Implementación de un Modelo de Autenticación Multifactor en Blockchain*

Guillermo Daniel Romero Arregin[1], Miguel Méndez-Garabetti[1,3], Eduardo Piray[1,2], Ricardo Elian Gonzalez[2], Santiago Araya[3]

[1] Universidad CAECE, Departamento de Sistemas, Mar del Plata, Argentina
gromeroarregin@gmail.com, {mmendezgarabetti,epiray}@ucaecemdp.edu.ar
[2] Universidad Siglo 21, Decanato de Ciencias Aplicadas, Córdoba, Argentina
eliangonzalez045@gmail.com
[3] Free and Open Source Software/Hardware Research Laboratory (FOSSHLab), Mendoza, Argentina
santiagoaraya913@gmail.com

Resumen Uno de los mayores problemas de seguridad a los que se enfrentan los usuarios de wallets en blockchains es la protección y seguridad de las claves privadas asociadas a ellas. Debido a su naturaleza, la pérdida o robo de las mismas compromete de manera permanente toda la información relacionada con una determinada clave privada. En este proyecto se propone la investigación e implementación de un modelo de autenticación que utiliza blockchains como medio para confirmar que un usuario que intenta acceder a un servicio a través de una dirección pública pueda comprobar su identidad a través de la creación y uso de distintas direcciones públicas que actúen a modo de factores de seguridad adicionales. El objetivo principal de este modelo será evitar que entidades no autorizadas puedan acceder a servicios en nombre del propietario de una cuenta existente al utilizar un registro de direcciones fiables almacenadas en forma de smart contract dentro de una blockchain, aprovechando la seguridad e inmutabilidad de la misma para mitigar los riesgos existentes relacionados con la pérdida y/o robo de una clave privada o frase semilla.

Keywords: Blockchain · Autenticación · Esquema · Seguridad · MFA

* Este artículo detalla los avances en la investigación del estudiante Guillermo D. Romero Arregin, cuyo trabajo final de grado se titula Ïmplementación de un Modelo de Autenticación Multifactor en Blockchain". La investigación forma parte del proyecto "Técnicas Avanzadas de Identidad Digital y Aplicación de Zero Trust para la Transición a la Web 3.0", llevado a cabo en la Universidad CAECE, Mar del Plata en el marco de la carrera Licenciatura en Sistemas. El Dr. Miguel Méndez-Garabetti dirige tanto el trabajo final como el proyecto de investigación, el trabajo ha dado inicio en el primer cuatrimestre de 2024.

1. Introducción

Cuando se interactúa con un sistema de seguridad, este debe poder confirmar quién es un usuario que intenta acceder a un sistema, y si dicho usuario es realmente quien dice ser antes de brindar acceso a los servicios que tiene permitido ingresar. Primero un usuario se identifica al sistema, proporcionando una identidad, y luego se confirma dicha identidad al autenticarla a través de algún mecanismo [1], el cual puede estar basado en algo que un usuario sabe, como una contraseña, algo que un usuario posee, como un token o algo que un usuario es, como su huella digital. Además, estos factores pueden ser combinados dentro del mismo proceso de confirmación de una identidad [2].

A través del mecanismo Sign-in With Ethereum [3], es posible utilizar una dirección de blockchain para registrar e iniciar sesión en servicios que lo integren, permitiendo reemplazar la combinación tradicional de nombre de usuario y contraseña por la verificación de una dirección de blockchain a través de una wallet que contenga la clave privada correspondiente.

Cuando los usuarios interactúan con blockchains, uno de los aspectos a tener en cuenta es la seguridad y protección de las claves privadas o frases semilla, ya que sólo a través de estas un usuario puede verificar que es efectivamente el propietario de la dirección asociada con las mismas. Si bien este sistema permite que un usuario pueda actuar sin depender de proveedores de identidad centralizados, la ausencia de estos también implica un mayor riesgo si el usuario sufre la pérdida o robo de su clave privada, ya que no habrá manera de recuperar el control de la dirección, los activos y los servicios asociados a ella.

