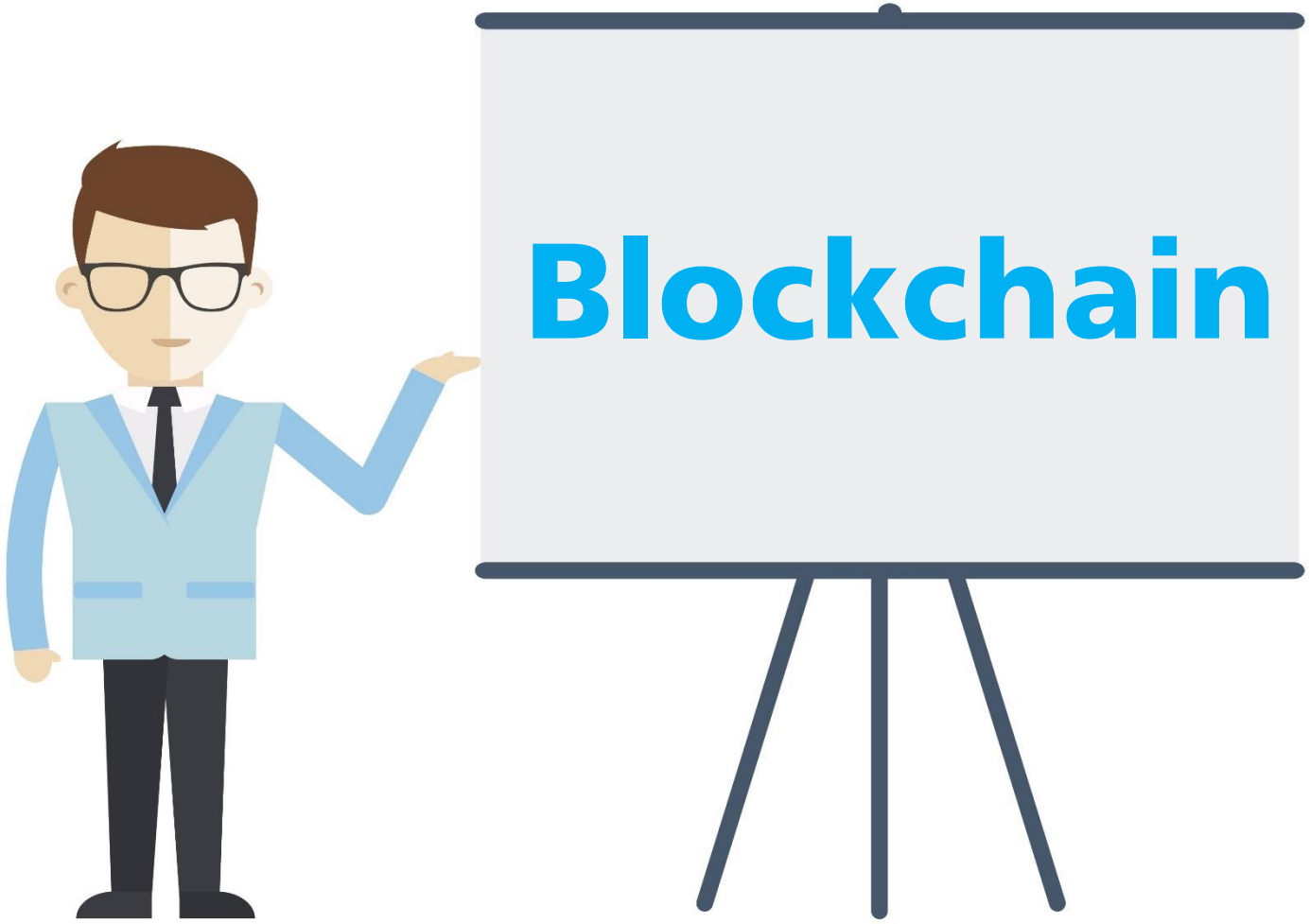


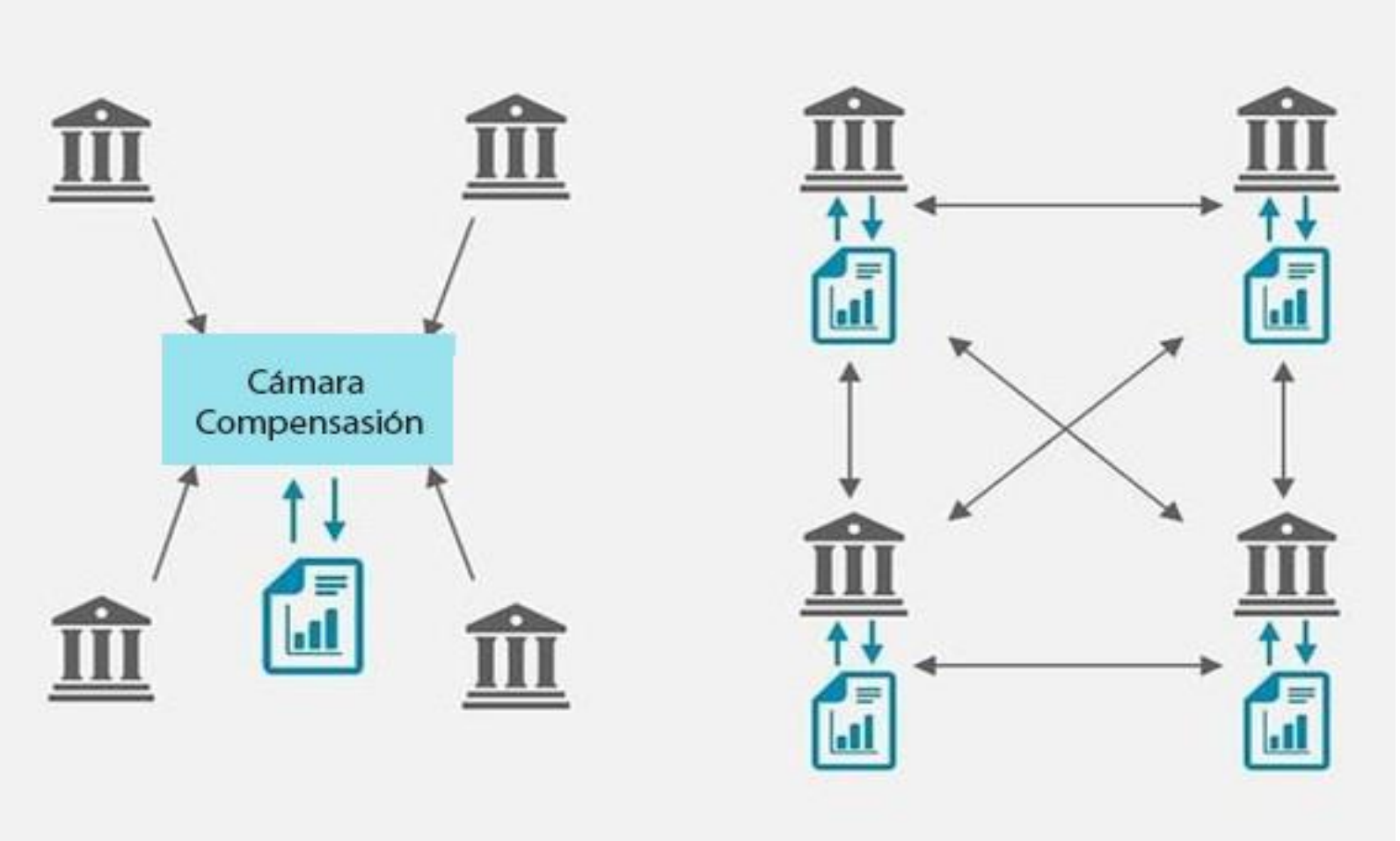
Motivación

En el mundo digital de hoy una información es tramitada de uno a uno o de muchos a muchos, de manera altamente distribuida (no centralizada). Sin embargo, DEPENDEMOS – e en muchísimos casos - de una autoridad central para verificar / validar un acuerdo, consumar una comunicación o si un movimiento es llevado a cabo.

Ejemplos son: un contracto, el estado de nuestra cuenta bancaria o si un mensaje de correo electrónico fue enviado. Entre otros tantos.

La figura de una autoridad central genera una “asimetría permanente” en las relaciones entre los pares de una red. Una propuesta de ruptura de este *statu quo* es la adopción de un **consenso distribuido**, que crea e mantiene un **verdadero registro** de eventos ocurridos en el pasado y que son constantemente producidos en el presente.

