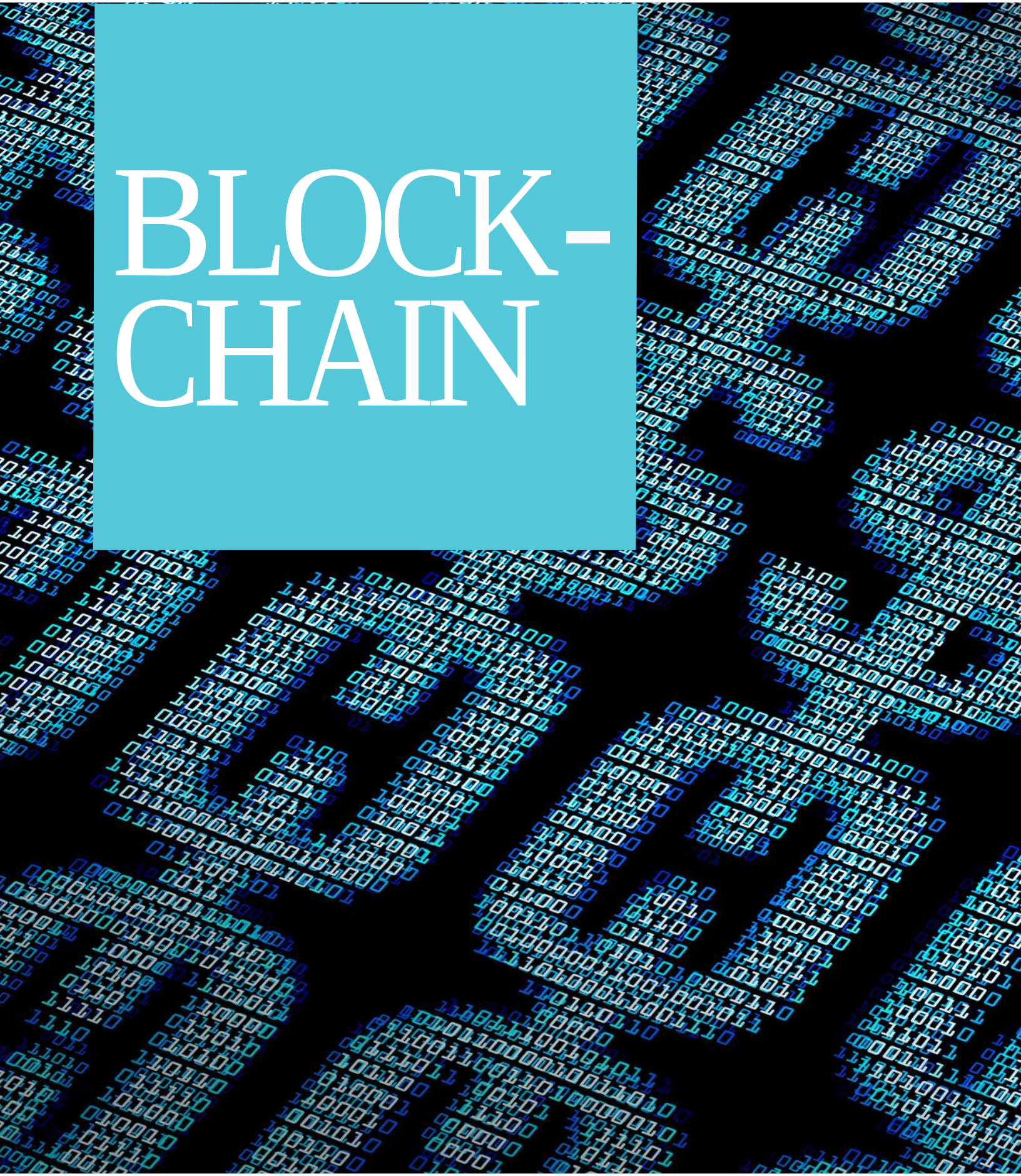
BLOCK-CHAIN



JENSHARDINGS

Doctor en Ciencias mención Computación, Universidad de Chile. Profesor part time en la Universidad de Chile entre 2004 y 2014, y full time en la Pontificia Universidad Católica de Chile entre 2005 y 2010. Áreas de interés en Impacto Social de las TI, incluyendo Software Libre, Seguridad Informática y Redes de Computadores, así como Software Social. Actualmente participa en directorios, emprendimientos y asesorías, con énfasis en Gobernanza.

jens@hardings.cl

Pocas veces hemos visto una tecnología que genera tanta expectativa como el Blockchain, la base sobre la cual pueden funcionar no sólo las criptomonedas, sino todo un ecosistema de agentes autónomos y semiautónomos. Se ha dicho que es lo único parecido a Internet desde la Internet, en el sentido que hará a las finanzas lo que Internet hizo a los datos.

