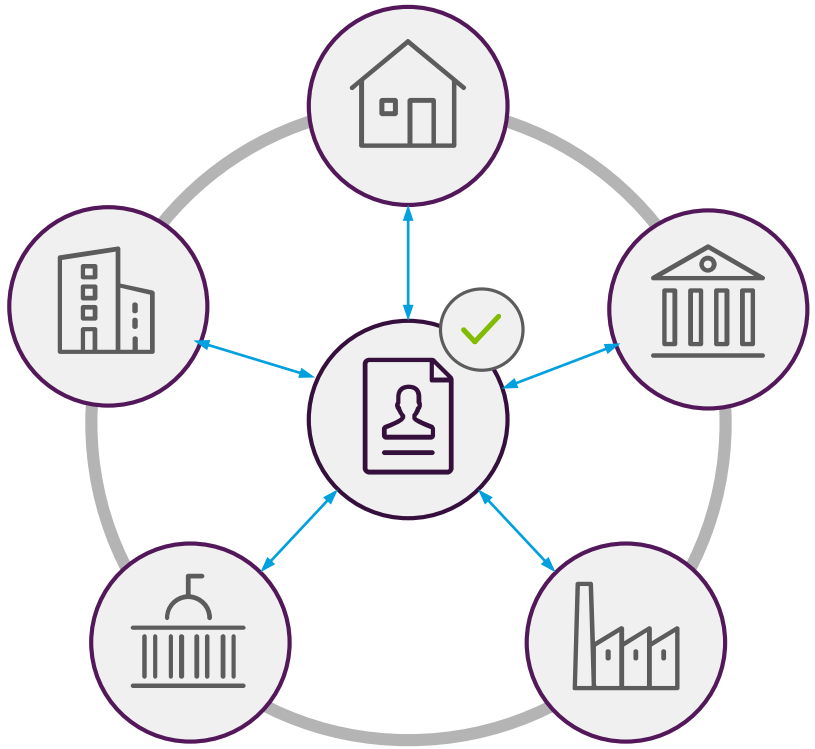
Caso de Estudio: Manejo de Identidad Digital

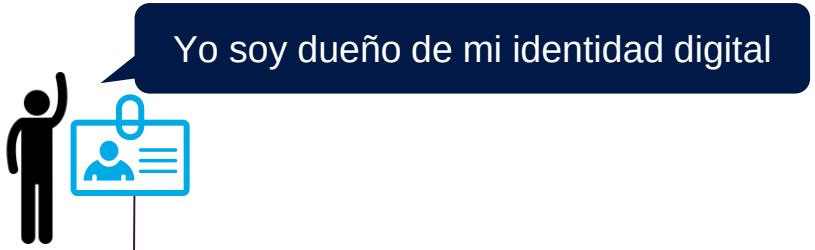
Problemática Actual en el Manejo de la Identidad

- Hoy en día los registros de identidad de los clientes existen en todas las organizaciones con las que los clientes tienen una relación
- Hay poca integración y los registros se des-actualizan constantemente
- Esta duplicidad de datos nos lleva a duplicidad de procesos como por ejemplo los de “conozca a su cliente”



Estructura de la Identidad Digital Soberana (Self-Sovereing Digital Identity)





Atributos*

*La información privada o sensible se guarda fuera del blockchain, pero la verificación instantánea se habilita a travez del blockchain