Blockchain - **Motivación**



Blockchain

Un **Blockchain** es una base de datos distribuida entre varias partes de una red e que utiliza criptografía para su validación y cuyo código fuente es abierto. Así como un "libro de contabilidad" comienza vacío y cuando alguien hace una entrada con éxito en su estructura el cambio se sincroniza con la copia de cualquier otra parte de la red que, por eso, se mantiene actualizada.

Una actualización puede ser hecha solamente por un mecanismo llamado de **consenso** por parte de la mayoría de los participantes en el sistema (50% +1). Una vez que un block es añadido el mismo no puede ser borrado.

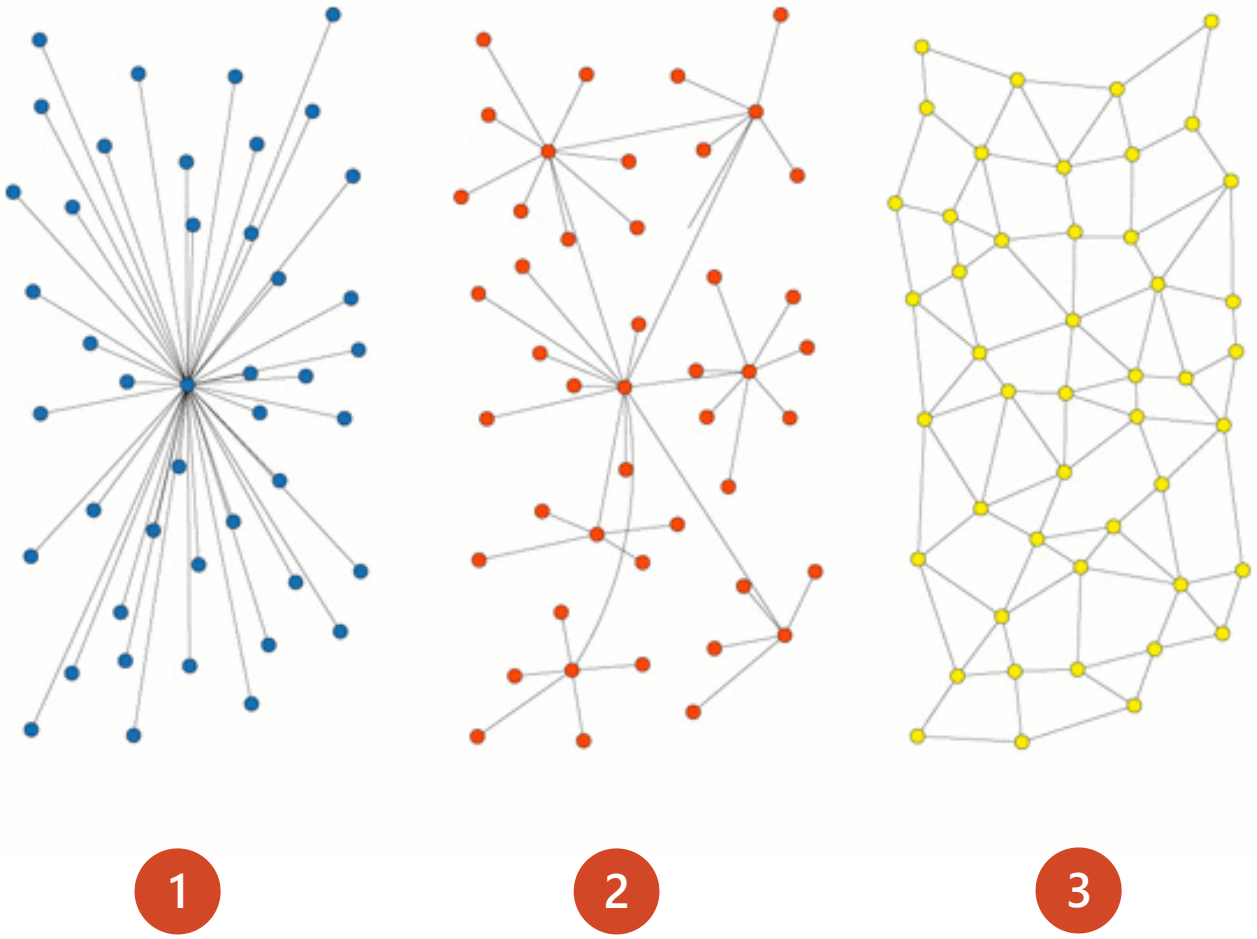
Cada *nodo* de la red es un diferente *nodo* de computación geográficamente y computacionalmente aislados unos de otros. La falsificación o modificación de datos en esa cadena de bloques es extremadamente difícil (si no imposible), ya que requeriría que cualquier intento actúe en más de la mitad de los participantes, aceptando así el cambio.