Con la incorporación al club por parte de Mastercard, la institución más reticente en lanzar públicamente proyectos con Blockchain, ya no queda ningún banco ni institución financiera de nivel global que se precie de tal, que no tenga alguna actividad relacionada al uso de esta tecnología. Al menos han aprendido a no seguir el contraejemplo de la industria musical y del cine, que tomaron la ruta de la negación y lucha contra el cambio, y sumarse más que restarse a la revolución *Fintech* que según muchos va a cambiar dramáticamente el paisaje de la industria financiera en el corto o a lo más mediano plazo. Y claro, los bancos no tienen ningún recurso parecido a las estrellas del Rock, Pop o Cine de los cuales intentar colgarse y no conozco a nadie que diga sinceramente que es fanático de su banco (en el mejor de los casos es un sentimiento de indiferencia), así que parece una decisión más que razonable. De hecho, normalmente en cualquier evento sobre Fintech los servicios prestados por la banca e instituciones relacionadas quedan muy mal parados en cuanto a eficiencia relativa con respecto a las soluciones nuevas que ya funcionan en todas las áreas de negocio relacionadas, por lo que cualquier mejora en imagen debiera ser bienvenida.

Tenemos que ser justos y mencionar que el fenómeno Fintech no se debe únicamente al Blockchain y en gran parte está relacionado con la forma de ver el mundo que tienen los Millenials, pero aun filtrando solamente las iniciativas basadas en Blockchain, los números siguen siendo muy impresionantes. Y por otro lado, Blockchain no solamente tiene una componente financiera sino, y aquí se pone realmente interesante, permite interacciones genéricas, como una máquina virtual no meramente distribuida, sino descentralizada a nivel físico, administrativo y político (con todas las ventajas y desventajas que ello implica).

Tanta expectativa respecto del Blockchain hace parecer inevitable a su vez muchas desilusiones cuando se disipe el polvo. Con toda seguridad en 2017 ya no será tan fácil levantar un par de decenas de millones de dólares sólo por mencionar Blockchain en un pitch. Pero hay aspectos que rescatar dentro de todo el *hype* y en general si se llega a cumplir sólo una fracción de las promesas, y éstas sólo parcialmente, tendrán un impacto muy importante en nuestra sociedad.

El Blockchain ha tomado relevancia después de haber sido algo así como el hijo desatendido del Bitcoin. Esto surge cuando nos damos cuenta que sus usos van mucho más allá de criptomonedas y medios de pago, y además incide la relativamente mala fama que estaba comenzando a recibir Bitcoin por *affaires* como MtGox, Silk Road y grupos dedicados al Ransomware, entre otros.

LA TECNOLOGÍA

Dada la facilidad con que se pueden crear copias idénticas de objetos digitales a costo prácticamente cero, el principal problema que se debe resolver para poder usar una moneda digital es el del doble gasto. O sea, cómo evito que alguien pueda tomar un símil de un billete o una moneda en formato electrónico y gastar cada copia paralelamente en distintas transacciones. En términos prácticos, sería el equivalente a sacarle copia a un billete de $1.000 y con uno de los billetes comprarme un diario y con el otro comprarme un café.

Las soluciones a ese problema generalmente toman uno de dos caminos posibles:

a) *Asociar el valor a un* ***medio físico****, con procesos que garantizan que cuando se transfiere haciendo un pago, ya no seguirá estando vigente en ese medio. Esto es lo que se hace por ejemplo con las tarjetas de prepago tipo MiFare o Cipurse.*

b) *Mantener un* ***registro de todas las transacciones****, o al menos todos los saldos que están asociados a cada cuenta o sujeto.*

En ambos casos, si múltiples actores pueden generar ingresos y egresos en las cuentas, y/o transacciones entre cuentas, no hay garantía de que el resultado sea consistente (alguien podría agregar valor a una cuenta sin que exista el correspondiente ingreso ni se saque de otra) ni correcto (inclusión de transacciones inválidas u objetadas). Por lo mismo, todos los sistemas propuestos antes del Bitcoin tenían al menos la desventaja de requerir de un tercero en quien todos confiaran para entregar esas propiedades (consistencia y correctitud), y si bien se pueden implementar sobre sistemas distribuidos, la autoridad y control sobre la información siempre había sido centralizada.

