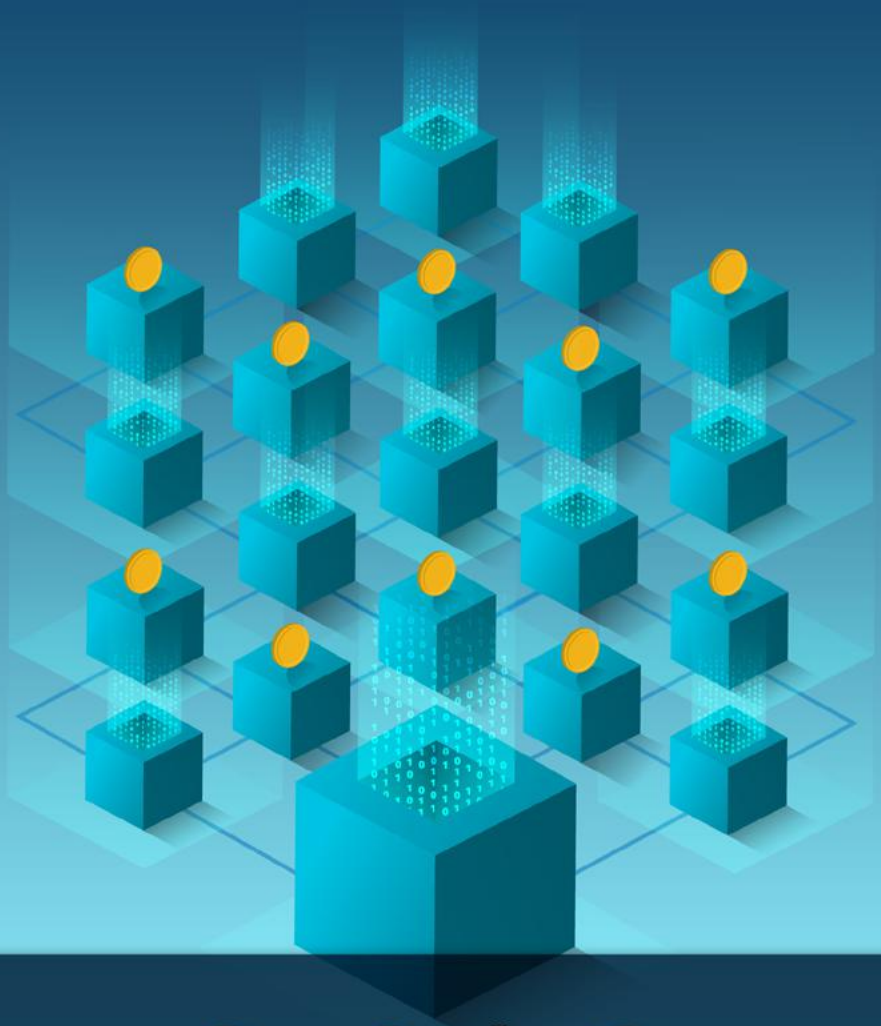


Capítulo 3: ¿Cómo funciona Blockchain?

CertiProf®

Professional Knowledge

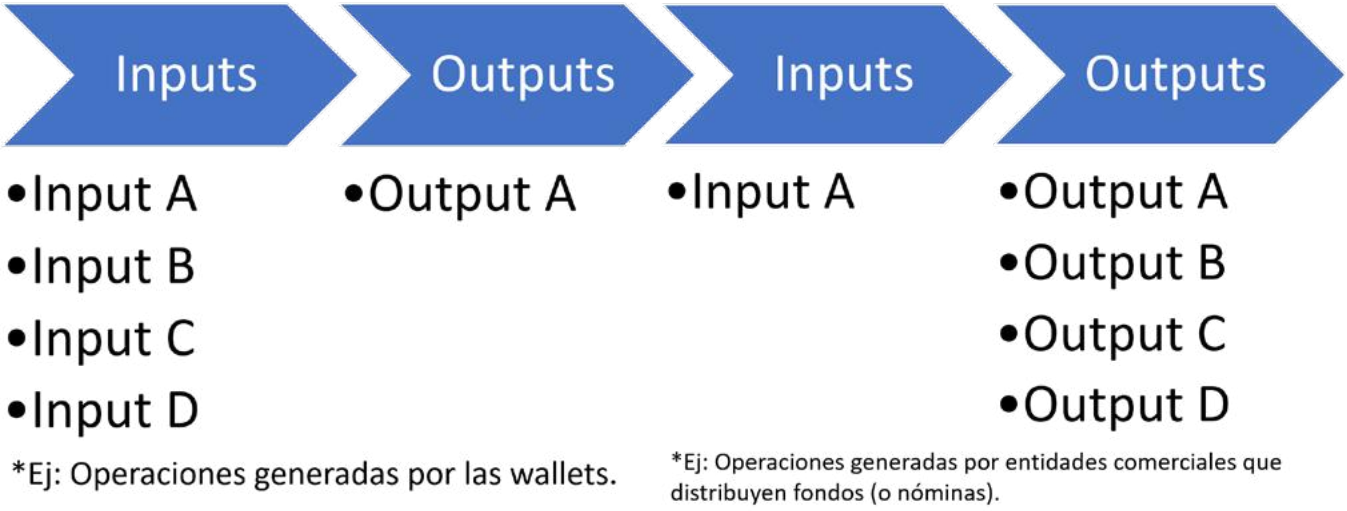
www.certiprof.com

¿Cómo funciona Blockchain?

Transacciones y Bloques en Blockchain

Mediante la dirección (address) es que se recolectan los beneficiarios de cada cantidad transaccionada (se basa en la clave pública, pero registra la dirección en vez de éstas). Una vez se procede con la transacción, es esencialmente la transferencia autorizada del propietario hacia otro propietario para que éste último le dé uso bajo su propiedad, creando así una transacción adicional en una "cadena de propiedad". Así pues, los elementos dentro de las transacciones son inputs y outputs (débitos y créditos), siendo que los outputs suman ligeramente menos de lo que los inputs suman en total debido a que hay una cuota de transacción implicada en la operación. Finalmente, los nodos son los responsables por procesar estas transacciones y así se mantienen dentro de estos los registros de propiedad previamente mencionados.

El flujo de transacciones funciona de la siguiente manera: Existe uno o más inputs, por cada input hay uno o más outputs (aunque también puede haber muchos inputs para un solo output), y estos outputs a su vez representarán una transacción subsecuente dentro de la cadena de propiedad.



