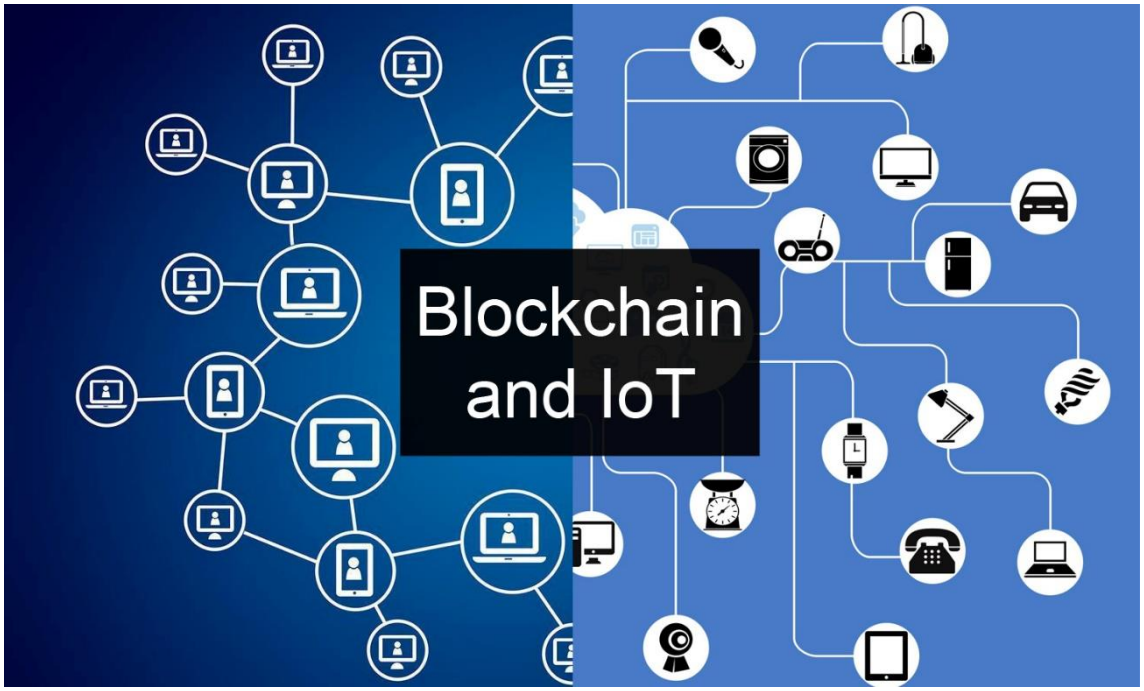
PROYECTO PERSONAL

TEMA: Blockchain & IoT medical



ALUMNO: ADRIÁN BENNASAR POLZIN

ASIGNATURA: 21754 - SEGURETAT EN SISTEMES I SERVEIS

PROFESOR: BARTOLOMÉ JAIME SERRA CIFRE

1. ESTADO DEL ARTE

Blockchain

Blockchain[1], una tecnología que consiste en bloques de datos enlazados criptograficamente, es la clave detrás de la famosa criptomoneda Bitcoin.

Sin embargo, blockchain puede ser util para mas casos aparte de las criptomonedas. Esta tecnologia tiene utilidad en cualquier industria que genere y transfiera datos.

En el caso de las criptomonedas, se utiliza para gestionar transacciones peer-to-peer de una manera que no permite que los datos de la transaccion sean manipulados ni por uno de los involucrados en la transacción, ni por terceros. Esto es un proceso valioso que otras industrias podrian aprovechar.

La tencología Blockchain se ha aplicado ya a muchas configuraciones inteligentes como [4]“smart cities”, “smart homes”, etc y exibe un gran potencial si se integra con la tecnología IoT que existe en muchos de los sistemas inteligentes, como se puede ver en la figura 1. Blockchain provee los servicios de seguridad requeridos por la mayoría de aplicaciones, como confidencialidad de datos, integridad, autenticacion y disponibilidad.