Atestados / Credenciales

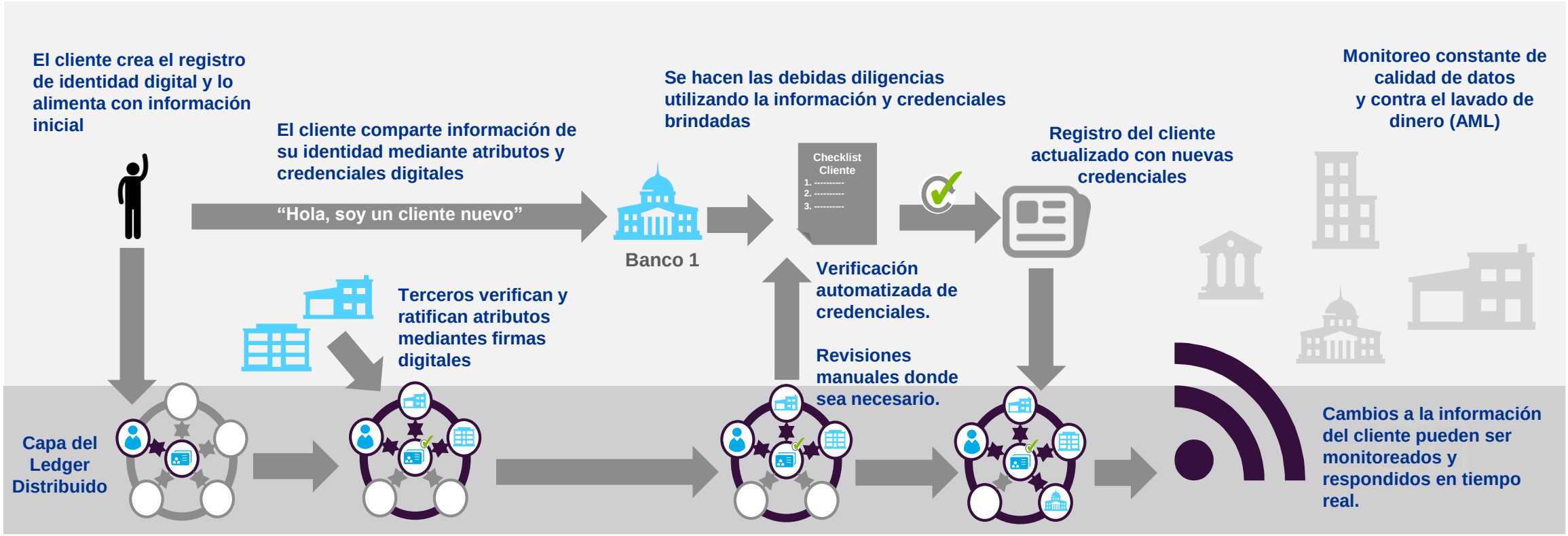
Los atestados validan los atributos de la persona y son firmados digitalmente por autoridades o terceros que pueden ratificar la validez del atributo

Activos / Propiedades

Apps

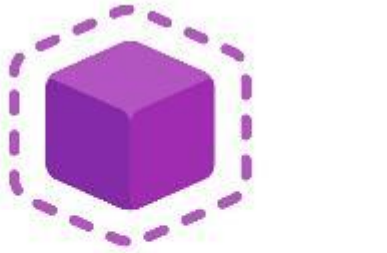
Actualización Distribuida de Datos de Clientes

¿Como puede un Ledger Distribuido reducir la fricción y costos de los procesos KYC en la industria de servicios financieros?

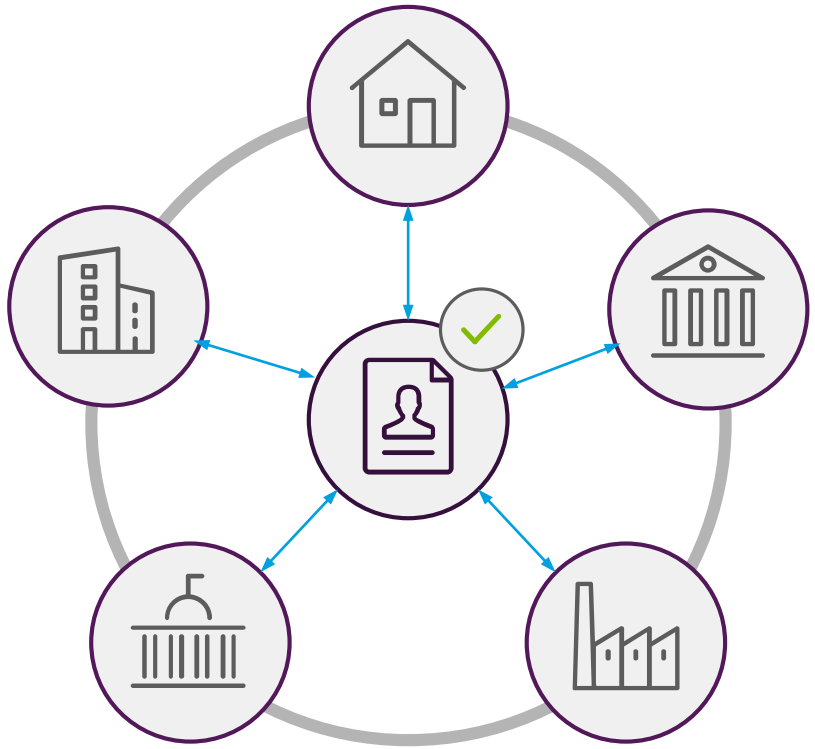


Startups de Blockchain Enfocados en Identidad Digital

Muestra representativa de algunos startups enfocados en este caso de uso:



Oportunidades en Costa Rica para el Identity Management



Firma Digital (Bloque Fundacional)

La infraestructura de llaves públicas (PKI) y firma digital ya es reconocida por la legislación costarricense

Utilización de SIM Cards de las Operadoras

En vez de tradicionales tarjetas de firma digital. Las llaves privadas pueden ser grabadas en la memoria de los SIM cards y pagar una taza de uso por transacción a las operadoras