Cabe resaltar que la primera transacción entre Satoshi y Hal Finney no contaba con un input, pero desde ahí empezó este flujo mencionado.

Figura 12. Tipos básicos de flujos transaccionales. Información adaptada de University of Nicosia (2018).

Tipos de Bloques

Existen diferentes tipos de bloques, pero independientemente de su tipo, todos los bloques se componen de 1) un block header y 2) una o más transacciones dentro del bloque.

Bloque génesis	Bloque huérfano	Bloques duros (stale)	Bloques umer
• Es el primer bloque creado dentro de una red Blockchain	• Bloques validados, comúnmente referidos en Bitcoin. Ocurren cuando dos bloques se crean al mismo tiempo pero uno se escoge por encima de otro por problemas de latencia, esto lleva a una bifurcación en Blockchain	• Son bloques que se tornaron en duros (stale) o viejos porque un minero tuvo éxito minando el bloque mientras otros mineros trabajaban en sus propias versiones de bloques similares	• Bloques validados, comúnmente referidos en Ethereum. Son rechazados en la red debido a la formación de otra larga bifurcación, pero aquí existe una recompensa para el minero (inferior a la de un bloque normal) a diferencia de los huérfanos.

Mohanty, D. (2019). R3 Corda for Architects and Developers - With Case Studies in Finance, Insurance, Healthcare, Travel, Telecom, and Agriculture. https://doi.org/10.1007/978-1-4842-4529-3

Figura 13. Tipos de bloques en una blockchain. Información adaptada de (Mohanty, 2019).

Encabezado del Bloque

El encabezado del bloque (block header) es un compendio de información que caracteriza a cada bloque dentro de una red Blockchain, la cual sigue una lógica. Estos elementos y sus detalles son los de la tabla 2 y su funcionamiento dentro de la red es como se ilustra en la figura 14, adaptadas ambas de Murray, M. (2019). La red parte desde un bloque génesis y desde ese punto, todo bloque posterior contará con el ID del bloque anterior.

Campo	Descripción
Versión de software	Denota las reglas de validación utilizadas en esta versión del software blockchain
Estampa de tiempo	Hora de creación del bloque (segundos desde la época de Unix)
ID del bloque anterior	Hash del encabezado del bloque del bloque anterior
Raíz de Merkle	Identificador de resumen único derivado de los hash de todas las transacciones incluidas en el bloque
Objetivo de dificultad	El nivel objetivo de dificultad del desafío matemático del mecanismo de consenso: en Bitcoin, este nivel se relaciona con la cantidad de ceros a la izquierda que el hash del encabezado del bloque debe incluir
Nonce	Valor numérico que resuelve el desafío matemático

Tabla 2. Metadata en los encabezados de bloques. Información adaptada de (Murray, 2019).

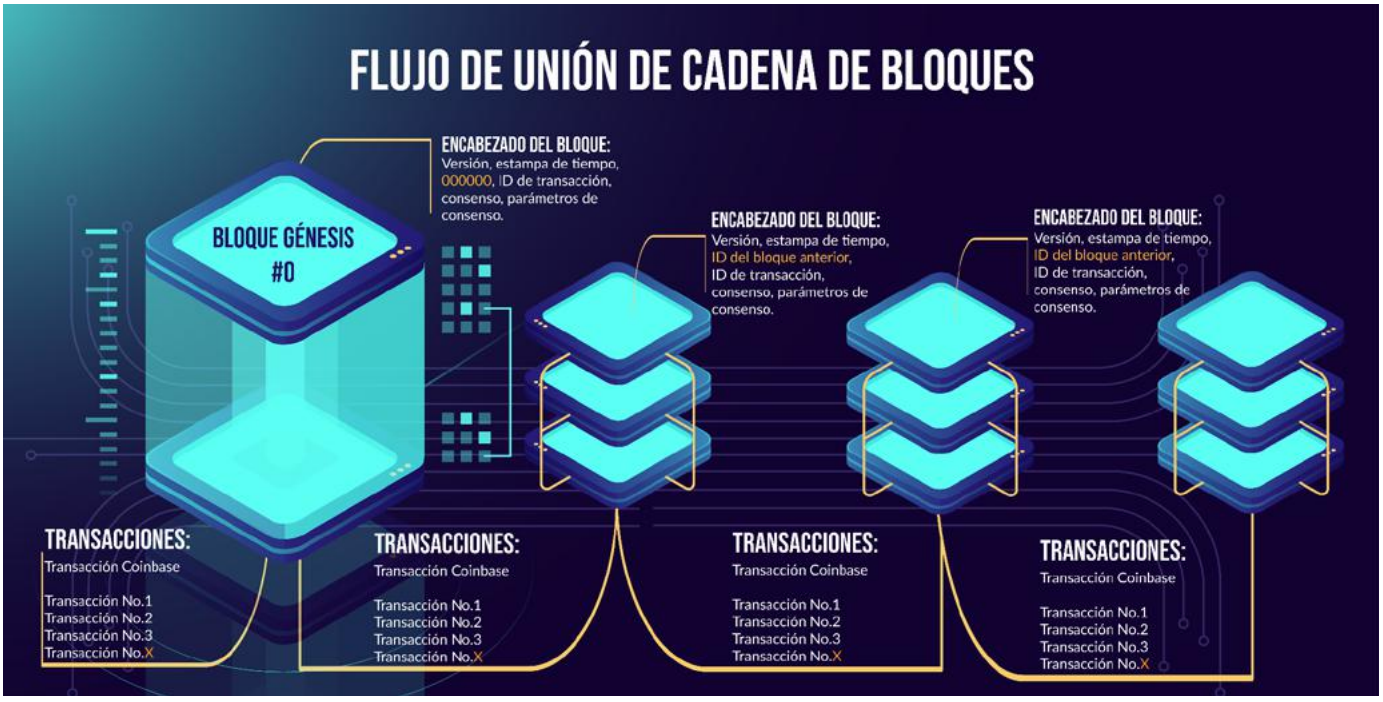


Figura 14. Flujo de unión de cadena de bloques. Información adaptada de (Murray, 2019).

Árbol de Merkle

Los árboles de Merkle son en esencia árboles binarios que cada vez se desglosan en más y más hojas donde está al fondo la data subyacente, un conjunto de nodos intermediarios que son el hash de sus hijos, y en la cabecera del árbol un nodo único que se forma del hash de sus dos hijos (Ethereum, 2021). Este tiene como función que cada bloque obtenga la data que le corresponde de manera correcta y relevante de la forma en que los flujos de información ocurren como ya se ha abordado. Asimismo, este árbol funciona porque los hashes se propagan hacia arriba y esto causa que en últimas un bloque afectado (el cual será de la parte inferior) termine por alterar su hash y se le terminaría reconociendo como un bloque totalmente diferente al original y así invalidando el consenso PoW para ese bloque.

