INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS QUERÉTARO

ESCUELA DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA



**Realización de un protocolo de autenticación para el mejoramiento de la privacidad del usuario**

Por

Daniel Adalaid Carranza Alvarez

Sometido a la Escuela de Tecnologías de Información y Electrónica

División de Ingeniería y Arquitectura

para la acreditación de la materia

Proyecto Integrador para el Desarrollo de Soluciones Empresariales

Asesor(es): 1) Benjamín Valdés Aguirre

2) Rocío Alejandra Aldeco Pérez

Santiago de Querétaro. Querétaro, México.

03/05/2018

**Tabla de Contenidos**

[1. Introducción 8](#_Introducción)

[1.1 Contexto del Problema 8](#_Contexto_del_problema_1)

[1.2 Motivación del trabajo de investigación 19](#_Motivación_del_trabajo)

[1.2 Objetivo de Investigación 19](#_Objetivo_de_investigación)

[1.2 Estructura del Documento 19](#_Estructura_del_documento)

[2. Estado del Arte 21](#_Estado_del_Arte)

[2.1 Seguridad de la Información 21](#_Sistemas_centralizados_y)

[2.2 Sistemas Centralizados y Distribuidos 22](#_Tipos_de_autenticación)

[2.3 Tipos de autenticación 24](#_Tipos_de_autenticación)

[3. Planteamiento del Problema 21](#_Planteamiento_del_Problema)

[3.1 Introducción al problema 21](#_Introducción_al_problema)

[3.2 Contexto del problema 22](#_Contexto_del_problema)

[3.3 Objetivo del trabajo 24](#_Objetivo_del_trabajo)

[3.4 Alcance del trabajo 24](#_Alcance_del_trabajo)

[3.5 Metodología 20](#_Trabajo_Futuro)

**[4. Propuesta de Solución 26](#_Trabajo_Futuro)**

[4.1 Herramienta propuesta 26](#_Trabajo_Futuro)

[4.3 Tecnología utilizada 34](#_Trabajo_Futuro)

[4.4 Diseño 34](#_Trabajo_Futuro)

**[5. Metodología de Evaluación 42](#_Trabajo_Futuro)**

[5.1 Prueba 42](#_Trabajo_Futuro)

[5.2 Métricas 43](#_Trabajo_Futuro)

**[6. Evaluación de Resultados 45](#_Trabajo_Futuro)**

[6.1 Resultados obtenidos 45](#_Trabajo_Futuro)

[6.2 Análisis de resultados 47](#_Trabajo_Futuro)

[6.3 Conclusiones 49](#_Trabajo_Futuro)

**[7. Conclusiones 50](#_Trabajo_Futuro)**

[7.1 Conclusiones 50](#_Trabajo_Futuro)

[7.2 Contribuciones 51](#_Trabajo_Futuro)

[7.3 Trabajo Futuro 51](#_Trabajo_Futuro)

[Bibliografía 53](#_Bibliografía)

**Índice de Ilustraciones**

[Ilustración 2‑1 Protocolo de autenticacion C.A.S. 9](#Ilustracion21)

[Ilustración 2‑2 Protocolo de autenticacion P.K.I. 10](#Ilustracion22)

[Ilustración 2‑3 Protocolo de autenticacion Kerberos 10](#Ilustracion23)

[Ilustración 2‑4 Protocolo de autenticacion OpenID 11](#Ilustracion24)

[Ilustración 2‑5 Sistemas actuales contra Blockchain 12](#Ilustracion25)

[Ilustración 2‑6 Funcionamiento de PGP 14](#Ilustracion26)

[Ilustración 4‑1 Imagen de los módulos 14](#Ilustracion42)

[Ilustración 6‑1 Autenticación C.A.S. 14](#ilustacion61)

[Ilustración 6‑2 Autenticación de la partyA exitosa 14](#ilustacion62)

[Ilustración 6‑3 Autenticación de la partyB exitosa 14](#ilustacion63)

[Ilustración 6‑4 Ticket de la partyA 14](#ilustacion64)

[Ilustración 6‑5 Ticket de la partyB 14](#ilustacion65)

[Ilustración 6‑6 Creación del nodo partyA 14](#ilustacion66)

[Ilustración 6‑7 Creación del nodo partyB 14](#ilustacion67)

[Ilustración 6‑8 Creación del contrato exitoso 14](#ilustacion68)

[Ilustración 6‑9 Autenticación fallida 14](#ilustacion69)

[Ilustración 6‑10 Ticket de la autenticación con un certificado falso 14](#ilustacion610)

[Ilustración 6‑11 Inicio de sesion exitoso 14](#ilustacion611)

[Ilustración 6‑12 Encontrado por el Doorman, no accede a transacciones 14](#ilustacion612)

**Índice de Tablas**

[Tabla 2‑1 Protocolos Centralizados 13](#tabla21)

[Tabla 2‑2 Protocolos Distribuidos 18](#tabla22)

[Tabla 3‑1 Desventajas de protocolos centralizados y distribuidos 23](#tabla31)

**Índice de Diagramas**

[Diagrama 4‑1 Diagrama de arquitectura 34](#diagrama41)

[Diagrama 4‑2 Diagrama de casos de uso 23](#diagrama42)

[Diagrama 4‑3 Diagrama de actividad 23](#diagrama43)

# Introducción

Este documento presenta al lector con una investigación centrada en el problema que enfrentan los usuarios al autenticarse en diferentes sitios que esto se realice de manera privada y segura, sin exponer la información del usuario o entidad que se está autenticando.

## Contexto del problema

Anormalmente tu como persona tienes una identidad, algo que te permite diferenciarte de otras personas. Esta identidad se utiliza para identificarte, es decir, para corroborar que tú eres en realidad quien dices ser y comprobarlo mediante una autenticación. La autenticación e identificación son utilizados en diferentes tipos de sistemas, no solo informáticos, sino también para sistemas como bancos, votación, entre otros que han estado con nosotros desde el boom de las computadoras. Por lo tanto, en un sistema, una autenticación es muy importante para darte accesos a diferentes recursos del sistema.

Ala 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. Tomando C.A.S., Centralized Authentication Service como un ejemplo de ello.

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 por ejemplo.

## Motivación del trabajo de investigación

La motivación principal surge del mayor obstáculo para migrar muchos servicios, el cual es la capacidad de asegurar los datos y verificar la identidad de los usuarios del mismo. Esto provoca que la información del usuario quede expuesta o que su privacidad se vea comprometida. La solución óptima sería un protocolo que solo otorga acceso a cierta información. Es decir, que el protocolo le ayude al sistema 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.

Corda, utilizando tecnología tipo blockchain, nos 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 ledger que es distribuido a cada nodo de la transacción, reflejando un registro de cada transacción realizada. Mientras que C.A.S. ayudará a regular a las entidades que intenten ingresar al sistema otorgando certificados a cada entidad. Que estos posteriormente se utilizarán para la autenticación distribuida.

## Objetivo de investigación

Se Los protocolos de autenticación, tanto distribuido como centralizado, cubren ciertas partes para generar una autenticación y verificación de la entidad lo más eficaz que su arquitectura lo permite. Así mismo, **generan desventajas que pueden ser utilizadas para ataques que perjudiquen la confidencialidad de la entidad que desea autenticarse.**

El objetivo del presente trabajo es el siguiente: **Utilizar las ventajas de un protocolo de autenticación centralizada y de un protocolo de autenticación distribuida para garantizar la confidencialidad y privacidad de la información del usuario que desea autenticarse**.

## Estructura del documento

A continuación, se presentan los objetivos de los capítulos de este trabajo:

En el **estado del arte** se exploran algunos conceptos de la seguridad de la información, así como de que se tratan los sistemas distribuidos y centralizados. Además de ver distintos protocolos de autenticación, tanto centralizados como distribuidos, sus ventajas y desventajas que representan a cada uno de ellos.

El **planteamiento del problema** describe el problema como tal, aclarando por qué es un problema y por qué se debe de resolver, dando el contexto del problema, que alcance tendrá el trabajo y el objetivo de este**.**

En la **propuesta de solución** se presenta la herramienta a desarrollar, que permite una autenticación de un protocolo que usa tecnología tanto centralizada como distribuida. También se presenta el diseño del protocolo.

En la **metodología de evaluación** se define la prueba que se llevó a cabo con el fin de determinar el cumplimiento del objetivo.

La **evaluación de resultados** muestra los resultados obtenidos en las pruebas especificadas, que fue lo que se realizó y como se realizó además de la interpretación de dichos resultados.

En las **conclusiones** se observa el resumen del trabajo y sus contribuciones. Se proponen los puntos de trabajo futuro que pueden mejorar la herramienta.

# Estado del Arte

Este capítulo presenta inicialmente una breve descripción de las propiedades de la información en una arquitectura segura. Posteriormente, los distintos protocolos de autenticación que existen actualmente para la autenticación de los diferentes usuarios existentes. Además de dar contexto de sistemas centralizados y distribuidos, seguridad de la información, e introducir conceptos como autenticación e identificación, utilizados en el diseño de solución propuesta. Finalmente, se presenta una discusión de las ventajas y desventajas de cada protocolo.

## Seguridad de la Información

La seguridad de la información es la práctica de defender la información del acceso, uso, revelación, ruptura, modificación, inspección o destrucción de forma no autorizada. Es un término general que puede ser utilizado de forma independiente de la forma que los datos pueden tomar [1].

