BLOCKCHAIN

Comparativo Distributed Ledgers (DLTs)

Marzo del 2018

C MINDS

Índice

Blockchain y distributed ledgers

Originalmente se le llamó *blockchain* a la tecnología de bases de datos distribuidas en redes *peer-to-peer*. Un nombre heredado de su principio básico de funcionamiento: una lista enlazada (*chain* o cadena), donde cada elemento (*block* o bloque) de la misma contiene segmentos de información y un apuntador al bloque anterior e integra sistemas criptográficos para detección de cambios y la trazabilidad de transacciones. Sin embargo, la tecnología, originalmente hecha popular en 2008 por *Bitcoin* para la implementación de una criptomoneda, ha cambiado radicalmente desde su concepción. Ahora existen decenas (si no es que cientos) de variaciones al funcionamiento de *blockchain* propuesto por Satoshi Nakamoto[1]; algunos propuestos enteramente para nuevas criptomonedas con casos de uso no cubiertos por *Bitcoin*, otros enfocados a construir sistemas de confianza genéricos que permitan repensar el funcionamiento de procesos y sistemas existentes. Por tal razón, el término *blockchain* se ha quedado corto ante la amplia oferta de los últimos años; jugando ahora el papel de un sabor individual de tecnología dentro de una categoría mucho más grande: *distributed ledgers* (también conocidas como *DLTs* por sus siglas en inglés)

El componente común entre todas las tecnologías de *distributed ledgers* es un sistema de almacenamiento de información que se replica (en poco tiempo: e.g. minutos o segundos) entre múltiples nodos en una red (la cual puede ser de cualquier tamaño y encontrarse distribuida por todo el mundo). Con esta funcionalidad, se da pie a una base de datos (un buen símil, para fines de simplicidad) inmutable, trazable, confiable y precisa; objetivos que diferentes tecnologías permitirán a mayor o menor grado y que implementarán de maneras distintas. Asimismo, uno de los pilares de este tipo de software es la criptografía, un área de la informática que permite (de manera simplista) firmar, ocultar, procesar e identificar información. Los algoritmos criptográficos han permitido también la implementación de un acertijo o prueba computacional que formó parte del núcleo funcional de *Bitcoin*: el *proof-of-work* (prueba de trabajo), un método de validación de bloques que requiere de un alto poder computacional para encontrar la respuesta de dicho acertijo; pero, en contraste, validar la respuesta es computacionalmente de bajo costo y fácil de hacer. El *proof-of-work*, de manera general, utiliza *hashes* criptográficos[2] para que un nodo de la red valide transacciones

[1] La persona o grupo de personas que crearon Bitcoin y el software que lo rige.
[2] Una función de digestión de datos que recibe cualquier cadena de información y genera un valor de longitud fija de alta entropía, el cual es determinista (es decir, no aleatorio) pero no predecible.

al resolver esta prueba (proceso coloquialmente denominado como minar/minería) y las agregue a la red (una vez que la respuesta de la prueba es validada); con lo cual se le recompensa a través de una criptomoneda.

En principio, esta tecnología es muy atractiva para el sector financiero ya que, por un lado, evita que las personas cometan fraudes al realizar gastos dobles[3]; y también remueve la necesidad de que el cuentahabiente deposite su confianza en una institución financiera, ya que esta última no tiene control de la base de datos y por lo tanto, no puede editarla sin que el otro lo sepa (o lo apruebe, incluso). Sin embargo, como la gran mayoría de las herramientas tecnológicas, la tecnología puede ser utilizada para otras aplicaciones, por ejemplo: registros de inmuebles; la emisión y rastreo de documentos legales y de identidad; compra-venta de bienes y servicios; loterías, apuestas y juegos de azar con alta transparencia; almacenamiento de datos; sistemas de votación y democracia; entre muchas otras aplicaciones. Sin embargo, la implementación original de *Bitcoin* no permite ninguna de estas aplicaciones[4] y su tecnología no es lo suficientemente flexible y madura para lidiar con algunos de sus más grandes defectos (causados principalmente por las actividades de minería). Por ejemplo, la red de *Bitcoin* consume más energía al año que países enteros (42TWh[5], superior al consumo eléctrico de Irlanda, Hungría o Nueva Zelanda) y ha llevado la demanda de semiconductores para circuitos integrados y *hardware* de minado a niveles insostenibles a largo plazo.

Por ello, la comunidad de *blockchain* comenzó la búsqueda y desarrollo de nuevas tecnologías que permitieran resolver estos problemas, de la mano de proveer nuevas herramientas que puedan ser utilizadas para un espectro más amplio de aplicaciones. Una de las primeras y más exitosas tecnologías inspiradas en *Bitcoin* es *Ethereum*: una plataforma descentralizada que permite la implementación y ejecución de contratos inteligentes (*smart contracts*): *software* que tiene su código fuente almacenado en los bloques de una red *blockchain* con la intención de que los usuarios de esta red puedan ejecutar dicho programa sin la necesidad de un servidor central y, virtualmente, sin posibilidades de indisponibilidad (*downtime*), censura, fraude o interferencia de terceros. De esta manera, *Ethereum* abrió la puerta a la posibilidad de un *distributed ledger* de uso genérico (en el cual, cualquier persona puede construir y publicar aplicaciones), potencialmente ilimitado en términos de uso y aplicaciones; muy similar a lo que

[3] Por ejemplo: un usuario tiene $10 y, de alguna manera (e.g. falsificación, engaño), gasta esos $10 con dos actores al mismo tiempo. Es decir, termina gastando $20.
[4] La red de *Bitcoin* solo permite transacciones financieras con la criptomoneda.
[5] Fuente: theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

logró el Internet a finales del siglo XX. Por ello, *Ethereum* se posicionó como una de las tecnologías más prometedoras del momento, y *Ether*, la criptomoneda[6] que mantiene todo el sistema operacional, como la segunda moneda más valiosa después de *Bitcoin*[7].