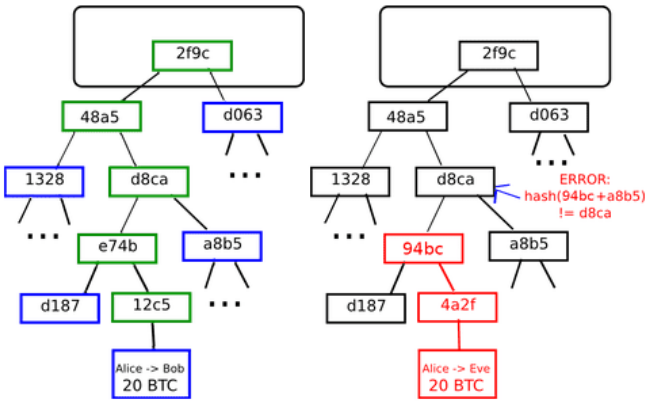


Figura 15. Árboles de Merkle. Obtenido de (Ethereum, 2021).

Cómo se Soluciona el Problema del Doble Gasto

El problema del doble gasto se origina a raíz de que en el mundo digital como las operaciones requieren de una confirmación de transacción, si dos operaciones a dos propietarios diferentes fueron realizadas por el mismo valor y su sumatoria excede la cantidad base que puede transaccionar el propietario que emite las transacciones, habiendo ocurrido estas a tiempos similares, entonces podríamos hablar de un doble gasto que cuenta las transacciones como independientes. No obstante, su prevención se aborda mediante el seguimiento meticuloso de cada transacción y asignando una cantidad finita del criptoactivo a transaccionar para la red cuando se crea un nodo génesis, siendo que los mineros siempre están evaluando cuidadosamente el abasto dentro de la red cada vez que se agrega un nuevo bloque y así evitando el doble gasto. (Mohanty, 2019).

Hash de Blockchain

El Hash es la función que se utiliza dentro de Blockchain para verificar la integridad de la data mediante la transformación de data idéntica en un código único, representativo y con un tamaño ajustado, implicando esto que toda alteración a la data original se traduce en un cambio inmediato al Hash. Se cuentan con distintos estándares de algoritmos de hashing como lo son HA-1, SHA-2, SHA-256, entre otros (Mohanty, 2019). Independientemente de cuántas veces o cuál sea el intervalo de tiempo para el input del Hash, el output siempre será el mismo, así como su extensión. Esto es utilizado comúnmente con el manejo de las contraseñas, pero a nivel de Blockchain es usado para calcular valores Hash de la data y así obtener un Hash de Hashes que se almacenaría en la cabecilla de cada bloque como se vio con anterioridad. Los valores Hash de los bloques de una red son similares a la de sus bloques antecesores, así uniendo la red con una lógica compleja que impide intromisiones no deseadas por atacantes externos (Mohanty, 2019). En la ilustración 3 se puede apreciar cómo luce un Hash, mediante la ejemplificación de la palabra "Bitcoin" pues ésta genera la producción de uno de SHA-256 (uno que se presenta comúnmente como un texto de 64 caracteres hexadecimales).

Ilustración 3. Hash de Bitcoin.

```
# sha256sum
Bitcoin
b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4
```

Llaves Públicas y Privadas

Cuando se hablan de las llaves/claves, hay dos, las cuales son la pública (visible por todos) y la privada (todo miembro de la red de Blockchain la tiene, y no debe ser compartida, como la contraseña bancaria). De la privada a la pública hay una transformación matemática mediante derivación y posteriormente una función de Hash que permite que se genere la dirección (address) que servirá para las transacciones como ya hemos visto. La figura 16 representa este flujo, y no es lograble con facilidad volver matemáticamente de una llave pública hacia una privada porque el algoritmo utilizado hace que sea fácil el proceso de pasar de la privada a la pública, pero muy complejo regresar de la pública a la privada por parte de un tercero.

Figura 16. Flujo de transformación de las llaves en una red Blockchain. Información adaptada de Mohanty (2019).

Asimismo, la figura 17 ilustra que cuando a un propietario le llega la llave pública de otro propietario, entonces su tarea es desencriptar el mensaje (ciphertext es como se denomina en inglés al concepto de mensaje encriptado) utilizando su propia llave privada para obtener el mensaje (plaintext se denomina en inglés a este resultado). Si un mensaje se encripta con llave pública, entonces una privada lo desencripta, y viceversa, encriptar un mensaje con llave privada se desencripta con una pública.

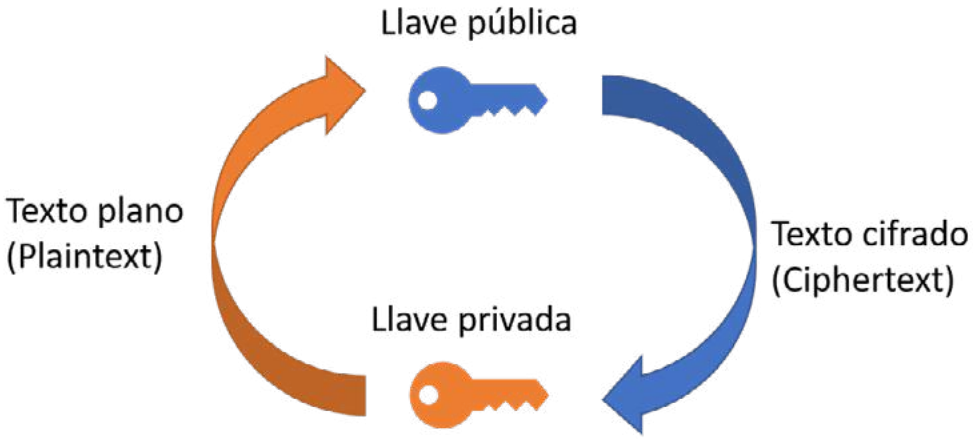


Figura 17. Flujo de encriptación/desencriptación de las llaves en una red Blockchain. Información adaptada de University of Nicosia (2018).

