Trabajo Fin de Máster
Máster en Sistemas de Energía Eléctrica

# Potenciales aplicaciones de la tecnología *blockchain* al sector eléctrico

Autor: Francisco Javier Parra Parra
Tutor: Pedro Luis Cruz Romero

**Dpto. Ingeniería Eléctrica**
**Escuela Técnica Superior de Ingeniería**
**Universidad de Sevilla**

Sevilla, 2023

Trabajo Fin de Máster
Máster en Sistemas de Energía Eléctrica

# Potenciales aplicaciones de la tecnología blockchain al sector eléctrico

Autor:
Francisco Javier Parra Parra

Tutor:
Pedro Luis Cruz Romero
Profesor titular

Dpto. de Ingeniería Eléctrica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2023

Trabajo Fin de Máster: Potenciales aplicaciones de la tecnología blockchain al sector eléctrico

Autor: Francisco Javier Parra Parra

Tutor: Pedro Luis Cruz Romero

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2023

El Secretario del Tribunal

# Agradecimientos

Este trabajo ha sido posible gracias al apoyo de varias personas e instituciones, a las que me gustaría dedicar unas palabras.

En primer lugar, me gustaría agradecer a mi tutor Pedro Luis Cruz Romero su ayuda, su amabilidad y que me permitiese escoger el tema de este trabajo. Igualmente, al resto de profesores del máster y del Departamento de Ingeniería Eléctrica de la Universidad de Sevilla, por enseñarnos e inspirarnos tanto.

Agradezco también a todas las instituciones de la educación pública que me han formado como profesional y como persona. Sin ellas, no habría llegado hasta aquí.

A mis compañeros de estudios y de trabajo, por todos los momentos que hemos compartido en estos años. Es un placer trabajar juntos en un sector con un gran impacto en la sociedad, y que, sin duda, tendrá un papel fundamental en la deriva que tome nuestro mundo.

A mi abuelo, por su infinito cariño y por inspirarme con sus historias de una vida vivida en su dimensión más pesada y autentica: la lucha por la subsistencia.

A mi abuela, por su cariño. Por cuidar tanto de su familia. Por estar siempre atenta a los pequeños detalles.

A mi madre, por enseñarme a no conformarme nunca, animándome a mejorar y a tratar de superarme siempre.

A mi padre, por ser un ejemplo. Por hacerme ver las cosas desde una perspectiva diferente a la mayoría. Por demostrarme que se puede prosperar siguiendo nuestros principios, con humildad, empatía y generosidad.

A mi hermana, porque siempre sé que puedo contar ella. Creo que nunca una relación ha tenido una proporción tan grande entre amor y palabras.

A mis amigos, por su constante apoyo y cercanía. Agradezco especialmente a Jero, Mariano y Nuria que se atreviesen y dedicasen su tiempo a leer algún fragmento de este trabajo y a darme su opinión. Y también, a Zarah, por todo su apoyo en los estudios de este máster durante nuestra etapa en Sevilla.

*F. Javier Parra Parra*

*Almería, 2023*

# Resumen

Los sistemas eléctricos se encuentran actualmente expuestos a grandes cambios. Están inmersos en un proceso de descarbonización, donde las centrales de generación térmica convencionales están siendo reemplazadas por generación renovable, con gran parte distribuida en pequeñas instalaciones. Además, han surgido nuevos actores, como los *prosumidores* (consumidores que también generan energía) o el vehículo eléctrico. Estos nuevos elementos se encuentran generalmente distribuidos y en manos de usuarios finales y pequeñas entidades, haciendo necesario un cambio de paradigma en la forma de gestionar y operar los sistemas eléctricos. Así, se está pasando de modelos de gestión centralizados a modelos cada vez más descentralizados, tomando las redes eléctricas de distribución mayor relevancia y donde las microrredes y las comunidades energéticas podrían jugar un papel importante. Todo esto, junto con la digitalización de las redes eléctricas, transformándose progresivamente en *smart grids,* requiere la búsqueda de soluciones innovadoras para garantizar y mejorar su funcionamiento. Este trabajo se centra en explorar posibles aplicaciones de la tecnología *blockchain* para abordar estos desafíos.

En el primer capítulo, se introducen los fundamentos técnicos de *blockchain*, una tecnología disruptiva que en los últimos años ha atraído gran atención.

En el segundo capítulo, se exponen potenciales aplicaciones de *blockchain* en sistemas eléctricos. Estas aplicaciones se han dividido en tres categorías:

- Ciberseguridad
- Mercados eléctricos
- Gestión, operación y control de redes eléctricas

Para cada una de estas categorías, se comienza identificando los desafíos que los sistemas eléctricos manifiestan en el área correspondiente. Posteriormente, se expone como la aplicación de *blockchain* puede contribuir a resolver estos desafíos. Finalmente, se examinan casos de estudio que ilustran aplicaciones concretas de *blockchain*.

En el tercer capítulo, se presenta una aplicación innovadora que propone utilizar *blockchain* para mejorar la gestión de comunidades de autoconsumo solar colectivo. En primer lugar, se define el concepto de comunidad energética y autoconsumo solar colectivo, y se explica el marco normativo que actualmente establece su funcionamiento en España. A continuación, se introduce el modelo propuesto y se exponen las ventajas que su implementación supondría frente al mecanismo actual. Por último, se incluyen los pasos que se han seguido y las herramientas utilizadas para simular el funcionamiento del modelo propuesto. La simulación ha consistido en el desarrollo de una *blockchain* local y el diseño de una comunidad de autoconsumo colectivo formada por 10 viviendas y una instalación fotovoltaica compartida. Para ello, se han utilizado datos de consumo y generación correspondientes a un año. Por último, el código de programación utilizado durante la simulación se ha incluido en el Anexo A.

# Abstract

Power systems are currently facing significant changes. They are undergoing a decarbonization process, where conventional thermal generation plants are being replaced by renewable generation, with a significant portion distributed in small installations. In addition, new players are emerging, such as prosumers (consumers with generation capacity) and electric vehicles. Involvement of these new elements which typically are geographically distributed and owned by several end-users, make necessary a change in the way power systems are managed and operated. As a result, there is a trend from centralized to decentralized models, where distribution grids take more importance together with microgrids and energy communities. All together with the ongoing digitization of electric grids, becoming then in smart grids, requires searching for solutions to ensure and improve their performance. This work focuses on exploring possible applications of blockchain to address these challenges.

The first chapter introduces the technical fundamentals of blockchain, a disruptive technology that has received significant attention in recent years.

In the second chapter, potential applications of blockchain in power systems are presented. The potential applications have been divided into three categories:

- Cybersecurity

- Electrical markets

- Management, operation and control of electrical grids

For each of the three categories, first, the challenges that power systems face are presented. Subsequently, how the application of blockchain can contribute to address these challenges is explained. And finally, some case studies which uses blockchain in power system are shown.

The third chapter present an innovative application that proposes the use of blockchain to improve the management of collective solar self-consumption communities. First, the concept of an energy community and collective solar self-consumption is defined, and the regulatory framework that currently governs their operation in Spain is explained. Next, the proposed model is introduced, highlighting the advantages its implementation would bring compared to the current mechanism. Finally, the steps that have been followed and the tools that have been used to simulate the operation of the model are included. During the simulation process: a local blockchain has been developed, a collective self-consumption community consisting of 10 homes and a shared photovoltaic installation has been designed. Also, consumption and generation data corresponding to one year have been used. Finally, the programming code used during the simulation has been included in Annex A.

# Índice

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# 1 FUNDAMENTOS DE LA TECNOLOGÍA *BLOCKCHAIN*

*No hay que temer nada en la vida, sólo hay que entenderlo. Ahora es el momento de comprender más para temer menos.*

*- Marie Curie -*

*Blockchain* es un registro o base de datos distribuida entre varios participantes, organizada en bloques y protegida criptográficamente. Para mantener la base de datos distribuida, los participantes forman una red tipo P2P (*peer-to-peer*), que básicamente consiste en conjunto de ordenadores (nodos) conectados a una misma red y que intercambian información directamente entre sí. Todos los nodos de la red almacenan de forma local una copia de la base de datos.

La información se organiza en bloques ordenados cronológicamente y que están relacionados matemáticamente entre sí mediante funciones criptográficas. Así, cada bloque contiene una función criptográfica del bloque anterior, haciendo que los bloques estén encadenados. De esta forma, cualquier alteración en la información contenida en bloques anteriores es fácilmente detectable, dificultando la alteración maliciosa de los datos y haciendo el registro inmutable.

Los nuevos bloques son incorporados a la cadena después de un proceso de validación y consenso entre los nodos. En *blockchain* a este proceso se le conoce como mecanismo de consenso, y consiste en una serie de reglas que permite a los nodos llegar a un acuerdo sobre la veracidad de la información contenida en el nuevo bloque. Habitualmente, al nodo encargado de incorporar el nuevo bloque a la cadena, después del proceso de consenso, se le llama minero. Posteriormente, el resto de los nodos replican la cadena de bloques en su copia local. El consenso es una de las claves de *blockchain*, ya que permite que partes que no confían plenamente las unas en las otras, puedan mantener un acuerdo sobre la existencia, el estado y la evolución de una información compartida.

La primera *blockchain* que se popularizó fue Bitcoin, una divisa digital o criptomoneda, descentralizada y que funciona sin la supervisión de una autoridad central. En aplicaciones de *blockchain* como criptomonedas, la información contenida en la cadena de bloques es algo similar a un libro de contabilidad, donde en cada bloque se actualiza el estado de éste. Sin embargo, la información contenida en una *blockchain* puede ser de cualquier tipo, haciendo posible su aplicación en numerosos sectores.

En *blockchain* a las operaciones que se realizan para agregar información a la cadena se le denominan transacciones. Los bloques están formados por varias transacciones empaquetadas. En usos como criptomonedas, la información contenida en las transacciones representa transferencias monetarias entre usuarios. [1]

En la Figura 1-1 se muestra en un esquema simplificado como el registro o base de datos se organiza en forma de cadena de bloques, donde cada bloque está relacionado con el anterior. En esta misma Figura se muestra como cada nodo en la red P2P contiene una copia de esta cadena de bloques.

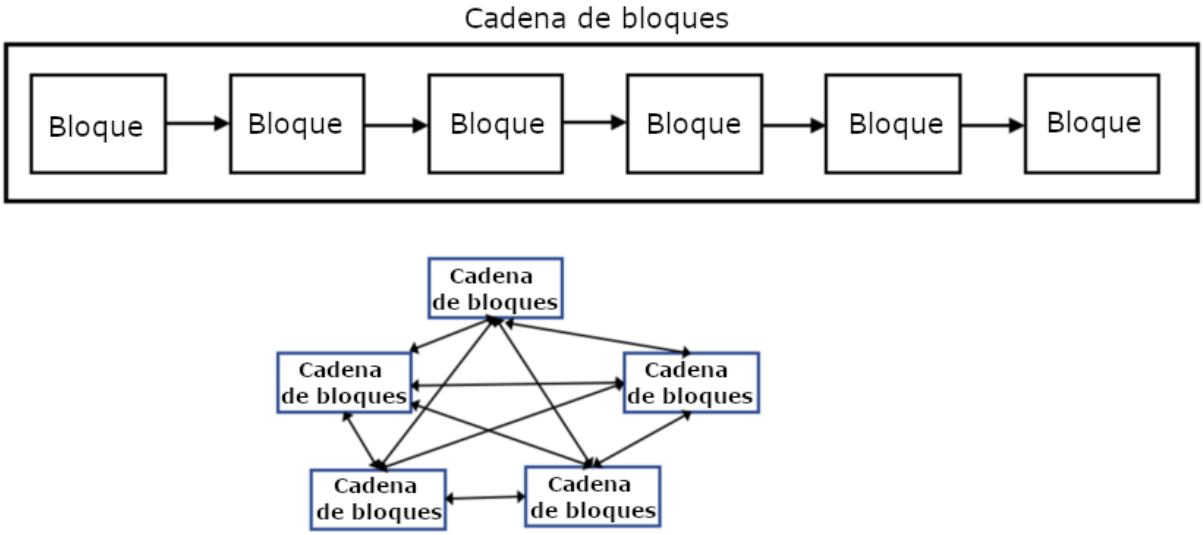


Figura 1-1. Esquema simplificado de una cadena de bloques (arriba) y esquema de una red P2P formada por nodos que almacenan una copia de la cadena de bloques (abajo) [2]

En *blockchain* existen tres aspectos clave, que combinados permiten que *blockchain* cumpla con su propósito:

- **Criptografía**: Para asegurar la integridad de la información de la cadena de bloques, se usan un tipo de funciones criptográficas llamadas *hash.* En una función *hash*, las salidas serán iguales siempre que las entradas sean iguales, una pequeña variación en la entrada arrojará una salida totalmente distinta. De este modo, gracias a que los bloques de la cadena siempre incorporan el *hash* del bloque anterior y un *hash* de las transacciones, es posible detectar cambios malintencionados en el contenido de la cadena de bloques. Otro mecanismo criptográfico ampliamente utilizado en *blockchain* es la criptografía de clave pública. En este mecanismo se emplean dos claves, una privada y otra pública, relacionadas entre sí por una función matemática especial. Conociendo la clave privada es sencillo averiguar la clave pública, pero hallar la clave privada conociendo la pública es muy costoso. Con este sistema un usuario puede autorizar mediante firmas digitales transacciones con su clave privada (secreta), y el resto de los usuarios puede verificar su legitimidad con la clave pública (conocida por todos). En el Apartado 1.2 se trata este tema con mayor detalle, donde se explican distintos tipos de criptografía usados en *blockchain*.
- **Cadena de bloques**: Es la base de datos donde se almacenan la información, organizada en estructuras de datos denominadas bloques. Para su correcto funcionamiento, debe actuar bajo un protocolo, denominado mecanismo de consenso, que asegure la validez de cada bloque, fijando unas reglas determinadas para que un nuevo bloque pueda ser incluido en la cadena. Un bloque está formado por un conjunto de transacciones, y alguna información adicional como el *hash* del bloque anterior o una marca temporal para asegurar la ordenación cronológica de los bloques. En el Apartado 1.5 se muestra con mayor detalle el contenido y la estructura de datos contenida en un bloque y como se relacionan entre sí los bloques adyacentes de la cadena.
- **Consenso**: El mecanismo de consenso se trata de un conjunto de reglas que tratan de asegurar la veracidad de la información o transacciones incluidas en cada bloque. Existen numerosas propuestas de mecanismo de consenso, pero todas ellas consisten básicamente en un método para elegir el nodo encargado de crear un nuevo bloque (minero) y permitir al resto de nodos auditar y validar el proceso, de manera efectiva. El mecanismo más extendido es el conocido como *Proof of Work,* utilizado por Bitcoin y otras *blockchains*. En este mecanismo de consenso, usuarios de la red *blockchain* conocidos como mineros compiten por resolver un puzzle criptográfico siendo necesario aportar cierta capacidad de cómputo para ello. Una vez hallada la solución, esta debe ser fácilmente verificable por el resto de los usuarios, y el minero que consigue resolverlo en menor tiempo recibe una recompensa. En el Apartado 1.4 se profundizará en el funcionamiento de varios algoritmos de consenso.

Desde un punto de vista físico una *blockchain* está compuesta por los siguientes elementos:

- **Nodos**: Son ordenadores conectados a la red desde los que se puede crear, enviar y recibir información. Para participar en la red y comunicarse entre ellos, deben tener todos instalados un software con el mismo protocolo. En una *blockchain* habitualmente existen distintos tipos de nodos, dependiendo de sus funciones y la información a la que acceden. A los nodos que descargan una copia íntegra de la cadena de bloques se les denomina nodos completos, si además participan en el mecanismo de consenso se les llama nodos mineros. También existen otros nodos que sólo descargan una pequeña parte de la cadena de bloques, aquella que es relevante para cumplir sus funciones, se les llama nodos ligeros.
- **Protocolo estándar**: Se trata de un sistema de reglas que dota de un estándar común y define la comunicación entre los nodos de la red. Un ejemplo de protocolo muy conocido es el TCP/IP, utilizado para navegar por internet.
- **Red *peer-to-peer* (P2P) o entre pares**: Es una red de ordenadores en la que ninguno actúa como cliente o servidor, sino como nodos iguales entre sí, actuando simultáneamente como clientes y servidores respecto a los demás nodos de la red. En una red P2P, los nodos están distribuidos e interactúan entre ellos sin necesidad de una autoridad centralizada.

A continuación, se recogen otros conceptos relevantes en *blockchain*, a los que se recurrirá en varias ocasiones a lo largo de este trabajo:

- ***Wallet* (billetera):** Es un software que almacena las claves privadas y públicas de los usuarios. Este software permite firmar transacciones y enviarlas a la red *blockchain*. Así, puede considerarse como una interfaz entre la *blockchain* y usuarios propietarios de unas claves privadas que le permiten "autenticarse" e interactuar con la *blockchain*.
- **Dirección**: La mayoría de *blockchains* usan las direcciones como forma de identificar el destino y origen de una transacción. Normalmente se trata de una cadena de caracteres alfanuméricos derivados de una clave pública de un usuario usando una función *hash*. Una dirección también puede estar asociada a un *smart contract*, y es usada para interactuar con él.
- **Transacción**: Es la unidad datos más pequeña de una *blockchain* y representa una transferencia de información o valor entre dos direcciones.
- ***Token***: Los *tokens* son unidades de valor almacenadas en *blockchain*, y que representan la propiedad de un activo (digital o físico) o de un derecho. Un *token* puede representar valor no sólo como unidad de una divisa digital, también como representación de otro tipo de activos. Los *tokens* son fácilmente transferibles entre usuarios.
- ***Smart contracts***: Se trata de una de las funcionalidades más potentes de *blockchain*. Los *smart contracts* (contratos inteligentes) son piezas de código informático que se almacenan en la cadena de bloques y que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Esto permite a varias partes llegar a acuerdos codificados, teniendo la certeza de que las premisas recogidas en ellos se cumplirán. Con el desarrollo de *smart contract* en *blockchain*, la cadena de bloques deja de ser un mero libro de contabilidad para criptomonedas, abriendo las puertas a otras aplicaciones en sectores muy diversos.

La existencia de un mecanismo de consenso entre los participantes de una red de *blockchain*, permite a los usuarios operar con confianza, **sin necesidad de una autoridad central** que asegure la veracidad de la información. La información contenida en la cadena de bloques es accesible por todos los participantes, que pueden auditar las transacciones y acciones realizadas, mejorando así la **transparencia** de los procesos. Su uso permite **mejorar la eficiencia** en aplicaciones que necesitan compartir información entre varias partes, ya que todos los participantes de una *blockchain* comparten la información y pueden acceder a ella sin interactuar de forma bilateral entre ellos. Además, mediante el uso de *smart contracts* almacenados en la *blockchain*, es posible **automatizar procesos**. También, debido a que la información está distribuida y es difícil de alterar, *blockchain* contribuye a **mejorar la ciberseguridad** de los sistemas, asegurando la integridad, disponibilidad y confidencialidad de los datos.

Para tratar de ilustrar todo lo anterior, veamos paso a paso como sería una transferencia en *blockchain*, utilizando como ejemplo el caso más sencillo y extendido de una criptomoneda basada en *blockchain*.

Se parte de una *blockchain* formada por varios nodos. Cada nodo es un ordenador donde se instala un software

diseñado para: conectar este ordenador a la red P2P, descargar una copia íntegra de la cadena de bloques, participar en el mecanismo de consenso como mineros y funcionar como *wallet* para gestionar y verificar el saldo del propietario. Para aquellos usuarios que quieran participar en la *blockchain* simplemente enviando y recibiendo transacciones (sin participar en el mecanismo de consenso ni almacenar en su ordenador toda la cadena de bloques), existen *wallets* que se conectan a la red, pero sólo almacenan cierta información limitada de la cadena de bloques o incluso acceden a través de proveedores externos de nodos de *blockchain*.

Ahora, supongamos que un usuario A quiere realizar una transferencia de criptomonedas a un usuario B. Para ello, deberá tener instalado en su ordenador o *smartphone* una *wallet*, introducir en ella sus claves privadas, e iniciar desde la propia *wallet* una transacción indicando la cantidad monetaria a transferir y la dirección del usuario B. La *wallet* firmará digitalmente la transacción, utilizando la clave privada del usuario A, y la enviará a la red P2P para su distribución entre los nodos. En este momento, entra en juego el mecanismo de consenso, es decir, los nodos deben decidir si la transacción es correcta e incluirla, junto con otras transacciones, en un nuevo bloque que se añadirá a la cadena. Los nodos verificarán que la transacción está debidamente firmada con la clave privada del usuario A, utilizando para ello la clave pública de éste, gracias a las propiedades de la criptografía asimétrica. Si el mecanismo de consenso implementado en la *blockchain* es el *Proof of Work*, los nodos competirán entre sí para resolver un problema criptográfico. El primer nodo en completar el problema será el encargado de crear un nuevo bloque, y recibirá por ello una recompensa. Por último, el resto de los nodos verificará que la creación del nuevo bloque es legítima (el nodo creador ha resuelto correctamente el problema y las transacciones incluidas en el bloque son correctas y están debidamente firmadas). Una vez confirmada la validez del nuevo bloque, el resto de los nodos actualiza su copia incluyéndolo en su copia de la cadena. Ahora, el usuario B, utilizando también una *wallet* configurada con su clave privada, podrá comprobar que la cantidad transferida ha sido recibida en su dirección.

En otras aplicaciones, más allá de las criptomonedas, la información contenida en las transacciones puede ser de cualquier tipo, por ejemplo, una lectura de consumo eléctrico en kWh de un contador eléctrico inteligente capaz de enviar automáticamente el valor medido a una *blockchain*.

Una transacción también puede contener el código de un *smart contract*, incorporando en la cadena de bloques una pieza de código informático y asignándole una dirección concreta. Otras transacciones pueden tener como destino la dirección de este *smart contract*, aportando información o realizando una llamada a cierta función, provocando un cambio en su estado según su programación. Cuando los nodos mineros se encuentran con transacción destinada a un *smart contract*, ejecutan el código informático. El resto de los nodos valida que la ejecución del *smart contract* es correcta, incorporándose el nuevo estado del *smart contract* a la cadena de bloques.

De forma resumida, podemos decir que *blockchain* consiste en una base de datos donde la información está replicada en varios ordenadores sincronizados y organizada de una forma particular. Y que, hace uso de tecnologías como la criptografía para asegurar la integridad de la información sin la necesidad de una autoridad central de confianza. Volviendo una vez más al ejemplo de una moneda, gracias a *blockchain*, las criptomonedas logran operan sin necesidad de una autoridad central, en contraposición a las monedas convencionales que requieren de bancos centrales, entidades bancarias, y de organismos de regulación para su funcionamiento.

En los próximos apartados se profundizará en los conceptos clave y fundamentos técnicos de *blockchain* expuestos en esta parte introductoria.

## 1.1 Historia de *blockchain*

El 31 de octubre de 2008, Satoshi Nakamoto, un usuario del que se desconoce su identidad, publicó el artículo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System* [3]. En el artículo Satoshi Nakamoto propone un sistema de dinero electrónico basado en una red *peer-to-peer* (P2P), capaz de funcionar sin la necesidad de involucrar a una tercera parte de confianza. Un año después, en enero de 2009, la red de Bitcoin fue implementada, y con el tiempo, fue la primera divisa digital o criptomoneda que se popularizó. El lanzamiento de Bitcoin también supuso el punto de partida para *blockchain*, la tecnología que Satoshi Nakamoto propuso en su artículo.

Una parte importante del funcionamiento de *blockchain* es la criptografía. Durante la década de los años 70, la criptografía pasó de ser una disciplina prácticamente controlada y mantenida en secreto por organizaciones

gubernamentales, a hacerse pública gracias al trabajo de unos pocos pioneros [4]. En 1976 Whitfield Diffie y Martin Hellman crearon el concepto de criptografía de clave pública [5], un método que usa dos claves, una pública que se puede dar a conocer y otra privada que debe ser guardada por el propietario. Poco tiempo después Ralf Merkle hizo otra contribución decisiva, los árboles de Merkle (*Merkle Tree*) [6], una forma de organizar los datos de forma concatenada. Casi a la vez, Ron Rivest, Adi Shamir y Leonard Adleman inventaron el algoritmo RSA [7], un sistema de clave pública que utiliza factorización de números enteros. En el Apartado 1.2 se profundizará en estos conceptos y se verá cómo han sido esenciales para el desarrollo de *blockchain*.

Con estos avances en criptografía como telón de fondo, en los años 90 surgen varios movimientos filosóficos y sociales que abogan por la libertad de expresión, el acceso universal a la información y la privacidad. Estas corrientes de pensamiento han sido enmarcadas dentro del movimiento denominado *cyberpunk* [4][1]. Con las bases técnicas de la criptografía y las nuevas tendencias del *cyberpunk* se inicia un proceso de exploración de nuevas tecnologías y propuestas que promuevan los valores de estos movimientos.

Aunque Bitcoin fue quién sentó los cimientos de la tecnología *blockchain* tal y como la conocemos ahora, hubo varios trabajos previos que fueron decisivos para su desarrollo. El primer trabajo que propone un sistema de cadena de bloques con seguridad criptográfica fue publicado en 1991 por Stuart Haber y W. Scott Stornetta [8]. Estos dos científicos desarrollaron un método para crear marcas temporales sobre documentos digitales, impidiendo que estos pudiesen ser manipulados. En 1997, Adam Back con Hashcash hizo una propuesta para combatir el correo spam que inspiró el mecanismo de *Proof of Work* que usa Bitcoin. [9]

Ya en 1989, David Chaum fundó DigiCash [10], una propuesta de dinero electrónico que hacía uso de varios protocolos de criptografía creados por él mismo. Unos años después, en 1998, Wei Dai y Nnick Szabo proponen B-money [11] y Bitgold respectivamente. Ambos fueron sistemas de divisas digitales que usan *Proof of Work*. Además de crear Bitgold, Szabo fue el primero en conceptualizar los *smart contracts* (contratos inteligentes) [12]. Estos trabajos son los precursores de Bitcoin y Satoshi Nakamoto referenció a muchos de ellos en su artículo.

Posteriormente, la tecnología *blockchain* exploró otras vías más allá de su uso para crear divisas digitales. Así, en 2015 emerge Ethereum, una plataforma *blockchain* que posibilitó la implementación de *smart contracts* y aplicaciones distribuidas [13].

En los últimos años, la tecnología *blockchain* se ha extendido a diversos sectores, y aunque probablemente su aplicación más conocida son las criptomonedas, se están explorando e implementado aplicaciones en múltiples áreas.

## 1.2 Criptografía

Para entender el funcionamiento de la tecnología *blockchain* y su potencial, es importante conocer unos de sus elementos básicos, la criptografía.

La criptografía es la ciencia de mantener los secretos en secreto [14], es decir, su objetivo es proteger el acceso no autorización a determinada información.

De una forma u otra, *blockchain* hace uso de estos tres tipos de criptografía:

- Funciones *hash*
- Criptografía simétrica
- Criptografía asimétrica

### 1.2.1 Funciones *hash*

Una función criptográfica *hash* es una función que siempre tiene una salida de un determinado tamaño, independientemente del tamaño de su entrada. La salida, o *digest,* es en principio única para una determinada entrada, el más mínimo cambio en la entrada de una función hash, arrojará una salida totalmente distinta. Esto permite que varios usuarios puedan aplicar una función *hash* a una información y comprobar que el resultado es el mismo, probando de esta forma que la información no ha sido modificada.

Una función *hash* debe ser capaz de procesar todo tipo de información de una forma eficiente. Además, para garantizar su seguridad, debe tener las siguientes propiedades:

- Resistencia a preimagen. Dada una salida, es computacionalmente muy difícil calcular la entrada de la función. Además, el proceso es unidireccional, no se puede conocer de antemano la salida que se obtendrá con una entrada.
- Resistencia a segunda preimagen: Dada una entrada y su salida, es computacionalmente muy difícil encontrar una entrada que tenga la misma salida.
- Resistente a la colisión: Es computacionalmente muy difícil encontrar dos entradas que produzcan la misma salida.

Las funciones *hash* son usadas en *blockchain* para varios propósitos:

- Generación de direcciones a partir de claves públicas. En ocasiones también se utilizan determinadas funciones *hash* para hacer más legibles las direcciones.
- Almacenar información con seguridad frente a su alteración, de forma que algún cambio se detecte de forma rápida y fácil.
- En *blockchains* que implementan el algoritmo de consenso *Proof of Work*, las funciones *hash* se utilizan para resolver un puzle criptográfico. En el Apartado 1.4, se profundizará en el concepto de *Proof of Work*.

Existen distintos tipos de funciones *hash*, y con el avance de la tecnología su diseño se ha ido mejorando. A su vez, los algoritmos más antiguos han ido quedando obsoletos y su seguridad ha sido quebrantada o está seriamente amenazada [15]. De modo que, una de las decisiones que deben tomar los desarrolladores de una *blockchain*, son las funciones *hash* a implementar en su funcionamiento. Una de la más utilizadas es SHA256, usada por Bitcoin como función *hash* principal. SHA256 es un algoritmo perteneciente a la familia de funciones SHA-2, diseñadas por la National Security Agency (NSA), y que produce una salida de 256 bits. Algunas *blockchains* usan otras funciones como SHA-3 o incluso algunas han diseñado sus propias funciones *hash*, como es el caso de IOTA con su función Curl-P [16].

Las funciones *hash* también se usan para organizar la información en forma de *Merkel Tree* (árbol de Merkle). Los *Merkel Tree* (Figura 1-2) consisten en una formación encadenada de *hashes* piramidales en la que cada *hash* es resultado de aplicar una función *hash* sobre otros de un nivel inferior, hasta llegar al *hash root* o *Merkle Root* [6]. Este sistema permite verificar la integridad de gran cantidad de datos de forma eficiente. El árbol de Merkle es utilizado en *blockchain* para crear un *hash root* formado por los *hashes* de todas las transacciones incluidas en bloque, así cualquier modificación en la información de una transacción es fácilmente detectable.

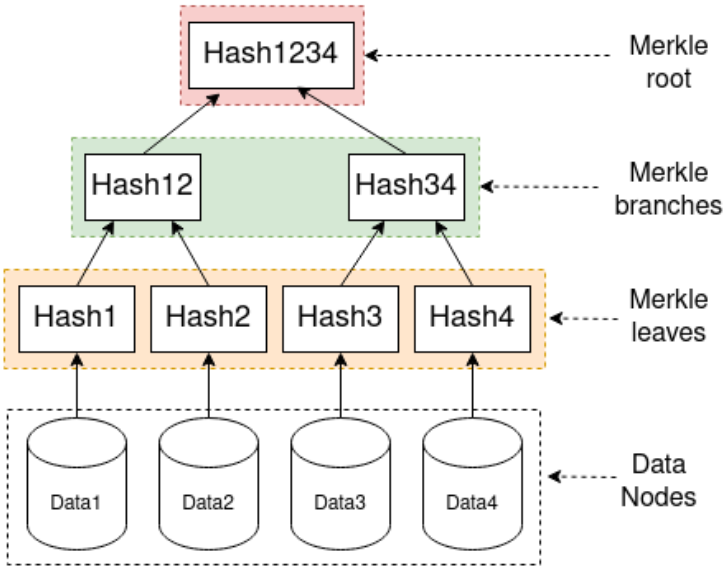


Figura 1-2. Esquema de un *Merkle Tree* [17]

### 1.2.2 Criptografía simétrica

La criptografía simétrica utiliza la misma clave para cifrar y para descifrar el mensaje. Cualquiera que conozca la clave puede descifrar el mensaje, por lo que ésta deber ser guardada en secreto [14]. Así, la criptográfica simétrica es útil cuando no es necesario enviar la clave a otras personas, por ejemplo, para cifrar información en un disco duro. Esto hace que este tipo de criptografía no sea ampliamente utilizada en *blockchain*, usándose en su lugar criptografía asimétrica. Sin embargo, algunas *wallets* la usan para cifrar las claves privadas. Uno de algoritmos más conocidos es AES que utiliza claves hasta 256 bits [18].

### 1.2.3 Criptografía asimétrica

La criptografía asimétrica o de clave pública usa dos claves, una pública y otra privada. La clave privada se mantiene en secreto y la clave pública es compartida. Con la clave pública cualquiera puede cifrar un mensaje que sólo podrá ser descifrado con la clave privada [14]. Lo importante es que la clave usada para cifrar el mensaje, y conocida por todos, no puede ser usada para descifrarlo.