A continuación, se muestran las propiedades de seguridad:

* Confidencialidad
  + Garantiza que la información sensible solo pueda ser manipulada o accedida por usuarios, entidades o procesos autorizados [1].
* Autenticación
  + Garantiza que la identidad de la entidad sea la correcta. Tres aspectos pueden ser evaluados al autenticar usuarios [1].
    - Algo que eres.
    - Algo que sabes.
    - Algo que tienes.
* Integridad
  + Garantiza que la información no pueda ser modificada por entidades no autorizadas [1].
* No repudio
  + Protege al usuario o entidad contra cualquier otro usuario que niegue la ejecución de la transacción [1].

### Autenticación e identificación

Se denomina identificación al momento en el que un usuario o identidad se da a conocer en el sistema, mientras que autenticación a la verificación que realiza el sistema sobre esta identificación. En cuanto a eficiencia, es conveniente que los usuarios puedan ser identificados y autenticados una sola vez, accediendo a todas sus aplicaciones y datos a partir de ahí, esto se denomina Single Sign On [2].

La seguridad se basa, en gran medida, en la efectiva administración de los permisos de acceso a los servicios, basados en la autenticación, identificación y control de accesos. El protocolo de autenticación se basa principalmente en la propiedad de seguridad que es autenticación y que de esa manera un usuario mediante una identificación se autentique según se requiera.

Autenticación es el proceso de intentar verificar la identidad digital del usuario o entidad que se desea conectar. El autenticar a esta entidad es un modo de asegurar que los usuarios son quien dicen ser, es decir, que el usuario que desea realizar distintas funciones en un sistema es el usuario que tiene la autorización para hacerlo de esa manera. Mencionando a autorización como el proceso por el cual la red de datos accede que el usuario identificado utilice determinados recursos del sistema. Como se mencionó, los métodos de autenticación están basados principalmente en algo conocido, algo poseído, o alguna característica física [8].

## Sistemas centralizados y distribuidos

### Sistemas centralizados

Un sistema centralizado es cuando el proceso de computo es realizado en una localización central, usando terminales conectadas a una entidad central. La entidad central en sí puede controlar todos los periféricos directamente, si están físicamente conectados con la entidad central, o conectados a través de sistemas remotos [3].

[4] En otras palabras, los sistemas centralizados se caracterizan por:

* Una entidad central que ejecuta todas las aplicaciones.
* Recursos locales compartidos.
* Administración única del sistema.
* Un único sistema operativo.

### Sistemas Distribuidos

Un sistema distribuido se define como una colección de computadoras separadas físicamente y conectadas entre sí por una red de comunicaciones distribuida; cada entidad posee sus componentes que el usuario percibe como un solo sistema [3].

Un ejemplo de sistemas distribuidos es Blockchain, siendo una base de datos distribuida que funciona como libro para el registro de operaciones compra-venta o cualquier tipo de transacción. Esto genera un cambio en el que, Blockchain, se usa como notario público distribuido no modificable de todo el sistema de transacciones a fin de evitar el problema de que na moneda se pueda gastar dos veces [4].

[4] En otras palabras, un sistema distribuido se caracteriza por:

* Tener varias entidades en sitios diferentes.
* Existencia de uno o varios canales de comunicación.
* Dispersión de los datos entre diferentes sistemas.
* Independencia del Centro de Proceso de Datos.
* Diferentes Sistemas Operativos.

## Tipos de autenticación

En la autenticación se utilizan estos conceptos de centralizada y distribuida, partiendo de que un protocolo de autenticación centralizado se maneja con una única autoridad certificadora en la que todos confían y, como usuario, identificarte ante ella para poder acceder a los diferentes recursos que existen en el sistema.

Por otro lado, los protocolos de autenticación distribuida surgen como una necesidad para los distintos usuarios. Dando seguridad a la información del usuario, mediante las propiedades mencionadas anteriormente, generando así una autenticación basada en confianza y, a grandes rasgos, en anonimato.

### Autenticación Centralizada

### C.A.S.

Servicio de autenticación centralizada, por sus siglas en inglés, es un protocolo de autenticación creado por la Universidad de Yale que provee una forma de autenticación de confianza. Esta construido en estándares abiertos para ser integrado en diferentes aplicaciones y sistemas. C.A.S. provee servicios de autenticación única [5] . El protocolo se genera de la siguiente manera:

* Primera Autenticación.
  + El servidor requiere usuario y contraseña.
  + Si todo sale bien el servidor envía un ticket al cliente.
  + El ticket es opaco y no contiene información del cliente.
* Autenticación a un servicio autenticado.
  + La autenticación redirige al navegador al servicio C.A.S.
  + El navegador presenta su ticket
  + El servidor C.A.S. envía un ticket de servicio.
  + Se redirige el navegador a la aplicación.
  + La aplicación valida el ticket de servicio con C.A.S.
  + La aplicación permite el acceso al navegador.

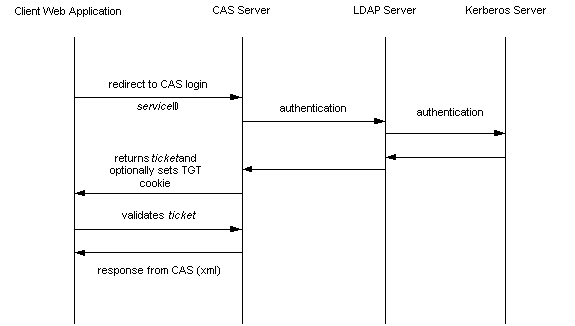


Ilustración 2‑1 Protocolo de autenticación C.A.S.

### P.K.A.

Autenticación de clave pública, por sus siglas en inglés, Esta tecnología permite a los usuarios autenticarse ante otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes.

La seguridad en P.K.A. depende en parte de cómo se guarden las claves privadas. Existen dispositivos especiales denominados tokens de seguridad (siendo un dispositivo que se le da al usuario autorizado de un servicio para facilitar su proceso de autenticación [9]) para felicitar la seguridad de la clave privada, así como evitar que pueda ser exportada. Existen diferentes componentes en P.K.I. [10].

* Autoridad de certificación.
  + CA, por sus siglas en inglés, es la encargada de emitir y revocar certificados. Es la entidad de confianza que da la legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
* Autoridad de registro.
  + RA, por sus siglas en inglés, es responsable de verificar el enlace en los certificados y la identidad de sus titulares.
* Repositorios.
  + Son las estructuras encargadas de almacenar la información relativa a la P.K.I., Infraestructura de clave pública por sus siglas en ingles. Los repositorios más importantes son el de certificados y el de las listas de revocación de certificados (CRL).
* Autoridad de Validación.
  + VA, por sus siglas en inglés, es la encargada de comprobar la validez de los certificados digitales.
* Autoridad de sellado de tiempo.
  + TSA, por sus siglas en inglés, es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
* Usuarios o entidades finales.
  + son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

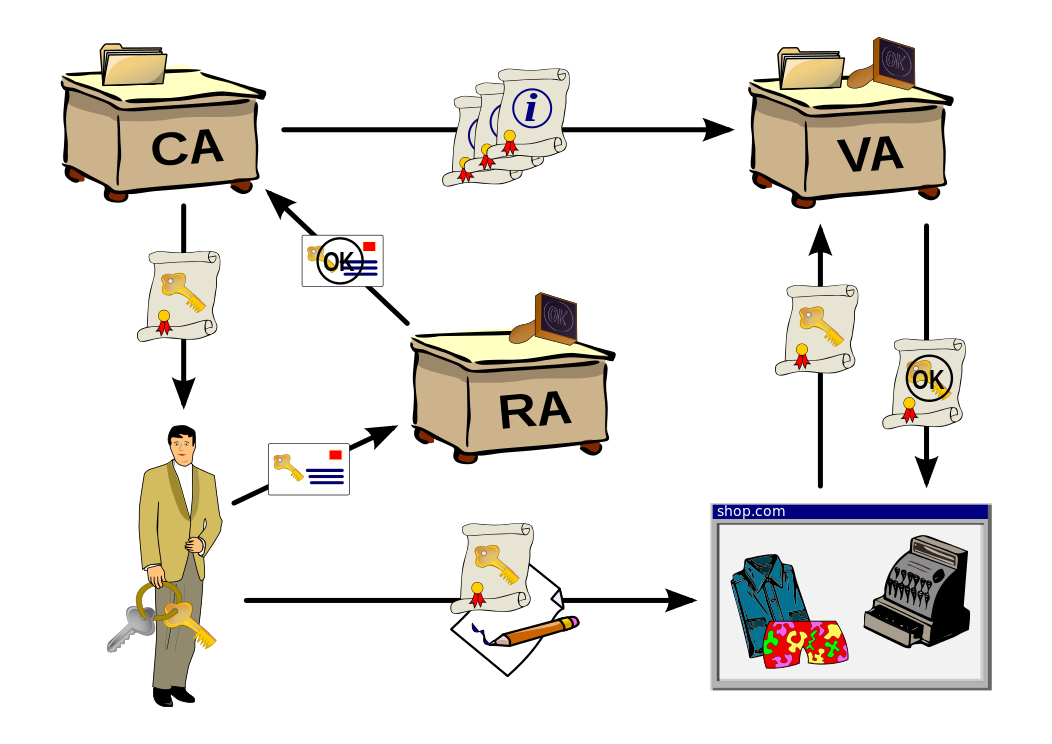


Ilustración 2‑2 Protocolo de Autenticación P.K.I.



### Kerberos

Siendo un protocolo de autenticación de redes de ordenador creado por el MIT permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura. Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza, denominado Centro de distribución de claves, cual consiste en dos partes lógicas un Servidor de autenticación y un servidor de emisor de tickets [6].

