Decentralized Culture Magazine

ÁGORA

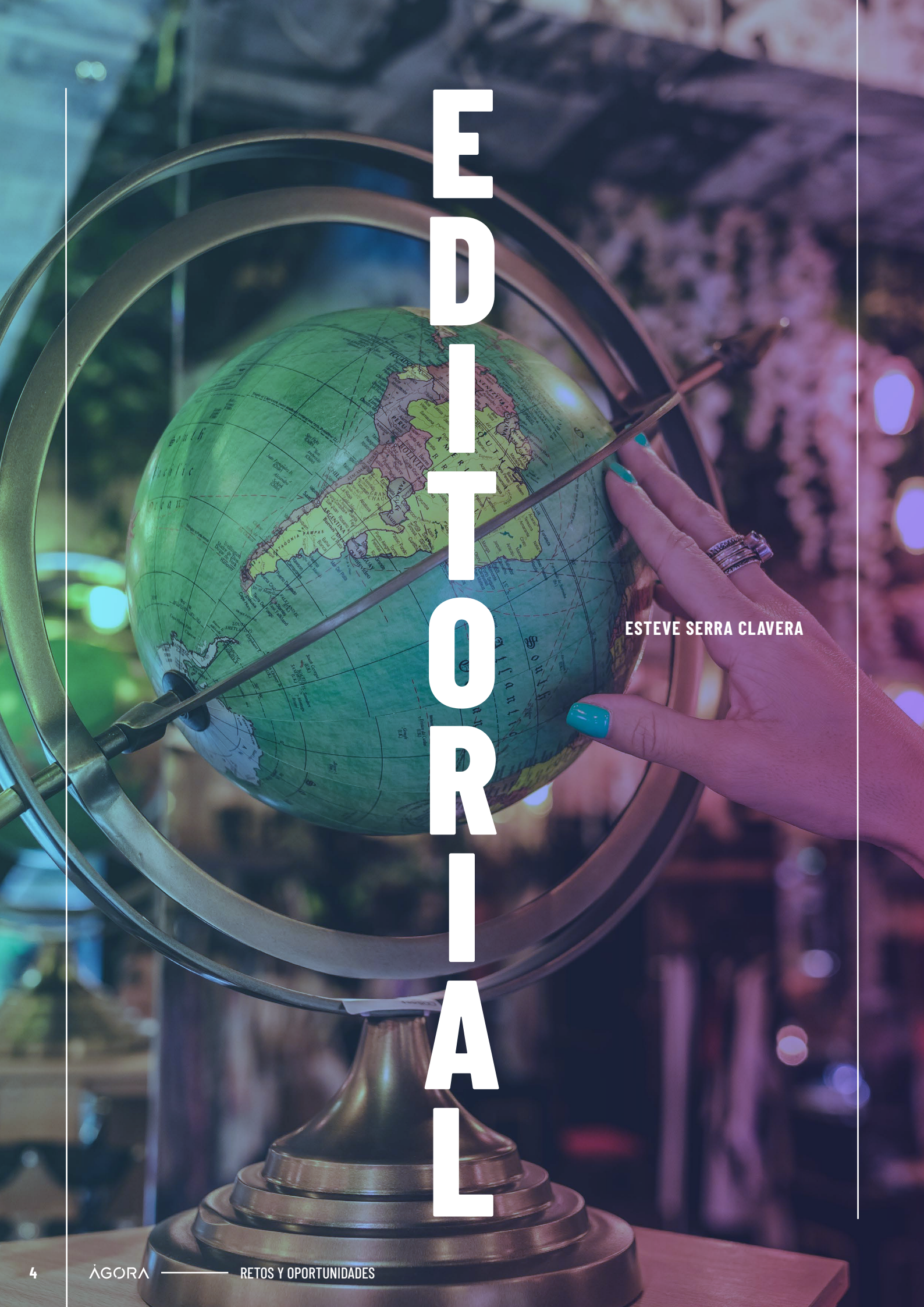
AGORACHAIN.ORG

11

RETOS Y OPORTUNIDADES

SUMARIO

EDITORIAL



ESTEVE SERRA CLAVERA

Latinoamérica no es un descubrimiento

Desde un principio, el proyecto de ÁGORA, aun siendo de alcance global, ha tenido la mirada puesta en gran medida en España y Europa, por ser la región geográfica donde residen los miembros del equipo, y las comunidades de las que forman parte.

No obstante, en el sino de AgoraChain debería aparecer siempre el espíritu de avanzar, innovar y adaptarse.

Está claro que el papel de Latinoamérica no debe limitarse a la simple audiencia, sino que ha de formar parte intrínseca si se persigue seguir constituyendo la plaza de referencia en el mercado *blockchain* de habla hispana. Esto requiere desplazar el eje para situarnos donde las comunidades se esfuerzan a diario por desarrollar, impulsar y mejorar la sociedad desde abajo. Aprender del extenso y rápido desarrollo que allí acontece.

Latinoamérica tiene la oportunidad de saltarse los pasos intermedios por los que ha pasado España. Al mismo tiempo, dispone de una vitalidad pujante para afrontar los retos cara a cara, algo que a veces se echa en falta en nuestro país por una situación ligeramente acomodaticia que adormece el ingenio.

El castellano es una lengua potente, a la par que moderna, permitiendo comunicarnos, aprender y dialogar gracias a su extenso bagaje. Un lazo que nos une allende los mares.

Una forma de afianzar la pujanza del mundo hispanohablante es la de seguir conversando en nuestro rico y variado idioma como contrapunto al extenso uso del inglés en muchos proyectos y comunicaciones.

Así pues, es un placer poder contar a partir de este número con la participación de tres comunidades que estrenan sección, tales como «Sapere Aude!» (BAES; Blockchain Aplicado a las Administraciones Públicas y las Empresas), «Tecnologías para el desarrollo» (BID; Banco Interamericano de Desarrollo) y «Rincón humanitario» (b4H; Blockchain4Humanity).

Ésta es la casa de quien quiera compartir, dialogar y escuchar.

PARTICIPA

MIGUEL PRADOS RODRÍGUEZ

«Los electores probablemente prefieren mandar a decidir»

Todo es gobernanza. Descentralizar, ¿para qué?

Completaba este artículo reflexionando sobre las pasadas elecciones generales y el camino que ahora finaliza el partido político que fundé, Democracia Participativa («Participa»), hace ahora ocho años. Basado en la desintermediación política, en nuestro partido decidía la población mediante consultas y el representante político era elegido en listas abiertas (listAbierta.org), por lo que se debía a sus electores y no al «aparato» que pudiese o no colocarlo en una lista (el problema aparece cuando organizaciones que funcionan distinto se unen en un mismo escenario político; no hay Interledger, Cosmos o Polkadot que lo solucione, pero ésta es otra historia).

Después de algunos años con representación en instituciones locales y bastantes consultas populares, una de las conclusiones a las que llegaba en esta reflexión es que los electores probablemente prefieren mandar a decidir. Es importante el matiz: decidir implica un esfuerzo cognitivo considerable, pues supone sopesar opciones, constrastar y valorar. ¿Qué esperamos de un mundo descentralizado gracias a la *blockchain* (y otras DLTs)? ¿Mandar, decidir o participar? ¿Y para qué? Otra de las lecciones aprendidas es que el objetivo no es la posibilidad de decidir colectivamente, sino que estas decisiones sean mejores para el conjunto.

Hay muchos ámbitos que se pueden descentralizar (ver la infografía con algunos ejemplos). No obstante, habría que preguntarse si en una economía participativa (con naciones, corporaciones, identidades, comunicaciones, pagos y energía descentralizados) viviremos mejor que con las naciones-Estado y las grandes corporaciones.

La mayor parte del tiempo estamos eligiendo y no decidiendo. Elegimos entre nuestras opciones de forma impulsiva y con posterioridad las justificamos con una capa argumental *ad hoc*. Le debemos al premio nobel de economía David Kahneman la explicación de este mecanismo de autoconvicción. El problema es que «conocido el mecanismo, conocida la trampa». Si queremos hacer que la gente tome determinadas elecciones, sólo tenemos que saber activar las teclas que «puentean» el sistema racional y llegar directamente a los centros de decisión: el miedo, la rabia y el deseo.

Desgraciadamente, en política nunca ha hecho falta cubrir de argumentos racionales el uso y abuso de estos mecanismos para activar la toma de decisiones: «viene el fascismo» (miedo), «están rompiendo España» (rabia) o «quiero parecerme a ella/él» (deseo).

Así que las decisiones colectivas (descentralizadas) no constituyen *per se* una garantía de decisiones mejores, aunque sí pueden percibirse como más justas, porque todo el que está censado puede votar.

Cuando hablamos de sesgo cognitivo y decisiones irracionales, estamos hablando de una experiencia de usuario (UX) mal diseñada (aunque sea a propósito). La solución no es la gobernanza on-chain (recordemos el caso del hackeo de la DAO) ni tampoco la gobernanza off-chain. Tampoco es un problema de elección del protocolo de descentralización. El problema es que cuando «nos dejan» participar (en unas elecciones, por ejemplo) trasladamos un mandato influido irracionalmente, en lugar de una decisión con perspectivas racionales de ser la mejor opción, y pasa lo que pasa.

TODO ES GOBERNANZA

1 DESCENTRALIZAR ¿PARA QUÉ?

OLD WORLD		DESCENTRALIZACIÓN
GRANDES CORPORACIONES	2	ECONOMIA COLABORATIVA
NACIONES ESTADO	3	NACIONES DESCENTRALIZADAS
MONOPOLIO ENERGÉTICO	4	DER Y SMART GRIDS
INTERNET SERVICE PROVIDERS	5	MESH NETWORKS
CONFIANZA CENTRALIZADA	6	CONSENSOS DESCENTRALIZADOS
BASES DE DATOS CENTRALIZADAS	7	BASES DE DATOS DISTRIBUÍDAS
TESTIGOS NOTARIADOS	8	ORÁCULOS
BANCOS Y PAGOS CENTRALIZADOS	9	PAGOS PEER TO PEER
IDENTIDAD CENTRALIZADA	10	IDENTIDAD DISTRIBUIDA
EMPRESAS INTERMEDIARIAS	11	EMPRESAS SIN INTERMEDIARIOS
APLICACIONES CENTRALIZADAS	12	DAPPS
NAVEGADOR	13	BROWSER DAPPS

14 GOVERNANCE AS A SERVICE

No nos fustiguemos: la energía que tenemos es limitada, el cerebro es el órgano que más consume y estamos diseñados antropológicamente para minimizar el consumo de energía. Ante una sobredosis de información y necesidad de acción, tomamos atajos. Si aparece un tigre en la Gran Vía, hay que correr, no sopesar las diferentes opciones. El problema es que la política actual está diseñada para que tomes decisiones de esta forma: el tigre es «el fascismo» o «los bolivarianos» del discurso actual, el sistema está diseñado para tomar decisiones irracionales cada cuatro años.

El problema que hay que resolver entonces es: ¿cómo podemos diseñar una experiencia de usuario que nos permita tomar buenas decisiones desintermediadas y seguras gracias a *blockchain*? Pues en eso estamos. Empecemos por interpretar qué es una «buena» decisión.

Algunas pistas: hacer que la toma de decisiones se realice en un contexto sin excesiva presión (un plazo corto), que el grupo de decisión sea diverso y que tenga un mayor número de mujeres, disminuir la influencia social excesiva de algunos miembros del grupo sobre otros, aumentar el coeficiente empático del grupo, etc. Todos estos factores incrementan (estadísticamente) la inteligencia en la toma de decisiones de un colectivo. Estamos diciendo que un grupo de *stakeholders* extraordinariamente motivados y activos pero que sólo representan al 2% del censo del grupo de decisión en el que influyen mucho los desarrolladores/fundadores (la gran mayoría de las decisiones del «universo *blockchain*» se están tomando ahora mismo así) tomará estadísticamente peores decisiones (independientemente del protocolo y el peso del voto) que un grupo elegido al azar con unos parámetros predeterminados *ad hoc*. Y, si la participación del censo pasa del 2% al 40%, gracias a algún mecanismo perverso de democracia líquida, lo único que se consigue es que la decisión tenga una apariencia de mayor consenso, conteniendo los mismos errores.

Empecemos por el diseño de la capa de usuario (UX) para tomar decisiones (más a menudo y más inteligentes) sobre aquello que debamos decidir colectivamente (gobierno, economía, energía, identidad, comunicaciones), desintermediemos después el sistema (más oráculos y menos políticos), y entonces hablaremos de qué mecanismo sirve mejor para estos objetivos: democracia directa, voto cuadrático, voto líquido, etc., *on-chain* (con su mejor protocolo: POA, POS, POW, POL, etc.) u *off-chain,* y por último midamos y asegurémonos de que estamos tomando mejores decisiones de forma colectiva sobre lo que nos afecta.
Todo es gobernanza.

De nuevo, no es un problema de técnica, no se trata de democracia líquida o voto cuadrático, es un problema de diseño previo, de planificación. No se trata de cómo «pesar» decisiones o votos, se trata de estudiar las preguntas, cómo y cuándo hacerlas, y a quién.

Un buen comienzo puede ser el trabajo que (entre otros) el departamento de Inteligencia Colectiva del MIT (Massachusetts Institute of Technology) está haciendo y que intenta responder a la pregunta: «¿Cómo un grupo de personas puede tomar decisiones "estadísticamente" más inteligentes?». En un contexto de incertidumbre sobre los acontecimientos futuros, una decisión tomada de forma más inteligente no garantiza que la solución sea la más adecuada, pero al menos que se ha tomado de la forma mejor posible, es un mecanismo de diseño previo.

«¿Cómo podemos diseñar una experiencia de usuario que nos permita tomar buenas decisiones desintermediadas y seguras gracias a *blockchain*?»

GREEN BLOCKS

Blockchain: salvando el mundo (móviles sostenibles)

BORJA MESTRE

Septiembre de 2005. «Juanjo, voy a entrar. 50.000 € largo en café». De camino al colegio estuvo tratando de explicarme qué era ponerse largo (comprar) y que ese café jamás llegaría de su amigo Miguel. Fue ese día cuando la palabra especulación, además de significante, cogió significado.

El mercado de las materias primas *(commodities),* a la vez que la tecnología, ha ido evolucionando a lo largo de la historia. Lejos ha quedado ya el **frenesí** que se vivía en el *pit* del Chicago Board of Trade desde el momento en el que sonaba la campana para abrir el mercado hasta que ésta misma lo cerraba.

En este artículo vamos a ver cómo la cadena de bloques puede dar un nuevo rumbo a esta práctica. Ahora bien, *first things first.*

¿Qué son las *commodities*?
Son las materias extraídas de la tierra que se transforman para elaborar materiales que más tarde se convertirán en bienes de consumo, desde teléfonos a zapatillas.

Como es de entender, hay una gran variedad de materias primas. Éstas se dividen en dos grandes grupos: *soft commodities* y *hard commodities.*

Soft commodities son todas aquellas materias que vienen de la agricultura o la ganadería. En el primer grupo, se englobarían materias como el grano, el azúcar, cacao, café, arroz o el aceite de soja. En el segundo, podríamos mencionar la carne de cerdo, o de vaca.

Las materias que deben ser extraídas o minadas son consideradas ***hard commodities.*** Tanto el oro o la plata como el petróleo o el gas natural forman parte de este grupo. Al mismo tiempo, las *hard commodities* pueden ser divididas en dos subcategorías: metales y energéticas.

Actualmente, existen cincuenta mercados organizados en los que se cotizan y se transmiten este tipo de bienes. *Blockchain* tiene la capacidad de simplificar el *trading* de *commodities,* haciéndolo así más barato y transparente para los *traders.*

¿Cómo es esto posible?
Existen grandes ineficiencias en el mercado actual de *commodities,* muchas de ellas provocadas por la disparidad de los procesos que se dan en los diferentes países que forman esta cadena, lo que las convierte en extremadamente volátiles. Esto se debe a que su cotización se puede ver afectada por la subida del precio del petróleo (transporte), problemas administrativos (una errata en un documento), o la baja calidad del producto.

Tanner Ehmke, mánager en la división Knowledge Exchange en CoBank, afirma que la tecnología de contabilidad distribuida implica que «información, que normalmente se quedaría en un libro, sería compartida en múltiples ordenadores. (...) Teniendo muchas personas la misma visibilidad, además de dar mayor transparencia, ayudará a evitar errores, así como a prevenir fraude. Lo cual traerá valor desde el principio de la cadena (granjeros) hasta el final de la misma (consumidores)».

Blockchain brindaría la posibilidad de cambiar esto, dando la bienvenida a la era digital utilizando *smart contracts,* potencialmente dándole velocidad y reduciendo los costes de los procesos *post-trade.*

El hecho de tener a muchos de los usuarios como validadores (nodos) en la misma página, con una copia de los datos guardados en su ordenador y con la misma información, aumentará la confianza, transparencia y seguridad en el proceso de transacciones.

Komgo, empresa desarrollada mediante tecnología *blockchain,* busca ser un catalizador en el mundo de las materias primas. Respaldada por Ethereum, afirma que reducirá los costes entre un 20 y un 50%, dejando de lado numerosos intermediarios envueltos en este sector a día de hoy.

Esto no queda aquí. *Blockchain,* además, da la posibilidad de crear reportes de inventario de una forma segura. S&P Global Platts permite a la gente enviar informes semanales sobre el almacenamiento de petróleo en el Fujairah Oil Industry Zone.

En los mercados de la energía, *blockchain* puede usarse con redes inteligentes de paneles solares fotovoltaicos, lo cual podría ayudar a los propietarios de las casas a intercambiar energía entre ellos directamente. Este P2P rompe con el modelo de suministros públicos actual. Y es que independizarse del Estado en este tipo de prácticas es algo que se acerca, indudablemente, a la utopía.

¿Os imagináis un mundo totalmente descentralizado? ¿Un mundo que deja atrás la especulación y la corrupción?

El tiempo dirá. Ahora bien, hay problemas de mayor relevancia que esta nueva tecnología tiene el potencial de solucionar.

En mayo de 2018, la CNN hizo público un reportaje en el que a través de imágenes dejaba latente la explotación infantil que se estaba llevando a cabo en el Congo.

En 2017, dos tercios de la extracción mundial del coltán tuvieron lugar en la República Democrática del Congo. Este país, lejos de mostrar ningún tipo de iniciativa para acabar con estas prácticas, denominó al coltán, junto al cobalto, minerales estratégicos.

Se han visto, por tanto, aumentados los *royalties* de un 2% a un 10% a favor del Estado.

«Tenemos que aprovechar esta oportunidad y enriquecer el país lo máximo posible (...) los royalties subirán al mismo tiempo que la demanda por ellos».

ZANDI SHABALALA

Morgan Stanley prevé que para 2020 la demanda de cobalto se multiplique hasta ocho veces, especialmente por la tendencia del uso de coches eléctricos. Esta conjetura no resulta descabellada, pues tanto el coltán como el cobalto son dos minerales cruciales para la producción de baterías, ya que poseen unas propiedades **físico-químicas únicas.**

Así, **Ford Motors, junto a IBM, RCS Global, LG Chem y Huayou Cobalt,** anunciaron a principios de año la iniciativa de utilizar la cadena de bloques para hacer un seguimiento y validación de minerales y otras materias utilizadas en automóviles y otros productos de consumo electrónico.

Esta iniciativa ha nacido con la prioridad de que la extracción de estos materiales se haga de una forma sostenible, rompiendo así una lanza en favor del **ODS número 8** (trabajo decente y crecimiento económico) y el **número 10** (reducción de desigualdades).

La tecnología *blockchain* tiene el potencial de poner solución a muchos de los problemas a los cuales nos enfrentamos día a día. Hasta ahora, lo más sonado ha sido el ahorro de costes, la optimización en los procesos y sobre todo la capacidad, aún latente, que tiene de hacer el mundo más transparente.

Ahora bien, aun sabiendo que existe la posibilidad de dar solución a problemas de esta talla sin mirar, como es tendencia, hacia otro lado, son ya más de **5 mil millones de personas** las que tienen teléfono móvil. Se hace muy difícil mantener la integridad de los propios valores en estas circunstancias.

Blockchain no sólo tiene el potencial de hacer un mundo más transparente, no sólo tiene la capacidad de determinar la calidad del producto, no sólo tiene el poder de agilizar procesos. Es más, no sólo tiene la fuerza necesaria para, en un futuro, descentralizar los mercados, acabando con intermediarios y conectando directamente productores con consumidores —reduciendo la volatilidad provocada por la especulación—, sino que tiene el potencial de salvarlo.