Blockchain - **Motivación**

1. Centralizada
2. Descentralizada
3. **Distribuída**

Cualquier receptor final puede ser a la vez emisor.

De la misma forma que todos los receptores pueden escoger cual es la fuente (emisor) que más le conviene



Blockchain – **Base de Datos Descentralizada y Abierta**

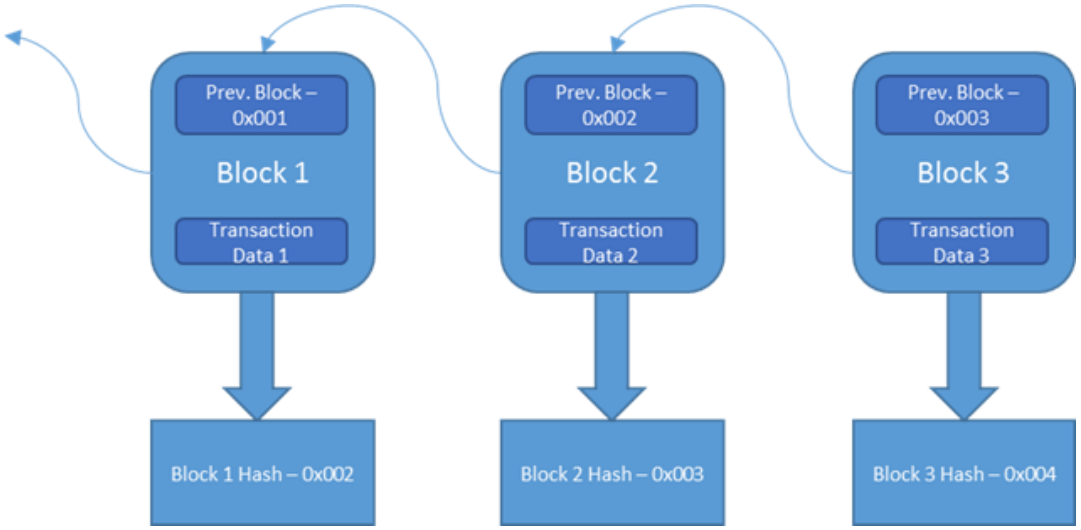
La arquitectura utilizada elimina al intermediario por completo y permite que los *nodos* pares posan llegar a un consenso.

Blockchain es un almacén de datos con las siguientes características:

- Contiene historial completo de transacciones.
- Repetidos a lo largo número de sistemas en una red punto a punto.
- Utiliza la criptografía para probar la identidad y la autenticidad.
- Puede ser escrito por todos los participantes.
- Puede ser leído por todos los participantes.
- Muy difícil de cambiar los registros históricos lo cual implica fácil de detectar cuando alguien trata/intenta de hacerlo.

Blockchain – Detalles

El **Blockchain** se compone de bloques individuales. Cada bloque contiene: El encabezado del bloque. La cabecera contiene metadatos sobre el bloque, la referencia al bloque anterior, hash de los datos contenidos en el bloque.



Cada bloque en el blockchain está identificada mediante una huella digital o almohadilla (generada utilizando SHA256 algoritmo criptográfico).

Blockchain – Función *Hash*

A las funciones **hash (**también llamadas de funciones picadillo) es una función computable mediante un algoritmo:

H: U → M

x → h(x)

que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M.

Ejemplo -> http://www.miraclesalad.com/webtools/md5.php

Blockchain Detalles 1

La referencia a bloque anterior - una huella dactilar o hash del bloque anterior.

Encadenamiento criptográfico hace que la manipulación sea muy difícil si no imposible. Cuando alguien trata de manipular un solo mensaje, toda la cadena de hash tiene que ser calculado a partir del punto en que se realizó el cambio. Esto mecanismo de igual a igual y el hash hace que sea prohibitivo manipular el contenido **Blockchain**, siendo este **inmutable**.