En resumen, el funcionamiento es el siguiente: el cliente se autentica a si mismo contra el Servidor de autenticación (Denominado AS por sus siglas en ingles), así demuestra al Servidor de Emisor de Tickets (denominado TGS por sus siglas en inglés) que está autorizado para recibir un ticket de servicio, recibiéndolo. De esta manera ya puede demostrar al Servidor del Servicio (denominado SS) que ha sido aprobado para hacer uso del servicio [6].



Ilustración 2‑3 Protocolo de autenticación Kerberos

### Discusión

La tabla 2-1 muestra una comparación de los protocolos de autenticación centralizada, que toma en cuenta las ventajas y desventajas de cada uno de los mencionados anteriormente [13].

|  |  |  |
| --- | --- | --- |
| Protocolo | Ventajas | Desventajas |
| C.A.S. | No necesita distribuir las claves públicas o validar huellas cuando se crea o se actualiza el par de claves.  Las credenciales de autenticación pueden ser revocadas centralmente.  Altamente escalable: No se necesita confiar en entidades individuales, sino en una sola AC.  Mismo nivel de seguridad en comparación con P.K.A.  Provee verificación de la identidad a través de la clave privada.  Los certificados pueden ser usados para diferentes propósitos. | Necesita una infraestructura de clave pública. Esto aumenta el costo de despliegue inicial en algunos ambientes en comparación con P.K.A. |
| P.K.A. | Es más seguro que utilizar contraseñas.  Provee verificación de la identidad a través de la clave privada.  Es posible el acceso no interactivo. | Si las claves privadas no se protegen, la seguridad es la misma que si se tuvieran contraseñas.  No es muy escalable, ya que la distribución de claves publicas puede ser engorrosa en entornos grandes. |
| Kerberos | Elimina la transmisión de contraseñas no cifradas a través de la red.  Elimina a los terceros maliciosos que busquen robar información a través de la red. | Es tedioso estar migrando las contraseñas en diferentes ambientes.  Asume que cada entidad es confiable, pero en un ambiente donde el host y la red no es confiable.  Es una solución de todo o nada. Si alguna aplicación se comunica con otra que no use Kerberos esto puede generar riesgo a la privacidad del usuario. |

Tabla 2‑1 Protocolos Centralizados

Como se puede observar los tres proveen la identificación de la entidad que desea acceder. Siendo C.A.S. la mejor opción para una autenticación en donde se requiera dicha identificación, además de proveer una infraestructura escalable a diferencia de los otros protocolos, y a su vez, utilizar los certificados para diferentes propósitos.

### Autenticación Distribuida

### OpenID

OpenID es un estándar de identificación digital distribuido, con el que un usuario puede identificarse en una página web a través de una URL, o un XRI, y puede ser verificado por cualquier servidor que soporte este protocolo.

En este tipo de autenticación los usuarios no tienen que crearse una nueva cuenta de usuario para obtener acceso. De esta manera, solo se necesita disponer de un identificador creado en un servidor que verifique OpenID, conocido como proveedor de identidad o IdP.

OpenID no especifica el mecanismo de autenticación. Por lo tanto, la seguridad de una conexión OpenID depende de la confianza que tenga el cliente OpenID en el proveedor de identidad [7].

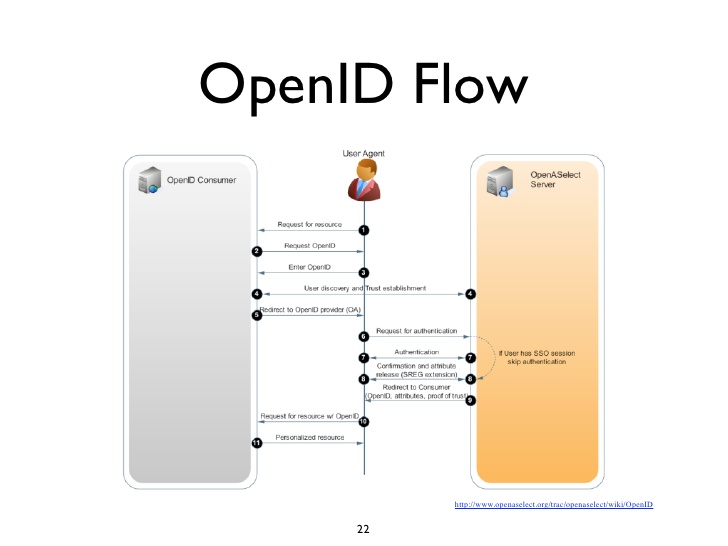


Ilustración 2‑4 Protocolo de autenticación OpenID.

### Blockchain

Blockchain es una base de datos distribuida que funciona como libro de registro de operaciones compra-venta o cualquier otra transacción. En otras palabras, Blockchain se usa como notario público no modificable de todo el sistema de transacciones a fin de evitar el problema de que una moneda se pueda gastar dos veces [11].

Blockchain se basa en tres grandes pilares (consenso, distribución y confianza) y la seguridad se deriva de una prueba del trabajo de resolución de problemas. Donde es necesario tomar una gran cantidad de potencia computacional para completarlos y, por lo tanto, donde a una sola persona puede tomarle años, pero para una red de computadoras puede tomar tan sólo unos minutos. Las pruebas de trabajo que están vinculadas a los datos de cada bloque son necesarias para que los bloques sean aceptados. La dificultad de este trabajo se ajusta para limitar la velocidad a la que nuevos bloques pueden ser generados por la red a una media de uno cada 10 minutos.

Así, la cadena puede continuamente agregarse y las transacciones se procesan de manera oportuna mientras se protegen los datos de la manipulación indebida, por los que la naturaleza de este problema hace matemáticamente imposible que alguien cambie la cadena de bloqueo.

Cambiar un bloque (que sólo puede hacerse haciendo un nuevo bloque que contenga el mismo predecesor) requiere regenerar a todos los sucesores y rehacer el trabajo que contienen" [12].

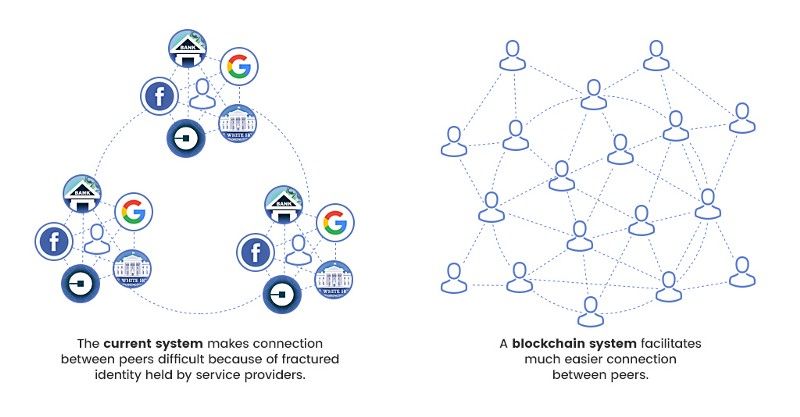


Ilustración 2‑5 Sistemas Actuales contra Blockchain.

### PGP

Pretty Good Privacy es un programa que sirve para cifrar y descifrar datos, de tal manera que solo se puedan acceder a ellos mediante una clave pública, con el objetivo de ofrecer un mecanismo de autenticación para algunas comunicaciones y mejorar la privacidad de las mismas. PGP es el sistema criptográfico de calidad más usado en el mundo.

PGP combina varios procesos de cifrado: hashing, compresión de datos, cifrado de clave simétrica y de clave pública. Para garantizar la autenticación, PGP utiliza un sistema de llaves públicas y privadas en la cual el usuario genera sus propias llaves. De esta manera el usuario, puede firmar con la llave publica con su llave privada para generar el no-repudio y enviar su llave publica al repositorio en donde usuarios verificaran la autenticidad de esta mediante la confianza que tengan y de esta manera garantizar la autenticidad de la misma.