Satoshi en la madriguera del conejo

IGOR DOMSAC

«Sólo unos pocos encuentran el camino, algunos no lo reconocen cuando lo encuentran, otros ni siquiera quieren encontrarlo».

ALICIA EN EL PAÍS DE LAS MARAVILLAS

Hay una oración, repetida hasta el infinito entre los legionarios de Crypto, que predica a sus discípulos las enseñanzas de DYOR. Son las siglas en inglés de **«haz tu propia investigación»** *(do your own research).* Si no la cumplimos, estamos perdidos, habiendo de confiar en lo que otros nos han vendido. Por si acaso, el lema de Bitcoin también nos avisa: «no confíes, verifica».

Pues bien, después de realizar mi propia investigación, y gritar a los cuatro vientos que **liberen a Ross,** he llegado a la convicción de que Craig Wright lideraba el grupo que, bajo el nombre de Satoshi Nakamoto, entregó Bitcoin al mundo. Sí, ese genio loco y autista, el egomaníaco maestro de los enigmas, ese artista creador de un inteligentísimo protocolo que funcionaba a la perfección antes de que su desarrollo fuera centralizado, cuando las élites del poder decidieron **secuestrarlo**. Entre secuestros y guerras, han ido transcurriendo los años, y hoy, todavía, la inmensa mayoría de usuarios lo siguen menospreciando. Le hemos hecho pasar un calvario, y lo seguimos crucificando. Aún no nos hemos detenido a escucharlo. Aunque parezca un tipo raro, un personaje muy extraño, él también es nuestro hermano. Y todos, al final, navegamos en el mismo barco. Lo queramos o no, vamos a tener que soportarnos. Tampoco juzgues tú, Satoshi, a tus hermanos libertarios, ni desprecies el mundo que soñamos, pues, en esencia, no dista demasiado de tu propio imaginario. Libertad, como tú bien dices, implica responsabilidad. Y la anarquía es, en el fondo, la única realidad. Aunque nos toque, de momento, convivir con el gobierno, el primer paso en el sendero es invitarlo a ser honesto.

Los oscuros mercados de la red profunda, que te hicieron llorar en el juicio, redujeron los riesgos asociados a la distribución y el consumo de compuestos psicoactivos. Resulta mucho más peligroso adquirir medicinas ilegales a mafias criminales en los suburbios más apartados de las grandes ciudades que recibir una carta en el buzón de tu casa con una sustancia de pureza contrastada que te envía el fabricante desde China o desde Holanda. La guerra contra las drogas, desde todos los planos, ha constituido un completo y absoluto fracaso. Ya es hora de firmar la paz con las medicinas tradicionales de nuestros antepasados, que se vendían en farmacias hace tan sólo cien años, cuando podemos, y debemos, reinventarnos. Silk Road suponía un desafío a la ley para poder avanzar, porque sólo nosotros mismos nos podemos gobernar, haciéndonos responsables de nuestra propia libertad, sin invadir ni violar la propiedad de los demás.

Craig, has creado una herramienta cuasi-perfecta para descentralizar el poder y sanear la economía. Personalmente, te doy gracias infinitas. Has encendido la chispa. Y ha prendido la llama que convertirá en cenizas la peligrosa mentira de la igualdad socialista. Hemos ampliado la consciencia, perfeccionando el potencial de las viejas herramientas. ¡Y todo lo que hemos aprendido, a base de equivocarnos, en el camino! Bitcoin es capitalismo. Competencia, mercado, juego limpio. Pero sigue representando una menudencia frente a la vanidosa hoguera de la macroeconomía. Si no abrazamos el consenso, más allá de nuestros egos, nos derriban de un plumazo nuestros otros hermanos, que, cegados por el miedo, se empeñan en controlarnos. En ese Gran Hermano, Facebook, Google y Amazon serían los nuevos bancos. Mundiales, omnipotentes, centralizados. En lugar de pelearnos, deberíamos concentrarnos en transmitir este legado. Yo quiero un mundo descentralizado. Lejos de colores, símbolos y uniformes, respetemos y abracemos la multiplicidad de visiones que puedan poner a prueba nuestras propias opiniones.

Para construir una casa, conviene comenzar por los cimientos. Establecer en la base unos sólidos fundamentos. Grabar en piedra el protocolo para asegurar su perdurabilidad en el tiempo. Bitcoin, desde el principio, funcionaba. Y ahora, además, escala, y lo hace de manera ilimitada. ¡Bienvenidos al hiperespacio! Comienza una nueva era. Metanet, en menos de un año, conjuga todo lo que, personalmente, llevaba tiempo buscando, vagando a la deriva entre cadenas de bloques que prometían y prometían pero nunca acababan de desinfectar la economía. Desde hace unos meses, Bitcoin ha vuelto. Y todo este humo se disipará con el viento. El dinero *p2p* no había muerto. En menos de lo que canta un gallo, hemos visto nacer sobre su cadena servicios como Twitter, Google, GitHub, Instagram, Youtube, identidad digital y hasta registros, contratos o licencias. Y la posibilidad de programar de manera automática nuestras contribuciones a Hacienda. Aplicaciones asentadas sobre piedra, no más castillos de arena. Grabando de manera inmutable nuestros datos en la red eterna. Recuperando nuestras pertenencias. Privacidad. Descentralización. Transparencia. En la *blockchain* cabe todo. Replicado en una red distribuida de múltiples nodos. En esta nueva dimensión, los usuarios constituyen los dueños de su propia información. Y la pueden monetizar a conveniencia durante el resto de su longeva existencia.

Llega la edad de la transparencia. La corrupción ya no se silencia. Se acabaron los tiempos de HODL, comienza la prueba de trabajo. Puedes hacerte rico, pero tendrás que demostrarlo: aquí se gana pasta currando. Y los micropagos resultan instantáneos. Ha llegado la hora de desvelar las ficciones, desenmascarar el anonimato, dejarnos de Satoshis y Piratas Roberts y mirarnos a los ojos, sin lamentos ni rencores, perdonándonos en los otros, para buscar juntos soluciones que transformen nuestras vidas, facilitando la maltrecha economía de comunidades y familias. Reguladores y gobiernos: si venís a poner obstáculos, no habéis entendido el juego. Para sacar tajada, id tomando

posiciones, construid herramientas sobre la cadena de bloques que solucionen problemas, creando mundos mejores, facilitad el proceso de adopción para así atraer la riqueza y la innovación.

El nuevo juego es imparable y se juega con reglas matemáticas que trascienden jurisdicciones. Y, aun así, el Bitcoin original cumple al pie de la letra todas las regulaciones, enmendando la avaricia de los malos actores. Tratar de controlarlo, apropiárselo o perseguirlo significa prolongar absurdamente el conflicto y seguir alimentando la lucha interna contra nosotros mismos.

Las matemáticas no conocen fronteras ni naciones, y como ciencia exacta no admiten injusticias ni corrupciones. Conviene pisar el suelo, mantenernos en el centro, recomponer energías, actualizar paradigmas, observar con amplitud de miras, y confiar en que, más allá de las mentiras, emerge una red distribuida, que se extiende y se replica, y muchos dicen que la entienden pero pocos **te la explican.**

Ya nadie se cree el argumento de la reserva de valor. La nueva estafa piramidal se llama HODL: comprar y mantener, y luego convencer a otros para que compren después, a medida que aumenta la escasez. Poco a poco, se va agotando el interés de compra en BTC. ¿Quiénes serán esta vez los primeros en vender? Bitcoin no se diseñó para quedarse inerte, inflando su valor a base de tethers para usurpar la riqueza de los siguientes. El valor se lo da la utilidad, la infinita posibilidad de sembrar, sobre terreno fértil, un nuevo vergel para la humanidad.

Digan lo que digan los medios, atados de pies y manos por la voluntad de sus dueños, Craig Steven Wright es Satoshi. Y BSV, el único Bitcoin verdadero. Hemos regresado al protocolo original. El destino nos ofrece una nueva oportunidad. Yo, por mi parte, no la pienso desaprovechar. Metanet ha roto aguas, y nada ni nadie lo pueden controlar. Y es que, desde el otro lado del espejo, una vez que te adentras en la madriguera del conejo, ya no existe vuelta atrás.

«Si crees que el gobierno no puede detener ninguna criptomoneda, te equivocas. Bitcoin funcionará porque se mantiene dentro de la ley de una manera que permite a la mayoría de las naciones establecer políticas. Bitcoin no ayuda a los gobiernos corruptos; para tales gobiernos, Bitcoin sería su peor pesadilla. Pero cuando un país sigue el estado de derecho, la rendición de cuentas, el gobierno abierto, la resolución judicial accesible e imparcial, y leyes justas y estables, Bitcoin puede ayudar a promover una sociedad mejor».

CRAIG S. WRIGHT

JURIDI&CO

PAULA PASCUAL CORTÉS

Identidad digital: dónde estamos y a qué retos regulatorios nos enfrentamos

Hoy en día, uno de los puntos críticos de los que más se habla alrededor de *blockchain* es la identidad digital. Y es que supone una base necesaria para que muchos de los casos de uso que se relacionan con esta tecnología puedan ser implementados de forma exitosa.

De hecho, hay pocos aspectos más centralizados para una sociedad y una economía actual que la identidad. Sin una forma de identificarse entre nosotros y nuestras posesiones, difícilmente podríamos construir grandes naciones o crear mercados globales. Desafortunadamente, existen problemas persistentes, y cada vez más graves, en la forma en la que funciona la identidad digital.

Por razones históricas y de otro tipo, la experiencia de la identidad digital actual está fragmentada, con pocos estándares o interoperabilidad, y es insegura, como nos lo recuerdan los informes casi diarios de *hackeos* y violaciones de datos. Para las personas, pero también para las empresas y los gobiernos, el *statu quo* se está volviendo cada vez menos sostenible. Por otra parte, la representación de esa identidad a través de documentos físicos hace que perdamos el control de la misma, pues no podemos tener certeza de quién cuenta en este momento con documentos que señalan nuestra identidad por cualquier parte del mundo (seguro que más de uno ha perdido en algún momento un documento identificativo).

La centralización aquí no significa que haya una fuente central para las identidades digitales, sino que las identidades digitales casi siempre son proporcionadas por alguna autoridad de terceros (a menudo una empresa privada) para un propósito específico propio. La información de identidad está «centralizada» dentro de esa entidad, y es aquí donde la *blockchain* y su *Self-Sovereign Identity* (SSI) juegan un papel clave.

En un enfoque de SSI, el usuario tiene tanto un medio para generar y controlar identificadores únicos (DIDs) como algunas instalaciones para almacenar datos de identidad. Los usuarios pueden entonces hacer uso de los datos de identidad que deseen. Éstos podrían ser credenciales verificables, pero también podrían ser datos de una cuenta de redes sociales, un historial de transacciones en un sitio de comercio electrónico o declaraciones de amigos o colegas.

Esta capacidad de recopilar y hacer uso de la identidad de un amplio conjunto de fuentes puede ayudar a los usuarios a crear conjuntos ricos y variados de identidades digitales para ellos mismos. También les permite un control mucho más preciso que el que tienen hoy sobre qué información personal comparten y en qué contextos. Incluso podría abrir la puerta a nuevos modelos de negocio, lo que potencialmente permitiría a los usuarios monetizar sus datos personales si así lo desean.

«El plano regulatorio supone la mayor causa de paralización de proyectos, debido a la necesidad de encuadrar estas nuevas funcionalidades en marcos legislativos específicos».

A pesar de que no se requiere *blockchain* para la identidad descentralizada, puede ser una solución poderosa para diferentes aspectos del marco de identificación descentralizado. Esto incluye respaldar la creación y el registro de DID, certificar las credenciales, proporcionar una infraestructura descentralizada para el control de acceso y el consentimiento del uso de datos, y vincular las credenciales con los contratos inteligentes para, por ejemplo, activar pagos automáticos.

¿Y a qué retos se enfrenta la SSI?

Como en casi todos los casos de uso que podamos encontrar en *blockchain,* el plano regulatorio supone la mayor causa de paralización de proyectos, debido a la necesidad de encuadrar estas nuevas funcionalidades en marcos legislativos específicos. Aquí, uno de los grandes retos a los que se enfrenta la identidad digital en *blockchain* es el cumplimiento con el Reglamento General de Protección de Datos y, sobre todo, por la caracterísitica de inmutabilidad inherente que posee *blockchain.*

Si queremos realizar un análisis más exhaustivo sobre los puntos críticos que quedan por definir para que estas soluciones puedan empezar a ser operativas, debemos nombrar los siguientes:

– Qué datos deben incluirse *on-chain* y qué datos *off-chain.* La mayoría de soluciones proponen que los datos de los usuarios, así como los *claims/credentials* que sean emitidos por un *issuer,* nunca estén grabados en *blockchain* sino en un sistema de almacenamiento diferente.

Sobre este tipo de almacenamiento se contemplan diferentes soluciones, como almacenamiento personal en un dispositivo móvil (con el riesgo asociado de que, si pierdo el dispositivo, pierdo los documentos que acreditan mi identidad), almacenamientos distribuidos tipo IPFS (con el riesgo asociado de perder la clave privada que desencripta los datos almacenados) o almacenamientos *on-premise* de proveedores de identidad (delegando la custodia en un tercero de confianza). Por ejemplo, soluciones como Alastria o Sovrin (basado en Hyperledger Indy) tienen fijado de momento un almacenamiento en el dispositivo móvil del usuario. Por ahora, es un planteamiento que puede ser utilizado para poder lanzar las soluciones. Sin embargo, y mirando en el largo plazo, este sistema conlleva un riesgo demasiado elevado.

– Cómo se realiza la compartición de datos entre diferentes agentes de forma que garantice una privacidad completa al usuario. Este punto tiene en cuenta cómo los agentes van a intercambiar esos *claims/credentials* sin que se pueda establecer una correlación entre las transacciones, comprometiendo la privacidad del usuario.

Aquí, la Comisión Europea ha dejado claro que el punto clave para la determinación del cumplimiento de la privacidad es el grado de correlación entre las diferentes actividades realizadas por el usuario. Es decir, debe ser imposible trazar las diferentes relaciones que tiene el usuario, con las que ha compartido ciertos atributos.

En este punto, las diferentes soluciones presentadas sí que difieren unas de otras. Por ejemplo, Sovrin propone un sistema de múltiples DID (identificadores descentralizados), únicos para cada relación y propósito con el que compartimos los datos, con el fin de que no utilicemos el mismo identificador para todas las relaciones y que sea imposible trazarnos dentro de la red.

Es decir, imaginemos que necesito acreditar que soy solvente, por lo que necesitaré acreditar un atributo por el que se emitirá un *claim* de mi entidad bancaria *(issuer)* porque necesito

acreditarlo ante la empresa en la que quiero alquilar un coche *(service provider 1)* pero también porque voy a solicitar una hipoteca en otro banco que no es el mío *(service provider 2).*

En este ejemplo, utilizaré un DID para compartir el *claim* con el *service provider 1,* y utilizaré otro diferente para el *service provider 2,* de forma que no se pueda trazar que es la misma persona la que va a alquilar un coche y solicitar una hipoteca.

Por otro lado, Alastria (un modelo que intenta convertirse en el estándar europeo) propone un sistema con un único identificador (Alastria ID) pero mediante un sistema de doble *hash,* de forma que no es posible trazar una misma credencial desde que es emitida por un *issuer* hasta que es presentada a un *service provider.*

El funcionamiento de este sistema se resume en que el usuario siempre tiene el mismo Alastria ID. Sin embargo, cuando un *issuer* emite un *claim* o *credential,* añade al *hash* su Alastria ID (que funciona como un *nonce*). De esta forma, hay un doble proceso de *hasheado* desde que se emite un *claim* hasta que se presenta a un *service provider,* garantizando la privacidad del usuario.

– Revocación y derecho al olvido de mis datos. Desde hace ya más de dos años, el derecho al olvido ha estado siempre presente en los debates sobre los distintos casos de uso de blockchain. Por eso, en este punto concreto, las soluciones analizadas ya han tenido muy en cuenta el RGPD. De hecho, es la razón por la cual los datos se encuentran almacenados en sistemas externos *off-chain* y tampoco se graban los *claims* emitidos por los *issuers,* de forma que se garantiza que ningún dato personal y privado se grabe en la cadena de bloques.

En cuanto al borrado de los datos almacenados en un sistema *off-chain,* dependerá de cuál sea el finalmente implementado. Por ejemplo, si se trata de un dispositivo móvil o una base de datos común, es sencillo ejercer este derecho. Sin embargo, nos encontramos con un debate muy interesante si lo que estamos implementando es un sistema de almacenamiento distribuido como IPFS.

Bajo mi punto de vista, el borrado de los datos se garantizaría con el borrado de la clave privada que permite descifrarlos (recordemos que los sistemas actuales se basan en una confianza por parte del usuario en que el *service provider* realmente está procediendo a la eliminación de los datos de su sistema, pero no tenemos acreditación de ello). No obstante, aquí parece que a la Comisión Europea no termina de convencerle este sistema para ejercer el derecho al olvido, ya que los datos se quedarían grabados, aunque no sea posible descifrarlos.

En definitiva, quedan todavía muchos puntos por definir (sobre todo los relacionados con el plano regulatorio) para poder contar con una solución de identidad digital que nos permita explotar el potencial de *blockchain* al máximo. Los esfuerzos por parte de las comunidades internacionales están siendo bastante importantes para poder crear un estándar que permita tener una identidad digital única. Y es que, de otra forma, si las empresas o consorcios trabajan por su cuenta sin tener en cuenta estos estándares (como, por ejemplo, w3c), nos encontraremos con silos de soluciones que no llegarán a ninguna parte.

Una identidad desagregada y no controlada por el usuario es lo que ya tenemos, por lo que el verdadero desafío es trabajar sobre una base común que permita utilizar una única identidad para todos los agentes con los que debamos compartir esta información. Aquí está el verdadero reto de *blockchain* y las empresas.

«Los esfuerzos por parte de las comunidades internacionales están siendo bastante importantes para poder crear un estándar que permita tener una identidad digital única».

Florian Bohnert

CMO EMURGO

En esta ocasión entrevistamos a dos representantes del proyecto Cardano: Florian Bohnert y Antonio Sánchez. Florian representa a EMURGO, uno de los tres pilares del proyecto, encargado de integrar toda clase de negocios empresariales en la *blockchain* de Cardano. Asimismo, buscan inversores y asociaciones con organizaciones que opten por utilizar Cardano como ecosistema.

Además de apoyar y ayudar al desarrollo, son los creadores de Yoroi, la *wallet* ligera de Cardano, y el último explorador de su cadena de bloques, Seiza.

Florian Bohnert, que lleva en Asia desde 2010, es el director de *marketing* de EMURGO. Su principal misión ha sido mejorar las condiciones ambientales gracias a la tecnología. Por ello, antes de entrar en EMURGO, fue el encargado de dirigir el negocio de bicicletas eléctricas Unicorn Mobike, además de crear alianzas públicas y privadas para el medio ambiente con MasterCard o la ONU. Florian se ha especializado en estudios del medio ambiente, tiene un máster en Administración de energía ecológica, y otro sobre Movilidad sostenible.

Cardano existe desde hace ya bastante tiempo. ¿Puedes hablarnos sobre los orígenes, la visión y la piedra angular del proyecto?

Cardano es un proyecto de *blockchain* pública de código abierto iniciado en 2015 por un consorcio de inversores y fundadores que querían abordar las cuestiones de escalabilidad, sostenibilidad e interoperabilidad presentes en las cadenas de bloques de primera y segunda generación. Se trata de una plataforma *blockchain* de tercera generación que busca ofrecer más funciones avanzadas que cualquier otro protocolo desarrollado anteriormente. Está desarrollada para durar generaciones y manejar la escalabilidad, la sostenibilidad y la interoperabilidad requeridas en una plataforma *blockchain* pública que ejecute muchas aplicaciones de datos intensivos para las partes interesadas. El equipo de desarrollo está formado por un colectivo global de ingenieros e investigadores expertos. EMURGO, como brazo comercial oficial de Cardano, ha tomado la iniciativa de comercializar el ecosistema de Cardano con un conjunto diverso de accionistas que desean una cadena de bloques de tercera generación a prueba de futuro que sirva mejor a sus mercados.