Consenso

Los algoritmos de consenso son el medio por el cual se logra la transparencia o un sistema libre de errores. Como se verá posteriormente, así es como se logran diferentes tipos de validaciones transaccionales. Por este mecanismo es que Blockchain es un repositorio universal, permanente, continuo, auditable públicamente, redundante y de mantenimiento de registros impulsado por el consenso (Guerra, 2020). Es necesario que los nodos cuenten con la misma data y así no se pueda transmitir ni publicar alguna falsificación de datos, por ello es que el consenso toma tanta relevancia y así se define este como todo proceso que un nodo realiza dentro de un sistema distribuido para llegar a ese acuerdo del único valor de datos aceptable dentro de la red (Fischer, 1983).

Capítulo 4:
Tipos de Consensos y Blockchain

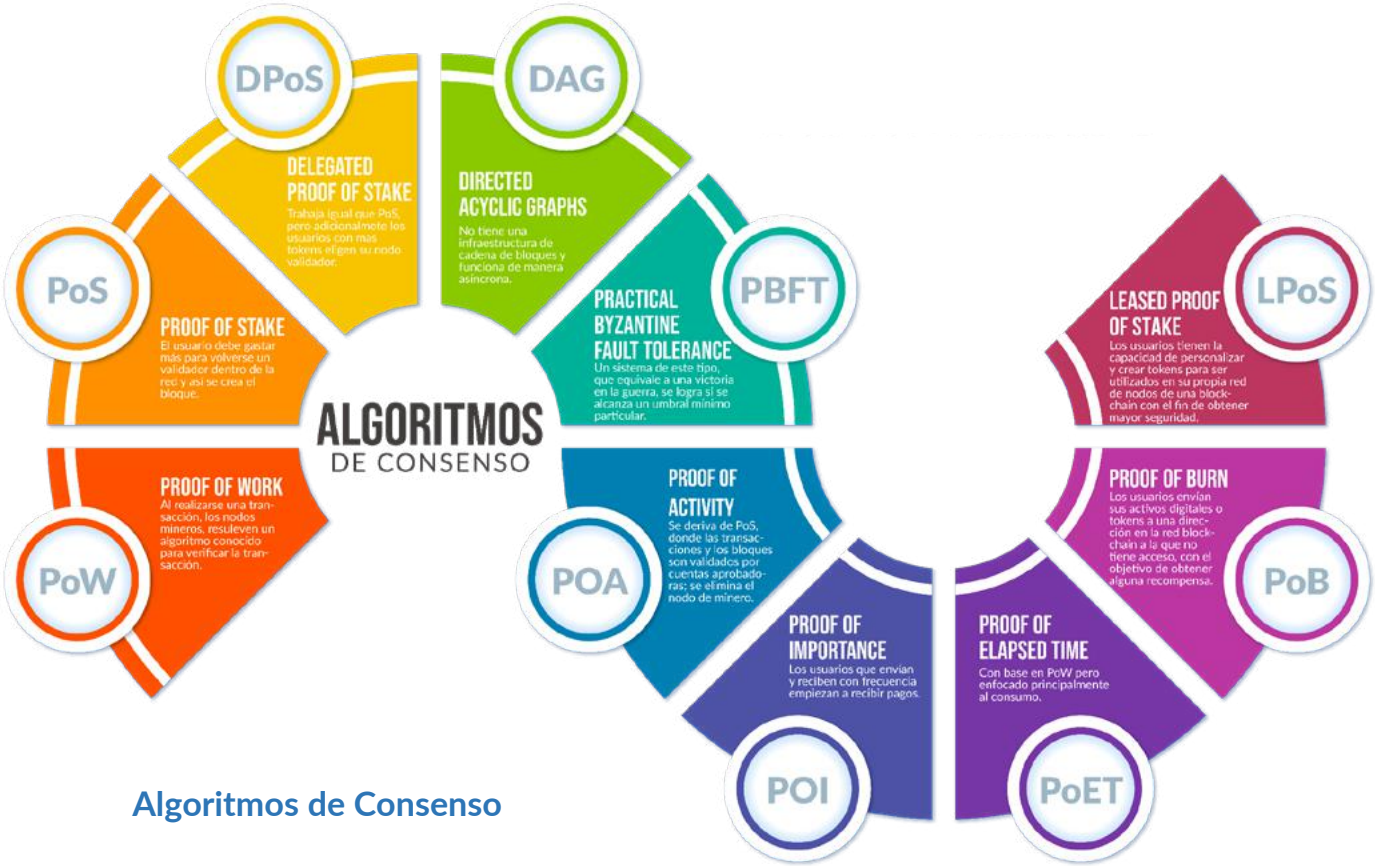
CertiProf®
Professional Knowledge

www.certiprof.com

Tipos de Consensos

Marcos de Confianza y Mecanismos de Consenso

Es normal que en los sistemas donde se utiliza Blockchain exista multiplicidad de entidades participando dentro de la red, y como existe esta multiplicidad pues también ha de existir un consenso para aceptar nuevos bloques dentro de la misma. Los consensos son entonces reglas para que las máquinas trabajen conjuntamente a pesar de que algunas puedan proveer información indeseada, y por ello surge la tolerancia de falla (fault-tolerance) y resiliencia (resilience) dentro de los mecanismos de consenso para crear y aceptar un nuevo bloque.



Algoritmos de Consenso

Figura 18. Algoritmos de consenso. Información adaptada de (Anwaron, 2018).

Consenso de Pruebas de Trabajo – Proof of Work

En el whitepaper de Nakamoto (2008) se propuso el proof-of-work (PoW), el cual hoy día lo conocemos como un sinónimo de minería y tiene -entre sus múltiples cuestiones- aspectos de especial interés para los criptoactivos. Esto incentivaba la participación de los nodos en verificar transacciones y resolver el problema del general bizantino, mientras el gasto de hardware y electricidad superara el de concesión de BTC (las recompensas). Por otro lado, esto implicaba encontrar un nonce cuyo nivel de dificultad varía dependiendo la cantidad de ceros a la izquierda, los cuales implicarán en mayor o menor medida iteraciones para poder encontrar un hash válido y es así como se efectúa el sistema de competencia y recompensa. Este nonce en últimas sirve para verificación y validación de la legitimidad, aunque entre los mayores problemas que tiene este método que incluye la minería es el exceso de recursos que se ha de utilizar (consumo energético).

