BLOCKCHAIN PROFESSIONAL CERTIFICATE BCPC®

BCPC® VERSIÓN 052021

CertiProf®

Professional Knowledge

www.certiprof.com

Objetivos de Aprendizaje

- Identificar que es la 4ta revolución industrial
- Reconocer qué es la tecnología Blockchain y sus tipos
- Relacionarse con los consensos propios de la tecnología Blockchain y los nuevos modelos de soluciones empresariales
- Explorar el ecosistema de la tecnología Blockchain
- Analizar los Smart Contracts, su funcionamiento y aplicación
- Distinguir la relación de la tecnología Blockchain con las demás tecnologías 4.0
- Detallar los diferentes casos de uso aplicados con tecnología Blockchain

¿Quién es CertiProf®?

CertiProf® es un instituto examinador fundado en Estados Unidos en 2015. Ubicado en Sunrise, Florida

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **CKA's (CertiProf Knowledge Ambassadors),** son personas influyentes en sus campos de experiencia o maestría, entrenadores, formadores, consultores, blogueros, constructores de comunidades, organizadores y evangelistas, que están dispuestos a contribuir en la mejora del contenido
- **CLL's (CertiProf Lifelong Learners),** se identifican como aprendices continuos que han demostrado su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digitalizado en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen
- **ATP's (Accredited Trainer Partners), U**niversidades, centros de formación y facilitadores de todo el mundo que integran la red de socios
- **Autores (co-creadores),** Expertos o practicantes de la industria que, con sus conocimientos, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria
- **Staff interno,** nuestro equipo distribuido, con operaciones en India, Brasil, Colombia y Estados Unidos que apoyan día a día la ejecución del propósito de CertiProf®

Our Accreditations and Affiliations

Quien Debe Atender a Este Taller de Certificación

Cualquier persona que esté interesada en ampliar sus conocimientos en Blockchain y desee ampliar sus habilidades en esta tecnología para conocer sus características, tipos y posibles implementaciones en los sectores privado y publico.

Presentación

¡Bienvenido!
Preséntese en el siguiente formato:

- Nombre
- Empresa
- Cargo y experiencia

Insignia

Type: Certification

Cost: Paid

https://www.credly.com/org/certiprof/badge/blockchain-professional-certificate

Lifelong Learning

Los ganadores de esta insignia han demostrado su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digitalizado en constante cambio y expansión de hoy. También identifica las cualidades de una mente abierta, disciplinada y en constante evolución, capaz de utilizar y contribuir con sus conocimientos al desarrollo de un mundo más igualitario y mejor.

Criterios de ganancia:

- Ser un candidato para la certificación CertiProf®
- Ser un aprendiz continuo y enfocado
- Identificarse con el concepto de aprendizaje permanente
- Creer e identificarse genuinamente con el concepto de que el conocimiento y la educación pueden y deben cambiar el mundo
- Querer potenciar su crecimiento profesional

CertiProf®
certiprof.com

COMPARTE Y VERIFICA

TUS LOGROS DE APRENDIZAJE FACILMENTE

#BCPC #CertiProf

Agenda

Capítulo 1: Problemas Empresariales

CertiProf®

Professional Knowledge

www.certiprof.com

Introducción

En este curso para certificarse como Blockchain Professional (BCPC) comenzaremos con la investigación de productos y servicios de la tecnología.

En primer lugar, daremos una vista a la evolución, el futuro de la industria y la tecnología Blockchain y cómo la tecnología 4.0 BiBi especialmente, Blockchain va a influir en el futuro de la evolución de la industria. Posteriormente, analizaremos más a fondo los productos y servicios que están influenciados por la Tecnología Blockchain.

A través de este curso, daremos las bases con la finalidad del primer acercamiento de una solución integral para una empresa que puede apoyar a la eficiencia, control, confianza, trazabilidad y procesos que van a generar cambios disruptivos y positivos para cualquier sector.

4ta Revolución Industrial

La combinación de la realidad con dominios digitales y los avances tecnológicos que permiten maximizar el valor generado a partir de éstos es a grandes rasgos lo que se entiende por cuarta revolución industrial, término acuñado por Klaus Schwab, fundador del Foro Económico Mundial, explicado justamente en el libro de la cuarta (4IR) revolución industrial. Esta revolución integra tecnologías tales como el Big Data, la inteligencia artificial (IA), Blockchain, Internet de las cosas (IoT por sus siglas en inglés), además de que existen otras tecnologías que están empezando a resaltar como la impresión 3D, la tecnología de la nube y la realidad aumentada.

Claramente, hoy día nos encontramos ante un panorama extremadamente digitalizado y las revoluciones industriales previas que comprendían la máquina de vapor (1IR), el motor de combustión interna (2IR), y la implementación de elementos electrónicos e informáticos más avanzados que los ya existentes transistores como lo serían los electrónicos y las tecnologías de la información que automatizaran la producción (3IR) fueron la serie de pasos necesarios para alcanzar hoy día el punto donde diferentes tecnologías pueden llegar a integrarse para maximizar el valor de lo que realizan tanto las empresas, como lo que experimentamos todos en nuestro diario vivir.

Entre estas, la que está creciendo a pasos agigantados por su impacto en los negocios es justamente Blockchain por las bondades que brinda a cada negocio que la implementa. Así pues, a continuación, se detalla el trayecto evolutivo desde la primera revolución industrial hasta la cuarta revolución industrial.

Figura 1. De la 1ra RI a la 4ta RI.

Los Problemas Empresariales

Antes de aprender Blockchain o la tecnología de contabilidad distribuida (DLT) en detalle, uno puede preguntarse ¿por qué el mercado está tan fascinado con Blockchain? Si Blockchain es un mecanismo de almacenamiento, muchos de estos mecanismos han existido en la industria durante décadas. La respuesta es que Blockchain no es útil para almacenar datos de un individuo, pero es útil para múltiples partes, especialmente aquellas que no confían entre sí, sin embargo, desean compartir datos para alguna transacción comercial.

Los actuales mecanismos en el mercado para que bancos, organizaciones financieras y sistemas distribuidos globales (GDS) en los sistemas de cadena de suministro o viajes han de poder comunicarse entre sí, y por ello suelen tomarse libros contables centralizados (con registro confiable) para la operación en vista de que no existía otra alternativa práctica. No obstante, un solo actor (parte dentro del sistema) que no sea confiable puede llevar a problemas de inconsistencias y fraude, cosa que empieza a hacer que no sean perfectos y se requiera de actuar como un guardián y representar un punto único de falla (SPOF).

Estos responsables pueden no ser necesariamente confiables ya que pueden aceptar sobornos o excluir partes específicas que desaprueben (por ejemplo, las redes de pago que se niegan a servir artistas adultos), o pueden llegar a perder registros importantes de las transacciones dado que existe el error humano o algún desastre de fuerza mayor (natural o no natural).

Figura 2. Transacciones comunes en un ambiente empresarial y de gobierno.