Las claves públicas y privadas están relacionadas entre sí mediante funciones especiales que calculan la clave pública a partir de la clave privada. Estas funciones deben asegurar una resistencia a la preimagen para la clave pública y permitir que conociendo cierta información (clave privada) sea computacionalmente sencillo calcular su inversa. Las funciones unidireccionales que cumplen estas propiedades son llamadas funciones *trapdoor* (trampa) [14]

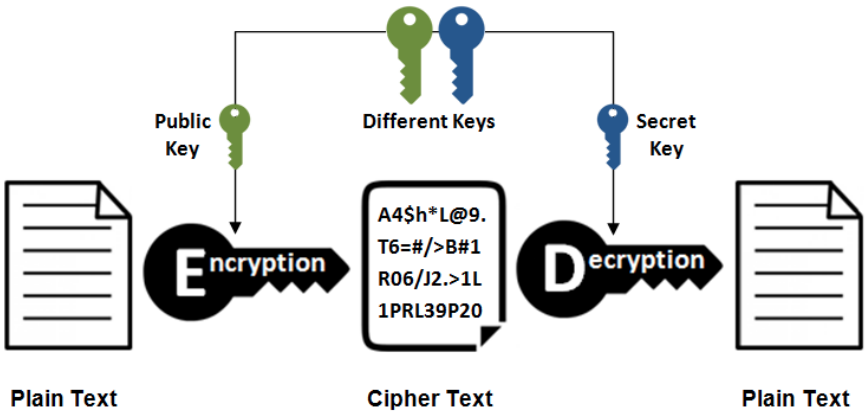


Figura 1-3. Criptografía de clave pública [19]

El algoritmo de clave pública más extendido es RSA, basado en la dificultad para factorizar números primos grandes. Otro algoritmo ampliamente usado en *blockchain* es ECDSA (*Elliptic Curve Digital Signature Algorithm*), es el utilizado por Bitcoin, Ethereum y la mayoría de los protocolos *blockchain*.

La criptografía de clave pública también es usada para crear firmas digitales. Con una clave privada conocida únicamente por un usuario, es posible firmar un mensaje, y con una clave pública, es posible que terceras partes verifiquen que la firma es legítima.

En *blockchain* la criptografía de clave pública es usada principalmente para [20]:

- Autorizar transacciones. Las transacciones son firmadas mediante firma digital usando la clave privada, y la clave pública es usada para verificar las firmas.
- Verificar la identidad de los usuarios. La criptografía asimétrica hace posible verificar que el usuario es poseedor de la clave privada.

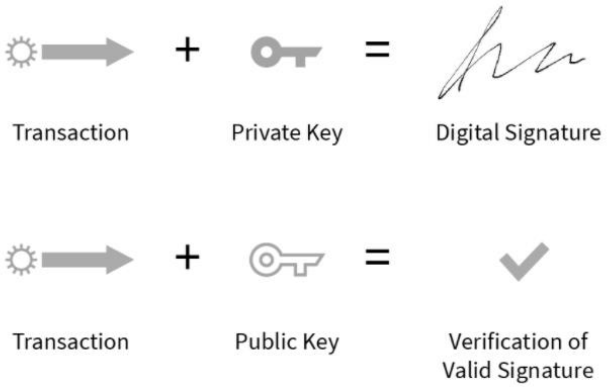


Figura 1-4. Criptografía asimétrica para firma y verificación de transacciones [19]

En la Figura 1-5 se muestra como en Bitcoin se utilizan funciones de clave asimétrica (ESDSA) y funciones *hash* (SHA256 y RIPEMD-160) para generar claves públicas a partir de claves privadas, y a su vez generar direcciones a partir de la clave pública. La claves privadas y públicas se almacenan y gestionan usando una billetera o *wallet*, un software específico. La única forma de iniciar una transferencia desde una dirección determinada es tener acceso a una *wallet* con la clave privada asociada a esa dirección, firmando la transacción con la misma.

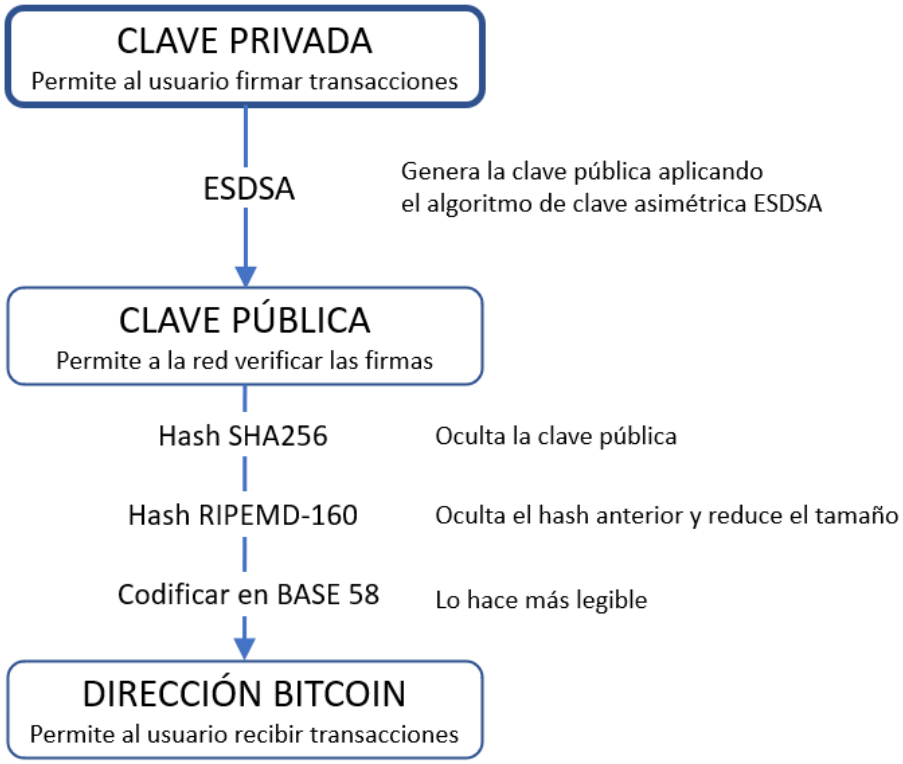


Figura 1-5. Funciones criptográficas utilizadas en Bitcoin [1]

## 1.3 Tipos de *blockchain*

Para tratar de mejorar algunas de las limitaciones técnicas que presentan las primeras redes de *blockchain*, como la de Bitcoin, se proponen modificaciones en algunas de sus funcionalidades. De esta forma surgen distintos tipos de *blockchain*, que pueden ser categorizadas en cuatro tipos [21], [22].

Según su funcionalidad de lectura y creación de transacciones una *blockchain* puede ser:

- Pública: Todos los usuarios o nodos tienen acceso de lectura y pueden crear nuevas transacciones.
- Privada: Sólo un grupo preseleccionado de usuarios o nodos tienen acceso de lectura y pueden crear nuevas transacciones.

En una *blockchain* pública, los datos son accesibles y auditables por todos los usuarios, asegurando la transparencia de ésta. Sin embargo, algunas aplicaciones pueden requerir que se refuerce la privacidad de los datos.

Según su funcionalidad de escritura, una *blockchain* puede ser:

- *Permissionless* (no permisionadas): Todos los usuarios o nodos tienen derecho de escritura, pueden verificar transacciones y añadir nuevos bloques a la estructura de datos
- *Permissioned* (permisionadas)**:** Sólo un grupo limitado de usuarios o nodos tiene acceso de escritura. Son usuarios de confianza y los únicos capaces de verificar transacciones y participar en el proceso de consenso.

La funcionalidad de escritura afecta al conflicto entre seguridad y rapidez. En una *blockchain permissionless*, donde todos los usuarios pueden añadir nuevos datos, el mecanismo de consenso debe ser lo suficientemente robusto para asegurar la veracidad e integridad de los datos. En una *blockchain permissioned*, los usuarios con capacidad de escritura se presuponen de confianza, haciendo posibles un consenso más rápido.

En la Tabla 1-1 se recogen los cuatros tipos de *blockchain* que surgen cuando se aplican los casos extremos de restricciones de lectura y escritura.

Tabla 1-1. Tipos de *blockchain*

| | **Acceso lectura y creación de transacciones** | |
|---|---|---|
| **Acceso escritura** | Abierto | Restringido |
| Abierto | Pública y *Permisionless* | Privada y *Permisionless* |
| Restringido | Pública y *Permissioned* | Privada y *Permissioned* |

Un subtipo de *blockchain* que puede considerarse un híbrido de las anteriores, es la *blockchain* tipo consorcio (*consortium blockchain*) [23]. Este tipo de *blockchains* son creadas y administradas por grupos de empresas o entidades del mismo sector que utilizan una red de *blockchain* para conseguir objetivos comunes. Los nodos participantes son previamente seleccionados y aprobados por el consorcio, pueden escribir y enviar transacciones, pero sólo un grupo de nodos cualificados son los encargados de incluir la información en la *blockchain* añadiendo nuevos bloques. Debido al limitado número de nodos y a la existencia de nodos cualificados de confianza, el mecanismo de consenso de este tipo de *blockchain* permite transacciones de información rápidas y eficientes.

## 1.4 Mecanismo de consenso

En una *blockchain* existen varios usuarios que pueden añadir nueva información, en el caso de *blockchains* de tipo *permissionless*, cualquiera puedo hacerlo. Debido a esta descentralización, donde no existe una tercera parte centralizada de confianza, es necesario implementar un conjunto de reglas que asegure la veracidad de la información. A este conjunto de reglas se le llama mecanismo de consenso.

En lo que respecta al consenso, existen dos problemas que deben ser resueltos: el problema del doble gasto y el problema de los Generales Bizantinos [24]:

- El doble gasto es el riesgo de emplear la misma unidad de cuentas (por ejemplo, una divisa digital) en distintas transacciones. Este problema tradicionalmente se soluciona gracias a la supervisión de

instituciones centralizadas. En *blockchain*, el mecanismo de consenso implementado hace que las transacciones sean verificadas por varios nodos distribuidos antes de ser aceptadas como válidas.

- El problema de los Generales Bizantinos [25], es un problema clásico de comunicación en sistemas distribuidos. En *blockchain* la información es enviada por los nodos a través de una red P2P. Si el envío de información se retrasa, se pierde o incluso sufre ataques maliciosos, el sistema puede ser susceptible de fallos y ataques. Por lo tanto, los mecanismos de consenso deben ser resistentes al problema de los Generales Bizantinos.

Los algoritmos de consensos más utilizados son *Proof of Work (*PoW*)* y *Proof of Stake (*PoS*)*, detallados en los siguientes apartados.

### *1.4.1 Proof of Work*

Este sistema recompensa a los nodos participantes que validan las transacciones de la red y crean un nuevo bloque. Para ello, deben resolver un puzzle criptográfico que requiere cierto esfuerzo computacional. Los nodos que participan en el mecanismo de consenso son llamados mineros.

El problema criptográfico suele ser obtener un *hash* con un valor inferior a un valor determinado, de forma que sea necesario realizar varias iteraciones hasta lograrlo. Aunque resolver el problema requiere un esfuerzo elevado, su verificación por el resto de los nodos debe ser eficiente. Con este sistema se pretende que cada nuevo bloque sea generado por un nodo distinto aleatoriamente. También permite controlar el tiempo de creación de nuevos bloques, modificando la dificultad del problema criptográfico en función de la capacidad de cómputo de la red.

*Proof of Work* es el método de consenso que usa Bitcoin [3], y consiste en los siguientes pasos [26]:

1. Los mineros extraen el encabezado del bloque anterior de la red. En el Apartado 1.5 se muestra la estructura de un bloque en Bitcoin.
2. Las nuevas transacciones emitidas en la red son agrupadas creando una propuesta de nuevo bloque.
3. Se computa el doble *hash* del encabezado del bloque anterior junto con el nuevo bloque propuesto y un *nonce* (valor numérico generado aleatoriametne), usando el algoritmo SHA-256.
4. Se verifica si el resultado del hash es inferior a un valor objetivo. Si lo es, se incluye el nuevo bloque en la cadena, y el minero que resuelve el PoW recibe una recompensa. La red de Bitcoin ajusta de forma dinámica el valor objetivo, modificando la dificultad del problema con el objetivo de mantener una generación de bloques constante (un bloque cada 10 minutos).
5. Si el resultado del *hash* es superior al valor objetivo, se repite el proceso incrementando el *nonce*.

El resto de los nodos, validan el proceso anterior y que todas las transacciones incluidas en el nuevo bloque son válidas. El proceso anterior se muestra en la Figura 1-6.

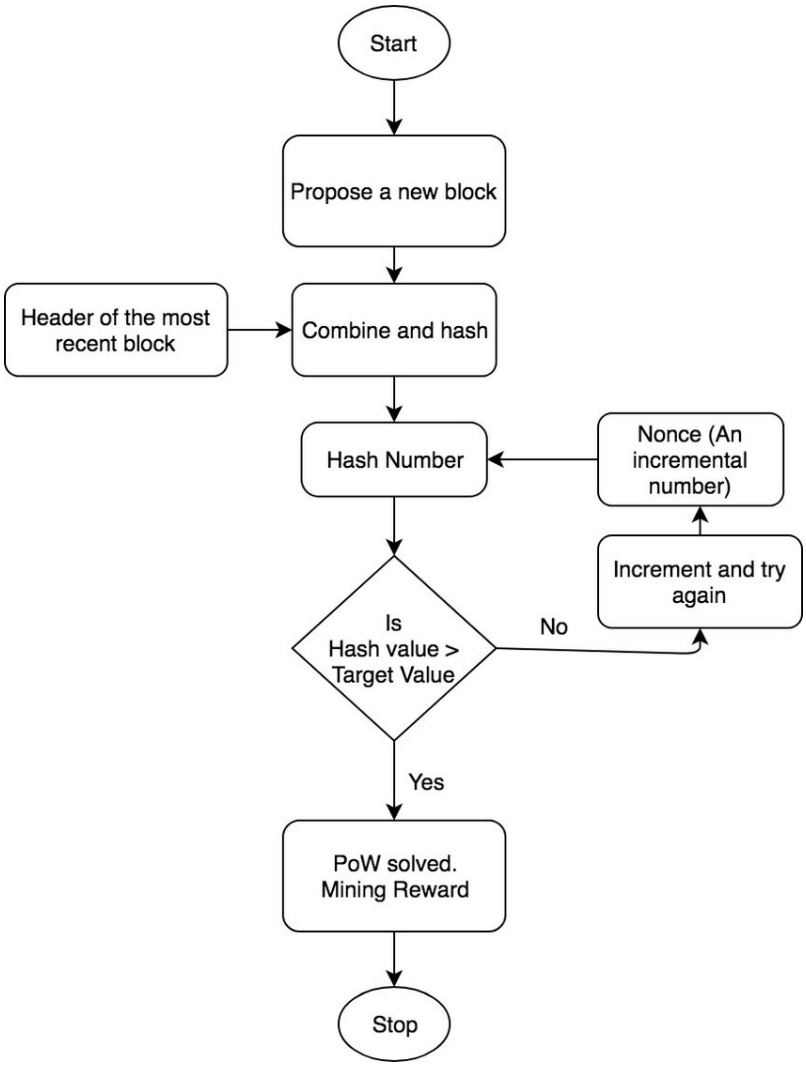


Figura 1-6. Diagrama de flujo del algoritmo *Proof of Work* [27]

Existe la posibilidad de que en algún momento varios bloques sean validados a la misma vez por distintos mineros, lo que resulta en la bifurcación de la cadena de bloques (*fork* en inglés). En estas situaciones, la red almacena ambas ramas hasta que en algún momento una de ellas se hace más larga. En la Figura 1-7 se observa esquemáticamente la bifurcación en dos ramas de una cadena de bloques. Se asume que la rama con mayor número de bloques ha sido producida por una red con una capacidad computacional superior y representa el estado más fiable. Esto hace a la red robusta frente a ataques maliciosos, que intenten crear bloques deshonestamente, siempre y cuando los nodos deshonestos no controlen más del 51% de la capacidad computacional de la red.

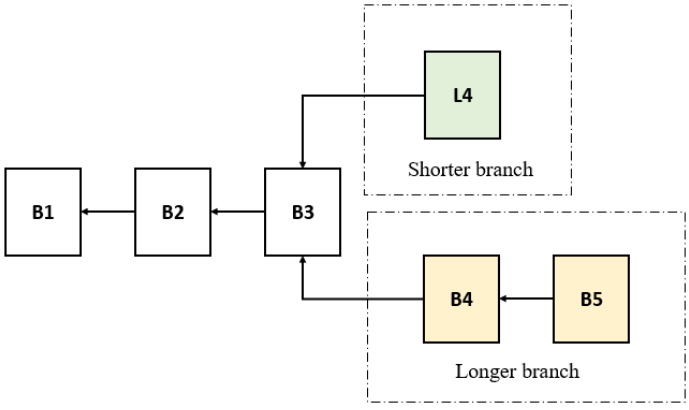


Figura 1-7. Bifurcación de cadena de bloques en dos ramas (*fork*) [28]

El mecanismo de *Proof of Work* ha sido objeto de críticas debido al uso extensivo que hace de recursos [29]. Actualmente los mineros hacen grandes inversiones en hardware para lograr suficiente capacidad de cálculo y obtener mayores recompensas, esto supone además un consumo energético elevado.

### 1.4.2 Proof of Stake

El *stake* es una cantidad de *tokens* que un usuario de una red *blockchain* invierte a través de algún mecanismo específico de la red (bloqueando los *tokens* a través de alguna transacción, enviándolos a alguna dirección o manteniéndolos en alguna *wallet* especial). El sistema de *Proof of Stake* usa la cantidad de *tokens* que los usuarios tienen en *stake* como factor determinante para publicar nuevos bloques. De esta forma, la probabilidad de que un usuario publique un nuevo bloque (y consiga así una recompensa) va ligada al porcentaje de su *stake* con respecto al *stake* total de la red. La recompensa obtenida por publicar un nuevo bloque son las comisiones cobradas por realizar las transacciones que contienen el bloque.

Usando este tipo de mecanismo de consenso, a diferencia de *Proof of Work*, no es necesario un uso intensivo de capacidad de computación con el consiguiente ahorro energético y en hardware que esto supone. Además, las transacciones pueden efectuarse mucho más rápido.

Uno de los problemas que pueden presentarse al usar algoritmos de consenso *Proof of Stake*, es el conocido como *nothing at stake* [30]. Este problema puede ocurrir cuando se produce un *fork* (bifurcación) en la cadena de bloques, ya sea accidentalmente o de forma maliciosa, cuando varios usuarios validan un bloque simultáneamente. Debido a que la validación de bloques o minado no tiene coste, los usuarios pueden seguir minando en ambas ramas de la bifurcación, tratando de maximizar sus beneficios.

Existen varias formas de implementar *Proof of Stake*. Algunas de ellas son [31]:

- *Chain-based Proof of Stake*: El usuario que publica cada bloque es elegido aleatoriamente en función del porcentaje de su *stake*. Cuanto mayor sea el *stake* de un usuario, mayor será su probabilidad de publicar el siguiente bloque.
- *Byzantine fault tolerance proof of stake*: La red selecciona varios usuarios con *stake* para crear propuestas de nuevos bloques. Posteriormente, el resto de los usuarios en *stake* votan por unos de los bloques propuestos. Este método asegura que todos los usuarios tienen voz en cada uno de los nuevos bloques.
- *Delegated Proof of Stake:* Los usuarios con *stake* votan o delegan en nodos que se convertirán en nodos publicadores, en lugar de participar directamente en la creación de nuevos bloques. Con este sistema, el esfuerzo computacional de los participantes no publicadores es nulo, haciéndolo un sistema muy eficiente.

## 1.5 Estructura de datos en un bloque

Como se ha expuesto anteriormente, un bloque es un paquete de información que junto con otros bloques, ligados unos con otros, forman la cadena de bloques. Un bloque se estructura en dos partes, una cabecera y un cuerpo con las transacciones o datos de valor. La cabecera incluye un *hash* de la cabecera del bloque anterior, asegurando la inmutabilidad de la cadena. En la Figura 1-8 se muestra la estructura de datos de un bloque dentro de la cadena.

De forma detallada, y tomando Bitcoin como ejemplo, la estructura de un bloque es la siguiente [20]:

- Tamaño del bloque: Determina el tamaño máximo de cada bloque.
- Cabecera del bloque: Incluye los siguientes elementos:
  - Versión: Número de versión del protocolo que implementa el minero.
  - *Hash* del bloque anterior: Es el resultado de aplicar doble *hash* a la cabecera del bloque anterior.
  - Raíz del árbol de Merkle: Raíz del árbol de Merkle resultante de todas las transacciones que incluye el bloque, tal y como se muestra en la Figura 1-8.
  - Tiempo: Marca temporal del momento en el que se crea el bloque.
  - Dificultad: Indica la dificultad de crear un nuevo bloque en el algoritmo de *Proof of Work*.

- *Nonce*: Es un contador que varía su valor en cada iteración del algoritmo *Proof of Work,* y es utilizado para generar el siguiente bloque válido.

- Cantidad de transacciones: Número entero que indica el número de transacciones contenidas en el bloque.
- Transacciones: Listado de transacciones recogidas en el bloque. Deben aparecer en el mismo orden que en el árbol de Merkel utilizado para generar la raíz del árbol de la cabecera.

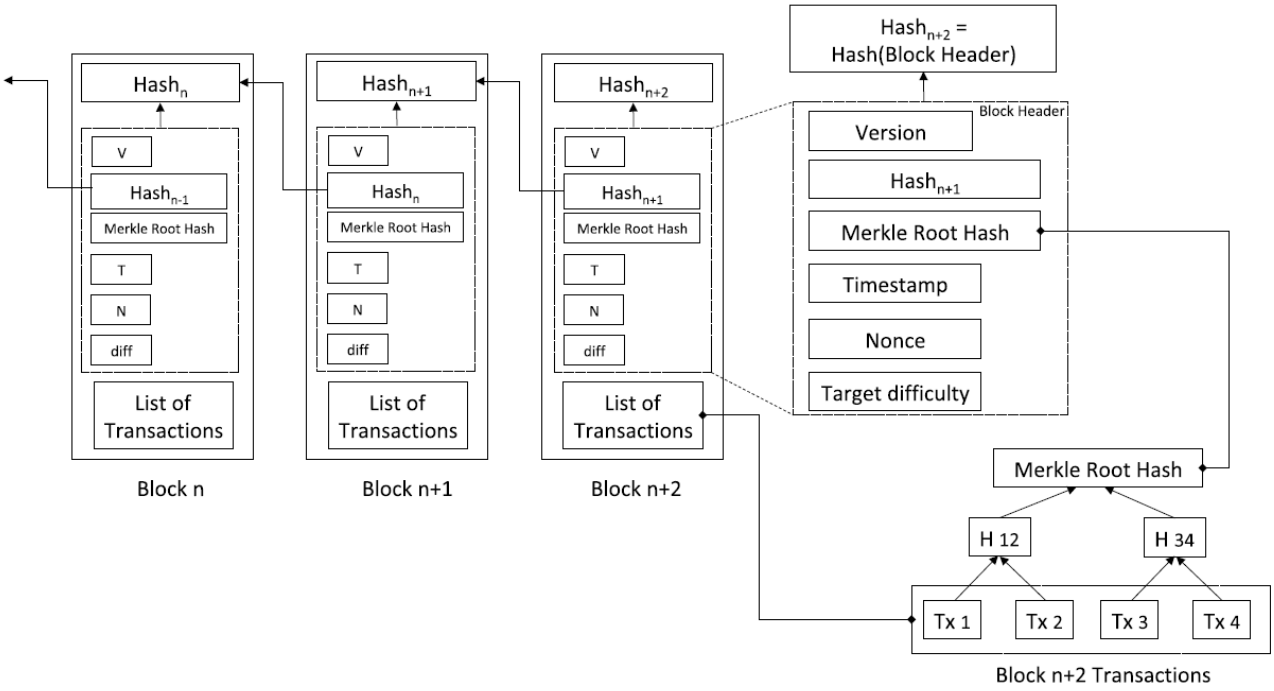


Figura 1-8. Estructura de datos dentro de un bloque [16]

## 1.6 Evolución de *blockchain*

La evolución que *blockchain* ha experimentado desde sus inicios, junto con el grado de sofisticación de sus aplicaciones, se puede clasificar de la siguiente forma [32]:

- ***Blockchain* 1.0**: Criptomonedas. Surge con la creación de Bitcoin, y engloba las aplicaciones de *blockchain* como soporte para la creación de divisas digitales, pagos y transacciones.
- ***Blockchain* 2.0**: *Smart Contracts*. Se introducen los *smart contracts* (contratos inteligentes). Las aplicaciones se extienden más allá de las criptomonedas, a ámbitos de mercados y finanzas principalmente.
- ***Blockchain* 3.0**: Aplicaciones. En esta última generación se implementan aplicaciones descentralizadas (*DApps*), que utilizan *blockchain* en alguna parte de su desarrollo. Su aplicación se extiende a ámbitos más generalistas como salud, ciencia, gobierno o arte.

## 1.7 *Smart contracts*

El concepto de *smart contract* (contrato inteligente) fue originalmente presentado por el criptógrafo Nick Szabo [33]. Sin embargo, la idea de *smart contracts* pasó desapercibida hasta la irrupción de *blockchain*.

En apartados anteriores hemos visto como una *blockchain* es usada como un libro de contabilidad distribuido, con unas determinadas características que aseguran su confiabilidad. Sin embargo, la información almacenada en una *blockchain* puede ser de cualquier tipo, incluso lógica basada en datos que permite programar y automatizar acciones.

Aunque la definición de *smart contract* en la literatura no está del todo clara [34], una definición general es la siguiente: Un *smart contract* es un código ejecutable implementado en una red *blockchain* que facilita, ejecuta y hace cumplir unos términos acordados entre dos o más partes. En otras palabras, un *smart contract* ejecuta de manera automática los términos acordados cuando se cumplen las condiciones determinadas.

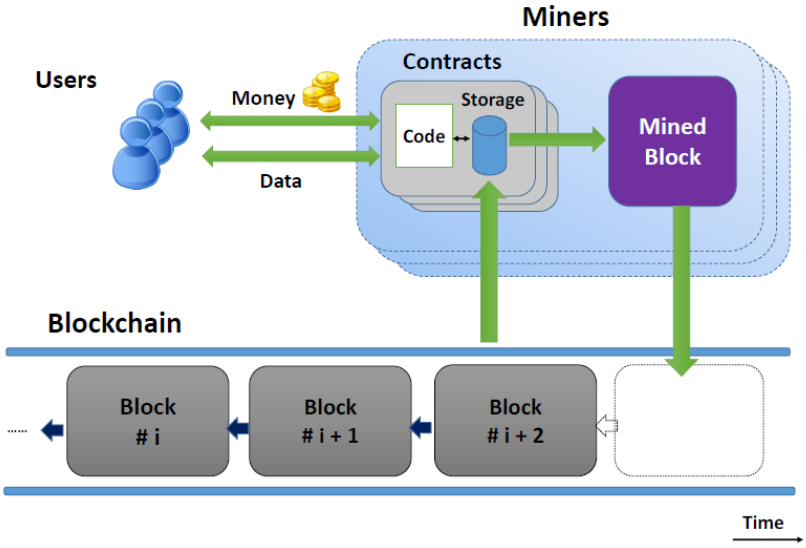


Figura 1-9. Esquema de un *smart contract* alojado en una *blockchain* [35]

En la Figura 1-9 se muestra un esquema simplificado del funcionamiento de una *blockchain* con *smart contracts*. En una *blockchain* pública, cualquier usuario puede crear un *smart contract*. Una vez que el *smart contract* es desplegado en la *blockchain*, su código es invariable y no puede ser modificado. Para interactuar con un contrato, los usuarios deben enviar una transacción a la dirección del contrato. El contrato es ejecutado por los nodos (o mineros) de la red, que deben llegar a un consenso sobre el resultado que arroja el código. El estado del contrato se actualiza y se almacena en la *blockchain*.

Según la necesidad o no de tomar información de una fuente externa a la *blockchain*, los *smart contracts* pueden clasificarse en deterministas y no deterministas [36]. Los primeros no necesitan información de una fuente externa, mientras que los segundos necesitan información de una fuente externa de confianza (llamada oráculo). Un oráculo puede ser, por ejemplo, la lectura de kWh consumidos en un contador inteligente.

A continuación, se profundiza en la operativa de los *smart contracts* usando como ejemplo dos de las plataformas más utilizadas para implementar *smart contracts*, Ethereum e Hyperledger.

- **Ethereum**

Es actualmente la plataforma más utilizada para el desarrollo de *smart contracts* y que también es ampliamente usada para crear aplicaciones distribuidas (*DApps*).

Es común usar la analogía de un registro distribuido para explicar *blockchain*, sin embargo, dando un salto adicional, Ethereum podría ser definido como una *state machine* (máquina de estado) distribuida. Esta máquina de estado es una estructura de datos que puede cambiar en cada bloque de acuerdo con una serie de reglas predefinidas. Las reglas que cambian el estado son definidas por la Ethereum Virtual Machine (EVM) [13].

La Ethereum Virtual Machine es una máquina virtual completa de Turing que es ejecutada por los nodos de la red. Un *smart contract* puede ser programado en lenguajes de alto nivel, como *Solidity*, compilado a lenguaje *bytecode* y desplegado en la *blockchain* [37]

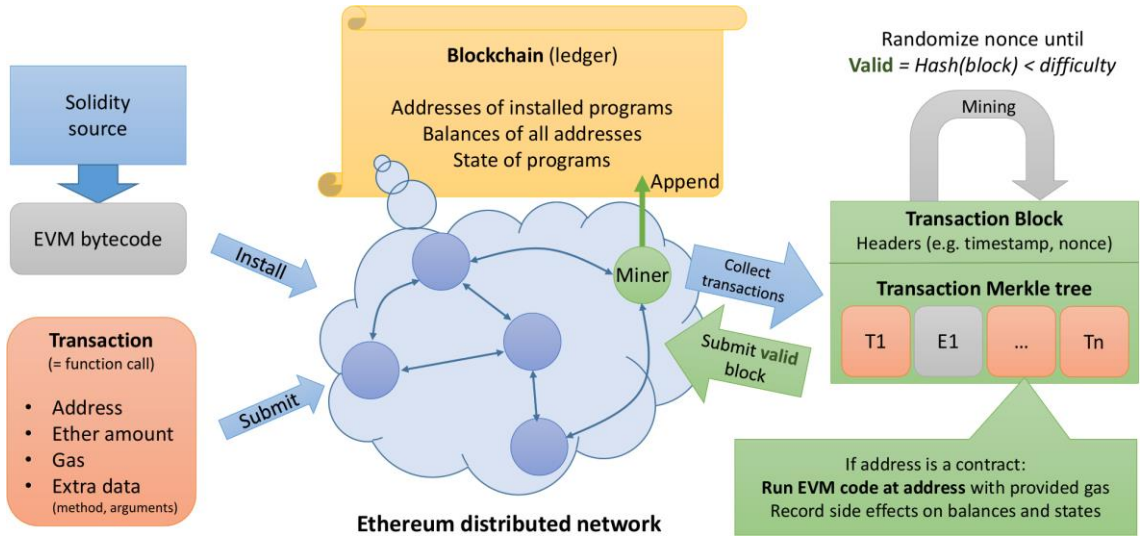


Figura 1-10. Proceso de creación y ejecución de *smart contracts* en Ethereum [38]

En la Figura 1-10, se muestra el funcionamiento de la red Ethereum. Los usuarios pueden iniciar una transacción desde una cuenta externa. Las transacciones pueden incluir datos en forma binaria (*payload*) y Ether (criptomoneda usada en la plataforma Ethereum). Si el destinatario de la transacción es un *smart contract*, su código es ejecutado en la EVM por los mineros, tomando como entrada los datos incluidos en la transacción (*payload*). El resultado obtenido de la ejecución del *smart contract* es emitido a la *blockchain* y el resto de los nodos se encargan de verificar la información. Un usuario puede crear un *smart contract* emitiendo una transacción con dirección de destinatario 0 [38].

En la red Ethereum, todas las actividades sujetas a computaciones de programación (crear nuevos contratos, hacer llamadas a contratos, ejecutar operaciones en la EVM, etc), están sujetas al cobro de comisiones, en concepto de recompensa para los mineros que aportan su capacidad de computación. La unidad usada para medir las comisiones requeridas para cada actividad es el *gas* [39].

- **Hyperledger Fabric**

Se trata de una de las iniciativas lanzadas por The Linux Foundation para el desarrollo de *blockchain*. A diferencia de otras redes, como Bitcoin o Ethereum, es una red privada y permisionada y no usa una criptomoneda en su ecosistema. La red está formada por una serie de participantes corporativos que deben solicitar un servicio de membresía [40].

En Hyperledger Fabric no todos los nodos de la red son iguales, según su función se clasifican de la siguiente forma [41]:

- *Peers*: Mantienen los datos del *ledger* (registro) actualizados. El *ledger* es el registro secuencial y resistente a modificaciones de las transacciones y cambios de estado. Los *peers* también almacenan *chaincode* (estructuras de datos que se usan para programar diferentes funciones, es decir *smart contract*). A su vez, un *peer* puede ser clasificado como *endoser* (simulan y avalan transacciones propuestas) o *committers* (verifican las propuestas de transacciones, validando el resultado antes de grabarlas en la *blockchain*).
- Clientes: Son aplicaciones que interactúan con la *blockchain* proponiendo transacciones, es decir, permite a los usuarios finales comunicarse con la red.
- *Ordereres*: Recibe las transacciones propuestas y las empaqueta dentro de un nuevo bloque en la *blockchain*. Se encargan de asegurar el consenso.

