ICANN75 | Reunión General Anual – Tecnologías de Identificadores Emergentes
Miércoles, 21 de septiembre de 2022 – 15:00 a 16:00 KUL

ADIEL AKPLOGAN: La sesión de hoy inicialmente estaba planificada para estar dedicada a los nuevos tipos de sistemas de nombres, sobre todo aquellos que se basan en sistemas de nombres alternativos. Ya hemos tenido sesiones sobre identificadores emergentes. Esta sesión es una continuación de aquellas sesiones previas en vista de la evolución de estas tecnologías. La OCTO también generó un documento en el cual se estudian estos sistemas de nombres alternativos y los desafíos que implican.

Hoy vamos a escuchar a Alain. Alain Durand es miembro de nuestro equipo de investigadores en la ICANN y él es el autor de este documento OCTO-034 en el cual se presentan los desafíos que abordaremos en esta sesión. Él va a comenzar dándonos un contexto sobre esta situación.

Luego tendremos a Luc van Kampen, de ENS, que nos hablará acerca del sistema de nombres de Ethereum. Luego tendremos también una sesión de preguntas y respuestas. Por último tendremos una presentación que no tiene que ver directamente con un sistema de nombres alternativo pero que está incluida en el título de esta sesión: identificadores emergentes. En este caso,

en esta última presentación escucharemos a Jacques Latour, de Cira. Vamos a avanzar con las presentaciones. Le voy a dar la palabra a Alain. Adelante, Alain.

ALAIN DURAND: Hola. Buenos días o buenas tardes o buenas noches. Sé que es un poquito más tarde en Kuala Lumpur. Me hubiera gustado estar con ustedes allí de manera presencial pero esto no ha sido posible. Espero que puedan recibir bien mi audio. Si me lo confirman, por favor, se lo voy a agradecer.

ADIEL AKPLOGAN: Sí, sí. Lo podemos oír.

ALAIN DURAND: Muchas gracias. Muy bien. Hoy les voy a hablar acerca de un documento que publicamos en este año. Es el documento OCTO-034. Este documento versa sobre los desafíos que representan los sistemas de nombres alternativos. El objetivo de este documento es ver los sistemas de nombres alternativos, no los sistemas suplentes o complementarios, que no es lo mismo que alternativo.

Veamos los desafíos técnicos que implica justamente la implementación de estos sistemas alternativos. Muy bien. El

objetivo es ahondar en las tecnologías subyacentes de estos sistemas de nombres y cómo funcionan. No vamos a abordar la cuestión de los procesos de políticas en relación a estos sistemas de nombres alternativos en esta presentación sino que más bien nos concentraremos en los desafíos de índole técnica. Aquí en la pantalla vemos un enlace que les permite a ustedes descargar este documento.

Estos sistemas de nombres alternativos no son nada nuevo. Existen e incluso algunos son previos a la ICANN. Eso llevó a una situación un tanto confusa y en el 2001 se publicó el documento ICP-3 de la ICANN en el cual se manifestaba que estos sistemas alternativos serían un tanto problemáticos.

Tengan presente que esto no es algo nuevo. Ya tiene algunos años. ¿Por qué esto está volviendo a ser el foco de atención? Bueno, eso se debe al tema de la tecnología blockchain que se está utilizando para sistemas de asignación de nombres. Tenemos tres sistemas muy populares, sistemas alternativos de asignación de nombres. Tenemos el sistema Handshake, tenemos el sistema ENS, de Ethereum, y tenemos también Unstoppable Domains que deriva de ENS.

No se requería utilizar sistemas basados en blockchain para crear esta tecnología porque se utilizaba el DNS pero, por algún motivo, los desarrolladores de los sistemas de blockchain

decidieron crear su propio sistema de nombres. Esta es la primera observación que quiero compartir con ustedes.

Ya sabemos que esto no es nuevo y que hay registradores acreditados por la ICANN que están vendiendo estos nombres que utilizan esta tecnología blockchain. Recordemos que estos dominios que utilizan blockchain no se rigen por las políticas de la ICANN sino por políticas propias e independientes. No sé si esto es bueno o malo. Simplemente les estoy describiendo un hecho. Siguiente, por favor.

Ahora veamos cómo se implementan estos sistemas de nombres alternativos. La pregunta que surge es cómo pueden los usuarios de Internet resolver un nombre mediante un sistema alternativo. Nosotros podemos comprar un nombre y eso es sencillo. Podemos utilizarlo en nuestro propio servidor y eso también es algo sencillo. La pregunta de fondo aquí es cómo hace un usuario común y corriente de Internet para acceder a estos nombres a través de los resolutores.

Hay diferentes maneras de lograrlo. Básicamente, si utilizamos una aplicación nativa podemos tener una biblioteca dedicada y tenemos distintos lenguajes de programación muy populares hoy en día que se utilizan. Es decir, no es muy difícil, no es algo nuevo. Se utiliza esta biblioteca y se puede hacer.