Consenso - Proof of Stake

Ahora bien, el consenso proof-of-stake (PoS) desconoce de la minería, pero mantiene la validación y la añadidura de bloques a la red. En contraposición al anterior, este se orienta a la participación económica del validador dentro del Blockchain, lo que significa que por pertenencia a la red hay una implicación económica. En el caso de las Blockchain públicas, los validadores se reúnen para dar unas propuestas sobre los siguientes bloques a añadir (Mohanty, 2019), y cada propuesta va ponderada con la participación económica de los validadores, similar a como Google hace las calificaciones de calidad para los Ads donde la participación económica tiene peso, pero en el caso de este consenso la participación económica es el único criterio. Entonces bien, el poder recae en la cantidad de propiedad de criptoactivos del propietario bajo este consenso y su gran beneficio para los que pertenecen a la red es que hay menos riesgo de un ataque externo (Frankenfield, 2019). Este modelo es utilizado Casper de Ethereum y reduce inmensamente el consumo excesivo de recursos energéticos.

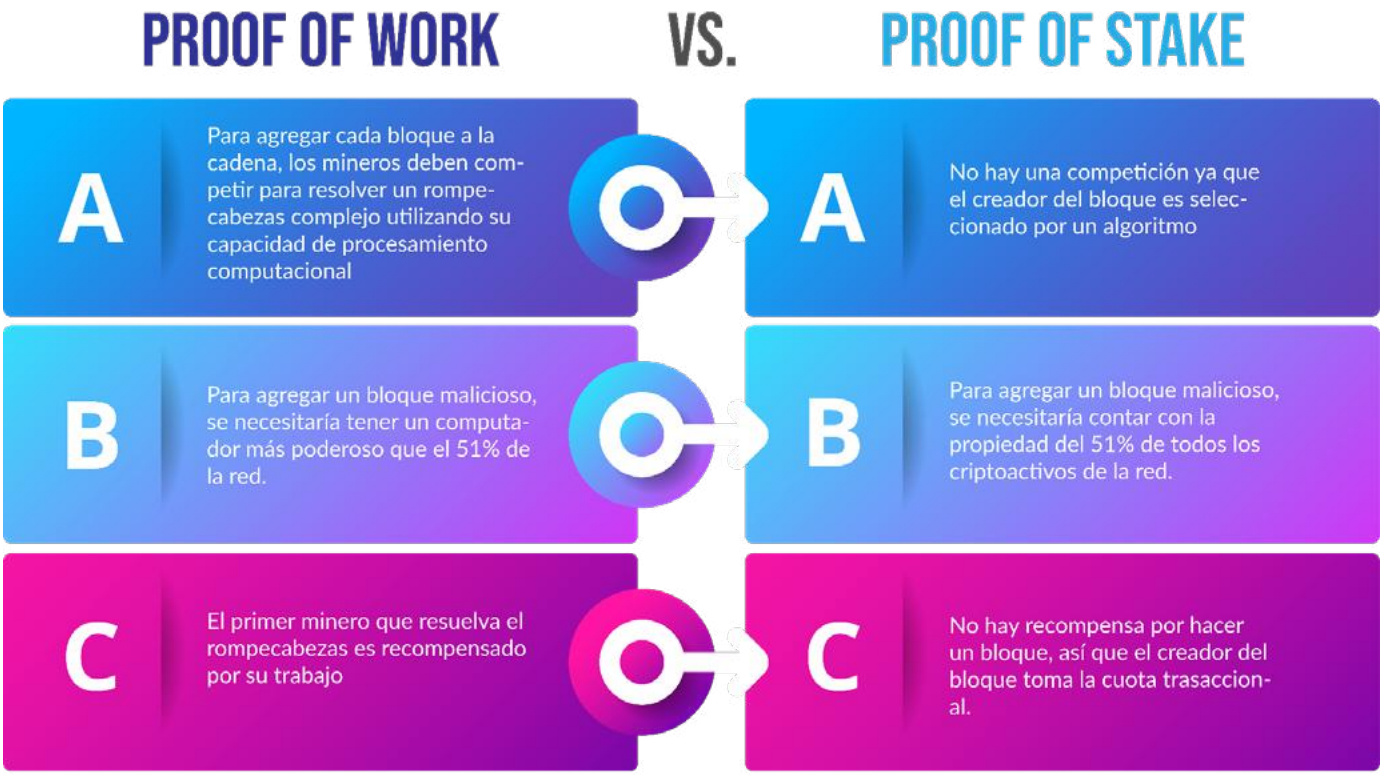


Figura 19. Comparativa simple de las características más relevantes entre los consensos más utilizados. Información adaptada de (Rosic, s.f.).

Fork de Blockchain

Las bifurcaciones (fork) en Blockchain son separaciones y tiene ocurrencia cuando el software de diferentes mineros se torna desalineado (CMC Markets, s.f.). Esto termina por poner una encrucijada y es decidir con cuál versión del Blockchain continuar ya que estos funcionan al introducir cambios el protocolo activo en el Blockchain. Entonces bien, es el consenso el que se asegura que la mayoría de los nodos terminen por rechazar las bifurcaciones, y este tipo de situaciones donde las bifurcaciones no intencionadas ocurren es más usual en los que emplean el consenso PoW, mientras que en el PoS no se ven para nada pues hay un creador único de bloques (Murray, 2019). Existen dos tipos de bifurcaciones, las que son suaves (soft fork) y las duras (hard forks), las cuales se representan en la siguiente figura.