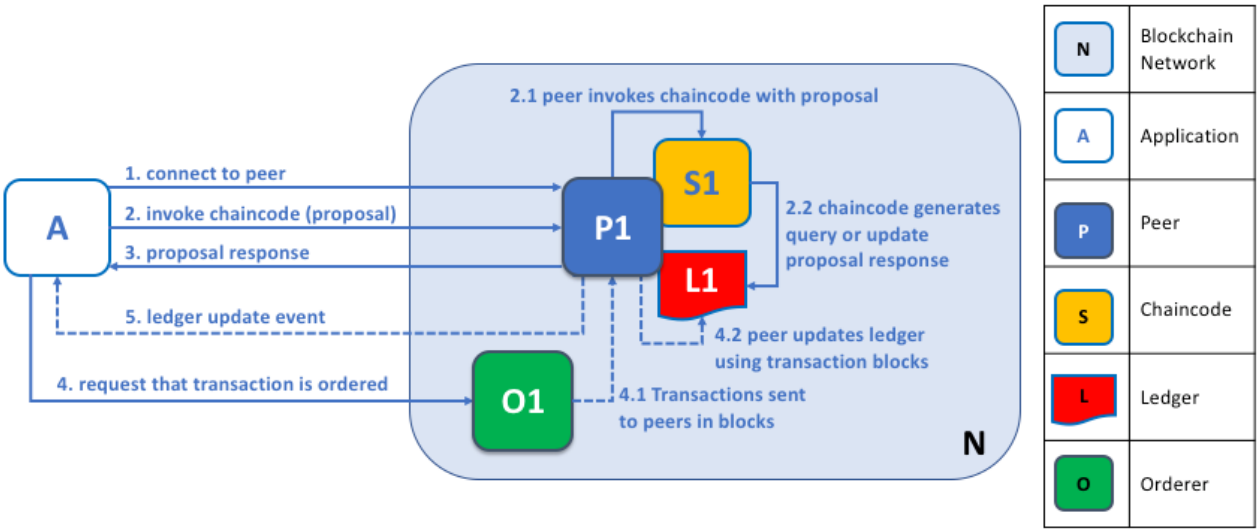


Figura 1-11. Llamada y ejecución de un *smart contract* en Hyperledger [42]

En la Figura 1-11 se muestra el flujo de una transacción en Hyperledger. Una aplicación envía una propuesta de transacción a varios *endoser peers* invocando una función *chaincode* (*smart contract*). La transacción genera una determinada respuesta (salida) que es enviada por los *endosers*, incluyendo una firma criptográfica, de vuelta a la aplicación. La aplicación verifica que la respuesta de todos los *endorsers* es igual y emite la transacción a un nodo *orderer*. El nodo *orderer* ordena la transacción junto con otras transacciones en un bloque que es enviado a la red. Los *peers* conectados a la red validan el nuevo bloque, verificando la firma de los *endorser*. En esta última fase no se ejecuta de nuevo el código, sólo se verifica que el resultado proviene de *endorser peers*. Una vez validado el bloque, los *peers* lo añaden a la cadena y el *ledger* se actualiza [40].

Algunas de las diferencias entre Hyperledger Fabric y Ethereum son [37]:

- Ethereum es una plataforma pública y *permissionless*, cualquiera puede participar en ella. Hyperledger está formada por un consorcio de organizaciones y es privada.
- Hyperledger no integra en su plataforma el uso de una criptomoneda. Tampoco tiene un sistema de comisiones para incentivar la participación de los nodos mediante recompensas, como el *gas* de Ethereum. El coste de operación de la red es asumido privadamente por los propietarios.
- En Ethereum el código de un *smart contract* es incluido en una transacción que es propagada a la red P2P, donde cada minero puede ejecutarlo en su EVM local. Sin embargo, en Hyperledger, el código (*chaincode*) es almacenado por nodos (*peers*) y el código sólo es ejecutado por *peers* específicos cuando una aplicación crea una transacción.

Estas diferencias permiten que Hyperledger Fabric tenga un mayor grado de escalabilidad, con transacciones rápidas y sin coste por transacción. Esto es posible gracias a que los nodos participantes son sometidos previamente a un proceso de aceptación, dentro de una red privada, pudiendo simplificarse el mecanismo de consenso.

## 1.8 Aplicaciones descentralizadas (*DApps*)

Las aplicaciones descentralizadas (abreviado en inglés como *DApps*), son aplicaciones con un desarrollo basado en estructuras descentralizadas. Parte de su código se ejecuta en redes tipo P2P, como una *blockchain*. Habitualmente el término *Web3* también es usado para referirse a este tipo de aplicaciones [43].

Una aplicación tradicional normalmente tiene una arquitectura similar a la presentada en la Figura 1-12 y está compuesta de:

- Base de datos centralizada donde se almacena la información necesaria, alojada en servidores.

- Código *back-end*, escrito en lenguajes de programación como Python o Java. Define la lógica de negocio de la aplicación. Es la parte oculta de la aplicación y define su comportamiento interno. Por ejemplo, qué sucede cuando un usuario ejecuta determinada acción.
- Código *front-end*, escrito en lenguajes de programación como HTML, JavaScript o CSS. Define la lógica de la interfaz de usuario (UI) de la aplicación. Es la parte visible de la aplicación, con la que los usuarios interactúan.

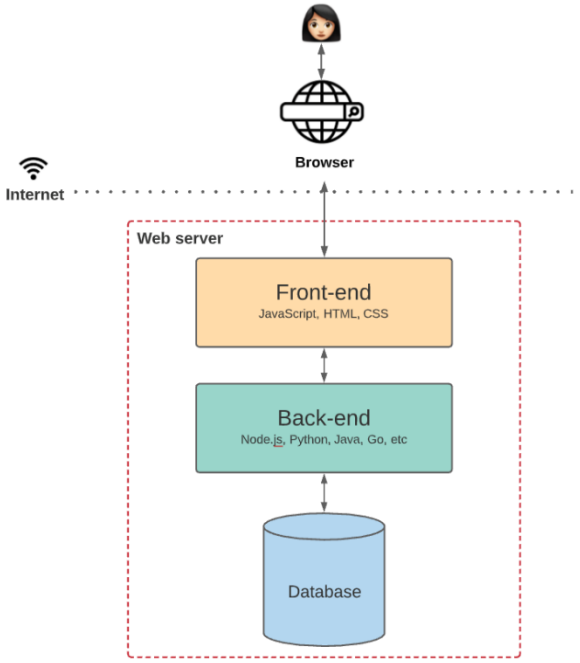


Figura 1-12. Arquitectura básica de una aplicación convencional [44]

En una aplicación descentralizada basada en *blockchain* no existe una base de datos alojada en un servidor, la parte *back-end* está compuesta por *smart contracts* que interactúan con la cadena de bloques, tal y como se observa en la Figura 1-13.

La parte *front-end* debe incorporar una *wallet*, como Metamask, para gestionar las claves criptográficas privadas y la dirección *blockchain* del usuario. Con el software de la *wallet* el usuario puede identificarse y autenticarse mediante la infraestructura de clave pública, y de esta forma puede interactuar con los *smart contracts* de la aplicación. Esta forma de identificación del usuario es más segura que la forma tradicional de usuario y contraseña empleada por las aplicaciones tradicionales, donde los datos se almacenan en servidores de proveedores.

Para que la aplicación se comunique con los *smart contracts*, y pueda invocar funciones, es necesario interactuar con alguno de los nodos de la *blockchain*. Para evitar que las aplicaciones tengan que desplegar nuevos nodos, es habitual el uso de nodos de terceros, llamados nodos proveedores, como pueden ser Infura o Alchemy. [44]

La interfaz de usuario o *front-end* puede estar alojada en servidores centralizados, igual que las aplicaciones tradicionales, o pueden estar alojada en almacenamientos descentralizados como son Swarm o IPFS. [44]

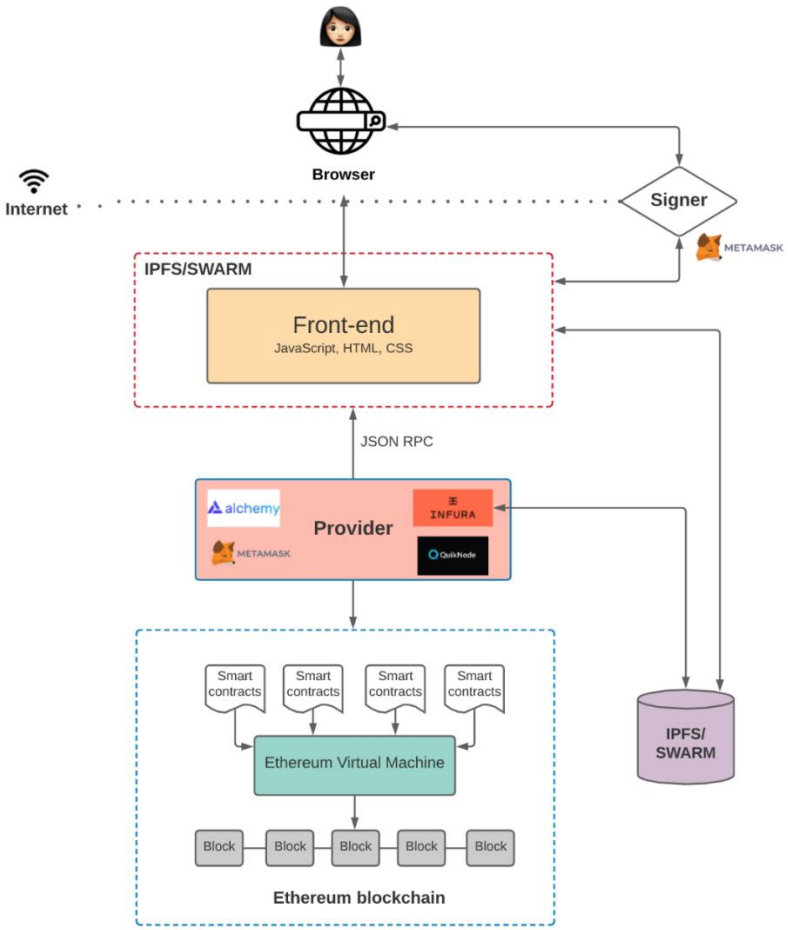


Figura 1-13. Esquema de aplicación descentralizada basada en *blockchain* [44]

## 1.9 Aplicaciones y usos de *blockchain*

*Blockchain* ofrece numerosas oportunidades de aplicación práctica en diversos sectores, además de su uso como criptomoneda. En general, *blockchain* puede ser de utilidad en situaciones donde intervengan varios participantes, sea necesario o eficiente prescindir de una tercera entidad de confianza, la identificación digital, demostrar propiedad de activos digitales, llevar registros descentralizados o automatizar procesos de naturaleza transaccional o fácilmente parametrizables. En la Figura 1-14 se muestra un flujograma que, de forma general, indica si para una determinada aplicación es conveniente utilizar *blockchain* en lugar de una base de datos convencional [45].

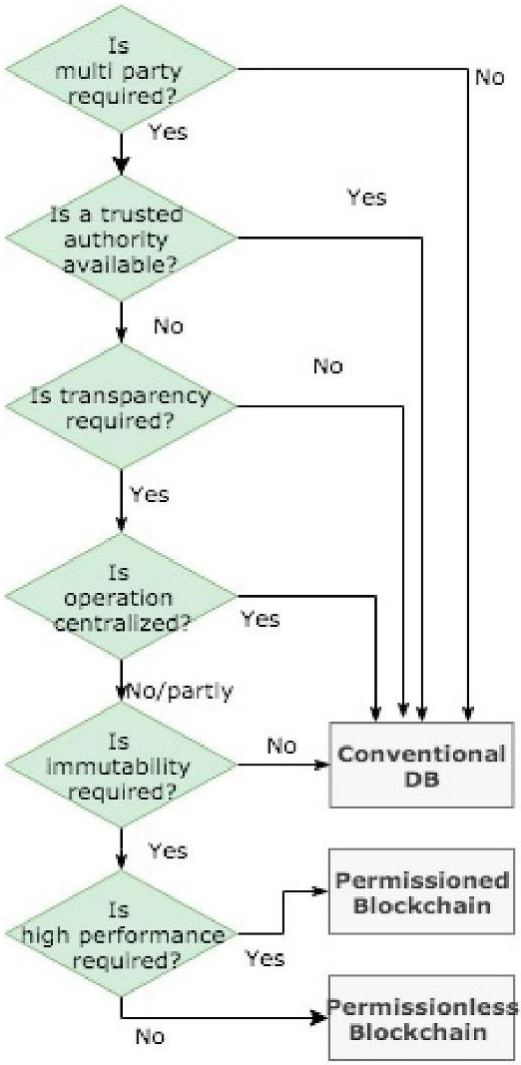


Figura 1-14. Flujograma de conveniencia de uso de *blockchain* frente a una base de datos convencional [45]

Existen varios sectores donde han surgido soluciones innovadoras aprovechando *blockchain*, como son:

- Finanzas: Las criptomonedas ha sido la aplicación más extendida hasta ahora. Las más populares son Bitcoin y Ethereum, pero existen multitud de propuestas con diferentes características. Por ejemplo, las denominadas *stablecoins* son criptomonedas cuyo valor va ligado a alguna moneda de curso legal, como es el caso de Theter ligada al valor del dólar [46]. También han proliferado numerosas plataformas o *exchanges* donde unas criptomonedas u otros activos pueden ser intercambiados por otros, haciendo que el público en general pueda acceder a la compra de este tipo de activos, normalmente con la intención de especular con su valor. El mercado de las criptomonedas ha llegado a alcanzar una capitalización de más de 2 billones de dólares [47].
- Gestión de la propiedad: *Blockchain* permite la verificación y autenticidad de documentos, y de otro tipo de archivos digitales, sin necesidad de una autoridad central, siendo posible certificar su propiedad, existencia e integridad (inalterabilidad). Además, la propiedad de un activo o el derecho a ciertos beneficios puede representarse a través *tokens*. Los *tokens* son unidades de cuentas transferibles dentro de una *blockchain*, y a diferencia de las criptomonedas, estos pueden representar cualquier tipo de valor. Es muy habitual que nuevas empresas o startups se financien ofreciendo *tokens* que representan una parte del negocio, a este tipo de financiación se le denomina ICO (*Inicial Coin Offer*) [48]. Los tokens también pueden usarse para representar la propiedad de activos únicos o no fungibles, son los llamados NFT (*Non-Fungible Token*), que han tomado gran relevancia principalmente en la certificación de propiedad de obras de arte digital. Dentro del sector eléctrico, la propiedad de activos como una planta de generación, se puede gestionar mediante *tokens* basados en *blockchain*.

- Cadena de suministro: La gestión de cadenas de suministro es una actividad que normalmente involucra muchas organizaciones y entidades (productores, fábricas, transportistas, etc), haciendo que existan muchas subactividades que deben ser planificadas, coordinadas, monitorizadas y verificadas. El proceso puede mejorar su eficiencia usando *blockchain* para verificar, almacenar y auditar las transacciones. También, mediante la implementación de *smart contracts* que se ejecuten de forma automática cuando se cumplen ciertas condiciones [49].
- Sector público: *Blockchain* puede utilizarse para gestionar registros de datos públicos, como registros de datos ciudadanos, censos o registros de propiedad, mejorando su seguridad y su accesibilidad desde distintas entidades. También es posible implementar sistemas de votación y de identidad digital [50].
- Sector eléctrico: La integración en los sistemas eléctricos de nuevos elementos como generación distribuida, vehículos eléctricos, contadores inteligentes, junto con un proceso de digitalización y transición hacia *smart grids* hace que sean necesarias nuevas soluciones para integrar y operar eficientemente estas redes. Existen numerosas propuestas que utilizan *blockchain* para mejorar la eficiencia, seguridad y transparencia durante la operación de sistemas eléctricos.

## 1.10 Debilidades

Aunque *blockchain* es una tecnología prometedora y ha demostrado tener utilidad en distintas aplicaciones, todavía existente algunas limitaciones y retos que esta tecnología debe superar. Algunas de las debilidades detectadas son las siguientes:

- Seguridad: Aunque *blockchain* se propone como solución a varios problemas de ciberseguridad, existen algunos aspectos que deben ser considerados al usar una *blockchain*, como es la posible vulnerabilidad al ataque del 51%. En una *blockchain* pública la veracidad de la información puede verse comprometida si más de la mitad de los nodos están controlados por la misma persona o entidad.
- Regulación: Actualmente no existe un marco regulatorio que sustente algunas posibles aplicaciones de *blockchain*. Aunque *blockchain* es capaz de dar pruebas técnicas de propiedad, consenso, acuerdos entre partes y responsabilidades, es habitual que las soluciones basadas en *blockchain* no estén legalmente soportadas.

Sin embargo, la mayor limitación de *blockchain* probablemente sea su escalabilidad:

- Escalabilidad: La escalabilidad de un sistema se refiere a su capacidad de gestionar un aumento en su volumen de trabajo sin disminuir su calidad del servicio. Debido a que normalmente en una red *blockchain* los nodos participantes deben almacenar y aportar capacidad de cómputo y llegar a un consenso para validar las transacciones, un incremento en el aumento del número de nodos o de transacciones provoca problemas de escalabilidad. Estos problemas implican mayores necesidades de almacenamiento, mayor consumo de recursos de cómputo y energéticos y disminución de la velocidad de transacciones [51].

Los problemas de escalabilidad se dan principalmente en *blockchains* con mecanismo de consenso basado en *Proof of Work* y de tipo *permisionless*. Las *blockchains* tipo *permissioned*, con posibilidad de implementar otro tipo de mecanismos de consenso que consuman menos recursos, pueden ser una alternativa en algunas aplicaciones. Sin embargo, esto supone una pérdida de descentralización, una de las características más interesantes de *blockchain* [52].

El llamado *blockchain "trilemma*" es un concepto que sugiere que la mejora en alguno de los tres atributos escalabilidad-seguridad-descentralización, supone una merma en los otros dos. Por eso, es necesario ajustar el diseño de cada *blockchain* en función de las necesidades de cada aplicación.

Existen muchas propuestas y soluciones para tratar de mejorar el problema de escalabilidad. Es habitual clasificarlas en soluciones de nivel 1 o nivel 2 [51]. En el nivel 1 se engloban las soluciones que implican cambios en el funcionamiento de la propia red de *blockchain*, es decir en la red principal o base. En contraste, las soluciones de nivel 2 operan por encima de la red principal, haciéndose cargo de la carga de procesamiento

con otros protocolos de consenso propios y descongestionando la red principal.

Algunas soluciones de nivel 1 son:

- Mejorar el algoritmo de consenso: Aunque el mecanismo de consenso de *Proof of Work* ofrece una gran fiabilidad, se considera un mecanismo lento. Otras alternativas como *Proof of Stake* no requieren mineros que empleen un uso masivo de potencia de cálculo.
- Sharding [53]: Se dividen las transacciones en conjuntos de datos más pequeños (llamados *shards*) y se separa la operación de la *blockchain* en grupos de nodos que procesan *shards* en paralelo, haciendo que se puedan procesar varias transacciones simultáneamente.

Algunas soluciones de nivel 2 son [54]:

- *Rollup*: Las transacciones se realizan en una capa externa fuera de la red principal de *blockchain* y se envían a la red principal como una sola transacción mediante *smart contracts*.
- *Sidechains*: Las *sidechains* son redes independientes, con sus propias reglas y mecanismo de consenso, que están unidas con la red principal mediante *smarts contracts*. El uso de *sidechains* permite implementar mecanismos de consenso que logren una capacidad de procesamiento de transacciones más eficiente. En la Figura 1-15 se ejemplifica el concepto de *sidechains*, éstas se crean sobre la red principal mediante *smart contracts* desplegados en ella. Las *sidechains* implementarán mecanismos de consensos más eficientes, mejorando su escalabilidad.

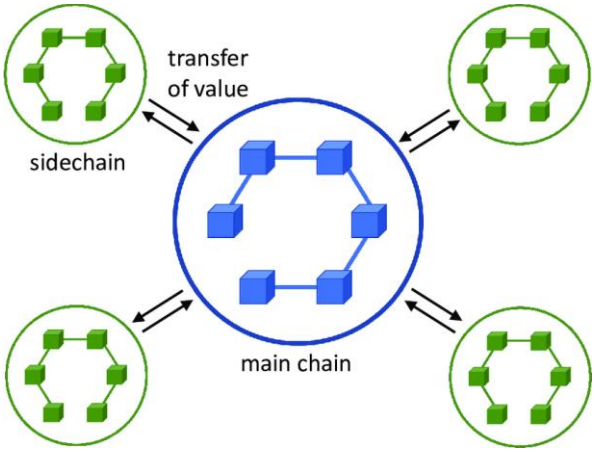


Figura 1-15. Conceptualización *sidechains* creadas sobre una red *blockchain* principal [55]

# 2 *BLOCKCHAIN* EN EL SECTOR ELÉCTRICO

*No es la especie más fuerte ni la más inteligente la que sobrevive, sino la que mejor se adapta a los cambios.*

*- Charles Darwin -*

Los sistemas eléctricos tradicionales se han visto expuestos en los últimos años a grandes cambios, con una masiva incorporación de producción renovable, y con parte de la generación distribuida en pequeñas instalaciones. La nueva generación, fotovoltaica y eólica en su mayor parte, es variable y difícil de predecir. Además, las pequeñas plantas de generación distribuida no están coordinadas por los operadores del sistema, y normalmente son muy pequeñas para participar en los mercados de servicios de ajuste del sistema. Estas nuevas condiciones hacen que sea necesario transformar los sistemas eléctricos para asegurar su estabilidad y seguridad.

Por otro lado, la tendencia hacia la digitalización e incorporación en los sistemas eléctricos de nuevos elementos con capacidades de computación avanzadas introduce el concepto de *smart grid* [56], [57]. Las *smart grids* son redes capaces de monitorizar y controlar de forma dinámica la red, gracias a la incorporación de contadores inteligentes, tecnologías de la información y comunicación y tecnologías de control avanzadas, habilitando flujos de potencia e información bidireccionales en la red.

Debido a la gran cantidad de recursos distribuidos y dispositivos involucrados en una *smart grid*, una solución para mejorar su gestión a gran escala es su integración con la tecnología de internet. De esta forma surge el término de *Internet of Energy* (IoE) o *Smart Grid 2.0* [58]–[60]. IoE, de forma similar al *Internet of Things* (IoT) es una solución basada en conexión de dispositivos a la red internet.

En el contexto de nuevas *smart grids*, se espera que una parte importante de los usuarios finales produzcan su propia energía, se conviertan en prosumidores e incorporen dispositivos de control inteligentes en el lado de la demanda, con sistemas de gestión energética que controlen determinadas cargas y con puntos de carga para vehículo eléctrico. Con los nuevos contadores y dispositivos inteligentes se establecerá un flujo de información bidireccional entre los operadores del sistema y los consumidores. Esto permitirá a los usuarios participar en nuevos programas de respuesta activa de la demanda y en los servicios de complementarios del sistema.

Con el aumento en la conectividad y la cantidad de dispositivos, el reto es integrar y coordinar las nuevas infraestructuras de información, comunicación, control y operación de generadores distribuidos, prosumidores, vehículos eléctricos y en general dispositivos inteligentes de la red. Gestionar estas nuevas redes de una manera centralizada requiere infraestructuras de comunicación e información sofisticadas y costosa. Por eso, la tendencia en las *smart grids* se dirige hacia la descentralización, no solo de la generación sino también de la información, operación y control [61], [62]. Siguiendo esta tendencia hacia la descentralización, surgen nuevas estructuras organizativas orientadas a agrupar consumidores y pequeños generadores, como pueden ser las comunidades energéticas o las microrredes. Sin embargo, la configuración descentralizada de redes inteligentes, con múltiples dispositivos conectados, presenta algunos retos de seguridad, privacidad y confiabilidad que deben ser abordados con tecnologías innovadoras [63]–[65].

La tecnología *blockchain* se presenta como una posible solución a algunos de estos nuevos retos, facilitando transacciones de información descentralizadas donde diversas entidades conectadas a una red pueden crear, mantener y almacenar una red de información encadenada en bloques, sin necesidad de una autoridad central [66]. Las distintas entidades pueden verificar la integridad de la información almacenada en la cadena de bloques, verificando que no ha sido alterada. Este sistema descentralizado hace que los sistemas sean redundantes y resistentes frente a ciberataques y resuelve gran parte de los problemas de un sistema centralizado [67]. Con aplicaciones basadas en *blockchain* se pueden crear mecanismos de incentivos justos, minimizar costes de gestión de datos y regulatorios, aumentar la transparencia y confianza entre entidades, asegurar la privacidad y seguridad, reducir las pérdidas de distribución y mejorar la estabilidad de la red.

Algunas de las características de *blockchain*, que hacen de esta una tecnología interesante para su aplicación en el sector eléctrico son las siguientes:

- **Prescindir de autoridad central**. Mediante el diseño de mecanismos de consenso entre los nodos participantes de la red *blockchain*, se logra que exista confianza en la veracidad de los datos que se incorporan en cada bloque, sin necesidad de involucrar a una tercera parte de confianza.
- **Integridad o inmutabilidad de datos**. Los datos almacenados en una *blockchain* no pueden ser alterados debido a que los datos están enlazados entre sí mediante funciones criptográficas *hash*, que permiten detectar fácilmente si algún dato ha sido modificado.
- **Privacidad de datos**. Mediante el uso de criptográfica asimétrica con pares de claves privada-pública, los datos pueden ser encriptados con seguridad.
- **Transparencia**. En una red *blockchain* todos los nodos participantes tienen acceso a los datos de la cadena de bloques, pudiendo auditar las transacciones y acciones que se realizan.
- **Automatización de procesos** mediante el uso de *smart contracts*, permitiendo el desarrollo de aplicaciones descentralizadas (*DApps*) para funcionalidades avanzadas.

En general, se considera que, para una determinada aplicación, existen varios requisititos básicos que hacen que el uso de *blockchain* sea mejor que otros tipos de tecnologías [45]:

- Existen varias partes involucradas, con distintos objetivos y que no tiene porqué confiar entre sí.
- La naturaleza de la aplicación hace que la operación descentralizada sea más eficiente o conveniente.
- Es necesario mantener un historial de transacciones y datos.
- No es necesaria una gran velocidad en el proceso.

Estos requisitos hacen especialmente interesante el uso de *blockchain* en agrupaciones orientadas a comunidades, ya sea para comerciar de forma local con energía o para implementar sistemas de control o de servicios de respuesta a la demanda. Un ejemplo claro, son las microrredes, conjuntos de cargas y recursos energéticos que forma una red eléctrica propia y que actúan como una sola entidad controlable [68]. Otro tipo de comunidades pueden ser agregaciones de consumidores y prosumidores, agregaciones de generadores formando plantas de generación virtuales (VPP por sus siglas en inglés), infraestructuras de carga de vehículo eléctrico, etc. Otras aplicaciones potencialmente útiles se encuentran en la relación entre los operadores de distribución y los consumidores finales o pequeños generadores, integrándolos en los sistemas de control de la red y permitiendo nuevas aplicaciones relacionadas con la respuesta a la demanda, su participación en servicios complementarios como control de frecuencia y voltaje y en la optimización de la operación.

En los siguientes apartados se recogen potenciales aplicaciones que la tecnología *blockchain* puede tener en los sistemas eléctricos. En estos apartados se exponen los retos que los sistemas eléctricos actuales enfrentan y como *blockchain* puede ayudar a superarlos. Además, se presentan ejemplos prácticos y casos de estudio. Siguiendo la línea de las publicaciones científicas hasta el momento, en este trabajo las aplicaciones de *blockchain* al sector eléctricos se han dividido de las siguientes tres categorías:

- Ciberseguridad
- Mercados eléctricos
- Gestión, operación y control en sistemas eléctricos

## 2.1 Ciberseguridad en sistemas eléctricos

Siguiendo la tendencia de digitalización de los sistemas eléctricos y de su conversión en redes inteligentes, desde las centrales de generación hasta los consumidores finales, incluyendo las redes de transporte y distribución, están cada vez más dotadas con dispositivos inteligentes, soportados por redes de comunicación bidireccionales para su monitorización y control. Esta digitalización es posible gracias al uso masivo de contadores inteligentes, sensores, actuadores y otros objetos inteligentes integrados en entornos de conectividad IoT (*Internet of Things*). El elevado número de dispositivos conectados, abarcando regiones amplias, hace que las redes eléctricas sean cada vez más vulnerables a ciberataques [69].

Las vulnerabilidades en los sistemas eléctricos frente a ciberataques pueden causar grandes perjuicios a la sociedad, con considerables pérdidas económicas. Según un artículo basado en datos de ciberataques reportados en Estados Unidos a infraestructuras consideradas críticas, el sector eléctrico es principal objetivo, con un 54% de los ataques (Figura 2-1) [70].

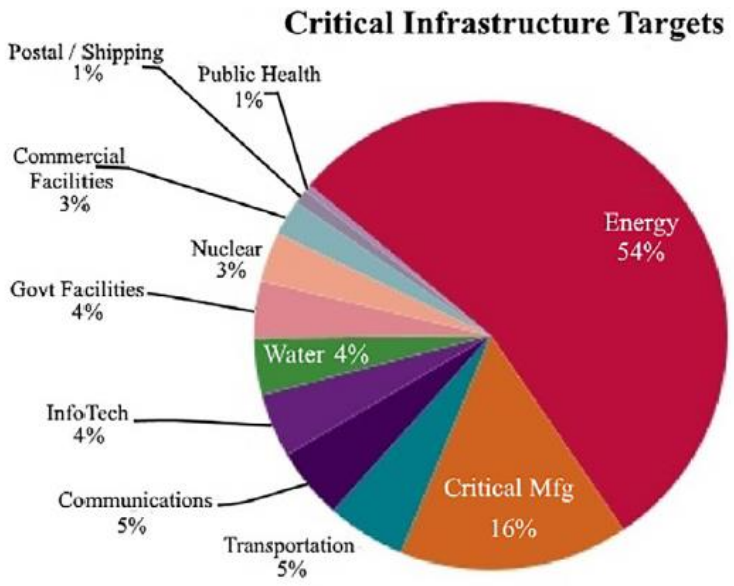


Figura 2-1. Porcentaje de ciberataques a infraestructuras críticas por sectores en EE. UU. [70]

Para lograr una comunicación eficiente y confiable entre los distintos componentes distribuidos en las *smart grids*, se desarrollan redes de comunicación compuestas por diferentes capas: red de área domestica (HAN), red de área vecinal (NAN), red de sensores (SN), red de área ampliada (WAN) y la red principal. Las redes HAN y NAN se forman mediante la interconexión de infraestructuras avanzadas de medición (AMI) mediante protocolo ZigBee/Z-Wave y estándares de IEEE. Dentro de la red WAN, las terminales remotas (RTU), los sistemas de monitorización de área amplia (WAMS) y los dispositivos electrónicos inteligentes (IED) se agrupan primero mediante la red de sensores (SN) y después se comunican con los SCADA y los centros de datos mediante protocolos como DNP3, Modbus o IEC-60870. Alcanzado este punto, la información se transfiere a la red principal donde es usada por diversidad autoridades de control. En la red principal, los protocolos más comunes son TCP/IP, WiMAX y GPRS. Además, en lado de los consumidores también se están incorporando sistemas de monitorización y control avanzados, creando hogares inteligentes. Para facilitar la comunicación, lo habitual es que estos protocolos de comunicación se diseñen para transmitir datos brutos, sin encriptación ni restricciones de autentificación. Por esto, las redes eléctricas inteligentes presentan vulnerabilidades frente a ciberataques [71].

Los problemas de ciberseguridad más importantes en redes inteligentes pueden resumirse en cuatro aspectos [71]:

- Integridad
- Confidencialidad
- Disponibilidad

- Imposibilidad de rechazo

El ataque a la **integridad** consiste en la modificación, alteración o destrucción no autorizada y furtiva de datos de mediciones del sistema eléctrico. El ataque de inyección de datos falsos (FDI) es un ejemplo típico de ataque a la integridad que puede poner en peligro los datos de mediciones de campo, alterando los resultados en los sistemas eléctricos y causando decisiones erróneas en los centros de control [72].

El ataque de **confidencialidad** se centra en el acceso o difusión de información privada por parte de individuos o entidades no autorizados. Los contadores inteligentes son una de las principales fuentes de este tipo de vulnerabilidad. Los atacantes puedes aprovechar esta vulnerabilidad para acceder a los datos de consumo eléctrico de los usuarios, comprometiendo su privacidad [73].