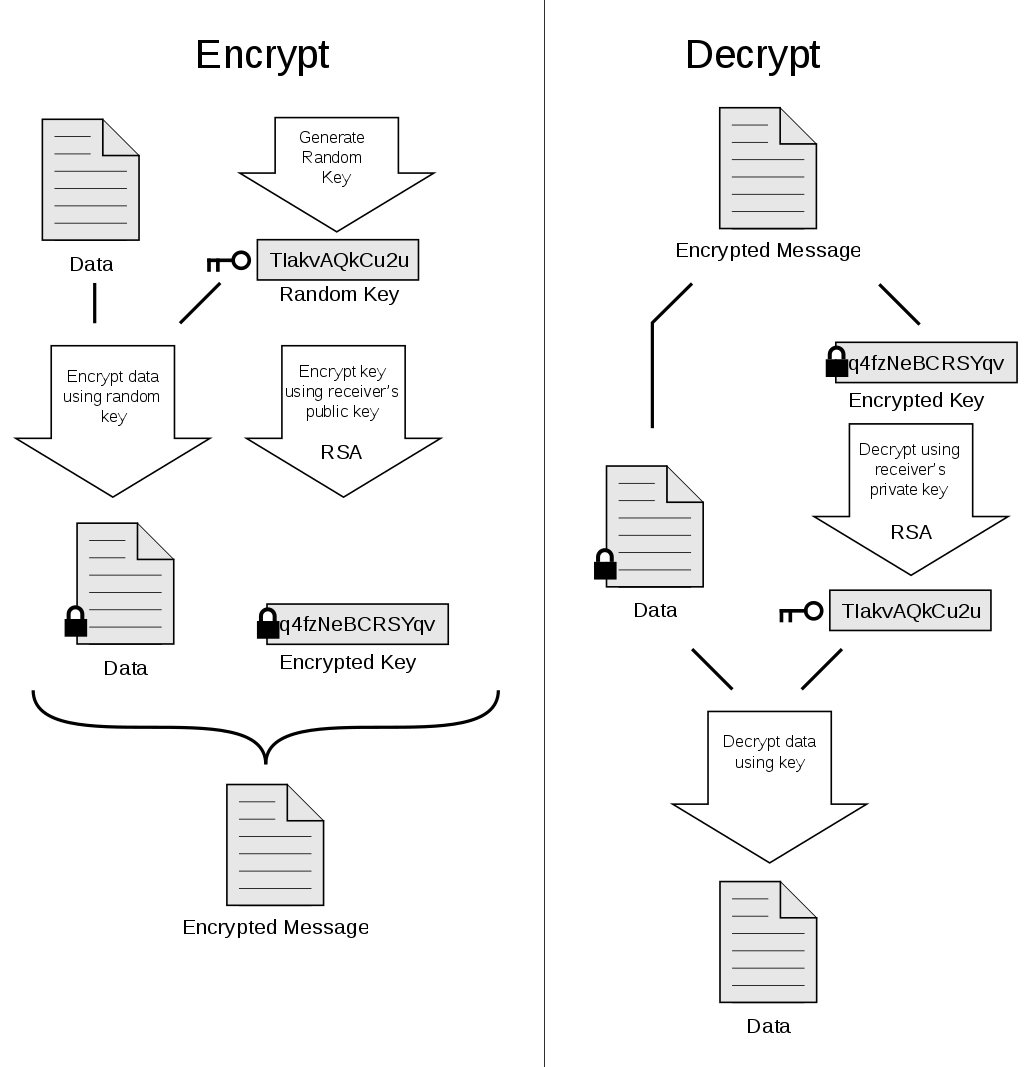


Ilustración 2‑6 Funcionamiento de PGP.

### Discusión

La tabla 2-2 muestra una comparación de los protocolos de autenticación distribuida, que toma en cuenta las ventajas y desventajas de cada uno de los mencionados anteriormente.

|  |  |  |
| --- | --- | --- |
| Protocolo | Ventajas | Desventajas |
| OpenID | Tiene un inicio de sesión único.  Provee información básica del usuario.  Mejora el esquema de usuario/contraseña.  No está obligado a usar el mismo proveedor. | Aun proporciona el esquema de usuario contraseña.  No es utilizado en autenticaciones importantes como la cuenta de banco, etc.  Puede rastrear los hábitos del usuario.  Usualmente maneja la contraseña como texto plano. |
| Blockchain | Empoderamiento de los usuarios  Durabilidad, rentabilidad y longevidad.  Transparencia y mutabilidad.  Transacciones rápidas.  El costo de las transacciones es menor. | No hay verificación de la identidad.  Redundancia.  Costo de implementación. |
| PGP | Tu información está siempre protegida.  La información puede ser compartida, solo con tu consentimiento.  Es una solución tipo hibrida. | Diferentes conflictos en cuanto a versiones.  Problemas de compatibilidad.  La complejidad de su uso puede ser problemática para los diferentes usuarios.  En caso de pérdida, los datos no son recuperables. |

Tabla 2‑2 Protocolos distribuidos

Como se puede observar estos protocolos proveen una autenticación muy eficaz. Siendo Blockchain la opción para realizar una autenticación más rápida y que logre empoderar a los usuarios sin arriesgar su información.

# Planteamiento del Problema

Este capítulo presenta el problema a tratar comenzando por una pequeña introducción al problema general, seguida por el contexto en el que se identifica el problema concreto. Se plantea el objetivo de investigación del trabajo y la metodología que se seguirá para conseguirlo. Se acota el alcance del proyecto y se introduce brevemente la propuesta de solución.

## Introducción al 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 romper dicha entidad. Este tipo de ataques pueden negar el acceso a servicios de la aplicación a diferentes usuarios, entre otras cosas. Un ejemplo de ello es el ataque de negación de servicios, DoS por sus siglas en inglés, que se realizó durante el 2016 a Dyn, un importante proveedor de nombres de dominio, que daba servicio a clientes importantes como Spotify, Netflix y Twitter [14]. Ya que el servicio de DNS es un servicio centralizado similar a la autoridad certificadora, es posible que un ataque sea similar sea realizado a un servicio de autenticación centralizada generando un impacto similar.

Por otro lado, la autenticación distribuida también tiene ciertos inconvenientes. Principalmente, por ser un sistema basado en confianza donde el usuario no es identificado, no existe una forma criptográfica de verificación de la identidad de las personas que están realizando algún tipo de transacción u otro tipo de transacción. Es decir, que un protocolo de autenticación distribuido sólo se puede autenticar a la entidad involucrada más no identificarlo, provocando el anonimato del usuario y de esta manera que, si una transacción ilícita es realizada, no sea posible identificar al usuario de esa transacción.

## Contexto del problema

Como se ha mencionado anteriormente, los protocolos de autenticación centralizada tienen características como el uso de distintas claves para generar la autenticación ante el sistema, por lo tanto, estas claves suelen ser muy fáciles para que la entidad las pueda recordar. Por lo tanto, si una clave se pierde puede haber riesgos en la confidencialidad de la información, además de la integridad de dicha información que puede ser modificada una vez que un tercero malicioso obtenga los datos de cualquiera de las dos entidades. Inclusive, se podría perder la disponibilidad de la información a la cual la entidad que se autentica desea ingresar. La desventaja más clara de una autenticación centralizada es que las claves están en un solo lugar y, por ende, les da más oportunidades a los criminales de apropiarse de información crítica en un solo ataque objetivo.

Se En el caso de los sistemas distribuidos, los usuarios desean operar sus propios sistemas, a su manera, por lo que hay mayor libertad que en los protocolos centralizados, ya que la identidad de un usuario no es conocida por el sistema. Sin embargo, esto genera que los usuarios muchas veces realicen cosas de manera ilícita, sin que haya un control por este tipo de transacciones. Además de que la distribución de datos y programas en múltiples localidades pueden generar muchos problemas de seguridad e integridad que difícilmente son resueltos y que muchas veces requieren un proceso paralelo que ayude a solucionar dichos problemas, esto provoca que la carga del sistema aumente y el rendimiento pueda verse afectado.

Otras de las desventajas entre los protocolos centralizados y los protocolos distribuidos son presentados a continuación en la Tabla 3-1.

|  |  |
| --- | --- |
| Protocolo | Desventajas |
| Centralizado | 1. Si las claves privadas no se protegen, la seguridad es la misma que si se tuvieran contraseñas. 2. Asume que cada entidad es confiable, pero en un ambiente donde el host y la red no es confiable. 3. Única autoridad certificadora, por lo tanto solo hay un objetivo de ataque. |
| Distribuido | 1. Problemas de compatibilidad. 2. La complejidad de su uso puede ser problemática para los diferentes usuarios. 3. No hay verificación de la identidad. 4. Redundancia. |

Tabla 3‑1 desventajas de protocolos centralizados y distribuidos

Para garantizar un la confidencialidad y la privacidad de de la información del usuario es necesario que el usuario se identifique con la información necesaria y, a su vez, que la aplicación con dicha información sepa que usuario se está autenticando.

## Objetivo del trabajo

Los protocolos de autenticación, tanto distribuido como centralizado, cubren ciertas partes para generar una autenticación y verificación de la entidad lo más eficaz que su arquitectura lo permite. Así mismo, **generan desventajas que pueden ser utilizadas para ataques que perjudiquen la confidencialidad de la entidad que desea autenticarse.**

El objetivo del presente trabajo es el siguiente: **Utilizar las ventajas de un protocolo de autenticación centralizada y de un protocolo de autenticación distribuida para garantizar la confidencialidad y privacidad de la información del usuario que desea autenticarse.**

## Alcance del trabajo

Se pretende alcanzar el objetivo a través de un protocolo de autenticación distribuido que permita al usuario, la autentificación y validación de su identidad en un sistema, y de esta forma garantizar la privacidad de su información.

A partir de la intervención de la asesora, se acota que el alcance de dicha herramienta a la unión de los dos protocolos, distribuido y centralizado:

* Se realizará primeramente la autenticación centralizada, siendo la autoridad certificadora quien verificará su identidad y así darle un ID para la autenticación distribuida.
* Para el momento de la transacción el usuario se autenticará con el ID recibido anteriormente para que sea autenticado por las diferentes entidades.

El alcance del proyecto busca asegurar la autenticación como propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

## Metodología

Para lograr complementar esta investigación, se desarrollará un prototipo de protocolo de autenticación que permita autenticar a los usuarios de una manera segura, simple y lo más distribuida posible. Así mismo, para el desarrollo del protocolo se utilizará un marco de referencia para desarrollar el proyecto, en este caso se utilizarán algunas prácticas que sugiera Discipline Agile [13] para el desarrollo del proyecto. Además de esto, se utilizarán procesos previamente definidos para el desarrollo del protocolo que faciliten la implementación, utilizando el marco de referencia CMMi [14]. Esto con la finalidad de que se logren hacer pruebas al protocolo y pueda ser comparable con algunos de los protocolos de autenticación centralizados.

# Propuesta de Solución

Este capítulo presenta el prototipo propuesto para alcanzar el objetivo del trabajo. Mostrando como propiedad de seguridad la autenticación en que se basó, la tecnología elegida para el desarrollo y distintos diagramas utilizados en su diseño.