Así pues, se empiezan a considerar otros modelos donde la evolución de los libros mayores (ledgers como se les conoce en inglés) entra a jugar un rol importante, ya que no solo existe el modelo centralizado que es el común donde se encuentra el problema empresarial, sino que también existe el modelo descentralizado, y justamente entra el modelo distribuido que es uno de los que se adentrará con mayor profundidad al avanzar esta certificación.

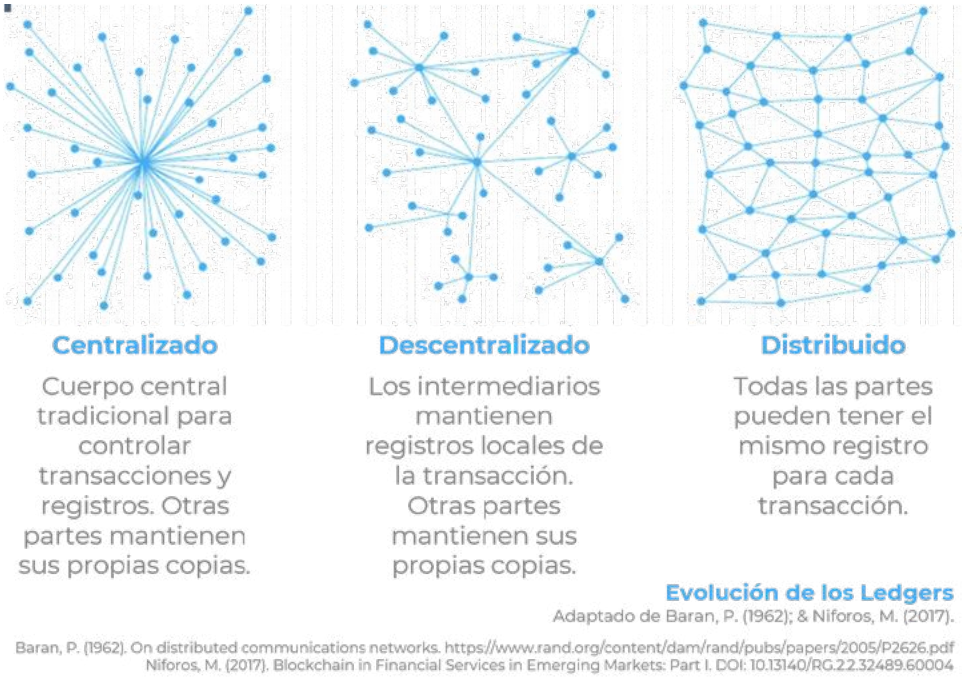


Figura 3. Evolución de los ledgers. Información adaptada de (Baran, 1962; Niforos, 2017).

Historia de la tecnología Blockchain (Tecnologías previas a Blockchain).

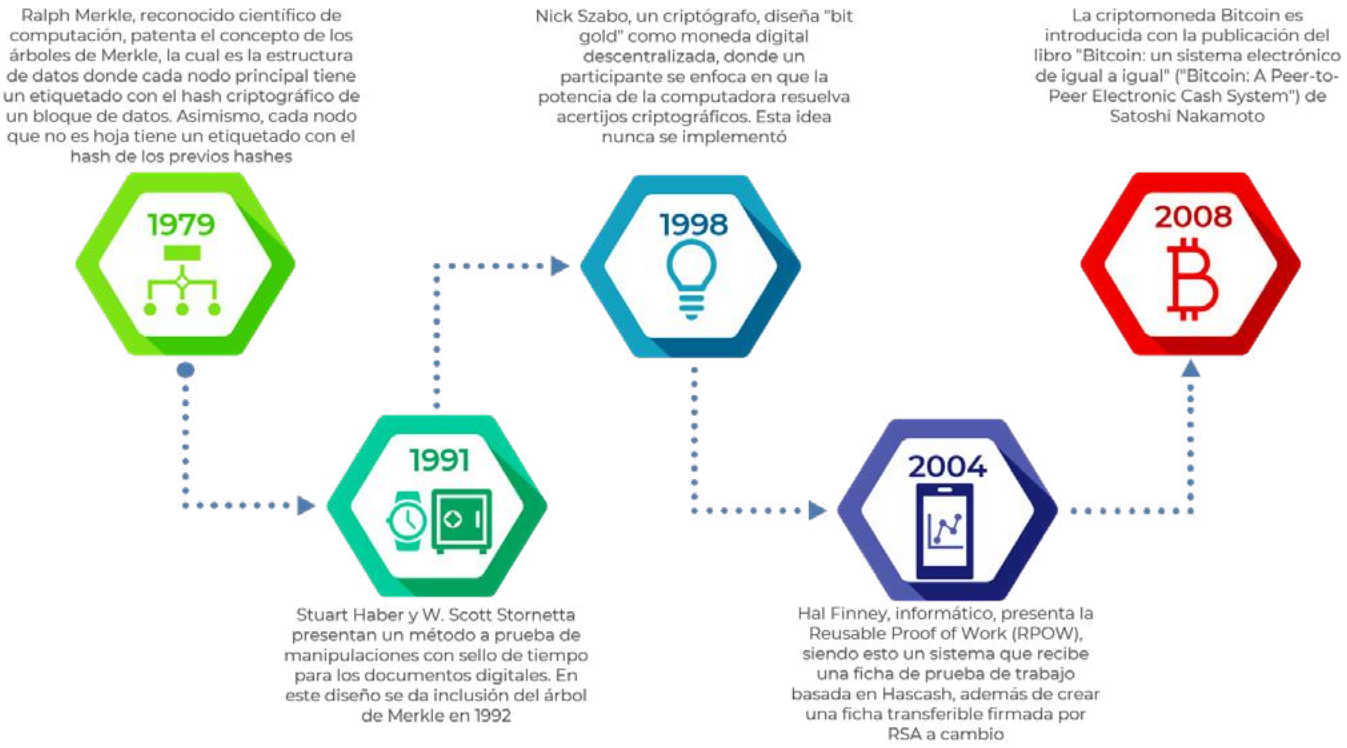


Figura 4. Historia de la creación de la tecnología Blockchain y tecnologías previas a Blockchain. Información adaptada de (Nakamoto, 2008; Sharma, 2021; Singh, 2020).

Capítulo 2: ¿Qué es Blockchain?

CertiProf®

Professional Knowledge

www.certiprof.com

¿Qué es Blockchain?

De acuerdo a como se expresa en el libro "Blockchain blueprint for a new economy" de Swan (2015), el Blockchain como arquitectura para un nuevo sistema de transacciones descentralizadas cuya confianza es nula es el componente clave de innovación con el que se cuenta. Asimismo, Blockchain es como otra capa de aplicación que se ejecuta en la pila existente de protocolos de Internet, donde se da añadidura de todo un nuevo nivel a Internet para permitir las transacciones económicas (aquí se comprenden pagos inmediatos en moneda digital, como contratos financieros más complicados a largo plazo).