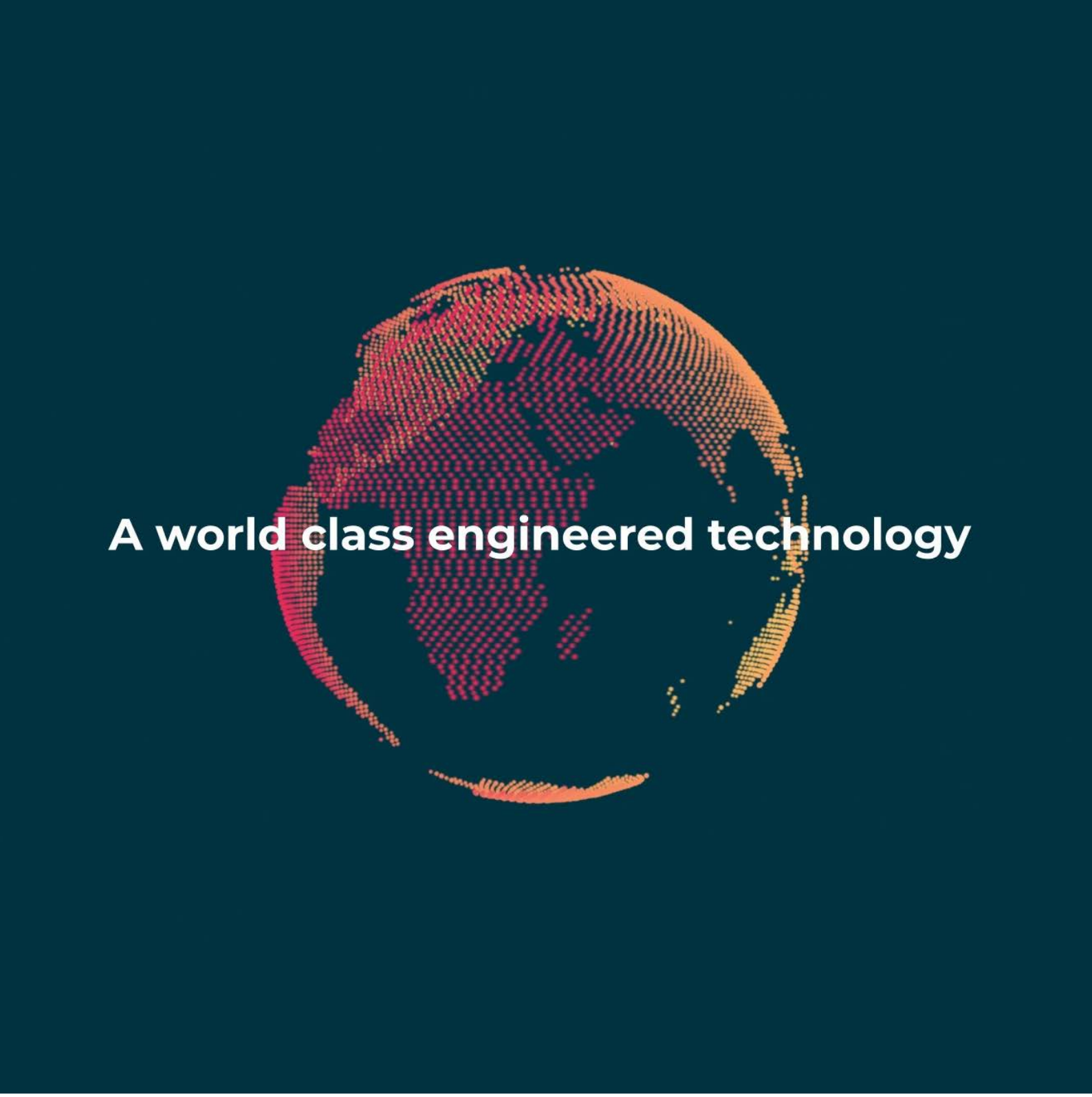
¿Quiénes son los principales actores que dirigen la iniciativa?

Cada entidad se formó en un principio para centrarse en diferentes roles durante la construcción del ecosistema de Cardano. Cada una de ellas se encuentra separada y son totalmente independientes entre sí, pero todos nos esforzamos por construir Cardano y trabajar juntos de manera cercana. EMURGO es el brazo comercial oficial de Cardano y reúne a empresas, desarrolladores y partes interesadas en el ecosistema para impulsar la adopción de Cardano. IOHK es responsable del desarrollo técnico del protocolo y se centra en las normas técnicas. Y la Fundación Cardano es una rama sin fines de lucro de Cardano enfocada en la gestión de la comunidad, trabajando en temas de estándares y cumplimiento, y asegurando la responsabilidad de las partes interesadas.

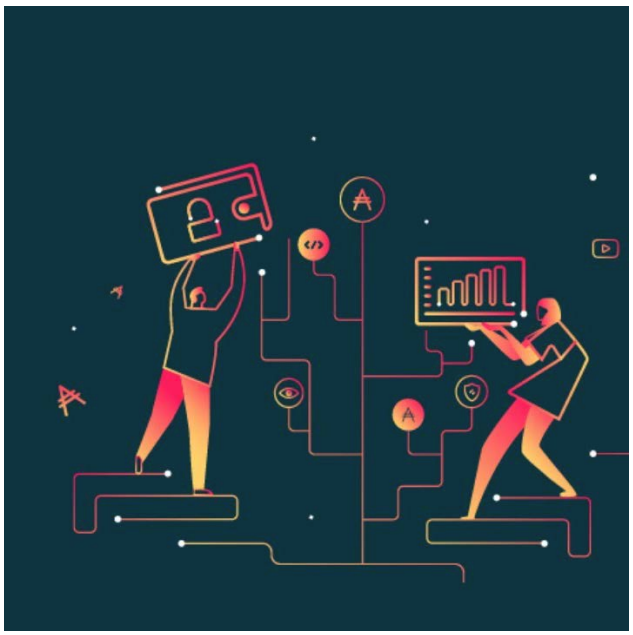
¿Qué hace que Cardano sea único y diferente de otras implementaciones de cadenas de bloques?

Cardano es la primera cadena de bloques de tercera generación que evoluciona a partir de una filosofía científica y un enfoque impulsado por la investigación. Como tal, Cardano se basa en dos principios fundamentales:

1. Utiliza la revisión por pares mediante la participación en conferencias académicas y de criptografía a gran escala, la participación de universidades líderes y la redacción de informes técnicos adecuados.
2. Implementa código de alta seguridad utilizado en los niveles más altos de la ingeniería científica para proporcionar una plataforma de cadena de bloques sostenible.



Estos dos principios fundamentales hacen que Cardano se destaque como una plataforma pública de *blockchain* rigurosamente probada y a prueba de futuro que es escalable, sostenible e interoperable.



¿Cuáles son las principales áreas de negocio y clientes que Cardano pretende abordar?

Cardano es un proyecto completamente de código abierto y puede ser adoptado por cualquier persona interesada en implementar la primera cadena de bloques de tercera generación en su mercado vertical. Como Cardano está diseñado para ser escalable, sostenible e interoperable, se alinea con las necesidades del gobierno, instituciones públicas y privadas, empresas y desarrolladores que manejan una gran cantidad de datos. Las entidades que lideran el desarrollo de Cardano también se centran en proporcionar más oportunidades en mercados subdesarrollados y desarrollar mercados a través de cursos de educación para desarrolladores de cadenas de bloques y, en última instancia, en ayudar a los no bancarizados con un sistema justo y transparente. EMURGO ha abierto un curso de educación de *blockchain* para una amplia gama de clientes a través de EMURGO India, ha organizado *hackatones* en Tokio y trabaja en estrecha colaboración con varias universidades indonesias a través de EMURGO Indonesia.

¿Cuáles son las principales características de la prueba de participación (PoS) de Ouroboros y cómo se protege la red contra ataques e infracciones?

Ouroboros está en la base de la cadena de bloques descentralizada de Cardano. Se trata de un nuevo y seguro protocolo de prueba de participación (PoS). Ouroboros permite a los grupos de interés de ADA ayudar a actualizar y mantener seguro el libro de contabilidad público de Cardano con todas las transacciones que tienen lugar entre las personas a nivel mundial. Todo esto se conseguirá sin necesidad de consumir la misma cantidad de recursos que Bitcoin. Es uno de los protocolos de consenso más eficientes en cuanto a recursos en el espacio, y es el primero que se ha probado seguro de una manera criptográfica muy rigurosa que ha pasado por una revisión por pares. Ouroboros también está diseñado para ser resistente a la radiación cuántica y las futuras versiones están siendo revisadas por expertos académicos.

Por lo tanto, Cardano está construido para durar generaciones, ser a prueba de futuro y constituir una plataforma que acoja a millones de usuarios en todo el mundo.

Las comunidades de habla hispana están deseosas de ponerse al día con el proyecto e incluso involucrarse con una actitud proactiva. Después de haber realizado el primer evento de Cardano España en enero de 2019, ¿cuáles son los planes para mantener el contacto y aprovechar estas comunidades en España y América Latina?

EMURGO aprecia mucho a nuestra comunidad global y apoya de todo corazón los esfuerzos para aumentar el conocimiento de Cardano en varios mercados. Algunas de las metas a corto plazo de EMURGO son hacer más promoción, eventos y conferencias de Cardano en las comunidades de habla hispana y producir más contenido en español también. Es muy grato escuchar que hay una creciente comunidad de hispanohablantes seguidores de Cardano y EMURGO. Si desean ayudar para organizar un *meetup* o para traducir el contenido al español, no duden en ponerse en contacto directamente con nuestro CMO en el correo electrónico **florian@emurgo.io.**

En comparación con las regulaciones de Wyoming relacionadas con *blockchain*, ¿se han puesto al día otras jurisdicciones en Europa y América Latina para atraer a los negocios relacionados con las cadenas de bloques?

EMURGO está constantemente investigando y manteniéndose al día con las últimas noticias y tendencias en la industria *blockchain.* EMURGO también se unió recientemente a la Cámara de Comercio Digital de EE UU como miembro del Comité Ejecutivo para facilitar el diálogo con los principales responsables políticos sobre la promoción de políticas favorables a las cadenas de bloques. Cada jurisdicción del mundo sigue avanzando a su propio ritmo en lo que respecta a la tecnología *blockchain* y algunas son muy positivas en cuanto a la aplicación

de una regulación que favorezca las cadenas de bloques. EMURGO publica constantemente contenido útil sobre los últimos desarrollos en regulaciones y tendencias alrededor del mundo. Con respecto a los observadores a corto plazo en Europa, la UE parece dispuesta a debatir para ver qué valor pueden aportar.

Por lo tanto, enfatiza la importancia de aumentar la conciencia sobre Cardano y la cadena de bloques como un todo para educar a los accionistas potenciales sobre la utilidad real que Cardano y la *blockchain* pueden ofrecer sobre los procesos existentes. El contenido de EMURGO, reuniones, conferencias y entrevistas como ésta son esenciales para atraer interés a Cardano y a nuestra industria de la cadena de bloques como un todo.

Háblanos un poco de dLab y a qué tipo de proyectos empresariales se dirige.

Nuestro acelerador de *blockchain* dLab/EMURGO en Nueva York fue lanzado en febrero de 2019 con el primer lote que consistía en cuatro *startups* y un par de socios de Cardano. Esta primera tanda se «graduó» recientemente del programa y estamos buscando otras empresas prometedoras para acelerar. EMURGO está dirigido a empresas que muestran un gran potencial de negocio, sinergias con el ecosistema de Cardano, y que han alineado sus objetivos de proporcionar equidad, inclusión y oportunidad. Estas nuevas empresas se enfrentan a problemas del mundo real y requieren un protocolo fuerte capaz de ser escalable, interoperable y sostenible.

Por ejemplo, una de las empresas que se «graduó» en nuestra primera tanda, Helixworks, puede mejorar y aumentar los estándares tecnológicos utilizados en toda la industria de la cadena de suministro global en el futuro. Dado que hay muchos componentes humanos en todo el proceso a lo largo de la cadena de suministro, Helixworks puede proporcionar un valor esencial. En un ejemplo particular, Helixworks puede rastrear cada grano de café y probar que un café tostado específico es genuino y auténtico de acuerdo con las etiquetas de identificación basadas en ADN que se integrarán en una cadena de bloques. La incorporación de la *blockchain* en la industria de la cadena de suministro permitirá una mayor creación de riqueza para todas las partes interesadas.

La transparencia crea más confianza, lo que significa que los clientes estarían dispuestos a comprar más productos o productos más fiables a precios más altos, beneficiando así a toda la cadena de valor. Si podemos mostrar datos muy transparentes, los problemas actuales que existen en la industria de la cadena de suministro debido a incentivos desalineados y procesos tecnológicos obsoletos se resolverán por completo. La transparencia total beneficiará a los procesadores existentes, ya que también añadirá valor a las tiendas minoristas y a las cafeterías. Aumenta la confianza entre el minorista y el cliente, aumentando así las ventas. A medida que esto haga que los procesadores envíen más, habrá un efecto dominó de beneficios en forma de aumento de la demanda de trabajo e incremento de los beneficios.

«EMURGO promueve esta visión de Cardano y las utilidades que ofrece cuando se involucra con potenciales inversores que quieran adoptar Cardano como el protocolo de elección.»

Con muchos proyectos de cadenas de bloques en el mercado, ¿cuál es la visión de su interoperabilidad? ¿Cuál es la propuesta de Cardano?

Cardano realmente se propone abordar los problemas de escalabilidad, sostenibilidad e interoperabilidad de la cadena de bloques de la primera y segunda generación anterior. Cardano se construye con la idea de que no habrá una sola cadena de bloques/activo digital que será utilizada por millones de usuarios. Por lo tanto, la interoperabilidad o la capacidad de cualquier cadena de bloques para «hablar» con otra cadena de bloques o sistema heredado es una característica muy importante que debe ser abordada.

Actualmente, hay muchas cadenas de bloques diferentes en el espacio de las *blockchains* e incluso más sistemas heredados, como el antiguo sistema bancario que se utiliza en todo el mundo. Todos estos sistemas hablan su propio idioma y tienen sus propias reglas. No existe un solo estándar o forma de comunicación entre los diferentes sistemas tecnológicos.

Una de las filosofías centrales de Cardano es la de ayudar a «bancarizar a los no bancarizados», por lo que la interoperabilidad entre las cadenas de bloques y el sistema bancario heredado es necesaria para cumplir con esta visión, al menos en el futuro próximo. Dado que los dos sistemas son muy diferentes desde el punto de vista tecnológico y con respecto a las normas reguladoras actuales, Cardano tendrá la capacidad tecnológica necesaria para asegurarse de que las partes interesadas cumplan con las normas y, al mismo tiempo, preserven la privacidad de los datos de forma responsable.

EMURGO promueve esta visión de Cardano y las utilidades que ofrece cuando se involucra con potenciales inversores que quieran adoptar Cardano como el protocolo de elección.

EMURGO

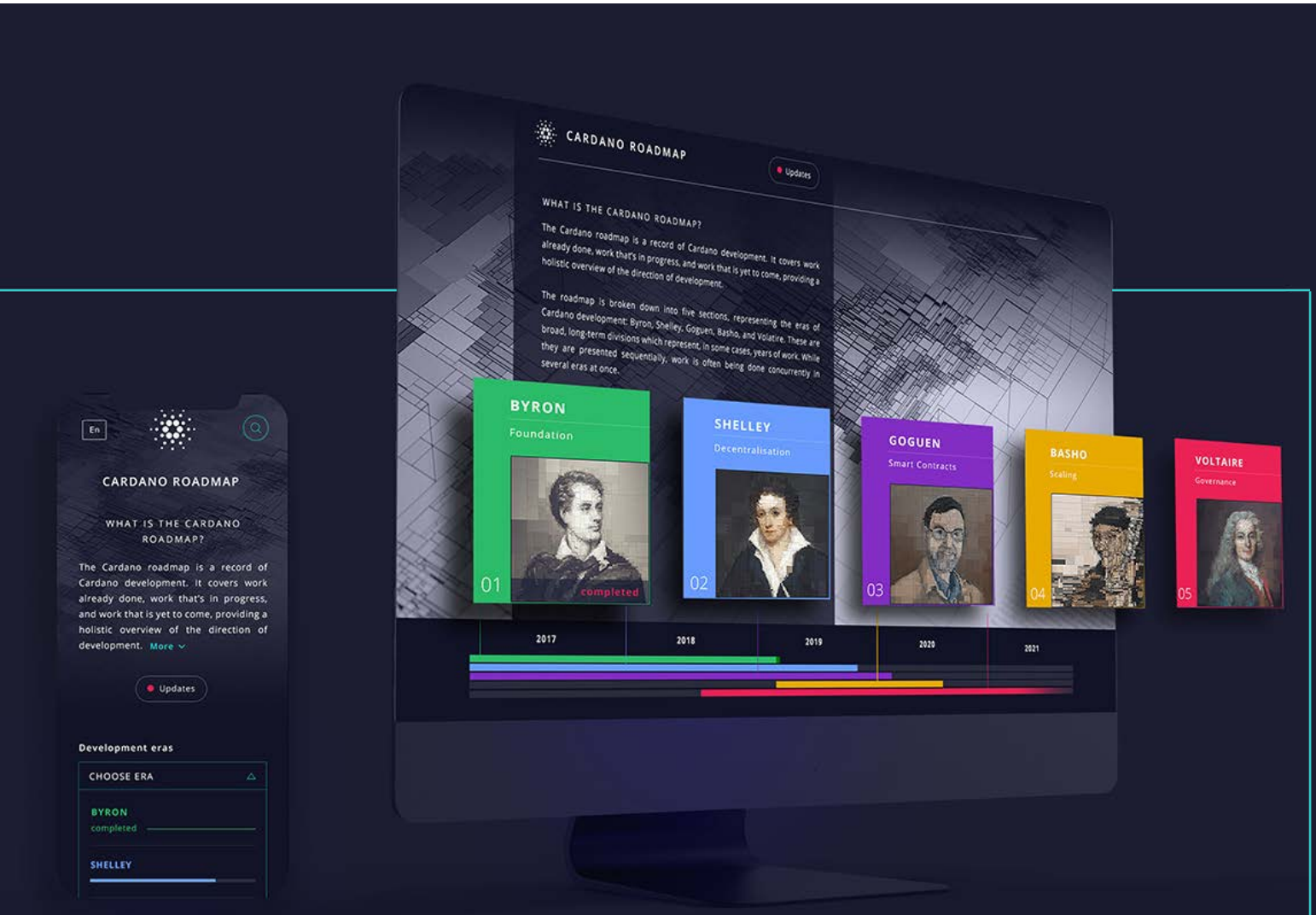
ENTREVISTA

Antonio Sánchez

EMBAJADOR CARDANO

Aparte de ser miembro de ÁGORA, es el primer embajador de Cardano en España. Fiel seguidor desde casi antes de que naciera, ya que sigue a su CEO Charles Hoskinson desde que dejó Ethereum, tiene la misión de promover la adopción de este proyecto, así como ayudar a resolver dudas sobre la *blockchain* de Cardano o crear contenidos que apoyen e informen a los seguidores del proyecto.

«El día en el que Cardano esté finalmente lanzado con Voltaire, tendremos una de las soluciones *blockchain* más avanzadas y potentes del mercado»



¿Quién es Antonio Sánchez?

Os voy a contar mi historia. Yo empecé conociendo Bitcoin gracias a uno de mis profesores del módulo de Informática, en el cual yo estudiaba en 2010. Este profesor nos habló del nuevo dinero digital, y me llamó mucho la atención. En aquel entonces, yo navegaba mucho por la *deep web* y era un asiduo en el IRC. Ahí es donde empecé a conocer más aún el poder de Bitcoin, y lo que estaba a punto de nacer: la era de la *blockchain.*

Quien me conozca sabrá que siempre me ha encantado el cacharreo: montar y desmontar cosas. Por ello, siempre he estado practicando y estudiando sobre el funcionamiento y montaje de nodos, desde el primero de Bitcoin que monté hace años, hasta el ultimo de Storj que monté ayer mismo. Siempre he tenido varios, y siempre para apoyar los proyectos y ayudar a su descentralización.

Soy autónomo, tengo una empresa de servicios y seguridad informática, y principalmente llevo el mantenimiento de sistemas y redes en varios institutos de Almería. Me encargo de todo lo relacionado con el mantenimiento informático, montaje de redes y reparación de equipos informáticos. Por mis conocimientos y prácticas, soy unos de los miembros dentro del grupo principal de la *testnet* de Shelley, donde analizamos el funcionamiento del futuro PoS de Cardano.

He de decir que el trabajo de IOHK es impecable: han surgido algunos errores en las etapas vistas hasta ahora, pero se han solventado rápidamente. Shelley va por muy buen camino, tenemos que estar contentos de poder construir algo tan bueno, y que en breve se lance la *mainnet* para poder delegar nuestras ADA con el PoS y fortalecer así la descentralización del proyecto.

¿Tener que trabajar en Haskell puede limitar la participación de desarrolladores y la adopción de usuarios finales?

