Blockchain y Criptomonedas

Un camino hacia la adopción de las criptomonedas.

INDICE

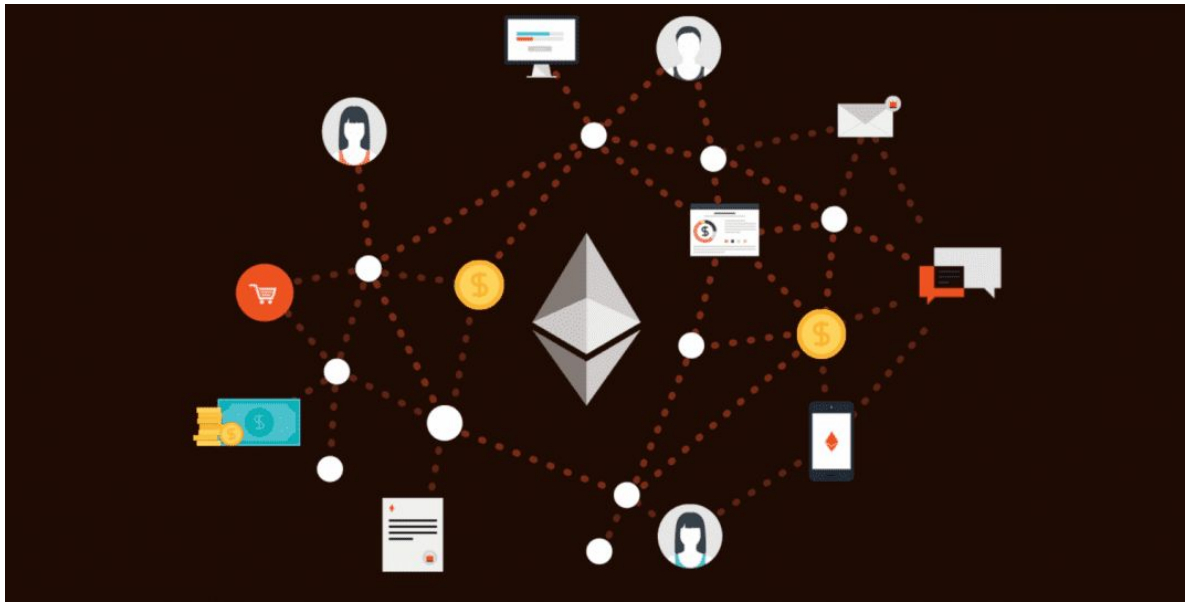
DAPPS

El futuro de las aplicaciones.

DAPPS

¿QUÉ ES UNA DAPPS?

Son aplicaciones descentralizadas que utilizan 'BlockChain' para que los usuarios se relacionen directamente entre ellos y cierren acuerdos sin que exista una entidad central que gestione el servicio.

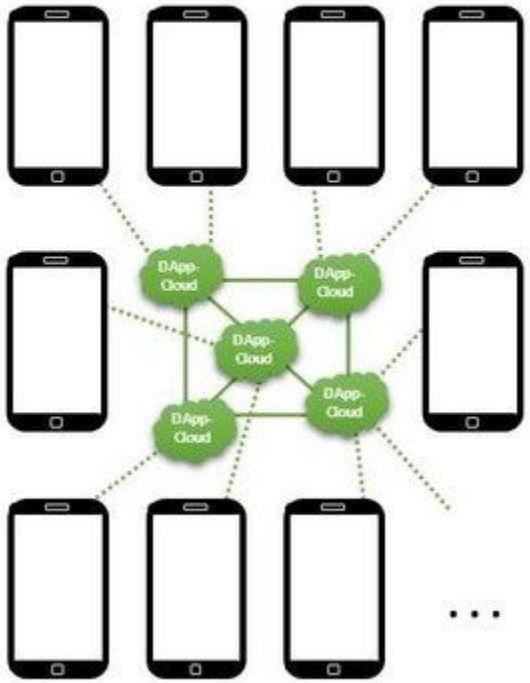


Apps

(classically centralized)

DApps

(decentralized)