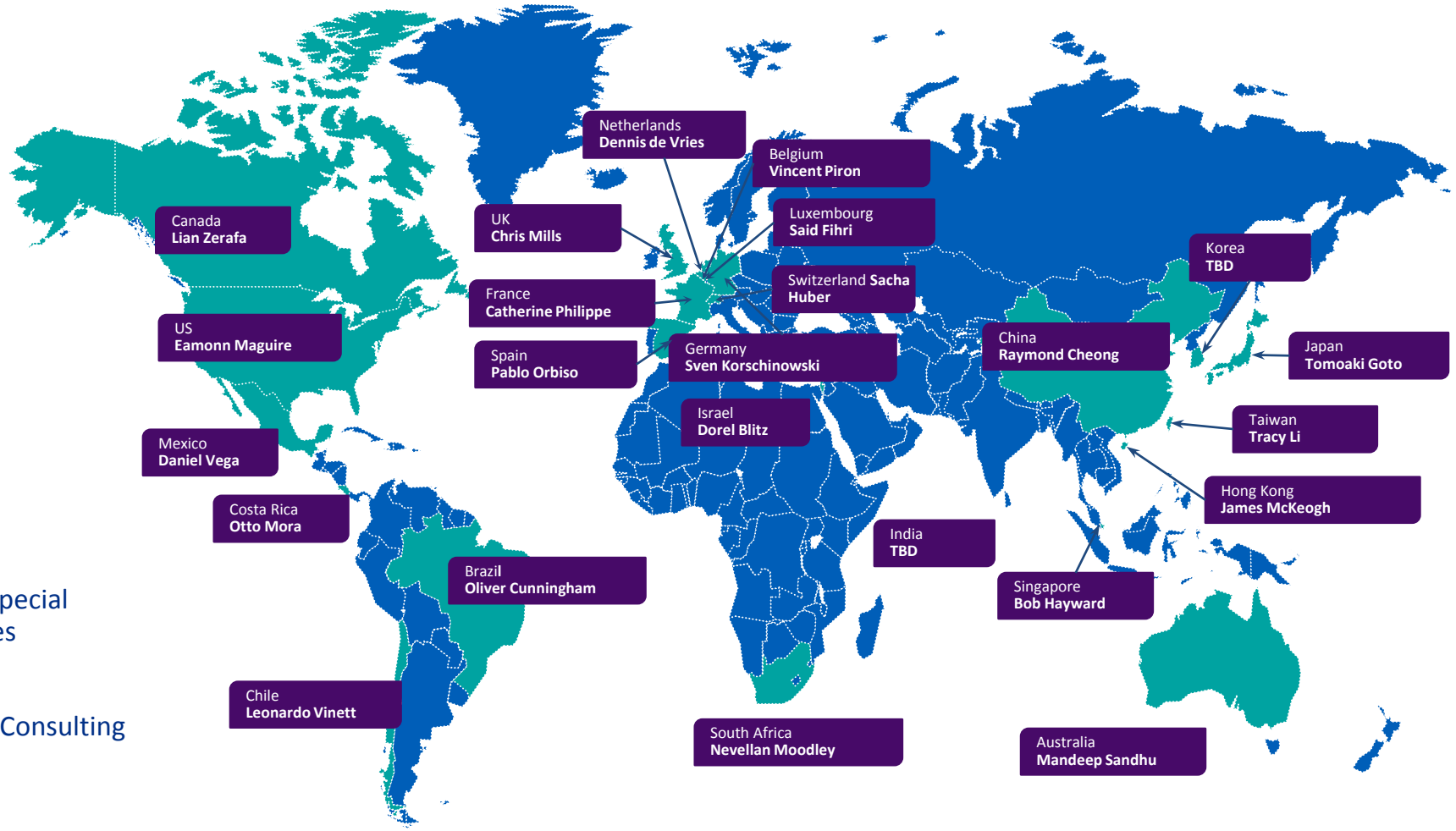
Plataforma Blockchain Distribuida

Un consorcio de Bancos y empresas interesadas en el uso de la identidad digital con los clientes hostean la infraestructura

Manejo de la Identidad Digital

KPMG Global DLS Response Team

Con presencia en 24 países participando en el desarrollo y comercialización de tecnologías Blockchain.



Global DLS development:
Eamonn Maguire – FS DLS Lead
Wei Ng – Growth & Innovation Special Projects, Global Financial Services

Costa Rica:
Otto Mora, KPMG Management Consulting

Para mas información

Otto Mora
Supervisor
Management Consulting
KPMG
ottomora@kpmg.com

Luis Rivera
Director
Management Consulting
KPMG
lgrivera@kpmg.com