Si tenemos una aplicación más antigua, por ejemplo un correo electrónico o un buscador web de los que usamos siempre, ahí la cosa se complica un poquito. Necesitamos técnicas de puenteo o *bridging*. Podemos utilizar un puente de URL para llegar a estos dominios. Podemos ingresar un nombre en nuestro resolutor local o en un resolutor que opera nuestro ISP o tener buscadores web dedicados, específicos.

De todo esto siempre surge algún inconveniente, sobre todo si uno le dice a la gente que utilice tal o cual buscador o que agregue una extensión a su buscador para encontrar el nombre. Eso requiere cierto tipo de intervención manual. Funcionaba bien para los entusiastas al principio pero no se puede utilizar bien a gran escala.

Tenemos un desafío que consiste en comunicarles esto a nuestros posibles clientes. También hay que decirles cuál es el nombre de dominio y también hay que darles instrucciones acerca de qué es lo que tienen que hacer para poder resolver ese nombre. Le tenemos que decir: “Tienes que usar este buscador en particular pero no puedes usar este otro”. Eso es un tanto problemático.

Como les comentaba, este *bridging* o puenteo se puede hacer en un resolutor recursivo. Siempre se decía: “Bueno, quizá lo puede hacer el ISP, los resolutores públicos”, pero hay que ser

cauteloso porque esto puede derivar en cierta inestabilidad del servicio porque la resolución de los resolutores depende del resolutor que se utilice. Hay algún resolutor que tiene tal o cual función y otro resolutor que tiene tal otra función. Esto genera problemas en la uniformidad.

Por ejemplo, estamos en casa. Tenemos una red inalámbrica wifi y nuestro operador de tecnología celular no es el mismo que opera nuestra red inalámbrica. Si conectamos el teléfono móvil a la red celular o a la red inalámbrica vamos a tener un resolutor u otro resolutor y vamos a tener distintas respuestas si los resolutores no están configurados de la misma manera. En mi casa yo tengo red inalámbrica, que no es muy buena, entonces paso a mi red de contenido celular y en una red puedo ver algunos dominios y en otra no. Es decir, tengo estos problemas de uniformidad en el servicio. Es difícil explicar esto a los usuarios comunes y corrientes.

Esto tiene que ver con cómo implementamos un sistema alternativo, ¿pero qué pasa si implementamos varios? Yo les comenté que hay por lo menos tres sistemas alternativos principales. El problema es que no tienen coordinación entre ellos y tampoco hay coordinación entre estos sistemas alternativos y el DNS. Por eso es inevitable que surjan las colisiones de nombres que son problemáticas. Ya se han

publicado documentos del SSAC en los cuales se describen estos problemas de las colisiones de nombres.

Hay un enfoque un tanto ingenuo que consiste en decir: “Qué bueno. Tengo más sistemas de nombres. Si no consigo el nombre que quiero en un sistema, puedo ir a este otro sistema. Tengo mucha más posibilidad de elegir” y esto es un tanto ingenuo. La pregunta que surge es cómo hace la gente para encontrarte. Le digo que use esta aplicación pero esa aplicación te conecta con un solo sistema de nombres a la vez y a veces esto también es inestable con lo cual necesitamos una aplicación específica para cada sistema de nombres en el cual esté nuestro nombre y eso complica bastante las cosas. Si no, vamos a tener resoluciones de nombres inestables e impredecibles, que es lo que me pasa a mí en mi hogar cuando utilizo la red inalámbrica o la red celular, porque están configuradas de distinta manera y es muy difícil resolver estos inconvenientes. Los usuarios diarios, comunes y corrientes que no tienen conocimiento técnico, no pueden resolver estas cuestiones.

En realidad, el riesgo es la fragmentación. La fragmentación de Internet al crear ecosistemas separados. Uno para cada sistema de nombres. Yo puedo decir: “Yo estoy en esta familia de nombres alternativos y utilizo esta familia de aplicaciones” pero luego tengo que ir a esta otra familia de aplicaciones pero

ninguna funciona con la otra o se comunica con la otra. Ese no es el resultado que queremos.

Aquí entonces volvemos de nuevo al comienzo de la década del 2000, cuando se redactó este documento ICP-3. Aquí tengo algunos extractos de este documento ICP-3. Este documento reafirma el compromiso de la ICANN a una única raíz pública para poder tener justamente procesos desarrollados por la comunidad en pos del interés público. Es decir, surgen las mismas cuestiones. Quizá no las mismas cuestiones técnicas, porque estos sistemas no se basan en protocolos de Internet, pero surgen estas otras cuestiones, las colisiones de nombres, etc. que sí son las mismas.

No quiero decir que este documento, el ICP-3, se aplique a esta situación sino que debería ser nuestra fuente de inspiración y debería impulsarnos a medida que debatimos estas cuestiones. A veces las personas hablan acerca de colisiones de nombres y dicen que no es un problema demasiado grave. Ahora les voy a presentar una historia animada que les va a contar una situación que pueden experimentar los distintos usuarios finales a causa de las colisiones de nombres.