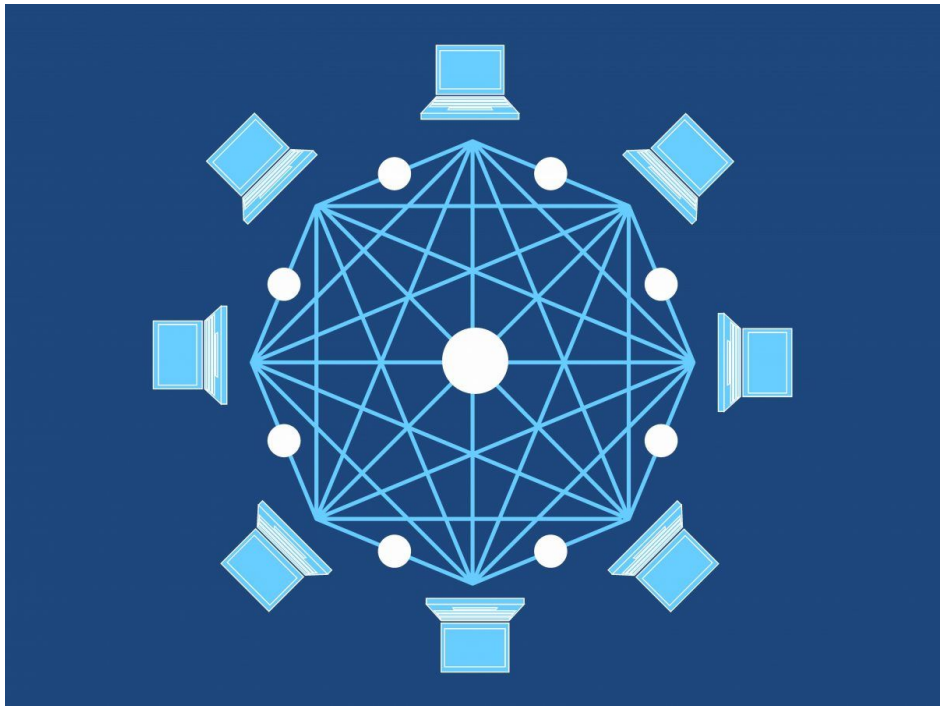


DAPPS

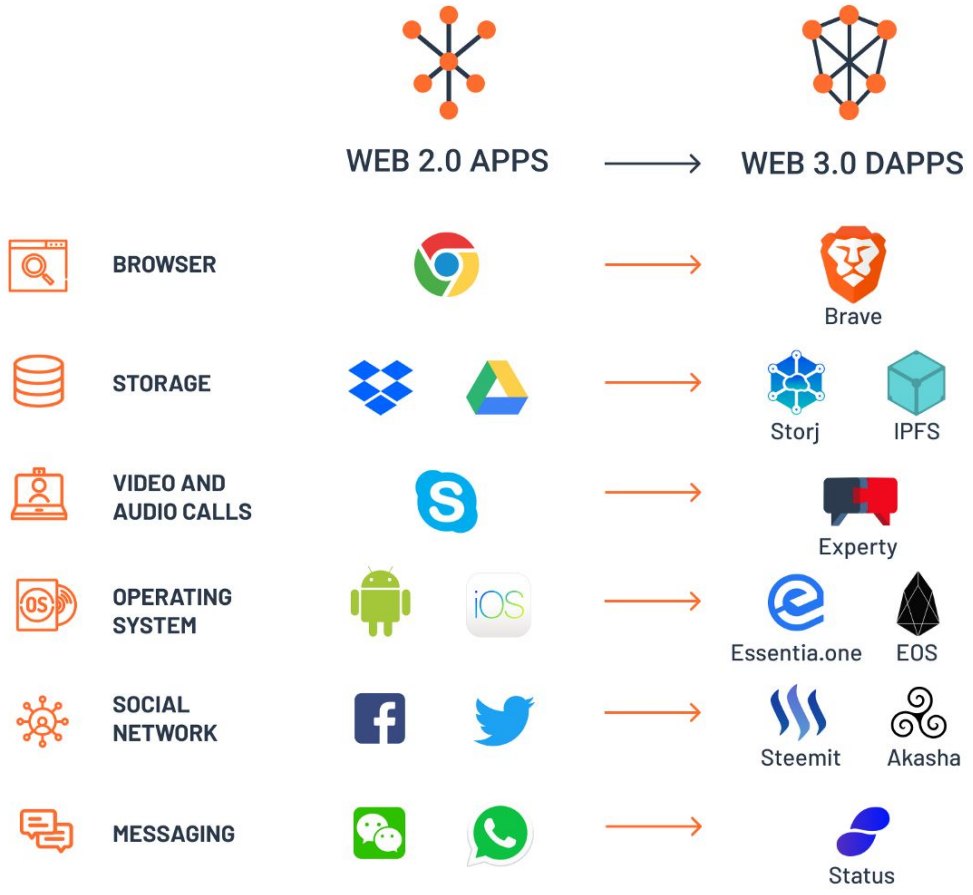
Las primeras DApps conocidas se vieron en los protocolos de compartición de archivos como BitTorrent o DC++.

Ambas aplicaciones, son sistemas peer-to-peer de comparación de archivos con alta resistencia a la censura.

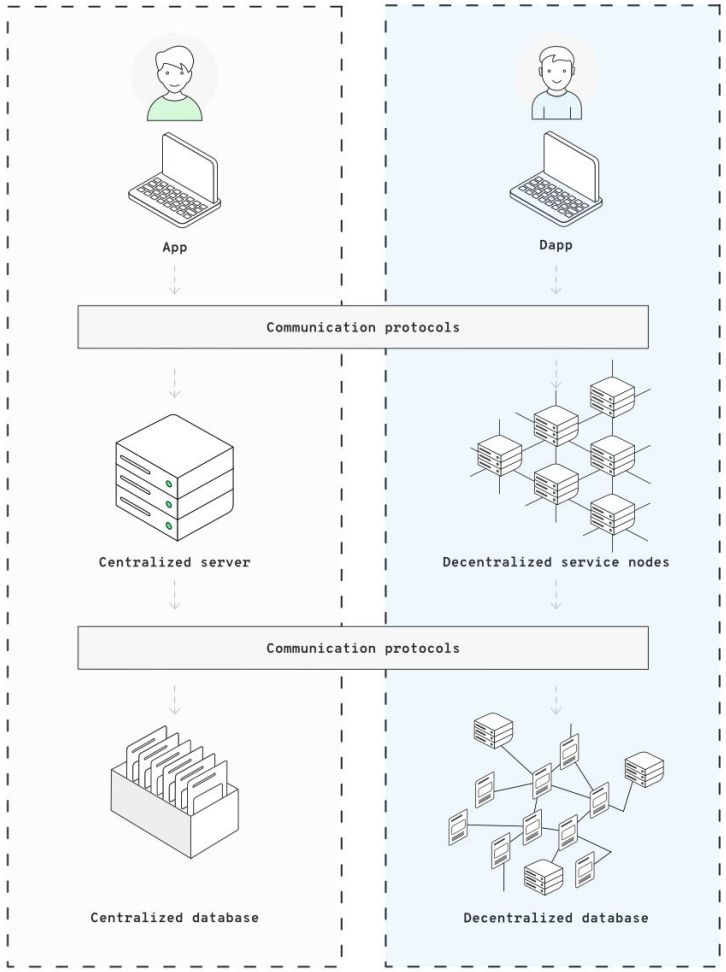
Sin embargo, la primera DApp usando BlockChain fue, el mismísimo Bitcoin. Ya que su estructura y funcionamiento describe con éxito la primera DApp de la historia.