Por otro lado, el Blockchain puede utilizarse no sólo para transacciones, sino también como sistema de registro e inventario para el registro, seguimiento, vigilancia y la transacción de todos los activos (entre otras aplicabilidades previamente vistas en los diferentes tipos de Blockchain). Así pues, es esencialmente similar a una hoja de cálculo gigante para registrar todos los activos y un sistema de contabilidad para realizar transacciones a escala mundial que puede incluir todas las formas de activos en poder de todas las partes en todo el mundo.

Figura 5. Blockchain como libro digital distribuido a prueba de manipulaciones.

- "En esencia, Blockchain es un libro compartido, programable, criptográficamente seguro y, por lo tanto, confiable, que ningún usuario controla y que puede ser inspeccionado por cualquier persona" -Klaus Schwab, fundador y presidente ejecutivo del Foro Económico Mundial
- Blockchain es un libro de transacciones compartidas entre las partes de una red, no controlada por una única autoridad central. Se puede pensar en un libro de registro: registra y almacena todas las transacciones entre los usuarios en orden cronológico. En lugar de que una autoridad controle este libro (como un banco), todos los usuarios de la red tienen una copia idéntica del libro, llamada nodos." –OECD
- "Blockchain" es un libro de contabilidad digital en el que las transacciones, por ejemplo, de Bitcoin y de criptografía, se registran cronológicamente y de forma pública (...). La idea es que mediante una transparencia radical, el bloqueo -creado mediante la posibilidad de que grandes porciones del público participen en la red- crea 'confianza' al hacer casi imposible el registro de entradas nefastas o el cambio de transacciones que ya han sido procesadas." -ONU
- "En esencia, Blockchain es una base de datos digital de información sobre transacciones que no vive en un lugar, sino en muchos puntos de Internet. Cuando alguien quiere hacer una transacción, los detalles son codificados y validados independientemente por una serie de usuarios que actualizan la base de datos y dejan un registro permanente. Esta tecnología es la más utilizada en el mercado de criptografía de Bitcoin." -BID

Blockchain entonces es un tipo de software que cuenta con una serie de transacciones digitales que se registran dentro del sistema y se agrupan a manera de "bloques" de información que comparten de manera segura la información entre los diferentes nodos (o computadores) dentro de la misma red. (UN Innovation Network, 2020). Cada vez que se genera una transacción, se suma un bloque y este bloque es "encadenado" a la cadena de bloques general, fortaleciendo así la red del Blockchain y el registro distribuido de la información, de manera segura, transparente e inmutable (Lapointe & Fishbane, 2018).

Por tanto, no se requiere de ninguna autoridad que autorice las transacciones y la manera en que se regula el proceso es con reglas de gobernanza previamente establecidas dentro del sistema frente al comportamiento de los actores (partes) que operan dentro de la red del Blockchain.

El Mundo Interconectado y su Relación con el Blockchain

El trayecto hacia esta tecnología ha sido un constructo de diferentes eventos que han permitido que se llegue a su alcance, lo cual se puede entender como los paradigmas informáticos, que de acuerdo con Swan (2015) son una forma de entender el mundo ya que estos varían dependiendo la década en la que se encuentren, tal como lo presenta la figura 6. Esto es debido a que primero se contaba con la PC y la computadora central, luego aparece internet y lo cambia todo porque esto llevó al paradigma de redes sociales y dispositivos móviles.

Estos elementos componen lo que se entiende como redes simples y estas redes simples lo que hacen es generar conexiones que permitan transferir información, puesto que esa es la finalidad última de lo que se ha querido desde la década de los 70s hasta la de los 2000s, mientras que ya la década de 2010 inicia con BItcoin, pero se extiende a lo que es la tecnología Blockchain en su variedad de aplicaciones en el negocio que permiten integrar distintas tecnologías a nivel emergente, como el IoT y el Big Data, todo con el objeto de asignar efectivamente los recursos suministrados.

Esta tecnología tiene el potencial de adquirir mayor adopción de la que el internet mismo tuvo, y resulta ser que mientras el paradigma 4 donde se incluyeron todas las aplicaciones móviles que permitieron transferencia de comunicación e interacción, da a establecer que para el paradigma 5 donde se encuentra el Blockchain se contará con transferencia de información y de funcionalidades de intercambio de valor, con lo que probablemente se tornará en mayores adopciones de dinero en el mundo digital.

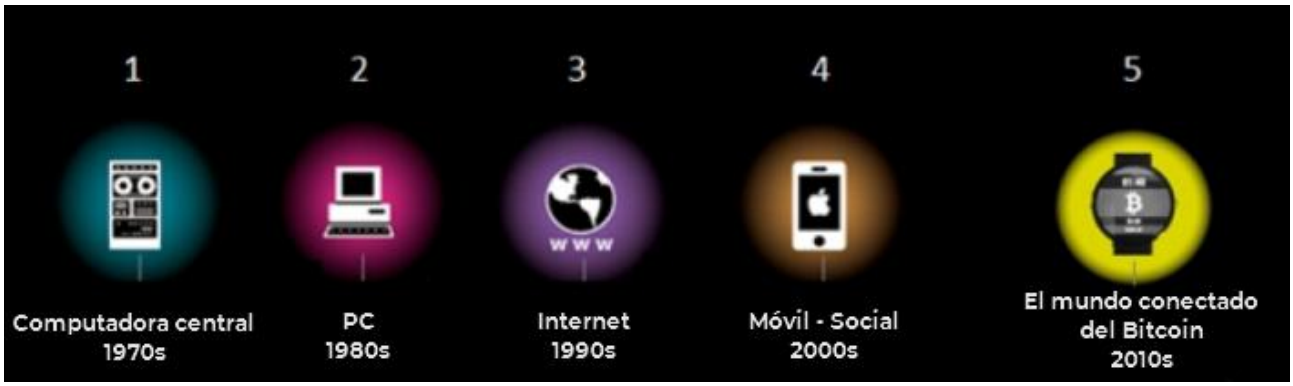


Figura 6. Computadores informáticos disruptivos de la década de los 1970s a los 2010s. Obtenido de Swan, M. (2015).