Hoy en día, creo que lo más importante del desarrollo y lo más esencial es la seguridad del código, y por desgracia actualmente supone un problema muy grave. Todos los meses leemos alguna noticia de algún contrato inteligente mal programado, o alguna brecha de seguridad en el código de alguna API. Por ello, Haskell es muy importante para este proyecto. Podemos verlo como el buen vino: no hay abundantes botellas pero su sabor es superior frente a los demás. Por eso, aunque no existan tantos desarrolladores de Haskell como puede haber en Java, lo veo más como una ventaja que como algo que limite al proyecto, porque Haskell da esa seguridad que otros lenguajes no aportan. Además, conviene añadir que todos los desarrollos de Cardano están revisados por pares.

Para los usuarios finales, es importante saber que no existen problemas con errores de escritura. Gracias a Haskell (pienso yo, como usuario también que soy), éstos estarán más tranquilos sabiendo que Cardano tiene como base un código seguro, y bien revisado.

¿Cuándo se prevé llegar al público?

La fecha final aún no está disponible para nadie. Estamos actualmente empezando la fase 2. Para que se entienda mejor, voy a comentar las tres fases que se desplegarán en la *testnet* de Shelley:

En la fase 1, se nos ha permitido montar un nodo propio, escrito en Rust, un lenguaje que personalmente me apasiona. Estoy intentando sacar tiempo para aprender algo más de este lenguaje, en el que Cardano también está trabajando. Al montar el nodo, dentro de nuestro equipo personal, establecimos una configuración básica, para ver cómo pueden operar los *pools.* He de decir que me ha sorprendido lo bien que ha salido todo, casi sin problemas, y con un soporte por parte de IOHK muy bueno.

Actualmente nos encontramos en la fase 2, donde pasamos a la interconexión entre los nodos de la *testnet,* para crear así una red de prueba unificada.

En la fase 3, la más esperada por todos, se agregaría el esquema de delegación, así como las recompensas e incentivos para los participantes honestos que componen la red.

Esas tres fases construyen la *testnet* de Shelley: vamos muy bien y avanzamos con buena letra, por lo que me atrevería a decir que antes de que termine el año tenemos Shelley implementada en la *mainnet,* pero también es posible que me pueda equivocar.

¿Se pueden desarrollar ya *dApps*? Existen librerías para conectar *backend/frontend* con nodos de Cardano, similar a las librerías existentes para otras cadenas de bloques?

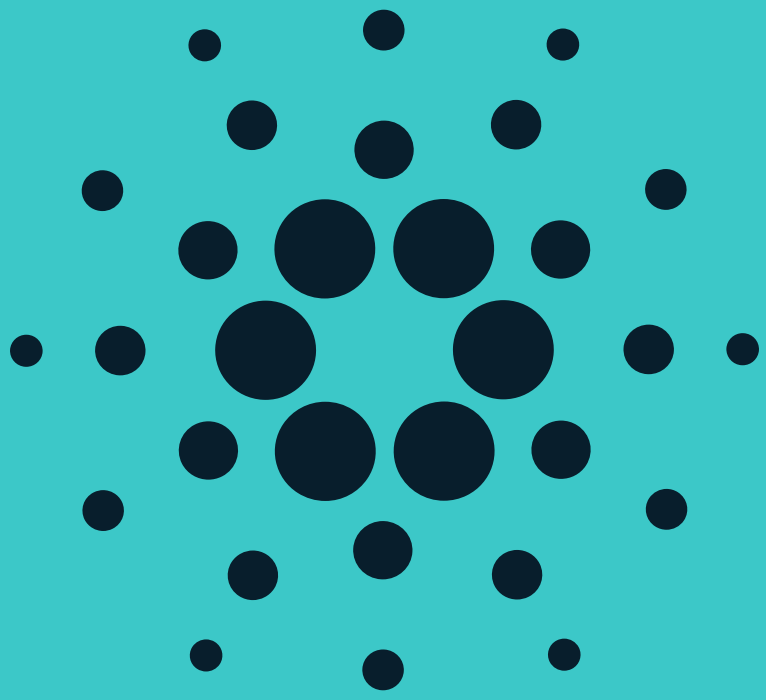
Actualmente no, todos sabemos que aún estamos en la *testnet,* pero sí que disponemos de muchísima información y herramientas para ir avanzando una vez sea lanzado. Cualquier desarrollador que quiera probar la *blockchain* de Cardano puede empezar estudiando Plutus, y así, una vez termine la *testnet,* construir contratos funcionales sobre su cadena.

También disponemos de IELE o KEVM, que voy a detallar de forma rápida. KEVM es una máquina virtual que nos permite experimentar con contratos inteligentes de Ethereum, añadiendo un rendimiento mejorado y más seguridad. Por su parte, IELE es otra máquina virtual, pero añade un mayor rendimiento, se basa en registros y no en pila como KEVM, que es muy importante a la hora de desarrollar, ya que podemos hacer contratos más baratos, gracias al menor coste de gas.

Para ir avanzando y posicionándose como desarrollador de esta *blockchain,* recomiendo ir familiarizándose con Plutus. Se trata de un lenguaje de programación funcional, basado en Haskell, que trabaja en la capa de liquidación de Cardano, y nos ofrece una seguridad mucho mayor que los lenguajes de programación de contratos inteligentes que conocemos hasta ahora.

Y, para quien no sea desarrollador, también dispone de una herramienta muy buena, llamada Marlowe, algo parecido a Scratch, que es un lenguaje de programación visual. Esta herramienta nos facilita la programación de contratos inteligentes de una manera mucho más sencilla que picar código, también bajo el lenguaje Haskell.

Creo que con todo lo mencionado respondo bien la pregunta, y añado una última opinión personal: el día en el que Cardano esté finalmente lanzado con Voltaire, tendremos una de las soluciones *blockchain* más avanzadas y potentes del mercado.



La verdadera historia de un auténtico fraude

LUIS MEIJUEIRO Y EMILIO TEREÑES

Se nota un hastío del consumidor... «Ya no te puedes fiar de nadie» o «todo el mundo miente» son quejas habituales. Mayoritariamente vivimos en ciudades, donde se vende de todo pero no se produce casi nada. El conocimiento directo, que antes se podía tener en los pueblos, sobre quién y cómo cultivaban los alimentos que comprabas, o de dónde venía la madera y cómo fabricaban tus muebles y utensilios, simplemente ya no existe.

Falsos artículos de lujo, falsos títulos de formación... ¡y hasta falsos huevos! De la misma forma que Frank, el protagonista de la película *Atrápame si puedes,* logró ganar mucho dinero engañando a la gente haciéndose pasar por quien no era, hay muchos otros Frank que tratan de engañarnos dándonos «gato por liebre» o algo que no se corresponde con lo anunciado.

De la mentira viven muchos; de la verdad, casi ninguno (nos hacen pensar a veces).

Las fábricas, fincas agrícolas y ganaderías están alejadas de nosotros, cuando no ubicadas en otros países, por lo que

necesitamos fiarnos de la información que nos llega desde complejas cadenas de transformación y distribución, en las que no es difícil que se produzcan errores, omisiones de información y hasta engaños o fraudes.

Para gestionar mejor la información de dichas cadenas de distribución, y poder dar mayor confianza al consumidor, las empresas involucradas pueden utilizar algún tipo de sistema de trazabilidad que, en definitiva, trata de mantener y actualizar un registro documental con la historia de los productos, con mayor o menor nivel de detalle. Esto puede llevar aparejado desde un proceso puramente manual de la información, en papel, hasta el empleo de sistemas TI más o menos complejos.

En general, el objetivo final de un sistema de trazabilidad es poder dar a los consumidores ciertas garantías acerca de la procedencia legítima y de una producción y distribución del producto conforme a las normas de calidad requeridas y a la legislación vigente que le sea de aplicación (sobre seguridad, etc.).

Blockchain veo, *blockchain* quiero

Y, cómo no, al calor del (pen)último avance tecnológico, en este caso *blockchain,* hay empresas como Alibaba, Carrefour, o hasta la cercana a nosotros Capsa Food, que anuncian estar probando, o planean introducir, una «trazabilidad con *blockchain*» para alguno de sus productos.

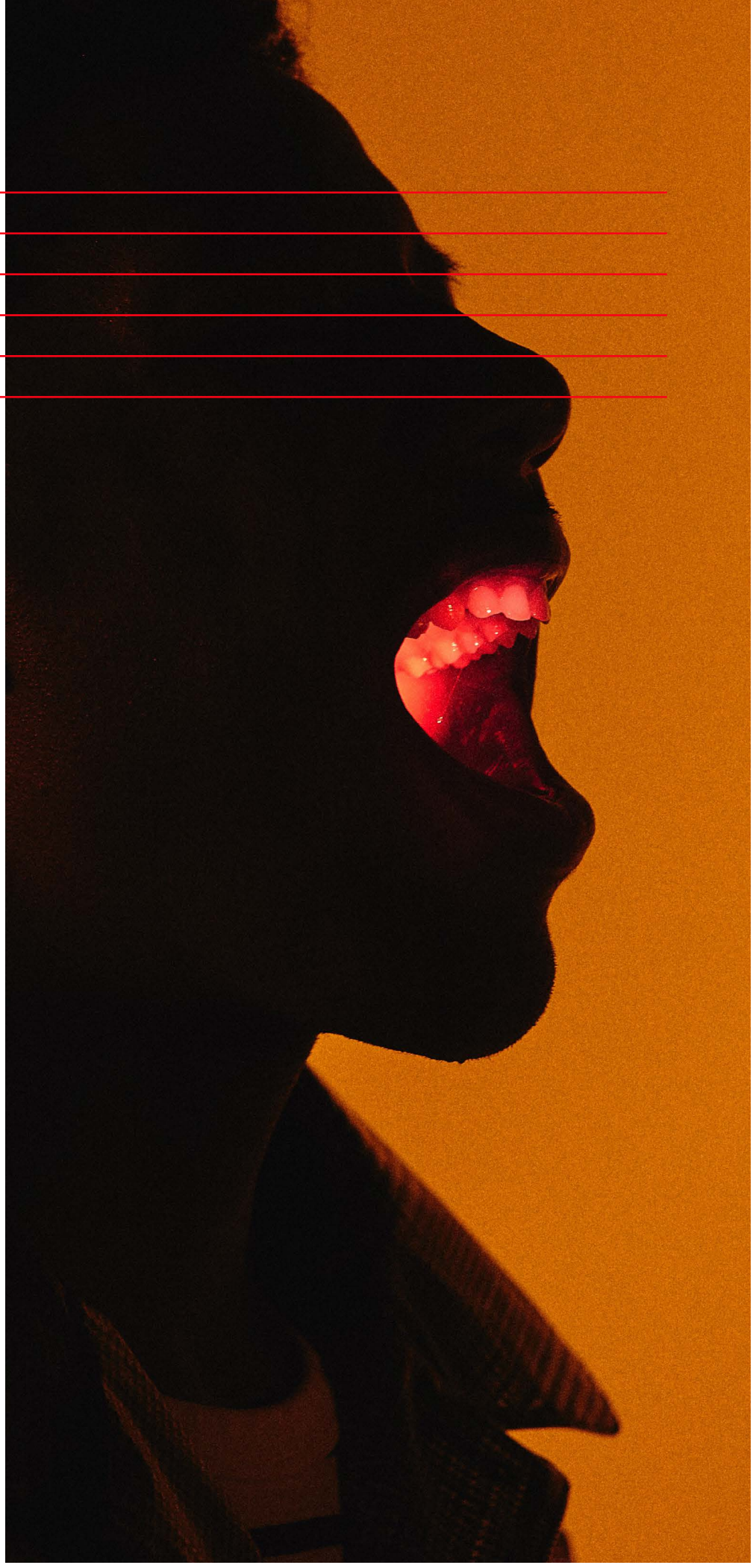
Sin dudar *a priori* de la veracidad de sus afirmaciones, lamentablemente no podemos comprobarlo observando de forma independiente el flujo de sus transacciones, es decir, la traza que realmente dejan en *blockchain.* La razón es que dichas empresas no usan una plataforma *blockchain* pública (como Ethereum o Telos), sino lo que algunos llaman «*blockchain* privada» o «*blockchain* permisionada» (ésta también conocida como «consorciada» o «federada»), una modalidad de registro distribuido que no suele permitir la consulta pública, ni mucho menos anónima, de sus transacciones.

Por ejemplo, en la aplicación de Carrefour para comprobar el origen de sus pollos camperos, se muestra una vista web con unos datos que pueden venir tanto de un sistema transaccional tradicional como de un registro en *blockchain.* El consumidor no tiene forma de comprobar por sí mismo los datos directamente en la plataforma *blockchain* (ni tampoco que sean ciertos, pero esta cuestión la dejaremos para más adelante).

¿Por qué cruzó el pollo la carretera? Quizás la respuesta esté en alguna blockchain...

Las empresas usuarias de esa plataforma «*blockchain* privada» quizás estén autorizadas a consultarla y hacer sus propias comprobaciones, pero entonces, ¿qué sentido tienen las campañas dirigidas al consumidor afirmando que usar *blockchain* les da «mayor visibilidad sobre la seguridad alimentaria, confianza y garantía sanitaria»? Quizás sean afirmaciones un tanto osadas, ya que, ¿de qué «confianza» se habla al privar al consumidor de poder verificar el sistema? En el fondo, ¿qué cambia respecto al tradicional sistema centralizado «sin *blockchain*»?

La transparencia es un atributo esencial del paradigma *blockchain,* y prescindir de ella simplemente da al traste con la confiabilidad del sistema, o de la solución propuesta.



Trazando gamusinos

No hace mucho, en un chat relacionado con *blockchain* en una conocida red social, un emprendedor pedía colaboración para desarrollar una innovadora idea de negocio: aplicar *blockchain* para certificar el origen de sus productos a la venta (¿nos suena de algo?). Se trataba de un producto cultivado que antes de su venta para consumo sólo precisa un empaquetado.

Su idea era que la gente pudiese «certificar visualmente» con su presencia la existencia del producto en una ubicación concreta, guardando la información correspondiente en *blockchain* como prueba de su veracidad.

Su propuesta era que cualquier persona, situada en la zona de recolección del producto, usase una aplicación *blockchain* desde su dispositivo móvil para «informar del producto mandando su geolocalización». A cambio recibiría una cantidad de *tokens* que podría acumular para canjearlos en el futuro por el mencionado producto.

Productos de nuestra tierra para su mesa. ¿Y quién te dice a ti que no vienen de otras tierras?

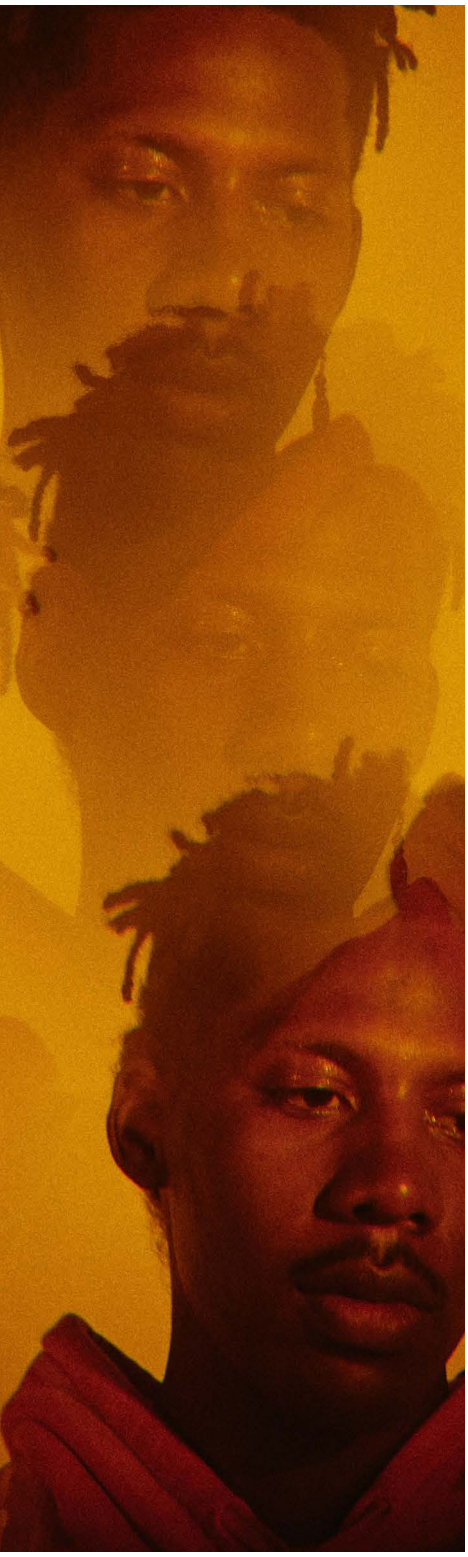
Sin embargo, no pretendía que la gente «fuese testigo» del origen de cada unidad de su producto, ni siquiera de una cantidad del mismo (lote). Simplemente pretendía que la gente dijese que un día concreto, en una determinada ubicación, su empresa había estado recolectando el producto, y «lo ideal, que cuanta más gente lo informe, pues mejor».

Le comentamos al emprendedor que lo que pretendía hacer no bastaba para garantizar al consumidor el origen de su producto, ya que, ¿qué impedía que llevase al supuesto lugar de recolecta cualquier cantidad de productos desde otro origen distinto?

A lo cual respondió desafiante: «Tampoco podemos estar seguros de que los certificados de origen que la Cámara de Comercio le expide a una empresa acrediten realmente que todo su producto proviene de un determinado país. Siempre se pueden hacer trampas».

Esto nos hace ver que solucionar problemas de trazabilidad tiene más que ver con mejorar los procedimientos y controles seguidos que con las tecnologías empleadas, las cuales pueden ser, eso sí, de gran ayuda, pero que no resuelven por sí mismas algo que fundamentalmente es de índole humana.

Espejito, espejito, ¿quién es el dato más bonito?



Si lo que verdaderamente se pretende es certificar el origen de algo, es imprescindible contar con fuentes de datos confiables, antes de poder «asegurar» esos datos mediante un registro en la *blockchain.* Si no puedes confiar en la veracidad de los datos, *blockchain* no va a cambiar eso. Únicamente te puede garantizar el momento de registro del dato, la cuenta que realizó el registro, y que *a posteriori* no ha sido manipulado. Pero si el dato era falso o incorrecto en el momento de su registro, falso continuará siendo cuando un *smart contract* o aplicación descentralizada lo trate.

Si no lo conocéis, os recomiendo ver el experimento de Terence Eden para aparecer como autor de *La Mona Lisa*... ¡porque lo dice una aplicación que usa *blockchain*! Esto que parece tan sencillo de entender, lamentablemente suele ser lo que se está intentando vender: que usar *blockchain* te soluciona la trazabilidad del producto, casi «por arte de magia».

Soy un pintor reconocido, y *La Mona Lisa* una de mis obras. *Blockchain* da fe de ello.

Pero la realidad es que la confianza la dará el mecanismo que se implemente para gestionar la trazabilidad, en el cual *blockchain* puede ser una pieza que ayude a lograr el objetivo, pero es el diseño global del sistema el que tiene que estar bien planteado.

Si los orígenes de datos son pocos, éstos tienen que ser extremadamente fiables, algo que muchas veces no es posible. Mientras que si los orígenes de datos son muchos, pueden establecerse niveles de fiabilidad y adoptar estrategias de *gamificación,* de red, para aumentar el grado de fiabilidad.

Llegados a este punto, os vendrá a la mente el concepto de «oráculos», algo que os pueden haber contado, o que hayáis leído, que podría mejorar la calidad de los datos de origen. Pero los oráculos de los que os hablan suelen ser sistemas tradicionales externos a *blockchain,* centralizados y habitualmente controlados por una sola entidad, por lo que, entonces, ¿por qué una *blockchain* iba a confiar en algo centralizado que no está bajo el control de su sistema de consenso y seguridad criptográfica?