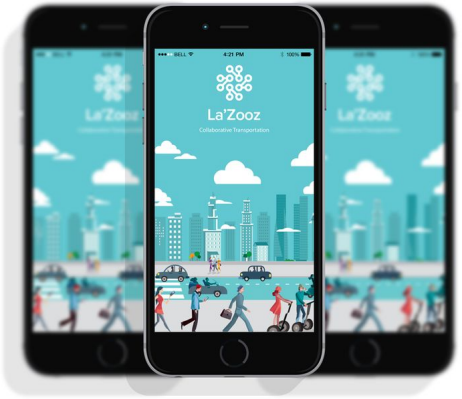
APPS vs DAPPS



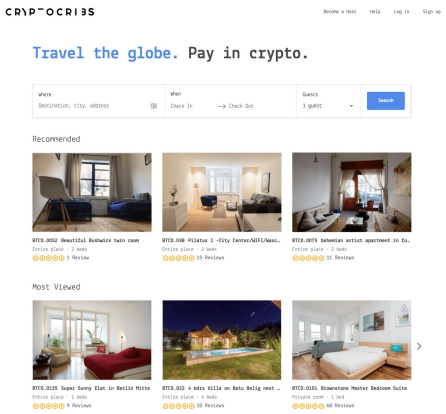
APPS vs DAPPS



DAPPS - APPS



UBER

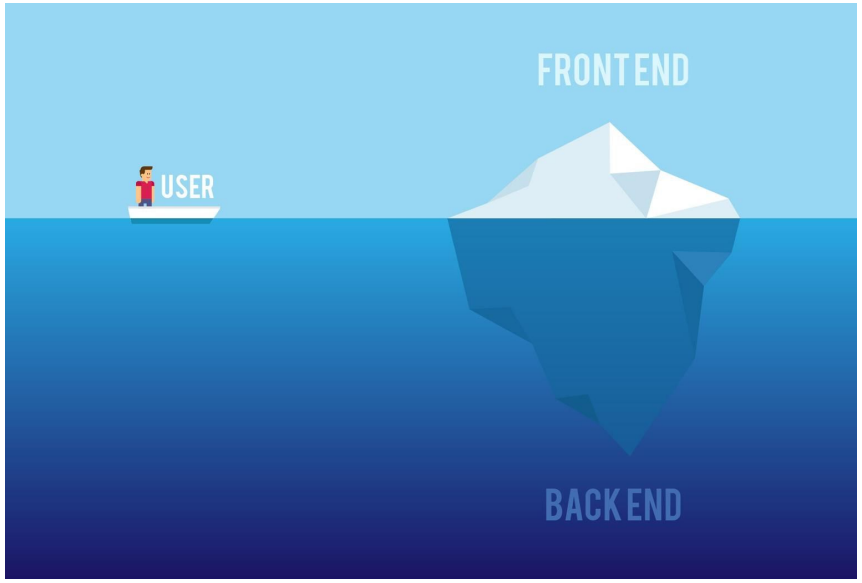


Diferencias entre una DApp y una App tradicional

Las DApps y las Apps tienen muchos elementos en común, sin embargo, su diferencia radica en cómo interactúan con dichos elementos.

Ambos tipos de aplicaciones tienen tres estructuras básicas que son:

1) El Frontend
2) El Backend
3) La capa de almacenamiento de datos.

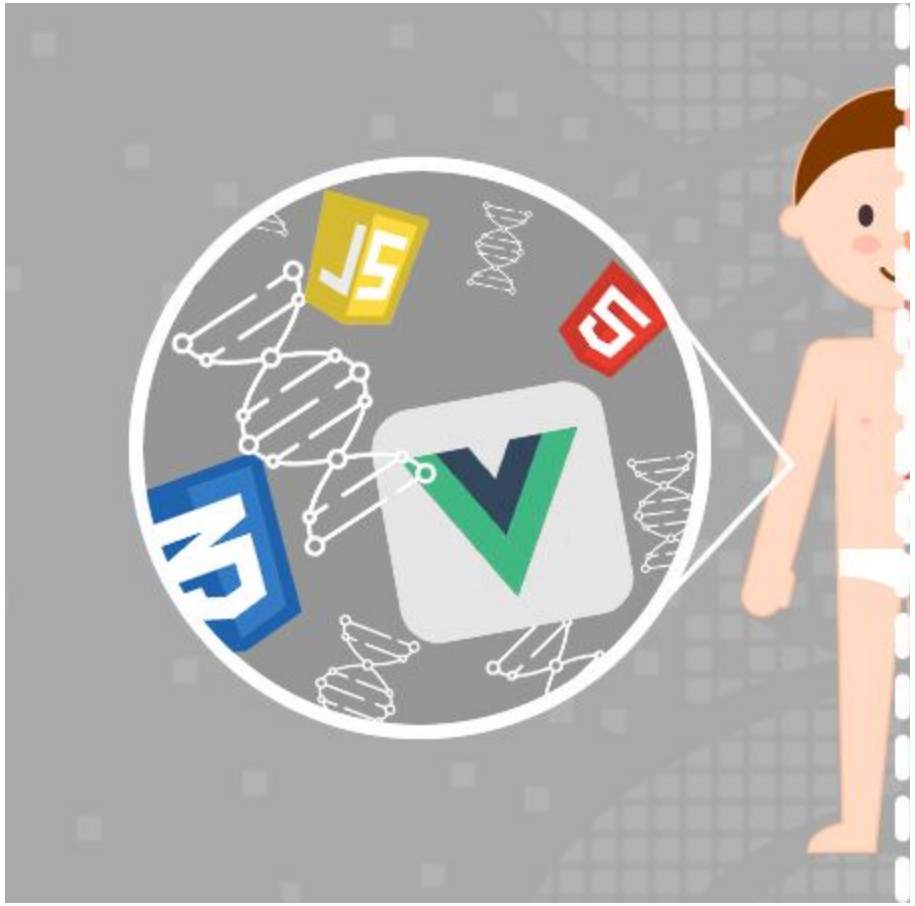


Frontend

La primera capa, el Frontend, viene a ser la interfaz que los usuarios utilizan para interactuar con la aplicación.

En este caso, tanto las DApp como las App tradicionales, pueden hacer uso de los inmensos recursos gráficos existentes para ello. Desde interfaces web escritas en HTML5 hasta las más elaboradas, tipo Framework .