BLOCKCHAIN: CONFIANZA, CONSENSO

El Blockchain permite, por primera vez, descentralizar la gestión de la base de datos de transacciones sin requerir que los participantes confíen entre sí, y así consensuar una única versión compartida entre todos los participantes. Es por esto que The Economist en su artículo de 2015 le llamó *"The Trust Machine"* [1](La Máquina de Confianza). Pero, ¿confianza en qué? Lo que provee el Blockchain es confianza en que los datos contenidos en él son consistentes y correctos, o sea que toda la creación y transferencias de valor o información genérica registrados cumplen las reglas. Para lograrlo, se necesita ordenar la información y mantener estas reglas en el tiempo, de forma que éstas tampoco pasen a ser una componente centralizada.

Otro punto relevante para efectos de mantener la descentralización es no depender de una fuente confiable de la hora actual. En el Blockchain, el tiempo se mide esencialmente en cantidad de bloques, específicamente el largo actual de la cadena de bloques. En cada bloque existe un *timestamp* que coloca quien genera el bloque, para lo cual debe seguir ciertas reglas. No por eso se considera una fuente confiable, pero a lo largo de la cadena de bloques permite mantener de forma agregada una sincronización suficientemente cercana a la hora real para todos los efectos prácticos, como por ejemplo mantener el promedio del ritmo de generación de bloques dentro del rango deseado.

TRANSACCIONES Y BLOQUES

Las transacciones en el Blockchain de una criptomoneda son esencialmente transferencias de valor desde una ubicación a otra, y para que sean válidas deben seguir ciertas reglas, como que el saldo que se transfiere debe estar disponible, tiene que contener la autorización de quien controla esos fondos, etc. Estas transacciones se agrupan en bloques que son los que efectivamente se agregan a la base de datos, y un bloque es válido si todas las transacciones (en el orden en que están en el bloque) son válidas. Las transacciones y los bloques se distribuyen mediante una red P2P, de forma que todos quienes quieran participar tienen acceso a esa información, y cada bloque depende directamente del anterior, de ahí el nombre Blockchain o cadena de bloques.

Para ser realmente un sistema descentralizado, no se puede imponer centralizadamente quién tiene la atribución de agregar datos al Blockchain ni cuáles son las reglas que debe seguir, tanto para las transacciones como para los bloques. Pero si aplicamos esto al pie de la letra, cualquiera podría agregar información al Blockchain en cualquier momento y con las reglas que estime convenientes, generando un caos. Lo que se necesita entonces es un sistema que ordene los bloques que se van agregando y permita dirimir diferencias en las reglas.

Para ordenar los bloques, se introduce un algoritmo de consenso con el que se logra que en promedio se genere un bloque cada X cantidad de tiempo (en Bitcoin, X = 10 minutos; en otros Blockchain no es raro que sea solo un par de segundos). Este proceso de búsqueda del siguiente bloque se llama **minado**. Un algoritmo de consenso permite distribuir la generación de bloques entre todos los interesados de forma proporcional a su involucramiento en el sistema, y por cada bloque el minero afortunado que lo encuentra se hace acreedor de una recompensa como incentivo para sostener el sistema en funcionamiento.

Para dirimir diferencias en las reglas y cualquier mal comportamiento, el esquema es sumamente simple: cada nodo participante acepta solamente bloques que considera válidos, o sea que cumplen con todas las reglas que considera válidas (en particular, las del algoritmo de consenso), y si hay más de una cadena de bloques que es válida, toma la más larga como la "verdadera".

1. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Todo esto redunda en que cualquier nodo que quiera hacer trampa va a incurrir en un esfuerzo mayor que seguir las reglas que la mayoría ha adoptado. En ese sentido, el sistema no gasta esfuerzo en detectar y perseguir o castigar a los tramposos, sino que simplemente los ignora; una solución elegante por lo demás.

Todo lo anterior es válido y ha demostrado funcionar muy bien en la práctica, siempre y cuando se cumpla con un requisito muy importante: que la generación de bloques esté bien repartida y no se concentre una porción cercana al 50% en un solo ente o grupo organizado. Y es un requisito no menor, sobre todo considerando que no hay cómo demostrar que esa concentración no existe.