Es importante tener en cuenta que el campo hash del bloque anterior está dentro de la cabecera del bloque y por lo tanto afecta el hash del bloque actual. La identidad de bloque niño cambia cuando cambia su bloque padre. Así que cuando se cambian los datos del bloque padre, su hash ha cambiado y por lo que el campo anterior bloque de hash de bloques del niño tiene que ser modificado. Esto se traduce en un efecto cascada y lo que una vez muchos se van creando bloques, sería muy difícil y requiere gran potencia de cálculo para realizar cualquier cambio en los datos.

Blockchain Detalles 2

En la sección anterior vimos la parte interna del **Blockchain** y cómo se mantiene su integridad mediante huellas digitales criptográficas.

Una vez que un cambio se ha hecho necesita ser comunicado a otros *nodos* de la red. **Blockchain** es una red peer-to-peer, donde cada par es independiente y tiene todos los datos y las actualizaciones están compartida alrededor.

Hay un desafío de resolución de conflictos en la red peer-to-peer, cuando más de un cliente actualiza la cadena. Uno enfoque adoptado es el de victorias más larga cadena. A modo de ejemplo dicen que hay dos *nodos* que quieran adjuntar un nuevo bloque a la cadena. Digamos que el nuevo bloque es E . En esta situación hay dos cadenas de bloques:

Blockchain Detalles 3

bloque de la cadena 1 ==> "A" -> "B" -> "C" -> "D" -> "E1“

bloque de la cadena 2 ==> "A" -> "B" -> "C" -> "D" -> "E2"

Dado que dos *nodos* están tratando de añadir un nuevo bloque a la misma **Blockchain** hay un conflicto. El conflicto se resuelve en función de donde se une el bloque "F". Si el bloque "F" está unido al bloque de cadena 1, entonces sería la cadena más larga. Así que dependiendo de donde el bloque "F" está unido que gana la cadena de bloques ya que sería la cadena más larga.

Este enfoque de las victorias más larga cadena tiene su inconveniente ya que alguien con una gran potencia de cálculo puede crear el caos empujando a aquellos con menor potencia de cálculo.

Blockchain Consenso

Las entradas en el libro mayor (libro de contabilidad) se sincronizan con todos los libros en la red. **Consenso** asegura que estos libros de contabilidad compartidos son copias exactas, y reduce el riesgo de transacciones fraudulentas desde la manipulación tendría que ocurrir en muchos lugares al mismo tiempo exacto.

- Todas las partes están de acuerdo con la transacción y validarla a través de la red de pares.
- Las reglas también se pueden establecer para validar las transacciones.
- Esta confianza y la participación sin esperanzas hace posible el compromiso a un bajo costo.

Blockchain Contratos Inteligentes

Un contrato inteligente puede incluir un activo digital que es algo que tiene un propietario y se puede convertir en valor.

los activos digitales pueden ser tangibles o intangibles. Un contrato inteligente también puede incluir una representación digital de un conjunto de reglas de negocio:

- Está incrustado en el **Blockchain**
- Se ejecuta en una transacción
- Verificable, firmado y codificado en un lenguaje de programación

Por ejemplo, define las condiciones en que se produce la transferencia de renta o derecho a una propiedad.

Blockchain Tipos

Hay dos conjuntos de **Blockchain** dependiendo del acceso disponible. Son pública vs privada blockchain.