Los Atributos Clave de Blockchain

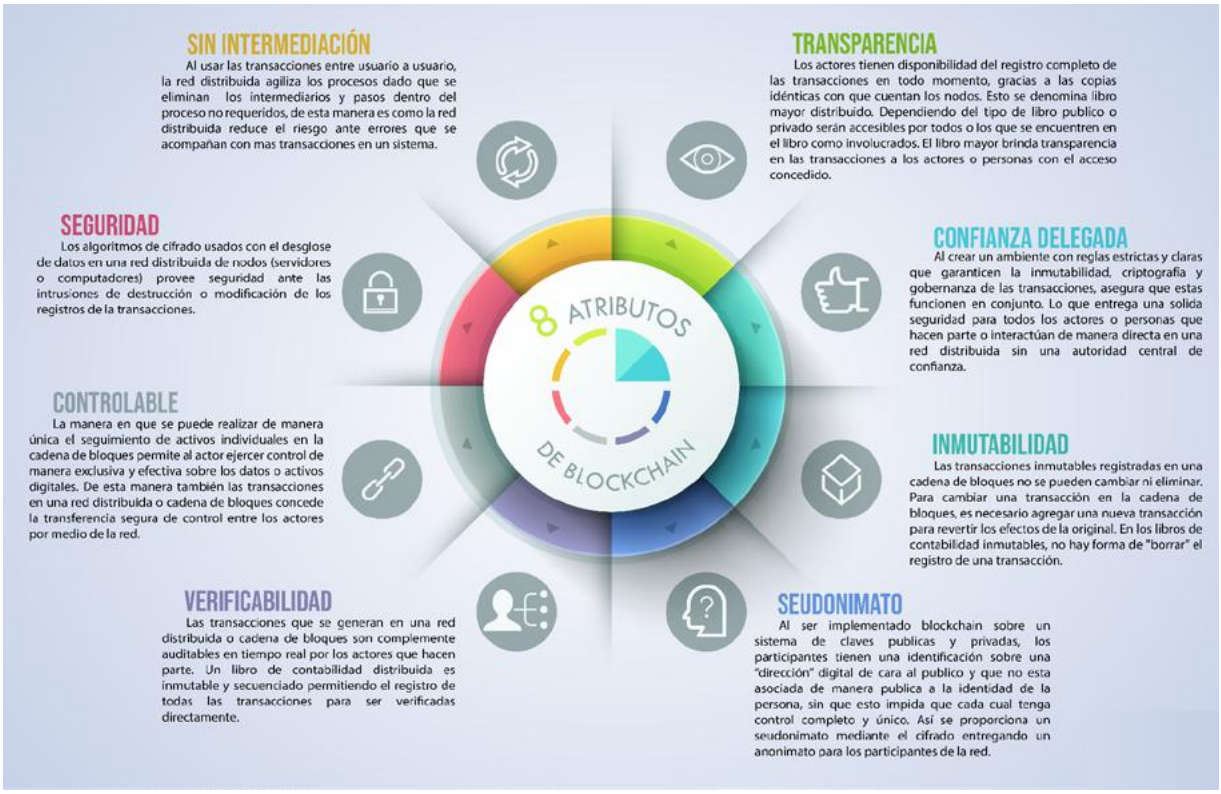


Figura 7. Atributos clave de Blockchain. Información adaptada de (Lapointe & Fishbane, 2019; UN Innovation Network, 2020).

La Evolución de Blockchain

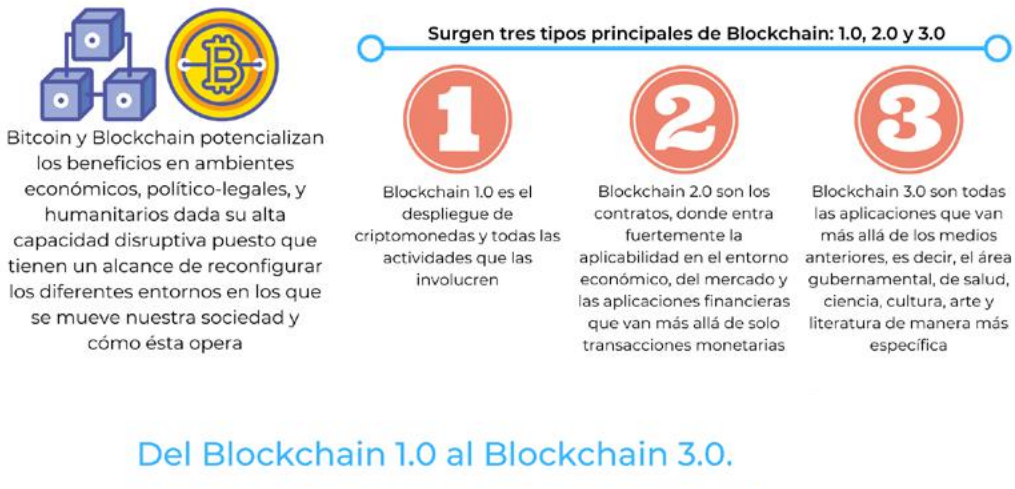


Figura 8. Del Blockchain 1.0 al Blockchain 3.0. Información adaptada de (Swan, 2015).

Blockchain 1.0

Criptomoneda: Primer Caso de Uso de Blockchain

“A menudo, Blockchain se utiliza incorrectamente de forma intercambiable con Bitcoin. Aunque Bitcoin fue el primer uso de blockchain, es sólo una aplicación de cómo se puede utilizar el libro mayor (ledger) para almacenar información” (UN Innovation Network, 2020).

Es común que se confunda Blockchain con Bitcoin, pero como se expresó con anterioridad, Bitcoin solamente es el primer caso de uso de Blockchain y cómo la información puede ser almacenada en el ledger. Estas criptomonedas de hecho son activos digitales que se mantienen justamente por Blockchain y que permiten las transacciones de igual a igual (peer-to-peer) con ayuda de un sistema distribuido y la criptografía pertinente. De acuerdo al UN Innovation Network (2020) estas no son creadas y/o emitidas por un banco central como las divisas FIAT ya que estas lo que hacen es depender de la red del Blockchain donde se almacena quién, cuándo y qué se ha enviado y recibido. Su valor se determina por condiciones económicas y de escasez, así como utilidad, y entre las que más destacan se encuentra el Bitcoin (BTC) y el Ether (ETH), las cuales operan con su respectivo token asociado a su propio Blockchain.

Bitcoin

Bitcoin (BTC) en esencia es dinero digital. Su creación fue en 2009 al haberse propuesto el whitepaper de Satoshi Nakamoto, dando origen a un sistema de pagos online con técnicas de encriptación usadas para la generación de unidades de la divisa y la verificación de las transacciones, cosas independientes a un banco central (Swan, 2015). Aunque su uso es de los más comunes para los criptoactivos, existen otras alternativas para esta finalidad, como Litecoin o Dogecoin, aunque no tengan una participación en el mercado nada cercana a la del BTC. Estos entonces, además de servir para transacciones entre dos partes iguales (peer-to-peer), son creados como "recompensa por el trabajo de procesamiento computacional, conocido como minería, en el que los usuarios ofrecen su potencia de computación para verificar y registrar los pagos en el ledger público" (Swan, 2015).

A partir de esto, entonces Bitcoin es "una transformación fundamental del dinero. Una invención que cambia la más antigua tecnología de nuestra civilización, (...) sustituyendo fundamentalmente la arquitectura subyacente por una, en la que todos los participantes son iguales." (Antonopoulos, 2017). Al ser el dinero descentralizado se rige únicamente por el consenso, por lo cual da un empoderamiento de que el dinero es del propio usuario y nadie más tiene dominio sobre él, y finalmente, es su propio origen lo que hace que las fronteras no sean una barrera para su transaccionalidad.