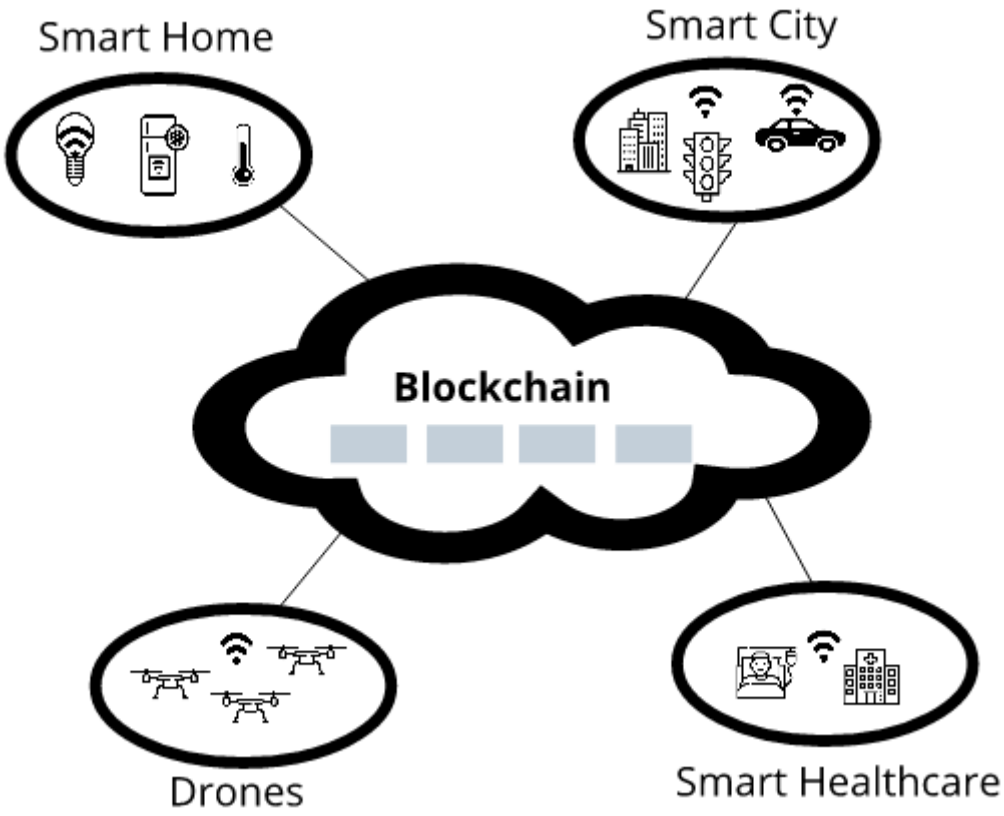


Figura 1. Adaptada de Fig. 1. mostrada en [4]

Internet of Things (IoT)

El Internet of Things (IoT) [2] es una red que consiste en dispositivos sensores que se pueden conectar a la internet de manera inalámbrica. La estructura agrega y gestiona los datos generados por los dispositivos sensores en un nodo que actua como administrador central.

Una de las maneras de dividir la arquitectura IoT actualmente es en 7 capas[6], cada una con unos elementos y funciones en concreto:

7. **Colaboración y procesos:** involucra procesos empresariales y de personas.
6. **Aplicación:** reportar, analíticas, control.
5. **Abstracción de datos:** agregación y acceso.
4. **Acumulación de datos:** almacenamiento.
3. **Edge computing:** análisis y transformación de elementos de información.
2. **Conectividad:** unidades de comunicación y procesamiento.
1. **Dispositivos y controladores físicos:** las “cosas” en IoT.

El campo ha evolucionado debido a la convergencia de múltiples tecnologías[5], incluyendo computación ubicua, sensores de mercancía, sistemas encastados cada vez más potentes y machine learning.

Hay varias preocupaciones respecto de el aumento de popularidad de las tecnologías IoT y productos, especialmente es las areas de seguridad y privacidad, y consecuentemenete, movimientos industriales y gubernamentales han comenzado para afrontar estas preocupaciones, incluyendo el desarrollo de estantares internacionales y locales, pautas y frameworks regulados.

El extenso conjunto de aplicaciones para dispositivos IoT se suele divididir en los siguientes subcampos:

- Consumidor.
- Comercial.
- Industrial.
- Infraestructura.