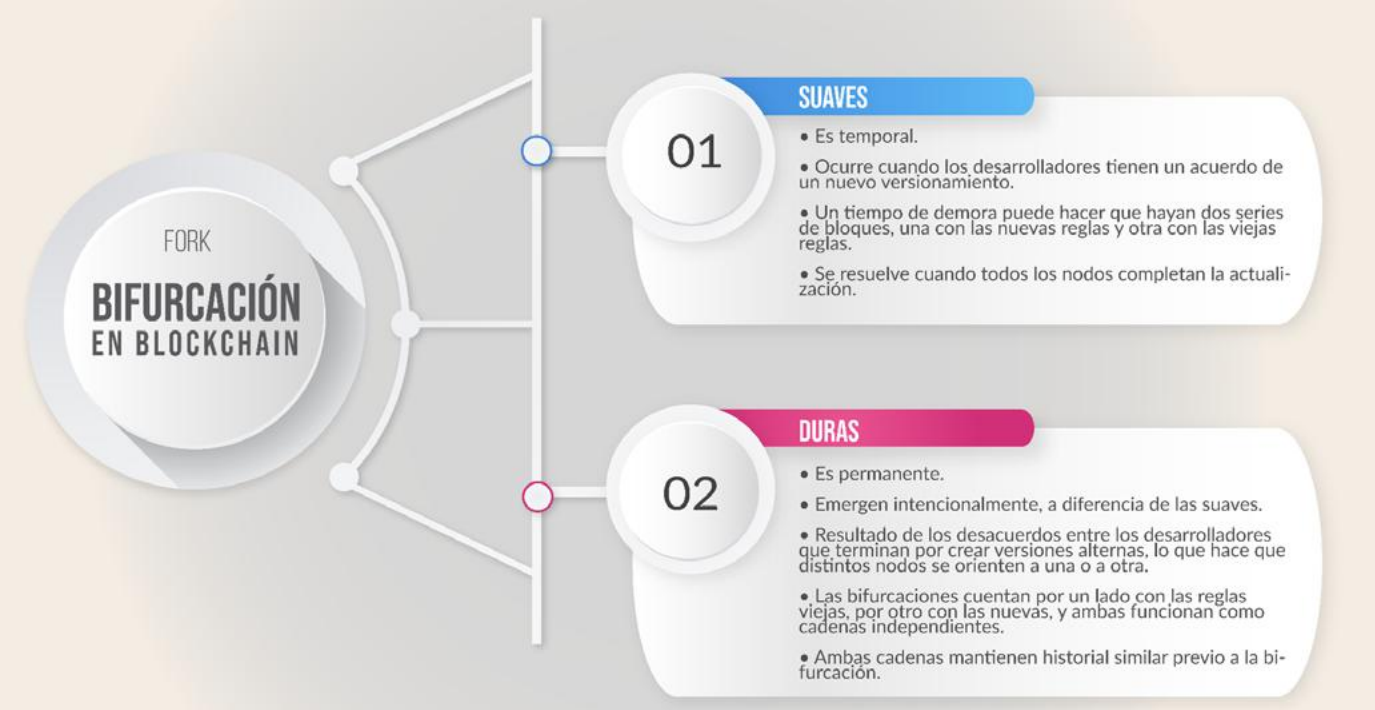


Figura 20. Tipos de bifurcaciones en Blockchain. Información adaptada de (CMC Markets, s.f.; Murray, 2019).

Tipos de Blockchain

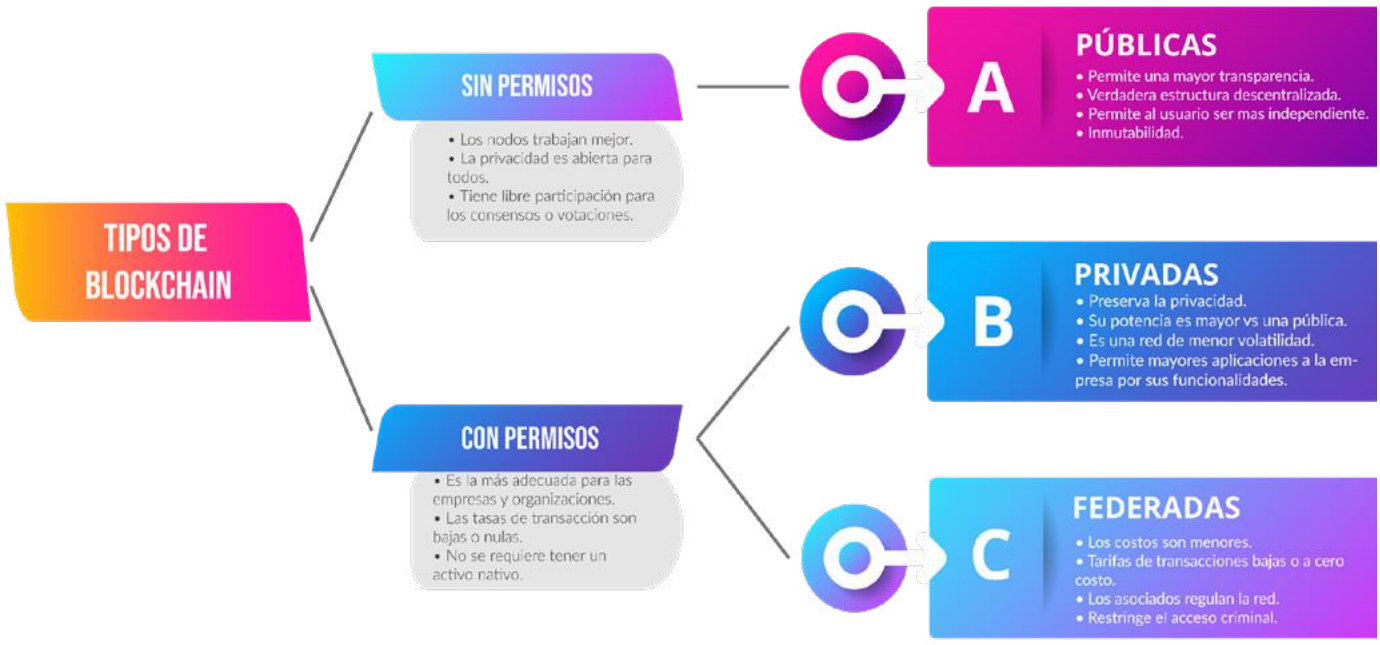


Figura 21. Tipos de Blockchain - Permisionadas (privadas, federadas) y no permisionadas (públicas).