Cómo Funciona Bitcoin

"Blockchain es el libro de cuentas público de todas las transacciones de Bitcoin que se han ejecutado. Crece constantemente a medida que los mineros añaden nuevos bloques (cada 10 minutos) para registrar las transacciones más recientes." (Swan, 2015). Cada bloque dentro del ledger tiene una añadidura cronológica y cada cliente dentro de esta red cuenta con su respectiva copia, y absolutamente toda la información desde el origen mismo del primer bloque hasta el más actual se ve registrado. Como se dice que es dinero entre iguales a manera de relación entre los participantes y un sistema, se da que la arquitectura del BTC es de dicha forma y cada participante habla el protocolo a un mismo nivel, suponiendo a su vez que esta arquitectura de igual a igual es diferente a las que comúnmente conocemos como las de cliente-servidor que maneja Facebook donde no se usan protocolos y todo el estado y mantenimiento de datos es controlado por Facebook (Antonopoulos, 2017). A groso modo, los BTCs se almacenan en billeteras digitales con llaves públicas (cuenta o dirección) y privadas (contraseña) por usuario, las cuales permiten el intercambio del criptoactivo una vez han sido configuradas exitosamente (Mohanty, 2019).

Doble Gasto – Problema de los Generales Bizantinos

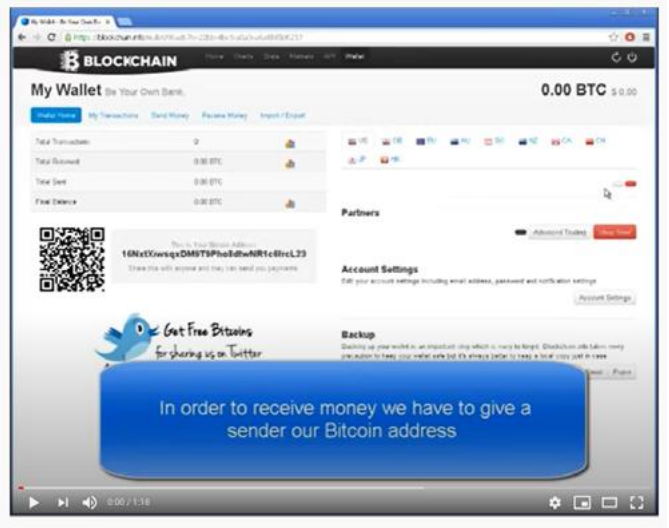
El problema de construir un sistema puramente distribuido pero confiable no es nuevo en informática. Es un desafío común en los sistemas distribuidos sin control central para hacer cumplir la confianza y, en general, es un subconjunto del estudio de la tolerancia a fallas. Imagine, por ejemplo, un sistema informático con componentes distribuidos que necesitan comunicar información entre sí, pero esa información podría no comunicarse con precisión (o no) debido a fallas técnicas.

El problema de los generales bizantinos, propuesto por primera vez por Marshall Pease, Robert Shostak y Leslie Lamport en 1982, proporciona una descripción estilizada de este problema.

“Imaginamos que varias divisiones del ejército bizantino están acampadas fuera de una ciudad enemiga, cada división dirigida por su propio general. Los generales pueden comunicarse entre sí solo por mensajería. Después de observar al enemigo, deben decidir sobre un plan de acción común. Sin embargo, algunos de los generales pueden ser traidores, tratando de evitar que los generales leales lleguen a un acuerdo. Los generales deben tener un algoritmo para garantizar que (A) Todos los generales leales decidan sobre el mismo plan de acción y (B) Un pequeño número de traidores no puede hacer que los generales leales adopten un mal plan " (Lamport et al., 1982). También existe un acercamiento a la relación entre el problema de los generales bizantinos con el problema de los algoritmos distribuidos (ICC, 2018), o intentos pasados de resolver el lado que tiene que ver con divisas (Chaum, 1984; Chaum et al., 1990; Okamoto & Ohta, 1992; Wei Dai, 1998).

eWallet - Billetera Digital

Para que se pueda hacer una recepción de criptoactivos, es necesario que se brinde la dirección, por ejemplo, la dirección BTC. Entonces, para que se haga el uso transaccional mediante una eWallet, se ingresa la dirección y la cantidad y una vez enviada, se actualiza el balance actual de la eWallet (también se actualiza si estamos recibiendo criptoactivos). Con la dirección BTC se puede verificar en un portal de transacciones de Blockchain las transacciones ligadas a esta dirección, y si es muy reciente cabe la posibilidad de que diga que "no está confirmada"; sin embargo, una vez pasen unos minutos aparecerán las confirmaciones de la transacción.



Cómo enviar y recibir bitcoin
https://www.youtube.com/watch?v=kh43-cC42-o&feature=youtu.be

Cómo Escoger una Wallet de Bitcoin

La selección de una Wallet digital puede depender en gran medida de qué se desea asumir para dicha tarea, por ello es que se tienen que considerar el control, la validación, la transparencia, el ambiente, la privacidad y las cuotas (Bitcoin, 2021). Hoy día contamos tanto con sistemas operativos móviles como de escritorio, por lo que, dependiendo del sistema operativo, las wallets disponibles cambiarán, y en todos los casos siempre hay que tener en cuenta el estado de las mismas, entre bueno, aceptable, con cautela y no aplicable.

Finalmente, las características propias de lo que pueden tener las wallets pueden jugar un rol importante, como por ejemplo la autorización de doble factor para aumentar la seguridad. Como se puede ver en la ilustración 1, filtrando por ciertos criterios para el sistema operativo de Android, las dos Wallets a escoger vendrían a ser entre la Bitcoin Wallet y la Unstoppable ya que Mycellum tiene una alerta de cautela en validación; mientras que, la ilustración 2 muestra los diferentes portales donde se puede realizar una compra de BTC.