Tenemos dos personajes en esta historia. Tenemos a John, que es un geek, alguien muy técnico, y tenemos a Sally, que le gusta un poco la cosa técnica pero no tanto. Luego tenemos a otro

personaje que se llama Mercado. John dice: “Yo quiero tener un nuevo nombre de dominio porque le quiere causar una buena sensación a Sally. Le voy a pedir al Mercado que me venga algo que sea lindo, que sea atractivo” y el Mercado dice: “Te vendo este nombre: john.criptonita” y John le dice a Sally: “Sally, ¿por qué no te conectas conmigo? Mira, tengo este nuevo nombre: john.criptonita”. Sally dice: “Claro, sí, sí” pero no funciona y John le explica: “Ah, no te lo había dicho. Primero tienes que instalarte este buscador web” y Sally dice: “No lo conozco. ¿Será seguro?”

Más adelante, John le dice: “Mira, ahora tengo esta tecnología blockchain que también está buenísima. Le voy a pedir al Mercado que también me dé un nombre de dominio en esa tecnología” y el Mercado dice: “Claro, claro. Te puedo vender john.superblockchain”. John le dice a Sally: “Sally, tengo otro nombre que se llama john.superblockchain” y Sally le responde: “John, instalé el buscador especial que me dijiste la otra vez y ahora, con este nombre john.superblockchain no funciona. ¿Qué pasa?”. John le dice: “Ah, Sally, me olvidé. Este es otro nombre de blockchain. Necesitas instalar otro buscador con otra extensión” y Sally le dice: “Per por favor…”

Más adelante Sally y John se comunican, y Sally le dice a John: “Bueno, seguí todos los pasos que me dijiste y llegué a john.superblockchain pero cuando vuelvo al primer nombre, john.criptonita, veo el perfil de mi exnovio”. “¿Cómo?”, dice

John. “Yo no hice nada. Este es mi perfil”. Entonces John vuelve al Mercado y le dice: “Sally no está contenta con este resultado porque ella ve una cosa y yo veo otra cuando escribimos john.criptonita” y el Mercado dice: “Bueno, esta es la colisión de nombres. Hay por lo menos tres tecnologías blockchain que lo están utilizando. Tú estás buscando en un espacio. Ella está buscando en otro y por eso ven cosas diferentes”.

John dice: “¿Qué pasa? ¿Por qué mi nombre no es único, john.criptonita?” y el Mercado le dice: “Bueno, porque nadie te garantiza que estos nombres sean únicos. Además tengo otro nombre, john.criptonita en un tercer sistema blockchain. ¿Te lo vendo a ti o se lo vendo al exnovio de Sally?” John dice: “Esto no funciona. Esto es algo muy estúpido. Voy a volver a mi TLD, john.icann.tld, que realmente era único” y el Mercado le dice: “Ahora no te puedes escapar de la colisión de nombres porque también ese TLD está disponible en distintos sistemas de nombres alternativos”. Muchísimas gracias por su atención. Por prestar atención a esta historia que muestra un poco qué es lo que puede suceder con las colisiones de nombres.

ADIEL AKPLOGAN: Muchas gracias, Alain, por haber terminado con un buen comentario usando esa escena cómica. En base a su presentación, puedo señalar tres puntos clave. Nosotros

tenemos la confusión del usuario que estuvo bien ilustrada por las caricaturas que nos mostró y el enfatizar los elementos que pueden llevar a la fragmentación del DNS. Al principio también puede afectar a Internet globalmente.

Habiendo dicho esto vamos a seguir con la siguiente presentación antes de aceptar preguntas con respecto a la primera parte de la sesión. Luc, le voy a dar la palabra. Usted es de ENS, que es uno de los espacios alternativos. Tiene la oportunidad de compartir con nosotros lo que está haciendo allí. Gracias.

LUC VAN KAMPEN: Okey. ¿Me ven? ¿Me escuchan? ¿Ven mi pantalla? Qué bien. Muy bien. Buenos días, buenas tardes y buenas noches, donde estén, ya sea que estén aquí con nosotros presencialmente o remotamente, ya sea en Kuala Lumpur o a través de Zoom. Gracias por estar aquí. Gracias por su tiempo. Como se ha dicho, mi nombre es Luc van Kampen y estoy aquí para hablarles acerca del servicio de nombres de Ethereum.

Internet está evolucionando a diario y estamos aquí manteniéndolo. En [1989] se comenzó ICANN para darle claridad y lógica al Internet caótico fragmentado. En el 2004 tuvimos las redes sociales, centralización, casi 80 millones de sitios web que daban servicio a mil millones de usuarios. Lo decidimos llamar la

era de la web 2.0. Hoy en día vemos a 5.000 millones de usuarios en Internet y aproximadamente el 63% de la población. Con esto el mundo está cambiando rápidamente y con esto también está cambiando la autenticación.

Estamos viendo un cambio bastante rápido de autenticación basada en la contraseña a una llave pública. La autenticación no es algo nuevo. Ya lo estamos viendo constantemente. La tecnología se usa siempre. El HTTPS, SSL, PGP y más importante aún DNSSEC. Obviamente hay muchos más.

¿Cómo afecta esto a la autenticación? La autenticación soluciona muchos problemas o cuestiones. Aquí hay un par. Por ejemplo, contraseñas inseguras, escapes de contraseña, hackeo masivo de las cuentas y disponibilidad de nombre. Con la autenticación pública ya se les acabará el tiempo para estas cosas.