La finalidad de esta capa es simplemente, dar al usuario la capacidad de interactuar, recibir y enviar información a la aplicación que esté usando.



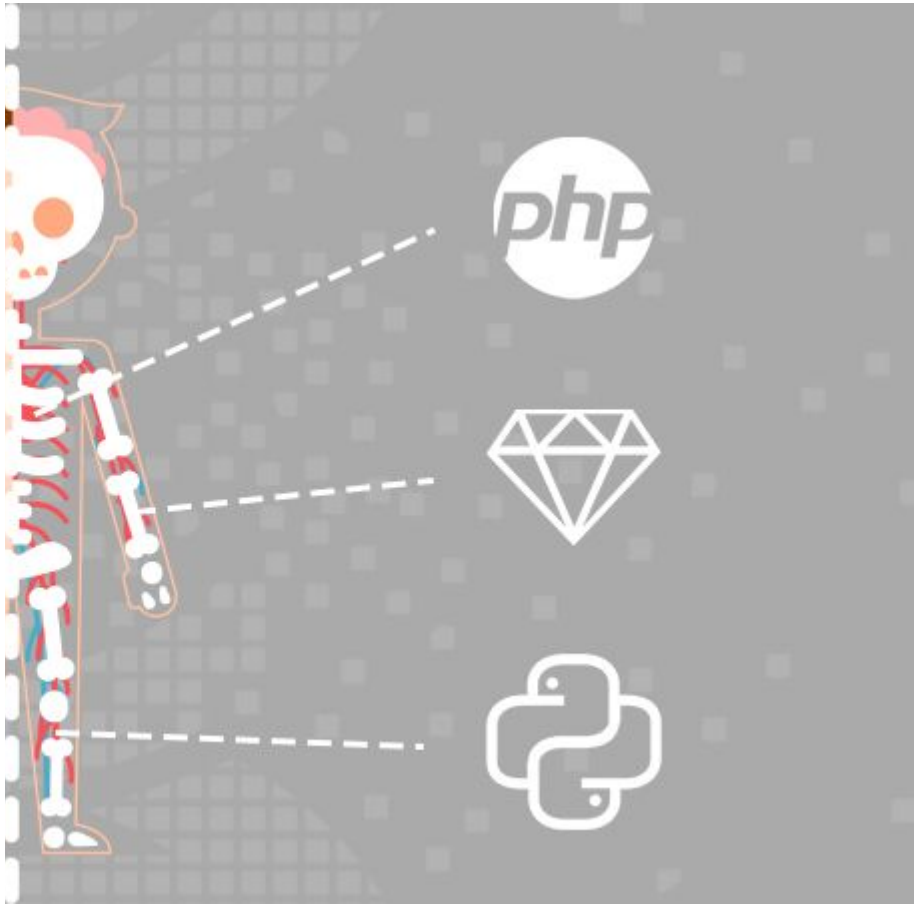
Backend

Esta segunda capa hace mención a la lógica principal de la aplicación. En una aplicación tradicional, esta lógica es centralizada, a diferencia de las DApps en la que está es descentralizada.

En las DApps, el Backend está relacionado a un smart contract que se ejecuta sobre una BlockChain, por ejemplo Ethereum. De esta forma, un smart contract tiene una programación que garantiza el funcionamiento de la DApp.

Al ser los smart contract visibles y públicos, esto garantiza un alto nivel de transparencia y seguridad. Los usuarios pueden estar seguros que la DApp no hará nada distinto a lo que especifica el smart contract.

Adicional a esto, el Backend es soportado por las API (Interfaz de Programación de Aplicaciones) y capacidades de la BlockChain.



Almacenamiento de Datos

Por último, la capa de almacenamiento. En una APPS, está capa también es centralizada. Normalmente los datos son almacenados en el computador del usuario o en servidores controlados por terceros. Esta forma de trabajo, tiene muchos puntos negativos. Un usuario por ejemplo, puede perder la información de la aplicación si su computador se daña. También puede suceder que los servidores queden fuera de servicio o sean bloqueados. Lo que nos impediría usar la aplicación de forma correcta o incluso perder información.

Pero en las DApp, el almacenamiento de datos es completamente descentralizado también. Cada usuario de la DApp almacena un historial completo de las acciones que se realizan en la red DApp. Adicional a esto, las interacciones son almacenadas en la BlockChain dentro de los bloques de la misma. Todo ello de forma criptográficamente segura, impidiendo acceso no autorizados por terceras personas.

¿Como funciona una DAPPS?

Una DApp funciona de forma parecida a una red BlockChain. En este caso, cada usuario de la DApp es un nodo dentro de la red. Cada usuario, vela por el correcto funcionamiento y las operaciones que se realizan en dicha red.

El canal de comunicaciones que usa la DApp es la BlockChain. En ella, se deja registro de cada operación que pasa por el SC que controla la DApp.

¿Como funciona una DAPPS?

El SC en este caso, es un punto intermedio que se encarga de corroborar la validez de cada interacción. Cada vez que hay una nueva operación en la DApp, la información de la plataforma se actualiza en cada nodo. Con ello se garantiza que la información quede almacenada en cada uno de ellos. De esa manera, cada usuario contribuye a mantener en pie la aplicación con los recursos de su ordenador.

Esta estructura también garantiza que la plataforma siempre estará en servicio. Esto debido a la imposibilidad de dar de baja a todos los nodos de la red al mismo tiempo. Una situación que puede darse por un ataque informático u otras razones como la censura.

Características de las DApps

Seguridad

Esta es una de las principales características de las DApps. Esto es gracias a que, la misma funciona sobre una BlockChain que usa criptografía fuerte para asegurar los datos que maneja.

Este primer punto, asegura que la información solo puede ser vista por quien la origina y el resto solo puede verificar su validez o no. En ningún momento, la información originada por un usuario es visible para otros.

Características de las DApps

Código abierto

(Open Source)

Una DApp tiene que ser 100% de código abierto. Esto significa que el código fuente bajo el que está programada la DApp está abierto a posibles modificaciones y mejoras por parte de sus usuarios.