ALGORITMOS DE CONSENSO

Existen varias alternativas para definir el algoritmo de consenso, pero los dos principales son *Proof of Work* (PoW) y *Proof of Stake* (PoS). El objetivo de estos algoritmos es resolver dos problemas:

1. *Llegar a un consenso sobre el estado del Blockchain controlando la velocidad de generación de bloques y definiendo un orden no objetable entre ellos, y*

2. *la incorporación y salida de nodos sin requerir un registro o inscripción de ningún tipo.*

PROOF OF WORK (POW)

Tomado del esquema Hashcash para limitar el Spam, consiste en encontrar un número que se incorpora al bloque de tal forma que el hash del bloque sea menor a cierto número objetivo. El cálculo de ese número objetivo forma parte de las reglas, por lo que si alguien quiere usar un objetivo más fácil, verá que los demás le rechazarán sus bloques.

Dependiendo del número objetivo, encontrar el adecuado para el bloque requiere muchas iteraciones y por ende como todos los participantes pueden comenzar a buscar el siguiente bloque apenas esté publicado el anterior, la cantidad de bloques que puede encontrar un nodo es proporcional al poder computacional que le dedica a ello.

La frecuencia en la generación de bloques se mantiene constante en promedio ajustando la dificultad (aumentando o reduciendo el número objetivo) cada cierto tiempo. La mayor crítica que se le hace al PoW es que genera un malgasto de energía importante, considerando que a mayo de 2017 se estima que se calculan ~$4x10^{18}$ Hash por segundo[2] para mantener el Blockchain de Bitcoin, lo cual implica unos 393MW (Mega Watt) de consumo eléctrico permanente si se usara el hardware más eficiente del mercado[3]). Esto es casi un 7,5% de la capacidad de generación del Sistema Interconectado del Norte Grande de Chile, o cerca de un 1,8% de la capacidad total de generación instalada en Chile[4]. Un gran consumo considerando que esa es la cota inferior. Otra crítica que se le puede hacer es que, pasado un nivel mínimo de disponibilidad de recursos aportado por todos los nodos para un correcto funcionamiento del sistema, recompensar el exceso de capacidad dedicada a minar bloques no parece justo ni correcto.

PROOF OF STAKE (POS)

Una alternativa interesante, que igualmente puede incluir una proporción de PoW, es que aquellos que tienen más involucramiento en la plataforma, medido en fracción del total del valor que controlan, debieran ser quienes tienen más influencia. Después de todo, mientras más valor controlas, más interés tendrás en mantener el valor y no realizar ninguna acción que atente contra ese valor. Adicionalmente, al no involucrar más recursos de lo necesario, los costos de transacción debieran tender a ser mejores con un esquema de este tipo que no premia el exceso de capacidad computacional y por ende baja los costos.

Es importante mencionar eso sí que PoS puede funcionar en un sistema que ya tiene valor, donde quienes participan arriesgan algo en caso que se devalúe su participación, pero que no cumple su objetivo en un sistema nuevo o de bajo valor total. Tanto Bitcoin como Ethereum, los Blockchain con mayor valor monetario, tienen planes de cambiar su operación a Proof of Stake, pero aún no son concretos en cuanto a fechas o detalles de implementación definitivos.

PRIVACIDAD

Dado que todas las transacciones son públicas, cabe preguntarse dónde está esa privacidad o anonimato que tanto se asocia a las criptomonedas. La verdad es que el modelo de privacidad es diametralmente opuesto al que manejan los bancos e instituciones financieras, que conocen perfectamente los detalles de todos sus clientes, y de hecho tienen una obligación legal de conocerlos *(Know Your Customer)* a través de leyes contra el lavado de activos. Estas instituciones mantienen las transacciones y los saldos en privado, protegidos por el secreto bancario.

En el caso de las criptomonedas es justo al revés: todas las transacciones con sus respectivos montos son públicas, pero nadie sabe a quién pertenecen salvo que el dueño quiera demostrar su vinculación a esas direcciones. Si se desea mantener la privacidad, es necesario seguir ciertas recomendaciones como por ejemplo usar distintas direcciones para cada transacción y otras. Pero cierta información es más difícil de ocultar, por ejemplo si debo pagar un monto alto necesito juntar fondos de más de una dirección, con lo cual queda publicado que todas esas direcciones están relacionadas.