De la misma manera, otros actores del ecosistema han lanzado plataformas basadas en *blockchain*, con una serie de aplicaciones distinta para cada una, algunos ejemplos entre los casi cientos de opciones están: *Zcash*, *Ripple*, *Monax*, *Corda*, *Hyperledger* (de la que se desprenden *Sawtooth*, *Fabric, Iroha, Burrow* e *Indy*) y *Hashgraph*. Dentro de esta gran diversidad se pueden identificar principalmente dos grandes categorías: soluciones empresariales (*enterprise*) y genéricas. La de mayor uso, incluyendo *Ethereum*, se encuentran en ésta última, mientras que las empresariales forman parte de una nueva ola de productos y servicios inspirados en los genéricos pero con la intención de proveer valor a gobiernos o grandes corporativos e instituciones. Dentro de esta categoría se encuentran *DLTs* como *Monax*, *Corda* o *Ripple*, los cuales integran nuevas funcionalidades y niveles de personalización al *blockchain* tradicional, en algunos casos, más allá de lo que el nombre *blockchain* usualmente engloba; por ello, de nuevo, el uso del término bitácora distribuida. Algunas de las nuevas características más importantes de las nuevas *DLTs* son:

1. Acceso: se puede elegir si la red es pública (cualquier persona puede unirse a la red), privada (sólo algunos actores pre-autorizados pueden acceder) o híbrida (redes segmentadas). Por ejemplo, *Ethereum* es una red pública, mientras que *Ripple* es privada, aunque algunas opiniones la marcan como híbrida (permite transacciones al público en general, pero hay segmentos sólo accesibles a ciertos actores).
2. Roles: permite elegir si los nodos de la red son homogéneos en permisos o no. Con ello, se limita que sólo algunos actores puedan realizar acciones que otros no. Bitcoin es el mejor ejemplo de una red sin sistemas de permisos, todos los usuarios tienen acceso a todas las funcionalidades; mientras que otras redes pueden definir nodos específicamente enfocados a la validación u otros roles.
3. Métodos de consenso: uno de los componentes más importantes pero también más cambiantes entre *DLTs*, define la manera en la que una red alcanza confianza de que la información que almacena es verdadera. Hay múltiples algoritmos y procesos, con sus

[6] La integración de una criptomoneda es crucial para como incentivo de validación (minería) de transacciones y ejecución de los contratos inteligentes en la red. Sin *Ether* la red sería pequeña, vulnerable y sin aplicaciones útiles.
[7] Hasta la escritura de este documento: marzo de 2018.

respectivas ventajas y desventajas cada uno. El primero en utilizarse en *blockchain* fue *proof-of-work* (descrito anteriormente), pero debido a sus implicaciones negativas (uso excesivo de recursos computacionales), se ha migrado a modelos como:

a. *Proof-of-stake*: una nueva propuesta para la validación de transacciones en criptomonedas. En lugar de resolver un problema matemático complejo, el validador deposita 'monedas' como garantía, después se elige al nodo que más riqueza destinó al proceso de validación. Si la transacción se demuestra fraudulenta, el validador pierde la garantía; de lo contrario, recibe las comisiones por la transacción. Este método requiere menor poder computacional, pero aún está en una etapa temprana.
b. Consenso notariado: el método de consenso más sencillo pero de menor seguridad, ya que consiste simplemente en contar con nodos que están autorizados para validar transacciones. Completamente basado en confianza, por lo que pierde la estructura descentralizada de *blockchain* tradicional.
c. *Raft*: una mezcla entre un modelo notariado y un proceso descentralizado. De manera general, la red elige un líder de validación y la validación se realiza a través de la replicación de *ledgers* a sus seguidores. Los líderes fungen este rol de manera temporal y se realizan elecciones de manera periódica.
d. *Byzantine Fault Tolerance* (BFT): un concepto que integra complejos sistemas de detección, corrección y consenso de información cuando existen actores defectuosos o de intenciones fraudulentas. De manera general, estos algoritmos son capaces de identificar información falsificada siempre y cuando los actores honestos sean más de $3m + 1$, donde *m* indica a los deshonestos. Es decir, si existe un nodo deshonesto, debe haber al menos cuatro honestos. De esta manera, entre más pequeña es la red, más vulnerable es; sin embargo, conforme la red se acerca a infinito, la relación se convierte en aproximadamente un tercio de tolerancia a fallo (por ejemplo, 1000 actores deshonestos son detectables con 3001 nodos honestos).
e. Otros métodos: el diseño de algoritmos y procesos de consenso distribuido aún es un área fértil para innovación, por lo que el ecosistema está encontrando más y mejores métodos que puedan ser usados para *distributed ledgers.*
f. Consenso versátil (e.g. *Corda*): Una red que permite a la aplicación definir qué método de consenso seguirán los nodos que la usen. En otras palabras, el consenso no se define por la red, puede hacerse para cada caso de uso.