Miremos la última diapositiva con las redes sociales. Aquí hay algunas. Está @icann, @icannorg, porque el Facebook de ICANN lo tomó la persona que se llama [inaudible], @icann en Instagram, @icannnews, que es un canal de vídeos de perros en YouTube, ICANN fotos, en Flickr e ICANN en SoundCloud y también la página web de ICANN.

La llave pública soluciona ciertos problemas. Normalmente los usuarios tienen una llave pública que los identifica en Internet.

Se ve como este. Este es el mío, por si se lo preguntan. Una llave privada se queda en el dispositivo. El usuario puede usar su dispositivo local para inscribirse con una autenticación de dos vías. Comunicarse a través de su contraseña, pueden ser su biométrica, su contraseña favorita, un código PIN, que es algo normalmente local y parte de su dispositivo.

Desde la perspectiva de seguridad, esto es muy bueno porque tiene una seguridad inquebrantable. Se necesitarían muchos recursos por mucho tiempo para poder entonces entrar en esto. La escalabilidad es increíble porque ya no necesitamos los servidores para rastrear los nombres y las contraseñas. Simplemente se usan en el dispositivo y se usa la clave del dispositivo para esto. Desde la perspectiva de la lectura de máquina es igual porque se usa un carácter fijo predefinido, etc. además de más información.

Por último, aunque no menos importante, es la lectura humana. Les voy a decir seriamente. De pronto yo entro en la página web una vez y no lo voy a volver a hacer porque es muy largo y es de 64 caracteres. Aquí es donde hablamos del tema de ENS. ENS es el servicio de nombres de Ethereum. Integra la autenticación de la llave pública con el sistema de nombres de dominio existente. Esto quiere decir que cualquiera que tenga un DNS existente se le puede identificar a través de toda la web.

Si se acuerdan de la última diapositiva que mostraba los diferentes nombres, esto se podría cambiar a icann.org en todas partes. Este emoji de una llave, eso quiere decir que cualquier acción que yo tome se puede autorizar con un solo usuario, con un solo dispositivo o multisincronización. Cualquier persona puede acceder a eso por Internet.

¿Quién soy yo? Como dije anteriormente: luc.computer. Es un dominio que yo registré con un registrador y lo usé con mi nombre primordial. Cualquiera de las páginas web o sitios web a los que vaya van a ver esto visiblemente y van a poder luc.computer. Si lo buscan y ponen luc.computer, lo van a encontrar con 0x225 y demás. ¿Cómo se ve esto? Se ve igual aquí, como se ve aquí en la pantalla. Esto se encuentra en el sitio web de ENS. O como en este. O como en este. O como en este. También en Edge Server y en muchos más sitios. En este momento, 2.4 millones de nombres ya se han conectado través de ENS esparcido a través de 600.000 usuarios y a través de más de mil sitios web diferentes.

¿Cómo funciona esto exactamente? Como solo tengo 10 minutos para hablar, tengo tiempo limitado, trataré de decirlo brevemente. ENS es el servicio de nombres de Ethereum. Se usa el blockchain de Ethereum. Es una hoja de cálculo pública que permite tener la información de una manera descentralizada. ENS también son unos contratos inteligentes que se guardan en

blockchain, que tiene reglas predefinidas de qué acciones se permiten y cómo se deben hacer. Esto permite que nosotros almacenemos toda la información en blockchain.

¿Cómo es esto? Es muy sencillo. Este es uno de los contratos inteligentes donde puede guardar mi nombre y mi dirección pública, mi nombre de dominio. Mi dirección pública es lo que yo utilizo por toda la web para la autenticación y obviamente información adicional donde puede señalar hacia otro resolutor donde puede estar mi nombre y mi avatar, mi biográfica o mi información de LinkedIn o de Twitter, y obviamente mucho más.

Esta es la esencia nuclear. Nosotros en ENS visionamos un mundo donde todos pueden usar su dominio como un identificador visual. Cualquier dominio de DNS válido da su apoyo a DNSSEC. Puede ir a cualquier contrato inteligente, enviar su nombre de DNS junto con su reclamación de que usted es dueño de eso, y así acuden al servidor de DNSSEC, hacen una validación y después dicen: “Luc, sí es el dueño de luc.computer” y eso me da la autorización en los records.

También es igual la transferencia de propiedad. Si yo decido por ejemplo que por alguna razón quiero vender luc.computer a otro individuo y hago el cambio en el registro adecuadamente, entonces el otro individuo que es dueño de luc.computer puede ir al contrato DNS y decir: “Mire, quiero reclamar este nombre y

este es mi comprobante". El contrato ENS hace la validación de esto y entonces el nuevo dueño se establece.

Como mencioné anteriormente, nosotros sí proveemos un registro on-chain y se provee para los usuarios de blockchain. Esto se hace en .ETH. Es el único TLD que proveemos. Este TLD permite que nosotros podamos hacer más cosas de lo que puede hacer ICANN. Nos permite alojar estas web descentralizadas.