La **disponibilidad** de los datos, que permite un acceso confiable, es importante para el funcionamiento de las redes eléctricas. Mediante la interrupción de la transferencia oportuna de datos, los ciberataques pueden corromper o bloquear señales de monitorización y control causando graves impactos en la estabilidad, eficiencia y seguridad de los sistemas eléctricos [74].

La **imposibilidad de rechazo** significa que las acciones realizadas por los participantes no pueden ser negadas a posteriori. Por ejemplo, los ciberataques contra la imposibilidad de rechazo son especialmente relevantes en los mercados locales de electricidad. Por esto, es necesario que las redes de comunicación en los sistemas eléctricos sean auditables para que sea posible reconstruir el historial completo de información a partir de históricos de forma confiable [74].

En las redes habitualmente se utilizan diferentes tecnologías de ciberseguridad, como *firewalls* y sistemas de encriptación y autentificación. Sin embargo, los requisitos de comunicación en tiempo real y operación continua de las redes inteligentes hacen que estas técnicas no se adapten correctamente. Por otro lado, los sistemas eléctricos están formados cada vez por generación y sistemas de control distribuidos, sin embargo, las redes de comunicación siguen organizándose de manera centralizada. Esto hace a las redes vulnerables a ataques de punto único de fallo, es decir el fallo o vulneración de un solo elemento puede tener un impacto significativo en la operación segura del sistema [71].

Gracias a las características de *blockchain*, su implementación puede ser utilizada para abordar algunos de los problemas de ciberseguridad expuestos anteriormente. Los datos de medidas y transacciones locales pueden ser transferidos de manera P2P dentro de las redes. Estos datos se almacenan de forma distribuida en varios dispositivos en lugar de en único centro de datos [75]. De esta forma se evita la vulnerabilidad de punto único de fallo y se garantiza una alta disponibilidad de datos. También, debido a la verificación continua por parte de los nodos de la *blockchain*, la información es casi inmutable, protegiendo la integridad, confidencialidad y disponibilidad de los datos en las redes inteligentes. Es decir, una vez que la información se incorpora a la *blockchain* no puede ser manipulada. Esta propiedad de *blockchain* dota de una alta auditabilidad a las redes eléctricas con comunicaciones basadas en *blockchain* y hace que los ataques contra la imposibilidad de rechazo sean improbables. La criptografía asimétrica utilizada en *blockchain* permite aumentar los niveles de seguridad de autentificación y autorización, especialmente en infraestructuras avanzadas de contadores inteligentes (AMI), protegiendo la privacidad de los usuarios y la integridad de la información [76]. Por último, los *smart contracts* y las aplicaciones descentralizadas (*DApps*) basadas en *blockchain*, son la base para crear entornos de desarrollo ciberseguros sobre los que crear aplicaciones avanzadas para redes inteligentes. Estos entornos seguros son la base para algunas de las aplicaciones que se recogerán en los siguientes apartados y hacen que el uso de *blockchain*, en lugar de otros enfoques más tradicionales, tenga sentido.

En la Figura 2-2 se muestra un ejemplo de arquitectura de *smart grid* basada en *blockchain*, compuesta por varias capas con comunicaciones bidireccionales [71]. La arquitectura está dividida en cuatro redes: red principal (*core network*), WAN (*wide area network*), NAN (*neighborhood area network*), SN (*sensor network*) y HAN (*home area network*).

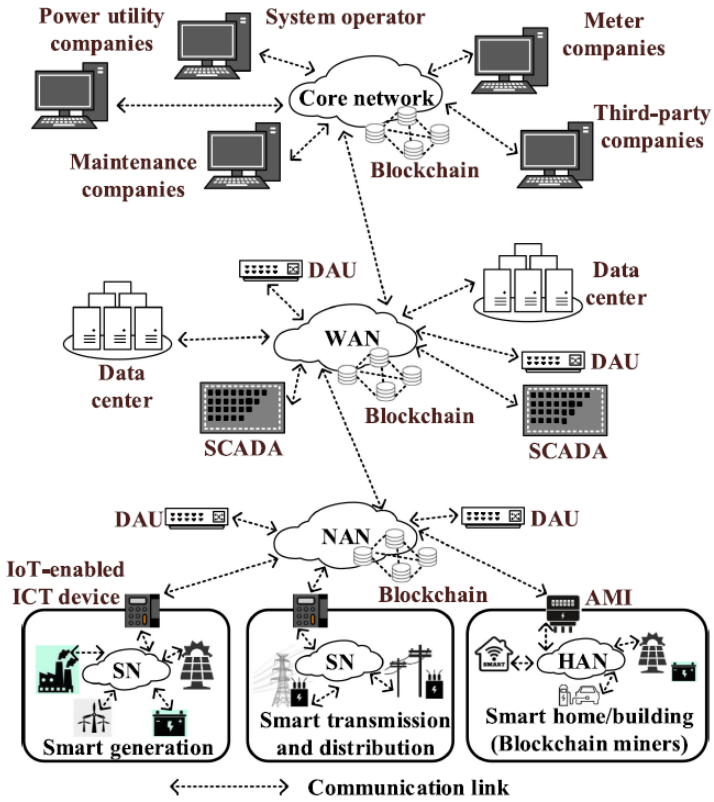


Figura 2-2. Arquitectura de comunicaciones de una *smart grid* basada en *blockchain* [71]

La red principal es utilizada por las autoridades de control como compañías eléctricas, operadores del sistema, etc. Los usuarios de la red principal tienen acceso a monitorización y a pasar instrucciones a las redes SN y HAN. Se pueden utilizar varias redes *blockchain* para diferentes actividades, como mercados mayoristas o para monitorización en sistema de gestión de la energía.

La capa WAN hace de intermediaria entre la capa principal y NAN. Igualmente, pueden implementarse diversas *blockchain* para aplicaciones específicas como agregación de mediciones de campo o almacenamiento.

En las capas NAN y HAN, los consumidores y generadores locales están directamente conectados entre sí, y *blockchain* se utiliza para facilitar aplicaciones como el comercio de energía local. La mayor parte de las aplicaciones de *blockchain* en *smart grids* propuestas en la literatura se desarrollan en el entorno de las capas NAN y HAN. Tiene como objetivo integrar los nuevos dispositivos inteligentes instalados como contadores o sistemas de gestión energética del hogar (HEMS) e incrementar la participación de los usuarios finales en la operación de las *smart grids*. Así, pueden desarrollarse de forma segura y eficiente esquemas de respuesta a la demanda o facilitarse la implementación de microrredes, por ejemplo.

El flujo de datos a través de estas redes se publica en su correspondiente *blockchain* y esta información es verificada por todos los nodos y dada por válida mediante el mecanismo de consenso correspondiente.

Los productores y consumidores conectadores a redes HAN pueden ser utilizados como nodos que aporten capacidad de cómputo y actúen como mineros que soporten el mecanismo de consenso cuando la *blockchain* implementada sea de tipo público [77]. Para *blockchains* de tipo consorcio o privadas, los nodos de confianza que participan en los mecanismos de consensos normalmente son elegidos y autorizados por autoridades de control como operadores de sistema.

En las *smart grids*, la generación, transporte, distribución y los consumidores son monitorizados y controlados por dispositivos e infraestructuras de información y comunicación de tipo IoT, tales como RTU (*remote terminal unit*), IED (*intelligent electronic device*) y WAM (*wide area monitoring*) para la operación de los sistemas y AMI (*advanced metering infrastructure*) para hogares y edificios. Mediante la incorporación de *blockchain* con *smart contracts* en las comunicaciones de estos dispositivos IoT conectados en WAN, NAN y

SN/HAN la información de campo puede ser asegurada y recolectada de forma automática. Además, mediante el uso de aplicaciones descentralizadas (*DApps*) sobre las infraestructuras de medición basadas en *blockchain* pueden desarrollarse sistemas de respuesta a la demanda descentralizados, gestión local y comercio de energía, todo dentro de un ambiente seguro.

La información de campo puede ser recolectada por agregadores basados en *blockchain* en las capas WAN y NAN. La ventaja de utilizar *blockchain* para esta agregación es la mejora en la protección de la confidencialidad de los datos en las *smart grids*. Además, la recolección de datos puede ser procesada y almacenada de forma automática mediante *smart contracts* y *DApps*, donde *blockchain* puede asegurar la integridad y auditabilidad de los datos.

Para la operación de sistemas, mediante el uso de *smart contracts* y *DApps* las decisiones de operación puede realizarse automáticamente con menor intervención humana, reduciendo el riesgo de ciberataques debidos a errores humanos. También, el historial de decisiones almacenado en la *blockchain* facilita la auditabilidad de estas.

A continuación, se recogen algunas aplicaciones de *blockchain* en el ámbito de la ciberseguridad de sistemas eléctricos [71]:

- **Prevención frente a ataques de inyección de datos falsos (FDI)**: FDI es un tipo de ataque contra la integridad de los datos, manipulando furtivamente los datos recolectados de los dispositivos de campo sin ser detectados por los sistemas de detección de *bad data*. Este tipo de ataques incluye la alteración de datos de mediciones para fines fraudulentos, alteración maliciosa de transacciones de energía para desestabilizar la red y el control sin autorización de dispositivos IED críticos. *Blockchain* puede proporcionar una protección más eficiente contra este tipo de ataque.
- **Protección de confidencialidad e integridad de datos de consumidores:** Mediante el uso de contadores inteligentes y la criptografía de clave asimétrica de *blockchain*, la información de los consumidores puede ser encriptada para proteger su privacidad y para verificar que la información no ha sido modificada. Un ejemplo simple, tal y como se muestra en la Figura 2-3, el contador inteligente de un consumidor puede utilizar la clave pública de una determinada compañía eléctrica para encriptar sus datos de consumo, de esta forma, sólo la compañía eléctrica puede desencriptar los datos utilizando su clave privada, que nadie más conoce. Además, la clave privada del contador inteligente del consumidor puede utilizarse para firmar los datos de consumo, pudiendo la compañía eléctrica verificar la integridad de los datos mediante la clave pública del consumidor.

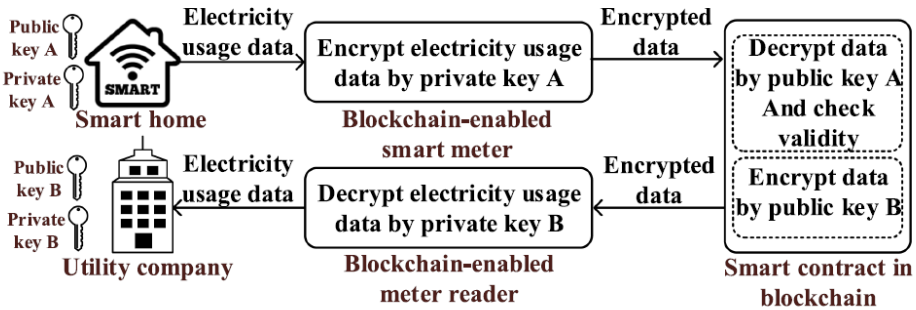


Figura 2-3. Sistema de medición de consumo eléctrico basado en *blockchain* [71]

- **Implementación de estructuras de control descentralizadas más seguras.** La gestión de un gran número de generadores distribuidos y consumidores con objetos inteligentes siguiendo una estructura convencional centralizada hace que las compañías eléctricas se enfrenten a costes elevados para mantener la ciberseguridad y las infraestructuras de comunicación y control de estos sistemas. Además, este tipo de estructuras centralizadas expone los sistemas de control a la vulnerabilidad del punto único de fallo, es decir, si el sistema central falla, el sistema completo quedará inoperativo. Un ejemplo claro de la tendencia hacia la descentralización en la operación y control de redes eléctricas es la proliferación de microrredes cuyos sistemas de control pueden implementar *blockchain* para mejorar su eficiencia y seguridad. El uso de *blockchain* en estos sistemas permite que los datos de mediciones y transacciones puedan ser almacenados de forma fiable y segura sin necesidad de una autoridad central. Protegiendo la integridad y confidencialidad

de los datos. Además, mediante el uso de *smart contracts* pueden implementarse sistemas de control automáticos y algoritmos de optimización para efectuar, por ejemplo, despacho económico.

- **Protección frente a otros ataques contra la integridad de datos.** Algunos de los ataques contra la integridad de datos en sistemas eléctricos pueden ser *DDoS* (ataque distribuido de denegación de servicio) o ataques de cibertopología.

## 2.2 Mercados eléctricos

El funcionamiento de los mercados eléctricos ha experimentado un gran cambio durante los últimos años, pasando de un modelo verticalmente integrado a un modelo más horizontal donde las actividades de comercialización y generación están liberalizadas. En Europa, el proceso de creación de mercados eléctricos comenzó con la primera directiva sobre normas comunes para el mercado de la electricidad (Directiva 1996/92/CE), transpuesta a la legislación española con la Ley 54/1997. Con estas y sucesivas reformas se pasa de un modelo fuertemente regulado por el Estado, a un modelo liberalizado donde existen numerosos agentes que participan en él [78]. Algunos de estos agentes son:

- Productores
- Consumidores y prosumidores
- Comercializadores
- *Traders*
- Operadores del Mercado
- Operadores del Sistema
- Organismos reguladores
- Diversas entidades de carácter financiero como cámaras de compensación (*clearinghouses*) o *brokers*

En los mercados eléctricos existen distintos tipos de operaciones entre productores, comercializadores, consumidores y resto de agentes. Los mercados a futuros cubren acuerdos a largo plazo de venta de energía, desde meses hasta años. Estos acuerdos también pueden producirse entre partes de forma bilateral, como los PPA (*Power Purchase Agreement*). Las transacciones a largo plazo pueden ser de tipo físico o financiero, en las primeras existe una obligación de entrega física de energía mientras que en los segundos sólo se produce una liquidación financiera entre las partes. También existen mercados diarios donde la energía se negocia con un día de antelación, y mercados intradiarios donde se negocia la energía el mismo día. Por último, en el muy corto plazo se producen transacciones para mantener equilibrada la oferta y la demanda, estos servicios son ofertados por el Operador del Sistema, junto con otros servicios auxiliares como regulación de voltaje y frecuencia.

Debido al elevado número de operaciones de distinto tipo, los mercados eléctricos funcionan mediante procesos complejos que requieren la intervención de numerosos agentes intermediarios. Con el uso de *blockchain* y *smart contracts*, la eficiencia de estos procesos puede mejorarse y la intervención de algunos agentes intermediarios podría limitarse o eliminarse. La reducción de costes asociados también permitiría que pequeños generadores, que actualmente están prácticamente excluidos del mercado, puedan participar en él.

En el marco de las nuevas redes inteligentes y de la presencia cada vez mayor de generación distribuida, *blockchain* puede servir de soporte en algunas propuestas de organización de nuevos mercados eléctricos que se están planteando actualmente en la industria. Estos nuevos planteamientos dividen el mercado en distintos niveles [79]:

- Mercados financieros. Este tipo de mercados permite a los participantes acotar los riesgos debidos a la fluctuación del precio en los mercados.
- Mercados mayoristas. Son mercados ya establecidos en la mayoría de los sistemas eléctricos.
- Mercados a nivel de redes de distribución. Aunque este tipo de mercados no son aún una realidad, están siendo objeto de debate y se está explorando su regulación en países de Europa y Estados Unidos, entre otros. El papel de los Operadores de Distribución está tomando mayor relevancia debido a la mayor complejidad y carácter dinámico de estas redes, que incluyen generación distribuida, almacenamiento, vehículos eléctricos, microrredes, etc. El objetivo de los mercados a

este nivel sería gestionar y optimizar la operación de los sistemas, manteniendo de forma efectiva una operación segura y confiable.

- Mercados a nivel local. El desarrollo de mercados locales también es actualmente objeto de debate en el sector eléctrico. Este tipo de mercados pretende involucrar a pequeños productores y prosumidores, dando también soluciones a problemas sin necesidad de implicar niveles mayoristas o incluso de distribución. Dentro de este tipo de mercados tienen cabida los mercados a nivel de microrredes y otras comunidades energéticas.

La aplicación de *blockchain* en mercados eléctricos que por su naturaleza distribuida probablemente tiene mayor potencial es el comercio de electricidad directamente entre entidades o comercio P2P (*peer-to-peer*), normalmente orientados a mercados locales y comunidades. Por esto, un parte importante de las iniciativas relacionadas con *blockchain* en el sector eléctrico están relacionadas con comercio y mercados eléctricos, y dentro de estos, con transacciones tipo P2P [80].

### 2.2.1 Mercados mayoristas

Los mercados mayoristas de energía eléctrica están formados por múltiples agentes que generan una gran cantidad de transacciones y procesos, actuando muchos de estos agentes como intermediaros o terceras partes. Estos procesos implican comunicaciones a través de distintos canales y procesado de información de forma manual. Tal y como se muestra en la Figura 2-4, cuando se efectúa una transacción entre dos compañías, existen varias interacciones que implican diversos canales, sistemas y procesos. Debido a que la información debe ser compartida y validada en varias ocasiones y por distintas partes, los procesos suelen ser lentos y costosos [81].

A diferencia de modelos de mercado orientados al comercio dentro de comunidades o entre usuarios directamente, donde *blockchain* propone soluciones a nuevos modelos que surgen dentro del contexto de las *smart grids*, en el mercado mayorista *blockchain* puede ayudar a mejorar la eficiencia de los procesos existentes sin que existan modificaciones importantes en el funcionamiento actual de estos mercados. Estas mejoras también estimularían la integración de pequeños generadores y prosumidores en el mercado mayorista.

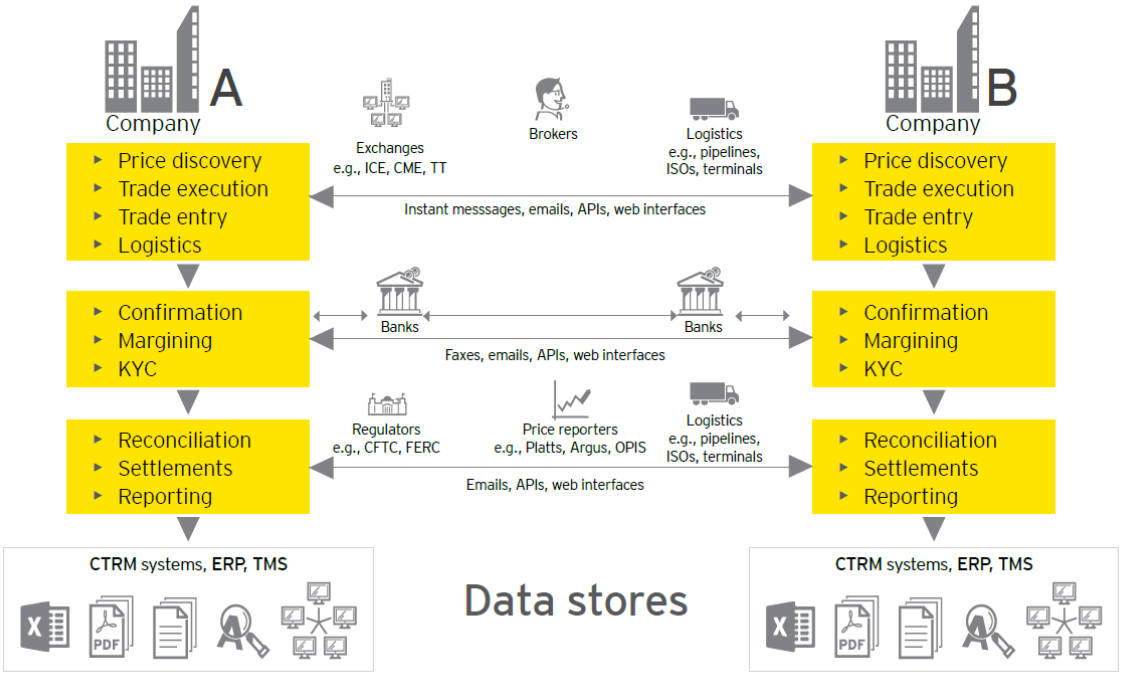


Figura 2-4. Ciclo de una transacción entre compañías en un mercado eléctrico mayorista [81]

Una de las primeras publicaciones donde se hace referencia a las potenciales aplicaciones de *blockchain* al

mercado eléctrico mayorista es el capítulo *Potential of the Blockchain Technology in Energy Trading* del libro *Blockchain technology Introduction for business and IT managers*, publicado en 2016 [82]. En él se proponen varios escenarios de integración de la tecnología *blockchain* en los mercados mayoristas de electricidad:

- ***Blockchain* como canal de comunicación**

En este escenario, el objetivo es respaldar los procesos actuales sin cambiarlos. Es decir, el funcionamiento del mercado y los agentes que intervienen en él se mantienen, pero la forma en que se intercambia la información es sustituida o mejorada mediante el uso de una red *blockchain*.

Los participantes del mercado gestionan un nodo de la red *blockchain*, que debe ser de tipo *permissioned* y privada, es decir, solo los participantes autorizados tienen acceso de lectura y escritura.

Mientras que actualmente los procesos tienen lugar a nivel de aplicación, interactuando las partes directamente entre sí, con *blockchain* cada parte interactúa con la *blockchain* común. Para ello, se usa un adaptador de interfaces que mapea estados y datos en la red *blockchain*. Este adaptador soporta una interfaz técnica hacia el lado de la *blockchain* y una interfaz funcional hacia el lado de la aplicación.

*Blockchain* es usado meramente como un vehículo para distribuir la información. Es decir, los generadores, comercializadores, reguladores, operadores del mercado y el sistema y otras terceras partes, dejan de comunicarse directamente entre sí y lo hacen a través de la red *blockchain*. En este caso, *blockchain* funciona sólo como una base de datos compartida.

Un efecto inmediato de esta aplicación es la estandarización. Sólo debe existir una red *blockchain* en un determinado sistema y todos los participantes deben escribir y leer datos en el mismo formato.

De esta forma, por ejemplo, un Operador del Mercado que necesita enviar un programa al Operador del Sistema, podría escribirla en la *blockchain* y el Operador del Sistema podría leerla. Los Reguladores también pueden ser usuarios de la *blockchain*, y recibir información sobre las transacciones en tiempo real leyendo directamente de la *blockchain*. De esta forma las partes que están obligadas a reportar información sobre las transacciones a los Reguladores no tendrían que hacer un esfuerzo adicional.

- ***Blockchain* para mejorar el proceso de liquidación física (en inglés *physical settlement*)**

Este escenario se puede considerar una aplicación directa de la propuesta anterior a uno de los procesos que quizás más recursos informáticos consume, la liquidación o entrega física de la energía eléctrica. Al igual que en el caso anterior, en esta propuesta de uso de *blockchain*, el funcionamiento y procesos del mercado actual no varía.

Tomando como ejemplo el caso del sistema español, tal y como se recoge en el procedimiento operativo *P.O. 3.1 Proceso de programación,* publicado por REE (Operador del Sistema en España), este proceso implica una cantidad ingente de comunicaciones entre REE, el Operador del Mercado, los Participantes del Mercado, proveedores de servicios de balance, etc.

En primer lugar, REE debe comunicar una serie de informaciones a los participantes del mercado (previsión de demanda, situación prevista de la red de transporte, previsión de capacidad de interconexiones internacionales, etc). A su vez, para elaborar el Programa Diario de Base de Funcionamiento (PDBF) el Operador del Mercado debe comunicarle el resultado de la casación de ofertas en el mercado diario, junto con la nominación de los contratos bilaterales con entrega física que debe ser comunicada por los sujetos vendedores y compradores. Sobre el PDBF, utilizando las programaciones de cada una de las unidades de programación y aplicando restricciones técnicas de la red, REE elabora el PDVP (Programa Diario Viable Provisional). Tras el resultado del mercado intradiario elabora y difunde a los participantes del mercado los Programas Finales (PHF y PHFC) y los Programas Operativos (P48 y P48CIERRE). Además, REE debe gestionar los servicios de balance del sistema, comunicaciones de desvíos e indisponibilidades, la Subasta Diaria de Respaldo (SDR), regulación secundaria y terciaria, programas de intercambio internacionales, etc.

Actualmente los intercambios de información, tal y como se recoge en el *P.O. 9.1 Intercambios de información relativos al proceso de programación* [83], se hacen a través de los Sistemas de Información del Operador del Sistema (SIOS). Para ello, se hace uso de medios de comunicación electrónicos convencionales, implementando canales cifrados y uso de certificados digitales para garantizar la seguridad.

Con la implementación de *blockchain*, las comunicaciones necesarias para completar el proceso de

programación pueden simplificarse, además con *smart contract* algunos procesos pueden automatizarse, mejorando la eficiencia, ahorrando recursos y aumentando su seguridad.

- ***Blockchain* para mejorar el proceso de liquidación financiera (en inglés *financial settlement*)**

En este escenario se propone integrar soluciones de *blockchain* a las transacciones financieras que se realizan en el mercado. Esto podría lograrse mediante el desarrollo de una criptomoneda exclusiva para el intercambio de energía eléctrica o mediante un sistema de contabilidad que implícitamente lleve asociado un cobro a una transacción de energía.

Una de las consecuencias que tendría este sistema sería un cambio en el rol que actualmente tienen las Entidades de Contraparte Centrales (CCP por sus siglas en inglés). Las CCP son las entidades encargadas de intermediar entre compradores y vendedores en los mercados, se hacen cargo de centralizar los pagos tomando como base el resultado físico del mercado. También actúan como avalistas en caso de que algún participante falle en su obligación de pago, socializando las perdidas entre el resto de las participantes.

Con la introducción de *blockchain* para los pagos, ambas partes tienen la certeza de que su contraparte será capaz de cumplir los términos de la transacción. De esta forma, no sería necesaria la intervención de una CCP, especialmente en los mercados SPOT, donde las transacciones realizadas son a corto plazo o tiempo real.

- ***Blockchain* para comercio P2P**

En el escenario anterior se ha expuesto como el uso de *blockchain* puede suponer la eliminación de los intermediarios financieros del mercado (CCP). Dando un paso más, este escenario propone el comercio sin necesidad de un mercado centralizado y gestionado por una entidad central, tal y como lo conocemos. En este mercado, los participantes realizan sus operaciones interactuando directamente con la *blockchain*. De forma similar a los mercados tradicionales, un mercado P2P también debe incorporar en su diseño mecanismos propios de mercado: establecer reglas de fijación de precios, restricciones técnicas, como se efectuarán los pagos, etc.

La arquitectura de un prototipo de mercado P2P descentralizado sería la siguiente (Figura 2-5):

- En la base del desarrollo, *blockchain* da soporte como registro distribuido para realizar las transacciones (órdenes de venta, compra, pagos, etc).
- Comunicación *peer-to-peer* para sincronizar los nodos de la red.
- Adaptador. Es una interfaz que permite unir la capa de interfaz de programación de aplicaciones (API) técnica, genérica de la *blockchain* (utilizada para interactuar con la *blockchain*), con la capa API funcional sobre la que los participantes del mercado desarrollaran sus aplicaciones.
- Aplicaciones funcionales de los participantes del mercado, son aplicaciones con interfaz de usuario propia de cada cliente, utilizadas para el comercio de energía y gestión del riesgo (ETRM por sus siglas en inglés *Energy Trading and Risk Management*).

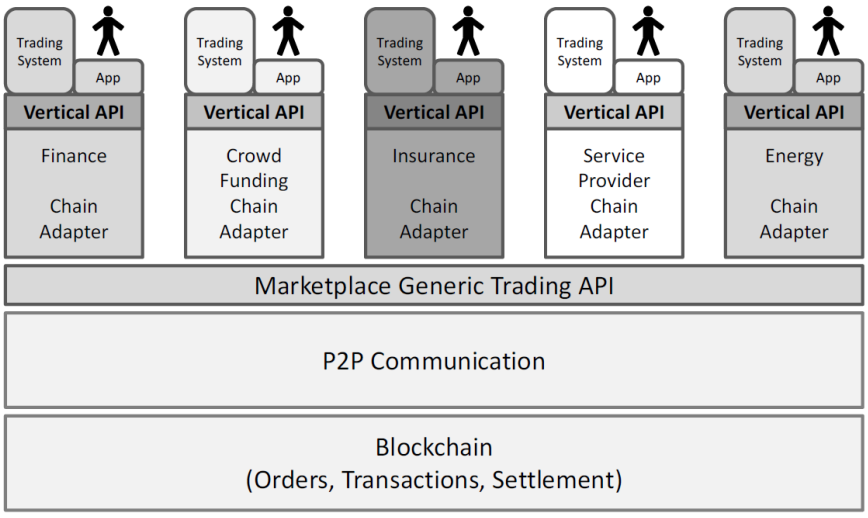


Figura 2-5. Arquitectura tipo de un mercado mayorista tipo P2P con *blockchain* [82]

- ***Blockchain* completamente integrada en un mercado eléctrico**

En este escenario se plantea una red unificada y con una infraestructura que permita el comercio a nivel de continente. Los participantes de esta red son plantas generadoras (incluyendo grandes centrales convencionales y pequeños generadores distribuidos), proveedores de almacenamiento eléctrico y prosumidores.

Como se observa en la Figura 2-6, se propone la existencia de un mercado formado por varios mercados inteligentes locales, junto con un mercado mayorista. En los mercados locales los participantes intercambian energía dentro de una misma zona de distribución (bajo la supervisión de un mismo Operador del Sistema de Distribución (DSO por sus siglas en inglés). Estos mercados locales están completamente automatizados y el comercio se hace a corto plazo. Además, también participan agentes transregionales que compran y venden energía entre regiones ya que la generación y demanda puede variar significativamente entre regiones.

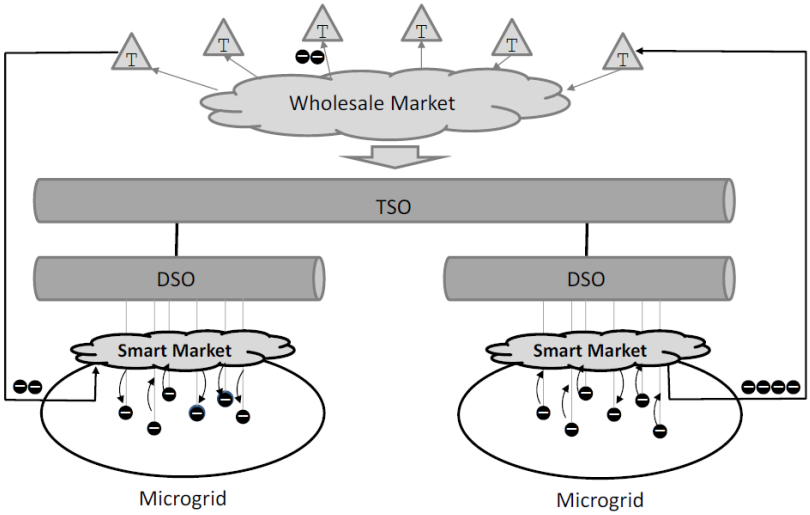


Figura 2-6. Mercados inteligentes locales a nivel de distribución integrados en mercados mayoristas [84]

Para incentivar que la producción de energía sea usada de forma local, se puede establecer un sistema dinámico de pago de tasas por uso de la red. El Operador del Sistema aplicará unos precios por kWh a cada transacción en función de si el intercambio se hace en la red local de baja tensión, la red local de media tensión o si se hace fuera de las fronteras de distribución local.

Los prosumidores participarán en el mercado a través de algoritmos de control que decidirán en cada momento si almacenan la energía generada o si la vierten a la red. El algoritmo tomará esta decisión en base a un objetivo de optimización en función de las condiciones de cada momento (precio de mercado, consumo actual, etc). En caso de vertido a la red, se enviará una oferta automática al mercado local.

La separación del mercado en mercados regionales dará lugar a la formación de precios zonales donde los precios entre regiones pueden ser diferentes. Esto, junto con las tasas aplicadas por uso de la red, incentivará la inversión en generadores en zonas donde el consumo y el precio sean mayores.

Por último, también se propone el uso de una criptomoneda que sería usada por todos los participantes del mercado. Todas las personas que deseen comprar electricidad deberán poseer esta criptomoneda. La criptomoneda tendría un valor ligado al valor de monedas de curso legal (como el Euro), para evitar la volatilidad de su precio.

Existen varios informes de consultorías que esbozan mercados basados en *blockchain* similares al expuesto en el escenario anterior [85] [86]. En la Figura 2-7 se muestra la transformación de un mercado actual a uno basado en *blockchain*. El uso de *blockchain* y *smart contracts* permitiría el comercio directo entre generadores y comercializadores o consumidores, eliminando entidades centralizadas. Un agente puede buscar la oferta del mercado que mejor satisface la previsión de demanda de un consumidor para un periodo concreto y llegar a un acuerdo. Este acuerdo es almacenado de forma segura en la *blockchain* y es automáticamente ejecutado cuando llega el momento específico de la entrega de energía. Los pagos se ejecutarán de manera automática, tal y como esté especificado en el acuerdo. La información de la transacción será accesible para todas las

partes a través de un punto de acceso a la *blockchain*, incluyendo Operadores del Sistema y Reguladores.