El método consenso es de extrema importancia para un *distributed ledger* y las aplicaciones que se monten sobre este. En general, se pueden identificar dos categorías de consenso: centralizados (la validez de las transacciones se deja a nodos de confianza previamente seleccionados) y distribuidos o de desconfianza (la validez de las transacciones se deja a terceros anónimos); esta separación es indispensable de entender para las implicaciones de construir aplicaciones sobre una red u otra, dependiendo de quién determina la validez de las transacciones (nodos de confianza o terceros anónimos). Algunas de las ventajas y desventajas se resumen en la sección de análisis de diferentes tecnologías y sus implicaciones.

Consideraciones generales de los distributed ledgers

Es importante también explorar algunos de los posibles riesgos de usar *distributed ledgers* en el año 2018. Un punto al que se debe prestar atención es la etapa en la que se encuentra la tecnología. *Gartner*, una de las empresas más importantes del mundo de investigación y asesoría en términos de tecnologías emergentes, ha desarrollado y popularizado el ciclo de expectativas de tecnología (*hype cycle*) para medir el momento en el que se encuentra cada una. Este tiene la apariencia y estructura que se muestra en la Figura 1 y sus cinco fases se explican debajo de la misma:

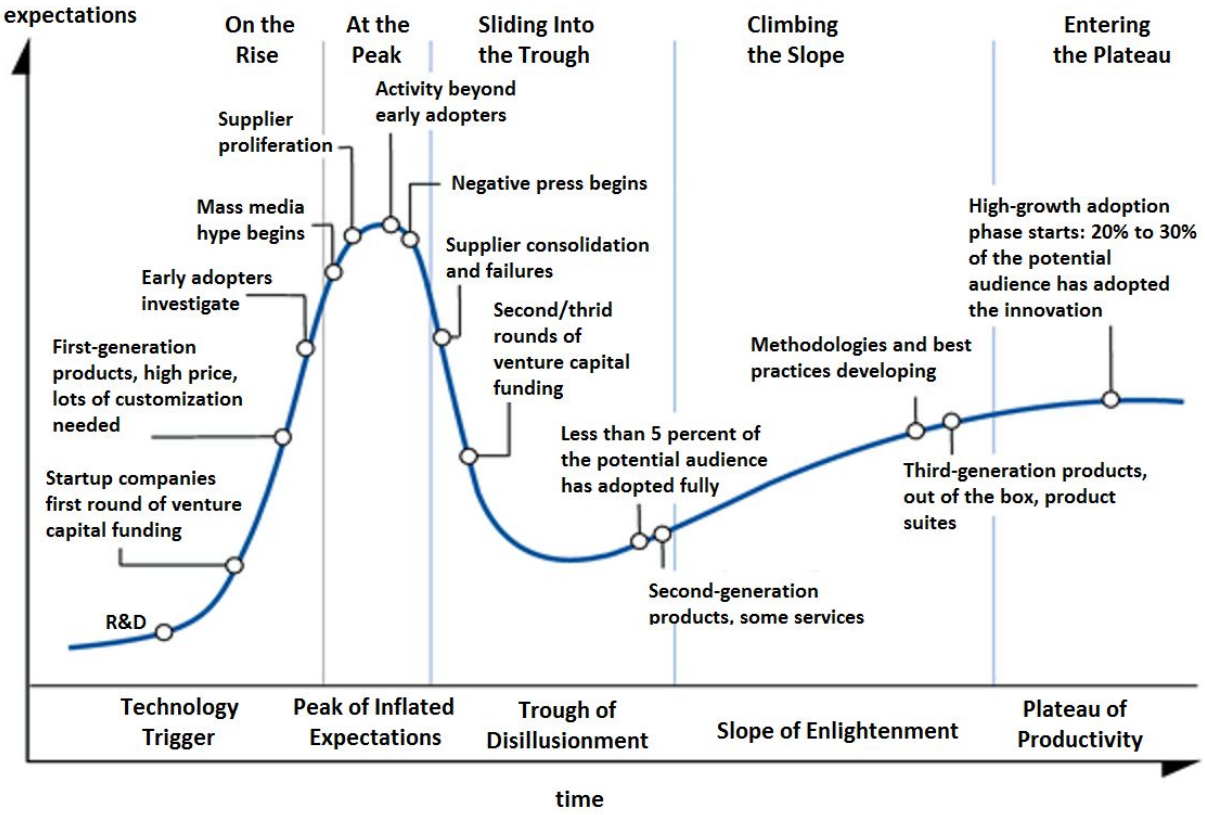

Figura 1. Ciclo de expectativas de la tecnología[8]

1. Nacimiento: la tecnología aparece en un laboratorio, los inversionistas empiezan a inyectar capital y algunos actores de la industria comienzan a enterarse; sin embargo, la tecnología no está lista para uso masivo.
2. Cima de expectativas: los medios masivos detectan la innovación y la sobrevenden, generando un mar de promesas y potenciales inflados que causan que su popularidad se dispare, al igual que las inversiones y la aparición de nuevos actores al ecosistema.
3. Abismo de desilusión: las excesivamente altas expectativas en conjunto con la acumulación de numerosos actores que fracasan en la implementación de la tecnología causan que los medios masivos traten negativamente a la tecnología y se invierten las expectativas de la misma. El público se vuelve escéptico.

[8] Fuente: www.gartner.com

4. Pendiente de iluminación: La tendencia y el entusiasmo generalizado se apagan y sólo algunos actores con objetivos claros y productos viables se mantienen operando. Comienzan nuevas generaciones de la tecnología que resuelven las causas de los fracasos y se logra madurar la tecnología para uso masivo.
5. Meseta de productividad: Por último, la tecnología se integra a la economía y se vuelve parte del día-a-día humano.