Características de las DApps

Descentralización

Otra de las principales características de la DApps es su descentralización. O lo que es lo mismo, la capacidad de funcionar sin servidores centrales.

Cada usuario de la DApp tiene un historial completo de las acciones llevadas en la DApp. Algo así como una copia global de todo lo que ha pasado.

Características de las DApps

Protocolo

Si la DApp está basada en BlockChain, eso significa que la información de las operaciones realizadas dentro de la aplicación tiene que ser almacenada en bloques y estos tienen que ser verificados.

Esto se da de acuerdo con un protocolo que actúe como prueba de que esas verificaciones son llevadas a cabo.

Este protocolo puede estar basado en el algoritmo Prueba de Trabajo ('Proof of Work', PoW) o de Prueba de Participación ('Proof of Stake', PoS).

Características de las DApps

BlockChain

Las DApp interactúan sobre la BlockChain en la que se ejecuta su smart contract. Esto significa, que cada interacción en la DApp genera una entrada de datos en la BlockChain.

Estos datos son almacenados de forma criptográfica para así añadir transparencia y seguridad. Todas estas acciones pueden ser revisadas públicamente en el explorador de bloques de la BlockChain.

Clasificación de las DApps

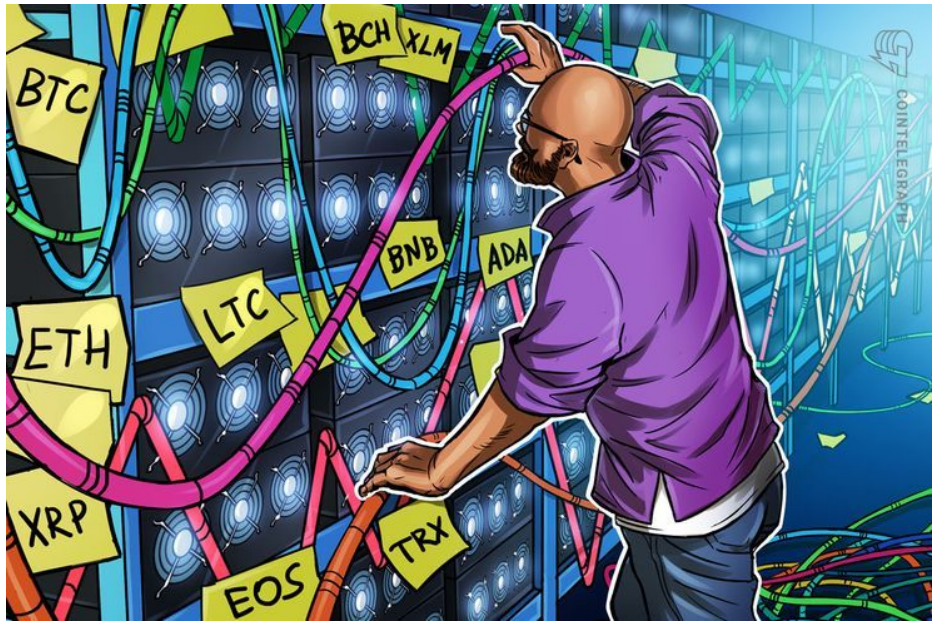
Esta clasificación de las aplicaciones descentralizadas se hace en base a si poseen su propia BlockChain o si estas utilizan la cadena de bloques de otra DApp.

Existen 3 clases diferentes.

Clasificación de las DApps

DAPPS Tipo 1

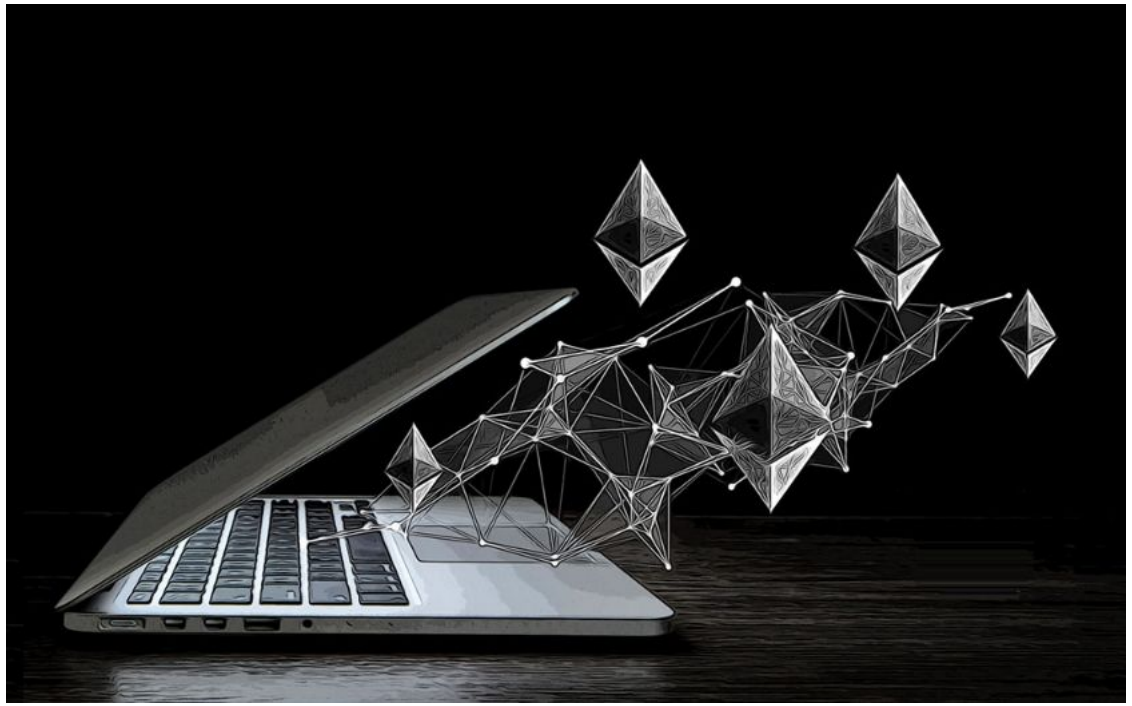
Estas son las que tendrían su propia cadena de bloques independiente.



