**Plantilla del Estado del Arte**

**Author (s):** Guy Zyskind, Oz Nathan, Alex ’Sandy’ Pentland

**Títle of paper:** Decentralizing Privacy: Using Blockchain to Protect Personal Data

**Journal:** Conference: 2015 IEEE Security and Privacy Workshops (SPW)

**pag – pag (year): 1-5 (2015)**

**Problema que el autor desea resolver (Max 0.5 página)**

La cantidad de datos en nuestro mundo está aumentando rápidamente. En la era de Big Data, los datos están siendo constantemente almacenados y analizados, lo que lleva a la innovación y el crecimiento económico, convirtiendo hoy en día, los datos como un activo valioso en nuestra economía, pero recientes aumento de los incidentes de vigilancia notificados e infracciones de seguridad que comprometen la privacidad de los usuarios.

Desde una perspectiva de seguridad, los investigadores desarrollaron diversas técnicas dirigidas a los problemas de privacidad se centraron en los datos personales, pero son actualmente demasiado ineficientes para ser ampliamente utilizado en la práctica.

**Descripción del aporte del autor (1 – 1.5 páginas)**

{Contribución del autor}

1) Combinamos Blockchain y almacenamiento off-Blockchain para construir una plataforma de gestión de datos de carácter personal centrado en la privacidad.

2) Se ilustra a través de nuestra plataforma y una discusión de las futuras mejoras en la tecnología, cómo Blockchain podrían convertirse en un recurso vital en informática de confianza.

{Procedimiento realizado}

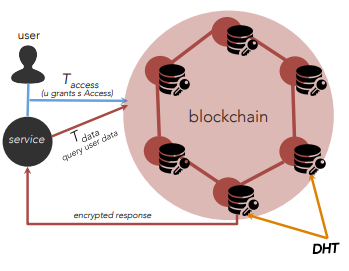
Comenzamos con una visión general del sistema, se describen las tres entidades que componen el sistema, usuarios de teléfonos móviles, interesados en descargar y utilizar servicios, los proveedores de dichas aplicaciones que exigen el tratamiento de datos personales para fines operativos y comerciales (por ejemplo, anuncios dirigidos, servicio personalizado); y nodos, entidades encargadas del mantenimiento de la cadena de bloques y una de datos privados distribuidos de clave-valor a cambio de incentivos. Tenga en cuenta que mientras que los usuarios en el sistema normalmente permanecen (pseudo) anónimos, podríamos almacenar perfiles de servicio en la cadena de bloques y verificar su identidad.

Para ilustrar, se considera el siguiente ejemplo: un usuario instala una aplicación que utiliza nuestra plataforma para preservar su privacidad. Cuando el usuario se registra por primera vez, un nuevo usuario compartido (user, servicio) se genera y se envía la identidad, junto con la información asociada a la cadena de bloqueo en una transacción de Taccess. Datos recopilados en el teléfono (por ejemplo, datos de sensores como la ubicación) se encripta utilizando una clave de encriptación compartida y se envía a la base de datos cadena de bloqueo en una transacción de Tdata, que posteriormente enruta a una tienda de llave-valor fuera de bloque, mientras que se conserva sólo

un puntero a los datos (el puntero es el icono SHA-256 hash de los datos).

El almacén de llaves de valor fuera de bloque (Blockchain off) es una implementación, un hashtable distribuido (o DHT), con la adición de persistencia utilizando una interfaz para la cadena de bloqueo. El DHT es mantenido por una red de nodos (posiblemente de la red de cadenas de bloques), que cumplen con las normas aprobadas transacciones de lectura/escritura. Los datos están suficientemente aleatorizados entre los nodos y replicados para asegurar una alta disponibilidad. Es

Instructivo observar que las soluciones alternativas fuera de la cadena podrían ser consideradas para su almacenamiento. Por ejemplo, un la nube puede ser usada para almacenar los datos. Si bien esto requiere un poco de confianza en un tercero, tiene algunas ventajas en términos de escalabilidad y facilidad de implementación.



{Conclusiones}.

Los datos personales y datos sensibles en general, no se deben confiar en manos de terceros, donde son susceptible a los ataques y el mal uso con lo que nuestra plataforma permite asegurar los datos mediante la combinación de un Blockchain, re-utilizados como un moderador de control de acceso, con una solución de almacenamiento Blockchain así los usuarios no están obligados a confiar en ninguno de terceros y están siempre al tanto de los datos que se están recogiendo sobre ellos y cómo se utiliza. Además, el Blockchain reconoce a los usuarios como a los propietarios de sus datos personales. Las empresas, a su vez, pueden centrarse en la utilización de datos sin preocuparse demasiado acerca de la seguridad y la compartimentación de manera adecuada.

**Referencias bibliográficas referenciadas en el informe (0.5 página)**

* Scaling the facebook data warehouse to 300 pb, 2014.
* James Ball. Nsa’s prism surveillance program: how it works and what it can do. The Guardian, 2013.
* Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proceedings of the twentieth annual ACM symposium on Theory of computing, pages 1–10. ACM, 1988.
* EUROPEAN COMMISSION. Commission proposes a comprehensive reform of data protection rules to increase users’ control of their data and to cut costs for businesses. 2012.
* Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen, and ´ Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, 2013