A su vez, *Gartner* publica, de manera anual, un análisis de las tecnologías más prometedoras del mundo usando este modelo. El correspondiente al año 2017 se muestra a continuación.

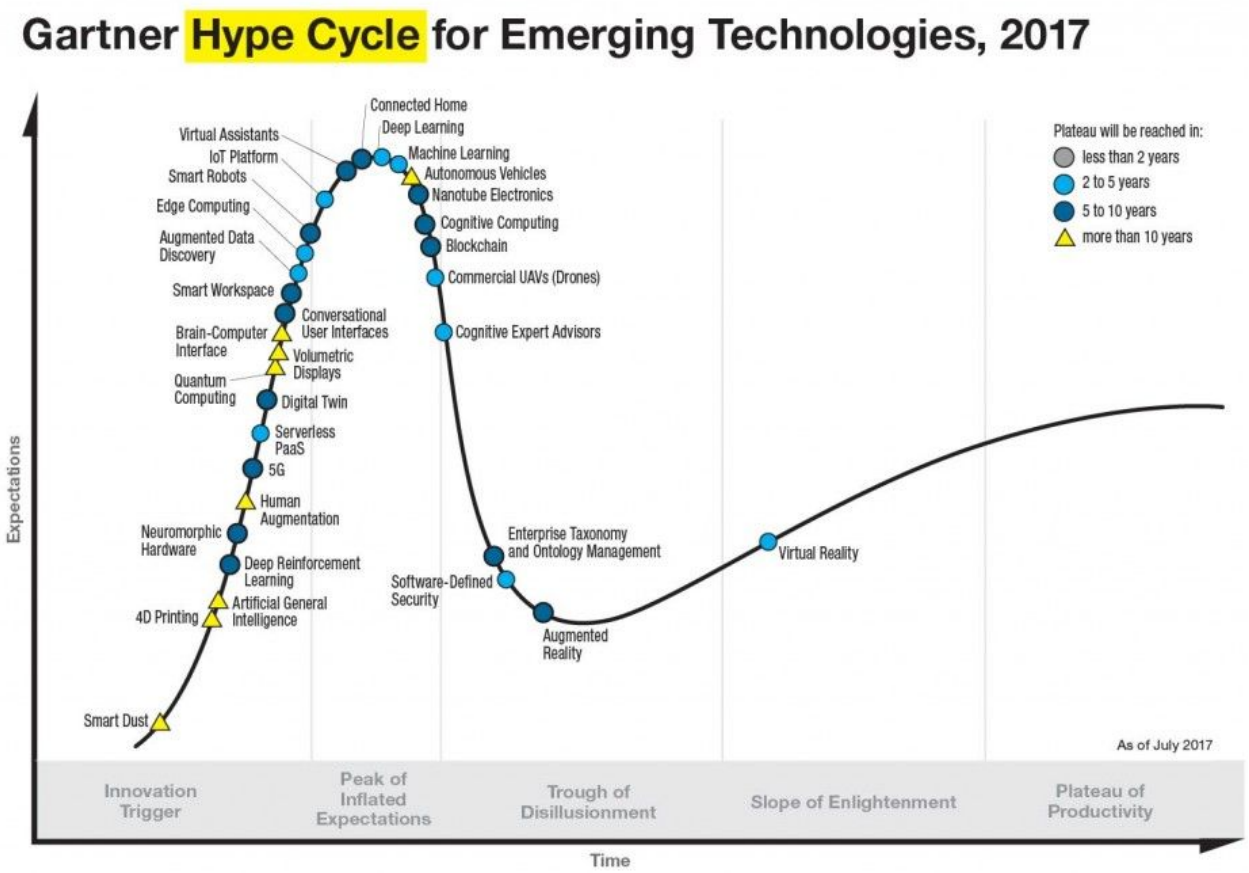

Figura 2. Tendencias para 2017[9]

Como se puede observar en la gráfica, blockchain aún se encuentra en la cima de expectativas y está entrando a la etapa de la desilusión. Es muy claro el por qué, considerando que desde 2015 los medios saturaron al público sobre *bitcoin* y *blockchain* al grado que el simple hecho de agregar estos términos al nombre o descripción de una compañía hacía que su valor en bolsa se disparara[10]. Las criptomonedas se convirtieron en la gran promesa de riqueza, hasta llegar a límites nunca antes pensados; lo que impulsó su crecimiento y expuso sus problemas: rumores de burbujas, fraudes[11] salen a la luz, *bitcoin* se vuelve un problema ambiental, los gobiernos comienzan a prohibir la tecnología, etcétera. En general, la tecnología comienza a recibir mala prensa. Lo que muestra la historia es que el ecosistema de esta tecnología entrará en crisis en este o los próximos años, causado probablemente por el colapso de muchas criptomonedas y empresas (empujando a los inversionistas y al público en general a ser escépticos). Al mismo tiempo, el tema será politizado, la tecnología regulada y el ecosistema perderá un gran número de seguidores, causando una escasez en la oferta de servicios y productos para su desarrollo.

Esto, sin embargo, es un proceso positivo muy común de limpieza del ecosistema por el que pasan la gran mayoría de las tecnologías que causan disrupción. Por ejemplo, se puede usar como analogía la impresión 3D, la cual hace algunos años prometía revolucionar la vida humana; esta tecnología no desapareció, simplemente se enfocó en algunos nichos de mercado y sigue creciendo, pero de manera mucho más conservadora. A su vez, cabe destacar que los *distributed ledgers*, como otras tecnologías, no son completamente inmunes a vulnerabilidades de seguridad: son más difíciles a ser objeto de un ciberataque ya que se tendría que atacar simultáneamente todas los nodos conectados a la red, pero aún hay un potencial de que alguien encuentre una falla o punto débil en sus mecanismos de seguridad.