ALMACENANDO MÁS QUE VALOR MONETARIO: ETHEREUM

A partir de aquí la cosa se pone realmente interesante. Recomiendo leer cada una de las próxi-

2. https://blockchain.info/charts/hash-rate
3. https://en.bitcoin.it/wiki/Mining_hardware_comparison
4. Boletín Mercado Eléctrico sector Generación abril 2017: http://generadoras.cl/documentos/boletines/boletin-mercado-electrico-sector-generacion-abril-2017

mas tres secciones a conciencia y tomarse el tiempo de digerirla completa antes de seguir con la siguiente, porque cada sección se construye en base a los conceptos de la anterior.

Criptomonedas como el Bitcoin tienen propiedades interesantes que las hacen mucho más flexibles que el dinero en efectivo, como por ejemplo poder definir que cierto fondo no se puede gastar antes de que pase una cantidad de tiempo, o que se requieren varias firmas simultáneas, entre otros. Sin embargo, se puede hacer mucho más que eso. El caso más interesante es **Ethereum**, un Blockchain en el cual no solamente se almacena un valor, sino que se agrega código ejecutable (un lenguaje Turing-Completo, a diferencia del scripting intencionalmente limitado disponible en Bitcoin) y variables, en el cual una transferencia o mensaje hacia una dirección gatilla la ejecución del código. A partir de esto, se nos abren diversas posibilidades: contratos inteligentes, propiedad inteligente, Organizaciones Descentralizadas Autónomas (DAOs por sus siglas en inglés).

Todo nodo que participa en la mantención del Blockchain debe ejecutar el código correspondiente a cada transacción para validarla, y debe almacenar la información de las variables de cada contrato incluido en el Blockchain. Es entonces importante que ese código y el almacenamiento que usa sean eficientes, por lo que quien agrega una nueva transacción (estilo "quien llama paga") debe pagar una tarifa de procesamiento que es proporcional a las operaciones ejecutadas y espacio de memoria usado para validar la transacción. Quien inicia la transacción define un límite máximo a pagar *(gas limit)*, y si esos fondos no alcanzan la transacción se elimina (y el iniciador paga igualmente el máximo que indicó). Esto evita problemas como *loops* infinitos y en general ejecutar operaciones que no son valiosas para alguien.

Una problemática relevante se presenta al querer incorporar información que no está presente *per se* en el Blockchain, dado que necesitamos poder validar las transacciones en todos y cada uno de los nodos participantes en el sistema de forma determinista. Para mantener la naturaleza descentralizada quisiéramos obviamente que esta comunicación con el mundo exterior también lo fuera, por lo que las soluciones a este problema, los Oráculos, son más complejos que un simple RPC e incorporan múltiples fuentes con su respectiva reputación, respaldada o no por garantías en el mismo Blockchain, o hasta mercados predictivos completos.

CONTRATOS INTELIGENTES (SMART CONTRACTS) O DAPPS

No soy muy amigo de asociarle el atributo de inteligencia a sistemas que son meramente automatizaciones básicas como ejecutar código gatillado por la recepción de un mensaje, pero no voy a luchar contra la corriente en este tema por ahora. En términos simples, un contrato inteligente es una cuenta o dirección en el Blockchain que además de tener fondos disponibles, está asociada a un código que se ejecuta cada vez que llega una transacción a esa dirección. La ejecución de lo establecido en el contrato se realiza de forma automática según las condiciones que establece ese programa o contrato. Se hace realidad lo que describía Lawrence Lessig en 1999[5] cuando mencionaba que el código legal es interpretado y ejecutado por humanos dentro del contexto (caro, lento y difícil de operar en un mundo global) de una legislación basada en jurisdicciones geográficas, mientras que el código computacional es ejecutado en un ambiente (barato, rápido e indiferente a las fronteras geográficas) del ciberespacio o como le queramos llamar. La promesa aquí es un sistema que regula las interacciones y que no está sujeto a interpretación ni atención humana, salvo que se desee y ésta se incorpore dentro de las condiciones del contrato.

BIENES INTELIGENTES (SMART PROPERTY)

Complementando contratos inteligentes con dispositivos conectados, conocidos hoy en día como "Internet of Things" (IoT), obtenemos lo que se ha llamado Bienes Inteligentes. O sea, objetos en el mundo real que se comportan de acuerdo a lo que un contrato en el Blockchain les indica. Esto es muy práctico si queremos por ejemplo realizar un arriendo de diversos tipos de recursos: automóviles, salas de reuniones, estacionamientos. Estos arriendos pueden ser de largo o corto plazo, y no requieren un contrato jurídico previo ni intermediarios salvo por el Blockchain que sería un intermediario que no tiene asimetrías de control, poder o información respecto de nosotros (tanto en nuestro potencial rol de arrendador como de arrendatario).