IoT medical

Una de las industrias donde se está aprovechando la tecnología IoT es la industria médica. Hospitales alrededor de todo el mundo se estan inclinando hacia mejores y más avanzadas tecnologías. En los tiempos recientes, la integración de el Internet of Things con las tecnologías médicas disponibles así como con los pacientes y su ambiente, ha proporcionado una nueva perspectiva[3] para obtención de datos y mejores decisiones.

Los dispositivos IoT pueden usarse de varias maneras para mejorar la salud de las personas junto con asegurar que no existen errores en el proceso de medicación y distribución de medicina.

Pueden usarse para habilitar monitorización médica remota y sistemas de notificación de emergencias[5]. Estos dispositivos de monitorización de salud pueden ir desde monitores de presión sanguínea y ritmo cardiaco hasta dispositivos avanzados capaces de monitorizar implantes especializados, como marcapasos, pulseras electrónicas Fitbit, o ayuda auditiva avanzada.

Algunos hospitales incluso han empezado a implementar “smart beds” que pueden detectar cuando están ocupados y cuándo el paciente está intentando levantarse. Las capacidades de estas camas llegan a características como adaptarse automáticamente y por si solas para asegurar la presión y soporte apropiados sin intervención del personal médico.

BLOCKCHAIN + IoT

Una red compuesta de disposivitos como los utilizados en IoT tiene problemas debido a los recursos limitados.

Estos recursos limitados[2] consisten en:

1. Falta de espacio de almacenamiento.
2. Baja potencia computacional.
3. Capacidad de bateria limitada.

Estos problemas presentan retos considerables en la aplicación de la tecnología de seguridad, como la aplicación de software de alto rendimiento.

Como resultado, se ha investigado y se está investigando aún cómo incrementar la seguridad, ligereza y eficiencia de la red IoT mediante la aplicación de blockchain a IoT.

Al combinar blockchain con IoT, se asegura seguridad robusta a través del uso de la anticorrupción, integridad, almacenamiento distribuido y seguimiendo basado en tiempo de transacciones para la construcción de redes confiables.

BLOCKCHAIN + IoT medical

Una de las potenciales aplicaciones de blockchain en la industria médica es la habilidad para los doctores de obtener datos del paciente y administrar tratamiento de una manera mucho más ágil de la que pueden hoy en día.

Ser capaz de adquirir datos de pacientes rápidamente de otras localizaciones como las oficinas principales de los doctores mientras el paciente esta inconsciente en el hospital o en la sección de tratamiento de emergencia podría significar una importante ventaja. Ayudaría en la eficiencia del tratamiento y

incrementaría las probabilidades de un resultado positivo. Sin embargo, una preocupación común que los pacientes tendrán es la seguridad de los datos que están siendo transferidos.

Introducir blockchain en la industria médica tiene el potencial de dar a los pacientes más (o total) control sobre los datos y mantener los datos seguros e immutables a través de ténicas de encriptación como la pseudo-anonimidad y la infraestructura de clave pública.

Otro ejemplo de aplicación potencial de blockchain es en combinación con los accesorios de tecnología smart que algunas personas llevan puestos hoy en día.

Tener una manera segura de tranferir los datos generados por estos accesorios puede ayudar a los doctores y otros proveederos de salud a tratar y monitorizar a los pacientes. Monitorizar a los datos de los pacientes de forma remota podría ayudar a los doctores a permitir a los pacientes seguir con su estilo de vida normal y habitual incluso cuando estan en una situación de riesgo o complicación.

2. DETECCIÓN DE UN PROBLEMA REAL

Como se ha mencionado, las redes IoT presentan vulnerabilidades y problemas de seguridad. Estas redes tienen un nodo central donde los datos de todos los sensores son acumulados. Entonces un atacante podria atacar el nodo central y robar o modificar estos datos.

Se ha pensado en aplicar blockchain combinado con IoT en la sanidad para permitir a los doctores obetener datos de pacientes de manera remota y administrar tratamiento de una manera mucho más rápida. El problema es que los pacientes se preocupan por las seguridad de los datos que están siendo transferidos. Introducir blockchain en la sanidad tiene el potencial de dar a los pacientes más (o total) control sobre sus datos y mantener estos immutables con la ayuda de tecnicas de encriptación.