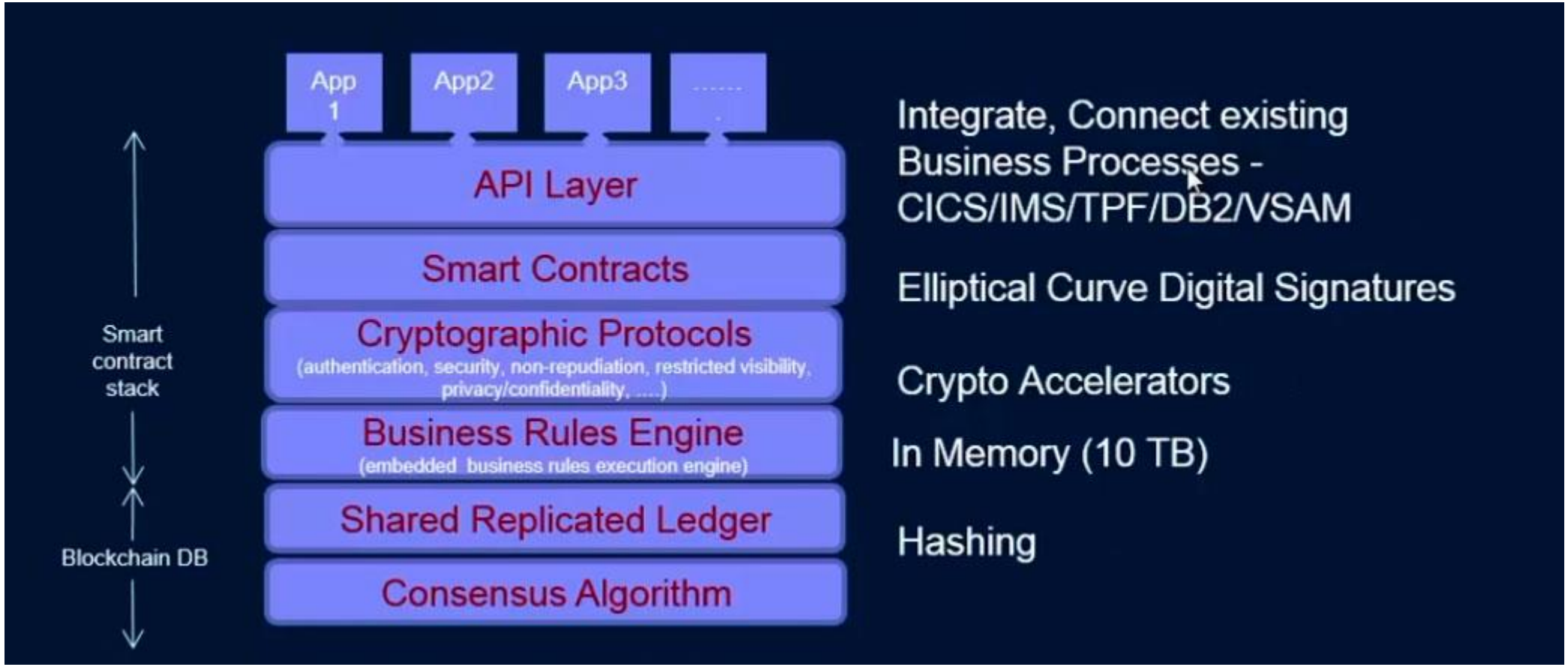
A Pública

B Privada

El tipo Público cualquiera puede escribir en el libro mayor / Diario pecado sin necesidad de aprobación. Pero then Lo Que Se Necesita ALGÚN mecanismo m para el Manejo de discrepancias en ausencia de autoridad f centro y también el mecanismo m de defensa contra los Usuarios / atacantes maliciosos.

El Privado donde los participantes se encuentran dentro de una organización o grupo de empresas.

Blockchain Apps/Estructura



Blockchain Analogía

En diciembre de 1974, Vint Cerf y Robert Kahn presentaran Internet TCP (*Protocolo de Control de Transmisión*) / IP (*Protocolo de Internet*)

Sin embargo, las tecnologías de base se han mantenido sin cambios. La dirección IP todavía actúa como una dirección única que permite a cualquier dispositivo con acceso a Internet para identificarse en internet, mientras que las garantías de tecnología TCP entrega de los paquetes de datos mediante la división en segmentos, lo que se conoce como la conmutación de paquetes

Aprovechando este modo de funcionamiento, Tim Berners - Lee creó el Protocolo de transferencia de hipertexto o HTTP.

La comprensión del **Blockchain**

Hoy en día, el protocolo **Blockchain** está siguiendo un camino similar de evolución con una diferencia importante. Tal como TCP / IP y HTTP son protocolos de comunicación, el **Blockchain** es un protocolo de intercambio de valor.

- Comunicaciones Inmediatas: INTERNET
- Transacciones Inmediatas: **BLOCKCHAIN**

Miguel Russo
Teléfono Móvil: +34 691 261 853
Correo electrónico: europeus.russo@gmail.com
LinkedIn: https://es.linkedin.com/in/miguelrusso/es
Portafolio: http://www.fermo.com.br/blockchain

miguelrusso