La exploración de este tipo de tecnologías en el caso de gobiernos (e.g. Estonia, Reino Unido) ha sido con la intención de moldear, supervisar y participar en el diseño y maduración de la

[9] Fuente: www.gartner.com
[10] Fuente: https://qz.com/1175701/putting-bitcoin-or-blockchain-in-a-company-name-is-sometimes-enough-for-a-pop-on-the-stock-market/
[11] Fuente: https://techcrunch.com/2018/01/16/bitconnect-which-has-been-accused-of-running-a-ponzi-scheme-shuts-down/

propia tecnología; así como aprovechar su popularidad para la justificación del uso de los recursos y facilitar el entendimiento ciudadano sobre el tema. En este mismo tenor, es importante notar que este tipo de aplicaciones (en particular las del Reino Unido) han optado por elegir *DLTs* más novedosas que se alinean a sus expectativas y necesidades (e.g. *Corda*) y que tienen menores probabilidades de colapsar una vez se alcance el punto más bajo de la curva de desilusión. Si bien la tecnología ha llegado a los diez años desde su primera introducción (hablando de *bitcoin*), aún es muy pronto para considerarla madura y tampoco existe una sola rama que domine el ecosistema de manera masiva. Debido a la apertura y popularidad de *Ethereum*, es altamente probable que continúe operando por muchos años, pero es imposible determinar su rumbo para los siguientes diez años (debido a su alta democratización). En contraste, tecnologías como *Hyperledger Fabric* o *R3 Corda* tienen inversionistas que respaldan su evolución y crecimiento. Asimismo, siendo estas últimas iniciativas de código abierto, tienen la posibilidad de garantizar su supervivencia, ya sea por una comunidad que las adopte o por las empresas que las utiliza.

Características principales

De manera superficial, los *DLTs* cumplen con las siguientes características:

1. **Inviolable**: al recibir las transacciones en la red, ésta se encargará de replicarla y de generar consenso sobre su validez y su almacenamiento. Una vez almacenados, los registros que se realicen en el *ledger* no pueden ser alterados, modificados o borrados. Esta característica es única, ya que un sistema centralizado tradicional (en un modelo cliente-servidor) no puede ser confiado con esta información; los servidores pueden ser destruidos, o las credenciales de acceso pueden ser robadas y la información alterada por un actor deshonesto.
2. **Seguro**: una bitácora distribuida es casi imposible de atacar de manera exitosa. Cambiar los datos almacenados en la red requiere de un esfuerzo titánico en términos computacionales y humanos[12].
3. **Siempre disponible**: alineado a los dos últimos puntos, al no estar centralizado, el sistema siempre estará disponible para realizar operaciones y transacciones. Asimismo, al ser resistente a ataques, se requeriría derribar la red completa para perder el servicio.

[12] Más información en https://bitcoin.org/bitcoin.pdf y los casos de estudio de Ethereum encontrado en https://github.com/ethereum/yellowpaper y otras tecnologoías.

Aunado a esto, su continua disponibilidad también asegura que la información siempre estará correcta.

4. **Transacciones rastreables**: si bien estas tecnologías son, de manera reduccionista, una base de datos compartida, el modelo de datos gira alrededor de traspasos o movimientos de objetos, por lo que se puede seguir todo su ciclo de vida y, en consecuencia, hacerlo rastreable y trazable.
5. **Confiable y transparente**: finalmente, dada su descentralización, la tecnología distribuye el control, haciendo al sistema neutral y transparente (debido a que comparte los datos entre actores).

Análisis comparativo de tecnologías

Característica	Ethereum	Corda	HyperledgerFabric
Lanzamiento	2015	2017	2017
Comunidad[13]	Grande	Pequeña, pero creciente	Mediana y de rápido crecimiento
Tipo	Blockchain genérico	DLT modular	DLT modular y elástico
Criptomoneda	Ether	No	No (Posible)
Método de consenso	Proof-of-work, por cambiar a proof-of-stake	Versátil: Notariado, Raft y, en el futuro, BFT	Versátil: SOLO, Kafka y, en el futuro, SBFT
Acceso	Público	Privado	Privado
Privacidad entre nodos	No	Sí	Sí
Permisos	Sin permisos	Alta Granularidad	Alta Granularidad

[13] Medido por el número de preguntas en el foro de desarrolladores (ej. StackOverflow), foros corporativos, número de manuales y otros foros de comunidad oficiales de estas tecnologías.

Soporte Empresarial	No	Sí (R3)	Sí (IBM)
Arquitectura	Distribuida	Descentralizada	Descentralizada
Contratos inteligentes	De código público	Código privado	Código privado
Lenguaje de programación	Solidity (nuevo lenguaje, muy limitado)	Java, Kotlin o cualquier lenguaje para la JVM	Go y, en el futuro, Java y Python
Soporte	Comunidad Ethereum	R3	Linux Foundation
Licenciamiento	Open-Source	Open-Source	Open-Source

Código de colores: Verde - fortaleza; Amarillo - riesgo; Rojo - debilidad. Tabla creada para este Reporte.

De manera general, en esta tabla se puede observar: a) *Ethereum* tiene como ventajas principales haber sido pionera de la tecnología y contar con una gran comunidad que mantiene viva la red; b) existen *DLTs* emergentes que cubren necesidades particulares de instituciones. Es importante notar que si bien *Ethereum* ha dominado los medios en los últimos años, en ocasiones no es la mejor tecnología disponible en el mercado[14] para todas las aplicaciones, especialmente hablando de aplicaciones corporativas o institucionales.

