Concepto MONA – UPL

Esta plataforma se enfoca en la privacidad e integridad de datos del usuario.

Se entiende por privacidad el derecho de cada individuo, empresa, agencia o administración en mantener seguras sus comunicaciones con terceras partes. No es el propósito de este ecosistema el ser utilizado para la comisión de delitos en forma alguna, así como organizar, financiar o coordinar acción alguna que pueda perjudicar a terceros, sus bienes o intereses. Es fundamental y se espera, se establezcan los mecanismos y regulaciones necesarias a fin de garantizar ambos requerimientos.

Se considera integridad de datos el hecho de recibir información, sea el medio de difusión de esta (análogo, digital u otros) en la forma en que el emisor de la misma la ha enviado a su destinatario. De lo contrario se estaría recibiendo información parcializada, imprecisa o falsa de parte un intermediario u operador mal intencionado. Es parte de dicha integridad el recibir la información en el tiempo pertinente según sea la velocidad de difusión de esta en función del medio.

Partiendo de los conceptos anteriores se procedió a diseñar una plataforma que cumpla en la medida posible con tales desafíos.

Como funciona:

El siguiente escenario describe dos individuos o partes estableciendo un mecanismo de comunicación seguro. Para nuestro ejemplo la parte (a) solicita a la parte (b) el consentimiento de esta ultima para enviarle (x) información: documento, archivo, programa, contenido multimedia, etc.

Lo anterior se puede acometer de varias formas, siendo lo más común: uso de dispositivos telefónicos, vía mensajes de texto, red social, correo electrónico, etc. Una vez la parte (a) a recibido la confirmación de envío, la parte (b) procede a solicitar al sistema (descargar App) para configurar la misma en función de lo acordado con (a). Dicha configuración básica consta de fijar un tiempo de vida para dicha información. Este concepto se incorpora para de esta forma no conservar información alguna pasado el momento de recepción de (b) o el tiempo fijado por el usuario. De esta forma en un escenario en el cual dicha plataforma se vea comprometida solo sera accesible el contenido existente en ese momento, más no así el contenido anterior o futuro. Más adelante ahondaremos en el concepto de cifrado de datos que se encuentren almacenado en dicha plataforma.

El usuario (b) instala la App en sus terminal o dispositivo, esta tiene un tiempo de vida y es de un solo uso. Es decir la App se puede configurar para ser eliminada una vez recibida la información y guardada fuera de la misma pudiendo ser esto ultimo en el propio dispositivo, medio extraible, el reenvío de la misma o una combinación de lo anterior. Aun cuando el usuario dese conservar dicha aplicación el motor de cifrado sincrónico el cual se describe en documento adjunto [Formula extemporánea] debe de ser descargado para realizar una nueva recepción de información.

Lo anterior es gran utilidad debido a que de estar comprometido el dispositivo del usuario (b) nuestra plataforma procederá a notificarle al mismo de su situación. Esto se logra con mecanismo propietario que se incorpora en en la plataforma principal, por razones obvias se omite en esta descripción o concepto de funcionamiento.

Una vez realizado lo anterior el usuario en su terminal genera un pseudo-usuario el cual sirve para: que nuestra plataforma le genere un (smart contract) y su respectiva Wallet. Así como para enviar este pseudo-usuario a la parte (a). Entonces la parte (a) procede a realizar una consulta a nuestro sistema para verificar si en efecto dicho usuario es valido. De ser así y utilizando su llave de cifrado (no la de la parte (b)) envía dicha información a nuestra plataforma. Misma que puede ser consultada por la parte (a) dentro del limite de tiempo fijado por el mismo.

Por cada proceso de interacción con nuestra plataforma ambas partes están bajo supervisión del modulo de verificación de usuario (App), esto es así para evitar diferentes ataques, pudiendo ser estos provenientes de un usuario autentico pero mal intencionado. Es por esa razón que de detectarse irregularidad alguna el sistema notifica a la parte involucrada de su condición y se aborta el servicio.