De la misma manera, este problema de seguridad ocurre cuando se piensa en utilizar IoT en el campo médico aprovechando la tecnología de accesorios smart como los relojes fit. Monitorizar remótamente los datos que estos dispositivos proporcionan podría ayudar a los pacientes a mantener un estilo de vida normal aún cuando estuvieran en estado de complicaciones. Pero de nuevo surge el problema de la seguridad. Estos datos podrían ser atacados, borrados y modificados por atacantes maliciosos.

Algunos datos estadísticos[10] hacen evidente el problema de la seguridad en IoT:

- SonicWall reporta que los ataques de malware IoT se incrementaron un 215.7% a 32.7 millones en 2018 (comparado con 10.3 millones en 2017). En 2019, los ataques continuaron, pero el incremento fue en un 5%. Este incremento sigue vigente a medida que pasan los años, y se estima que en 2020 los ataques IoT fueron más que los de 2018 y 2019 combinados.
- Palo Alto Networks reporta en su 2020 Unit 42 IoT Threat Report que el 83% de los dispositivos médicos de imaging se ejecutan en sistemas operativos no mantenidos.

- Palo Alto Networks comparte de nuevo en la 2020 Unit 42 IoT Threat Report que el 98% de todo el tráfico IoT **NO** esta encriptado, exponiendo datos personal y confidenciales en la red.

- El **63%** de los consumidores opinan que los dispositivos conectados no les transmiten tranquilidad cuando se trata de obtener datos. Esto es un resultado de Consumers International and Internet Society survey.

- El **47%** de las compañias no evaluan la seguridad IoT y políticas de privacidad de terceros antes de trabajar con ellos, según el Ponemon Institute and Shared Assessment survey.

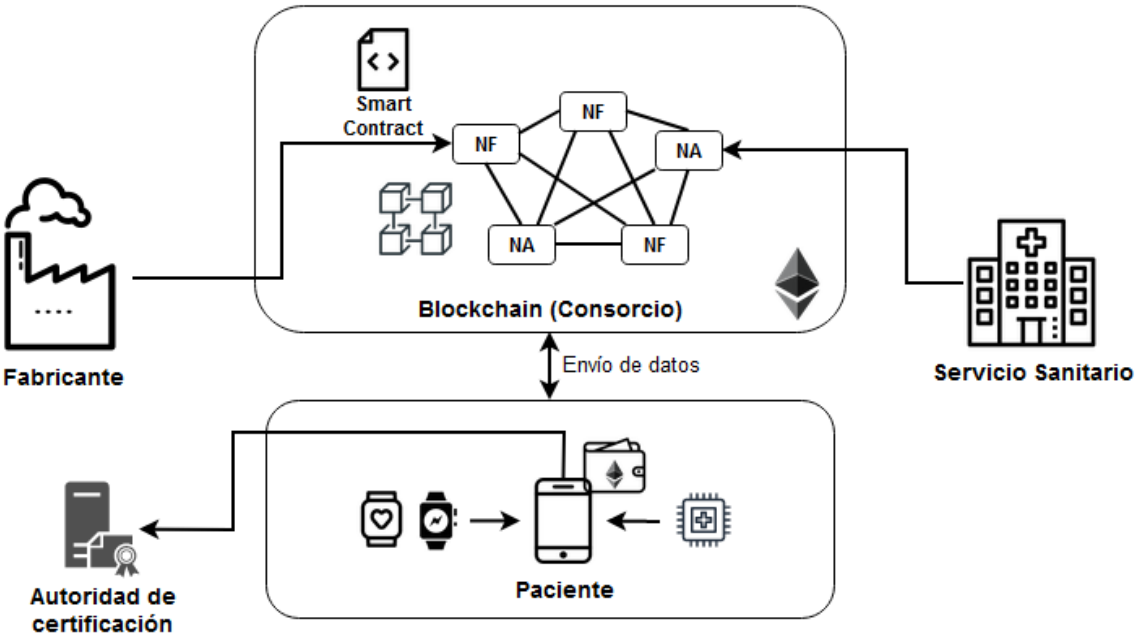
Muy recientemente, investigadores han descubierto que en el **primer semestre de 2021**, ha visto un **incremento del 100%** en ciberataques contra dispositivos IoT. Según los análisis de la telemtria de **Kasperky** de los honeypots, la empresa detectó más de **1.5 billones** de ataques IoT.