Clasificación de las DApps

DAPPS Tipo 2

En esta clasificación nos encontramos aquellas DApps que dependen de una BlockChain y sus características para funcionar.

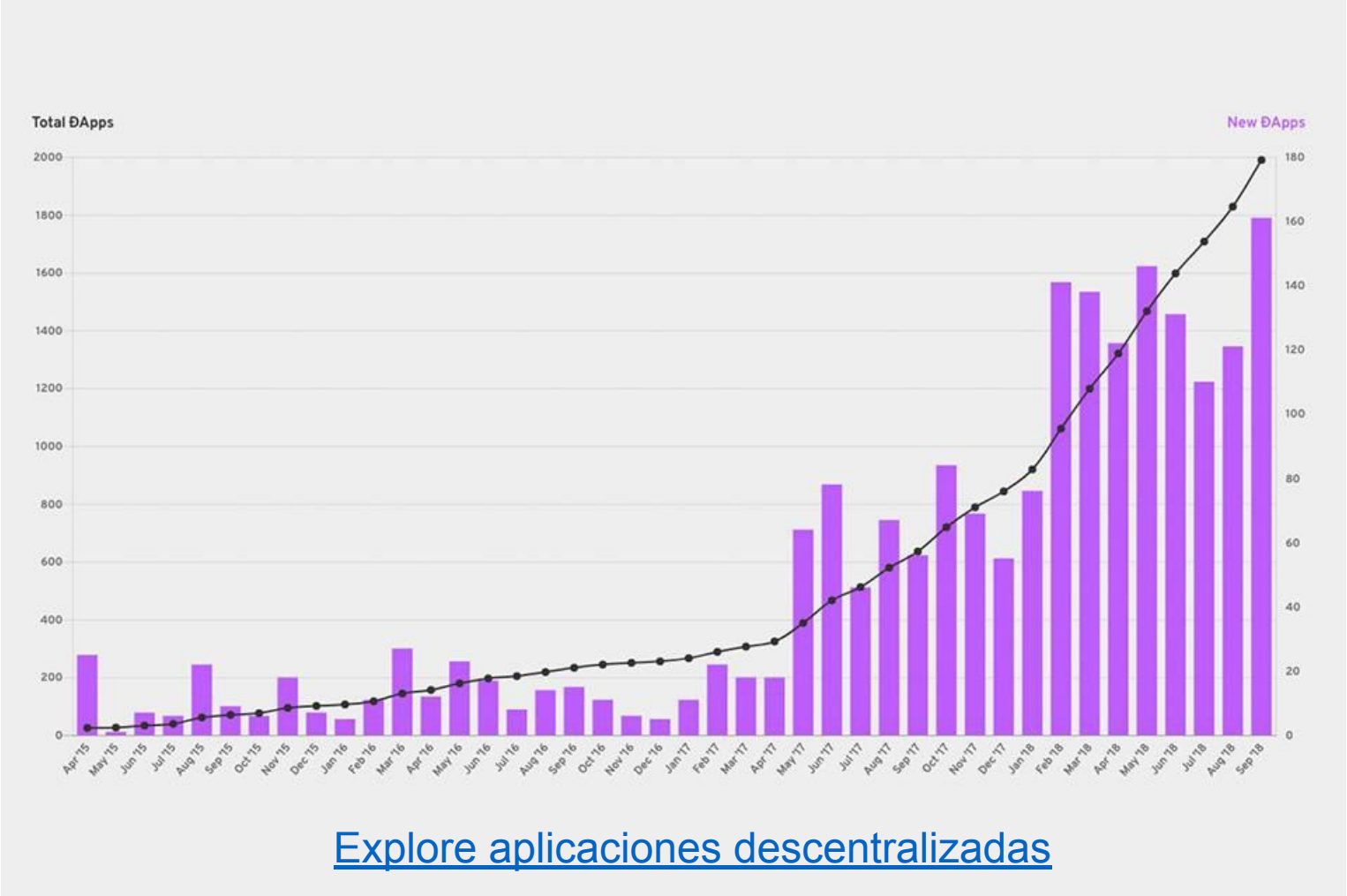


Clasificación de las DApps

DAPPS Tipo 3

Las DApps de este tipo, utilizan DApps de tipo 2 para su funcionamiento. Generalmente, los DApps tipo 3, usan los tokens de las DApps tipo 2, para realizar sus operaciones.

DAPPS



[Explore aplicaciones descentralizadas]

DAPPS

Metamask es una extensión para Chrome, Firefox y Brave que ofrece una cartera en Ethereum y sus redes de prueba y además en cada página inyecta la librería web3 permitiendo que cada aplicación DApp pueda integrar Metamask para que el usuario pueda usar la aplicación de una manera fácil e intuitiva.

Contratos Inteligentes

¿Contratos con capacidad de cumplirse de forma automática?

Contratos Inteligentes

Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas.

Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

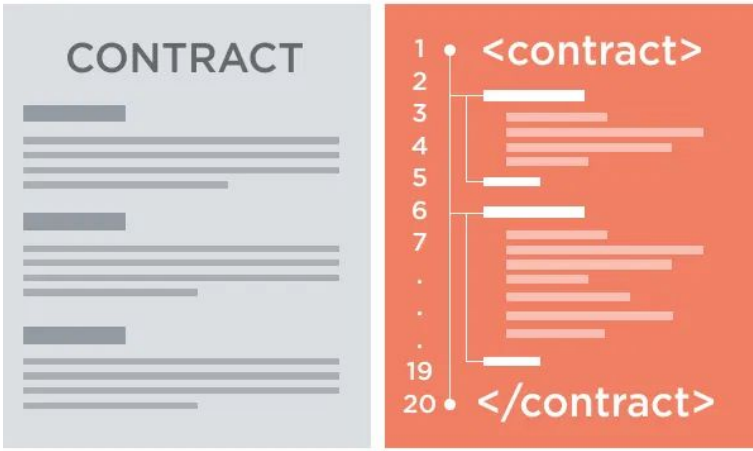
Son contratos que se ejecutan y se hacen cumplir a sí mismos de manera automática y autónoma.