ORGANIZACIONES DESCENTRALIZADAS AUTÓNOMAS

Una organización, pensemos en una empresa o una ONG, esencialmente es una entidad que maneja recursos, tiene un propósito o un objetivo e interactúa con diversos otros entes para ir alcanzando ese objetivo. Con los contratos inteligentes tenemos un ente que controla recursos, tanto monetarios como físicos, e interactúa con terceros en base a reglas establecidas en su contrato. Un contrato suficientemente completo, que posiblemente se podría actualizar siguiendo esquemas como los que rigen una Sociedad Anónima u otras corporaciones según estatutos y votaciones de los socios, podría perfectamente existir en el Blockchain, sin necesidad de una contraparte constituida legalmente. Sería para todos los efectos prácticos, una organización autónoma, en el sentido que no requiere de personas (gerentes, administrativos, etc.) que actúen a nombre de ella, y en caso de requerir acciones por parte de humanos, los contrata para esos efectos específicos y en caso de cumplimiento le paga lo convenido.

EJEMPLOS APLICADOS

Dicen que es muy difícil hacer predicciones, sobre todo si es sobre el futuro, pero es necesario intentar mostrar ejemplos concretos de aplicación de todos los conceptos abstractos mostrados. A continuación algunas ideas para entender de forma macro de qué estamos hablando.

5. Lessig, L."Code and Other Laws of Ciberspace", Basic Books, 1999.

MICROPAGOS

El problema de los micropagos es difícil de resolver, esencialmente porque siempre es posible definir el monto de los pagos a realizar tan bajo que el costo de la transacción tienda a ser más grande (incluso varias órdenes de magnitud) que el monto a pagar. En el caso del Blockchain, el costo es muy pequeño, pero tiene un límite: no puede ocupar menos que cierta cantidad de bytes (al menos dirección de origen y destino además de la firma digital o autenticación similar requerida). Esos bytes deben registrarse en el Blockchain, donde el tamaño de los bloques, si bien se puede expandir, siempre está limitado a un tamaño máximo. Y finalmente, cada transacción se guarda para siempre en el Blockchain, por lo que el crecimiento que requiere almacenar toda la base de datos debe ir de la mano con el crecimiento de la capacidad de almacenamiento para evitar incrementar demasiado el costo de mantener el sistema funcionando.

DESINTERMEDIACIÓN

La mayor promesa del Blockchain es la desintermediación. Mientras más intermediarios tengamos entre un producto o servicio y el consumidor final que lo necesita, más costos le agregamos a ese producto o servicio, y en los últimos años hemos visto tendencias a reducir ese número. Sin embargo, en la mayoría de esos casos, quien se apropia de esos ahorros en eficiencia no es el productor ni el consumidor final, sino uno de los intermediarios, ya sea uno existente o uno nuevo. Peter Thiel lo explica brillantemente desde el punto de vista del nuevo intermediario que ingresa al mercado o crea uno nuevo, en lo que podríamos llamar su "apología al monopolio"[6]. Dentro de esta categoría caben la mayoría de lo que los inversionistas de riesgo llaman "Unicornios" (empresas que alcanzan valorizaciones de 1.000+ Millones de USD), en particular: Uber, AirBnB, Spotify, iTunes (Apple), Netflix, etc. Estoy dejando fuera otros como Facebook, Whatsapp y Google que también generan sus ingresos en base a la asimetría de información y poder que logran establecer, pero donde la aplicación de soluciones sobre Blockchain son menos obvias (aunque hay propuestas).

La desintermediación es relevante no solamente porque se le traspasa prácticamente todo el ahorro en eficiencia a los extremos (productor y consumidor), sino además porque las transacciones, identificación de las partes y otra información relevante es manejada de forma transparente y entrega mayor nivel de control. Considerando que, salvo por Spotify, todos los mencionados están sujetos a una jurisdicción que los obliga a entregar todos sus datos al Gobierno de Estados Unidos y mentirle a sus usuarios al respecto, es un punto que adquiere cada vez mayor relevancia.