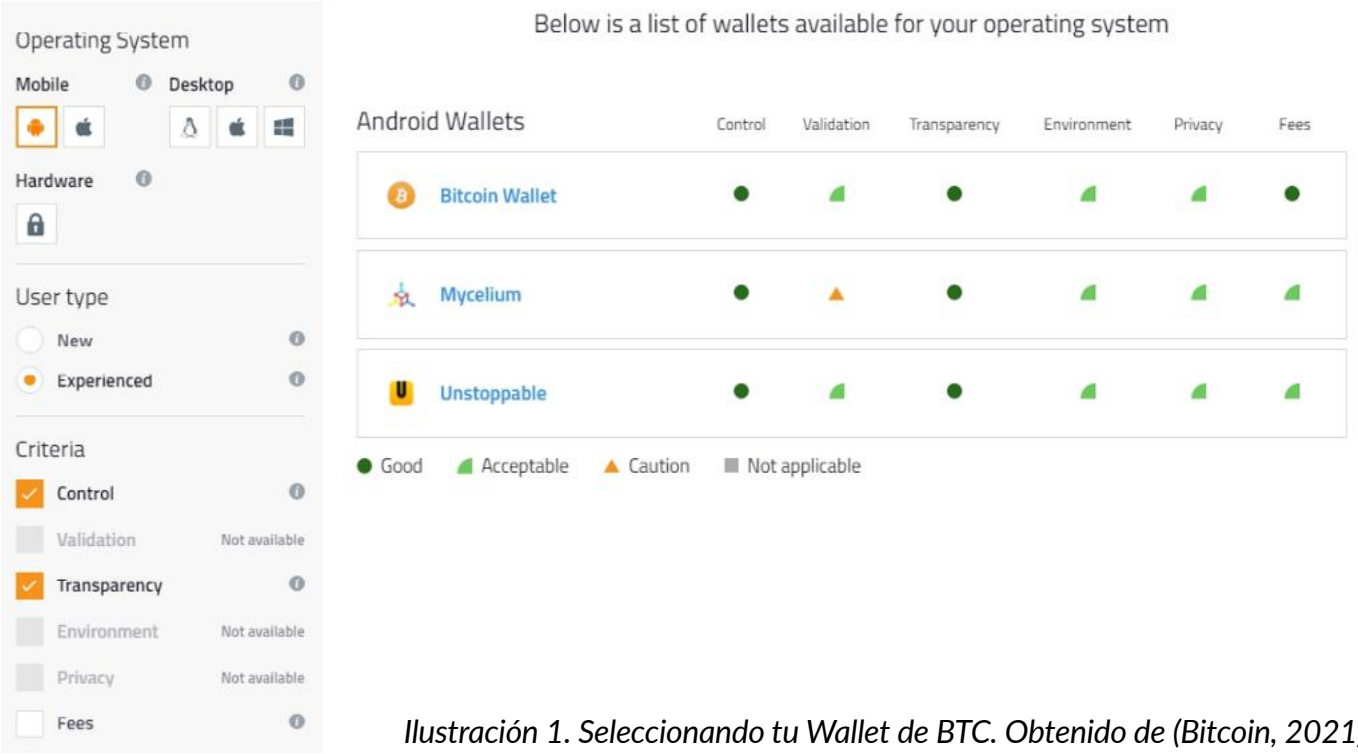


Ilustración 1. Seleccionando tu Wallet de BTC. Obtenido de (Bitcoin, 2021).

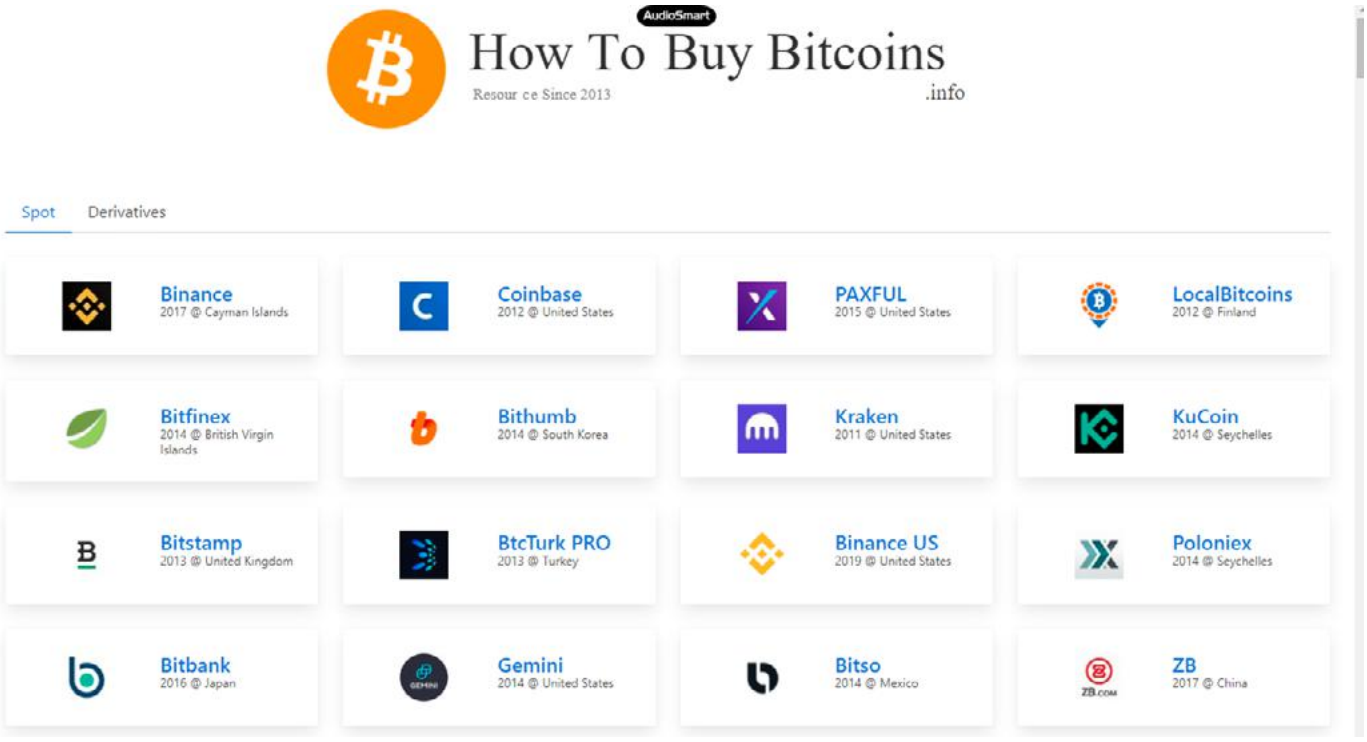


Ilustración 2. ¿Dónde comprar BTC? Obtenido de (Bitcoin, 2021).

Blockchain 2.0

Después del nacimiento del Blockchain 1.0 con el despliegue basado en el whitepaper de Satoshi Nakamoto, para la versión del 2.0 era necesario poder sostener una mayor complejidad en cuanto a grabación y transferencia de activos como Smart Contracts y propiedades inteligentes. Es natural entonces pensar que el Blockchain 2.0 incluye lo que fue Bitcoin 2.0 con sus protocolos, Smart Contracts, Smart Propery, Dapps, DAOs y DACs, llevando así una descentralización de mercados e intercambio de activos más allá de solo criptomonedas (Swan, 2015).

Smart Contracts

Como Bitcoin al implementar los Smart Contracts (entre otras funcionalidades) hace que emerja el Blockchain 2.0, estos se pueden entender como una forma de llegar a acuerdos entre las partes de la red, facilitando tareas que ya existían pero que o bien por consumo de tiempo o por asuntos de confiabilidad se tornaban engorrosas, por ello el despliegue de los Smart Contracts sirve como un apoyo a esta labor. Asimismo, al construir protocolos de baja confianza que tengan interacción con Bitcoin, se pueden crear nuevos productos como Smart Property, propiedad virtual transferible, agentes (programas autónomos que mantienen su propia wallet) y mercados distribuidos (Bitcoin, 2021).

Dapps, DAOs, DACs, and DASs: Increasingly Autonomous Smart Contracts

Dentro del Blockchain 2.0 es que se empieza a contar también con las aplicaciones descentralizadas (DApps), las organizaciones autónomas descentralizadas (DAOs, también conocidas como DACs), y las sociedades autónomas descentralizadas.