Contratos tradicionales vs Contratos inteligentes

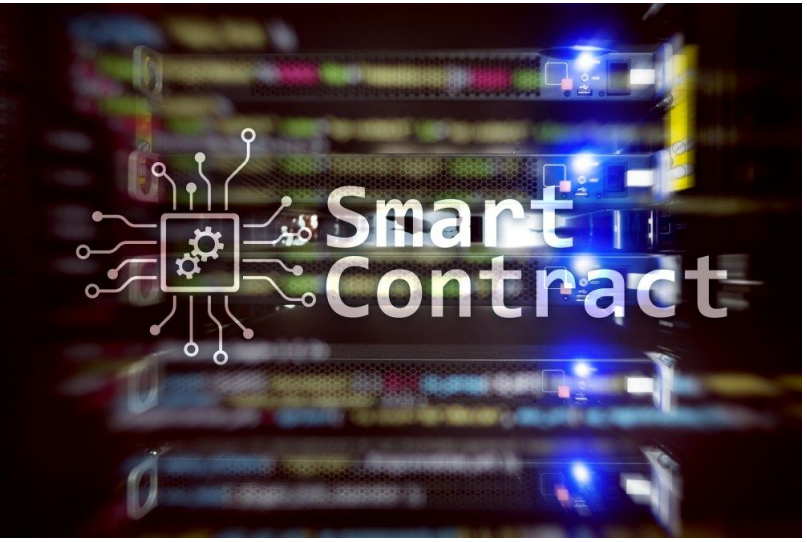
Cuando hablábamos de los contratos en papel, sabemos que éstos están escritos en un lenguaje natural: se puede escribir en cualquier idioma, pero en un lenguaje legal comprensible entre las dos personas que lo firman.

Una vez que se aceptan los términos y se firma, según las leyes aplicables, la responsabilidad legal de ambas partes tiene unos costes que usualmente provienen de un notario, dando validez a ese contrato.

También sabemos que su modo de cumplimiento depende del punto de vista de cada parte implicada: en un contrato, las cláusulas tienden a beneficiar a una de las partes por encima de la otra.



Contratos tradicionales vs Contratos inteligentes



El lenguaje no es natural, sino que es un lenguaje virtual, un lenguaje de programación informática. Al igual que cada programa de ordenador o cada aplicación móvil están programados para realizar una serie de tareas, los contratos inteligentes también realizan tareas bajo unas instrucciones introducidas previamente.

Esto hace que en el modo de cumplimiento no haya diferentes puntos de vista, sino una única lectura: Si se da la condición establecida, el contrato ejecuta automáticamente a consecuencia de dicha acción.

La responsabilidad legal del SC sigue en desarrollo. Lo que es indudable es que no requiere de un intermediario (como el notario) ya que el contrato en sí es el intermediario de confianza, reduciendo así los costes y el tiempo de las interacciones.

Contratos Inteligentes

Los contratos inteligentes llevan desarrollándose desde 1994, cuando el famoso criptógrafo **Nick Szabo** acuñó el término por primera vez.

Nick propuso este sistema de contratos por aquel entonces, sin embargo la infraestructura tecnológica del momento lo hacía inviable.

Era necesario un sistema de pagos que los pudiese llevar a la práctica y esa situación no apareció en escena hasta la creación del Bitcoin en el año 2009.

Contratos Inteligentes

Los SC buscan mejorar los contratos actuales siendo más seguros, más baratos, ahorrándonos tiempo.
Gracias a:

- Se programan las condiciones,
- Se firman por ambas partes implicadas
- Y se ‘coloca’ en una BlockChain para que no pueda modificarse.

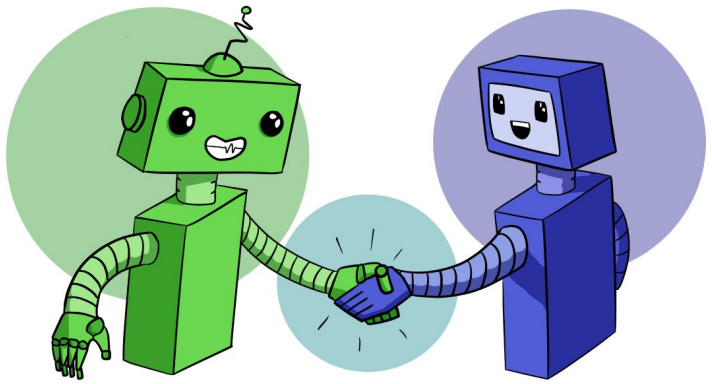
Su objetivo principal:

- Implementar una estado de seguridad mayor al del contrato tradicional.
- Reducir costes.
- Reducir el tiempo asociado a este tipo de interacciones.

Contratos Inteligentes
Doble Depósito

Esta es otra característica de los contratos inteligentes que hace que funcionen correctamente, eliminando al intermediario del proceso.

Permite a dos o más partes que no se conocen entre sí y que carecen de confianza el uno en el otro, realizar una transacción segura para ambos a través de un contrato inteligente.



Contratos Inteligentes Multifirma

La función multifirma en los SC es una función a través de la cual dos o más personas se deben de poner de acuerdo para hacer cumplir las condiciones de un contrato.

Contratos Inteligentes
Oráculos

Un oráculo es una plataforma externa a BlockChain que brinda información especial que utilizan los contratos inteligentes. Debido al amplio uso y aplicaciones que tienen los contratos inteligentes es que pueden existir infinidad de oráculos.

Contratos Inteligentes

Aplicación de la lógica empresarial con los *smart contracts*

1

- Las contrapartidas establecen las obligaciones y las instrucciones de liquidación
- Activos puestos bajo la custodia del contrato inteligente
- Condiciones de ejecución ("Si... entonces...")