## Herramienta propuesta

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.

El protocolo se comportaría de la manera en que el centro de la autenticación 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 que solo muestre la información necesaria.

Para la verificación se usará un algoritmo de firma digital de manera que, cuando se añada un ID a Blockchain un servicio de emisión de identificación enlace una clave pública de forma predeterminada y luego transfiera la propiedad de la clave privada al usuario. Esto permite que solo el usuario firme una firma que se puede verificar contra la clave pública almacenada en la cadena de bloques. Esta identificación de un usuario sería una fuente distribuida de autenticación. Sería esencialmente un portal de inicio de sesión único al que cualquier aplicación puede acceder pero que no pertenece a ninguna entidad individual.

El prototipo se comportará de la siguiente forma:

* El usuario solicita acceder, por lo tanto, da sus credenciales a la autoridad certificadora.
* La autoridad certificadora revisa las credenciales del usuario que desea autenticarse y lo identifica.
* Si el usuario es identificado correctamente, se le da un ID para realizar las transacciones que desea realizar.
* En el caso contrario, se le niega el acceso al usuario.
* Una vez accedido el usuario, utiliza el ID dado por la autoridad certificadora para que el ID sea verificado por algún tercero para que pueda ser autenticado, mostrando solo la información necesaria.
* Si el usuario es autenticado por el tercero correctamente, podrá realizar la transacción que desee.
* En el caso contrario, el usuario no podrá realizar las transacciones.

## Tecnología utilizada

La solución será desarrollada con C.A.S. para la autenticación de manera centralizada. Mientras que para la autenticación de manera distribuida se realizara por medio de Blockchain utilizando Corda, siendo una plataforma abierta que está inspirado en Blockchain para realizar transacciones.

## Diseño

### Arquitectura

Para el funcionamiento del protocolo se desarrollará un pequeño sistema de transacciones en el cual se realizará la autenticación por la parte centralizada y distribuida. Lo anterior se muestra en el diagrama 4-1:

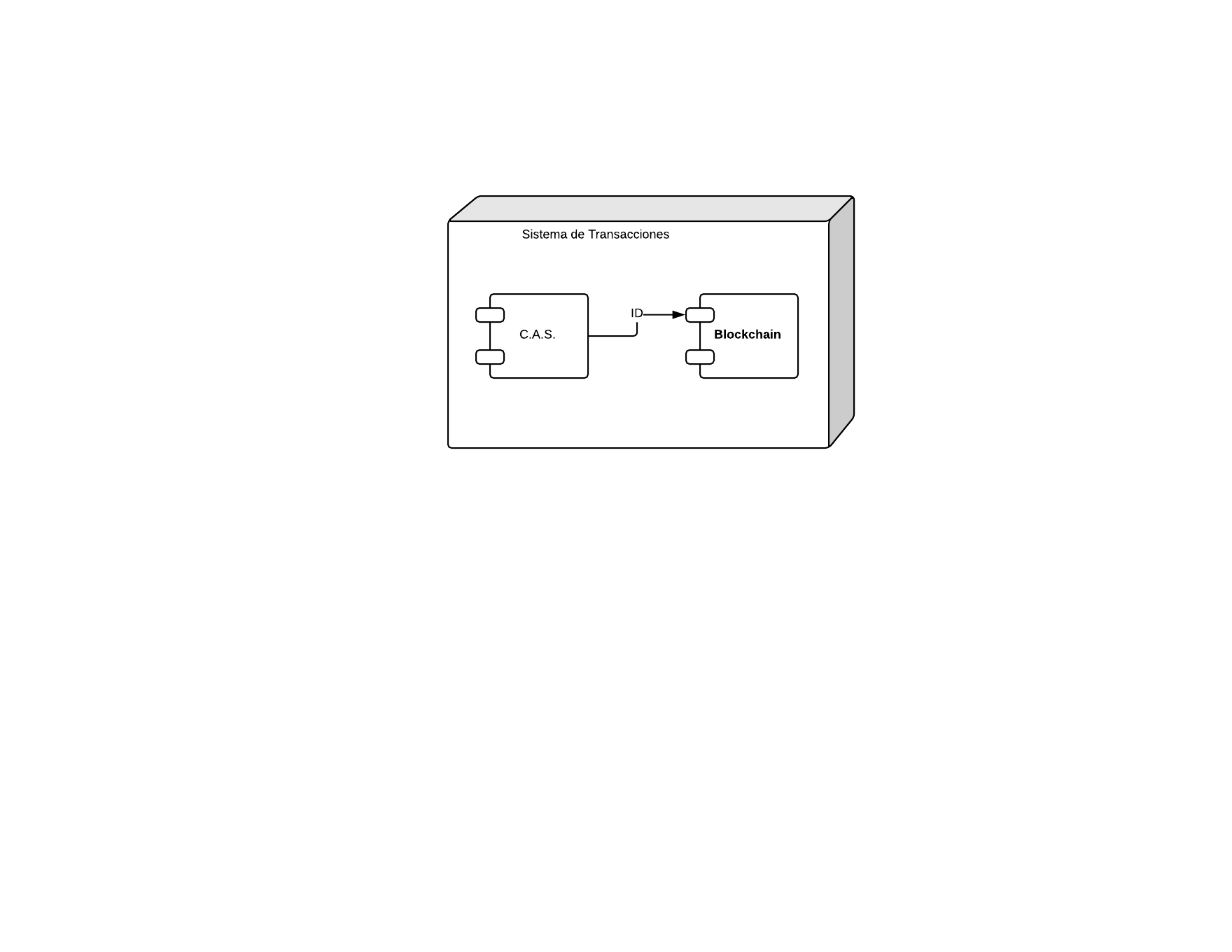


Diagrama 4‑1 Diagrama de arquitectura

### Funcionalidad

La funcionalidad será únicamente en la autenticación y que esta se haga correctamente. Se realizará una transacción mediante las funcionalidades que brinda Corda y esta autenticará al usuario y lo identificará mediante un certificado otorgado por la autoridad certificadora de C.A.S.

La funcionalidad se muestra en el siguiente diagrama 4-2:

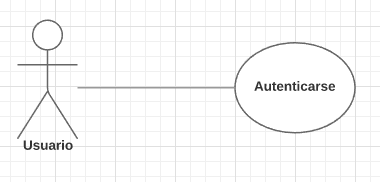


Diagrama 4‑2 Diagrama de casos de uso

### Componentes

La funcionalidad de la herramienta se aloja en dos distintos componentes. La autoridad certificadora, utilizando C.A.S. para su configuración, y las transacciones distribuidas, donde se utiliza Corda como configuración de Blockchain. Estos módulos se presentan en la ilustración 4-1:

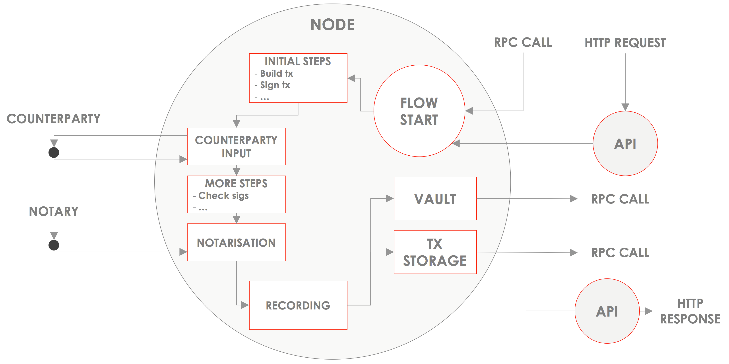
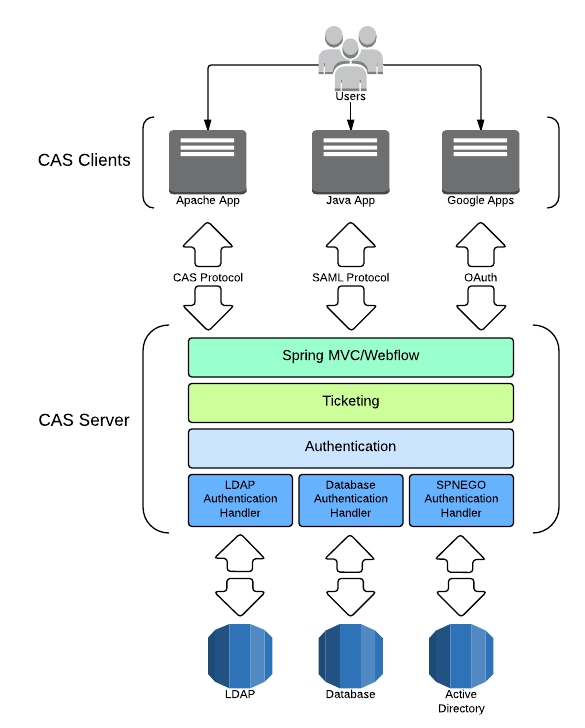


Ilustración 4‑1 Imagen de los Módulos

#### Diagramas de Actividad

El siguiente diagrama de actividad muestra la interacción del usuario con la herramienta.