- En el primer caso, las DApps son unas aplicaciones que corren en la parte superior del Blockchain o de un DLT, soportándose en Smart Contracts y sin necesidad de un tercero, pero a diferencia de un Smart Contract per se, las Dapps cuentan con participantes ilimitados en ambos lados (Anand & Chauhan, 2020). Por otro lado, estas DApps son divididas entre tres categorías, las cuales son las que administran dinero, las que administran tareas semi-financieras (el dinero se involucra, pero se requiere otro aspecto aparte del dinero), y "otros" que incluye aspectos de gobernanza y votación (Ethereum, 2021)
- En el segundo caso, las DAOs son Smart Contracts soportados en algoritmos para la ejecución de decisiones que requieren que se les suministre información sin un manejo jerárquico, donde los humanos interactúan bajo lo estipulado por un protocolo que permite que las decisiones se tomen de manera autónoma por el DAO, y que considera a su vez a los individuos como esa ayuda para lo que no se puede hacer de forma automatizada (Anand & Chauhan, 2020). En esencia, funciona como una organización virtual con autorización de manejo de fondos y de alteración de reglas, pero este tipo de cosas deben ser preconfiguradas y los miembros de la red han de decidir cómo se manejarán los fondos, pero no existirá como tal una jerarquía directa. A estas también se les puede conocer como corporaciones autónomas descentralizadas (DACs) ya que igualmente están los accionistas (shareholders) que reciben los dividendos y también se cuenta con las acciones intercambiables (Ethereum, 2021; Ouyang et al., 2019)

- En el tercer caso, si bien las organizaciones descentralizadas se encasillan en las DAOs y estas pueden entenderse directamente como DAO o como DAC, empieza también a emerger el concepto de DAS donde ya no se habla de entidades organizacionales, sino a nivel sociedad virtual que no tendría una relación de asociación con organizaciones, gobiernos o naciones-estado específicas. En compendio, múltiples DAOs y DApps tendrían que funcionar autónomamente dentro del Blockchain conformando una DASs donde la ejecución de los Smart Contracts sería una de inmensa multiplicidad y complejidad a su vez, y si bien no está ligado directamente a un gobierno, sí adapta muchas de las aplicabilidades de Blockchain al aspecto gubernamental

Figura 9. Pasos básicos para implementar una DAOs. Información adaptada de (Anand & Chauhan, 2020).

Blockchain 3.0

Si bien Bitcoin nació directamente siendo un 1.0, y luego con sus funcionalidades en constante actualización evolucionó al 2.0, se podría decir que Ethereum llegó directamente siendo 3.0 al generarse empezó a permitir construcción y publicación de aplicaciones distribuidas. Entonces, se cubre más allá del punto A al B pues la implementación de dinero programable y las características que lo permitiesen empezaban a tener lugar en esta fase. De manera que, la infraestructura de Blockchain que se designaba a ser fuerte y sólida en su sistema de scripts y una plataforma "turing complete" se terminó por denominar Ethereum.

Ethereum

Ethereum es un Blockchain que da la permisibilidad de construir y publicar DApps, y también manejar las DAOs. En esta se contemplan la criptografía y una máquina virtual que ejecuta tanto cualquier moneda, como cualquier script o proyecto de criptoactivos, y permite la ejecución de todas las cadenas de bloques o protocolos mediante lo que es entendido como una plataforma unificada universal. Esto hace que Ehtereum se torne en un Blockchain agnóstico y de protocolos enfocado en desarrollo de aplicaciones e implementación de Smart Contracts con involucramiento de interacciones de cualquier variedad de cadena de bloques, criptoactivo o protocolo (Ethereum, 2021).

Blockchain 4.0

Nueva Era de las Blockchain

Como ya se ha visto, el Blockchain 1.0 es sinónimo de Bitcoin, el 2.0 es la integración de nuevas aplicaciones y funcionalidades, y el 3.0 es sinónimo de Ethereum; sin embargo, ¿Qué vendría a ser el 4.0? Hasta el momento no es como que exista una serie de definiciones ligadas a las diversas fuentes de la literatura que expliquen lo que es, pero en esencia es tanto la construcción como el manejo de aplicaciones y que se cuente con dos factores: 1) Corran rápido y fluido dentro del sistema, y 2) Preserven los beneficios únicos que provee la tecnología Blockchain.

Claramente, la verificación es algo que es costoso, pero por ello estructuras criptográficas alternas pueden llegar a ser inclusive más eficientes y manteniendo los dos puntos anteriores. Así pues, una tipología como "Bloques sin bloques" entra en vigor mediante los gráficos acíclicos dirigidos (DAGs por sus siglas en inglés) y estos incluyen dentro de sí IOTA, Hashgraph, Byteball y DAGCoin (Swan & Dos Santos, 2018). En la tabla 1 se puede apreciar una comparativa entre estas DAGs y otras.

Característica / Tecnología	IOTA	DAGCoin	Byteball	Nano	XDAG	NXT	Orumesh
Método de distribución	ICO	DAG basado en Byteball como referencia	Rondas Airdrop a los poseedores de BTC	Grifo oficial	N/A	N/A	N/A
Tiempo promedio de confirmación	1 60 segundos	Alrededor de 30 segundos	Minutos	1 10 segundos	N/A	Minutos	Posiblemente 3 segundos
Wallets disponible	Windows (Full/Light) | MAC (Full/Light) | Linux (Full/Light)	Mac | Android | Windows | Linux | Web wallet	iOS (Light) | Android (Light) | MAC (Full/Light) | Windows (Full/Light) | Linux (Full/Light)	Windows (Full) | MAC (Full) | Linux (Full) | iOS (Light) | Android (Light)	Windows | Android | MAC | Mineros de GPU	Cliente NXT (Linux, Windows, MAC, Android)	OruWallets
Protección de spam	PoW al adjuntar transacciones	Cuenta con un método de protección, pero no revelado	Cuotas/Tarifas	PoW al adjuntar o recibir un bloque	Algoritmo ECDSA con una llave privada de 256-bits. La sesión de la llave es transmitida utilizando el algoritmo RSA de llave de 8192-bits. No es una protección de spam per se, son algoritmos de seguridad	N/A	N/A
Open source / Descentralizado	Parcialmente. Son de código cerrado los coordinadores de puntos de control	Descentralizado	Totalmente	Totalmente	Descentralizado	Descentralizado	Descentralizado
Estado de la red	WIP	N/A	Avanzado	Avanzado	N/A	N/A	N/A
Cuotas	Ninguna	Casi nulas	Bajas	Ninguna	N/A	Cuotas mínimas	Ninguna

Tabla 1. Comparación entre tecnología DAG existente. Información adaptada de (Pervez et al., 2018).

Corda

Por otra parte, dentro de las Blockchains/DLTs existentes, Corda aumenta la eficiencia de los procesos para una base empresarial, donde toda la data se almacena en bases de datos individuales o ledgers después de una validación contractual y las verificaciones notariales debido a que siempre está la existencia de un nodo notario en la red que valida y verifica toda transacción entre las partes que conforman la red. Este sistema único aparte de contar con elementos de identidad, estados, contractos, transacciones, consensos y flujos, también tiene las bondades del notario (privacidad y balanceo de carga de información entre distintos notarios), el manejo de ventanas de tiempo y los oráculos (esencialmente la llamada de datos externos a la red privada de Corda).