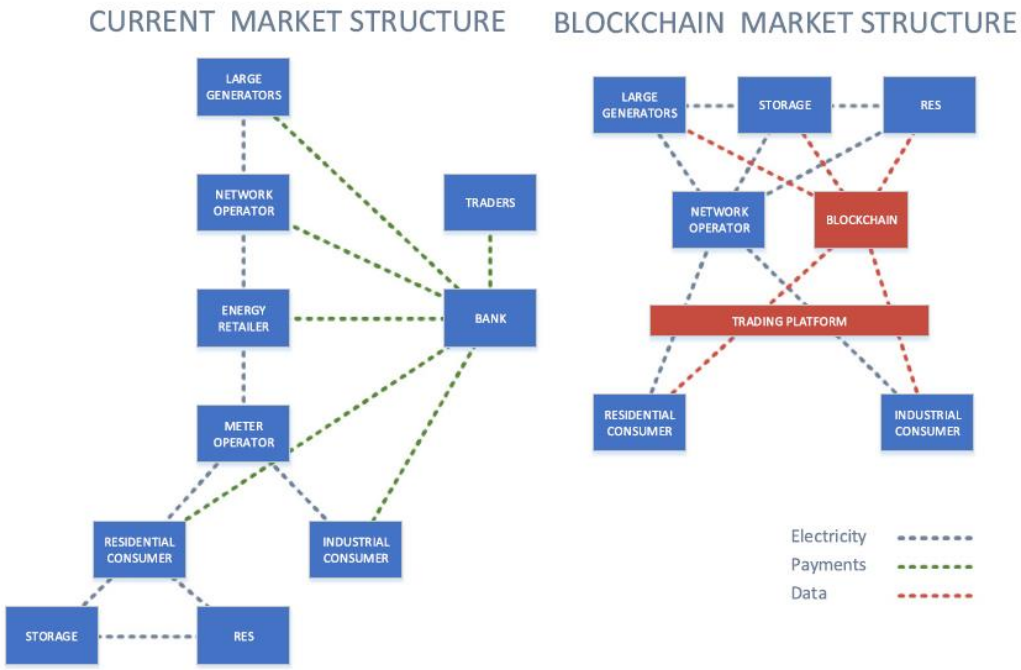


Figura 2-7. Transformación de un mercado eléctrico mayorista con *blockchain* [66]

Sin embargo, aunque varias publicaciones y propuestas plantean un mercado como el expuesto en las líneas anteriores, actualmente existen diversas limitaciones técnicas y regulatorias [66]:

- Por un lado, el número de transacciones que se pueden realizar en una *blockchain* es habitualmente inferior a los sistemas tradicionales, especialmente cuando se usa *Proof of Work* como algoritmo de consenso. Esta limitación de escalabilidad ha sido tratada en el Apartado 2.10 de este trabajo, junto con posibles propuestas de solución.
- Por otro lado, la estructura del mercado actual y su funcionamiento sufriría un cambio radical. Esto implicaría fuertes cambios regulatorios y la adaptación de todos los sujetos del mercado actuales. Por esto, algunas propuestas de *blockchain* en mercados mayoristas se centran en partes específicas del mismo, tratando de implementar soluciones más inmediatas. Algunos ejemplos pueden ser: la gestión de liquidación de desvíos (*imbalance settlement*) o sistemas de comercio P2P para contratos OTC (*over the counter*).

#### 2.2.1.1 Caso de estudio: Enerchain

Enerchain [84] es un proyecto desarrollado con el objetivo de crear una infraestructura técnica que permita a sus participantes operar en mercados mayoristas de energía (electricidad y gas) de una forma descentralizada con tecnología *blockchain*. Inicialmente fue desarrollada por la empresa PONTON y actualmente el proyecto está auspiciado por un consorcio de empresas europeas del sector energético (entre ellas varias españolas como Endesa, Iberdrola o Repsol).

Enerchain desarrolló una prueba de concepto (PoC por sus siglas en inglés) entre mediados de 2017 y mediados de 2018, difundiendo las conclusiones en un informe público [84]. El PoC abarcó el desarrollo de una infraestructura de software basada en *blockchain*, de una interfaz de usuario de referencia y una API abierta que permite a los participantes operar en la plataforma. También se han llevado a cabo pruebas funcionales con las empresas que forman el consorcio, probando el desempeño de la plataforma. Estas pruebas consistieron en varias transferencias reales entre participantes, en primer lugar, albergando la red *blockchain* en servidores externos y después desplegando los propios participantes la red *blockchain* en sus sistemas. Estas transacciones fueron nominadas y reportadas a los organismos que correspondía en cada caso. Como ejemplo, Endesa y Gas Natural Fenosa realizaron una transacción de 5,95 GWh, en este caso de gas natural [87].

Durante el PoC los productos implementados en Enerchain fueron: Transacciones intradiarias cuartohorarias y horarias, diarias con un día de adelanto, mensuales, cuatrimestrales y anuales. Soportando entrega física de la

energía, para gas y electricidad, abarcando toda la zona europea.

Los participantes pueden operar utilizando la interfaz de usuario de referencia o implementar desarrollos propios o incluso de terceros utilizando la API abierta de Enerchain.

Desde el punto de vista regulatorio, Enerchain tiene la consideración de infraestructura de comunicación usada para intercambiar mensajes *peer-to-peer*. Es decir, no está sujeta a la directiva europea MiFID (*Markets in Financial Instruments Directive*) al no considerarse un producto tipo MTF (*Multilateral Trading Facility*) o OTF (*Organised Trading Facility*). Las transferencias realizadas en Enerchain, deben ser notificadas por los participantes a ACER (*Agency for the Cooperation of Energy Regulators*) siguiendo la regulación europea REMIT (*Regulation on Wholesale Energy Market Integrity and Transparency*).

Enerchain utiliza Tendermint [88] como base para construir su *blockchain*, un software de código abierto utilizado para el lanzamiento de *blockchains*. Terdermint utiliza como mecanismo de consenso PBFT (*Practical Byzantine Fault Tolerance*), permitiendo el consenso entre nodos de forma mucho más ágil y eficiente que el mecanismo *Proof of Work*. Esto permite la creación de nuevos bloques de forma rápida, por debajo del segundo, lográndose velocidades de transferencia notables. Así, la ejecución de operaciones puede realizarse casi en tiempo real, haciendo posible su uso para aplicaciones de mercado.

La arquitectura de software de Enerchain, tal y como se muestra en la Figura 2-8, está compuesta por una parte de almacenamiento y otra de aplicación. A su vez, la primera está formada por nodos que forman la red descentralizada y participan en los procesos de *blockchain*, y adaptadores de nodos. La segunda por adaptadores de cliente y aplicaciones de cliente.

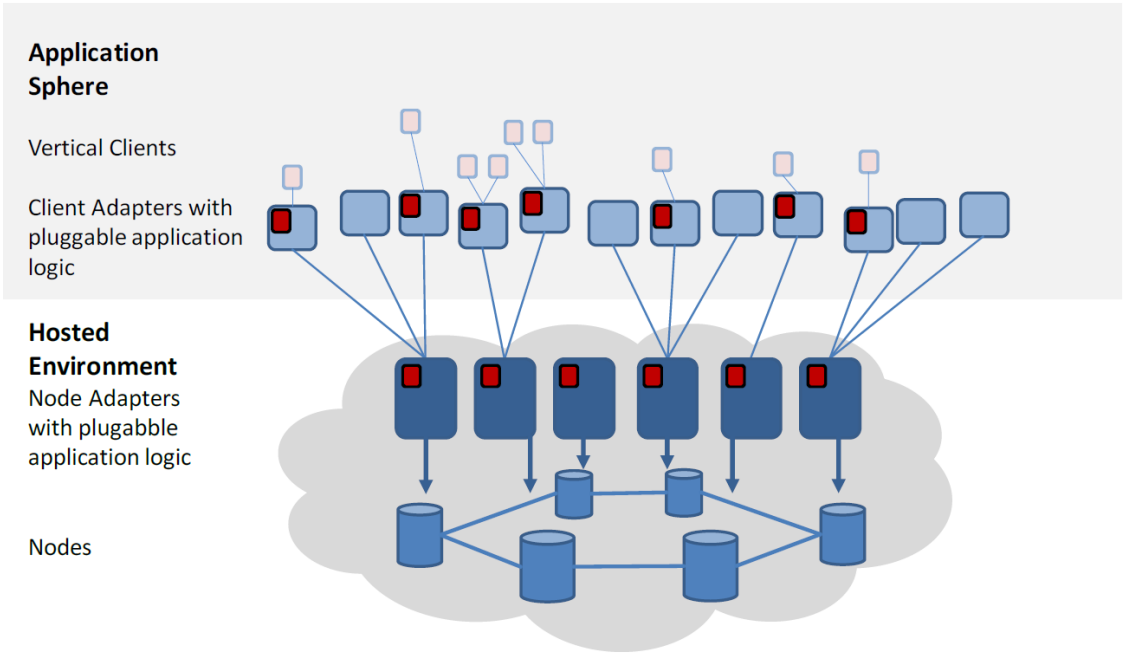


Figura 2-8. Arquitectura del sistema propuesto por Enerchain [84]

Se ha utilizado un enfoque de arquitectura de software habitual distinguiendo entre una capa horizontal y otra vertical. La capa horizontal, sirve de plataforma genérica de comunicación de datos válida para todos los participantes, mientras que la vertical aporta flexibilidad a los clientes para diseñar sus lógicas de procesos de forma individualizada. La capa vertical puede ser implementada en las aplicaciones de cliente o en los adaptadores de cliente y nodo utilizando los *plug-ins* de Enerchain. En la Figura 2-8, los espacios destinados a la capa horizontal están coloreados en azul y los destinados a la capa vertical en rojo.

Algunas de las funciones principales implementadas son:

- Capa horizontal: Gestión de llaves públicas y accesos para autenticar a los participantes. Gestión de conexión a nodos y reconexión en caso de que alguno falle. Almacenamiento de la *blockchain*. Ruteado de mensajes entre aplicaciones del cliente a través de la jerarquía adaptador de cliente, adaptador de nudo y nudos de la *blockchain*.

- Capa vertical: Ruteado de órdenes y ejecuciones. Funciones de validación de transacciones a nivel de cliente. Proveer de datos a sistemas ETRM (*Energy Trading and Risk Management*).

### 2.2.2 Mercados locales P2P

El aumento de generación distribuida y de prosumidores hace que éstos tengan cada vez un rol más importante en el funcionamiento de las redes eléctricas. Los prosumidores están pasando de ser meros contribuyentes a participantes que pueden gestionar sus propios recursos y que persiguen rentabilizar sus inversiones [89].

Sin embargo, la capacidad de estos pequeños prosumidores es todavía mínima comparada con los generadores convencionales, y en la práctica se ven excluidos de participar directamente en los mercados mayoristas. Para ello, participan a través de intermediarios (entidades de agregación o comercializadoras). Aunque esto ayuda a que los prosumidores inviertan en nuevas instalaciones y los motiva a responder a los precios de mercado, siguen sin tener el control directo. Además, deberán compartir el beneficio con los intermediarios [90].

Los mercados locales P2P habilitan flujos bidireccionales de potencia e información en los sistemas eléctricos, cambiando el paradigma de flujo unidireccional, de generadores a usuarios, de los sistemas eléctricos tradicionales. Estos mercados permiten a los usuarios ofertar directamente, planificar sus propios recursos y adaptar su consumo acorde a las condiciones del mercado. Tienen una estructura descentralizada donde los participantes pueden comerciar directamente entre sí sin necesidad de intermediarios ni de una autoridad central [91].

La transición hacia mercados eléctricos descentralizados puede suponer importantes mejoras a la red en su conjunto, a las comunidades locales y a los consumidores finales. Por un lado, los mercados locales, ya sea en forma de microrredes físicas o virtuales, pueden propiciar el balance entre generación y demanda dentro de la comunidad reduciendo sobrecargas en las redes de transmisión y distribución. Las pérdidas de la red también se reducirían, gracias al fomento del consumo local y autoconsumo. Por otro lado, los costes de transacción se reducirían al evitar intermediarios.

Este tipo de mercados también aumentaría la elasticidad de la demanda eléctrica, muy poco elástica en los mercados tradicionales. Los usuarios pueden reaccionar a los precios del mercado ajustando sus recursos con flexibilidad (baterías o carga de vehículo eléctrico) y gestionando consumidores flexibles.

La tecnología *blockchain* puede servir como soporte para conseguir la descentralización y desintermediación que los mercados P2P requieren.

En función del grado de descentralización y la topología, algunas propuestas clasifican los mercados P2P en distintos tipos. En [92] se clasifican en totalmente descentralizados, basados en comunidades y en modelos híbridos. En [93], además, se hace una distinción para los mercados basados en comunidades, entre una topología compuesta por microrredes físicas y otra por agrupaciones organizadas en microrredes virtuales.

- **Totalmente descentralizados**: Los usuarios pueden participar directamente en un mercado tipo *pool* o comerciar bilateralmente con otros participantes sin necesidad de ninguna autoridad central. En este tipo de estructura, no existe ningún mediador, tal y como se observa en la Figura 2-9. En esta Figura las líneas azules representan intercambio de tipo P2P (directamente entre participantes) y las líneas naranjas representan intercambios con mercados existentes.

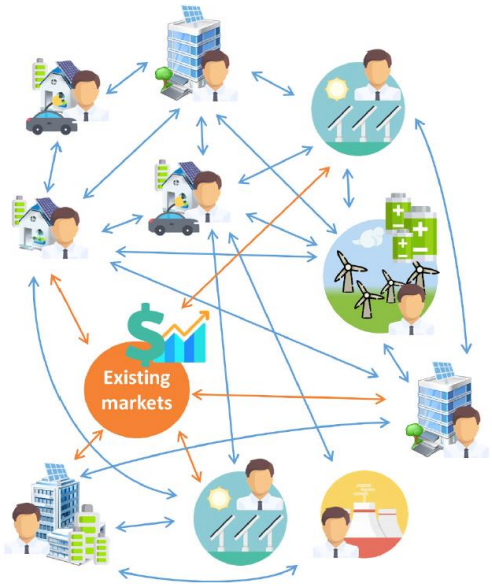


Figura 2-9. Mercado P2P totalmente descentralizado [92]

- **Basados en comunidades**: En este diseño, más estructurado, existe un gestor de la comunidad o *community manager* (CM) que organiza el comercio dentro de la comunidad y actúa como intermediario entre la comunidad y el resto de la red, tal y como se muestra en la Figura 2-10. En esta Figura las líneas azules representan intercambio entre comunidades, las líneas naranjas representan intercambios con mercados existentes, las líneas negras intercambios dentro de una comunidad y los cuadrados formados por líneas discontinuas representan comunidades. Este tipo de mercado puede ser aplicado a microrredes o a comunidades de usuarios que comparten un mismo objetivo.

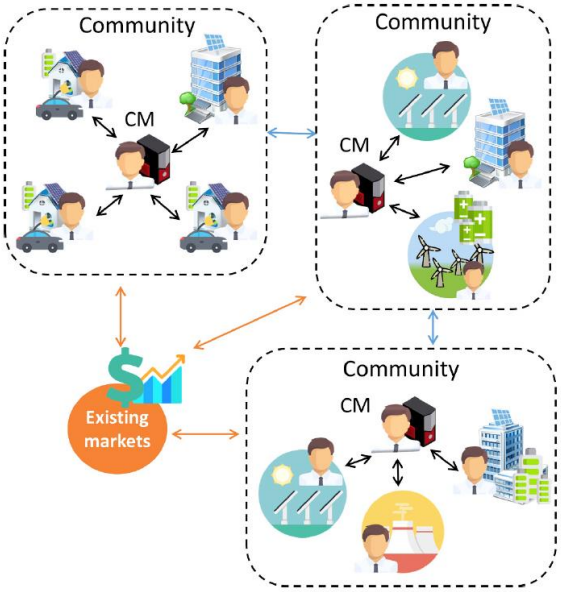


Figura 2-10. Mercado basado en comunidades [92]

- **Híbridos:** Este diseño, es una combinación de los dos anteriores, tal y como se muestra en la Figura 2-11. Por un lado, existen pares individuales que pueden interactuar directamente entre ellos y con los mercados existentes. Y a la vez, también existen comunidades como las expuestas en el caso anterior, donde un gestor o *community manager* (CM) supervisa el funcionamiento dentro de su comunidad e interactúa con el resto de los participantes. Además, también pueden darse casos

donde existan comunidades dentro de otras comunidades de mayor tamaño. En la Figura 2-11, las líneas negras representan intercambio dentro de una comunidad, las azules intercambio P2P directos entre participantes y los naranjas intercambios con mercados convencionales, los círculos formados por líneas negras discontinuas representan comunidades.

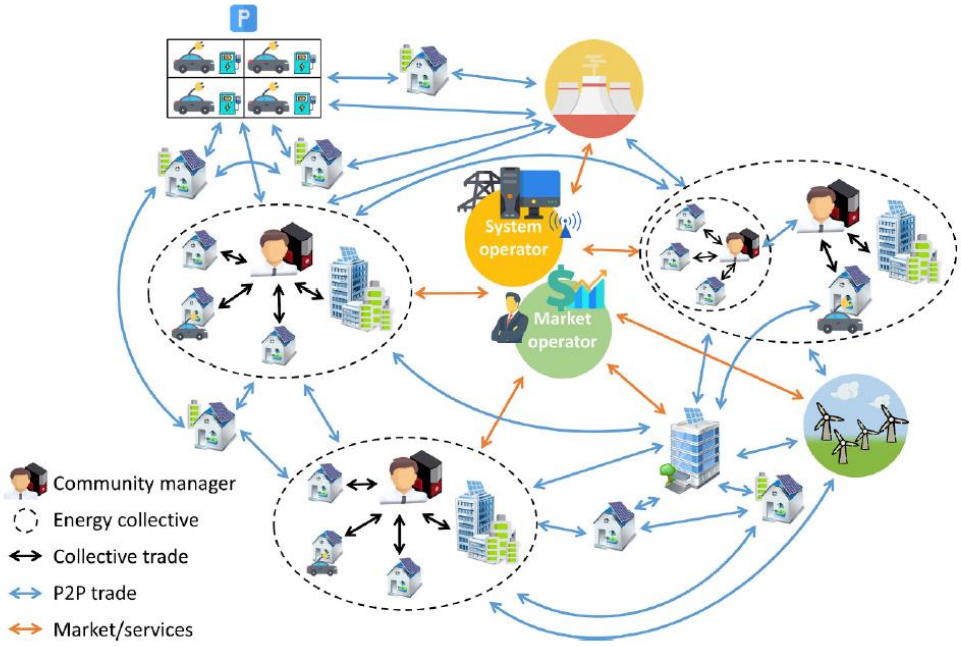


Figura 2-11. Mercado P2P híbrido [92]

Es importante remarcar que el papel de los operadores de red, tanto de Transporte como de Distribución tienen en este tipo de mercados. Las transacciones deberán ser revisadas por los Operadores para evitar violar las restricciones técnicas de la red.

Dentro del uso de *blockchain* en mercados basados en comunidades, el caso particular de las microrredes es el que mayor atención acapara en las publicaciones científicas y técnicas. Debido a que las microrredes tienen fronteras bien definidas con el resto de la red eléctrica y a que cuentan con cierta independencia, la implementación de nuevos esquemas de mercado propios e internos presenta mayor viabilidad.

Según [94], los siete componentes que un mercado basado en *blockchain* dentro de una microrred debe tener para funcionar de forma eficiente son:

- **Componente 1 (C1): Configuración de la microrred**
  Para establecer la configuración de microrred, inicialmente es necesario marcar el objetivo, identificar a los participantes del mercado y definir si la red de distribución tradicional se usa para el transporte de energía o si se construye una microrred física independiente. Es necesario que existan un número mínimo de participantes del mercado, además un subgrupo de ellos debe tener la capacidad de generar energía.
- **Componente 2 (C2): Infraestructura de conexión a la red**
  En una microrred física, se cuenta con una infraestructura de red propia, que puede estar unida en uno o unos pocos puntos a la red de distribución ordinaria, normalmente con medición en estos puntos frontera. También, llegado el caso, una microrred física puede separarse de la red y funcionar independientemente operando en modo isla. En el caso de una microrred virtual, el enlace entre los participantes se hace meramente a través del sistema de información (C3), usándose la red de distribución ordinaria para los intercambios físicos.
  Es importante tener en cuenta que los intercambios de energía deben estar sometidos a las restricciones de la red y estas deben ser tenidas en cuenta.
- **Componente 3 (C3): Sistema de información**
  Un sistema de información eficiente es necesario para conectar a todos los participantes, proporcionar una plataforma de mercado y acceso al mercado y monitorizar las operaciones. Un

protocolo de *blockchain* basado en *smart contracts* puede cumplir con estos objetivos. Este protocolo *blockchain* permite la implementación de aplicaciones descentralizadas, asegurando la consistencia y seguridad de los datos, sin una plataforma central. Es necesaria una conexión entre los contadores inteligentes de los participantes y la *blockchain*. Los contadores inteligentes monitorizan la generación y la demanda y escriben esta información directamente en su cuenta de *blockchain*.

El mecanismo de consenso utilizado en la *blockchain* depende directamente de la configuración de la microrred (C1). Si la participación en el mercado está reservada solo a miembros de la comunidad, puede implementar un mecanismo de consenso basado en identidad de forma lo suficientemente segura. Los mecanismos de consenso basados en identidad tienen un coste computacional mucho menor a los basados en *Proof of Work*. La identidad de los participantes inicialmente puede ser verificada por entidades gubernamentales o por *utilities*.

- **Componente 4 (C4): Mecanismo de mercado**
  El mecanismo de mercado se implementa a través del sistema de información (C3). Su objetivo es permitir una asignación eficiente de los intercambios de energía haciendo de nexo entre la oferta y demanda de los participantes del mercado. También fija las reglas de pagos y provee un formato de oferta unificado para todos los participantes. Además, debe tener en cuenta las restricciones técnicas de la red. Normalmente implementa diferentes horizontes temporales (día anterior, intradiario, etc) y debe adaptarse según este horizonte.
- **Componente 5 (C5): Mecanismo de fijación de precio**
  El mecanismo de fijación de precios se implementa a través del mecanismo de mercado y su objetivo es diseñar sistemas que permitan formar precios de forma eficiente en función de la generación y la demanda. Normalmente, los precios señalarán la escasez o exceso de generación. Teniendo en cuenta que la generación renovable normalmente tiene un coste marginal cercano a cero, un productor obtendrá beneficio siempre que venda la energía por encima de los hipotéticos costes de impuestos o tarifas de uso de red, que en una microrred pueden ser distintos a los de una red tradicional. Desde el punto de vista económico, los participantes del mercado se beneficiarán debido a que habitualmente el precio promedio del mercado local será inferior al precio de la red.
- **Componente 6 (C6): Sistema de gestión de comercio de energía** (EMTS por sus siglas *Energy Management Trading System)*
  El objetivo del EMTS es gestionar automáticamente el suministro eléctrico de los participantes e implementar su estrategia de oferta de compra y venta. Es necesario que el EMTS tenga acceso a los datos de generación y demanda de los participantes. Mediante el uso de estos datos, el EMTS desarrolla la estrategia de oferta según los intereses del participante. Además, puede reaccionar a las señales de precio utilizando sistemas de gestión de la demanda o sistemas de almacenamiento de los participantes. Estas estrategias inteligentes de oferta son unos de los pilares de los mercados locales activos. En caso de que el sistema de información (C3) se implemente con *blockchain*, el ETMS debe tener acceso a la cuenta de *blockchain* del participante del mercado, para facilitar los intercambios de energía automáticamente.
- **Componente 7 (C7): Regulación**
  El marco regulatorio determina como los mercados organizados en torno a microrredes encajan en la actual política energética. La legislación determina qué diseños de mercado están permitidos, como se aplican tasas e impuestos y de qué forma estos nuevos mercados se pueden integrar en los mercados y el sistema eléctrico tradicionales. De esta forma, a través de cambios regulatorios, los gobiernos pueden fomentar la implantación de este tipo de comunicades que promueven el uso de recursos de generación locales.

#### 2.2.2.1 Caso de estudio: Brooklyn Microgrid

Un de los primeros proyectos que habilitó un mercado P2P a nivel local utilizando *blockchain*, fue el proyecto BMG (*Brooklyn Microgrid*) llevado a cabo por la compañía LO3 Energy en el área de Brooklyn (New York) [94]. Este trabajo ha sido ampliamente citado como caso de estudio exitoso en la literatura relacionada con aplicaciones de *blockchain* a mercados eléctricos locales.

El proyecto BMG ha implementado y probado un mercado eléctrico local dentro de una microrred, donde los miembros de la comunidad pueden comerciar sus excesos de generación de forma P2P con sus vecinos. En

principio se trata de una microrred virtual donde sus participantes se extienden en tres áreas distintas de la red de distribución existente.

La infraestructura técnica de la plataforma está formada por los desarrollos de TransActive Grid, creados por LO3 Energy junto a ConsenSys (una compañía de desarrollos *blockchain*):

- La arquitectura *blockchain* TransActive Grid. Se trata de una *blockchain* privada desarrollada utilizando el protocolo Tendermint [88]
- Contadores inteligentes TansActive *Smart* Meters, capaces de interactuar directamente con una *blockchain*, actuando como billeteras (*wallets*). Los contadores se instalan junto a los contadores analógicos tradicionales de los participantes, tal y como se puede observar en la Figura 2-12.

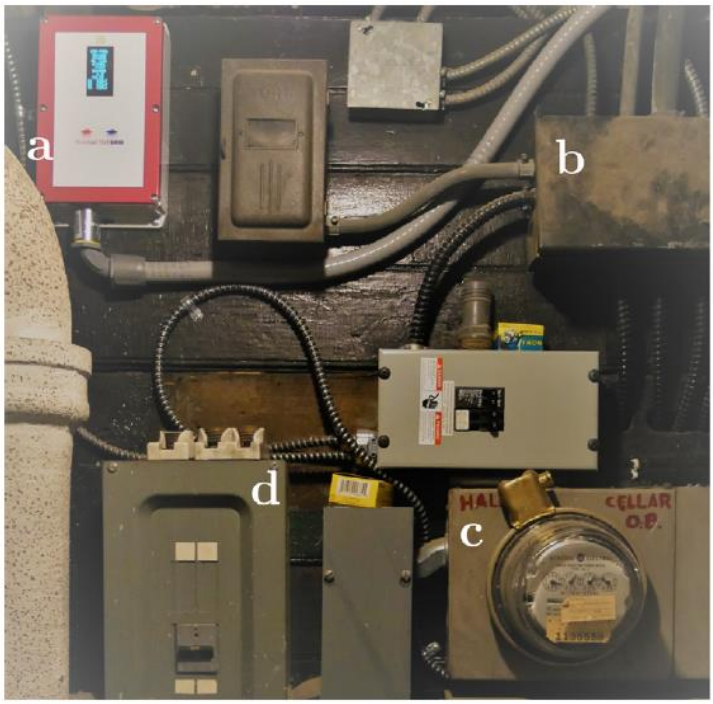


Figura 2-12. Instalación de TransActive *Smart* Meters (a) a continuación del contador analógico de facturación ordinario (c). (b) y (d) son, respectivamente, la caja de distribución y la caja de fusibles [94]

En la Figura 2-13 se muestra la topología de BMG, compuesta por una capa física y otra virtual. La capa física, donde se producen los flujos de energía, está formada por la propia infraestructura de la red de distribución, gestionada por Con Edison, el Operador de Distribución. La capa virtual es la plataforma de mercado virtual que se ejecuta sobre una red *blockchain* y es donde se transmite la información.

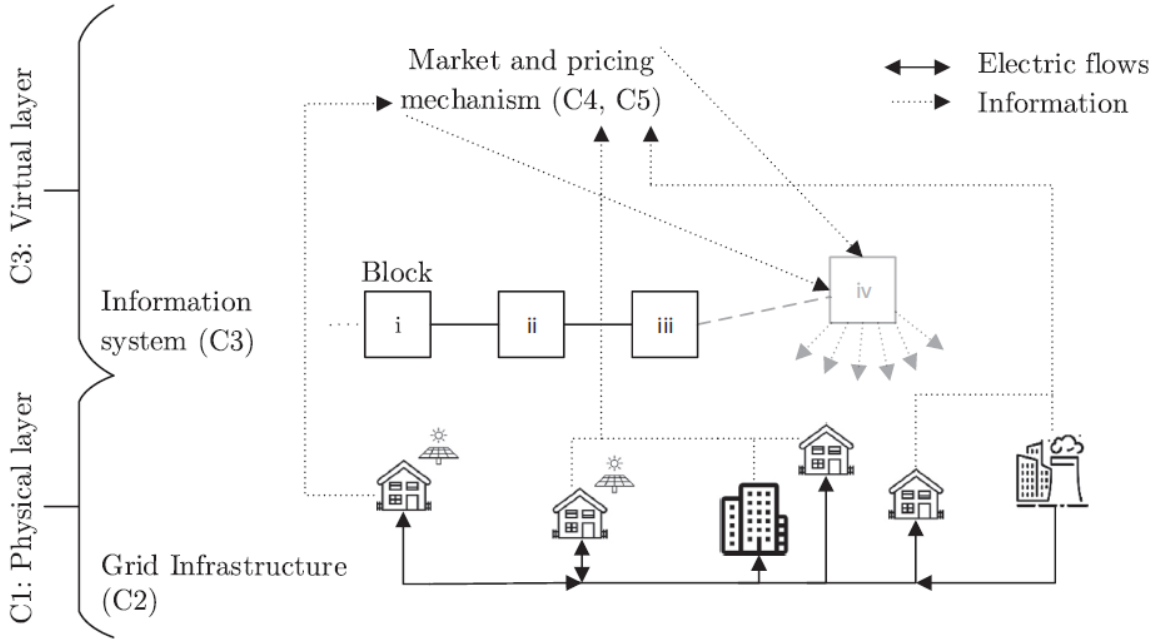


Figura 2-13. Topología de alto nivel de la red BMG [94]

Los participantes del mercado (C1) son consumidores y prosumidores locales que conforman la microrred virtual. La conexión entre la configuración de la microrred (C1) y la infraestructura de la red (C2) se hace a través de los contadores inteligentes que miden la generación y demanda de energía y trasladan los datos al sistema de información (C3). Estos contadores inteligentes escriben los datos directamente en las cuentas de *blockchain* de los participantes. Las órdenes de compra y venta son creadas a partir de estos datos y son enviadas al mecanismo de mercado (C4) que está basado en *smart contracts*. Una vez que se produce casación entre compradores y vendedores, se liquida el pago automáticamente, siguiendo las consignas programadas en el *smart contract*. Cuando se cierra el proceso de liquidación, un nuevo bloque se añade a la *blockchain* (ilustrado como bloque iv en la Figura 2-13). Este bloque incluye toda la información del mercado y es accesible para todos los agentes involucrados a través de sus cuentas de *blockchain*.

La plataforma registra y muestra datos y precios casi en tiempo real, a través de una interfaz intuitiva para los usuarios. De esta forma, los participantes pueden acceder a esta información y configurar su estrategia de intercambios según sus necesidades. El proceso de comercio se realiza casi enteramente de forma automatizada gracias al EMTS (C6) implementado y solo requiere que los participantes configuren sus preferencias. Algunos ejemplos de preferencias pueden ser: minimizar el precio de la energía, maximizar la compra de energía renovable producida localmente, o priorizar la energía producida por tu bloque de vecinos.