A pesar del aumento de su popularidad, el aspecto de la seguridad del IoMT apenas se toma tan en serio como debería.

Muchos hospitales y pacientes ni siquiera son conscientes de que esos dispositivos médicos llevan incorporados un firmware, que debe ser actualizado/parcheado con frecuencia para evitar que se infecten con malwate o ser el objetivo de ataques Zero Day.

A medida que está creciendo el número de firmwares obsoletos y sin ser parcheados, los agujeros de seguridad para compremeter estos dispositivos lo hace en paralelo, lo que puede poner en peligro la vida de los pacientes.

3. DISEÑO DE UNA SOLUCIÓN



El escenario para el que se piensa esta solución es el del uso de IoT medical para la monitorización de señales de pacientes. Estos dispositivos se comunican con un gateway específico, que en el caso de monitorización en smart homes por ejemplo, para enfermedades crónicas, puede ser el Smart Phone del paciente, o un dispositivo dedicado en el caso de monitorización en un centro hospitalario.

Los atacantes realizan frecuentemente ataques del tipo:

1. Suplantación de identidad.
2. Dispositivos falsificados.

La solución se dividirá en 2 partes:

- Sistema de autenticación.
- Blockchain ethereum consorciado.

Creo que los enfoques tradicionales de autenticación basados en contraseñas o claves secretas no son suficientes por si solos para solventar problemas de seguridad importantes hoy en día.

Por lo tanto propongo un esquema de autenticación basado en dos elementos (multifactor).

Pensando en esta idea, se podría aprovechar el uso de los conocidos **PUF (Physical Unclonable Function)** como un elemento adicional para autenticar los dispositivos IoTM.

El PUF es una primitiva emergente basada en la criptografía que está ganando popularidad en el campo de la seguridad IoT. En resumen, el PUF de un dispositivo es un identificador generado de manera única en el proceso de fabricación a través de la introducción de variaciones físicas aleatorias dentro de la microestructura de un circuito integrado.

La primitiva es una función de un solo sentido que es muy difícil de predecir o clonar, haciendola un candidato deseable para ser utilizado como identificador para los dispositivos IoT en un entorno de autenticación.

Por otra parte, blockchain, que ya se ha explicado en la introdución, se usará en combinación con el sistema de autenticación, utilizando un smart contract en contra de los dispositivos IoMT flasificados.

Consiste en un **blockchain ethereum consorciado**, que sería gestionado por proveedores de servicio sanitario y fabricantes IoMT confiables. A su vez, los pacientes tomarían el rol de creadores de datos y a todo esto se suma la utilización de una **autoridad de certificación** en la fase de registro.

El esquema de autenticación PUF basado en blockchain está pensado para verificar la **autenticidad** de los dispositivos IoTM y al mismo tiempo comprobar y proporcionar actualizaciones de firmware confiables, todo de una manera descentralizada, mitigando la carga de una sola entidad centralizada al aprovechar la tecnología blockchain distribuida y tolerante a fallas.

En cuanto a los “participantes” de la cadena de bloques, se podrían dividir de la siguiente manera, en el contexto de esta solución:

- **Nodos autorizados (NA):** es un nodo sellador semiconfiable responsable de minar transacciones, procesar los datos sanitarios compartidos, y gestionar reglas de acceso. Estos nodos estarían bajo la supervisión de los servicios sanitarios y desplegados basándose en un mecanismo de consenso consistente en PoA (Proof of Authority), para asegurar la escalabilidad del blockchain tipo consorcio, ya que este protocolo no requiere de un minado extenso si no que se basa en peers selladores preestablecidos.

  Cada transacción causante de la iniciación del contrato inteligente de autenticación se ejecutaría entre estos nodos, que agruparían las transacciones en bloques basándose en sus marcas de tiempo, y estos son sellados en el ledger.

Por otra parte, serían responsables de el almacenamiento de datos, ya que cada nodo guarda una copia del ledger que contiene todos los datos transaccionales para una auditoría segura.

Finalmente, serían también responsables de actualizar regularmente las credenciales de los pacientes y sus dispositivos (por ejemplo, direcciones Ethereum).

- **Nodos fabricante (NF):** consiste en nodos fabricantes autorizados que no son responsables de sellar bloques en la cadena porque su función sería actualizar las listas de dispositivos autenticados en la cadena y estar al día con las actualizaciones de firmware. Cada fabricante certificado designaría un número de bloques que considere adecuado para llevar acabo las funciones mencionadas.