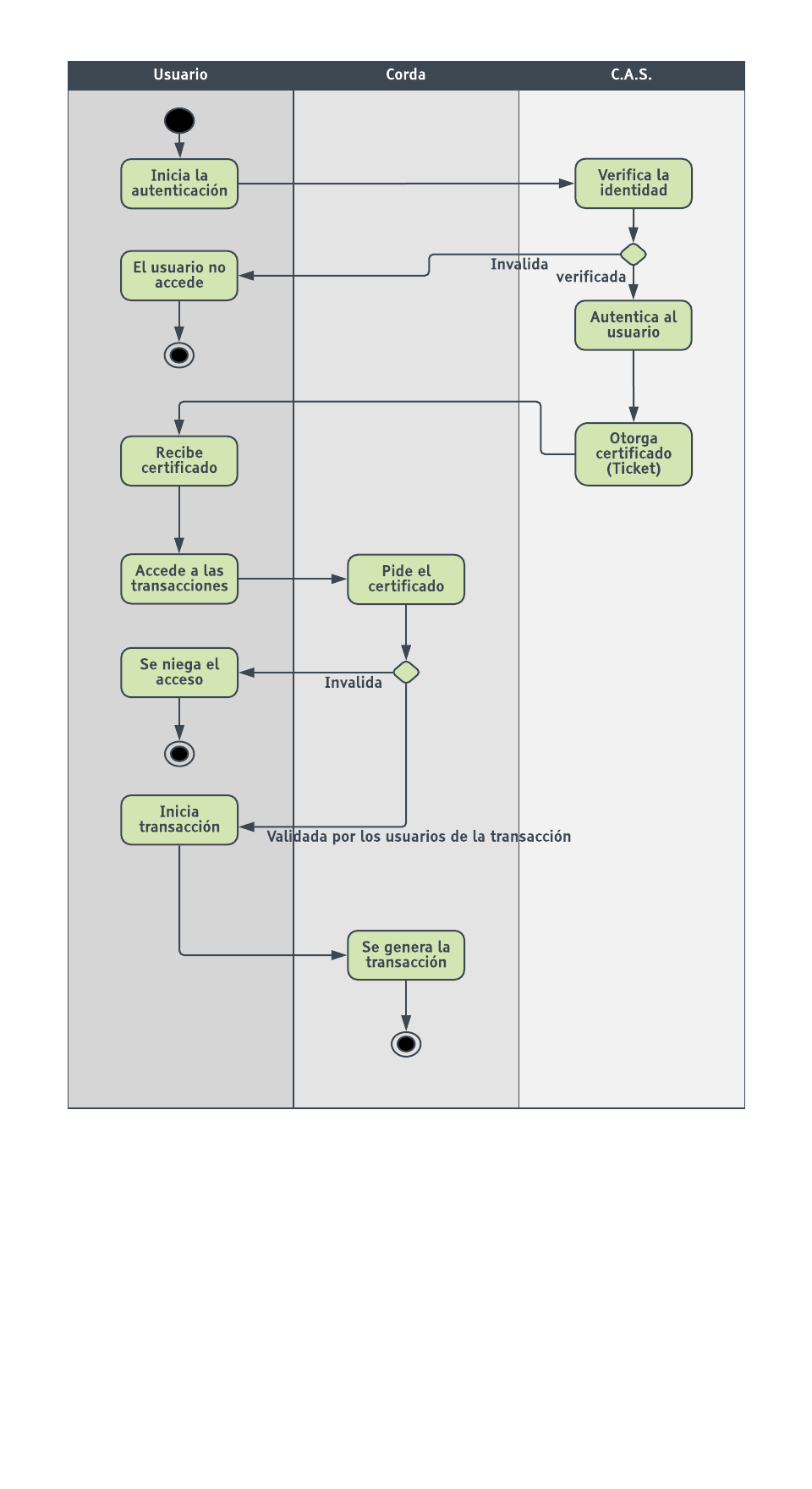


Diagrama 4‑3 Diagrama de actividad

# Metodología de Evaluación

Este capítulo presenta la prueba que se realizará y las métricas que se obtendrán de ella, para definir si el objetivo del trabajo ha sido cumplido.

La evaluación de la solución se hará a través diferentes entidades que se deseen autenticarse. Una entidad responderá por su identidad y se autenticará por ser quien dice ser, mientras que la segunda entidad se tratará de autenticar personificando otra identidad.

## Prueba

Las pruebas A/B son experimentos controlados en los que los usuarios de algún servicio de software son divididos de forma aleatoria para probar dos variantes del software (alternativa A y alternativa B). Las variantes pueden ser dos versiones nuevas completamente diferentes, o una versión actual y una mejorada [15].

Se seleccionó la prueba A/B como opción para evaluar la solución propuesta, ya que se desea comparar tiempo que tardan los usuarios en obtener reportes de forma manual (lo cual puede ser considerado la versión actual) los usuarios que desean autenticarse con su identidad de manera correcta, contra los usuarios maliciosos que tratan de autenticarse siendo una persona diferente a la de su identidad.

La prueba se realizará con la simulación de 40 personas, de los cuáles 20 se autenticarán identificándose de manera correcta, y los otros 20 se autenticarán como entidad maliciosa.

## Métricas

La prueba será realizada con el propósito de verificar si el objetivo del trabajo se cumple. Las métricas utilizadas se analizan a continuación.

### Cumplimiento del objetivo

Objetivo: Generar un prototipo del protocolo que pueda asegurar la autenticación como una propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

El sistema deberá ser capaz de identificar a los usuarios y que estos sean quien dicen ser. Por lo que aquellos que se identifican una identidad diferente a la suya no puedan acceder al sistema.

Se registrará que usuarios sí pudieron acceder con su identidad y cuantos con una identidad diferente a la que son en realidad.

A partir de esto se obtendrá el resultado de asegurar la autenticación como propiedad de seguridad.

El objetivo se considerará cumplido si todos los usuarios son identificados correctamente.

# Evaluación de Resultados

Este capítulo presenta los datos obtenidos en las pruebas propuestas dentro del capítulo 5. Se interpretan los resultados evaluando el cumplimiento del objetivo planteado en el capítulo 3. Por último, se muestran las conclusiones de estas interpretaciones.

## Resultados obtenidos

Revisando las tecnologías usadas, observamos que las identidades en Corda representan las identidades legales o las identidades de los servicios, Estas muestran las identidades conocidas en el mapa de red y la identidad confidencial solo se comparte cuando es necesario. Corda al ser un blockchain de autorización, es decir que para poder participar requieres un permiso previo otorgado por una entidad central. Corda tiene una jerarquía de certificados:

* La entidad central: Que es donde se enfocó la investigación, en donde se busca que está entidad pueda ser otro tipo de entidad certificadora, que normalmente usa certificados X.509. En este caso que pueda utilizar Central Authentication Service (C.A.S.).
* Doorman: Es quien se encarga de verificar diariamente las claves que acceden para reducir el riesgo que la autoridad certificadora se vea comprometida.
* El nodo: Cada nodo sirve como Autoridad certificadora al emitir certificados secundarios para firmar sus claves de identidad.
* La identidad legal: La identidad legal del nodo, además de firmar transacciones también puede emitir certificados para identidades legales confidenciales. [17].

La prueba se realizó creando diferentes nodos, partyA, partyB, partyC, el notario y dos entidades que tratan de acceder a la red sin tener certificado o con un certificado falso.

* La primera prueba se realizó con las partyA y partyB accediendo exitosamente y realizando una transacción exitosa de un ledger.

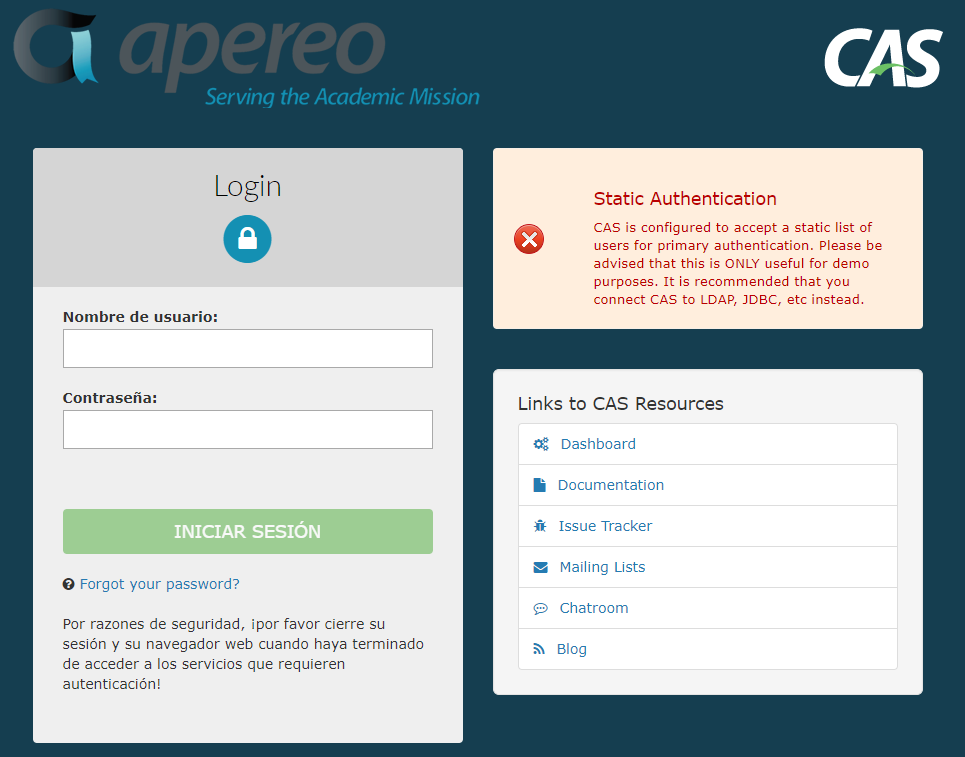


Ilustración 6‑1 Autenticación de C.A.S.