No vamos a entrar en los detalles aquí, pero la esencia de la desintermediación es que permite a un conductor de vehículo, a un dueño de un bien inmueble, a un compositor o un productor de películas contactarse directamente con quien quiere usar su bien o servicio y cobrarle directamente, evitando así el empoderamiento de un tercero que tarde o temprano va a usar esa asimetría en su favor.

Hay que tener en claro que sí existiría un intermediario, y ese sería el contrato en el Blockchain, pero a diferencia de los nombrados, todas sus acciones son públicas y por la naturaleza del Blockchain es muy fácil que algún otro contrato reemplace al anterior si ofrece mejores condiciones a los extremos de la cadena. Dado que la potencial ganancia que tienen esos mercados es más medida, estando más a la altura del esfuerzo, los incentivos son menores y se demorarán más en concretarse. Pero en la medida que surjan más organizaciones que vean su propósito más importante que potenciales ingresos multimillonarios, más cercanas a lo que Frederic Laloux llama Organizaciones Evolutivas o Teal[7], seguramente veremos más y más iniciativas de este tipo concretarse y abarcar una gran porción del mercado.

MERCADOS DE PREDICCIÓN, SEGUROS P2P, CROWD*ING

En estricto rigor estos ejemplos también son formas de desintermedación, pero en este caso no se ven por el momento grandes actores que dominen el mercado tan marcadamente, y es más probable que soluciones basadas en Blockchain pudieran surgir de los mismos actores actuales. Además, son todos casos en los cuales es crucial lograr trasladar información fidedigna desde el mundo real al Blockchain (cuál fue el resultado de un evento tal como una elección presidencial, hubo o no un siniestro y cuál fue el monto, pagó o no su préstamo el beneficiario).

Los mercados de predicción prometen ser mucho más fidedignos que las encuestas, pero también tuvieron resultados desastrosos en las últimas elecciones presidenciales de Estados Unidos, lo cual implica que aún falta camino por recorrer. La idea es ofrecer a la venta un número limitado de acciones en base al resultado de un evento (deportivo, político o de cualquier otra índole), y según oferta y demanda el precio de esas acciones.

Los seguros P2P apuntan a segmentos en los cuales las compañías de seguros generalmente no están interesados, ya sea por el corto plazo, el bajo valor del bien asegurado u otros, haciendo que los beneficios esperados no cubran los costos administrativos de generar el contrato, pero también tiene aplicaciones en seguros más tradicionales. Aplicaciones específicas incluyen equipaje en viajes, bicicletas, automóviles, etc.

Crowdfunding, Crowdlending y otras iniciativas del estilo permiten que muchas personas financien iniciativas y mantengan una participación baja en cada iniciativa, diluyendo el riesgo. Usando esquemas en Blockchain se reduce la complejidad de temas administrativos como votación de accionistas, repartición de dividendos, etc. Además, se permite participación completamente anónima

6. Thiel, P., "Zero to One", Crown Business, 2014.
7. Laloux, F. "Reinventing Organizations", Nelson Parker, 2014.

sin dejar de hacer uso de los derechos de voto, recepción de dividendos y sin requerir intermediación de un tercero.

TRANSPARENCIA Y VALIDACIÓN

Aprovechando que los contenidos en el Blockchain son públicos, tienen validación de fechas (timestamping) y son inmutables, se abre un abanico de posibilidades donde nos interesa registrar hechos en un Blockchain como forma de demostración de hechos que se registraron antes de cierta fecha, o incluso asociar tokens en el Blockchain a derechos de propiedad sobre objetos en el mundo real.

CONSERVADOR DE BIENES RAÍCES

El registro de títulos y propiedades está lleno de historias donde se han perdido los papeles, han aparecido transferencias falsas y otros tantos. La promesa del Blockchain es que los registros son públicos y tan indestructibles como el Blockchain, por lo que no les afectan desastres naturales (locales por naturaleza) como inundaciones, fuegos o amigos de lo ajeno. Hay muchos detalles que quedan por definir, como qué pasa si no está disponible la llave privada para realizar una transferencia, pero con contratos inteligentes es posible agregarle una cantidad suficiente de reglas para que sea más robusto que cualquier sistema actual. Suena bastante futurista, pero ya hay planes piloto en Suecia, Georgia, Honduras y otros.

