

# Escuela de Ingenierías Industrial, Informática y Aeroespacial

## GRADO EN INGENIERÍA INFORMÁTICA

### Innovación tecnológica



### Antivirus descentralizado

Autor: José Martin Brioso

(01, 2019)



# Índice

1. Resumen .....	3
2. ¿En qué consiste?.....	4
2.1 Tecnologías utilizadas.....	4
2.2 Arquitectura del sistema.....	4
3. Retos .....	5
4. Análisis DAFO .....	6
4.1 Fortalezas .....	6
4.2 Debilidades .....	6
5. Conclusión .....	7

## 1. Resumen

El objetivo de este trabajo es definir algunas pautas para el posterior desarrollo de Software distribuido mediante la tecnología Blockchain que sirva principalmente para proteger y recompensar a los usuarios de dicho software.

El desarrollo distribuido podría resultar muy prometedor, ya que conseguiríamos lograr un producto gratuito en el que todos los usuarios colaborasen con simples tareas cotidianas de navegación mandando informes de seguridad de las páginas que visitan.

Hoy en día existen los llamados antivirus, pero la forma por la cual estos recolectan la información y la tratan sigue estando centralizada, es decir un usuario de Avast por ejemplo envía informes y es protegido, no obstante si la información de que paginas son peligrosas o si un mail es spam realmente solo lo sabe la empresa. Si esto ,no fuese así los navegadores podrían mejorar la protección a los usuarios o se podrían detectar fallos en el sistema tal como ocurre con otros software open source como Linux.

Surgen muchas dudas a la hora de plantear el proyecto, como por ejemplo quien o como decidirá si una página es maliciosa y si se sube o no a la base de datos distribuida (Blockchain). Pero estas soluciones nos la brinda la propia tecnología con un aspecto muy importante, la prueba de trabajo.

En resumidas cuentas podríamos hacer que cuando uno de los usuarios, a partir de ahora llamado nodo. Encuentre una página de phishing este la reporte y otros nodos (una parte importante de la red) verifiquen que esta página si se trata en realidad de phishing y que este nodo ha realizado un reporte correcto.

Estos usuarios podrían ser recompensados por su contribución con algún tipo de moneda criptográfica y que esta sirva por ejemplo para adquirir mejora de los servicios de protección u otras recompensas que estudiarían más adelante.

## 2. ¿En qué consiste?

Básicamente se trata de un antivirus open source descentralizado. Haciendo uso de las áreas punteras y de las cuales se conoce una mayor previsión de futuro en el mundo de la informática, estas son:

### 2.1 Tecnologías utilizadas

- Blockchain
- Inteligencia artificial
- Ciberseguridad

El papel que juega cada una de estas áreas en nuestra aplicación es fundamental para crear un software fresco e innovador.

Necesitaremos la tecnología Blockchain por que como ya comentamos antes nuestra intención es la creación de una que contenga bloques de información sobre todo lo relacionado con ataques informáticos.

El uso, el tratamiento de esta información almacenada por todos los nodos será procesada con un sistema de inteligencia artificial que nos ayudara, tanto a mejorar las pruebas de trabajo de Blockchain, (por uso de la localización para juntar los nodos más cercanos, para asignar un grado de confianza a cada nodo, para hacer pasar un primer filtro antes de tener que involucrar a ningún otro nodo) como haciendo de primer “filtro” para detectar informes erróneos.

Todo esto se llevara a cabo para mejorar la ciberseguridad global y poder de una vez por todas acabar con los ataques informáticos y tener una red en la que los usuarios puedan confiar.

### 2.2 Arquitectura del sistema.

Podríamos entender la arquitectura como una red en la que todos los nodos están conectados indirectamente.

Los cuales recaban información y verifican. Estos datos seria primeramente sometidos a un filtro de inteligencia artificial (desarrollado en conjunto) con lo que obtendríamos un resultado verificable.

En la siguiente imagen podemos observar cómo sería la arquitectura básica de nuestro sistema.