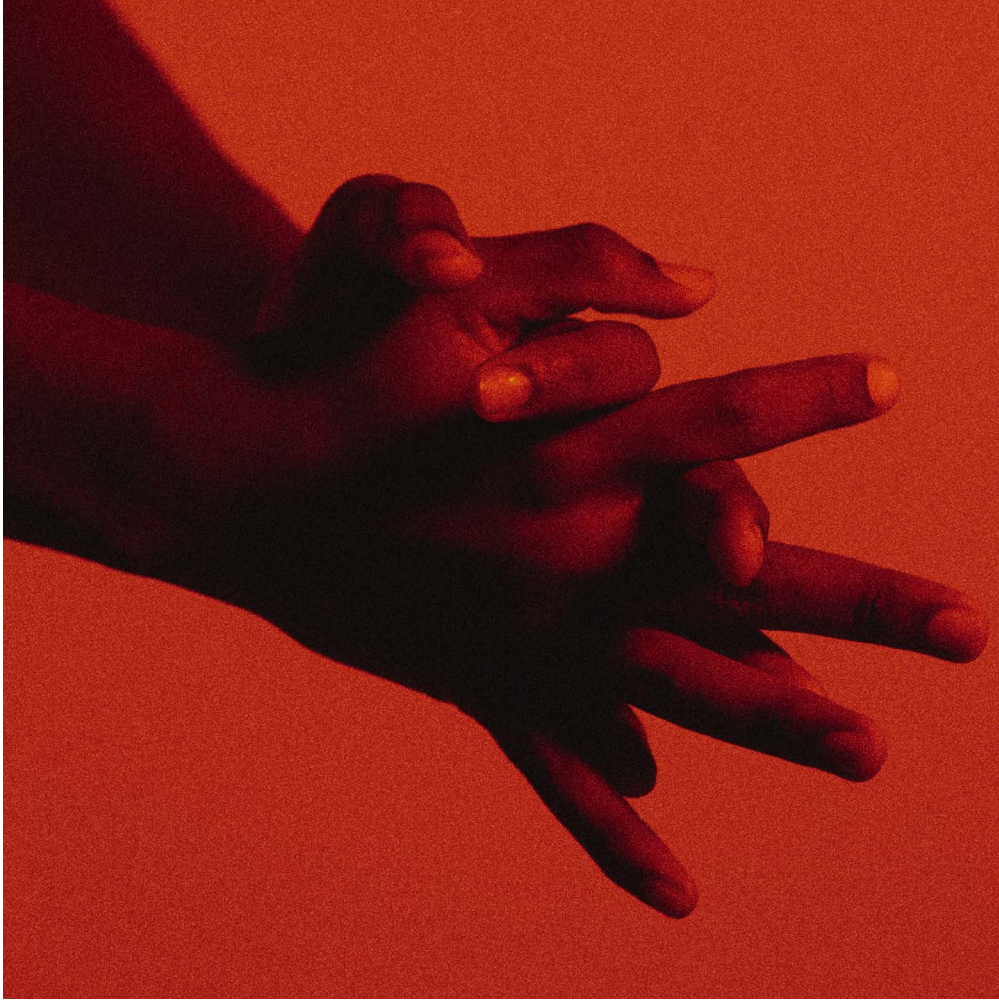
A nuestro juicio, los únicos «oráculos» a los que se podría otorgar un grado de confianza aceptable serían oráculos descentralizados, que son aquellos basados en un sistema de incentivos/*gamificación* capaz de controlar que los informantes (sistemas o personas) se comporten mayoritariamente de forma honesta (porque mentir no les conviene).

El sentido de *blockchain*

Al comenzar un proyecto de trazabilidad, no es extraño encontrarse con esta absurda situación, similar a una escena («Part I: The Miracle of Birth») de la película *El sentido de la vida* de los Monty Python:

Un desconocido hace su aparición: «¡Hola!»

¿Hemos preguntado al potencial consumidor del producto qué le preocupa realmente? ¿Qué información demanda? ¿Qué grado de confianza o desconfianza tiene en el origen y proceso de elaboración de un producto? ¿Si está dispuesto a pagar más por algo que podría no interesarle o necesitar? En CTIC, éstas son algunas de las primeras cosas que pedimos tengan en cuenta las empresas promotoras de un sistema de trazabilidad basado en *blockchain.*



Si yo fuese un producto, ¿qué destacaría en mi currículo y cómo se comprueba?

Como nos hemos cansado de repetir en muchas ocasiones, el término *blockchain* equivale a descentralización, y no sólo de las infraestructuras tecnológicas, sino también una descentralización de tipo decisorio o político. E implantar *blockchain* con éxito exige que todas las partes implicadas logren más beneficios que perjuicios. Y, para una cadena de producción y suministro, todos son todos, incluidos los consumidores finales.

La revolución que las tecnologías de Internet ha traído, tanto al mundo de los negocios como a la sociedad, ha sido posible gracias a su uso público, no a su aplicación en forma de Intranets privadas. Igualmente, en CTIC, desde que empezamos a investigar en el campo *blockchain* allá por el 2015, siempre hemos apostado por el empleo de plataformas *blockchain* públicas. Intentamos que el planteamiento inicial que tengan las empresas a las que ayudamos sea ése, porque creemos firmemente que es la forma en la que puede lograrse la verdadera utilidad y ventajas de su aplicación.

Por eso, para nuestros pilotos de aplicación y proyectos para clientes hemos trabajado principalmente con la plataforma pública Ethereum y más recientemente con plataformas basadas en el *software* EOS.io, como la *blockchain* pública de Telos, de la que formamos parte como entidad validadora, o en la «jerga» de la red, como productor de bloques (BP) bajo el nombre The Teloscope. Ambas plataformas *blockchain,* Ethereum y Telos, permiten variantes para despliegue y funcionamiento en modo «privado» o «permisionado», por lo que esto nos asegura que si finalmente los promotores del proyecto deciden no lanzarlo en modo público, los desarrollos serán compatibles.

Blockchain opera como una tecnología de infraestructura, no finalista. Más que aplicarse en la resolución de problemas puntuales, *blockchain* está destinada a formar parte de soluciones complejas, que muchas veces incluyen diversas tecnologías. Para ejemplificar esto, comparemos implementar *blockchain* con la aplicación de una tecnología de infraestructura como Internet, y una finalista como *Big Data,* en un problema concreto: la atención al cliente.

Si pensamos en cómo ha cambiado Internet las relaciones de atención al cliente, no podemos negar su importancia. Pero estos cambios han sido graduales y se han basado más en cambios de comportamiento que en soluciones puntuales. La instantaneidad de respuesta ya existía con los teléfonos de atención al cliente. En cambio, la cercanía, la espontaneidad y la difusión de las preguntas en redes sociales era algo difícilmente cuantificable, o inimaginable hace no demasiados años. Por su parte, la aplicación del *Big Data* al análisis de quejas resuelve problemas puntuales, sin alterar necesariamente al resto del proceso.

Y me dicen: «pon una queja por fax o en nuestra Intranet». Y yo partido de risa...

En CTIC consideramos que la aplicación de *blockchain* ha de ser transversal, y para sacarle partido las empresas han de estar dispuestas a adaptar su negocio al nuevo paradigma, y saber cómo hacerlo, algo en lo que también podemos ayudarles. De lo contrario, muchas correrán el riesgo de fracasar, como sucedió con grandes empresas en los albores de Internet, que incapaces de adaptarse, se vieron por ejemplo superadas por una pequeña tienda *online* de libros (Amazon).

Volviendo al sentido que puede tener *blockchain,* aplicada al campo de la trazabilidad u otros, desde nuestro punto de vista, las principales características que ha de tener una buena solución son:

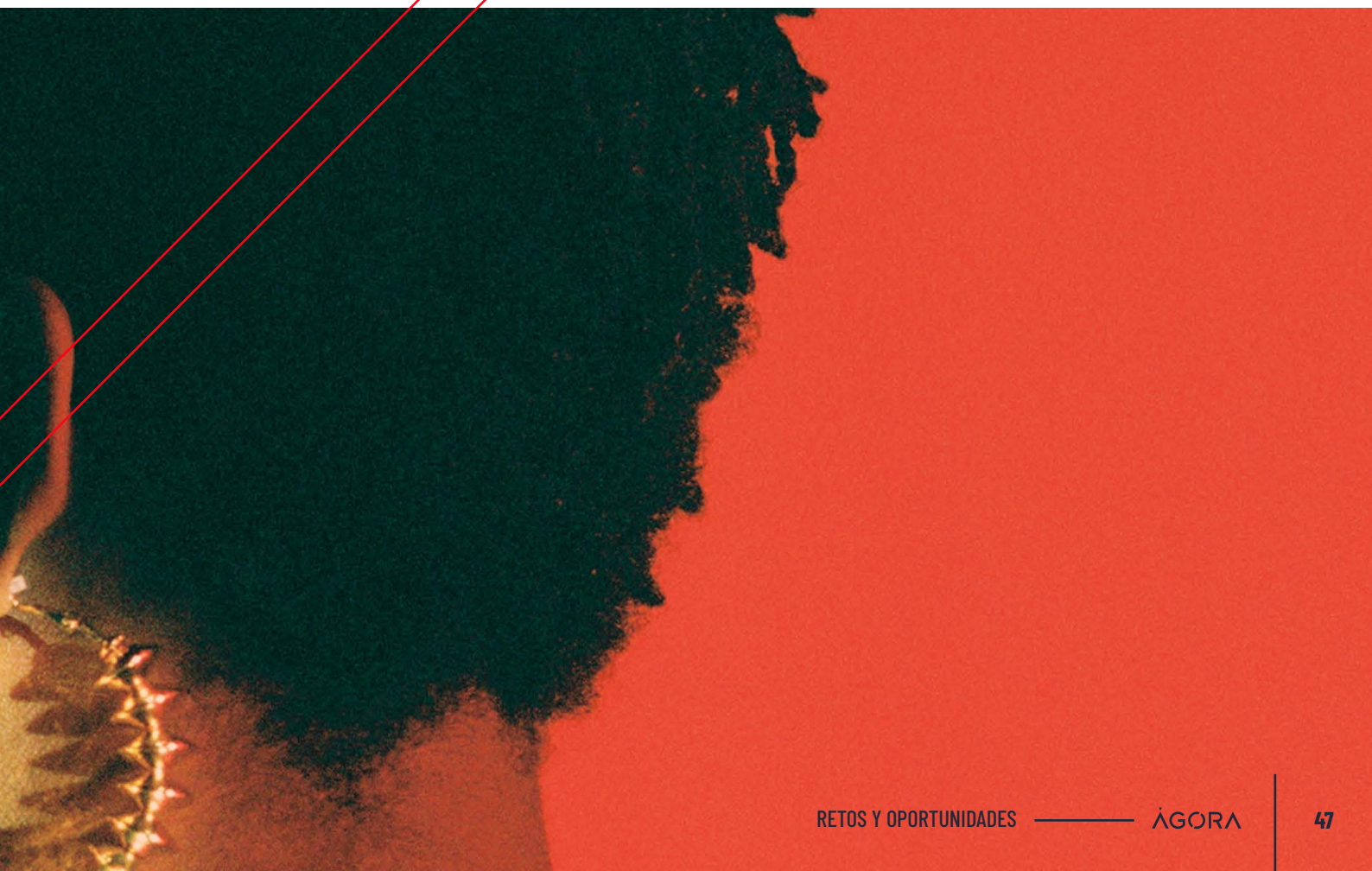
- Información pública e inmutable: el acceso a la información no debe estar controlado por un solo actor, y las trazas de ésta han de estar disponibles.

- Descentralización: no solamente la infraestructura ha de estar descentralizada, sino que las aplicaciones también han de serlo. Todos los diferentes actores han de colaborar en un espacio de juego común, y a ser posible, público.

En resumen, la aplicación de las tecnologías *blockchain* se basa más en un cambio de paradigma que en resultados inmediatos. No se trata de pretender usarla a modo de «base de datos irreversible», sino de adaptar la forma de trabajar para aprovechar la ventaja que nos da poder realizar transacciones con diversos actores, incluso desconocidos, en los que ya no es necesario tener *a priori* una confianza, pues la tecnología subyacente y el código de *software* que controla las relaciones se encarga de forma automática y transparente de dar seguridad a la solución.

En CTIC lideramos el futuro de *blockchain,* y podemos ayudar tanto a empresas como a entidades públicas a diseñar y poner en marcha proyectos que incluyan verdaderamente tecnologías *blockchain,* de la forma más adecuada para aprovechar sus beneficios reales. Si está interesado en conocer más detalles, puede contactar con nosotros.

«Traigan las tecnologías más innovadoras, por si viene el director», dice el experto en trazabilidad. «Sí, *blockchain,* así está mejor. Pero todavía falta algo. ¡El producto!». «¿Quién es usted?», le pregunta sorprendido el experto. «Soy el consumidor», responde atónito el visitante. El experto le da la espalda y sigue a lo suyo. «Lo siento. Sólo la gente involucrada puede participar aquí».



CUADERNO DE

BITÁGORA

CYPHERPUNKS, EL ORIGEN

ALFRE MANCERA

La siguiente historia forma parte de la colección de relatos que surgen de la **California** de los ‘70 en adelante. La historia del desarrollo de la computación es también la historia de las relaciones entre los personajes que coincidieron durante décadas en aquella región estadounidense, y en esta ocasión vamos a realizar una introducción al capítulo de los cypherpunks.

En el año 1979, **Timothy C. May** había pasado a la historia junto a **Murray H. Woods**, por ser los ingenieros que descubrieron cómo las partículas alfa ocasionaban un error de *software,* alterando los datos almacenados en la memoria de las computadoras, **su investigación está publicada en la IEEE** (Institute of Electrical and Electronics Engineers).

En 1986, May se estaba retirando de la compañía Intel a los 35 años, con dinero y acciones suficientes como para vivir sin necesidades económicas el resto de sus días. Lejos de planear un retiro tranquilo, Timothy May tenía un plan: promover la cultura del uso de criptografía fuerte para preservar la privacidad de los individuos en las transferencias de información y valor a través del medio digital.

El primer punto destacado de esta historia es sin duda la redacción del **«Manifiesto criptoanarquista»** en 1988, un documento abierto donde Tim May expone su previsión de lo que serán las interacciones digitales en un futuro cercano, destacando la necesidad de implementar protocolos criptográficos para preservar la confianza entre las partes y proteger a las personas de las interferencias de poder de los Estados y gobiernos. Ésa es la idea principal sobre la que se basa lo que May denomina la «criptoanarquía».

Según explica el mismo Timothy May, el «Manifiesto criptoanarquista» fue distribuido inicialmente entre asistentes y participantes de la conferencia **Crypto'88** y la **Hackers Conference** de ese mismo año. El buen *feedback* recibido reforzó la creencia de May acerca de la necesidad de crear una comunidad activa para el debate y desarrollo de soluciones basadas en criptografía fuerte que garantizaran lo descrito en su manifiesto.

Posteriormente, May participó en las Hackers Conferences de los años 1989 y 1990, profundizando en sus ideas sobre la criptoanarquía. En estos tres años, Timothy May fue fortaleciendo relaciones con personas de alto talento en diversas áreas técnicas relacionadas con la computación, especialmente con criptólogos y criptógrafos destacados que simpatizaban con la visión de May sobre la creación de una comunidad activa.

Como resultado de estos acontecimientos, en el año 1992 tuvo lugar una reunión que, cuando menos, cambiaría la historia de Internet.

Tim May mantenía relación con **Eric Hughes**, matemático y desarrollador estadounidense que había trabajado con uno de los mejores criptográfos del mundo: **David Chaum**, el cual fue fundador de Digicash, la primera empresa del planeta en implementar criptografía fuerte para desarrollar una forma de dinero electrónico que llegaría a integrarse en los bancos de ambos lados del océano Atlántico.

En los largos debates que mantenían May y Hughes sobre criptoanarquía, pseudónimos digitales, dinero criptográfico (denominado originalmente como *digital cash*) también participaba con frecuencia **John Gilmore**, alguien muy importante en esta historia.

Gilmore fue uno de los primeros empleados de **Sun Microsystems** y es cofundador de la **Electronic Frontier Foundation** (EFF) una organización sin ánimo de lucro que promueve desde 1990 el respeto a los derechos civiles en Internet. En 1989 fundó la empresa **Cygnus Solutions** con el fin de dar soporte a desarrollos de *software* libre, algo que ha hecho toda su vida, siendo especialmente conocido por la calidad y cantidad de sus aportaciones a un alto número de proyectos de **GNU** (GNU's Not Unix).

En septiembre de 1992, una conversación entre May y Hughes provocó que revisaran sus agendas y convocaran a un grupo de veinte personas expertas en áreas como programación, criptología, criptografía y matemáticas. No había vuelta atrás: había nacido la comunidad *cypherpunk.*

Esa primera reunión se realizó en una casa que Eric Hughes tenía en Oakland, muy cerca de San Francisco. Y, como el mismo Tim May contaría posteriormente en el documento titulado **«Cyphernomicon»**, el encuentro tuvo lugar la misma semana que se lanzó **PGP 2.0**, y todos los allí presentes ya tenían copias del *software* ese día. May describe cómo los presentes estaban sentados en el suelo, y cómo dividieron la jornada en dos sesiones: la de la mañana se centró en los conceptos básicos, y por la tarde estuvieron dedicados al *crypto game,* es decir, tratando sobre *remailers,* dinero digital, etc.

Una de las principales conclusiones que salieron de ahí es que necesitaban un *remailer* anónimo y una lista de correo para seguir debatiendo y mantener el contacto. John Gilmore ofreció sus servidores para alojar la lista de correo, y las propias oficinas de la empresa Cygnus para que el grupo pudiera reunirse cada mes presencialmente.

Tenían un grupo inicial de alto talento. Tenían conocimiento. Tenían influencia en otras personas. Tenían amigos en la prensa especializada. Sólo les faltaba un nombre.

En ese punto de la historia entró la figura de una mujer que tenía el afecto de todos ellos: la *hacker* **Jude Milhon**, también conocida como St. Jude. Milhon fue muy activa en los años sesenta en Estados Unidos por la lucha de los derechos civiles, participando en la organización de diversas marchas y acciones. En esa década, Milhon desarrolló la conciencia de que la tecnología era una gran aliada para su misión, y se convirtió en una programadora de alto nivel de forma autodidacta. Apasionada de la cultura *cyberpunk,* se mantuvo cerca de personas como May, Gilmore o Hughes, con quienes tenía muchas ideas en común.

Jude Milhon forjó el nombre de los *cypherpunks* haciendo un juego de palabras entre el témino *cipher,* que podría traducirse como clave de escritura o clave de cifrado; y el concepto ***cyberpunk*,** un género de ciencia ficción ambientado en una sociedad donde se mezclan bajos niveles de vida con patrones de desorden social y la presencia de tecnologías cibernéticas avanzadas.

Eric Hughes y **Hal Finney** (conocido, entre otras muchas cosas, por ser la primera persona en recibir una transacción de bitcoins) desarrollaron ese mismo año de 1992 un remailer anónimo que acabaría siendo conocido como ***Remailer Cypherpunk.***

El 9 de marzo de 1993, Eric Hughes hizo público el **«Manifiesto *cypherpunk*»**, una inequívoca declaración de intenciones sobre el principal interés de este grupo: «Los *cypherpunks* participan activamente para hacer que las redes sean más seguras para la privacidad de las personas».

Ahora sí. Tenían personas con un cerebro privilegiado, un nombre, un manifiesto, una lista de correo y un *remailer* anónimo. Había empezado el movimiento *cypherpunk,* y el resto es Historia.

En 1994, Timothy May publicará el «Cyphernomicon», un documento tipo FAQ (preguntas frecuentes) donde explica en profundidad las cuestiones más habituales sobre los principales temas que se tratan en la lista de correo de los *cypherpunks.*

Por supuesto, tanto el **«Cyphernomicon»** como un alto porcentaje de la correspondencia mantenida en la lista de correo de los *cypherpunks,* hoy día son contenidos públicos y accesibles para cualquier persona que quiera revisarlos.

Como si de un museo digital se tratase, la información publicada en la lista de correo *cypherpunk* y el contenido del «Cyphernomicon» ya son piezas de colección que deben ser preservadas por las siguientes generaciones de nativos digitales, para que no se olviden de que, en los albores de los ordenadores personales y las redes globales, ya había un grupo de personas velando por la libertad de navegar y explorar el ciberespacio sin renunciar al derecho a la privacidad.

[Continuará]

BREVES BLOCKCHAIN

EL BLOGUERO BLOCKCHAIN

Crónica de actualidad en el ecosistema de la cadena de bloques

LUIS CARRIÓN

Entrevista sobre impuestos, criptomonedas y otros temas legales

Por Juan Pablo Mejía para ***JuanEnCripto***

Entrevista a José Antonio Bravo Mateu, donde nos cuenta su experiencia y conversamos sobre impuestos y otros temas legales relacionados con bitcoin y otras criptomonedas.

Ir a la noticia >

Coinbase tiene un búnker bajo una montaña para custodiar tus bitcoins

Por Javier Pastor para ***Xataka***

Los responsables de Coinbase han querido expandir sus servicios e impulsar una parte del negocio cada vez más en auge: la custodia segura de criptodivisas.

Ir a la noticia >

¿Qué es MoneyButton?