El problema es que las claves privadas o frases semillas deben ser escritas en papel o en medios digitales ya que son difíciles de recordar, y una vez escritas pueden perderse, o alguien más puede encontrarlas. Si bien existen soluciones para este problema, suelen conllevar cierto grado de pérdida del anonimato característico de las direcciones de blockchains [4].

2. Objetivos del Proyecto

En este proyecto se propone la investigación, implementación y evaluación de un modelo que permita realizar el proceso de autenticación para acceder a servicios a través de un sistema de autenticación multifactor que consiste en el uso de distintas direcciones en blockchain, de manera que se cuente al menos con un factor adicional al momento de confirmar la identidad del usuario.

A través de este modelo, se podrá agregar una capa de seguridad adicional que permita negar el acceso a atacantes que hayan obtenido acceso a una cuenta obteniendo de alguna manera una clave privada o frase semilla asociada, y por lo tanto el control de la misma. Además, ya que la utilización de wallets para acceder a servicios permite cierto grado de anonimato, se buscará respetarlo exponiendo la menor cantidad de información posible en los datos que se publiquen en blockchain.

Por último, se analizará la factibilidad y eficiencia del modelo propuesto, analizando sus ventajas y desventajas, costos y experiencia de usuario.

3. Modelo

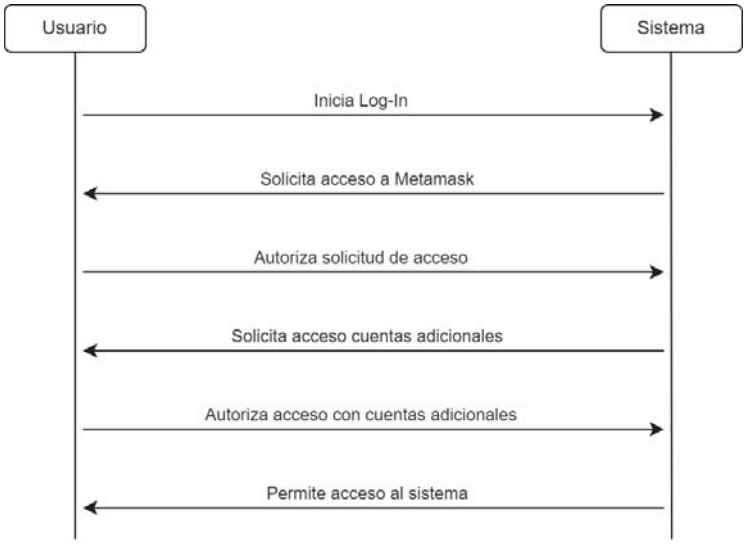

Figura 1. Diagrama de secuencia del modelo, vista de usuario

3.1. Usuario

El usuario utilizará al menos dos direcciones de blockchain, una actuará como principal, mientras que la otra tomará el rol de segundo factor. Para iniciar el proceso de autenticación se utilizará un servicio que acepte el mecanismo Sign-in With Ethereum (SIWE), de manera que el proceso de inicio de sesión pueda realizarse de manera sencilla contando con direcciones asociadas a wallets (ver Fig.1). En este caso, se utilizará la wallet Metamask [5] para autorizar los inicios de sesión. Una vez elegidas las cuentas a utilizar, el usuario deberá desplegar un smart contract en la blockchain donde se registrará la cuenta principal y las cuentas de factor adicional.

3.2. Blockchain

El modelo será probado en una blockchain local desplegada a través de Hardhat [6]. Hardhat es un entorno de pruebas para smart contracts que permite crear y desplegar una blockchain de Ethereum [7] dentro de una red local para propósitos de desarrollo, y que puede ser agregada y utilizada por una wallet. El smart contract a desplegar será lo más pequeño posible y sólo implementará funciones de solo lectura, de manera que no haya costos adicionales al momento