Esencialmente, los usuarios pueden visitar una página web sin utilizar ningún servidor de web centralizado. Ya no se necesita enrutamiento de DNS o una estructura bastante complicada. Simplemente uno puede poner su página web y cualquier dispositivo que cargue inmediatamente puede ser un cache para los usuarios, aunque ese ya es otro tema.

Aparte de eso, los dominios de .ETH tienen sus tarifas de registración para asegurase de que estén disponibles los nombres y asegurar el nombre. Son cinco dólares al año. Esta es una cantidad razonable. Como se define, el DAO tiene control de esto y por eso no es posible para una sola persona comprar todos los nombres disponibles.

Todas las tarifas de registración de .ETH se llevan al ENS DAO, que es una organización sin fines de lucro que ayuda en este sentido. Sus siglas significan Organización Autónoma Descentralizada. El modelo de ellos es igual casi al modelo de

múltiples partes interesadas de ICANN. Es transparente, gobernado por el público, tiene grupos de trabajo, propuestas de mejora, cualquier persona puede participar.

Ustedes preguntarán por qué o cuál es el motivo. Somos una colección de contribuidores fundada por el público y la financiación es a través de DNS DAO y cada año ponemos en la propuesta la cantidad que necesitábamos, la cantidad que se aportará a los salarios o al transporte o a mercadotecnia, contabilidad. Después ENS DAO entonces decide si acepta la propuesta o no. Decidimos entonces si hay alguna controversia. Entonces el DAO toma el mando.

Contrario a cualquier sistema de nombres, nuestra meta es extender y mejorar la funcionalidad corriente, tomando en cuenta el día de mañana. Creo que después de la siguiente charla tendremos tiempo para preguntas y respuestas. Si tienen una pregunta o no se contestó su pregunta puede comunicarse conmigo en luc.contact, que es otro dominio. Gracias por su tiempo. Estoy ansioso por poder ver las cosas excelentes que podemos hacer juntos.

ADIEL AKPLOGAN: Gracias. Esta es una presentación interesante ya que esto nos muestra qué está haciendo ENS. Lo que es interesante es el caso de uso para este sistema de nombres alternos que es diferente al

DNS como lo conocemos hoy. Antes de seguir con la siguiente presentación les propongo que empecemos una sesión de preguntas y respuestas sobre estas dos sesiones que están muy relacionadas. Podemos hacer eso por unos 15 minutos antes de seguir con la siguiente ponencia. ¿Tenemos alguna pregunta de los que están participando en línea, por Internet?

DAVID HUBERMAN: La pregunta es de Ajith Francis. Es para Luc. Es de dos partes. La primera parte es si el cambio de modelo de .ETH impacta en la accesibilidad y la descentralización de ENS. La segunda pregunta, desde la perspectiva del usuario final: ¿Cuándo será posible o se espera que pueda llevarse a cabo la integración entre los nombres de dominio y los nombres de dominio ENS?

ADIEL AKPLOGAN: Gracias.

LUC VAN KAMPEN: No está relacionado con ENS sino con el sistema de Ethereum. Se cambió el modelo y se redujo en un 98% el uso de energía. Esto quiere decir que la petición que se hizo de cambios en la red de Ethereum, se hizo mucha actualización del equipo Ethereum para mejorar los gastos de combustible, etc. Aunque esto afecta

un poco la vida de los que usan el ENS pero no es un conjunto. Funcionaba sin problemas y lo sigue haciendo.

¿Cuándo podemos esperar esta integración? Es difícil contestar a esto porque vemos que miles de sitios web se están desarrollando en este ecosistema usando esta autenticación pública junto con carteras excelentes para poder conectarse a estos sitios web.

Como mencioné anteriormente, todavía existen muchas cuestiones. La principal es la integración. Con tal de que el ENS no se implemente a nivel de DNS o a nivel de raíz, el usuario de ENS requiere una interacción manual, instalar una autenticación o un navegador. Espero que eso haya contestado su pregunta.

ADIEL AKPLOGAN: Gracias, Luc. ¿Alguna otra pregunta en la sala?

BEN MCILWAIN: Hola. Ben McIlwain, de Google Registry. ¿Qué ocurriría si en la próxima ronda de TLD de ICANN alguien solicitase .ETH en la zona raíz del DNS? ¿No causaría diferentes niveles de colisiones?

LUC VAN KAMPEN: Como dije, sí, es una situación difícil en cuanto a los nombres. Hay partes que están tratando de registrar grandes TLD y hasta

las tratan de subastar pero yo le puedo dar el .ETH a uno que no forme parte del servicio de Ethereum y eso sería algo malo para el ecosistema. Queremos asegurarnos de que esto no pase y hacer lo posible para apoyar y asegurarnos de que todo esté disponible y todavía funcionando.

ADIEL AKPLOGAN: ¿Tengo entendido que piensa entonces solicitar ese TLD?

LUC VAN KAMPEN: No estoy completamente seguro. Tendría que preguntar al equipo.

WARREN KUMARI: Según la guía lógica, Ethereum no puede solicitar el .ETH porque si uno no tiene un archivo de zona, no lo puede hacer. Obviamente eso es según la última guía para el solicitante. No sé si hay algo más corriente.