Entrevista de Ramón Quesada a Miguel Duarte

Particularidades técnicas de Money Button y el protocolo que utiliza Bitcoin Satoshi Vision (BSV) con Paymail.

Ir a la noticia >

Sólo los *bitcoiners* deciden qué hacer con sus bitcoins

Por Javier Bastardo para ***Cointelegraph***

Pero, ¿no nació Bitcoin para darle total control de sus finanzas a sus usuarios? ¿Cuál es la cualidad que tiene un usuario para enjuiciar el uso del dinero de otro?

Ir a la noticia >

¿El fin de Bitcoin y las criptomonedas?

Por Alter Consciens para ***tuCriptomoneda***

Steven Mnuchin, Secretario del Tesoro de Estados Unidos, ofreció una sesión informativa oficial sobre la reglamentación de las criptomonedas, con especial atención a activos como Bitcoin y Libra.

Ir a la noticia >

Libra: las criptomonedas ya no darán marcha atrás

Por Benjamí Anglès Juanpere para ***Retina***

En un mundo globalizado y basado en Internet, parece inevitable que tarde o temprano acabe apareciendo una moneda digital que pueda ser usada superando todas las fronteras, lo que va a permitir que la gente use un nuevo medio de pago.

Ir a la noticia >

Aunque Libra no sea una criptomoneda, va a permitir que la gente use un nuevo medio de pago

Por Miguel Elizondo para ***El Español***

En una década, los chicos que hoy tienen 13 años van a estar pagando su Coca-Cola o su entrada de cine con criptomonedas en Madrid y en Pekín.

Ir a la noticia >

Silicon Valley a la conquista de las finanzas con *blockchain*

Por Alex Preukschat para ***El País***

Silicon Valley asalta las finanzas. ¿El planeta va a ir mejor con los gigantes tecnológicos dominando también el mundo financiero? Probablemente, no.

Ir a la noticia >

¿QUIERES PARTICIPAR?

En la plaza descentralizada estamos buscando gente como tú, personas que apuestan por el nuevo paradigma. Queremos formar un equipo colaborativo para seguir construyendo y promover la tecnología *blockchain* a través de proyectos que busquen mejorar la sociedad.

¿Hablamos?

asociacion@agorachain.org / publicidad@agorachain.org / eventos@agorachain.org / revista@agorachain.org

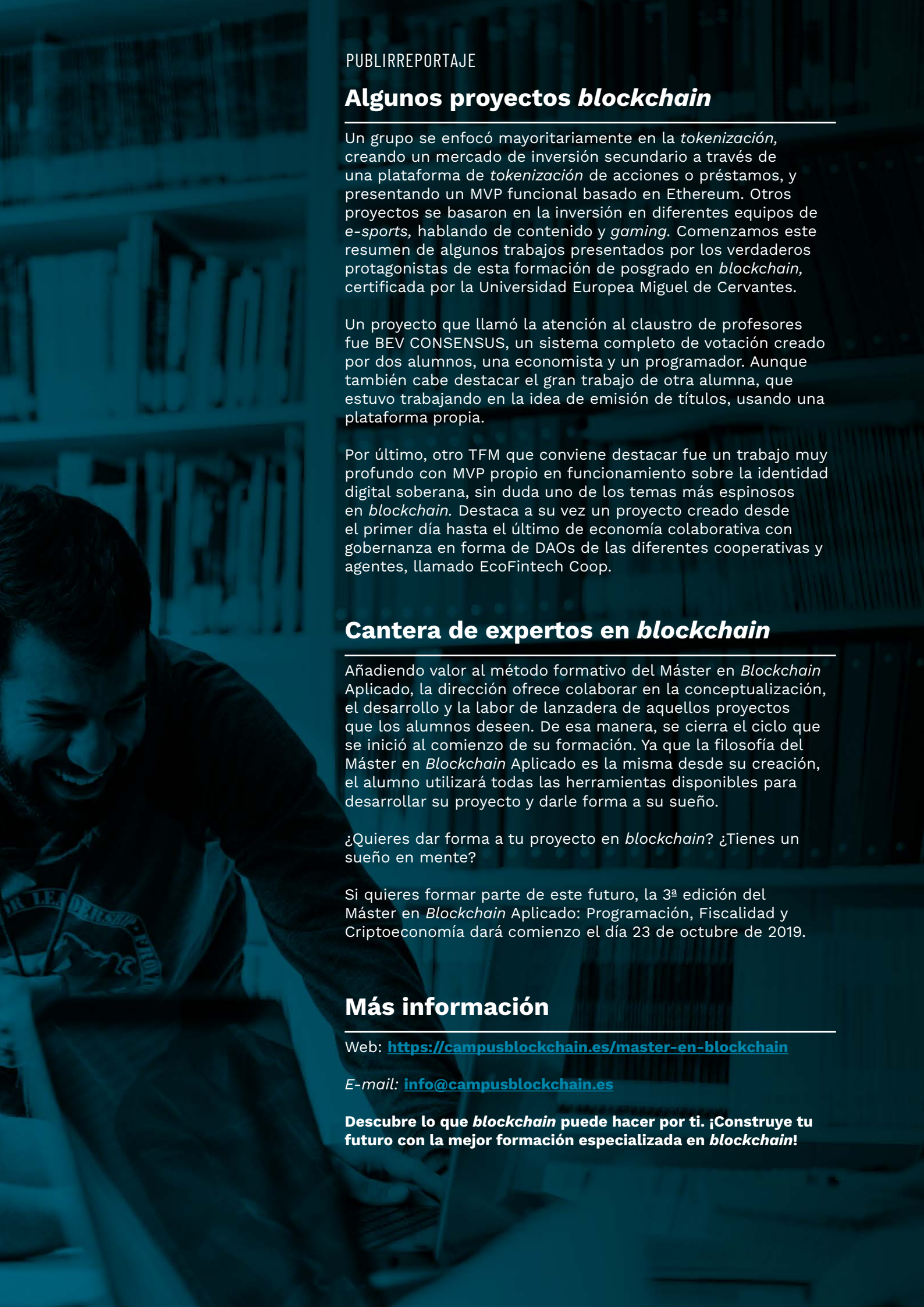
MASTER EN BLOCKCHAIN APLICADO

Crea tu propio proyecto de *blockchain*

Terminada la primera edición del Máster en *Blockchain* Aplicado y a medio camino de finalizar la segunda, la conclusión que podemos sacar es la excelencia del esfuerzo, tanto por parte de los tutores como de los alumnos. ¿Por qué?

Porque todos los alumnos del Máster en *Blockchain* Aplicado de esta edición han presentado proyectos que rozan la excelencia, certificando el refrán que asegura que «el buen discípulo supera al maestro».

Campus Internacional de BlockChain



PUBLIRREPORTAJE

Algunos proyectos *blockchain*

Un grupo se enfocó mayoritariamente en la *tokenización,* creando un mercado de inversión secundario a través de una plataforma de *tokenización* de acciones o préstamos, y presentando un MVP funcional basado en Ethereum. Otros proyectos se basaron en la inversión en diferentes equipos de *e-sports,* hablando de contenido y *gaming.* Comenzamos este resumen de algunos trabajos presentados por los verdaderos protagonistas de esta formación de posgrado en *blockchain,* certificada por la Universidad Europea Miguel de Cervantes.

Un proyecto que llamó la atención al claustro de profesores fue BEV CONSENSUS, un sistema completo de votación creado por dos alumnos, una economista y un programador. Aunque también cabe destacar el gran trabajo de otra alumna, que estuvo trabajando en la idea de emisión de títulos, usando una plataforma propia.

Por último, otro TFM que conviene destacar fue un trabajo muy profundo con MVP propio en funcionamiento sobre la identidad digital soberana, sin duda uno de los temas más espinosos en *blockchain.* Destaca a su vez un proyecto creado desde el primer día hasta el último de economía colaborativa con gobernanza en forma de DAOs de las diferentes cooperativas y agentes, llamado EcoFintech Coop.

Cantera de expertos en *blockchain*

Añadiendo valor al método formativo del Máster en *Blockchain* Aplicado, la dirección ofrece colaborar en la conceptualización, el desarrollo y la labor de lanzadera de aquellos proyectos que los alumnos deseen. De esa manera, se cierra el ciclo que se inició al comienzo de su formación. Ya que la filosofía del Máster en *Blockchain* Aplicado es la misma desde su creación, el alumno utilizará todas las herramientas disponibles para desarrollar su proyecto y darle forma a su sueño.

¿Quieres dar forma a tu proyecto en *blockchain*? ¿Tienes un sueño en mente?

Si quieres formar parte de este futuro, la 3ª edición del Máster en *Blockchain* Aplicado: Programación, Fiscalidad y Criptoeconomía dará comienzo el día 23 de octubre de 2019.

Más información

Web: **https://campusblockchain.es/master-en-blockchain**

E-mail: **info@campusblockchain.es**

Descubre lo que *blockchain* puede hacer por ti. ¡Construye tu futuro con la mejor formación especializada en *blockchain*!

SAPERE AUDE!

CARMEN PASTOR

«We believe that many more people should have access to financial services and to cheap capital.

We believe that people have an inherent right to control the fruit of their legal labor».

(Declaración de intenciones del texto del *whitepaper* de LIBRA)

Inauguramos esta nueva sección, «SAPERE AUDE!», con la intención de servir de observatorio sobre las adaptaciones de nuestro mercado a los cambios que la tecnología *blockchain* le marca. Casi podríamos decir que constituye hoy «el tema de nuestro tiempo»[1], y también podríamos añadir que el mercado es «el tema de nuestro espacio». La sección con la que BAES empieza su andadura en *ÁGORA* ha escogido el viejo axioma latino que significa «atrévete a saber». También se interpreta como «atrévete a pensar»[2]. El conocimiento no entiende de fronteras, credos, religiones, profesiones ni clases sociales, y se expresa a través de aquellos que de forma libre y respetuosa quieren humildemente difundirlo. Por ello, queremos compartir las experiencias de diferentes miembros de BAES. Empezaremos por nuestra contribución al CESE[3] con la propuesta de gobernanza cooperativa para las plataformas *blockchain.*

Pero toca primero descifrar el nuevo código con el que se escribe el sistema financiero al dictado de la compleja, rápida y cambiante disrupción e interacción con las *BigTech* que estamos viviendo en los últimos tiempos. Como en su día lo fue la electricidad y su aplicación «escalable» (*scalable system,* en inglés), los grandes disruptores tecnológicos producen enormes revoluciones que transforman la anatomía del mercado y de la sociedad. Pero escalabilidad también significa financiar empresas de elevado riesgo y llegar al mercado para, gráficamente, pasar «de la electricidad a la electrónica». Al mismo tiempo, llegar al mercado implica usabilidad, es decir, que las nuevas aplicaciones de *trading* sean fáciles de utilizar y no requieran conocimientos especializados para la inversión en Bolsa, en divisas o en criptomonedas.

Por ello, de entre todas las nuevas tecnologías destacan *blockchain* («cadena de bloques») y las DLT *(distributed ledger technologies),* pues pueden acelerar en los próximos años la expansión de la digitalización, cuando éstas alcancen su madurez, por ser la infraestructura del mercado que de forma eficiente y autoejecutable (mediante *smart contracts*) podrá automatizar amplias franjas de servicios, incluidos los financieros[4]. Cuando los intercambios descentralizados se generalicen, podremos asistir a la estructura del nuevo mercado europeo verdaderamente *peer to peer,* muy lejano a la actual y confusa economía colaborativa, de modo que *blockchain* podría contribuir a hacer efectiva la portabilidad de datos y activos en el Mercado Único Digital.

La apuesta del Parlamento Europeo parece clara en la Resolución de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación [(2017/2772(RSP), disponible **aquí**], al señalar que facilitará la transparencia de los mercados y la «simplificación de las cadenas de suministro y el aumento de la interoperabilidad entre empresas». En la Resolución comentada, el Parlamento insiste en «que los protocolos abiertos de cadena de bloques pueden reducir los obstáculos de entrada para las pymes y mejorar la competencia en los mercados digitales». Esta tecnología, por tanto, puede modelar mercados abiertos o cerrados, nuevos mercados de referencia, sin perjuicio de su contribución para que surjan nuevos conceptos en el Derecho de la competencia, en los que se tendrá que valorar si las *blockchains* son privadas, públicas o híbridas, las normas de gobierno de la red, los roles de los nodos, los «permisionados», etc.

Pues bien, en nuestra contribución al *Public Hearing* titulado «Blockchain: Technology for the Social Economy 4.0» el día 29 de mayo de 2019 en Bruselas (documentación accesible en el siguiente **enlace**), destacamos cómo se puede diseñar una plataforma *blockchain* inclusiva para las entidades que conforman la *Social Economy* en la UE, como «una puerta abierta a la cuarta revolución industrial». De hecho, nosotros lo hicimos con la red que une a las universidades públicas valencianas: blockUniversitas. Nuestra propuesta, como ya señalamos en la entrevista publicada en el número anterior de esta revista, se centra en conseguir una plataforma *blockchain* soportada con infraestructura pública que diera servicio «a todos». Como decíamos, nos hubiera encantado que fuera la primera «*BigTech* cooperativa de infraestructura pública», sostenible e inclusiva. Pero, a juzgar por los acontecimientos, todo apunta a que será infraestructura tecnológica privada. Aunque no nos resistimos a que también pueda ser pública.

Y es que, además de la tecnología, es clave una gobernanza cooperativa que soporte la infraestructura tecnológica y su mantenimiento «sostenible». Un ejemplo paradigmático de lo señalado podría ser la proyectada *blockchain* que soportará la moneda Libra. Si lo consigue, tal y como asegura Facebook a EFE, «para que una divisa global tenga éxito, no puede estar controlada por una sola entidad y aún menos por una entidad comercial como Facebook. Facebook tendrá voz en la asociación como todos los otros miembros».

Además de la tecnología, es clave una gobernanza cooperativa que soporte la infraestructura tecnológica y su mantenimiento «sostenible»

En definitiva, podemos concluir que estamos ante un nuevo ecosistema monetario (como ya adelanté en anteriores escritos sobre la materia), donde convivirá el dinero de curso legal emitido por una cooperativa de empresas privadas no bancarias (yo las denomino *Coop-Tech*[5]), y el tradicional emitido por los bancos centrales, comerciales (cada vez menos) y EDEs. También veremos desaparecer el efectivo tal y como lo conocemos (papel moneda y monedas), y surgir el nuevo efectivo digital, y resurgir los grupos de sociedades por coordinación.

Nuestro sistema capitalista, nuestro mercado, se encuentra ahora ante el mayor reto jamás conocido en su historia. Detrás hay un cambio de paradigma, y en ello ha sido determinante el cambio en la gobernanza. De una gobernanza consorcial típica a un nuevo modelo cooperativo inspirado en su diseño en los siete principios de la Alianza Cooperativa Internacional (ACI)[6].

[1]José Ortega y Gasset, «El tema de nuestro tiempo», en *Obras completas,* Madrid, Alianza Editorial & Revista de Occidente, 1983, vol., 3, pp. 143 y ss.

[2]Su divulgación se debe al filósofo Immanuel Kant en su ensayo *¿Qué es la Ilustración?,* aunque su uso original se da en la Epístola II de Horacio del *Epistularum liber primus: «Dimidium facti, qui coepit, habet: sapere aude, / incipe»* («Quien ha comenzado, ya ha hecho la mitad: atrévete a saber, empieza»). Hoy es el lema de muchas universidades (fuente: **Wikipedia**).

[3]Comprometido con la integración europea, el **Comité Económico y Social Europeo** contribuye a reforzar la legitimidad democrática y la efectividad de la Unión Europea al permitir a las organizaciones sociales de los Estados miembros expresar sus puntos de vista a nivel europeo.

[4]Ya nos referimos en trabajos previos (Pastor, C.: «Internet del valor», en VV. AA. (2018) *Blockchain: aspectos tecnológicos, empresariales y legales.* Editorial Aranzadi, 345 pp.).

[5]No debemos olvidar que Facebook Payments International Ltd. es una **EDE domiciliada en Dublín**.

[6]**«Principios y Valores Cooperativos»**, por la Alianza Cooperativa Internacional.

EL RINCÓN HUMANITARIO
BIENVENIDOS

ÁLEX CASAS

El pasado 5 de diciembre de 2017, durante LABITCONF en Bogotá, algunos de los organizadores, asistentes y patrocinadores del evento quisieron reconocer y premiar proyectos destinados a construir una sociedad mejor.

Ése fue el punto de partida de esta aventura que hoy inaugura esta nueva sección de **ÁGORA.** Se premiaron cuatro iniciativas en *Shapers (Social Hackers),* como una forma de reconocer proyectos que ya están teniendo un impacto positivo, y otros cuatro se otorgaron en la categoría *Dreamers,* proyectos con un equipo y una idea que están prosperando para hacerla realidad con un producto funcional.

Estos fueron los primeros proyectos premiados, y al día de hoy más de la mitad continúan generando sonrisas. En el próximo número conoceréis con detalle los proyectos premiados en 2018.

SHAPERS

- Alice.si (https://alice.si/)
- Slavefreetrade (https://www.slavefreetrade.org)
- IdBox (https://www.idbox.io)
- Moneda Par (http://www.monedapar.com/)

DREAMERS

- Ethic Hub (https://www.ethichub.com)
- Amply (http://www.amply.tech/)
- Usizo (http://secret.usizo.org)
- Blockchain 4 Transparency

Durante la conferencia en Bogotá, la iniciativa recibió apoyo de la comunidad en general, por lo que empezamos a darnos cuenta de que Blockchain 4 Humanity (B4H) no podía ser sólo un premio para reconocer estos proyectos y «nos vemos el año que viene...», sino un colectivo que debía mostrarse activo durante todo el año para hacer que algunos de estos proyectos se hagan realidad.

Y esta es la historia de cómo nació la fundación Blockchain 4 Humanity, un increíble grupo de personas que comparten su interés en proyectos que cambian la vida de personas, se unieron para crear esta plataforma de aceleración social sin ánimo de lucro.

Después de la entrega de los primeros premios, la familia Blockchain 4 Humanity, hizo del 2018 el año de definición y exploración de todas las posibilidades para ayudar a acelerar en forma pro-bono y proporcionar las herramientas necesarias para proyectos prometedores. Desde ya se puede decir que la segunda edición de los premios está siendo un reflejo de lo aprendido en el camino, un camino largo, pero muy bien acompañad@s.

No sólo pretendemos ser una interfaz para los donantes y patrocinadores que desean contribuir con los proyectos que necesitan fondos para su desarrollo; sino que también les integramos con un ecosistema donde se ofrece mentoría y *partnerships*. Adicionalmente, el equipo de contribuidores del B4H realiza un trabajo muy arduo con los proyectos donde se desarrollan los puntos técnicos, legales, de negocio o diseño, conectando las personas adecuadas, y dando acceso a foros de inversión y lanzamiento. Parte de la misión de B4H es hacer realidad proyectos con un enorme potencial de transformación para nuestra sociedad.

Por primera vez en la historia, hay muchas personas con ideales «distintos» que tienen los recursos para causar cambios (transformativos y positivos) en nuestro entorno; por lo tanto, queremos aprovechar este momento único en la historia para asegurarnos de que ese cambio suceda y que todos juntos seamos capaces de construir un planeta más equilibrado para todos. Por nuestra parte, queremos demostrar la capacidad sin precedentes para favorecer la colaboración entre seres humanos de la tecnología *blockchain*. Y colaborando, nuestra próxima acción se realizará durante Web3Summit en Berlín del 19 al 21 de agosto, donde el movimiento #Coalitions4GOOD tendrá un lugar de encuentro, aprendizaje y colaboración con toda la comunidad *4good,* remarcando la importancia de la independencia de protocolos, cadenas y algoritmos de consenso, *one love*. ¿Vienes?

Después de esta pequeña introducción sobre quiénes somos, por qué hacemos lo que hacemos o cómo queremos hacerlo, ¡te damos la bienvenida al Rincón Humanitario!

En esta sección, en la que la fundación Blockchain 4 Humanity tiene el honor de colaborar con **ÁGORA,** encontrarás mensualmente contenido relevante sobre el impacto social de *blockchain,* desde artículos de opinión hasta entrevistas con proyectos, pasando por tu proyecto (sí, sí, la recepción de aplicaciones para los premios 2019 está ya abierta para la entrega en Uruguay durante LABITCONF).

¡Accede a **www.b4h.world** y participa!

Queremos activar un movimiento de responsabilidad social crypto bajo el lema: «Si Crypto cambió tu mundo, ¿cómo quieres cambiar tú el mundo?».