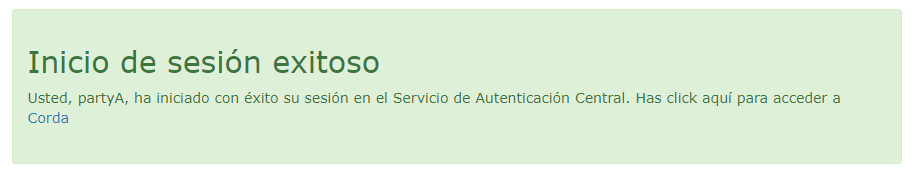


Ilustración 6‑2 Autenticación de la entidad partyA exitosa.

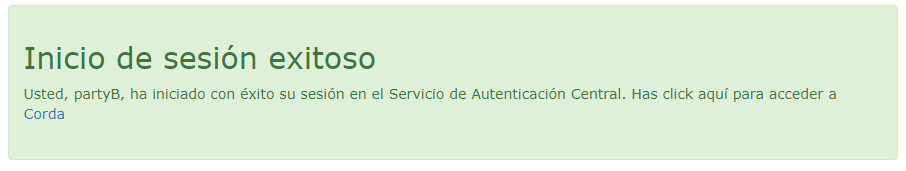


Ilustración 6‑3 Autenticación de la entidad partyB exitosa.

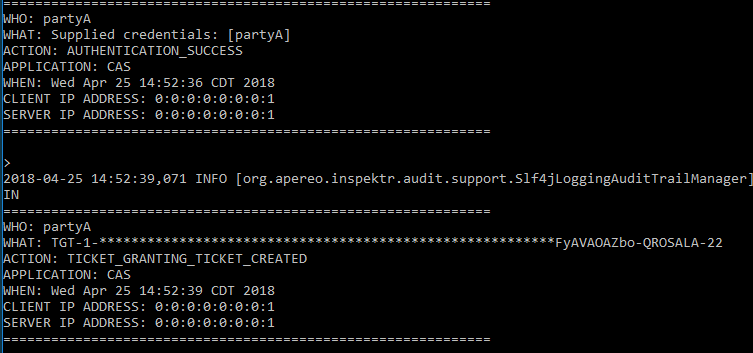


Ilustración 6‑4 Ticket de la partyA

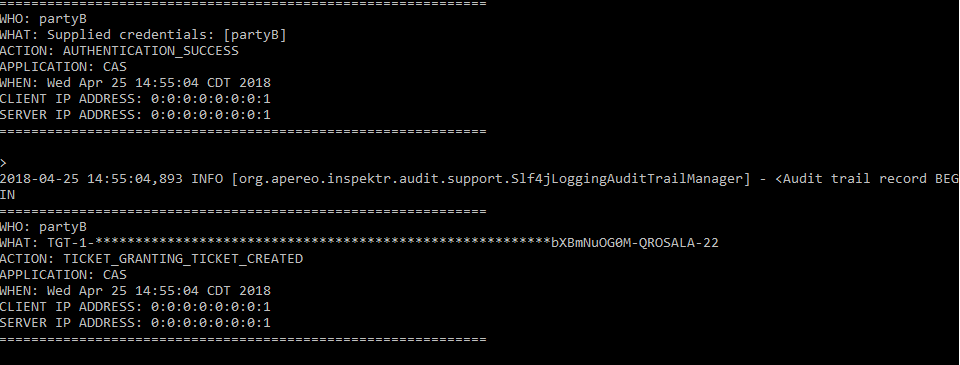


Ilustración 6‑5 Ticket de la partyB

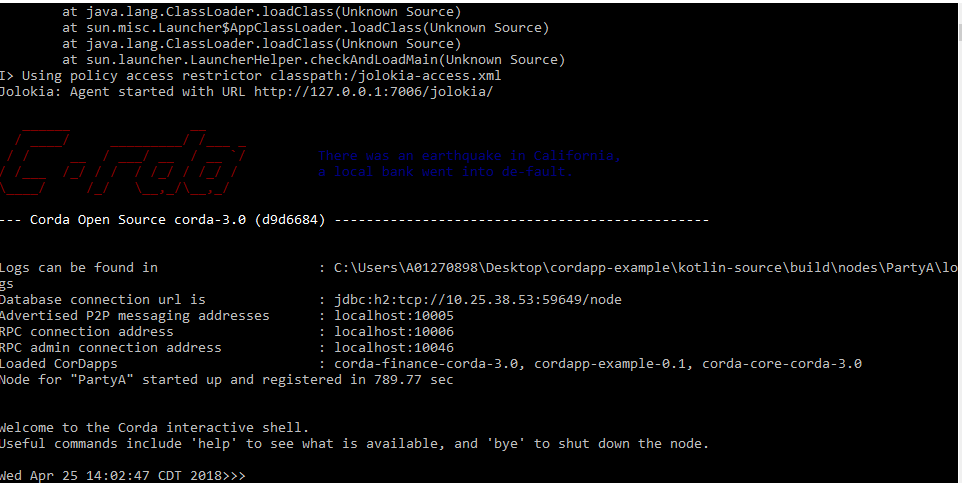


Ilustración 6‑6 Creación del nodo partyA

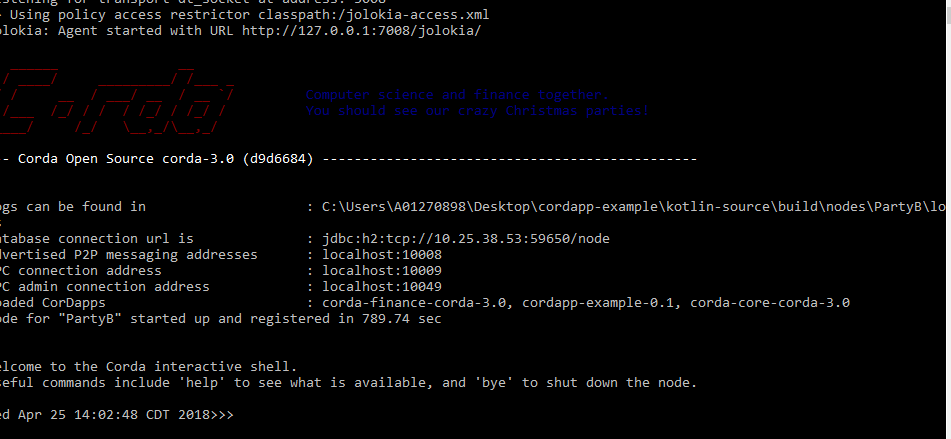


Ilustración 6‑7 Creación del nodo partyB

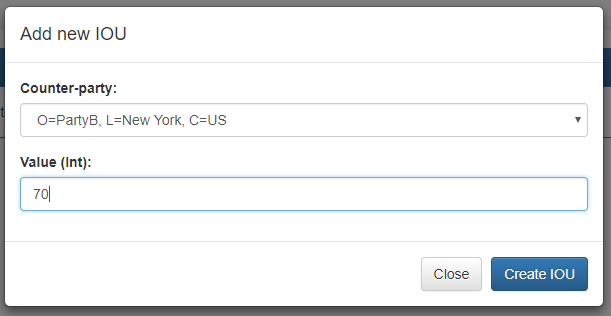
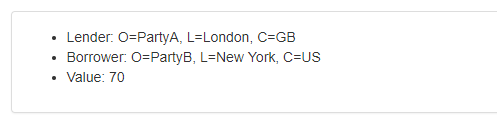
 

Ilustración 6‑8 Creación del contrato exitoso

* La segunda prueba se realizó con un nodo sin certificado. El cual no pudo acceder a la red por lo cual ni siquiera pudo llegar a los nodos interiores.

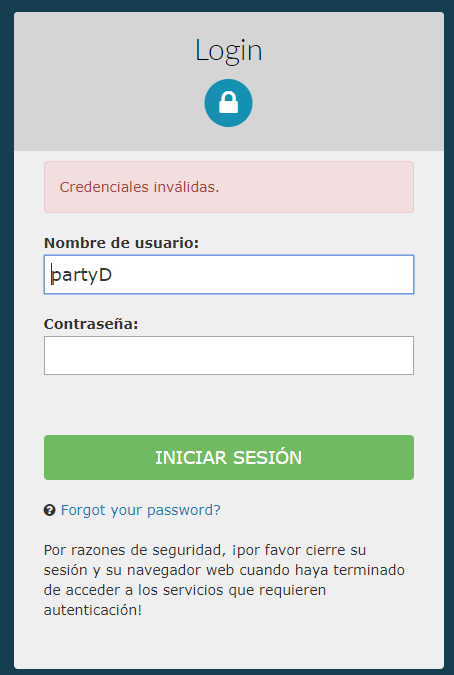
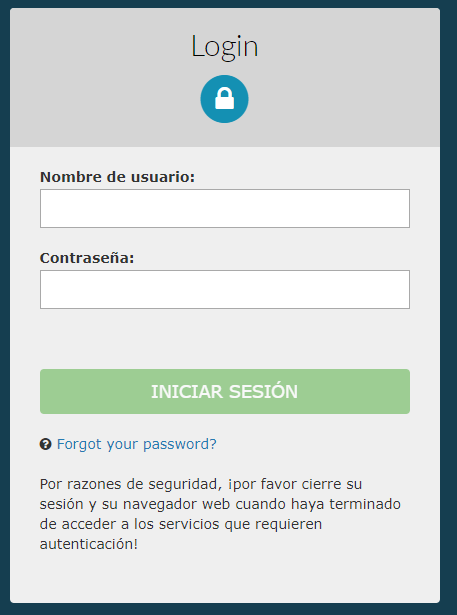


Ilustración 6‑9 Autenticación fallida

* La tercera prueba se hizo con un certificado falso. Durante esta prueba la entidad acceder a la red, pero al tener un certificado falso el Doorman y los nodos no pudieron reconocer está entidad y por lo tanto no pudo realizar ninguna transacción.