2

- Un evento desencadena la ejecución del contrato
- El evento puede hacer referencia a:
  - –Una transacción iniciada
  - –Información recibida

3

- Condiciones de contrato (Business Logic) dictadas en función de las condiciones que se encuentran

4a

- Valor transferido al destinatario al que va dirigido tal como lo estipulan los términos del contrato
- En el caso de los valores digitales de la cadena (ej. Bitcoin) las cuentas se liquidan atómicamente

4b

- En el caso de activos representados fuera de la cadena (p. ej. valores, activos inmobiliarios), las cuentas fuera de la cadena se ajustan a las instrucciones de liquidación
- Los cambios efectuados en las cuentas se reflejarán en el libro de contabilidad

Fuente: BBVA Research

Contratos Inteligentes
Casos de Uso

Los contratos inteligentes se podrán aplicar a prácticamente todas las cosas.

Contratos Inteligentes
Casos de Uso

Servicios financieros

- Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías.
- Micro seguros: Calculan y transfieren micro pagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso)
- Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.
- Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

Contratos Inteligentes
Casos de Uso

Servicios de la Salud

- Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.
- Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micro pagos automáticamente al paciente para su participación.
- Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT -Internet of Things- (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.

Contratos Inteligentes
Casos de Uso

Servicios del sector público

- Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto a nivel de encuesta como a nivel estatal.
- Apuestas: dos o más partes pueden apostar sin que se resienta su seguridad y sin necesidad de un tercero a través de un contrato inteligente que asegure unas condiciones concretas.
- Propiedades inteligentes: una casa, un coche, una nevera, una lavadora…todos los objetos que se puedan conectar a Internet se consideran propiedades inteligentes (del inglés, smart property). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos o alquilarlos de forma automatizada.

Contratos Inteligentes Beneficios

1) Actualizaciones en tiempo real. La naturaleza tecnológica del propio contrato inteligente hace que la velocidad de los procesos comerciales aumente considerablemente.

2) Menor riesgo de ejecución. El proceso de ejecución es inmutable y descentralizado, por lo tanto NO existe el riesgo de manipulación, incumplimiento o equivocación de la gestión de dicho contrato.

3) Mayor precisión. La automatización del sistema no solo proporciona rapidez sino mayor fiabilidad. No se producen errores en la transacción.

4) Menos intermediarios. Este tipo de convenios elimina directamente la intervención de terceros como bancos o notarios que dan fe y confianza a ese convenio.

5) Menor costo. Al no existir intermediarios que verifiquen o realicen el contrato los costos de las transacciones se reducen automáticamente.

ETH 2,0

El futuro de Ethereum

ETHEREUM

Al igual que Bitcoin, el Ether es un activo digital (y para simplificarlo lo solemos llamar criptomoneda). Y al igual que cuando utilizamos dinero en efectivo, no requiere que un tercero procese o apruebe una transacción.

Pero en lugar de operar como moneda digital o pago, el Ether busca proporcionar «GAS» para las aplicaciones descentralizadas en la red.

ETHEREUM

¿Cómo son creados los Ether?

Según la web oficial de Ethereum, la oferta total de Ether y su tasa de emisión fue decidida por las donaciones reunidas en la ICO de 2014.

Los resultados aproximados fueron:

60 millones de Ether creados a los contribuyentes de la preventa
12 millones de Ether (20% de los anteriores) para el fondo de desarrollo, la mayor parte de los cuales se destinaron a contribuyentes y desarrolladores iniciales y el resto a la Fundación Ethereum.
5 Ether se crean cada bloque (aproximadamente 15-17 segundos) al minero del bloque

ETHEREUM

Guía de medidas del Ether				
	wei		0,000000000000000001	10^{-18}
kwei	**lovelace**	femtoether	0,000000000000001	10^{-15}
mwei	**babbage**	picoether	0,000000000001	10^{-12}
gwei	**shannon**	nanoether	0,000000001	10^{-9}
	szabo	microether	0,000001	10^{-6}
	finney	miliether	0,001	10^{-3}
	ETHER		1	1
	kether		1.000	10^{3}
	mether		1.000.000	10^{6}
	gether		1.000.000.000	10^{9}
	tether		1.000.000.000.000	10^{12}

ETHEREUM
Tokens

Qué es un Token?

Un token es un activo digital que está implementado dentro de la BlockChain de una criptomoneda.

ETHEREUM

Token de utilidad

Los tokens de utilidad permiten a sus dueños acceder a diferentes servicios que ofrece una plataforma basada en una cadena de bloques. Se usan para dinamizar la micro economía de un ecosistema BlockChain, facilitando así el financiamiento de los proyectos.

Token de Seguridad

Los tokens de seguridad “son un tipo de tokens que dan a su propietario el derecho de reclamar sus intereses de inversión. Puede ser el derecho a participar en una entidad legal, para aportar capital, obtener ganancia, ser acreedor o prestamista, etc”.

ETHEREUM
Tokens ERC20

Un Token ERC-20, no es más que un smart contract que cuenta con una estructura de datos ya preestablecida. Esta estructura está pensada en facilitar la implementación de diversas funcionalidades sobre la BlockChain de Ethereum, facilitando el trabajo de creación a los desarrolladores.

ETHEREUM 2,0

Serenity o Ethereum 2.0 es el tan esperado y aún más largo movimiento de la red Ethereum desde la prueba de trabajo (PoW) a la prueba de participación (PoS), junto con algunas mejoras enormes en el lado de la escalabilidad.

ETHEREUM 2,0

Beacon Chain

Dentro de sus características destacan que es una cadena para la gobernanza de todo, funciona con prueba de participación e incluye bloques denominados Beacon.

Es la capa de consenso para todo: gestiona validadores, aplica recompensas y penalizaciones, sirve como punto de anclaje para los fragmentos a través de enlaces cruzados.

Parte Practica

CryptoZombies

Vamos a aprender programación con Solidity

https://cryptozombies.io/es/lesson/1/chapter/1

Marlowe

Muchas Gracias