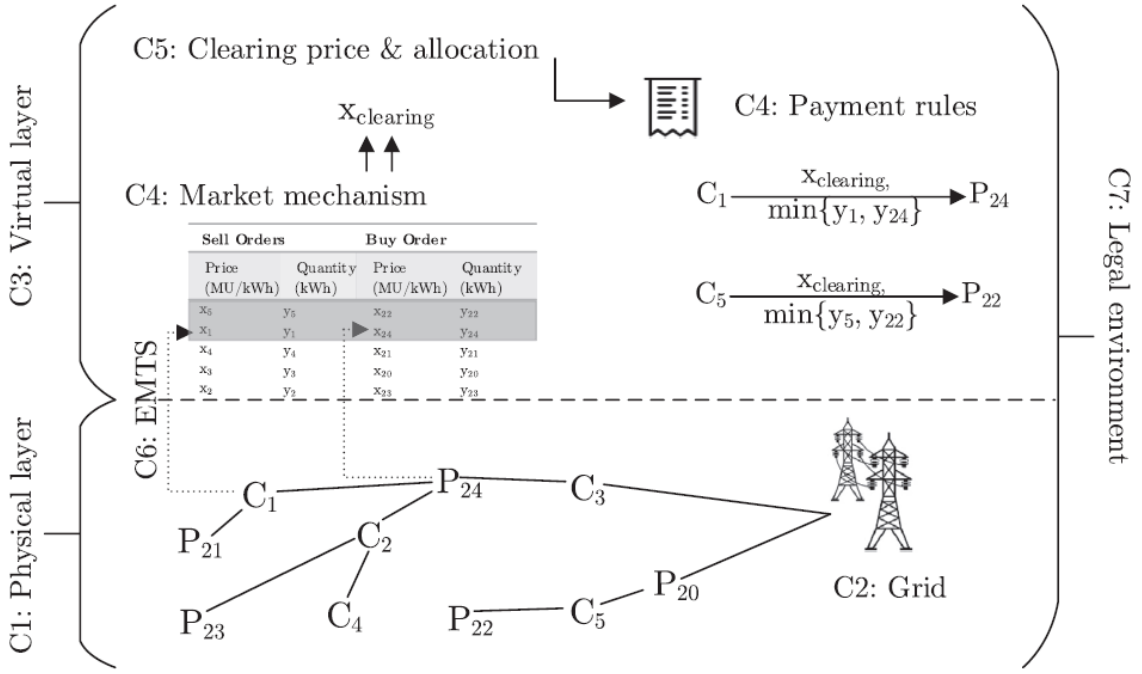


Figura 2-14. Representación esquemática de transacciones efectuadas en la red BMG. Cn y Pn representan a los consumidores y prosumidores respectivamente [94]

El mecanismo de mercado (C4) consiste en un libro de órdenes cerrado con mecanismo de doble subasta (*double auction*) para periodos discretos de 15 minutos. Los consumidores ofertan su precio máximo de compra para su fuente de generación preferidas y los prosumidores ofertan su precio mínimo de venta (C5). Las ofertas son casadas en orden descendente de precio, siendo las más altas casadas primero. La última oferta en ser casada marca el precio de la electricidad para ese periodo de 15 minutos. Los consumidores que no casen su oferta en ese periodo de tiempo serán suministrados con energía de la red de distribución ordinaria. Alternativamente, el proyecto BMG está probando otros mecanismos de mercado y fijación de precios, entre ellos el *pay-as-you-bid* donde cada transacción puede tener un precio individual.

Las transacciones financieras entre los participantes también son parte del mecanismo de mercado (C4). Se ejecutan automáticamente gracias a los *smart contracts*, y se hacen a través de *tokens* de energía que pueden ser comprados y vendidos en un *marketplace*. Los tokens son transferidos a través de la *blockchain* desde las *wallets* de los compradores a las de los vendedores.

En relación con el marco regulatorio (C7), el comercio de energía local P2P no está regulado en el área donde el proyecto BMG se ha implementado. Por lo tanto, ha sido necesaria la colaboración de la compañía de distribución para llevar a cabo el experimento.

La conclusión que se extrae del experimento BMG es que el mercado local implementado cumple con los requisitos necesarios de los componentes C1 a C6. Siendo estos los componentes expuestos en el apartado anterior, y que debe tener un mercado local. Además, se prueba que la tecnología *blockchain* puede ser utilizada como sistema de información (C3), habilitando un sistema descentralizado sin necesidad de una autoridad central. En este sistema, los participantes pueden autoorganizarse y confiar en la integridad de la información gracias las características inherentes de una red *blockchain*. Por último, el experimento pone de manifiesto que el componente C7 (Regulación) no se cumple, al menos en el área y el tiempo en el que el experimento fue llevado a cabo. Para ello, es necesario que reguladores, distribuidoras y comercializadoras colaboren y trabajen en elaborar un marco regulatorio donde este tipo de comunidades puedan desarrollarse.

## 2.3 Gestión, operación y control de redes eléctricas

La incorporación en los sistemas eléctricos de generación distribuida, contadores inteligentes, tecnologías de la información y comunicación y otros elementos inteligentes, posibilita y hace necesario la implementación de nuevos modelos de gestión, operación y control de las redes eléctricas. En este nuevo contexto de *smart grids,*

los usuarios finales incorporan recursos energéticos propios como generación y almacenamiento, y los flujos de potencia e información pasan a ser bidireccionales.

La transformación en *smart grids* de las redes tradicionales ha sido posible gracias a la implementación de nuevas tecnologías y soluciones de sensorización, instrumentación, actuación y de comunicaciones, que habilitan nuevas formas de operación y control más avanzadas. Algunos de estos nuevos habilitadores son [95]:

- Contadores inteligentes. Los contadores inteligentes fueron instalados para evitar la lectura manual por parte del personal de las compañías. Desarrollos posteriores han permitido la conexión y desconexión remota, comunicaciones avanzadas con las compañías distribuidoras e incluso comunicaciones con hogares inteligentes y sistemas de control [96]. Con los contadores inteligentes la información de consumo y generación en intervalos de una hora o menos puede estar a disposición de las compañías y los usuarios.
- Unidades de medición de fasores (PMU por sus siglas en inglés). Permiten obtener información de alta precisión a nivel de forma de onda con marca de tiempo referenciada globalmente. Esta información es comunicada en tiempo real a los operadores del sistema, que pueden comparar valores de voltaje e intensidad entre distintos puntos de la red permitiendo así evaluar el estado del sistema y actuar consecuentemente [97].
- Inversores inteligentes. Los inversores, por medio de electrónica de potencia, convierten la corriente continua en alterna. Se utilizan, por ejemplo, para conectar a la red sistemas de paneles fotovoltaicos. Los inversores inteligentes cuentan con funcionalidades de control y comunicación avanzadas, que aportan flexibilidad en la conversión y permiten regular la inyección de potencia reactiva a la red.
- Dispositivos FACTS. Los dispositivos FACTS, como los bancos de capacitancia y reactancia, permiten un control avanzado de la capacidad de transferencia de potencia en líneas de transmisión. Aunque este tipo de dispositivo lleva muchos años usándose, recientemente se han desarrollado FACTS con capacidad de control avanzado en tiempo real, abriendo la posibilidad a efectuar un control distribuido de voltaje y frecuencia.
- Intercambiadores de tomas en carga, compensadores de reactiva estáticos (STATCOM) y capacitores conmutables. Estos elementos introducen una capacidad de respuesta para intervenir en el control de voltaje que puede ir desde los milisegundos hasta los minutos.
- Usuarios finales. La incorporación de instalaciones de generación y almacenamiento en el lado de los usuarios ha supuesto un cambio de paradigma. Por otro lado, la automatización y los dispositivos conectados también están transformando los hogares. Mediante sistemas de gestión energética del hogar (HEMS), los usuarios son capaces de monitorizar y controlar sus dispositivos, modificando el comportamiento de su consumo según sus intereses. Cada vez más dispositivos, especialmente de climatización, incorporan sensores, funciones avanzadas de control y gestión de la energía. Los usuarios podrían llegar a acuerdos para apagar o modificar parámetros de sus aparatos de climatización, calentadores de agua o carga de vehículo eléctrico de forma automática para contribuir a las necesidades de la red, optimizando recursos e infraestructuras. Aplicaciones similares pude ser implementadas en comercios e industrias. De esta forma se multiplican las posibilidades de participación de los usuarios y de una respuesta activa en el lado de la demanda [98].
- Canales de comunicación. Los avances en comunicación hacen posible la recolección de información y el envío de comandos a actuadores, de forma rápida gracias al aumento de los anchos de banda y reducción de latencia. Tecnologías como el Zigbee y Wifi son útiles para comunicaciones de rango corto. PLC (*Power Line Carrier*), una tecnología con muchos años de uso también está tomando relevancia en las *smart grids* [99]. El desarrollo en las comunicaciones junto con los contadores inteligentes propicia el despliegue de infraestructuras avanzadas de medición (AMI por sus siglas en inglés). Las AMI proporcionan la red para el envío de información desde los contadores hasta las compañías eléctricas.

En la Figura 2-15 se muestra una comparación entre una estrategia de control centralizada típica de los sistemas eléctricos tradicionales, donde sólo intervienen los grandes generadores, y entre un sistema de control en *smart grid* donde el control se extiende hacia el lado de la demanda. Esto incrementa la cantidad de señales

a intercambiar, que van más allá de voltaje y frecuencia del modelo clásico.

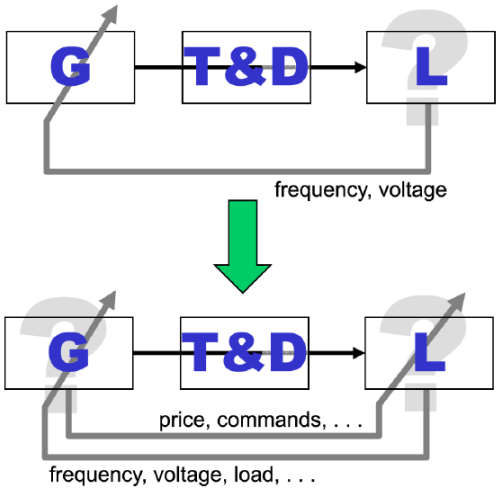


Figura 2-15. Esquema de control de una red convencional (arriba) y de una *smart grid* (abajo) [95]

Las estrategias de gestión, operación y control de *smart grids* de una forma centralizada convencional es difícil de implementar, costosa y obsoleta, debido al gran número de elementos a integrar. Esto hace que la tendencia sea hacia modelos descentralizados [100]. En estos modelos descentralizados, las *smart grids* se pueden dividir en microrredes autogestionadas, se pueden crear agregaciones de consumidores para participar conjuntamente en programas de repuesta a la demanda o de servicios complementarios y se pueden constituir agrupaciones de pequeñas instalaciones de generación para actuar como una sola entidad (como las VPP).

También, la incorporación de nuevos habilitadores expuestos anteriormente en las redes de distribución hace posible la implementación de nuevos esquemas de control avanzados. En estos, los inversores inteligentes y los sistemas de gestión energética de los usuarios toman un rol activo en la operación y optimización de redes activas de distribución.

Este tipo de sistemas descentralizados y nuevos esquemas de control en redes activas de distribución y microrredes, requieren de sistemas de gestión y operación innovadores como *blockchain*.

En general, las principales áreas y actividades donde *blockchain* puede ser de utilidad en la gestión, operación y control de las nuevas redes eléctricas son las siguientes [100]:

- **Colaboración entre entidades**: El aumento de nuevos actores en los distintos procesos de generación, distribución, comercio y distribución, junto con la aparición de nuevas tecnologías e inversiones, hace que la coordinación entre ellos sea complicada. Esta falta de coordinación puede causar desbalances en los valores de voltaje y frecuencia de la red, aumento de pérdidas y cortes de suministro. Por lo tanto, es necesario implementar sistemas de intercambio de información modernos para establecer una cooperación eficiente entre las distintas entidades del sector eléctrico. En grupos de colaboración cerrados como las *Virtual Power Plants* (VPP) o microrredes, las redes *blockchain*, pueden ser usadas para implementar sistemas de control, mejorar las actividades de operación y optimización, implementar mecanismos de mercado y aumentar la ciberseguridad.

- **Control de desequilibrios en la red**: Problemas como desviaciones de voltaje o frecuencia, sobrecargas, pérdida de sincronización, huecos de voltaje y ataques maliciosos pueden crear desequilibrios en la red. Por ejemplo, una planta fotovoltaica produce más energía durante las horas centrales del día, cuando la demanda puede ser menor, esto puede causar flujos de potencia inversos no deseados en redes de distribución. Controlar el voltaje en este tipo de redes también puede ser un reto. Por lo tanto, es esencial controlar y monitorizar la generación, consumo y distribución de las distintas entidades para regular la potencia activa y reactiva. Esto es un reto debido al gran número y diversidad de fuentes de generación.
  Las redes de distribución activas (ADN por sus siglas en inglés) son redes de distribución con diversos componentes que habilitan un control avanzado, y con topología de red flexible. En ellas, los operadores del sistema pueden operar y controlar la red buscando la máxima eficiencia y permitiendo integrar la generación distribuida. Este tipo de redes requiere la coordinación entre

operadores del sistema, generadores distribuidos, centros de control, subestaciones y otros componentes. Para lograr esta coordinación es necesaria una infraestructura de comunicación confiable, eficiente y segura [101].
Gracias a que *blockchain* sirve de mecanismo para sincronizar información procedente de diversas fuentes, puede ser usado para monitorizar, controlar voltaje y frecuencia, y coordinar las comunicaciones ente distintas partes. *Blockchain* sirve de soporte tanto para redes activas de distribución a nivel de operadores del sistema, como a sistemas de control en comunidades tipo microrredes.

- **Análisis y gestión de datos**: La gestión de información en las redes inteligentes se enfrenta a varios retos como la calidad en la agregación de datos, seguridad, controles de cumplimiento y eficiencia en los mecanismos de gestión [102]. Se genera y transfiere una gran cantidad de datos entre entidades, por ejemplo, predicciones de generación o climatológicas. La precisión y consistencia de estos datos permite a los operadores controlar y monitorizar correctamente el sistema eléctrico. El volumen de datos recolectados tiende a ser elevado, debido a los múltiples componentes de las redes inteligentes involucrados en los procesos. Por ejemplo, las AMI recopilan datos de consumos y generación con una resolución de minutos. Este gran volumen de datos (*big data*), también puede ser analizado y utilizado para operaciones de red, predicciones de demanda y generación, ajustes de precios, sistemas de alarma, etc.
  Las entidades de agregación, como las VPP o agrupaciones orientadas a respuesta de la demanda, proporcionan servicios de red agrupando conjuntos de generadores y consumidores. Estas entidades presentan despliegues complejos y a gran escala que requieren de sistema de gestión y control.
  Por esto, los sistemas de procesamiento de información necesitan nuevas tecnologías que modernicen y automaticen la gestión, almacenamiento y acceso de datos.
  *Blockchain*, es una base de datos distribuida en diferentes copias conectadas entre sí, que mediante ciertos mecanismos de consenso impide que los datos sean alterados sin autorización. Por eso, *blockchain* ha sido propuesto para solventar algunos de los retos mencionados, sirviendo como soporte para el análisis y gestión de datos, protección de datos y agregación.
- **Operación y gestión descentralizada de la red**: La operación descentralizada permite a distintas entidades controlar y gestionar los sistemas de forma local mediante el uso de dispositivos de automatización y monitorización distribuidos. Aplicaciones como el control activo de la demanda y la optimización de la operación de redes de forma descentralizada son temas que actualmente están en estudio y desarrollo [95]. Estos esquemas de gestión de la red se enfrentan a varios retos como la coordinación y la integración eficiente entre redes inteligentes, activos de generación e infraestructuras de respuesta a la demanda distribuidas.
- **Seguridad y privacidad**: Los sistemas SCADA de los actuales sistemas eléctricos reciben, transmiten y almacenan información de forma que en ocasiones pueden ser vulnerables a ciberataques. Además, el rápido aumento de dispositivos conectados a internet (IoT), integrados en redes inteligentes, y que presentan capacidades frente a la seguridad limitadas, hace que sea necesario implementar nuevas medidas para mantener la seguridad de los sistemas, así como la privacidad de datos personales y corporativos.
  La ciberseguridad es uno de los mayores retos a lo que se enfrentan las nuevas *smart grids*, en los últimos años se han documentado varios casos de ciberataques [69]. Debido a que una de las principales características de *blockchain* es la inmutabilidad de la información contenida en la red de bloques, se presenta como una solución a algunos de estos problemas. Por su importancia, la aplicación de *blockchain* para mejorar la seguridad y privacidad de sistemas eléctricos en general, se ha tratado en un apartado dedicado del presente trabajo.

En los próximos apartados, se recogen algunas aplicaciones prácticas donde *blockchain* tiene potenciales utilidades dentro de la operación, gestión y control de redes eléctricas. Además, se expondrán ejemplos de aplicaciones prácticas. Estas aplicaciones se han clasificado en tres áreas:

- **Plantas de generación virtuales o *Virtual Power Plants* (VPP)**
  - Caso de estudio:
    - Gestión descentralizada de VPP formada por prosumidores con casas inteligentes.
- **Microrredes**

- Casos de estudio:
  - Control distribuido con *blockchain* para regulación de voltaje en una microrred asegurando la equidad entre usuarios
  - Transacciones descentralizadas en microrredes interconectadas.

- **Respuesta a la demanda y servicios complementarios**
  - Casos de estudio:
    - Agregación de consumidores para sistemas de respuesta a la demanda.
    - Comunidad de estaciones de recarga de vehículo eléctrico con servicio de regulación de frecuencia.

### 2.3.1 Plantas de energía virtuales (VPP)

Las plantas de energía virtual o VPP (*Virtual Power Plants)*, se definen como un grupo de recursos de generación distribuida agrupados y organizados para funcionar como una sola unidad de generación despachable, con intención de participar en el mercado eléctrico o en los servicios de ajuste.

Aunque las VPP comparten algunas similitudes con las microrredes, existen diferencias importantes entre ellas. En una VPP, las unidades de generación no necesariamente están ubicadas en un área concreta, unas cercanas entre sí. Además, las microrredes tienen una mayor dependencia de elementos de hardware y de infraestructura física, mientras que las VPP están organizadas básicamente a través de software y su infraestructura está compuesta por contadores inteligentes que registran los flujos de energía y por sistemas de información y comunicación [103].

Las VPP funcionan como agregadores que permiten a pequeños y medianos productores participar en mercados eléctricos. Representan un porfolio de plantas de generación distribuidas para obtener unos beneficios que no podrían lograrse actuando por separado. Para ello, interactúan con los operadores de la red para proporcionar de forma colectiva energía y servicios de ajuste. Las interacciones entre operadores de red, operadores de VPP y generadores son complejas, tanto en términos de acuerdos contractuales como en el suministro de los servicios. La confianza entre los propietarios de la generación y el agregador es fundamental, por eso, es necesario un registro preciso del comportamiento de los generadores y de la ejecución de los acuerdos establecidos. La digitalización y automatización de procesos como el control de los recursos, verificación y pago de los servicios es necesaria para solventar la complejidad de involucrar a distintas partes agregadas.

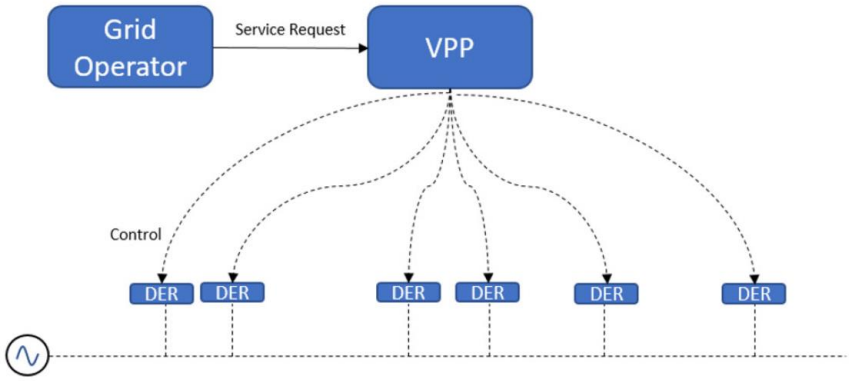


Figura 2-16. Esquema general de una VPP [104]

En la Figura 2-16 se muestran las interacciones entre el operador de red, el operador de VPP y los generadores distribuidos (DER). El operador de la VPP inicia el control de los generadores cuando recibe consignas del operador de red. Normalmente, la VPP efectúa un despacho económico interno para optimizar el beneficio, seleccionado y enviando consignas de control a los generadores para cumplir con el servicio de red solicitado por el operador. De esta forma, la función del operador de una VPP es controlar un porfolio de varios generadores distribuidos agregados cumpliendo las consignas del operador de la red.

Los operadores de VPP deben registrar y reportar el uso y contribución de los generadores, para que estos puedan ser compensados. Por ello, la confianza y trasparencia entre los propietarios de los generadores y el

operador de VPP es esencial para evitar disputas. Por ejemplo, un generador podría no cumplir con el despacho de la VPP no dando respuesta al servicio solicitado. Por otro lado, el operador de la VPP podría extender el uso de un generador sin registrar adecuadamente su contribución, o beneficiar a algunos generadores frente a otros durante el despacho. Esto puede suponer un problema en las VPP convencionales que normalmente actúan como una "caja negra" donde los participantes no pueden verificar su funcionamiento con trasparencia.

Otro problema en las VPP convencionales es que el operador de la VPP debe recolectar datos de uso de energía de los participantes, con el riesgo de privacidad y de filtración de datos que esto puede suponer, especialmente en VPP donde se involucre a hogares como prosumidores.

La tecnología *blockchain* puede ser utilizada para garantizar transparencia, confianza y privacidad en este tipo de esquemas de agregación. Dada la naturaleza de *blockchain* como marco digital de consenso, es posible crear plataformas de confianza que permitan registrar las operaciones de una VPP, y automatizar las relaciones contractuales mediante el uso de *smart contracts*. Además, el operador de VPP, puede pasar de ser una figura centralizada a una descentralizada mediante *smart contracts*.

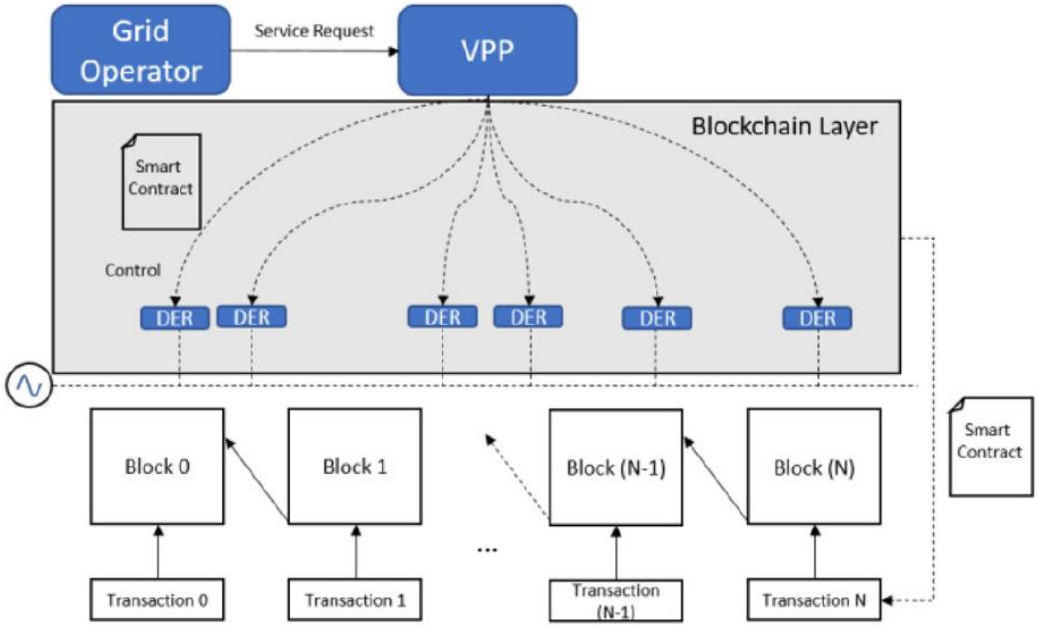


Figura 2-17. Esquema de una VPP con *blockchain* y *smart contracts*. [104]

En la Figura 2-17 se muestra un esquema simplificado de una VPP que integra una capa de *blockchain* con *smart contracts* para registrar transacciones y automatizar procesos. Cuando se activa un evento de control por parte del operador de la VPP para proporcionar un determinado servicio a la red, los generadores se despachan a través de *smart contracts* y toda la información es registrada directamente en la *blockchain*. Los registros pueden ser verificados y validados por todos los participantes de la red *blockchain*, e incluyen datos de generación, marcas temporales, desviaciones y cualquier otra información relevante en el acuerdo *contract*ual entre la VPP y los generadores. Los registros en la *blockchain* están encriptados, asegurando la privacidad y seguridad de los generadores, que solo pueden acceder a la información de sus activos a través de sus claves privadas.

Adicionalmente, los pagos a los propietarios de los generadores pueden automatizarse con *smart contracts*. Es posible realizar el pago a través de *tokens* que pueden tomar valor en función de distintos criterios, como energía en kWh, tipo de generación o tipo de servicio prestado (por ejemplo, inyección de energía reactiva o activa, *curtailment*, etc).

#### 2.3.1.1 Caso de estudio: Gestión descentralizada de VPP formada por prosumidores con casas inteligentes

A continuación, se propone un modelo de gestión de VPP formada por múltiples viviendas inteligentes

conectadas en una *smart grid* y que utiliza una plataforma de gestión energética descentralizada basada en *blockchain* [105]. En este caso, la VPP no sólo funciona como agregador de generación eléctrica y de servicios de ajuste, también ofrece servicios de respuesta de la demanda, funcionando como un agregador integral para prosumidores con dispositivos inteligentes capaces de modificar su comportamiento en función de las necesidades de la red.

En este ejemplo, tal y como se observa en la Figura 2-18, las viviendas están equipadas con

- Generación renovable (fotovoltaica o eólica)
- Almacenamiento
- Cargas controlables (como climatización) y flexibles (como lavadoras y secadoras)
- Contadores inteligentes que se encargar de gestionar los componentes anteriores y que conectan la vivienda con la red eléctrica local y con la VPP.

Los servicios de red que la VPP ofrece son:

- Venta de excedentes de generación a la red.
- Respuesta de la demanda, que motiva a los usuarios a ajustar su consumo energético según las necesidades de la red, a cambio de una compensación.
- Servicios de red complementarios, utilizando la capacidad de acumulación de los usuarios, que son recompensados por almacenar energía en sus baterías para regulación de carga y reserva rodante. La energía almacenada puede ser despachada por la VPP a la red para mantener su estabilidad.

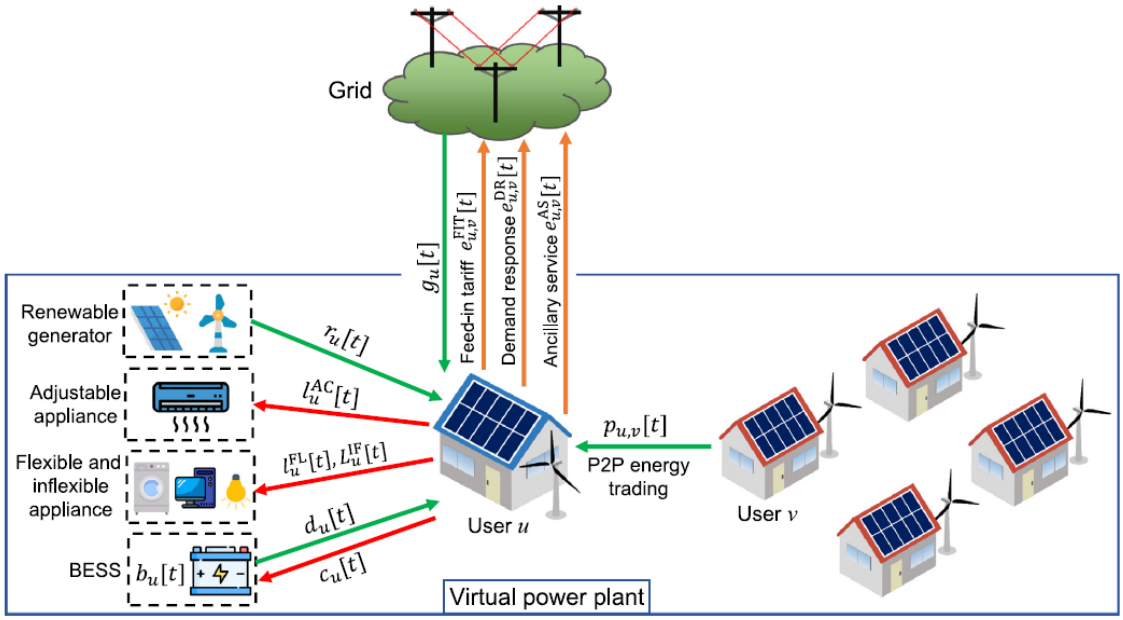


Figura 2-18. Principio de operación básico y componentes de la VPP [105]

Además, la VPP habilita la posibilidad de que los usuarios puedan intercambiar energía con otros usuarios de la VPP, evitando que los excedentes de generación se viertan a la red cuando otros usuarios tienen un déficit energético. Con esto, se busca minimizar el coste energético de la comunidad.

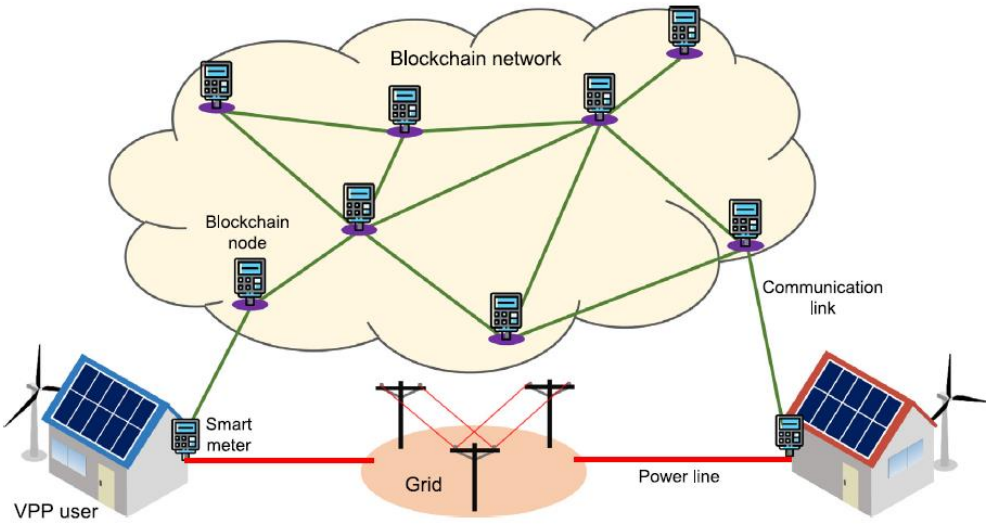


Figura 2-19. Red *blockchain* para implementar la plataforma de gestión descentralizada de la VPP [105]

Tal y como se observa en la Figura 2-19, los contadores inteligentes son utilizados como nodos en la red *blockchain*. Esto es posible gracias a que los contadores inteligentes actuales son dispositivos inteligentes embebidos capaces de llevar a cabo tareas de computación avanzadas. Los contadores se comunican con la red eléctrica convencional mediante *power line* y con la red de *blockchain* mediante LoRa y 5G Narrowband IoT.

El algoritmo de consenso implementado en la red *blockchain* es *Proof of Autority* (PoA), debido que su complejidad de computación es baja, especialmente si se compara con el algoritmo PoW. Eso hace que su implementación en contadores inteligentes sea viable. Además, con PoA los tiempos de confirmación de las transacciones son más reducidos. En el protocolo de consenso PoA un grupo de nodos son elegidos para formar el PoA "comité" y participar en el mecanismo de consenso generando nuevos bloques. Los nodos PoA son los encargados de recibir las transacciones, ejecutarlas y empaquetarlas en un nuevo bloque. El resto de los contadores inteligentes, o nodos normales, pueden realizar transacciones, pero no participan en el proceso de creación de nuevos bloques. Un nodo PoA puede proponer añadir o eliminar del "comité" a otro nodo como PoA, si más de la mitad de los nodos PoA acepta la propuesta, esta se ejecuta y los miembros del "comité" se modifican.

Para el funcionamiento de la VPP, en la red *blockchain* existen tres tipos distintos de transacciones:

- Transacciones con información de servicios de red. Este tipo de transacción se hace entre la VPP y la red eléctrica. Contiene información sobre la energía vertida, y las necesidades de respuesta de la demanda y servicios de ajuste.
- Transacciones con información de intercambio de energía P2P entre usuarios de la VPP. Este tipo de transacciones se hace entre usuarios de la VPP y la plataforma de gestión de energía de la VPP.
- Transacciones de transferencia de *tokens*. La transferencia de *tokens*, funcionando como divisas digitales, permite recibir el pago online de los intercambios de energía con otros usuarios, y de las recompensas por los servicios de red prestados.

Además, en este ejemplo se propone la implementación un algoritmo de optimización descentralizado, organizando los recursos de los usuarios con el objetivo de minimizar el coste operativo total. En un esquema de VPP convencional, habitualmente un coordinador autorizado se encargaría de recolectar la información de los usuarios y de forma global minimizar el coste global de operación resolviendo de forma centralizada un problema de optimización.

Sin embargo, este esquema centralizado presenta algunas desventajas. Por un lado, está el problema de la privacidad de los usuarios que deben compartir con el coordinador central toda la información de su gestión energética (incluyendo, por ejemplo, *set points* de temperatura de aire acondicionado o programación de consumos). Por otro lado, los usuarios no tienen la capacidad de comprobar y fiscalizar las operaciones del operador de la VPP.

Para abordar los problemas mencionados anteriormente, se propone un algoritmo de optimización

descentralizado. Utilizando el método *Alternating Direction Method of Mulpliers* (ADMM), se descompone el problema de optimización en los problemas primal y dual. El problema primal se resuelve de forma local en los contadores inteligentes de cada usuario. Debido a que los problemas primales de cada usuario están desacoplados, pueden ser resueltos en paralelo. Con esto, los usuarios minimizan la cantidad de información que deben compartir fuera de sus contadores inteligentes, en este caso sólo deberán compartir la cantidad de energía que están dispuestos a intercambiar con otros usuarios. El problema dual, se implementa en la *blockchain* a través de un *smart contract*.