Sin embargo, esto va un poco más allá de otras Blockchains en términos de compliance y por eso se podría considerar que no solo cumple con lo necesario para recaer pertenecer a esta categoría de Blockchains, sino que incluye un nuevo componente, garantizar desde su origen la alineación con el GDPR para la privacidad de data donde hay soluciones de conocer al cliente (KYC por sus siglas en inglés) directamente construidas en Corda (Mohanty, 2019).

DLT 5.0

Si ya los Blockchains 4.0 son algo de lo que es complejo hablar dado que no está revisado a profundidad en la literatura, pensar en un 5.0 ya es algo "futurístico", pero si bien este tipo de soluciones fueron conceptualizadas por Swan & Dos Santos (2018) mediante las redes inteligentes, hoy día R3 (la desarrolladora de Corda) sacó al mercado la solución Conclave. Esta solución es posiblemente la más ambiciosa para llegar a posicionarse en esta categoría y es que integra tanto las bondades del Blockchain como las de la analítica, y sin descuidar en ningún momento los previos alineamientos al compliance, transparencia y seguridad, por esto es que ya se puede discutir sobre una visión de Blockchain como la habilitante de las redes inteligentes.

Redes Inteligentes

Una red de campo de redes inteligentes es el siguiente paso a dar, a partir de éste se da una caracterización, monitoreo y control de los sistemas como lo pueden ser el Blockchain con redes económicas y las redes de aprendizaje profundo (deep learning). Claramente, existen distintos tipos de redes inteligentes, pero resaltan las dos previamente mencionadas por su capacidad, potencial e impacto. Estas redes cuentan con un funcionamiento autónomo e inteligente con construcciones de infraestructura directas en el sistema que lo permitan así. De manera más formal "las redes inteligentes son máquinas de estado que hacen conjeturas probabilísticas sobre los estados de la realidad del mundo y actúan sobre esta base" (Swan & Dos Santos, 2018). Siempre permitiendo que sea el software inteligente quien opere el sistema.

Figura 10. Dos eras de las redes informáticas: Redes simples y redes inteligentes. Obtenido de Swan, M. & Dos Santos, P. M. (2018).

Conclave

Conclave es una plataforma que permite el desarrollo de aplicaciones que permiten el análisis y el compartir data privada entre múltiples partes sin necesidad de que la confidencialidad de la data misma sea comprometida durante el proceso. Esto es debido a que el compartir la data mediante Conclave trasciende a un nuevo nivel donde la contribución de la data por parte de los miembros contribuye es directamente al análisis sin necesidad de revelar la data real de cada quien (r3, 2020). Así pues, Conclave, entre sus múltiples casos de uso, puede capitalizar directamente entre los siguientes:

- Detección de fraude
- Agregación de data de mercado
- Coincidencias de órdenes de pedido privadas
- Soluciones de analítica

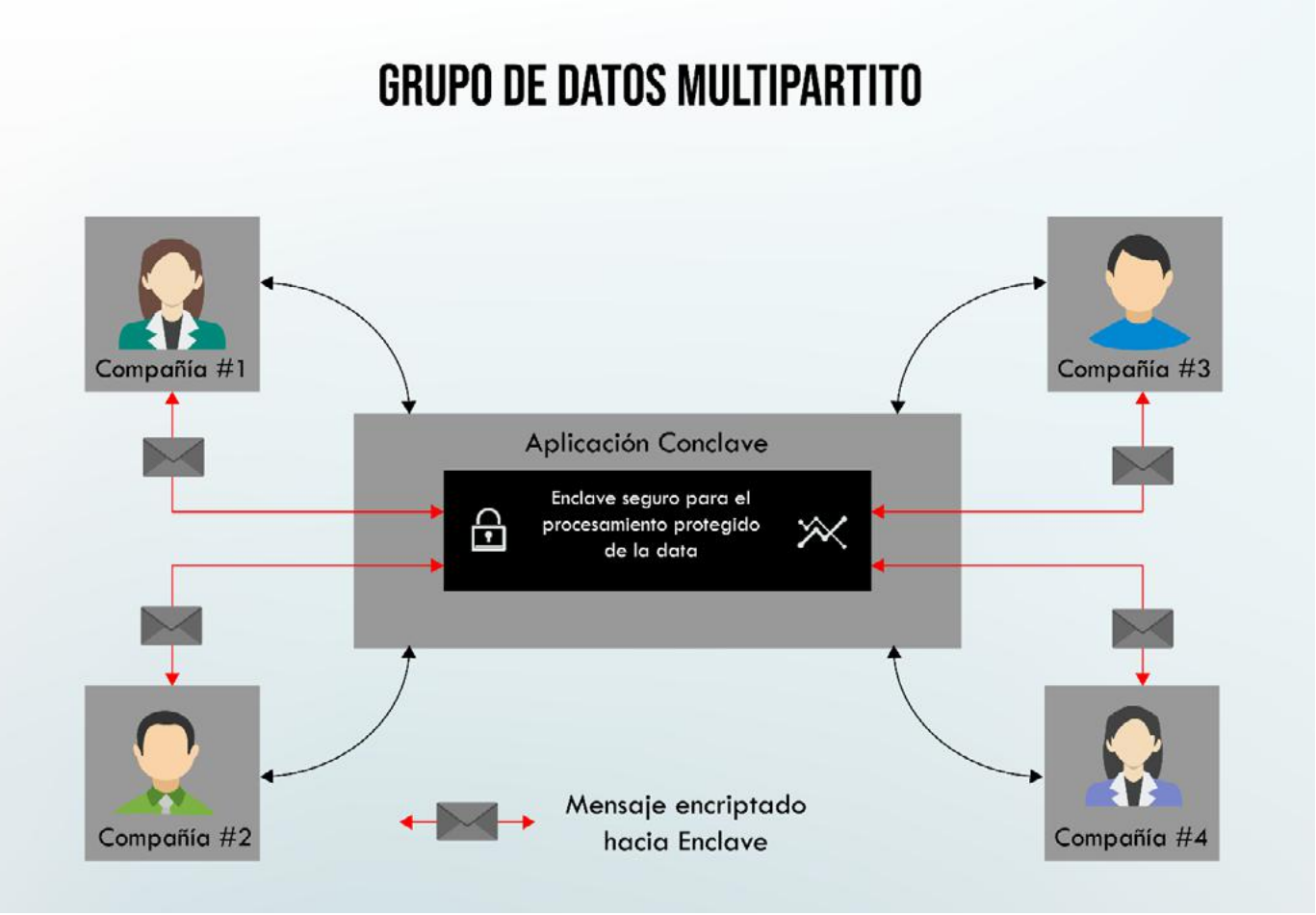


Figura 11. Grupo de datos multipartito con Conclave - Funcionamiento base. Información adaptada de (r3, 2020).