Y, si quieres involucrarte de alguna manera, ¡bienvenido! Nuestra red de mentores, patrocinadores, amigos y donantes debe crecer siempre y estaremos encantados de contar con ayuda, cualquier tipo de ayuda, para lograr nuestros objetivos.

Proporcionamos a donantes y patrocinadores y una forma efectiva de contribuir para lograr una sociedad más equilibrada y justa, y asegurarnos de que los fondos se destinan a proyectos curados por el equipo de B4H al completar los hitos predefinidos entre el equipo y la fundación, con el objetivo de ayudar a estos proyectos a ver la luz y comenzar a generar sonrisas.

B4H busca equipos sólidos que puedan hacer un buen uso de *blockchain* para el bien social, convencidos de que los resultados son arrolladores. Por ejemplo, los Premios b4H 2017 revelaron el increíble trabajo de la plataforma EthicHub, que hace que los préstamos sean accesibles para miles de productores de café en México, a la vez que se genera un retorno para inversores y un alto impacto social y económico, mientras se ofrece un retorno a los participantes de la plataforma.

EthicHub es un claro ejemplo del tipo de proyectos que B4H desea catalizar, y respaldar su adopción masiva.

Queremos que los unicornios existan, y ayudamos a proyectos de todo el mundo a convertirse en unicornios en el único sentido en que entendemos hoy en día el término: proyectos capaces de impactar positivamente la vida de mil millones de personas.

@GoTechMadrid

¿Buscas algo más que un coworking?

Disfruta además de un 2X1 en Hotdesking y un 10% de descuento
en todos los servicios de GoMadrid por ser lector de ÁGORA

Descubre el ecosistema tecnológico GoMadrid

#fintech #blockchain #tech

www.gomadrid.tech

ecosystem@gomadrid.tech

tu Criptomoneda

Crypto World News

www.tucriptomoneda.com

Información, entrevistas y artículos de opinión.
Blockchain, criptomonedas, criptoarte.
Herramientas de libertad.
Tienda *crypto*.

t.me/tucriptomoneda
twitter.com/tucriptomoneda
facebook.com/tucriptomoneda
instagram.com/tucriptomoneda2019

TECNOLOGÍAS PARA EL DESARROLLO

Cómo *blockchain* puede hacer más seguro el comercio

SANDRA CORCUERA-SANTAMARÍA

Primero veamos algunos antecedentes sobre esta tecnología. *Blockchain* puede ayudarnos a confiar en la información que se nos brinda. Saber que los datos son reales y no han sido manipulados es fundamental en todos los ámbitos, desde el etiquetado de los alimentos hasta las transacciones financieras.

Blockchain es la evolución digital de los registros que se utilizaban para contabilizar las transacciones en Mesopotamia, hace más de 7.000 años. A diferencia de la arcilla, el papiro o el papel, los registros en *blockchain* son seguros y pueden compartirse, replicarse y actualizarse desde distintos lugares, casi en tiempo real. Una tecnología que abre nuevas oportunidades para la colaboración entre pares.

El comercio encaja de manera natural con *blockchain* porque es rico en intercambios transfronterizos de información, desde conocimientos de embarque hasta las cartas de crédito y los certificados de origen. Las administraciones aduaneras son los puntos neurálgicos de este flujo de información sobre el que se sustentan nuestras redes de cadenas de valor.

Para facilitar el comercio y combatir el contrabando y el lavado de dinero de manera más efectiva, los organismos aduaneros necesitan saber cuáles de los actores involucrados en la cadena de suministro global —importadores, exportadores, transportistas, agentes aduaneros y operadores de bodegas— son confiables para gozar de trámites ágiles y cuáles deben estar sujetos a más escrutinio.

EL USO DE *BLOCKCHAIN* A PEQUEÑA ESCALA PUEDE GENERAR UN IMPACTO ENORME. UN EJEMPLO DE ESTO ES EL TRABAJO REALIZADO CON CUATRO ORGANISMOS ADUANEROS DE AMÉRICA LATINA Y EL CARIBE.

OPERADORES ECONÓMICOS AUTORIZADOS

En 2005, la Organización Mundial de Aduanas ideó un marco para identificar a los actores confiables y seguros, conocidos como Operadores Económicos Autorizados (OEA). Casi 80 países han compilado listas de entidades que están certificadas para cumplir con los estándares OEA.

Para que el sistema funcione, las administraciones aduaneras necesitan compartir sus listas de OEA con sus agencias homólogas. De lo contrario, un exportador recibiría un tratamiento expedito en un lado de la frontera, pero no en el otro.

El uso compartido de estas listas se conoce como acuerdos de reconocimiento mutuo o ARM. Hasta ahora se han firmado sesenta ARM y se están negociando otros cuarenta.

Estos acuerdos pueden ser bilaterales o multilaterales, como en el caso de las administraciones aduaneras de los países miembros de la Alianza del Pacífico: Colombia, Chile, México y Perú. Por ejemplo, para un exportador peruano que realiza envíos hacia México, contar con un ARM puede hacer la diferencia entre esperar en el puerto durante horas o durante días.

El problema es que las listas de OEA cambian al ser agregados o eliminados nuevos operadores. Para informar de estos cambios, los oficiales en cada administración aduanera envían por correo electrónico un archivo de Excel que contiene los datos de sus respectivos OEA. Esto suele suceder una vez al mes.

Los datos se incorporan a los sistemas de gestión de riesgos. Hay limitaciones obvias en esta configuración: los sistemas de correos electrónicos no son del todo seguros y la información de las entidades que son agregadas o suspendidas de las listas de OEA puede llegar con cierto retraso a las agencias de aduanas.

CADENA, *BLOCKCHAIN* PARA UN COMERCIO MÁS SEGURO

Es aquí donde entra en juego *blockchain.* Para generar un sistema seguro de intercambio de datos, en el Sector de Integración y Comercio del Banco Interamericano de Desarrollo (BID) hemos liderado un proyecto piloto desde 2018 con funcionarios de los programas de OEA y especialistas en tecnologías de la información de México, Perú, Chile y Costa Rica, en colaboración con Microsoft.

Con el nombre de CADENA, el programa tiene como objetivo desarrollar las funcionalidades de negocio y la arquitectura tecnológica de una aplicación basada en *blockchain.* La idea de esta solución es que cada transacción sea segura y esté protegida por un registro de auditoría inmutable.

Los bienes exportados por un OEA podrían recibir trato preferencial con menos inspecciones en el país importador una vez que el exportador haya obtenido la certificación de OEA en su país de origen. CADENA trabaja en tiempo real, reduciendo la burocracia y aumentando la transparencia y la confianza.

La solución tomó siete meses desde el concepto inicial hasta el diseño y, actualmente, está en la etapa final de la fase de pruebas. Ésta ha demostrado ser una herramienta adecuada y eficiente para compartir datos de un país a otro.

ALIANZAS CON LAC-CHAIN

Al igual que en otros proyectos tecnológicos, en este piloto han surgido algunos desafíos. Éstos incluyen:

- **Actualización de los marcos regulatorios**
- **Abordaje de aspectos de la gobernanza**
- **Integración con otros sistemas de administración aduanera**
- **Construcción de la arquitectura tecnológica adecuada para proteger la privacidad de los datos**
- **Escalabilidad**

Estos retos los estamos abordando en la segunda fase de CADENA, actualmente en proceso de diseño, en colaboración con LAC-Chain, una alianza para impulsar del uso de *blockchain* en América Latina y el Caribe lanzada en 2018 por el BIDLab y varios socios tecnológicos clave.

Somos optimistas respecto a la ampliación de nuestro proyecto piloto. Colombia acaba de unirse a la iniciativa y estamos en conversaciones con otros países para que se unan a CADENA. Lo ideal sería que cada administración aduanera de América Latina y el Caribe y de otros países se una a un sistema de intercambio de información basado en *blockchain.*

Los exportadores e importadores verían sus bienes procesados más rápido en las fronteras y puertos. Las aduanas podrían concentrar sus recursos escasos en los operadores no certificados.

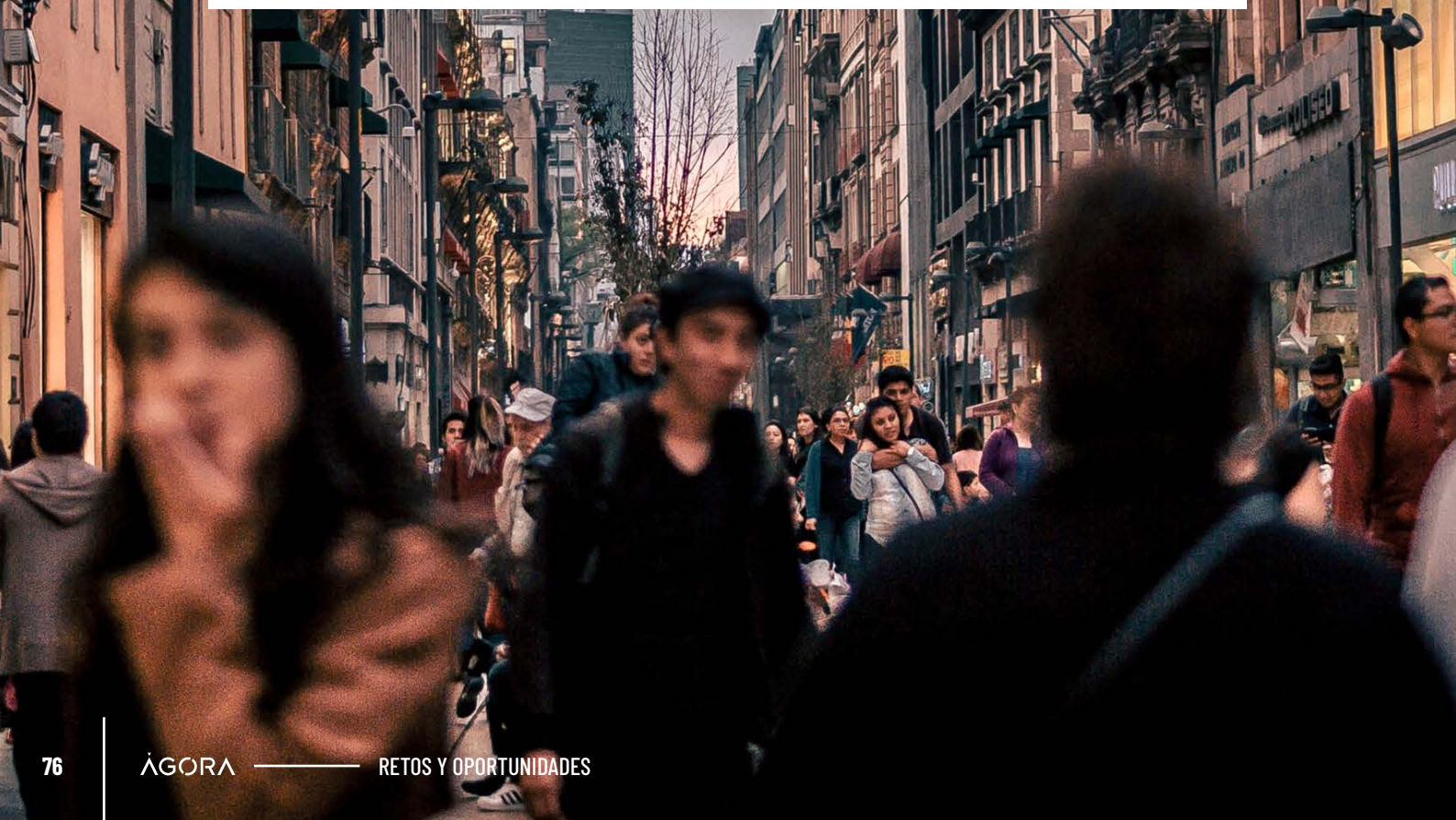
Esto no eliminará el lavado de dinero y el contrabando a través del comercio, pero hará más difícil llevar a cabo esas actividades.


GLDU 568655 3
22G1
GOLD
MGW.
TARE.
NET.
CU.CAP.
TAL
TCLU 303050 0
22G1
67.200 LBS.
2.200 KGS.
62.350 LBS.
MEDU 2744
22G1
M. G. W.
TARE
NET
CU.CAP.
DFSU 275472 3
22G1
MAX.GROSS
TARE
NET
CU.CAP.
XINES
XINU 109827 4
22G1
MAX.GROSS 30.480 KGS 67.200 LBS
TARE 2.200 KGS 4.850 LBS
NET 28.280 KGS 62.350 LBS
CU.CAP. 33.2 CU.M. 1.170 CU.FT.
www.xines.com
BSIU 2743
22G1
MAX.W.T.
TARE WT.
PAYLOAD
CU. CAP.
MEDU 229987 1
22G1
M. G. W.
TARE
NET
CU.CAP.
MEDU 146848 9
22G1
M. G. W.
TARE
NET
CU.CAP.
DONG FANG
DFSU 210
22G
MAX. GROSS
TARE
NET
CU. CAP.
IPXU 214850 6
22G1
MAX. GROSS 67.200 LBS
TARE 2.185 KGS
NET 62.380 LBS
CU.CAP. 33.2 CU.M. 1.173 CU.FT.
MEDU 163664 3
22G1
M. G. W.
TARE
NET
CU.CAP.
FLORENS
www.florens.com
FCIU 6044
22G1
MAX. GROSS 67.200
TARE 2.180
MAX. CARGO 62.390
CU. CAP.

SEGUNDA ENTREGA

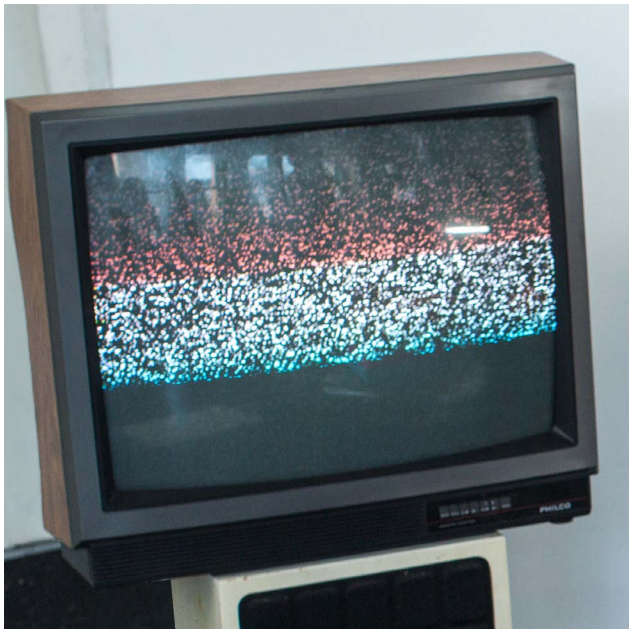
ELECCIONES EN MÉXICO
Una ruta hacia la votación electrónica

MARCO IVÁN VARGAS CUÉLLAR



En la primera entrega de esta serie, publicada en ÁGORA #10 hice referencia al marco general de reflexiones que comienzan a discutirse en México a propósito de una nueva reforma electoral. Como es común en muchos países democráticos, las reglas que hacen funcionar al sistema electoral no son estáticas y se encuentran sujetas a un proceso de revisión permanente. Este proceso de reforma se realiza en México más o menos cada seis años, empleando como puntos de referencia las debilidades y áreas de oportunidad que se identifican en las elecciones presidenciales ordinarias.

La ocasión de aprovechar la elección presidencial como punto de referencia para examinar el funcionamiento de nuestro sistema electoral no es un asunto menor. Se relaciona con uno de los eventos políticos de mayor importancia en un país, lo que le dota de una enorme presión social y escrutinio público sobre su operación. Aunado a ello, las elecciones presidenciales en México suelen tener un calendario concurrente con otras elecciones locales. Hay que recordar que en México el sistema de gobierno federal reconoce tres ámbitos gubernamentales: nacional, estatal y municipal, lo que implica la celebración de distintas elecciones en una sola casilla, dentro de un marco de colaboración entre distintas autoridades electorales.



Una reforma a nuestro sistema electoral puede tener distintos propósitos y motivaciones. Los focos de las reformas realizadas durante los últimos treinta años han partido, principalmente, de las demandas de los partidos perdedores, quienes desde la oposición han señalado diversos aspectos que a la postre se convirtieron en nuevas reglas que buscaron garantizar la competitividad y certeza de los comicios.

Pero en esta ocasión la demanda parece ser distinta. La narrativa del fraude electoral es más una bandera retórica que un testimonio documentado. La razón de ello tiene que ver con que el funcionamiento de los mecanismos y procedimientos electorales siguen rigurosos estándares de integridad electoral que todos los contendientes e interesados pueden verificar. Es de esta manera que hay voces que llaman a la revisión del costo de nuestras elecciones sin sacrificar un ápice de su confiabilidad. Y es ahí donde surge la necesidad de repensar nuestros procedimientos desde el potencial de las herramientas *blockchain.*

Una de las ideas que cobra mayor fuerza en esta discusión tiene que ver con la implementación del voto electrónico en México. Actualmente en el ámbito nacional se emplea de manera predominante la boleta en papel como el único instrumento para que un ciudadano ejerza su derecho al voto. Durante más de quince años, algunas autoridades electorales locales han desarrollado experiencias de votación electrónica empleando principalmente herramientas como la urna electrónica, pero su uso generalizado se encuentra todavía muy lejos de concretarse, principalmente por el componente de la desconfianza.

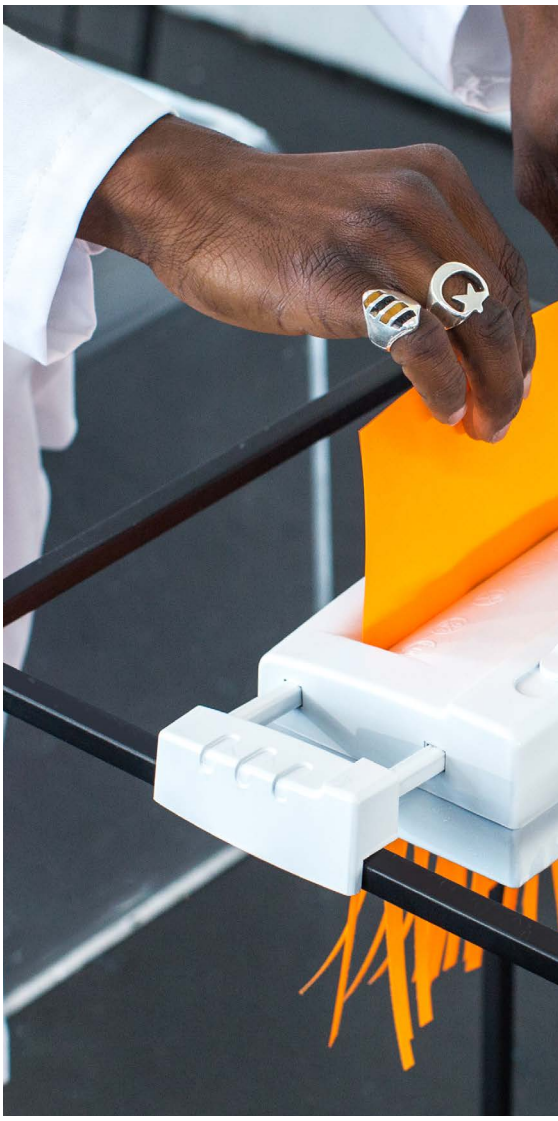
De acuerdo con la organización Institute for Democracy and Electoral Assistance, la mayoría de los sistemas de votación electrónica se encuentran dentro de cuatro tipos:

1. **Registro electrónico directo. Que puede o no arrojar un comprobante impreso verificado por el votante, que podría fungir como prueba física de los votos emitidos.**

2. **Reconocimiento óptico de marcas. La virtud de estos sistemas se encuentra en la rapidez de su lectura y procesamiento de resultados.**

3. **Impresoras de boletas electrónicas. Reproducen un papel para ser leído por una máquina, la cual hace el conteo de forma automática.**

4. **Sistemas de votación en línea. Donde los votos suelen ser transmitidos por Internet a un servidor central para su conteo.**