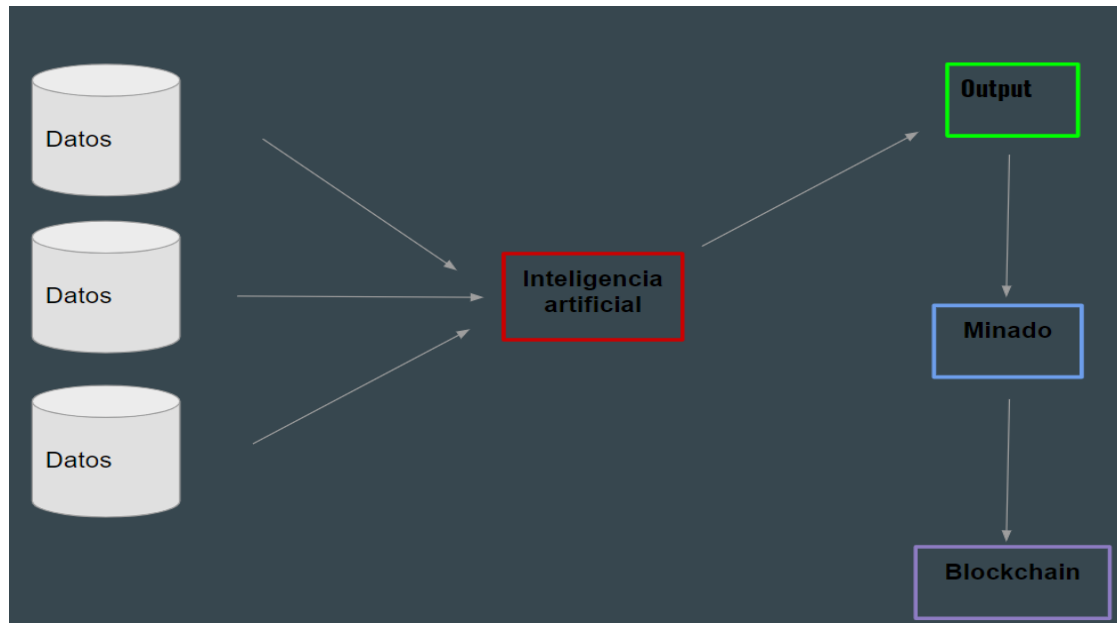


Figura 2.1 Arquitectura del sistema (08/2018, José Martin).

### 3. Retos

La dificultad para lograr este objetivo consiste en la creación de una buena red neuronal que nos permita distinguir ataques maliciosos, para que antes de que estas se añadan a la Blockchain tengamos la seguridad de que no estamos incluyendo en esta ningún servicio útil.

En un principio la dificultad de dar a conocer el producto también existiría ya que nadie quiere utilizar un antivirus que realmente no tiene los suficientes usuarios como para poder confiar en este. Creo que es una medida que cualquier compañía de Antivirus tendría que al menos intentar implementar.

Crear una criptomoneda y todo el sistema de recompensas parece una ardua tarea, no obstante en mi opinión las empresas que utilizan este método, véase STEEMIT (red social que paga por publicaciones). Creo que son el futuro ya que realmente tienen en cuenta el esfuerzo y el valor de todo lo que los usuarios aportan.

## 4. Análisis DAFO

Incluiré en este reporte un análisis de las fortalezas y debilidades del sistema aquí descrito, para así poder tenerlas en cuenta y desarrollar en función de los aspectos que mas tengamos que tener en cuenta.

### 4.1 Fortalezas

- Gratuito.
- Distribuido.
- Potencial de desarrollo.
- Open source.
- Utilización de tecnologías punteras.
- Poco presupuesto inicial.
- Sistema de recompensas basado en la utilidad.
- Alcance global

### 4.2 Debilidades

- Dificultad para su difusión
- Necesidad de un alto número de nodos y contribuidores
- Complejidad de implementación
- Competencia surgente.
- Alta responsabilidad

## 5. Conclusión

En mi opinión es una idea innovadora que surge del interés y la formación que recibí del profesor Enrique Lopez Gonzalez encargado de la asignatura optativa Business Intelligence.

Creo que la informática debe ser de todos para todos y hacer entender que la ciberseguridad tiene que ser una prioridad para todos los estudiantes de informática, tanto para usuarios como para desarrolladores todos podemos ser víctima de una estafa, un robo, una intromisión en nuestra vida privada.

Por todo ello creo que si este proyecto se llevase a cabo estaría dispuesto a aportar mis conocimientos y mis ganas de hacer de internet un lugar más seguro para todos.

Es quizás una tarea muy compleja para llevar a cabo durante el periodo universitario, pero las propuestas están ahí y quién sabe si en un futuro se llevara a cabo.