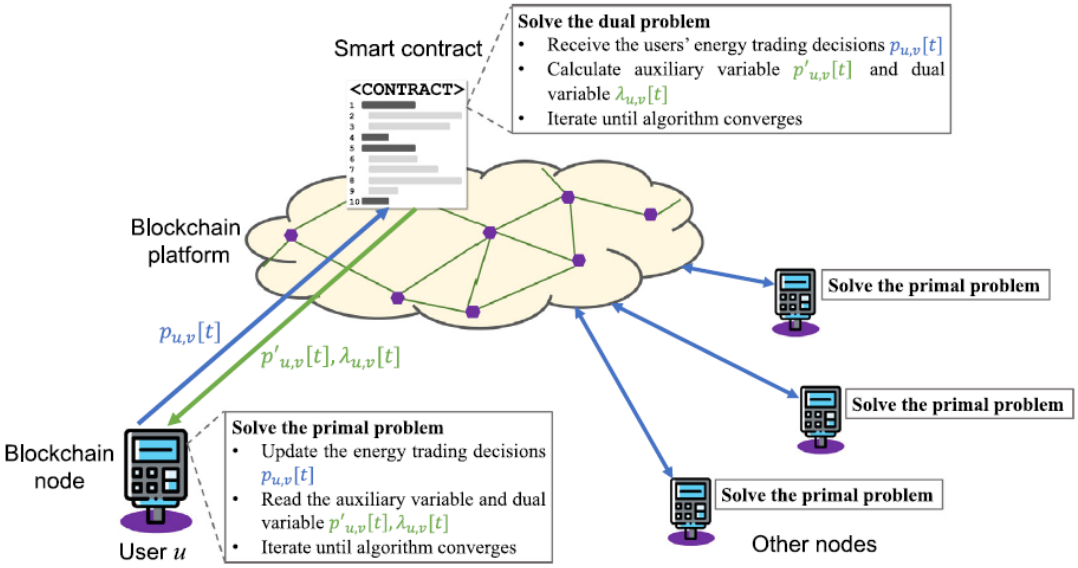


Figura 2-20. Algoritmo de optimización descentralizado [105]

Tal y como se muestra en la Figura 2-20, el algoritmo realiza varias iteraciones entre el problema primal y el problema dual hasta que converge. En cada iteración, los usuarios resuelven el problema primal en sus contadores, obteniendo su programación energética e intercambios de energía, actualizando este último valor en el *smart contract*. Una vez recibidos los valores de intercambios de energía de todos los usuarios, el *smart contract* automáticamente resuelve el problema dual obteniendo variables auxiliares que son enviadas a los usuarios para la siguiente iteración. El proceso de iteración finaliza cuando el error de convergencia está dentro del umbral de solución, obteniendo los usuarios la programación óptima de sus dispositivos. Finalmente, los usuarios ejecutan la programación energética óptima durante la operación de la VPP.

### 2.3.2 Microrredes

Una microrred es un conjunto de cargas y recursos energéticos distribuidos que forman un sistema eléctrico en baja o media tensión, con unos límites físicos definidos con la red eléctrica y que actúa como una sola entidad controlable [68]. Las características más importantes de las microrredes son:

- Capacidad para operar conectadas a la red o en modo isla.
- Pueden tener uno o varios puntos de conexión con la red eléctrica.
- Dentro de la red eléctrica general, las microrredes actúan como una sola entidad controlable.
- Tienen capacidad para interactuar con la red, buscando optimizar sus costes de energía y operación.

Debido a la numerosa cantidad de recursos energéticos distribuidos que se están introduciendo en las redes eléctricas, la idea de convertir los sistemas eléctricos en una agregación de pequeñas microrredes se presenta como una opción viable [103]. Por esto, se están dedicando numerosas investigaciones y propuestas de innovación para afrontar los restos que la gestión de una microrred presenta. Algunos de estos retos son el control y operación optimizada de microrredes. También, el comercio de energía en una microrred, tema que ya se abordó en el Apartado 2.1.

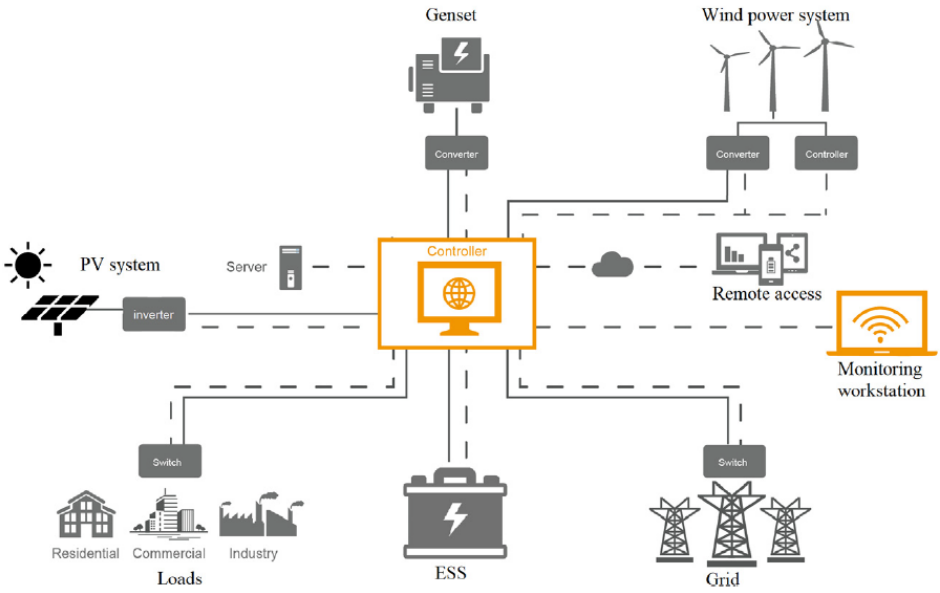


Figura 2-21. Esquema de una microrred tipo [103]

En la Figura 2-21, se muestra un esquema típico de una microrred. Se observa como una parte fundamental en una microrred es un sistema de control que coordine los activos de la red: cargas, generación distribuida y sistemas de baterías.

Las microrredes son sistemas eléctricos altamente descentralizados donde en las actividades típicas de su operación como comercio de electricidad, control y optimización de recursos intervienen diversas partes. *Blockchain*, debido a su naturaleza, es aplicable a muchas de estas áreas dentro de la operación de una microrred, aportando algunas ventajas y beneficios [106].

Algunas funciones donde *blockchain* puede ser útil dentro de la operación de microrredes son [67], [107]:

- Diseño de arquitecturas que faciliten el control y optimización de recursos energéticos distribuidos. Mediante *blockchain* y *smart contracts* el rol de operador de la microrred puede ser sustituido por un modelo descentralizado, asegurando una operación trasparente y segura sin la intervención de una compañía eléctrica u operador.
- Uso de *smart contracts* para programar los recursos de la microrred, como generadores, baterías y cargas controlables. Además, pueden implementarse modelos de Flujo Óptimo de Potencia (OPF por sus siglas en inglés) utilizando algoritmos de optimización descentralizados.
- Los *smart contracts* pueden trabajar como autoridades de control distribuidas, que cuenta con la confianza de todos los usuarios de la microrred. Uno de los aspectos de control más importantes en una microrred es el control de voltaje. Para abordar este problema pueden implementarse de algoritmos de control basado en Flujos de Potencia Reactiva Óptimos (ROPF, por sus siglas en inglés). Además, pueden emplearse esquemas de control donde todos los usuarios contribuyan al control de voltaje de una forma justa, y sean remunerados según su aportación a esta regulación.
- Dentro de los esquemas de control, también pueden implementarse modelos de respuesta de la demanda, incentivando a que los usuarios colaboren con la optimización y eficiencia en la operación de la red.
- Con *smart contracts* se pueden desarrollar sistemas de pago virtuales. Además de utilizarse para pagos en aplicaciones de mercados eléctricos, pueden emplearse en sistemas de remuneración para actividades como respuesta de la demanda y contribución a la regulación de la red (como inyección de reactiva o deslastre de cargas).

#### 2.3.2.1 Caso de estudio: Control distribuido con *blockchain* para regulación de voltaje en una microrred asegurando la equidad entre usuarios

Tal y como se muestra en la Figura 2-21, uno de los componentes fundamentales es una microrred es su sistema de control. El sistema de control es el encargado de asegurar la calidad del suministro y de optimizar la operación de la red, enviando consignas a los recursos disponibles en la red como inversores inteligentes y cargas despachables. Con el uso de *blockchain*, pueden implementarse sistemas de control distribuido, dando solución a algunos de los retos que la operación de microrredes presenta, y de una forma más eficiente que con soluciones centralizadas tradicionales.

Uno de los problemas que habitualmente se da en microrredes es el control de voltaje dentro de unos límites aceptables. Debido principalmente a que el comportamiento típico de los recursos de generación instalados en la red es operar a su máxima capacidad, sin tener en cuenta las condiciones de la red. Especialmente en redes con alta presencia de generación fotovoltaica, pueden darse caso de sobrevoltaje cuando la generación es elevada y el consumo local reducido. Una solución para prevenir estos casos es el control de los inversores de las instalaciones fotovoltaicas, bien mediante *curtailment* de potencia activa o ajustes en su potencia reactiva.

A continuación, se presenta una propuesta de control distribuido donde los usuarios con instalaciones fotovoltaicas en una red colaboran para mantener los valores de voltaje dentro de los límites, asegurando que todos los usuarios participan de forma equitativa. Utilizando *blockchain* se implementa un *smart contract* que actúa como autoridad de confianza del control distribuido [75].

Se considera una microrred compuesta por varios circuitos o *feeders* en baja tensión y con una alta presencia de generadores fotovoltaicos, tal y como se muestra en la Figura 2-22. Los usuarios hacen un esfuerzo común para mantener los valores de voltaje de la red dentro de los límites aceptables. Para ello, en cada circuito es elegido de forma alternativa una instalación fotovoltaica que actuará como regulador de voltaje.

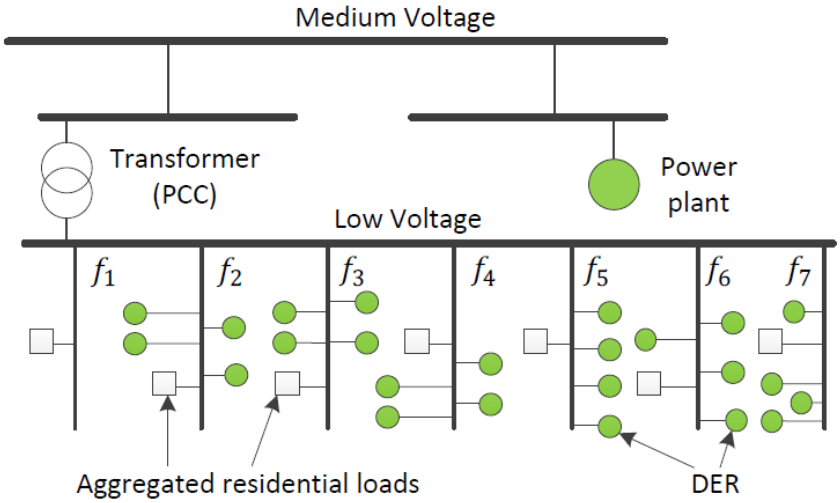


Figura 2-22. Esquema de la microrred. Compuesta por varios circuitos de baja tensión (f1 a f7). El transformador MT/BT es el punto de frontera físico de la microrred (PCC). [75]

Las instalaciones fotovoltaicas se conectan a la red mediante inversores de potencia inteligentes, capaces de operar en modo de entrega máxima de potencia, usando un algoritmo de seguimiento de máxima potencia, o en modo de control de voltaje. La regulación de voltaje se hace a través de un lazo de control *droop*, que puede implicar una disminución en la potencia activa entregada, con la consiguiente merma económica del usuario.

En el sistema propuesto, los usuarios con generación distribuida son incentivados a participar en la regulación de voltaje a través de un sistema de reparto de créditos. Para ello, en cada periodo de control, se escoge a una instalación por cada circuito y se redistribuyen los créditos de la siguiente manera:

- Cada usuario con generación distribuida envía una cantidad de créditos. Esta cantidad la determina estratégicamente, atendiendo a sus intereses particulares.
- Por cada circuito, se elige al usuario que envía una menor cantidad de créditos, para actuar como controlador de voltaje en el siguiente periodo de control.

- El usuario elegido recibe los créditos enviados previamente por el resto de usuario.

Los créditos, cuyo número total en circulación es constante, se redistribuyen recolectando los créditos enviados por todos los usuarios y entregándoselos al usuario que actúa como regulador de voltaje. De esta forma, los usuarios con pocos créditos tienen altas posibilidades de actuar como reguladores. Por otro lado, estos usuarios tienen pocos créditos porque con anterioridad no han actuado frecuentemente como reguladores. Con este sistema, a largo plazo y con suficientes periodos de control, se asegura que los usuarios participan de forma equitativa en el control de voltaje.

Para actuar como autoridad de control de forma distribuida, se implementan varios *smart contracts*, uno por cada circuito, todos desarrollados sobre una misma *blockchain*.

Durante cada periodo de control los usuarios transfieren al *smart contrat* su propuesta de créditos para el siguiente periodo de control. Cuando todos los usuarios envían su propuesta, el *smart contract* automáticamente elige el generador que deberá actuar como controlador, y notifica el resultado a todos los generadores para que adapten su modo de funcionamiento. Posteriormente, el *smart contract* transfiere los créditos recolectados previamente al usuario elegido para regular el voltaje en su circuito. Cada cambio en el estado de los *smart contract* es almacenado en nuevos bloques que son añadidos a la cadena y propagados a toda la red *blockchain*. Este proceso se muestra en la Figura 2-23. En verde y rojo se representa el envío y recepción de créditos respectivamente. El envío de créditos consiste en una transacción de créditos al *smart contract* (flechas azules), que actualiza su estado incluyendo las nuevas transacciones de créditos cada vez que se mina un nuevo bloque (indicado con equis azules). Antes del comienzo del nuevo periodo de control, el *smart contract* se bloquea (flecha de color morado) y automáticamente elige y distribuye el generador elegido. Por último, el *smart contract* envía los créditos actualizando nuevamente su estado, que se consolidará con su inclusión en un nuevo bloque.

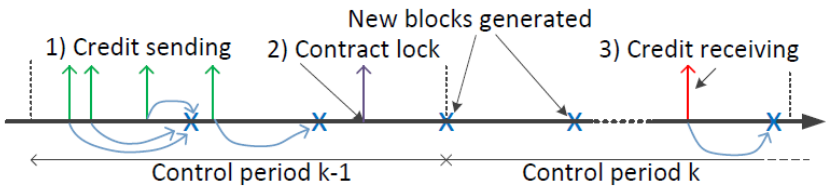


Figura 2-23. Secuencia de intercambio de comunicaciones [75]

#### 2.3.2.2 Caso de estudio: Transacciones descentralizadas en microrredes interconectadas

En lugares donde las redes de distribución clásicas pasen a configurarse como microrredes autónomas, se dará el caso en el que estas microrredes no sólo interactúen con la red de distribución, sino que también lo harán con otras microrredes cercanas, estando interconectadas entre sí. Así, los sistemas de distribución se convertirían progresivamente en una red de microrredes autónomas, capaces de manejar flujos de energía e información bidireccionales.

Las microrredes interconectadas ofrecen una solución flexible y escalable algunos problemas en la modernización de las redes de distribución. Suponen una manera de aumentar la penetración de recursos de energía distribuidos. Contribuyen a mejorar la eficiencia y seguridad de los sistemas de distribución debido a que responden mejor a las condiciones dinámicas de operación causadas por la variabilidad en la producción de los generadores distribuidos. Las microrredes interconectadas son más fiables que las microrredes individuales, ya que cada una de ellas puede ofrecer sus reservas al resto, reduciendo la probabilidad de cortes de suministro. También tienen mayores posibilidades de resistir ciberataques.

La proliferación de microrredes conectadas a la red también puede complicar la operación de la red de distribución. Por ejemplo, algunas premisas básicas en los sistemas de protecciones y análisis de la seguridad se han visto alterados con la aparición de flujos de energía bidireccionales. Por esto, las redes de distribución deben adaptarse para hacer frente a estos nuevos retos.

Para integrar la participación de microrredes en los sistemas de distribución, una evolución natural sería la implementación de señales económicas basadas en mercados para incentivar que las microrredes compartan sus recursos. En última instancia, estas señales económicas influirán en la forma de planear y operar los

sistemas eléctricos de distribución y transporte.

Los Operadores de Distribución pueden formar un sistema de comercio de energía a nivel de comercialización minorista donde las microrredes son participantes del mercado e interactúan para efectuar intercambios de energía de forma *peer-to-peer*. Estos sistemas son llamados sistema de energía transactiva (*transactive energy*) [108]. En la Figura 2-24 se muestra la comparación entre un esquema convencional y un esquema de energía transactiva.

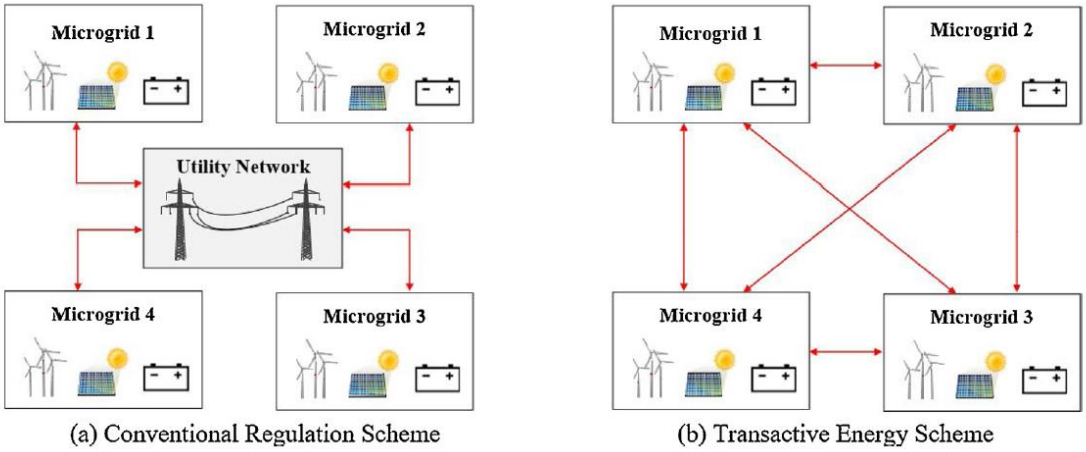


Figura 2-24. Organización de microrredes en sistemas de distribución [108]

La operación de sistemas de energía transactiva puede hacer frente a un nivel de complejidad elevado, donde ahora los sistemas de distribución, además de gestionar los flujos de energía, deben gestionar el mercado y las transacciones financieras, con transparencia y dando confianza a los participantes.

Las microrredes son consideradas como prosumidores agregados, con capacidad para producir, consumir y almacenar energía. El controlador de la microrred (MC en la Figura 2-25) es el elemento central de comunicación, coordinación y gestión de la operación. El controlador gestiona varios recursos internamente en su microrred, y se encarga de participar en el sistema de energía transactiva. Por otro lado, el Operador de Distribución (DSO en la Figura 2-25) participa en el sistema, mediando entre este y el mercado mayorista y asegurando el cumplimiento de los requisitos de seguridad.

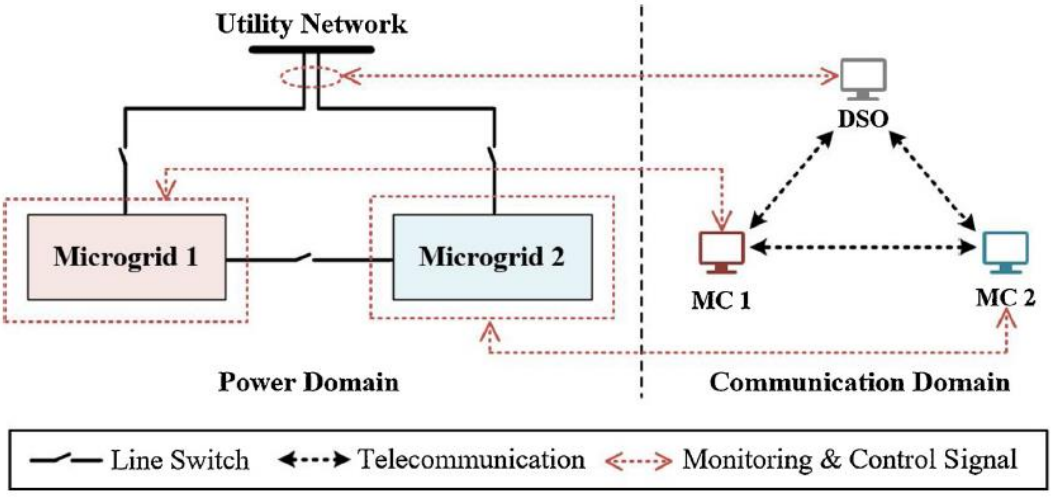


Figura 2-25. Comunicaciones en microrredes interconectadas [108]

Por otro lado, es necesario prevenir comportamientos maliciosos o descuidados que obstaculicen la normal operación del mercado y que incluso pueden provocar la desestabilización física del sistema. La privacidad es otro tema relevante: los participantes deberían evitar compartir información sensible de tipo comercial (como cantidad de generación local o costes de producción) y de tipo operacional (estado de operación o márgenes de seguridad).

En [109] se propone un sistema descentralizado de energía transactiva seguro, escalable y eficiente que trata de hacer frente a los problemas expuestos anteriormente, con el uso de *blockchain*. El sistema propuesto está formado por tres capas funcionales, como se muestra en la Figura 2-26. La capa física representa la infraestructura física de distribución eléctrica, incluyendo la red de microrredes y la red de distribución. La capa cibernética representa la infraestructura de comunicación e información, incluyendo *hosts* de comunicación, y dispositivos de control para intercambio de información y control automático. La capa de mercado representa las interacciones financieras entre participantes del mercado que interactúan y compiten para conseguir transacciones de energía óptimas. La capa cibernética recolecta y agrega las condiciones de operación de la capa física, para la toma de decisiones en la capa de mercado. También, automatiza la ejecución de intercambios de energía fijados en la capa de mercado mediante la operación real de la infraestructura de la capa física.

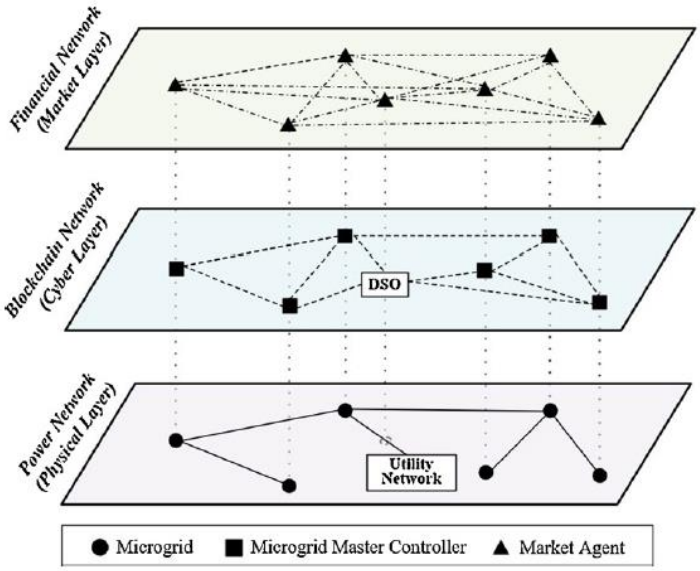


Figura 2-26. Sistema basado en *blockchain* para microrredes interconectadas [108]

Para automatizar y dar seguridad a las interacciones entre los controladores de las microrredes y el Operador de Distribución en la capa cibernética, se utilizan redes *blockchain*. La base de datos de *blockchain* es compartida entre las microrredes y el operador para auditar la integridad y validez de los datos de intercambios de energía en la capa física y las transacciones comerciales en la capa de mercado.

En un esquema tradicional, tal y como muestra en la Figura 2-27 (a), cada microrred mantendría una base de datos local con los registros de su operación, y se comunicaría con el Operador (intermediario central de confianza) para validar los datos. Esta forma de almacenar y gestionar la información de forma separada, que está sujeta a ineficiencias y vulnerable a ciberataques, no es apta para soportar la escalabilidad necesaria. Mediante el uso de *blockchain*, puede mantenerse una base de datos descentralizada y que no requiera un intermediario central, tal y como se muestra en la Figura 2-27 (b). Los nuevos registros de condiciones de operación son empaquetados en un bloque de información al final de una cadena de bloques por un minero, elegido en función del método de consenso implementado. En esta propuesta, el minero encargado de crear un nuevo bloque se elige mediante un método basado en la reputación de los participantes, teniendo mayor probabilidad de crear un bloque aquellos con mayor reputación. Una vez grabado en la *blockchain*, esta información no puede ser alterada ya que todos los participantes han alcanzado un consenso en cuando a la validez de la información.

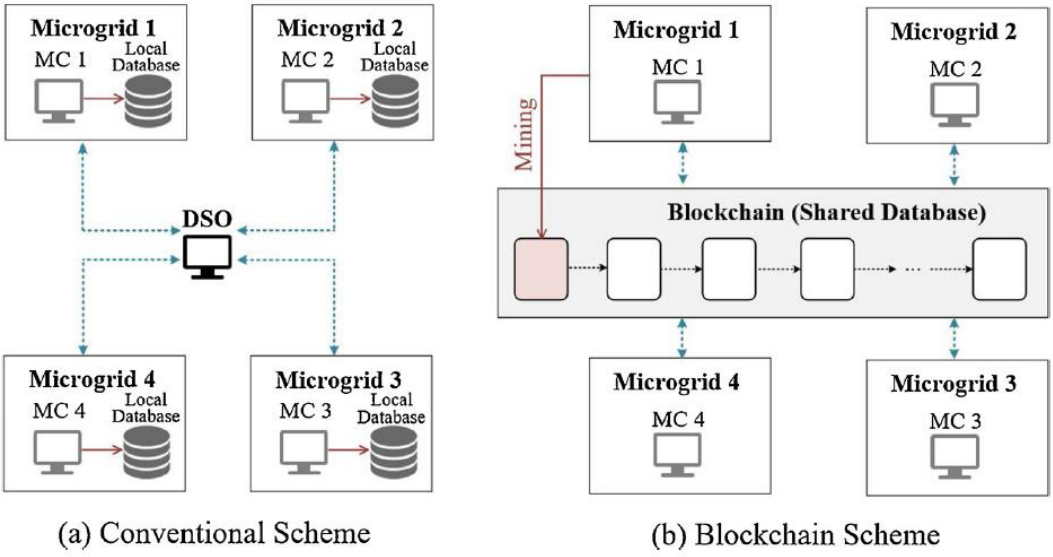


Figura 2-27. Almacenamiento de datos para microrredes interconectadas [109]

En [109] se propone el uso de cuatro *blockchain*s interoperables de tipo *permissioned*, cada una de ellas con tipos de datos distinto y con un propósito concreto. Sobre estas redes se despliegan *smart contracts* especialmente diseñados para lograr ciertos objetivos. De esta forma, el sistema de energía transactiva propuesto se divide en cuatro etapas, tal y como se muestra en la Figura 2-28. En la primera etapa (inicialización de mercado), el operador de distribución configura la topología de la red y ajusta la lista de microrredes que pueden participar en el comercio de energía. En la segunda etapa (comercio de energía), los participantes del mercado emiten sus ofertas de generación y consumo, para la casación de oferta y demanda. En la tercera etapa (estimación de estado), los participantes comparten información local de su estado de operación en sus límites físicos (puntos de acoplamiento) para estimar el estado de operación y conocer las transferencias de energía reales. En la cuarta etapa (liquidación de mercado) los participantes de mercado liquidan los intercambios de energía realizados, teniendo en cuenta las diferencias entre las transferencias comprometidas en la fase de mercado y las realmente efectuadas. Para limitar los impactos financieros y físicos de participantes con intenciones maliciosas o descuidadas, a cada participante se le asocia un indicador de reputación que refleja la honestidad de su comportamiento basada en su historial de transacciones. Cuando el comportamiento de un participante no sea adecuado, será penalizado disminuyendo su indicador de reputación. Si el indicador de reputación cae por debajo de un nivel determinado, el participante será expulsado del sistema.

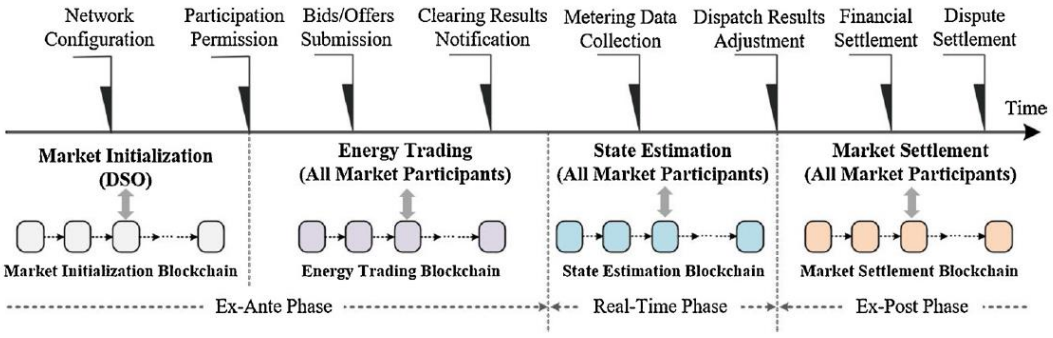


Figura 2-28. Etapas del sistema de energía transactiva basado en varias *blockchain*s [109]

Los datos originados durante las cuatro etapas son muy heterogéneos y con orígenes muy distintos (información topológica, ofertas de mercado, lecturas de contadores, liquidaciones financieras y pagos, etc). Por esto, la creación y mantenimiento de registros de datos tan diferentes y con múltiples escalas temporales, puede tener una implementación problemática si quiere hacerse en una sola red *blockchain*. En su lugar, se propone la creación de varias *blockchains* trabajando solapadas.

A continuación, se detalla el funcionamiento de cada una de estas cuatro *blockchains* propuestas:

- **Inicialización de mercado**

En cada ronda de negociación de energía, el operador de distribución determina una configuración de la red física, esto facilita el proceso de casación y contribuye a la eficiencia y seguridad del suministro. El operador determina la configuración de forma estratégica, basada en la experiencia o mediante el uso de herramientas como el *machine learning*, a la vez que tienen en cuenta algunas consideraciones como: excluir componentes de la red que están fuera de servicio, asegurar la calidad del suministro (valores de frecuencia y voltaje) y maximizar los beneficios ambientales y económicos (por ejemplo, reduciendo pérdidas en la distribución).

Parea mantener la privacidad de los participantes, el operador asigna a cada microrred un seudónimo generado aleatoriamente que es usado temporalmente para ocultar la identidad de la red. Esto reduce las posibilidades de exponer sus patrones de oferta y sus beneficios.

El operador difunde los datos de inicialización del mercado incluyéndolos en la *blockchain*, y las microrredes aceden a la *blockchain* para obtener su seudónimo y la información topológica. La información compartida se asegura mediante criptografía asimétrica, donde el operador encripta la información sensible de cada microrred utilizando la clave pública de ésta. La microrred utiliza su clave privada para leer la información. En la Figura 2-29 se muestra este proceso, por ejemplo, la microrred 1 sólo tiene acceso su seudónimo (0x8f1) utilizando su clave privada.

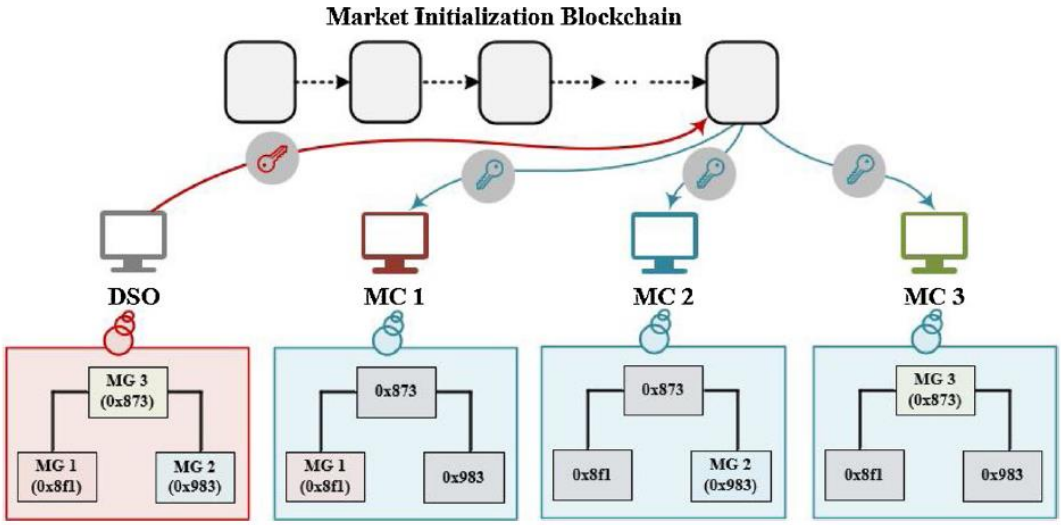


Figura 2-29. *Blockchain* para el proceso de inicialización de mercado [109]

- **Mercado de energía**

Cada participante del mercado, utilizando las señales de precio y la información que tiene disponible, elabora una estrategia de oferta. Como se muestra en la Figura 2.30, los participantes aprueban sus estrategias de oferta utilizando su clave privada, entonces estas ofertas son almacenadas en la *blockchain* sin posibilidad de alteración posterior.