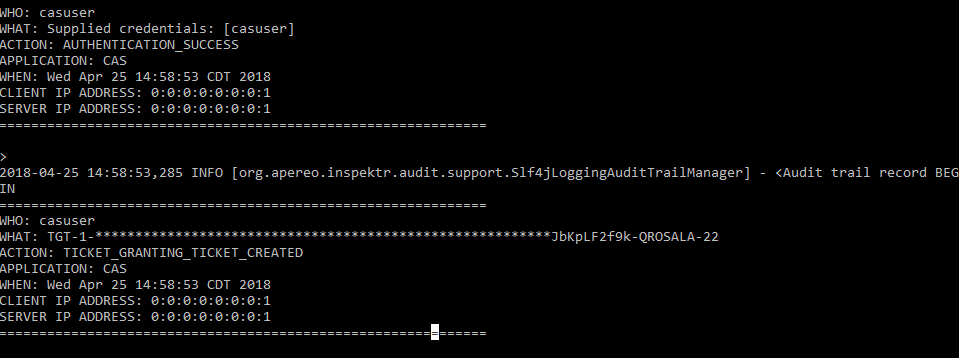


Ilustración 6‑10 Ticket de la autenticación con un certificado falso



Ilustración 6‑11 Inicio de sesión exitoso

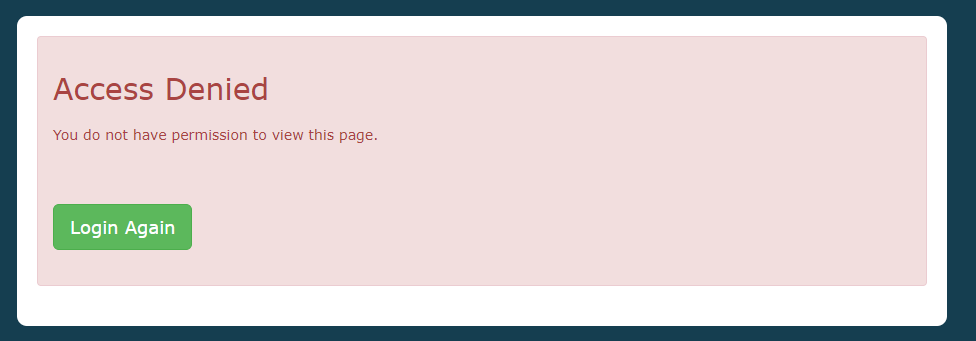


Ilustración 6‑12 Encontrado por el Dorrman, no accede a transacciones

## Análisis de resultados

Como se menciona en la sección 5.2 del capítulo 5, las pruebas se realizaron con el propósito de verificar si el objetivo del proyecto se cumple. Considerando lo anterior, los resultados son interpretados a continuación.

### Cumplimiento del objetivo

Objetivo: Generar un prototipo del protocolo que pueda asegurar la autenticación como una propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

Como se menciona anteriormente Corda es una red de autorización y con la jerarquía que está tiene para la autorización es muy difícil que una entidad maliciosa pueda acceder a la red sin que se detecte.

Durante las pruebas pudimos observar que al menos en un nivel de la jerarquía la entidad maliciosa fue detectada y por lo tanto está no pudo realizar ningún movimiento, además de que la entidad nunca pudo utilizar un certificado de las otras entidades, es decir que tuvo que generar uno. Por lo tanto, la identidad y la información de las otras entidades nunca fue comprometida. Dado a esta interpretación nos llevan a la conclusión de que el objetivo del trabajo se ha cumplido.

## Conclusiones

Las pruebas nos permiten considerar el objetivo del proyecto como cumplido. La herramienta permitió a los usuarios poder autenticarse y mantener resguardada su información mediante un certificado generado por la autoridad certificadora y que, para que está no se vea comprometida, firmada por un Doorman que permite los accesos a la red.

# Conclusiones

En este capítulo se presentan las conclusiones del trabajo tomando en cuenta las herramientas existentes en el mercado, expuestas en el capítulo 2, los objetivos planteados en el capítulo 3, el análisis a la solución propuesta en el capítulo 4, y los resultados arrojados por las pruebas, interpretados en el capítulo 6. También se propone trabajo futuro que puede mejorar la herramienta.

## Conclusiones

Las tecnologías actuales que permiten al usuario autenticarse en las diferentes plataformas a las que acceden diariamente muchas veces están expuestas a diversos ataques que ponen en riesgo la información del usuario. De lo anterior surge la necesidad de protección de datos para cada entidad que desee autenticarse, lo cual nos llevó al objetivo del trabajo planteado en el capítulo 3: generar un prototipo del protocolo que pueda asegurar la autenticación como una propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

En el capítulo 4 se muestra el diseño del protocolo y el resultado final del mismo. Esta solución fue probada siguiendo la metodología descrita en el capítulo 5, en la que dos grupos de entidades una maliciosa y otra normal que intentaran acceder al sistema y que pudieran que generar una transacción los que fueran capaz de hacerlo sin comprometer su información. Los resultados de dichas pruebas son presentados en el capítulo 6.

Dichos resultados nos llevan a concluir que el protocolo cumple con el objetivo al permitir a las entidades realizar las transacciones mediante nodos que se conocen y pueden emitir certificados mediante quienes confían y evitar o sacar de la red a quienes son entidades maliciosas. Cabe destacar que el objetivo se pensó para combinar los sistemas que utilizan los bancos, los institutos electorales entre otras cosas junto con nuevas tecnologías como lo es el blockchain para no dar más información de la necesaria a alguien que no la necesite o la pueda utilizar ilegalmente.

## Contribuciones

El trabajo arroja las siguientes contribuciones:

* Un prototipo de protocolo de autenticación descentralizado, que hace uso de una red de autorización mediante una jerarquía de autoridad. Siendo la cabeza el Central Authentication Service.
* El prototipo logra identificar la identidad de las entidades que acceden a la red para así, si ocurre una irregularidad poder identificar a las entidades maliciosas.

## Trabajo Futuro

En el estado actual, el protocolo permite a la entidad poder autenticarse de manera segura protegiendo su privacidad y sus datos, dentro de una red pequeña de nodos. Tomando en cuenta lo anterior, se proponen las siguientes mejoras:

* **Probarlo en una red aun mayor**

La solución permite la autenticación en una red pequeña de nodos, se propone probar dicha implementación en una red mayor para ver los resultados en donde acceden más personas y hay más entidades maliciosas, además de revisar el tiempo en que se tardaría en autenticarse en una red mayor.

* **Utilizar el protocolo para un protocolo de votación**

Se propone utilizar el protocolo en un sistema de voto en donde se mantienen los mismos aspectos, una autoridad certificadora debe saber la identidad del usuario para conocer quién es y que, si puede realizar un voto, mientras mantener anónimamente su identidad en el proceso de voto como tal en donde no es necesario conocer toda la información de dicha entidad.

# Bibliografía

[1] Internet Security Glosary in RFC 2828. In http://www.ietf.org/rfc/rfc2828.txt.

[2] Turner, D. Digital Authentication - the basics in Cryptomathic. In https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics.

[3] Massimo, F. Possible Evolution Strategies: Single centrilized system versus multi-processor architectures in ACM SIGSMALL 1993.

[4] Weihl, W. Using transactions in distributed applications. In ACM 1990*.*

[5] Central Authentication Service (C.A.S.) in Unicon. In https://www.unicon.net/opensource/cas.

[6] Bellovin, S.; Merritt, M. Limitations of the Kerberos authentication system. In ACM SIGCOMM computer Communication Review.

[7] Press Customizr. What is OpenID. In http://openid.net/what-is-openid/.

[8] Alvarez, G. Autenticacion y autorizacion en internet in Criptonomicon. In https://web.archive.org/web/20070313221944/http://www.iec.csic.es:80/CRIPTonOMICon/autenticacion/.

[9] Security LLC. Security RSA Token ID in RSA Products. In https://www.rsa.com/en-us/products.

[10] Gutmann, P. PKI design for the real world. In Proceeding on New Security Paradigms 2006.

[11] Hari, A. The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet. In Proceeding on HotNets 2016.

[12] Ramiro, R. Blockchain para la autenticación y verificación de nuestra identidad in ciberseguridad. In https://ciberseguridad.blog/blockchain-para-la-autenticacion-y-verificacion-de-nuestra-identidad/.

[13] SSH TECTIA®. Product Description. In https://www.ssh.com/manuals/server-zos-product/55/index.html.

[14] González, M. La gran inseguridad del internet de las cosas, la culpable del ataque DDoS qué noqueó la web. En https://www.xataka.com/servicios/los-responsables- del-ddos- a-dyn-usaron-camaras- ip-y- dvrs-para- tumbar-medio- internet.

[15] Peitsa Hynninen and Marjo Kauppinen. A/B Testing: A Promising Tool for Customer Value Evaluation. In the *1st International Workshop on Requirements Engineering and Testing.* 2014.

[16] Centrilized Authentication Service. In https://apereo.github.io/cas/5.2.x/index.html.

[17] Corda. In https://docs.corda.net/index.html.