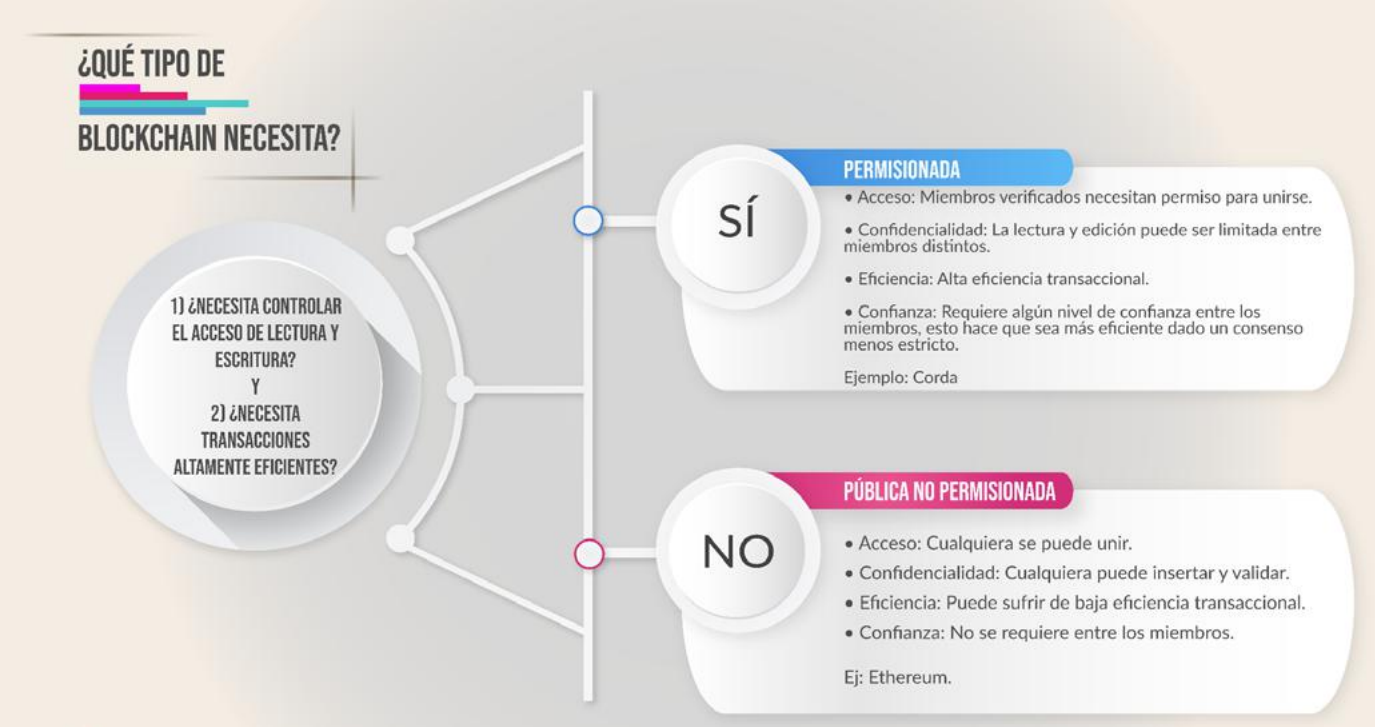


Figura 22. ¿Qué tipo de Blockchain necesita? Información adaptada de (Aseev, 2020).

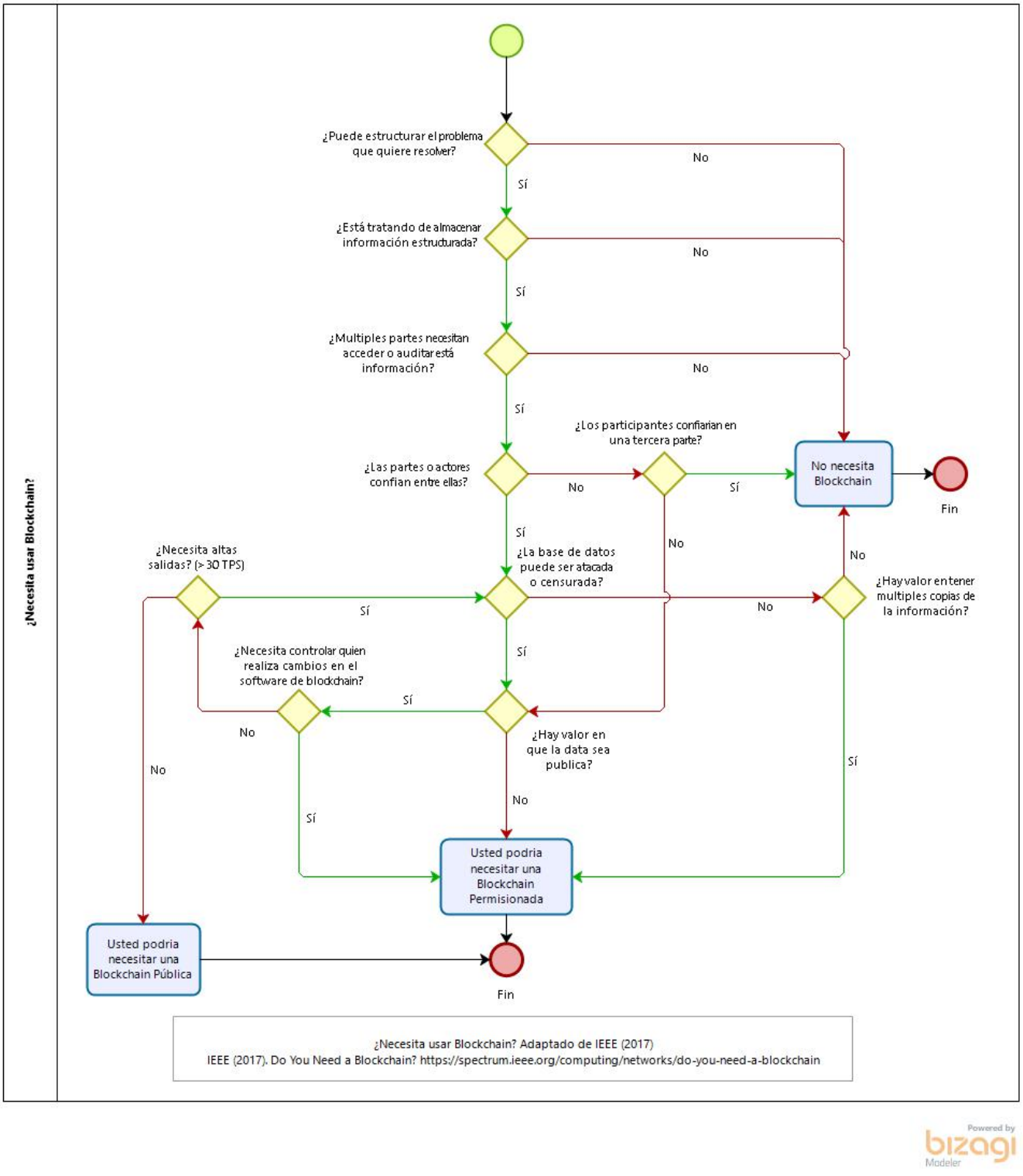


Figura 23. ¿Necesita usar Blockchain? Adaptado de (IEEE, 2017).

Figura 24. Construyendo tu propio proyecto Blockchain. Información adaptada de (Aseev, 2020).

Figura 25. Cómo seleccionar el protocolo. Información adaptada de (Aseev, 2020).