Análisis Ethereum

Existen dos formas de hacer el despliegue de una aplicación sobre *Ethereum*: usar la red pública global existente o crear una red propia utilizando el código fuente. Si bien *Ethereum* es pionero en la tecnología (y en hacer contratos inteligentes) y cuenta con una comunidad grande y creciente, hay varias consideraciones a tomar en cuenta, incluyendo:

a. **Actualizaciones**: Un problema que debe de ser considerado son las actualizaciones a la plataforma, ya que, debido a su arquitectura distribuida, la

[14] El mercado ha comenzado a encontrar problemas preocupantes en tecnologías *blockchain* tradicionales como *Ethereum*, por lo que el ecosistema comenzó a responder con mejores tecnologías para mejorar las herramientas disponibles y entregar los resultados esperados.

comunidad de *Ethereum* debe de aceptar de manera 'democrática' (por falta de un mejor término) las nuevas actualizaciones al funcionamiento de la red; esto implica que en algunos casos, estas mejoras o cambios podrían no estar en el mejor interés[15] de las instituciones que utilicen esta plataforma.

b. **Seguridad**: *Solidity* y *Ethereum* en general aún tienen vulnerabilidades de seguridad y potenciales riesgos para su uso; por ejemplo, todo el código de los *smart contracts* es público, por lo que cualquier persona puede activamente buscar e intentar atacar estos sistemas, de la misma manera que sucede con los sitios web en Internet y Javascript.

c. **Costo:** Asegurar el correcto funcionamiento de una red que cumpla las expectativas y estándares puede convertirse en un proceso costoso en el corto y largo plazo. No solamente para crear y mantener una red segura, sino también desarrollar y actualizar contratos inteligentes en *Solidity*, el lenguaje de programación de *Ethereum,* el cual es muy jóven y carece de herramientas básicas, suficiente documentación y robustez con las que otros lenguajes ya cuentan.

   Para las redes *Ethereum* (públicas y privadas) es importante contar un análisis de los potenciales costos operativos y la agilidad de las transacciones realizadas. El costo depende de: a) el valor de *Ether* al momento de uso ya que es volátil, b) tipo de configuración de la red y de la dificultad del tipo de validación que se escojan; c) la eficiencia del código del contrato inteligente; entre otros factores detallados más abajo.

   Para fines de este Reporte, se creó una tabla que contrasta las implicaciones para ambos tipos de red con el fin de generar mayor claridad respecto a cómo operaría un producto similar al descrito, las consideraciones de costos, tiempo necesario para la transacción y su posible impacto en el corto, mediano y largo plazo. Este modelo es sólo un ejercicio guía, ya que para su desarrollo se hicieron una serie de suposiciones del diseño de los contratos inteligentes y de la red en sí (para el caso de la red propia).

[15] Claramente, esto es un punto a favor de clonar la tecnología y crear una red propia. Aunque, es la opinión de esta recomendación que este punto no supera las problemáticas antes descritas.

Consideración	Red pública	Red privada (propia)
Eficiencia de código	De altísima importancia ya que cada operación (línea de código) cuesta dinero por cada ejecución del Contrato Inteligente. Se puede inferir también que entre más compleja e ineficiente es la ejecución del Contrato Inteligente, más costosa hace también todas sus transacciones.	De mediana importancia. Solamente se vuelve problemático si la red tiene alto tráfico, transacciones complejas, múltiples Smart Contracts de diferentes instituciones y la infraestructura no tiene las capacidades para atender la carga.
Costo transaccional	Adicional al costo por cada línea de código, la transacción tiene un costo base y se le pueden agregar montos adicionales basados en la oferta y demanda. Este precio ajusta la probabilidad de que la transacción sea minada de manera más rápida. Asimismo, debido a que *Ether* tiene un valor volátil, la inversión total por transacción nunca será la misma. Este es el costo operativo más alto al usar este tipo de red.	En este tipo de red, puede o no existir un costo por transacción. (Al menos no de manera directa. De forma indirecta, la ejecución de código implica costos por el uso de *hardware*, electricidad y todos los costos operativos y de mantenimiento relacionados.) Asimismo, es importante considerar que el *proof-of-work* es un proceso necesario para *Ethereum* que consume un alto poder de cómputo y por ende el costo de esta infraestructura tecnológica pudiera ser alta.
Costo de mantenimiento (software)	El costo del software depende de la cotización de los diversos proveedores. Se puede establecer que el costo de mantenimiento es más alto que un software tradicional debido al uso de un lenguaje nuevo y tecnología con baja oferta y alta	Si la red no fue personalizada o ajustada (en otras palabras se hace un clon de *Ethereum*), sólo se agrega el costo de mantener actualizado el software de los nodos de la red (así como otros subsistemas de infraestructura); de lo contrario, si fue

	demanda actual. (Tomando en cuenta que *Solidity* no es un lenguaje maduro, y que actualmente hay pocas aplicaciones empresariales e industriales para la tecnología)	personalizada la plataforma, el costo de mantenimiento podría ser más alto aún que en una red pública (dependiendo de los cambios).
Costo de mantenimiento (infraestructura)	Opcional: Puede ser nulo si se decide no tener nodos de validación; de lo contrario, los costos serían más bajos que en una red propia (ya que la red no depende enteramente de ellos), e incluso se podrían generar ingresos por la minería de transacciones de terceros.	El costo de mantenimiento (infraestructura) integra el costo más alto de una red propia. Asegurar escalabilidad, seguridad, disponibilidad y conectividad para una red de alta demanda computacional es un gran reto ingenieril (desde su diseño e implementación, hasta su mantenimiento). Asimismo, esta red nunca podrá proveer los recursos exactos requeridos, siempre tendrá recursos sobrantes o faltantes.