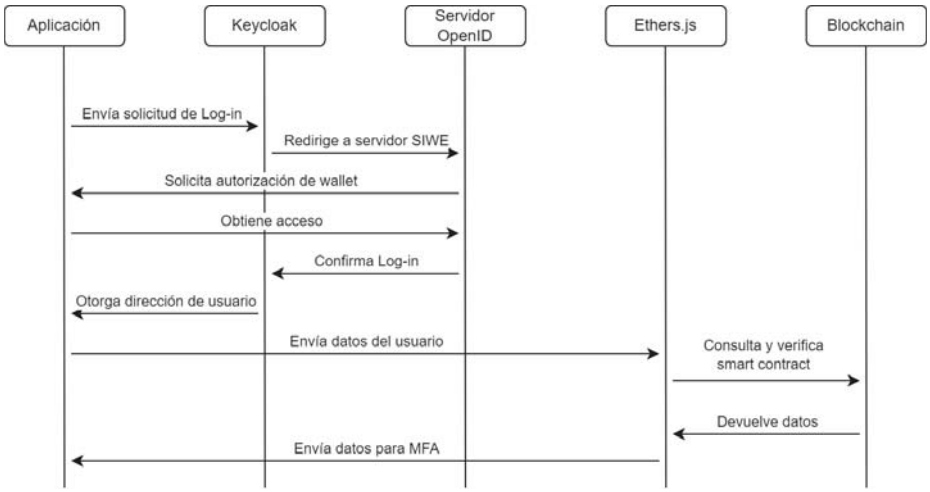

Figura 2. Diagrama de secuencia del modelo, vista de aplicación

de consultarlo. El resultado de la consulta será utilizado por la API Ethers.js [8], que verificará y obtendrá los datos necesarios para el funcionamiento del sistema MFA (ver Fig.2).

3.3. Aplicación

Para la implementación del servicio se utilizará una aplicación en Angular [9], cuya finalidad será la implementación del servicio de autenticación multifactor. Para facilitar la implementación, se utilizará el servicio IAM Keycloak [10] y el servidor público OpenID Connect de Sign-in with Ethereum para la autorización de los inicios de sesión por parte del usuario. Dicha autorización será aprobada o rechazada por el usuario a través de la wallet. Una vez iniciado el proceso de inicio de sesión, la aplicación podrá verificar el smart contract que contiene la o las direcciones a utilizar como factor adicional, así como la cantidad de ellas que serán requeridas para completar con éxito el inicio de sesión (ver Fig. 2). Para la interacción con la blockhain y los smart contracts se utilizará la librería Ethers.js, que permite conectarse de manera sencilla con los smart contracts y ejecutar sus funciones.

4. Conclusión

El principal objetivo del proyecto es la evaluación de smart contracts como factor adicional de autenticación, aprovechando las ventajas proporcionadas por las blockchains, al mismo tiempo que se busca proporcionar una manera de mitigar el riesgo existente relacionado con pérdidas y/o robos de claves privadas y frases semilla, permitiendo así una mayor adopción por parte de los usuarios hacia los sistemas descentralizados.

Por otro lado, el modelo permitirá la inclusión de características adicionales que pueden mejorar la seguridad y la experiencia del usuario, como la posibilidad de recuperación de cuentas asociadas a claves privadas perdidas y/o robadas, y el despliegue sencillo de smart contracts para facilitar la interacción con el sistema.

Referencias

1. Idrus, S.Z.S., Cherrier, E., Rosenberger, C., Schwartzmann, J.J.: A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences (2013)
2. Kim, J.J., Hong, S.P.: A Method of Risk Assessment for Multi-Factor Authentication. Journal of Information Processing Systems **7**(1), 187–198 (Mar 2011). https://doi.org/10.3745/JIPS.2011.7.1.187, https://doi.org/10.3745/JIPS.2011.7.1.187
3. Sign-In with Ethereum | Sign-In with Ethereum (Feb 2022), https://docs.login.xyz
4. Madnick, S.: Blockchain Isn't as Unbreakable as You Think (Nov 2019). https://doi.org/10.2139/ssrn.3542542, https://papers.ssrn.com/abstract=3542542
5. The Ultimate Crypto Wallet for DeFi, Web3 Apps, and NFTs | MetaMask, https://metamask.io/
6. Hardhat | Ethereum development environment for professionals by Nomic Foundation, https://hardhat.org
7. Ethereum, https://ethereum.org/en/
8. Ethers.js, https://docs.ethers.org/v6/
9. Angular, https://angular.dev/
10. Keycloak, https://www.keycloak.org/