Consorcios y Blockchains Federadas

Los consorcios en Blockchain son parcialmente privados donde nodos seleccionados son predeterminados, y por ello el acceso de lectura es posible que lo tengan todos los participantes de la red, pero el de escritura solo unos seleccionados. Asimismo, no es totalmente descentralizado como las Blockchains públicas y como las privadas, son rápidas, eficientes y segura, principios seguidos por Quorum, R3 Corda, o Hyperledger Fabric (Mohanty, 2019).

Blockchains Hibridas

Si bien existen Blockchains públicas o privadas, también está la existencia de las híbridas porque hay casos de uso que no pueden solventarse con una de las dos por sí mismas. Dentro de la diversidad de aproximaciones que pueda haber hacia las Blockchains híbridas, en su mayoría se tiene una pública donde cualquiera puede unirse y participar en la transacción, pero también pueden ser privadas asociadas con una pública donde un conjunto centralizado bien conocido es invitado (Mohanty, 2019).

Aquí es común que existan diferentes mecanismos de consenso, y por ejemplo, si se tienen PoW y PoS, entonces los mineros del PoW aún seguirán en la creación de los bloques con transacciones válidas, pero solo los que son seleccionados del PoS desde una red privada podrán ejercer el voto para la agregación del bloque y así todos dentro de la red cuenten con acceso a éste ya que esto elimina la falencia del riesgo del ataque por el 51% de propiedad (Mohanty, 2019).

Protocolos Blockchain y DLTs Líderes del Mercado

Los protocolos (independientemente de si es en Blockchain o en informática en general) son reglas o procedimientos relacionados a la gobernanza de los datos y su transferencia. Esta transferencia de data siempre ocurre entre dos o más partes (entendidas como dispositivos electrónicos) y permite que la estructuración de los datos esté lo suficientemente solidificada para que los computadores entiendan bajo qué parámetros hay intercambios de información, y cómo las partes tendrán un envío o una recepción de la data, que en el caso de Blockchains como Bitcoin o Ethereum se puede traducir en BTC o Ether.

Finalmente, lo que se agrega en un protocolo de Blockchain es que siempre hay un algoritmo detrás que define el comportamiento que se tendrá en la red y este varía dependiendo el que se esté manejando, el cual siempre servirá para la validación de las transacciones y esto irá ligado a la verificación de las partes involucradas. Así pues, existen protocolos basados en redes públicas y otros para permisionadas y empresariales, por lo que conocer tanto los diferentes tipos de protocolos como los tipos de redes existentes cobra valor.

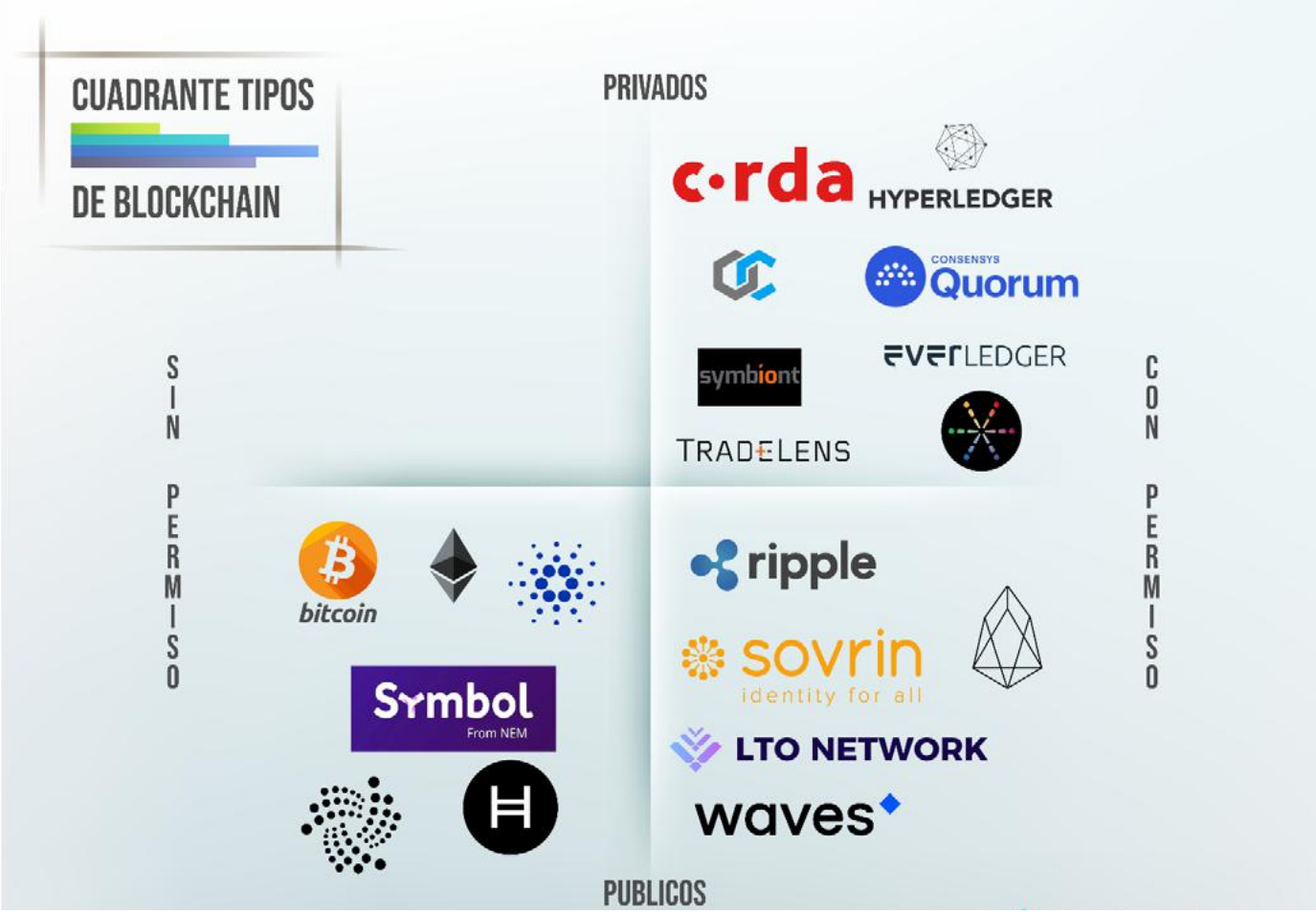


Figura 26. Cuadrante tipos de Blockchain.

Figura 27. Comparando protocolos Blockchain y DLT líderes del mercado. Información adaptada de (Aseev, 2020; Mohanty, 2019).