A continuación presentamos algunas otras consideraciones a evaluar en la decisión del uso de una red pública o privada:

Consideración	Red pública	Red privada (propia)
Tiempo necesario para transacción	En general, la producción de bloques dentro de *Ethereum*, es relativamente ágil (aunque más lento que otras *DLT*s), produciendo un bloque cada 17 segundos[16]. La cual varía con base al precio adherido a la transacción, la dificultad de	Estimar esta variable para una red propia es complicado, dependerá de las condiciones de la infraestructura y la configuración de la red.

[16] Fuente: https://etherscan.io/chart/blocktime

	validación, entre otros factores.	
Control de la Red	*Ethereum* es una red distribuida (ver Figura 3: Tipos de redes) que no es dominada por ningún actor, sólo por la comunidad y los nodos que deciden conectarse. Para apagar la red se requeriría que todos los nodos se desconecten lo cual es mitigable si el interés perdura y los nodos se sigan conectando. Esto es de baja probabilidad ya que el uso y adopción de la red sigue aumentando[17]. En el caso de dejar de existir, las aplicaciones que sean montadas en la red podrían seguir siendo utilizadas por el mismo, ya que estos nodos usuarios mantendrán viva la red (terminado, a final de cuentas, con una red dedicada o privada).	Clonar la tecnología y crear una red propia otorga un mayor control de la red, permite su personalización, facilita el monitoreo y la definición de costos con mayor precisión, mitigando la libertad de especulación. Sin embargo existen algunas consideraciones a tomar en cuenta: - Clonar la tecnología y crear una red propia haría más vulnerables a las aplicaciones que se montan sobre ella ya que entre menos nodos, más fácil es dominar la red y actuar de manera deshonesta[18]. - Para temas de percepción ciudadana, es más fuerte el mensaje de confiabilidad si se comunica que es una red pública ya que se evitarían dudas de la legitimidad de las verificaciones de las transacciones.

[17] Un posible indicador del uso de Ethereum es el creciente en el número de meetups alrededor del mundo sobre este tema: http://ethereum.meetup.com

[18] Es importante recordar que *Ethereum* utiliza métodos de consenso basados en *proof-of-work*, los cuales son probabilísticamente seguros cuando la falsificación es más difícil que la validación. Esto solo se logra cuando hay suficientes actores compitiendo por validar las transacciones.

Privacidad	La red *Ethereum*, por diseño, es pública, por lo que incluso aunque se construya una red privada alterna que pocos conozcan, los actores dentro de ella podrán acceder (y filtrar) cualquier información contenida. Para mitigar este riesgo, la red se puede personalizar y configurar para limitar el acceso, generar un sistema de permisos o blindar la información a través de procesos de encriptación; sin embargo, esto le resta al argumento de elegir *Ethereum* como una solución lista para usarse[19]. De aquí la importancia de analizar otras tecnologías como *Hyperledger Fabric* y *R3 Corda* para asegurar que la opción de tecnología selecta responda a las necesidades del proyecto.
Criptomonedas	El uso de criptomonedas en una red con consenso basado en *proof-of-work* o *proof-of-stake* representa el principal mecanismo de seguridad y las ventajas del uso tradicional de *blockchain*[20]. Sin embargo la moneda (Ether) es muy volátil (financieramente hablando) y su uso pudiera implicar para los gobiernos consideraciones legales, administrativas y de entendimiento por parte del ciudadano. Si no se utilizan las criptomonedas, es necesario utilizar otro método de consenso, de preferencia uno notariado, en el cual existen nodos de confianza que tienen atribuciones para realizar estas acciones.

[19] Por ejemplo, un sistema de permisos de nodos en *Ethereum* como el que propone *Fabric* o *Corda*, implicaría editar el código fuente; lo cual va mucho más allá de un *smart contract* o una *DApp*.
[20] Sin una criptomoneda, no hay beneficios tangibles para quienes validen transacciones, por lo que la red no crecerá más allá de los nodos que decidan hacerlo de manera voluntaria. Lo cual lleva de nuevo al problema de una red pequeña que es vulnerable a ataques de actores deshonestos.

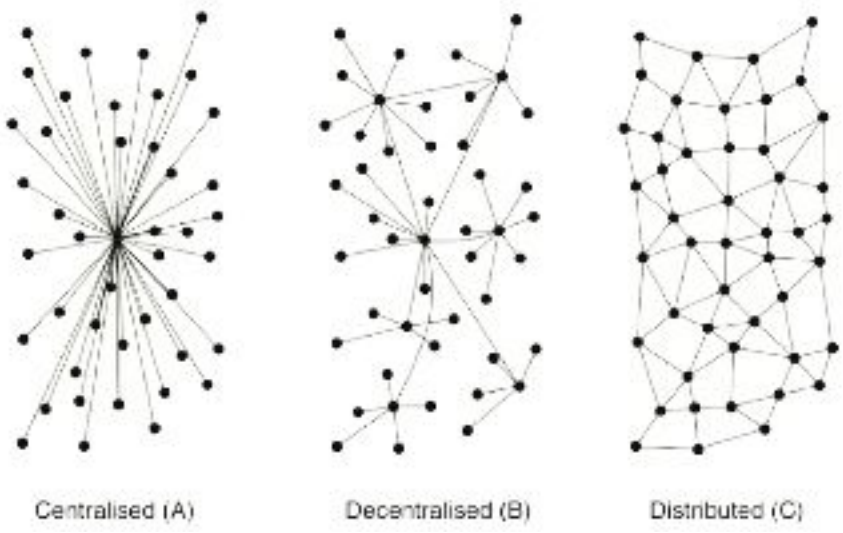

Figura 3. Tipos de redes[21]