- **Pacientes:** son los encargados de generar datos, mediante el envío constante de datos monitorizados con dispositivos IoTMedical. Por ejemplo, en un escenario con un paciente que se encuentra en una Smart Home o hospital supervisando sus señales como pueden ser el nivel de azúcar en sangre, presión, ritmo cardíaco, etc. Un paciente como este, estará preocupado con la seguridad y autenticidad de sus propios dispositivos, y saben que están en un entorno donde agujeros de seguridad pueden poner en peligro su vida.

  Para aliviar a los dispositivos IoTM de la carga de tener que interactuar directamente con la red blockchain, una idea sería que cada paciente tenga su propia cartera digital, que contendría las cuentas asociadas con los dispositivos que poseen y esta serviría de gateway conectando los dispositivos a la blockchain consorcio.

Utilizar un sistema de autenticación **centralizado**, tendría las siguientes **amenazas**:

1. **Ataque de suplantación de identidad**: alguien puede intentar obtener la firma de un usuario legítimo al enviar una transacción al sistema.

2. **Ataque Man-in-the-middle**: alguien puede interceptar transacciones entre una entidad y la blockchain para hacer un “temper” de los datos, sin que nadie se entere.

3. **Ataque Replay**: alguien puede reusar una firma previa y enviarla al recipiente.

4. **Ataque de divulgación de identidad**: alguien puede intentar descubrir la identidad real de un paciente mediante la recolección de sus datos.

5. **Ataque de entidad corrupta**: alguien puede ser un nodo fabricante malicioso e intentar engañar a los pacientes para la descarga de firmware corrupto.

Por lo tanto, para mitigar las desventajas de un enfoque centralizado, propongo utilizar los conceptos de blockchain y contratos inteligentes vistos en la asignatura para hacer un enfoque descentralizado. La propuesta facilitaría la gestión de los dispositivos IoTM aprovechando las carteras digitales de los pacientes, el consenso PoA y los nodos fabricantes autorizados.

Cada nodo autorizado es supervisado por un proveedor de servicio sanitario que sería responsable de:

- Encargarse de los nodos y recursos requeridos en una localización geográfica determinada.

- Generación de *n* direcciones Ethereum: generan las claves privadas de los selladores y después calculan la clave pública y de esta se obtiene la dirección Ethereum. Estas direcciones junto con las claves públicas deberían ser supuestamente hechas públicas por cada proveedor de servicio para garantizar que los nodos son entidades semiconfiables (lógicamente ninguna autoridad se beneficiaría de la publicación de una lista fraudulenta).