LUC VAN KAMPEN: Creo que en el evento de que sí consigamos .ETH es posible que nosotros podamos establecer un servicio separado porque el DNS y el sistema de nombres ICANN requiere que haya una IP central disponible. No podemos lidiar con las zonas [BGP]. En una situación hipotética, nosotros podemos montar servidores

para que esté disponible esto. Esto va a requerir una intervención manual, especialmente por el lado de los dueños de dominios. Si registro .ETH y quiero estar en el DNS, entonces hay que optar por hacer esto en el sitio web para asegurarnos de que estén cumpliendo con todos los requisitos de ICANN a tal punto.

ADIEL AKPLOGAN: Muchas gracias. John.

JOHN CRAIN: John Crain, CTO de la ICANN. La tecnología es muy interesante, sin duda. La organización para la cual trabajo, la ICANN, y la comunidad de múltiples partes interesadas se ocupan de la política y de la tecnología. Me pregunto qué clase de normas y medidas de protección tienen implementadas para afrontar todo tipo de conducta indebida que pueda surgir en estos nombres de dominio, amenazas a la seguridad en este espacio de nombres.

LUC VAN KAMPEN: Básicamente en la implementación actual del servicio de nombres de Ethereum y las extensiones implementadas y las integraciones que ya tenemos los nombres no pueden ser revocados ni se los puede remover bajo ninguna circunstancia. Sin embargo, si tuviésemos un gateway o puerta de acceso para los registros del DNS, seguramente podremos implementar esas

medidas y también asegurarnos de tener registros de WHOIS, etc. Vamos a estar en cumplimiento con la ICANN.

JOHN CRAIN: Si entendí bien, en la situación actual, si yo soy un delincuente y registro un nombre en su espacio, estoy a salvo a día de hoy. No voy a perder mi nombre.

LUC VAN KAMPEN: En el sistema actual todo lo que está en el servicio de nombres de Ethereum y registrado en .ETH está protegido de la censura por completo hasta tal punto que necesitamos un 51% de consenso a nivel de Ethereum o ENS para que se hagan cambios.

ADIEL AKPLOGAN: Gracias. Vamos a pasar a la próxima presentación. Si tenemos tiempo, al final de esta sesión haremos otro bloque de preguntas y respuestas. Ahora va a tomar la palabra Jacques para dar su próxima presentación que versa sobre las tecnologías de identificadores emergentes y la identidad digital.

JACQUES LATOUR: Hola. Espero que puedan oírme bien. Muy bien. Voy a continuar. Voy a tratar de ser rápido. Soy Jacques Latour. Trabajo en CIRA. Estamos a cargo del registro .CA. En los últimos años estuve

trabajando con DIACC, la Autoridad de Identificación Digital de Canadá, y creamos un laboratorio digital en Canadá para trabajar con la comunidad de identidades digitales en Canadá y entender más acerca de los desafíos que esto implica y los niveles de confianza. Ese es el tema de mi presentación.

En un mundo en el cual tenemos registros de conductores que son digitales, etc., no voy a hablar de billeteras digitales en esta presentación sino que más quiero hablar acerca del ecosistema. Tenemos emisores que emiten credenciales verificables que son enviadas a una billetera y esa billetera la guarda de la misma manera que nosotros podemos guardar nuestra licencia de conducir física en nuestra propia billetera y luego esto es verificado. Así es como funciona este ecosistema. Es todo digital y los usuarios pueden mostrar sus credenciales verificables o parte de ellas.

Esto se aplica a los diplomas universitarios, a la licencia de conducir, etc. Veamos un caso real. CIRA tiene un proceso de verificación de presencia en Canadá. En el caso de algunos nombres de dominio tenemos que verificar que el registratario sea canadiense o bien resida en Canadá para cumplir con este requisito. Hoy, en el mundo real, esto se utiliza en los pasaportes o se piden licencias de conductor o partidas de nacimiento y nosotros no queremos hacer eso. Nosotros vamos a emitir una credencial verificable. Esto es lo que hace el gobierno de Canadá.

Lo hace para la licencia de conducir, para el pasaporte, para el acta de nacimiento. Todos estos tienen firmas digitales y están dentro del dominio .CA que es conocido por todas las personas en Canadá y es confiable para las personas de Canadá.

Todo esto se firma y pasa a una billetera digital. Nosotros, en CIRA, somos los verificadores de estas identidades y el registratario simplemente nos da la información suficiente para demostrar que es canadiense o residente en Canadá. La pregunta que surge es: ¿Cómo sabemos que el emisor es confiable, el emisor que ha emitido esas credenciales? Por ejemplo, cómo sabemos que se trata de una licencia de conducir válida y no una licencia falsificada.

Por ejemplo, qué pasa con un pasaporte. El pasaporte va a ir a determinadas billeteras digitales y luego el verificador, que es CIRA, puede solicitar determinada información. Es decir, hay todo un tema con respecto a la confianza en todo este ecosistema que es necesaria. Es decir, hace falta la confianza para que este sistema exista, para que se puedan verificar sus componentes y para que funcione.