La parte (a) una vez que el sistema le confirme la existencia (vigencia) del usuario o parte (b) procede a enviar su información al sistema. Lo anterior se realiza de forma que al (a) solicitar servicio de búsqueda de usuario y posterior a verificación de la misma, nuestro sistema le comparte llave de cifrado de un solo uso, la cual es valida solo para ese usuario (b) y el momento de la solicitud de envío. Ese mecanismo es el utilizado para cifrar la información enviada a la parte (b). Para el caso de (b) de igual forma el sistema le solicita su llave o motor de cifrado solo cuando este procede a descargar su información.

Al completarse lo anterior nuestro sistema elimina ambos contratos así como sus respectivas wallet. Al realizar lo anterior los fondos o Tokens regresan a la wallet principal de nuestro sistema para comenzar el ciclo de nuevo con otros usuarios. De esta forma ninguna delas partes (a) o (b) retienen Tokens más allá del tiempo de vida de sus respectivos contratos. Siendo para (a) un evento muy breve ya que estos solo se utilizan para (codificar) la información a ser enviada a la parte (b). posterior a dicho envío o almacenamiento se procede a eliminar el contrato y la wallet asociado a esa transacción no sin antes recuperar cualquier excedente de Tokens remanentes posterior al envío de la información.

En el caso de la parte (b) su wallet conserva dichos Tokens hasta el termino o vigencia fijado por el usuario en lo referente a retención de información o hasta que este descargue dicha información. Posterior a lo cual nuestro sistema procede a eliminar dicho contrato y su respectiva wallet.

Si ambas partes deciden compartir información, nuevamente deben de realizar el proceso.
Por tal razón deben de volver a descargar sus respectivos motores de cifrados o llaves sincrónicas.

Como se almacena o (codifica) la información:

En publicación titulada: [Almacenamiento de datos en la red Blockchain] se describe dicho proceso. Descrito brevemente, cualquier contenido a enviarse se convierte a formato hexadecimal. Para posteriormente aplicar método de caracterización [Concepto de neurona de calculo y generación de fractal]. Al termino de dicho proceso tenemos un resumen o fractal matemático del contenido original mismo que con sus adecuado motor de cifrado o llave puede ser revertido al estado original devolviendo la información original exactamente y en el mismo orden en fue introducida antes de realizar dicho proceso.

Debido a la naturaleza de este ultimo procedimiento, de una data original extensa obtenemos un resumen, por lo tanto en cierta forma es como si comprimimos la información con un radio de compresión imposible de alcanzar por un método convencional.

Este resumen o fractal es lo que enviamos en forma de transacción al destinatario, es decir los tokens almacenados en sus wallet equivalen al mensaje cifrado y comprimido original. Para lo anterior la parte que tomamos es el decimal o fracción de token. Por lo tanto un usuario no tendría nunca un entero de unidad. Al termino de dicha operación y como describimos anteriormente el residual de dicha fracción se regresa a la Main wallet de nuestro contrato inteligente principal.

Entonces, en caso de intrusión por parte de terceros, lo que albergan las wallet que este a la espera de entrega a destinatario solo son tokens que no hacen referencia directa a información alguna. Lo anterior dado que requieren un proceso de descompresión que no es posible si alguna de las partes no se involucra en el debido orden y con las garantías de verificación de sistema. En el escenario de que un usuario se vea comprometido esto no perjudica al resto ya que las llaves de cada partes son únicas y para un solo uso, así como la opción que posee mayor tiempo de vida (24hrs) solo aplica a (b). Este ultimo parámetro es sugerido y se puede ajustar según requerimientos.

En futuro documento se estará ahondado en el tema de la seguridad dispositivo - dispositivo así como métodos anti spam (boot) desarrollados para esta plataforma y propietarios de la misma.

A reserva de abundar.

Julio C. Gómez.
Io-exchange.com (c)