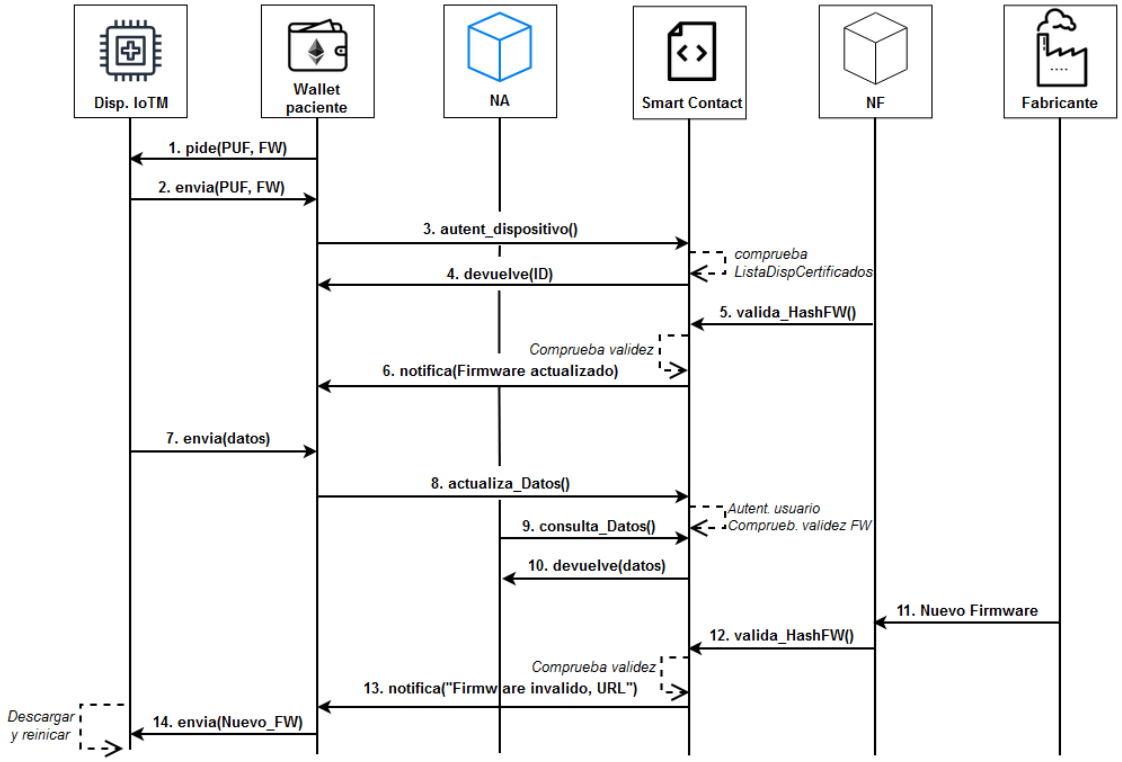
De manera similar, cada fabricante de dispositivos sería responsable de la generación de *m* direcciones Ethereum, que representarían todos los nodos fabricantes a ser gestionados por él. Al igual que los proveedores de servicio sanitario, generan las claves privadas con las que calculan las claves públicas y de esta última obtienen la direccion Ethereum. De nuevo, se haría pública la lista de direcciones Ethereum creadas y las claves públicas.

Estas listas pueden ser utilizadas posteriormente para la verificar si una determinada dirección desde la que se ha enviado una actualización de firmware es gestionada por un fabricante confiable.

El último paso para la construcción del sistema tiene que ver con los pacientes, concretamente con el registro de los pacientes, que se haría a través de una autoridad de certificación. Un paciente registraría su identidad así como los dispositivos IoTM que poseen para obtener las credenciales, incluyendo las de cada dispositivo en particular, que actuarían como las claves privadas y las claves públicas de los pacientes y los dispositivos. La AC generaría también las direcciones Ethereum de los pacientes y estos recibirían un desafío, que tiene

que ver con el PUF mencionado en esta solución, y se usaría para calcular la repsuesta PUF cada cada dispositivo que posee, que se usaría después para la autenticación.

A continuación muestro un diagrama hecho con draw.IO para ilustrar de manera visual y resumida el proceso explicado:



BIBLIOGRAFÍA

[1] K. Wilber, S. Vayansky, N. Costello, D. Berdik and Y. Jararweh, "A Survey on Blockchain for Healthcare Informatics and Applications," **2020** 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2020, pp. 1-9, doi: 10.1109/IOTSMS52051.2020.9340232.

[2] S. Cho and S. Lee, "Survey on the Application of BlockChain to IoT," **2019** International Conference on Electronics, Information, and Communication (ICEIC), 2019, pp. 1-2, doi: 10.23919/ELINFOCOM.2019.8706369.

[3] S. S. Mishra and A. Rasool, "IoT Health care Monitoring and Tracking: A Survey," **2019** 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1052-1057, doi: 10.1109/ICOEI.2019.8862763.

[4] A. Othman Albakri, "Blockchain and the Internet of Things: Opportunities and Challenges," **2021** International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), 2021, pp. 183-188, doi: 10.1109/ICSECS52883.2021.00040.

[5] "**Internet of Things**". Visitado por última vez **04-02-2022,** de https://en.wikipedia.org/wiki/Internet_of_things.

[6] CISCO Internet of Things Reference Model. Visitado por última vez **04-02-2022.**

[9] "**IoT Attacks Skyrocket, Doubling in 6 Months**". Visitado por última vez **04-02-2022,** de https://threatpost.com/iot-attacks-doubling/169224/

[10] "**Surprising IoT Statistics You Don't Already Know**". Visitado por última vez **04-02-2022**, de https://www.thesslstore.com/blog/20-surprising-iot-statistics-you-dont-already-know/