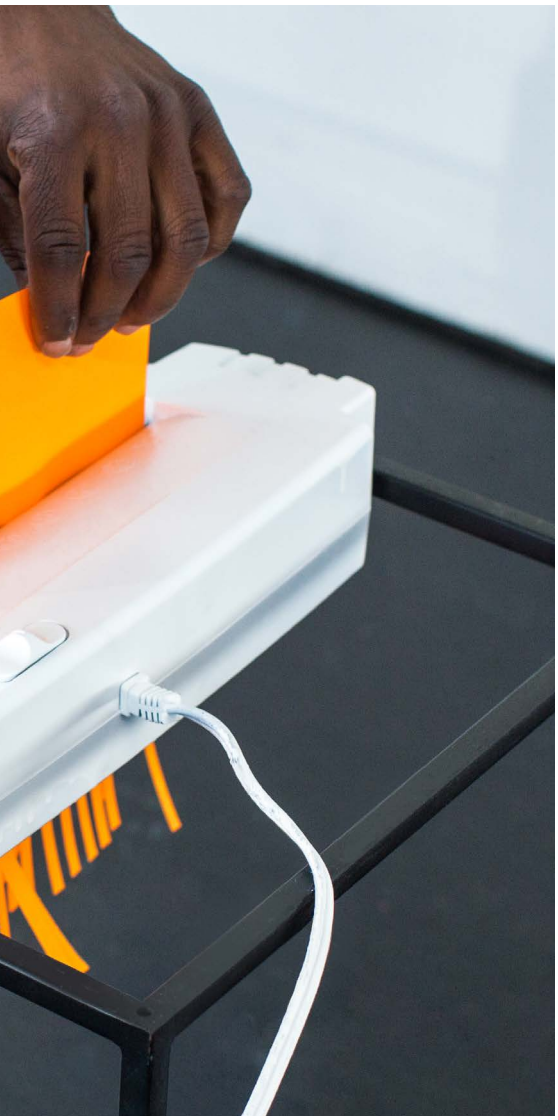


El Instituto Nacional Electoral ya ha comenzado los trabajos orientados a posibilitar el voto electrónico a través de Internet, señalando como una primera etapa de implementación la obtención del voto de las mexicanas y mexicanos residentes en el extranjero para las elecciones federales concurrentes del año 2021. Para ello se han definido un conjunto de «Lineamientos que establecen las características generales que debe cumplir el sistema del voto electrónico por Internet», que considera las siguientes actividades:

1. **Implementar las fases para el desarrollo del modelo operativo del sistema, el cual constará, al menos, de lo siguiente: creación de la llave criptográfica, apertura del sistema, autenticación del votante, monitoreo del sistema, cierre del sistema, descifrado y cómputo de los votos, y resguardo y preservación de la información.**

2. **Definir e implementar las medidas de seguridad necesarias para garantizar la secrecía del voto a partir de la autenticación del votante y hasta el cómputo de los votos; conservando la integridad de los votos en todo momento. Asimismo, dichas medidas deben garantizar que se emita un solo voto por ciudadano residente en el extranjero, y que éste tenga derecho a hacerlo.**

3. **Publicar el resultado de la votación electrónica por Internet de los mexicanos residentes en el extranjero en el Programa de Resultados Electorales Preliminares y en los cómputos distritales respectivos, conforme a la normativa vigente.**



Resulta evidente que la ruta de trabajo se orienta hacia la implementación de herramientas electrónicas para optimizar recursos y reducir tiempos en la jornada electoral. Sin embargo, no deben perderse de vista algunas de las preocupaciones que ya han sido recogidas desde experiencias internacionales. El contexto político de cada país determina la ruta de implementación de estas herramientas y el caso mexicano no debe ser la excepción. Convendría echar un vistazo a la experiencia en la implementación de voto electrónico en Brasil, donde la ruta de trabajo estableció en sus primeras etapas una campaña de educación cívica que duró varios años. Además, se orientó de manera paralela al desarrollo de capacidades de las autoridades electorales para implementar las herramientas, la creación de *hardware* y *software,* la realización de pruebas técnicas en el contexto real del desempeño. Sólo después de eso se tomó una decisión política pensando en todo momento en el contexto sociopolítico brasileño.

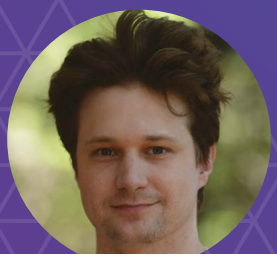
En la tercera y última entrega de esta serie profundizaré sobre los desafíos tecnológicos y políticos de algunos aspectos indispensables en el sistema electoral mexicano, a saber: la necesidad de garantizar la autenticación de los votantes a partir de un padrón confiable, el diseño de interfaces para las mesas de votación y emisión del voto, las medidas que garanticen el acceso universal a estas herramientas, las etapas críticas relacionadas con la tabulación, transmisión y publicación de resultados; todo en un contexto de desconfianza y probables resistencias al cambio.

7-8 NOV

MALTA A.I. & BLOCKCHAIN SUMMIT

AKON

TIM DRAPER



VIRGIL GRIFFITH

JOSEPH MUSCAT

ALEXANDER BORODICH

BILL BARHYDT

MALTABLOCKCHAINSUMMIT.COM

AGENDA CULTURAL

RECOMENDACIÓN DE
LOS MEJORES
MOMENTOS BLOCKCHAIN

Conferencias
Eventos
Meetups
Charlas
Cursos

Legal Blockchain

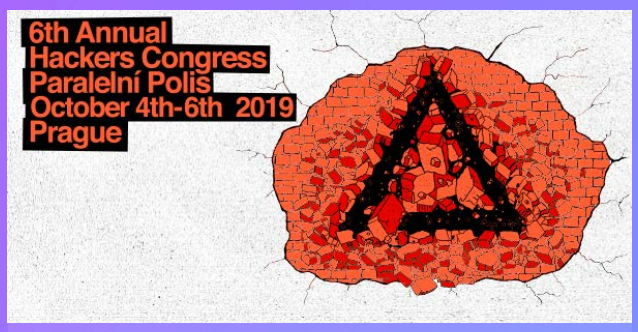
Un summit abierto en el ámbito legal

21 Septiembre

Hotel Vincci Zaragoza Zentro

Zaragoza

Más info >



Hackers Congress

Opt-out of the system

4 - 6 Octubre

Paralelní Polis

Praga

Más info >

Diffusion 2019

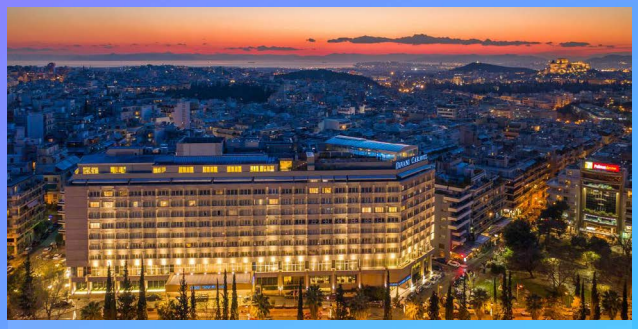
Exploring in DLT / IoT / Big Data / AI

19 - 20 Octubre

Factory Berlin Görlitzer Park

Berlin

Más info >



Decentralized

Blockchain and Digital Currencies

30 - 1 Noviembre

Divani Caravel Hotel

Atenas

Más info >

Convergence

The Global Blockchain Congress

11 - 13 Noviembre

Palacio de Ferias y Congresos

Málaga

Más info >

Crypto Unconference

50 CEOs de Empresa de Crypto

14 Noviembre

Edificio LOOM

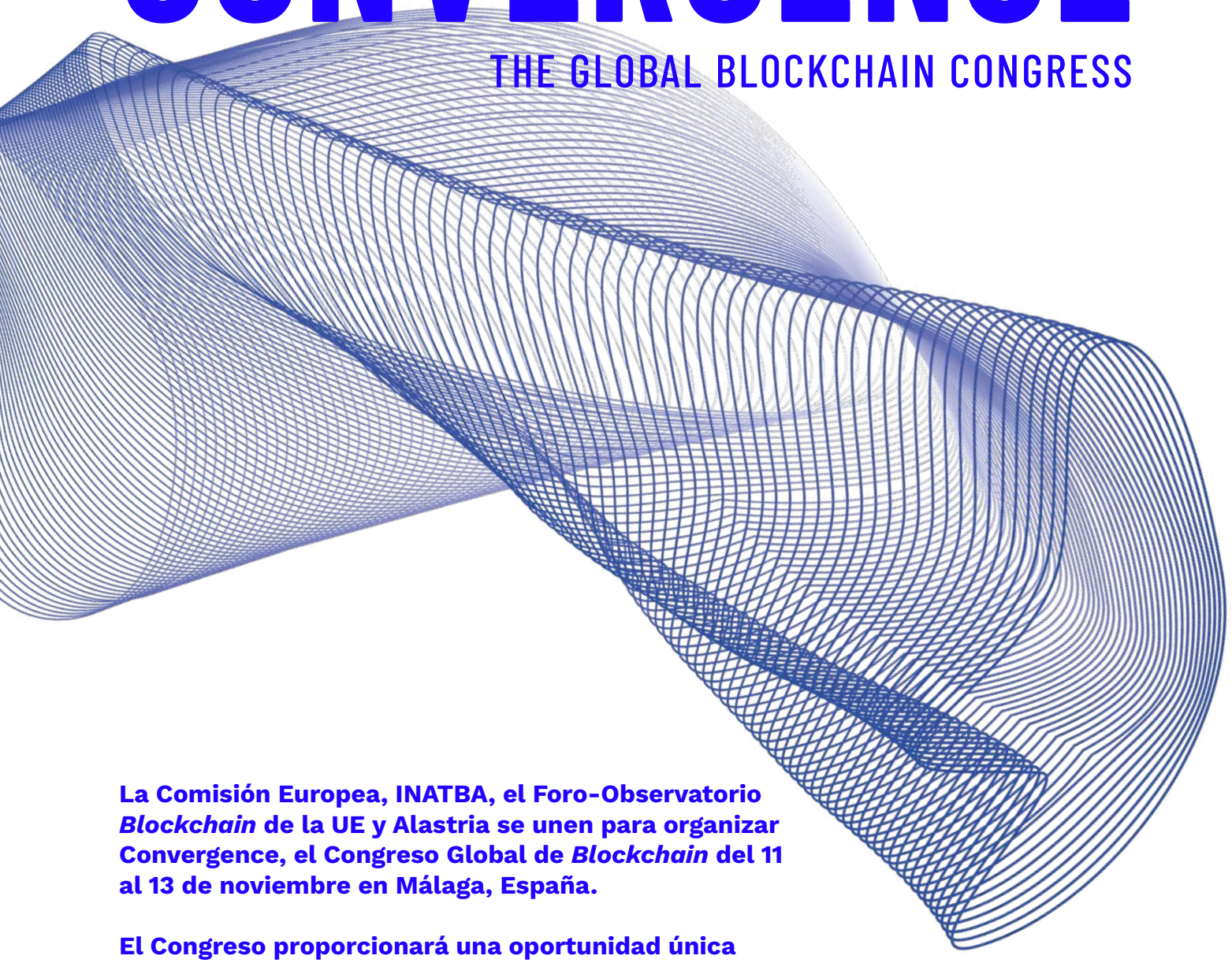
Madrid

Más info >

Descubre todos los detalles de éstos y otros eventos en: https://agorachain.org/eventos/

CONVERGENCE

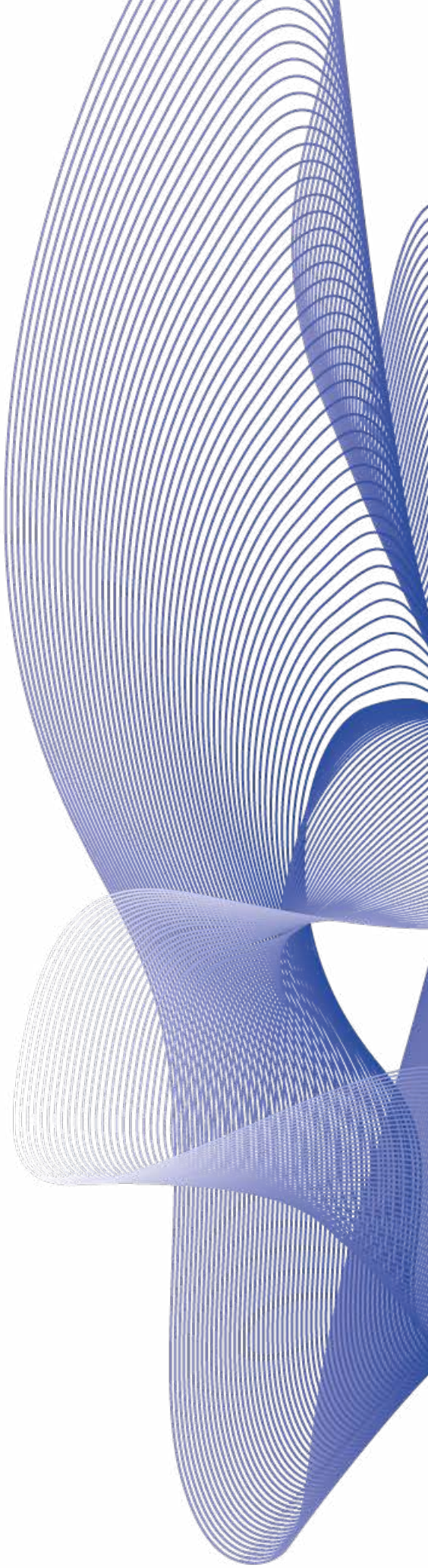
THE GLOBAL BLOCKCHAIN CONGRESS



La Comisión Europea, INATBA, el Foro-Observatorio *Blockchain* de la UE y Alastria se unen para organizar Convergence, el Congreso Global de *Blockchain* del 11 al 13 de noviembre en Málaga, España.

El Congreso proporcionará una oportunidad única para interactuar con reguladores y legisladores, y ayudar a dar forma al debate mundial sobre *blockchain*.

El objetivo de Convergence es reunir a una comunidad mundial de reguladores, responsables políticos, personas influyentes de la industria, desarrolladores, investigadores y emprendedores para un intenso diálogo sobre *blockchain*. El congreso ofrecerá a los participantes la oportunidad de tomar parte en un debate directo con los actores que impulsan y configuran de la industria *blockchain*, y así definir no sólo el futuro de esta tecnología, sino también la próxima generación de Internet y la economía digital.



UN EVENTO ÚNICO

Los participantes disfrutarán de una serie de oportunidades únicas que no han estado antes disponibles en ningún otro encuentro de *blockchain:*

- **Una oportunidad para hablar directamente con los reguladores y los responsables políticos.**
- **Oportunidad de ayudar a establecer las prioridades para el próximo año, resolviendo posibles obstáculos y permitiendo la innovación.**
- **Participación en un evento verdaderamente global con ponentes y participantes procedentes de la comunidad *blockchain* alrededor del mundo.**
- **Colaborar en la construcción de una visión común en términos de trabajo en red, colaboración, innovación, facilitando para ello un diálogo directo con los reguladores y líderes de la industria.**

QUÉ ESPERAR DEL EVENTO:

Convergence reunirá a 1.500 participantes durante un programa de tres días con ponencias, paneles, *workshops* y eventos culturales.

El programa incluye:

- **Un conjunto de ponencias y paneles de debate, dirigidos por conferenciantes de alto nivel y centrados en emprendimiento, casos de uso, investigación, regulación y tecnología.**
- **La definición y anuncio de las prioridades de *blockchain* para el próximo año, con concursos y premios asociados.**
- **Un Challenge Global que reunirá a desarrolladores, reguladores y expertos en negocios para abordar los desafíos prioritarios.**
- **Actividades y eventos paralelos con el objetivo de hacer que la conferencia sea atractiva y estimulante, con el fin de proporcionar una atmósfera inspiradora y propicia para el trabajo colaborativo y el intercambio informal de ideas.**
- **Sesiones «Pregúntame sobre *blockchain*» para fomentar el intercambio de conocimientos.**
- **Reserva la fecha. Las entradas estarán disponibles en las próximas semanas.**

www.blockchainconvergence.com/

COMPARTE Y COLABORA

¿Te ha gustado la nueva revista?

Para poder seguir desarrollándola, necesitamos tu colaboración. Tenemos muchos planes en mente y buscamos nuevos socios en la asociación.

Seguro que puedes ayudarnos de alguna manera.

¡Gracias!

DONACIONES

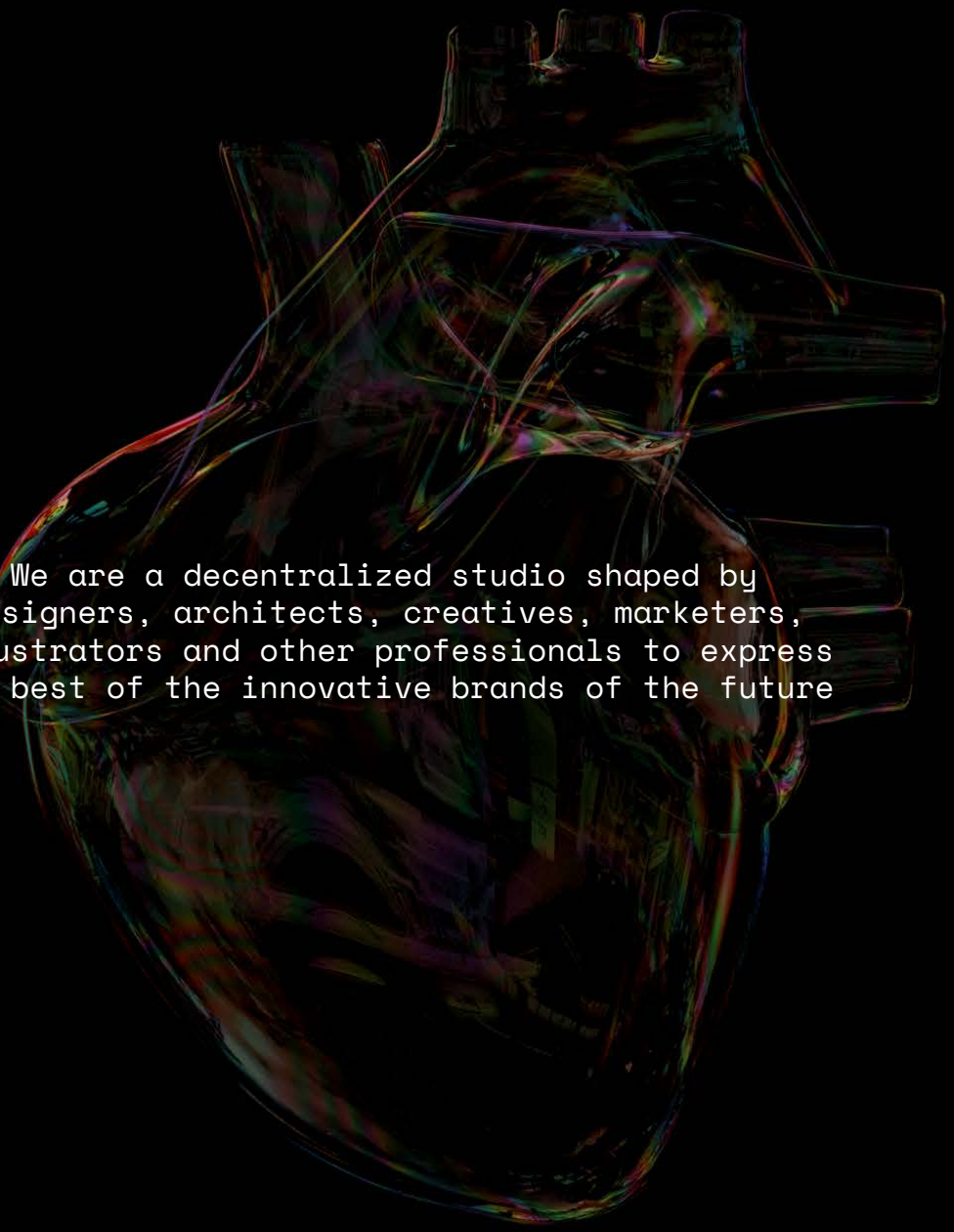
BTC:
125xFwYc6hEkAgVGVmWXHjsQvtP5QEfMJw

ETH:
0xAE905743D4c630e9B563e91CCC11cD94F6578Fd7

TIPPIN.ME
https://tippin.me/@AgoraChain

ASOCIACIÓN AGORACHAIN, con domicilio social en AVDA. DIAGONAL 460, 4-1 con NIF nº G67257329 está inscrita en el Registro Nacional de Asociaciones, Sección 1.ª, Número Nacional 616346. asociacion@agorachain.org
Impresión: Ulzama - Edita: Aguaclara - Diseño: FLOC* - Corrección: tuCriptomoneda - Depósito Legal: A263-2019.

FLOC*



We are a decentralized studio shaped by designers, architects, creatives, marketers, illustrators and other professionals to express the best of the innovative brands of the future

*FREE LEADERS ON COLLECTIVE

wearefloc.com

ÁGORA es un sistema abierto a
colaboraciones y uniones para mejorar
el ecosistema *blockchain.*

Ayúdanos a crear una plaza
pública y únete con tus
ideas para replantear el futuro.

AGORACHAIN.ORG