Análisis de *Hyperledger Fabric* y *Corda*

Consideración	***Hyperledger Fabric***	***Corda***
Eficiencia de código	Dado que ambas tecnologías permiten métodos de consenso distintos a proof-of-work y proof-of-stake, la ejecución del código del contrato inteligente no necesariamente está unido a una criptomoneda. Por ello, especialmente en un modelo de validación notariada, la eficiencia de código es de menor importancia que en *Ethereum*.	
Costo	Los costos se pueden dividir en tres partes: 1. Desarrollo: este proceso será considerablemente más accesible frente a *Ethereum* al permitir el uso de lenguajes de programación existentes y muy populares. 2. Operación: los costos de realizar una transacción en este tipo de *DLTs* serán muy accesibles y podrían ser incluso gratuitos usando un método de consenso descentralizado, en lugar de uno distribuido (como	

[21] *Diffused Art and Diffracted Objecthood: Painting in the Distributed Field - Scientific Figure on ResearchGate*. Disponible en: https://www.researchgate.net/Centralized-decentralized-and-distributed-network-models-by-Paul-Baran-1964-part-of-a_fig1_260480880

	Ethereum). 3. Infraestructura: la complejidad de operaciones disminuye de manera importante al usar métodos de consenso distintos al proof-of-work, por lo que los requerimientos computacionales son mucho más bajos, y la red puede incluso ser de menor tamaño.	
Tiempos	Al igual que los parámetros anteriores, el tiempo necesario para completar una transacción en este tipo de *DLTs* será dependiente del tipo de consenso utilizado y la complejidad de las operaciones de validación o de ejecución de la transacción. Sin embargo, en definitiva serán mucho más ágiles que en *Ethereum*; al no utilizar proof-of-work, el tiempo de ejecución será muy similar al de una transacción tradicional hecha en el Internet con una arquitectura centralizada.	
Privacidad	*Hyperledger Fabric* crea 'canales' al realizar operaciones entre 2 o más actores; esto permite que, de manera automática, las transacciones puedan ser privadas.	*Corda*, por diseño, es una red semi-privada de nodos que se asumen no confiables. Por ello, todas las operaciones realizadas a través de un contrato inteligente, pueden ocultarse y sólo aquellos que participan visualizarlas.
Control	La arquitectura de la red está pensada enteramente para uso empresarial, por lo que las funcionalidades atenderán a los clientes y usuarios de *Hyperledger Fabric*. Asimismo, el sistema de canales permite tener control absoluto sobre las transacciones o incluso sobre la forma que en se ejecuta el código en ellas. Por último, su apertura total de código fuente permite incluso hacer redes propias del sistema y controlar cualquier parte de la red.	Originalmente creado para el sector financiero, *Corda* fue igualmente diseñado para proveer una solución a empresas y gobiernos, proveyendo alta flexibilidad y control sobre el uso de información y la ejecución de los contratos inteligentes. De igual manera que *Fabric*, este *DLT* es de código abierto por lo que cualquier adecuación, mejora o clon es posible de manera privada y controlada.

Verificación de las transacciones	Desde un punto de vista técnico, esta es una de la mayores fortalezas de *Fabric* y *Corda*. La validación no está limitada a un algoritmo de consenso en particular y, en algunos casos, se puede dejar al contrato inteligente elegir que tipo de método usar (incluso si no es el usado por otros nodos). Esto hace la validación mucho más ágil, económica (computacional y financieramente), versátil y robusta.

Ventajas de las tecnologías nuevas: Las tecnologías más nuevas están resolviendo los problemas y limitaciones de Ethereum como pionera. Los esfuerzos nuevos están soportados por una comunidad de rápido crecimiento, y también por compañías e instituciones de gran renombre: por ejemplo, *Hyperledger Fabric* está apoyado por la *Linux Foundation* e *IBM*; mientras que *Corda* está siendo desarrollado por *R3*, una empresa con más de 107 millones de dólares en inversión[22] que trabaja de cerca con el Gobierno Británico[23] para integrar su tecnología a los intereses del sector público y privado. Estos esfuerzos están diseñados para ser una solución corporativa e institucional que resuelva temas sensibles que *Ethereum* tal vez no atenderá[24], como: privacidad de operaciones, sistemas de permisos, métodos de consenso descentralizados, lenguajes de programación que son estándar de la industria o proveer un soporte personalizado más allá de ser solo una solución de código abierto.

Cada una de las tecnologías ofrece oportunidades y retos a considerar y la velocidad de evolución de estas herramientas va con tal velocidad que éste análisis debe de hacerse con información actualizada a la fecha de la toma de decisiones.

[22] Fuente: https://www.crunchbase.com/organization/r3-cev
[23] Fuente: https://uk.reuters.com/article/us-r3-fca/r3-uk-regulator-and-banks-team-up-on-blockchain-based-mortgage-reporting-idUKKCN1BN0QX
[24] Con base en su naturaleza abierta actual y su visión como un producto democrático e independiente de intereses corporativos y gubernamentales.