¿Cuál es la solución? Tener un registro de confianza, que es un componente clave. Se lo puede utilizar para verificar la autenticidad del emisor. Por ejemplo, Luc hablaba de la clave pública. Tenemos la clave pública del gobierno canadiense en

este caso que coincide con lo que está en el registro y el registro puede decir que el emisor puede emitir tal o cual credencial. Este registro de confianza permite verificar que las partes pertinentes son quienes dicen ser.

Esta es la arquitectura del sistema. El desafío es el siguiente. Este registro de confianza hasta ahora no está bien definido. Tenemos esta definición de este registro de confianza, que sería una especie de directorio o repositorio donde tenemos registraciones similares dentro de una entidad que gobierna todo esto y dentro de un marco. Por ejemplo, podemos tener el ecosistema académico para las universidades en Canadá. Es decir, todas las universidades de Canadá pueden emitir un certificado o un diploma. Por ejemplo, podemos tener distintas entidades que son confiables y que pueden estar en este registro pero en Canadá tendríamos cientos de registros de confianza y este es el desafío que enfrentamos en este momento en la comunidad de identidades digitales. Es decir, qué hacemos. ¿Vamos a tener un registro de confianza? ¿Vamos a tener cientos de registros de confianza? ¿Cómo sabemos cuál es confiable, cuál no? Otra cosa. Si estoy en Canadá, ¿cómo hacemos con el registro de confianza académico? ¿Cómo sabemos que son quienes dicen ser? Hoy en día se están construyendo distintos ecosistemas de identidades digitales que dificultan que los

participantes puedan confiar en estos registros porque le falta algo desde el punto de vista jerárquico.

Cuando yo comencé a investigar el tema de la identidad digital, etc. lo primero que pensé fue: “No hay un identificador único”. Vimos y escuchamos que la gente puede crear su propio dominio, su propia identidad. Podemos tener al gobierno de Quebec, por ejemplo, utilizando blockchain. Hace falta tener una estructura de identificadores global e interoperable en Canadá. También necesitamos identificadores únicos para verificar las credenciales porque si no, no las podemos verificar.

Creo que podemos utilizar al DNS para los emisores y para verificarlos. Es decir, para quienes emiten documentos nacionales de identidad, licencias de conducir, pasaportes, etc. Es decir, todos ellos deben tener nombres de dominio y luego necesitamos utilizar DNSSEC como cadena de confianza para garantizar la confianza en todos estos pasos. Creo que la tienen todos los ccTLD del planeta. Tenemos un DNS único. Tenemos un anclaje de confianza global. Tenemos registros globales. Tenemos un registro de confianza nacional. La estructura, la arquitectura se vería como está aquí en pantalla.

Es decir, tenemos este anclaje global de confianza en la zona raíz y tenemos por ejemplo dentro de la ICANN la IANA. Tenemos un registro de confianza global para nombres de dominio con

códigos de país donde estarían todos los ccTLD y todos los registros de ccTLD. Ahí podemos tener el registro de confianza de Canadá, por ejemplo en este país, y luego podemos tener el registro de confianza nacional.

Por ejemplo, la universidad, la asociación profesional de tal o cual profesión. Es decir, todas las asociaciones que necesitan su propio ecosistema. Cada país puede tener su propia estructura y podemos hacer lo mismo en el ámbito comercial. Esta estructura permite tener un identificador único, una infraestructura única de identificadores que es lo que falta, por lo menos desde lo que yo veo, cuando se emiten credenciales en blockchain. Hay muchas cadenas de blockchain, muchas tecnologías de blockchain en distintos ámbitos y no sabemos dónde verificar todo esto. Es decir, vemos una proliferación de blockchain y de la tecnología *ledger* que hace que los identificadores únicos no sean únicos en el entorno de la identidad digital. Esto no es para las billeteras sino para los emisores, para que sus credenciales o las credenciales que emiten sean únicas y para que se las pueda verificar. Permite justamente verificar la información en consonancia con una estructura única.

Puedo seguir hablando acerca de este tema. Voy a agregar lo que compete al DNS y a las DNSSEC. Lo que tratamos de hacer es tener un mecanismo en el DNS para localizar a los registros de confianza asociados a un emisor de credenciales verificable.

Luego podemos ver si este emisor está registrado en un registro de confianza. También podemos ubicar documentos de identidad digitales (DID) de un nombre de dominio.

El DNS es descentralizado, distribuido y ampliable. Creo que es la plataforma correcta para registrar estos nombres, para trabajar con las identidades digitales y con los identificadores correspondientes para garantizar esta interoperabilidad única. Hoy en la sesión sobre DNSSEC, hace una hora o dos horas, se habló acerca de los detalles más técnicos para lograr esto que les estoy presentando. Muchas gracias.

ADIEL AKPLOGAN: Muchas gracias, Jacques. Este es un ejemplo de cómo podemos utilizar identidades digitales en el DNS para gestionarlo de manera descentralizada. Es un complemento del tema tratado previamente solo que incorpora al DNS. Tenemos algunos minutos todavía en esta sesión. Quiero ver si alguien tiene alguna pregunta para Jacques acerca de este tema tan interesante y que nos acaba de presentar de las identidades digitales y el DNS.