CONTABILIDAD DE TRIPLE ENTRADA

Hoy en día hay cada vez mayor exigencia de privacidad para las personas, y de transparencia para las instituciones. Para instituciones que quieran o deban informar de la forma más abierta posible sus actividades financieras, está la posibilidad de utilizar una contabilidad de triple entrada. Esto consiste en la misma contabilidad de doble entrada usada en todo el mundo, pero con una entrada adicional que se va publicando en tiempo real (o al menos casi real) en el Blockchain, y así cualquier interesado puede realizar una auditoría o análisis (incluso hacer seguimiento de su donación realmente anónima) sin requerir ninguna otra acción por parte de nadie ni confiar en el informe de un auditor externo (que por lo demás en los últimos años han dejado mucho que desear). Además, "arreglar" la contabilidad no va a ser posible a posteriori, y cualquier actividad poco ortodoxa debiera poder gatillar alertas si hay suficiente información (en particular de terceros) para contrastar los hechos publicados. Por ejemplo, alguien podría detectar que una organización no está informando sobre la deuda que mantiene con él o ella, lo cual implicaría que no tiene intención de reconocerla, o bien le está ocultando información a los *stakeholders*. Estas prácticas harían que los fraudes a nivel contable sean mucho menos comunes y se detecten con mayor rapidez, evitando que crezcan durante mucho tiempo sin ser detectados.

KNOW YOUR CUSTOMER

Las instituciones financieras tienen cada vez mayores obligaciones de conocer a sus clientes y el origen de los fondos que estos invierten, para efecto de prevenir operaciones de lavado de activos. El Blockchain puede ser una plataforma muy interesante para que diversos sujetos puedan actuar como entes certificadores de hechos de muy diversa índole, y las instituciones financieras podrán considerar aquellos que les dan confianza o bien tengan la validación de una autoridad competente según corresponda.

IDENTIDAD

La idea de registrar nuestra identidad en el Blockchain y poder asociar a esa misma identidad diversas cuentas o accesos. De esta forma, podríamos usar esa identidad como forma de autenticarnos ante diversas plataformas, tales como bancos, redes sociales o incluso instalaciones físicas, con lo cual ya no necesitaríamos diversas claves, tarjetas o llaves, y hasta carnets de identidad, licencias de conducir o pasaportes. También podemos asociar una reputación positiva a esta identidad al interactuar con personas o sistemas que no nos conocen y requieren que arriesguemos parte de nuestra reputación antes de arriesgarse a entregarnos recursos.

PRIVACIDAD: GESTIÓN DE DATOS PERSONALES

Cuando el objetivo es contrario a la transparencia y queremos por ejemplo recibir información de forma selectiva, también el Blockchain nos puede ayudar. Si bien hay una tendencia, liderada por Europa, de proteger los datos personales por ley y de entregarle la titularidad sobre esos datos a las personas sobre los cuales informan. Espero que en Estados Unidos sigan con la incipiente conciencia que ese es el camino a seguir, un nuevo trato respecto de los datos[8]. La idea de gestionar los datos personales ya tiene ejemplos concretos de cómo puede funcionar[9], y si se utiliza sobre el Blockchain, no requeriría de un tercero confiable ni infraestructura propia.

Es más, se podría incluso solicitar ofertas específicas según mi interés en el momento, y dado que yo estoy facilitando un *"lead"* de altísima calidad al permitir que me lleguen ofertas de cierto tipo para decidir sobre mi compra, sería justo que yo fuera quien reciba el pago que hoy en día se entrega a agencias que intentan hacer llegar el mensaje a través de distintos medios. Así, si por ejemplo me interesa realizar un viaje a medio oriente en tres meses más, comprarle una casa a mi perro y decorar una pared en mi casa, me gustaría que, mientras tomo la decisión, me lleguen diversas ofertas al respecto. Y para eso no necesito entregarle mis datos de contacto a los oferentes, sino simplemente tener un sistema (por qué no un contrato inteligente) que no solo reciba los mensajes, los filtre según mis intereses y acepte los que sabe me interesan, recibiendo al mismo tiempo mi pago por recibirlos. Y una vez tomada la decisión se cierra esa puerta y no me llegan más, no como hoy en día con las búsquedas por productos que detecta Google y me persigue con avisos durante meses sobre algo que ya compré. No vaya a ser que después aparezca una oferta mejor a la que tomé y termine arrepintiéndome. ■

8. http://hd.media.mit.edu/wef_globalit.pdf
9. Ver por ejemplo el proyecto OpenPDS/SA: http://openpds.media.mit.edu/