**Guía para la presentación de la propuesta**

**Introducción**

Bueno, muy buenas tardes. La propuesta de la que hablare es un protocolo de autenticación de transacciones con identificación de usuarios.

**Agenda**

Como la agenda nos indica, iniciaremos con los antecedentes y de ahí pasaremos al planteamiento del problema, la justificación, que contribuciones se esperan y, por último, la metodología que se utilizará.

**Antecedentes**

La autenticación e identificación son los mecanismos que más se utilizan hoy en día en los sistemas informáticos para acceder a los recursos que estos tienen. Redes sociales, correos electrónicos o inclusive cuentas bancarias necesitan una autenticación de tu parte y como tal una parte autenticadora que verifique tu identidad. Es decir, la autenticación es el proceso de comprobar la identidad del usuario o equipo que desea ingresar al sistema – hablando de identidad como algo que permite diferenciarse un usuario de otros. Mientras que la identificación es algo que sirve para corroborar que la entidad es quien dice ser.

La autenticación de usuarios se ha basado mayormente en arquitecturas centralizadas, es decir, aquellos sistemas que están organizados de tal forma que exista una sola entidad que se encarga de la mayoría de las tareas. C.A.S., Centralized Authentication System es un claro ejemplo.

Además de esto, también encontramos los sistemas distribuidos que son cada vez más importantes hoy en día. Caracterizados por ser un conjunto de computadoras separadas físicamente, pero conectadas entre sí, se percibe a este conjunto como un solo sistema. Blockchain es un ejemplo de esto.

**Planteamiento del Problema**

Actualmente, uno de los problemas que se generan al momento de la autenticación, presentados en los protocolos centralizados, es que quien identifica a los usuarios es una sola entidad, la autoridad certificadora. De esta manera, un ataque realizado por un tercero malicioso se centrará en corromper dicha entidad. Este tipo de ataques pueden negar el acceso a servicios de la aplicación a diferentes usuarios, entre otras cosas.

Por otro lado, la autenticación distribuida también tiene ciertos inconvenientes. Principalmente, al ser un sistema basado en confianza en donde el usuario no es identificado, es muy difícil saber la identidad de las personas que están realizando algún tipo de transacción u otro tipo de movimiento. Por lo cual, si una transacción es ilícita, no se sepa quiénes son los usuarios de esa transacción.

**Justificación**

Es por eso que, dado que uno de los protocolos más utilizados en los sistemas son los de autenticación, es muy importante que se realice de manera segura. La solución óptima sería un protocolo que solo otorga acceso a cierta información y quitando la necesidad de que cada sistema almacene credenciales por usuario. Es decir, que el protocolo le ayude al sistema o servicio a saber la identidad de sus usuarios y que a su vez permita cierto anonimato del usuario en transacciones en las que no se requiera ser identificado.

Blockchain ofrece este enfoque mediante la distribución de la propiedad de las credenciales y la disponibilidad de almacenar en una cadena inmutable de datos. Estos son almacenados en un libro compartido que es distribuido a cada entidad, reflejando un registro de cada transacción realizada. Mientras que C.A.S. o cualquier otro protocolo de autenticación centralizada permitirá que el usuario sea identificado mediante la autoridad certificadora y así poder conocer la identidad del usuario.

**Contribuciones Esperadas**

Es así como se espera contribuir con un prototipo de protocolo de autenticación para mejorar la autenticación del usuario tanto para la aplicación como para el usuario que desea autenticarse, utilizando ciertas características tanto de protocolos centralizados como distribuidos. Es decir, el protocolo se comportaría de la manera en que el centro de la autenticación de bloque de bloques sería un ID de bloque de bloques y sea otorgado por la autoridad certificadora. Este ID es un bloque de datos en la cadena que podrá ser verificada por algún tercero y que solo muestre la información necesaria. Se espera generar el prototipo del protocolo con estas características y que de esta manera se pueda asegurar la autenticación como una propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

**Metodología**

Para lograr complementar esta investigación, se desarrollará el prototipo de un protocolo utilizando un marco de referencia para desarrollo el proyecto, en este caso se utilizarán algunas prácticas que sugiera Disciplined Agile para el desarrollo del proyecto. Además de esto, se utilizarán procesos previamente definidos para el desarrollo del protocolo que faciliten su implementación, utilizando el marco de referencia de CMMI. Esto con la finalidad de que se logren hacer pruebas al protocolo y pueda ser comparable con algunos de los protocolos de autenticación ya existentes.

**Finalización**

Pues a grandes rasgos esa es la propuesta de mi proyecto. Alguna Duda, queja o sugerencia que quisieran hacer.

Bueno sin más por añadir, les agradezco su atención y sus sugerencias. Muchas Gracias.