GABRIEL KARSAN: Hola. Soy Gabriel Karsan, de Tanzania. Soy becario de la ICANN. Estas son tecnologías emergentes pero quiero saber cuál es la

estrategia de inclusión porque estoy escuchando mucho el tema de la confusión de los usuarios y yo vengo de una región en la cual los operadores no tienen muchos recursos y no entienden de qué tratan las DNSSEC.

¿Cómo vamos a hacer para conectar a los próximos mil millones de usuarios? Nosotros estamos en el sur global, donde la gente no tiene el conocimiento necesario para entender todas estas cuestiones técnicas. Entiendo la filosofía de Ethereum, que quiere incluir a más personas. Entiendo que esto sería más democrático a través de estas tecnologías emergentes. ¿Ustedes solamente se están dirigiendo a un tipo de participante en particular? ¿Cómo van a hacer para incluir por ejemplo a las personas de mi región? Gracias.

LUC VAN KAMPEN: Gracias. Creo que vale la pena decir que la DAO de ENS realiza votaciones. Los distintos participantes del ecosistema están invitados a sumarse y a participar. Esto está abierto a todos. No tienen requisito previo. No hay discriminación alguna por ningún motivo, raza, religión, ingresos económicos, nada de eso. Nosotros lo que hacemos es incluir a quienes tienen derechos de gobernanza. Tenemos a los fundadores principales. Luego tenemos a los integrantes de la organización DAO, que generan proyectos, que promueven el ecosistema. La DAO les da unas

identificaciones que les dan derechos de gobernanza y participación.

Una gran proporción de estos token fue distribuida a los registratarios de ENS. El año pasado lo que hicimos fue ver quiénes habían registrado un dominio y les distribuimos estos token. Creo que la participación mayoritaria es del 8% y luego todos tienen participación del 4%. Es decir, básicamente tenemos una representación distribuida y todos pueden participar sin discriminación alguna. No importa su país de origen, etc.

GABRIEL KARSAN: Okey. Yo necesito tener un dominio que utilice DNSSEC. ¿Qué pasa si vengo de una región en la cual no puedo tener DNSSEC por ejemplo? Además, ¿ustedes tienen programas de difusión desde las bases para poder incluir a más personas que no entienden estas tecnologías emergentes?

LUC VAN KAMPEN: Sí. Gracias por su pregunta. Estamos haciendo lo siguiente. La organización DAO distribuye estos token que dan derechos de gobernanza. Si el dominio no tiene DNSSEC pueden registrar los usuarios un punto .ETH que no necesita cumplir con ese requisito de tener un TLD que utilice DNSSEC. Eso lo vemos en

muchos TLD que no tienen que seguir las políticas de la ICANN para los ccTLD, etc. En ese caso, un usuario se puede registrar con otro TLD y a veces pueden utilizarlo con DNSSEC y en ese caso no utilizan el sistema ENS. En lugar de mostrar el dominio que ellos quieren, porque no lo tienen, simplemente lo que hacen es tener una cuenta que muestra su dirección pública con su clave pública.

Con respecto a las tareas de difusión, la organización DAO asigna ciertos fondos a programas de difusión para garantizar que todos tengan capacitación y educación y parte de lo que yo hago en ENS es visitar todas las regiones que necesitan entender estas tecnologías. Dentro de dos semanas voy a estar en un evento de la fundación Ethereum en Bogotá, en Colombia, para hablar con la comunidad local y para hablarles acerca de la red de Ethereum, de lo que puede hacer ENS y cómo afecta a las personas allí. Espero que eso conteste a su pregunta. Si no, puede acudir a mí después.

ADIEL AKPLOGAN: Gracias, Luc. Es interesante. Se nos está acabando el tiempo. Normalmente esta sesión de identificadores emergentes, son temas bastante indagadores e importantes. Disculpen. Se nos está acabando el tiempo. No sé si podemos aceptar alguna pregunta. Lo que sí quiero decir es que nosotros hemos recibido

el foro de partes interesadas. La razón por la que tenemos esto es porque así podemos tomar esta discusión en lo que tiene que ver con los identificadores emergentes y continuar con esta discusión en línea, por Internet, para poder profundizar más en el tema y también intercambiar con los presentadores y tener más discusión aparte de la hora u hora y media que normalmente se le asigna a esta sesión. Carlos.

CARLOS: Gracias, Adiel. Tengo una pregunta específica. Cómo trata usted con las solicitudes legítimas de los organismos de aplicación de la ley cuando ellos quieren registrar algún uso indebido en los dominios de ENS.

ADIEL AKPLOGAN: Como hay que cerrar esta sesión, le voy a pedir que hablemos después de esta sesión. Gracias, Carlos, por la pregunta. Hay otras preguntas en el chat con respecto a la propiedad intelectual y también con respecto a usar un nombre cuando no está autorizado a hacerlo. Fue una sesión interesante e informativa. Los volveré a ver a ustedes. Espero ver sus nombres en la lista de correo. Gracias.

[FIN DE LA TRANSCRIPCIÓN]