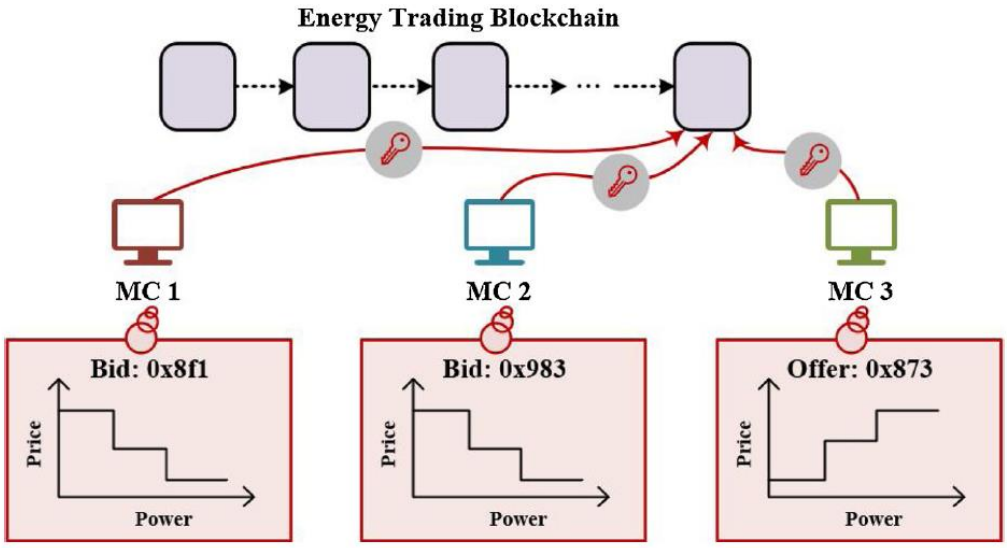


Figura 2-30. *Blockchain* para el proceso de presentación de ofertas [109]

Una vez que todas las ofertas son recolectadas, se determina de forma descentralizada la cantidad y precios de la energía intercambiada, considerando las restricciones técnicas de la red. El proceso de casación se efectúa resolviendo de forma descentralizada un algoritmo de flujo de potencia óptimo con restricciones técnicas (DSCOPF por sus siglas en inglés). La solución se obtiene mediante iteraciones donde cada microrred resuelve un DSCOPF local y el resultado se envía a un *smart contract* (coordinador) que ejecuta el paso agregado. Así, se evoluciona de decisiones óptimas locales a un equilibrio óptimo global que marca la programación de transferencias de energía. Las cantidades y precios de la programación de transferencias de energía se graban en la *blockchain*.

En la Figura 2-31, se ilustra el proceso donde tres microrredes interactúan con el *smart contract* (*Energy Coordination*), resolviendo el problema de optimización y obteniendo como resultado el consenso en la programación energética, que es incluido en la *blockchain*. Además, se observa como el *smart contract* toma de la *blockchain* de inicialización de mercado la configuración de la red.

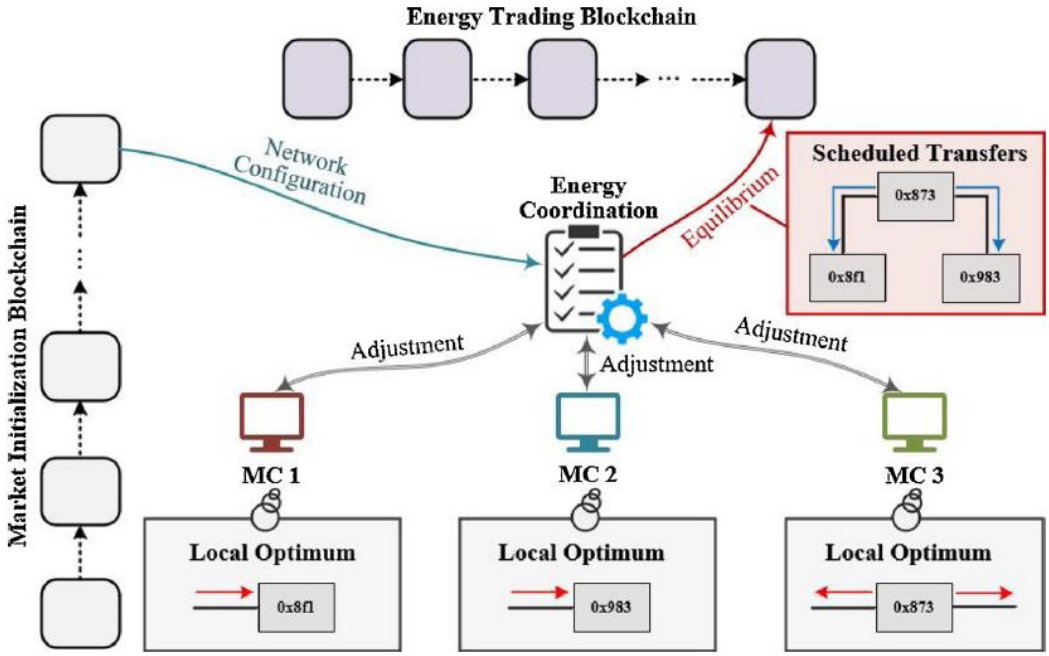


Figura 2-31. *Blockchain* para el proceso de casación de oferta y demanda [109]

- **Estimación de estado**

Durante los periodos en los que existen intercambios de energía comprometidos en la fase de mercados, los

participantes deben monitorizar y compartir las mediciones y estados de operación en los límites físicos de su microrred. Estas mediciones son tomadas de contadores inteligentes y PMU. De esta forma, los participantes colaboran en el proceso de estimación de estado descentralizado que contribuye al consenso en las cantidades de energía que realmente son transferidas.

Tal y como se muestra en la Figura 2-32, la estimación de estado se realiza mediante un *smart contract*, con accesos a la configuración de la red (almacenada en la *blockchain* de inicialización de mercado), y que, partiendo de la estimación de estado efectuada localmente por las microrredes, alcanza en un número finito de iteraciones el estado de operación en cada frontera de pares de microrredes. En consecuencia, de la estimación de estado pueden deducirse las transferencias de energía reales, que son almacenadas en la *blockchain* de estimación de estado.

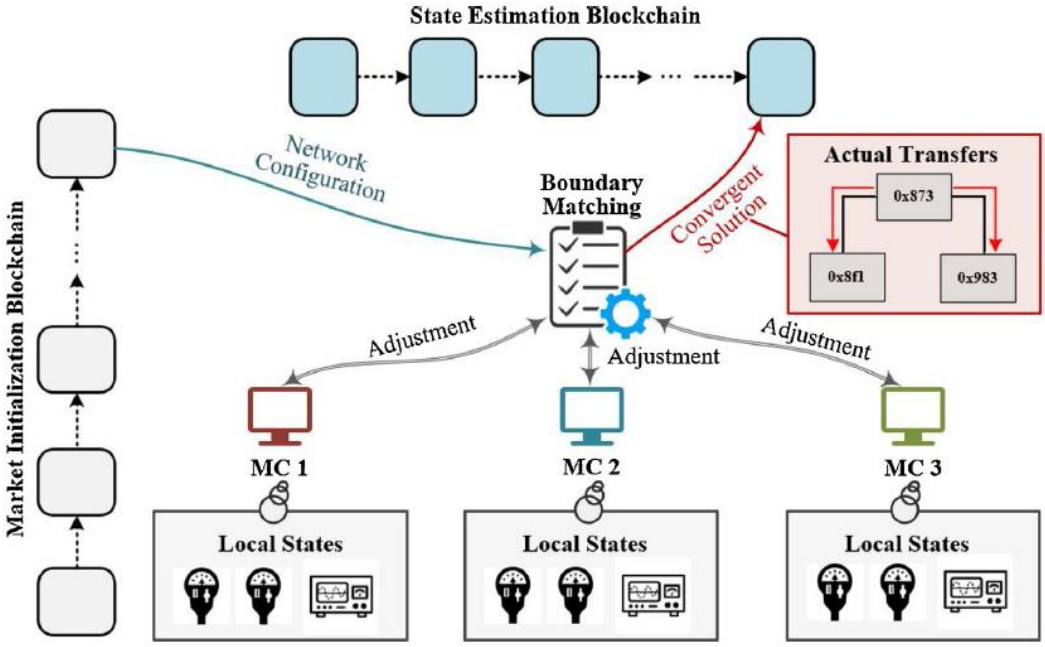


Figura 2-32. *Blockchain* para el proceso de estimación de estado [109]

- **Liquidación de mercado**

Una vez que la estimación de estado está disponible, la liquidación económica se efectúa automáticamente mediante *smart contracts*. Los ingresos o pagos de los participantes se determinan en base a las transferencias de energía reflejadas en los resultados de estimación de estado. En un escenario ideal, todos los participantes intercambian energía tal y como estaba planeado en la programación de mercado, registrada en la *blockchain* de mercado. Sin embargo, las cantidades transferidas pueden sufrir desviaciones respecto a las comprometidas en la programación, en este caso los participantes deberán pagar tasas adicionales para compensar el balance de energía necesario en el sistema. Las diferencias provocadas por estas desviaciones pueden ser compensadas bien por intercambios de energía con la red y el mercado mayorista, o por alguna microrred que actúe como *bus slack*.

Cuando la diferencia entre las cantidades de energía comprometidas y las reales superen un umbral determinado, los participantes serán penalizados reduciendo la puntuación de reputación.

Los resultados de la liquidación económica y los cambios en la reputación de los participantes son almacenados en la *blockchain* de liquidación del mercado. Los datos de pagos y beneficios son almacenados utilizando el seudónimo de los participantes, preservando la privacidad de esta información sensible. Por el contrario, la actualización de reputación se almacena asociada a la identidad de cada participante, para identificar a participantes maliciosos y contribuyendo a la selección de mineros encargados de extender las *blockchains* con nuevos bloques. Los participantes del mercado también tienen acceso a su balance actual, que es encriptado por el *smart contract* mediante la clave pública de cada uno de ellos, pudiendo consultarse solamente mediante la clave privada de éstos. En la Figura 2-33 se ilustra este proceso, las tres microrredes son notificadas de los movimientos financieros, de la reputación de cada participante y de su propio balance

financiero actualizado.

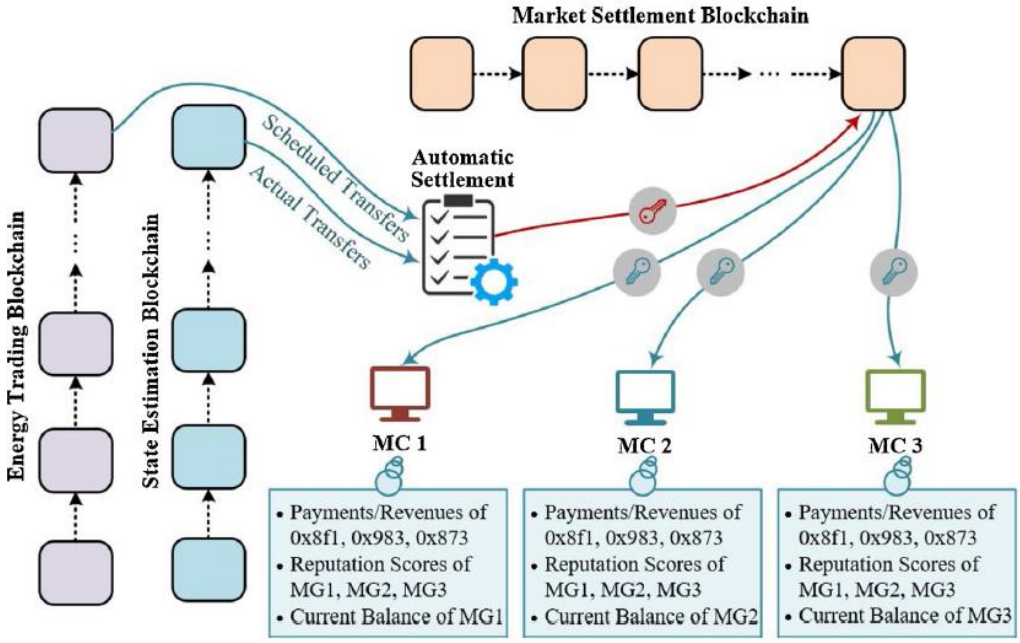


Figura 2-33. *Blockchain* para el proceso de liquidación de mercado [109]

### 2.3.3 Servicios complementarios y respuesta a la demanda

El incremento de generación renovable y distribuida, así como la previsión de un aumento en la demanda eléctrica, han intensificado la necesidad de mejorar la flexibilidad en la operación de los sistemas eléctricos. El objetivo es mantener el equilibrio entre la generación y la demanda, y asegurar condiciones de operación que garanticen la estabilidad del sistema. Para afrontar estos retos, dentro del marco de evolución hacía redes inteligentes, se están proponiendo nuevos esquemas de servicios de ajuste en la operación de redes eléctricas. Estos nuevos esquemas involucran la participación de la demanda, dotada cada vez más de nuevos elementos que pueden aportar flexibilidad como generación, almacenamiento, vehículo eléctrico y hogares inteligentes con sistemas de gestión de energía (HEMS por sus siglas en inglés).

Algunas de las arquitecturas de control que pueden utilizarse para el control de demanda son [95]:

- **Control directo de cargas**

El control directo de cargas es un esquema con una arquitectura sencilla (ver Figura 2-34) en el que el operador de distribución está directamente conectado con las cargas de los consumidores. Por ejemplo, el operador puede controlar los sistemas de climatización, calentadores de agua caliente u otras cargas controlables en industrias, sin la mediación del consumidor. A cambio, los propietarios reciben una compensación o reducción en su factura eléctrica por permitir el ajuste de sus cargas, dentro de lo acordado con la *utility*.

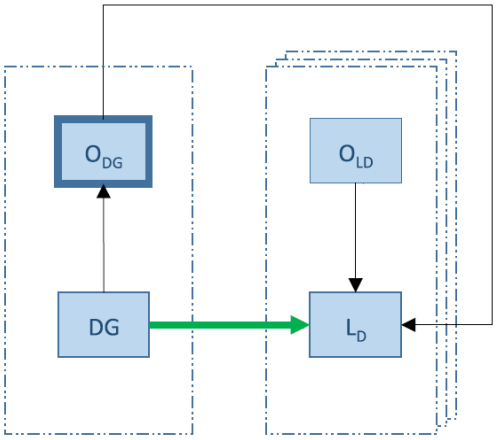


Figura 2-34. Esquema de control directo. La flecha verde simboliza el flujo de energía eléctrica y las negras las comunicaciones y control. El operador ($O_{DG}$) de la red de distribución (DG) controla directamente las cargas del consumidor ($L_D$), puenteando al propietario u operador de las cargas ($O_{LD}$). [95]

Además de controlar cargas, el control directo puede utilizarse para controlar otros elementos de los usuarios como generadores o almacenamiento, por ejemplo, efectuando *curltailment* (reducción de inyección de potencia) o controlando la inyección de potencia reactiva mediante los inversores de potencia.

Los servicios de ajuste, especialmente el de regulación de frecuencia, son una aplicación interesante para el control directo de cargas, debido a que es necesaria la respuesta en pocos segundos. El control directo de cargas tiene una respuesta más rápida que la respuesta automática de la demanda, especialmente cuando en éstos las señales pasan por agregadores intermediarios [106], [110].

- **Respuesta automática de la demanda**

En la respuesta de la demanda, a diferencia del control directo, el propietario de la instalación mantiene el control sobre el ajuste de los activos.

Los programas de repuesta a la demanda son inicializados por el operador de la red o *utility*, normalmente a través de intermediarios que agregan las cargas de varios usuarios finales y que finalmente envían señales a los consumidores para modificar el comportamiento de sus cargas o activos (ver Figura 2-35). Igual que en el caso anterior, además de cargas, la respuesta a la demanda puede involucrar el control de otros recursos como generación y almacenamiento.

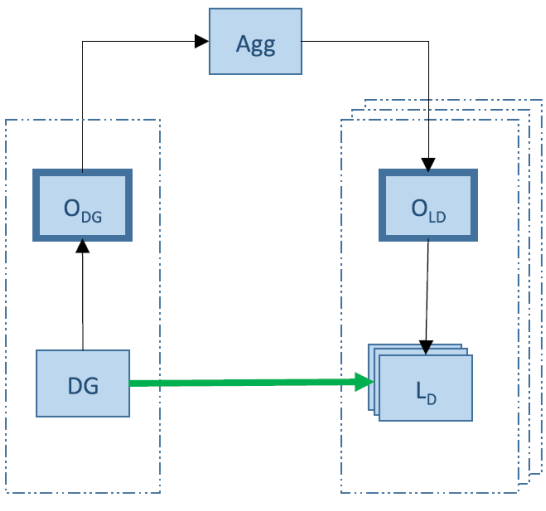


Figura 2-35. Esquema de respuesta de la demanda. La flecha verde simboliza el flujo de energía eléctrica y las negras las comunicaciones y control. El Operador ($O_{DG}$) de la red de distribución (DG) comunica una señal a un agregador (Agg). A su vez, el agregador gestiona internamente el control de las cargas. [95]

Un tipo de carga que está teniendo una particular atención en las publicaciones científicas es el vehículo eléctrico. Debido a la previsión del aumento de vehículos eléctricos y a que se trata de una carga controlable, que también puede actuar como almacenamiento, se le considera una de las piezas clave en el futuro de las redes inteligentes. En este sentido, los vehículos eléctricos pueden adoptar un rol importante en la mejora de la resiliencia de la red, contribuyendo en la respuesta a la demanda y en la reducción de picos y valles de demanda. Sin embargo, gestionar un gran número de vehículos en la red supone algunos retos, como la implementación de sistemas de programación de carga, uso de tecnologías de comunicación avanzadas, y desarrollo de mecanismos de carga confiables. Por eso, el uso de las nuevas tecnologías y herramientas en redes inteligentes es fundamental para evitar sobrecargas en la red y asegurar la privacidad y seguridad. Debido la naturaleza de operación descentralizada de las infraestructuras de carga de los vehículos eléctricos, *blockchain* y los *smart contracts* puede ayudar a hacer frente en estos retos [111]. En la Figura 2-36 se muestra un esquema simplificado de interacción entre *blockchain* y vehículos eléctricos para mejorar la seguridad y privacidad de la información y la seguridad de transacciones financieras.

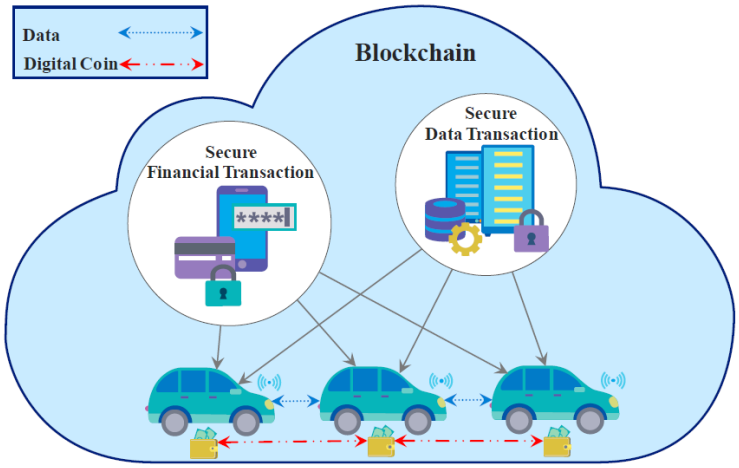


Figura 2-36. Esquema simple de interacciones entre una red *blockchain* y vehículos eléctricos en una *smart grid*. [111]

En general, algunas funciones donde *blockchain* puede ser útil dentro de la implementación de sistemas de servicios complementarios y respuesta a la demanda son [106], [111]–[114]:

- Los agregadores en los sistemas de respuesta a la demanda actúan como intermediarios y deben implementar métodos que permitan la comunicación con los consumidores eficazmente. Mediante el uso de *blockchain* y *smart contracts* el control de las cargas y la comunicación, pueden efectuarse de manera más eficiente, registrando transacciones y automatizando procesos. Además, el propio agregador, que habitualmente es una tercera parte centralizada, puede ser sustituido por un agregador descentralizado mediante *smart contracts*.
- La información relativa al proceso de respuesta a la demanda almacenada automáticamente en una *blockchain* puede ser verificada por todas las partes, aportando transparencia y trazabilidad de la información, ayudando en los procesos de liquidación de incentivos. Los datos pueden incluir señales enviadas por los operadores de distribución, variaciones de potencia en las cargas, desviaciones, etc.
- Los registros incluidos en una *blockchain* están encriptados, aportando privacidad y seguridad, sin que sea necesario ceder los datos a terceras partes como los servicios de agregación tradicionales. La privacidad en sistemas distribuidos de respuesta a la demanda es muy relevante debido a que los datos de consumo eléctrico se consideran información personal [115].
- Mediante *blockchain* y *smart contracts*, pueden habilitarse pagos automatizados, seguros y más ágiles a los usuarios, acorde a los acuerdos previamente pactados.

#### 2.3.3.1 Caso de estudio: Agregación de consumidores para un sistema de respuesta a la demanda

A continuación, se describe un sistema de agregación de consumidores para servicios de respuesta a la

demanda propuesto en [116]. El uso de *blockchain* y *smart contracts* permite la creación de un sistema distribuido, en el que los consumidores interactúan directamente con el operador de la red de forma transparente, segura y automatizada, para proveer de servicios de flexibilidad a la red.

En esta propuesta se plantea un escenario en el que el operador de la red requiere a los consumidores una modificación en su consumo, para cumplir con requerimientos técnicos de la red. El operador envía consignas de respuesta a la demanda, dentro del rango de la flexibilidad disponible, obtenida de la suma de flexibilidad total de los consumidores. Finalmente, los consumidores son remunerados en función del cumplimiento de la consigna de reducción de consumo. El cumplimiento se evalúa comparando el comportamiento de los consumidores con su línea base de consumo.

La línea base de consumo, es el perfil de consumo típico de un consumidor, y permite evaluar si los cambios en el consumo se deben a las indicaciones de respuesta a la demanda o no. La diferencia entre la línea base de consumo y el consumo real, representa el desempeño de cada cliente al programa de respuesta a la demanda. Por esto, el cálculo de la línea base es crucial para el buen funcionamiento de este tipo de programas de respuesta a la demanda. Se calcula utilizando el histórico de medidas tomadas de los contadores eléctricos, y existen distintas metodologías para su cálculo [117]. En este ejemplo se propone la metodología *HighXofY*, que utiliza como estimación para cada hora la media de los X consumos mayores durante los últimos Y días sin eventos de respuesta a la demanda. Los días Y son tomados categorizándolos en grupos (días entre semana, fines de semana, vacaciones, etc). El efecto de estacionalidad se minimiza al ser Y una ventana móvil de los últimos días.

La flexibilidad de cada consumidor para modificar su comportamiento se calcula mediante el perfil de disponibilidad. El perfil de disponibilidad representa la disposición de un consumidor a responder a los requisitos del operador. Se recalcula en cada evento de respuesta a la demanda, en función del desempeño que el consumidor tiene durante los pasado eventos.

Los diferentes pasos del programa de respuesta a la demanda propuesto son los siguientes:

1) Los contadores inteligentes miden el consumo energético de los clientes. A través de una aplicación cliente, los datos de mediciones se envían a la *blockchain*.
2) Se calculan las líneas base y los perfiles de disponibilidad mediante funciones programadas en un *smart contract*.
3) El operador de la red notifica un evento de necesidad de respuesta a la demanda en la *blockchain*, incluyendo el día, ventana temporal y cantidad de potencia a disminuir o aumentar.
4) En función de las líneas base y los perfiles de disponibilidad, el *smart contract* distribuye la potencia total requerida en la consigna del operador entre los consumidores.
5) Los consumidores leen de la *blockchain* la carga necesaria a reducir, y que ha sido calculada por el *smart contract* para cumplir con la demanda del operador.
6) El consumo durante la duración del evento de respuesta a la demanda se registra en los contadores y en la *blockchain* (como se explica en los pasos 1 y 2).
7) El *smart contract* evalúa si los consumidores han cumplido con la consigna recibida y son remunerados mediante *tokens* en función de su grado de cumplimiento.

Además, para facilitar la adaptación de los consumidores a las consignas de potencia que reciben del *smart contract* (punto 5), estas pueden integrarse en un HEMS (sistema de gestión energética del hogar) [118]. En hogares inteligentes con cargas tipo IoT, el sistema de gestión energética del hogar puede ajustar y programar cargas automáticamente según unos parámetros definidos por el usuario.

#### 2.3.3.2 Caso de estudio: Comunidad de estaciones de recarga de vehículo eléctrico con servicio de regulación de frecuencia

Los vehículos eléctricos pueden ser utilizados para proveer ciertos servicios a la red, actuando como almacenamiento, como reserva rodante o colaborando en la regulación de frecuencia y voltaje. Para ello, el mayor reto es el desarrollo infraestructuras de carga que se integren con la red y con tecnologías de información y comunicación capaces de proveer estos servicios. En [119] se propone un sistema para monitorizar y proveer regulación de frecuencia mediante estaciones de carga de vehículos eléctricos organizados en comunidades.

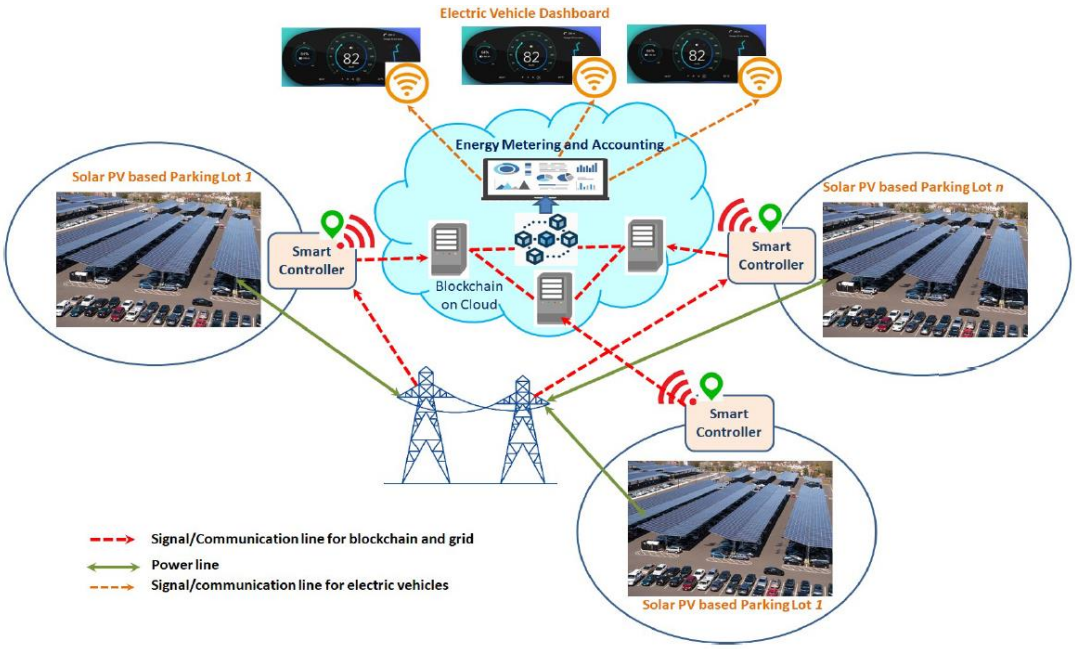


Figura 2-37. Arquitectura de la infraestructura propuesta [119]

En la Figura 2-37 se muestra la arquitectura de la propuesta. Cada estacionamiento cuenta con una instalación fotovoltaica y estaciones de recarga de vehículo eléctrico, conectadas a la red. Cuando la regulación de frecuencia es necesaria, la energía almacenada en los vehículos y la generada por el sistema fotovoltaico es inyectada en la red. Cuando la regulación de frecuencia no es necesaria, la energía producida se utiliza para cargar los vehículos, tomando de la red cuando ésta no sea suficiente. El estado de carga de cada vehículo y la información de transacciones de energía son almacenadas en la *blockchain*. Los propietarios pueden visualizar la información del estado de carga y los detalles de las transacciones de energía y financieras en el panel de su vehículo.

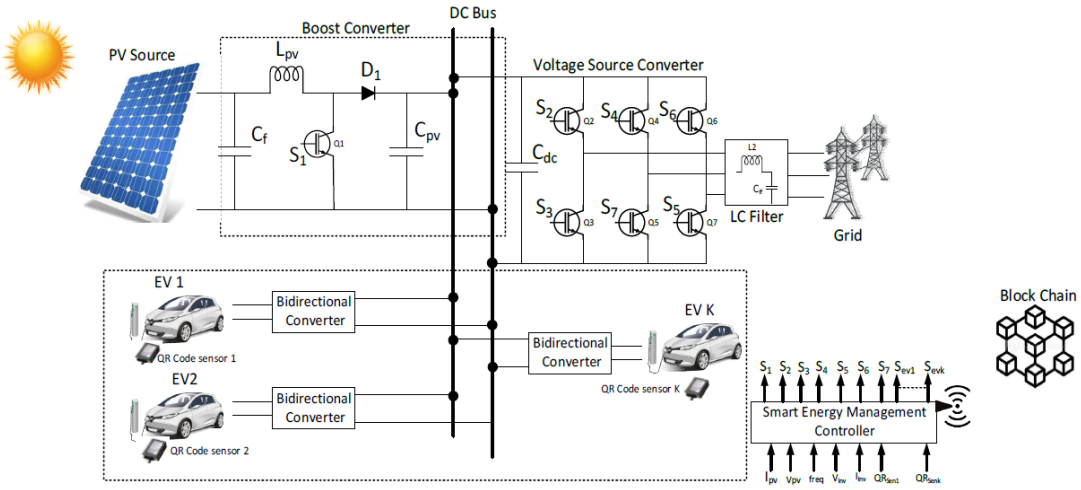


Figura 2-38. Esquema detallado de la infraestructura de los estacionamientos [119]

En la Figura 2-38 se muestra un esquema detallado de la infraestructura de carga, compuesta por paneles solares con su conversor para maximizar la potencia generada, un inversor para integrar el sistema con la red, cargadores de vehículos bidireccionales y un controlador inteligente de gestión de la energía (SEMC por sus siglas en inglés).

El SEMC se encarga de operar el sistema, calcular la potencia disponible para regulación de frecuencia y de ejecutar los *smart contracts*, actualizando la información del estado de los vehículos en la *blockchain*. Para cada vehículo conectado a una estación de carga el controlador toma el estado de carga y la información del propietario, y hace una llamada para ejecutar un *smart contract* donde se actualiza esta información. Si el estado de carga del vehículo es superior a un umbral determinado (por ejemplo, 50% de carga), puede ser

usado para la regulación de frecuencia, y el controlador lo incluye en el registro 1, si no cumple el requisito es incluido en el registro 2. Si la frecuencia se encuentra dentro de los límites, los coches se cargan de la fotovoltaica y de la red si es necesario. Si la frecuencia no está dentro de los límites, los vehículos incluidos en el registro 1 se descargan y suministran su energía a la red. Cuando un vehículo se desconecta del cargador, su estado de carga y detalles de las transacciones se actualizan en la *blockchain* y su *smart contract* se cierra, liquidándose los pagos según el intercambio de energía efectuado.

En esta propuesta blokchain es utilizado para mantener la cuenta de cada usuario, almacenando su información de forma segura, y para monitorizar la energía de cada estacionamiento participante. La integración de *blockchain* en los controladores inteligente permite mejorar la seguridad de los datos, la inmutabilidad de la información, la transparencia, la verificación y la confianza entre los usuarios. La red *blockchain* utilizada para su desarrollo en este caso es Ethererum. Y el flujo de trabajo del *smart contract* propuesto es el siguiente:

1) Para cada vehículo, toma la información del propietario (pseudo identidad, donde solo es necesario verificar las claves privadas el propietario) y su nivel de carga.
2) Si el vehículo se carga en la instalación, resta la cantidad de tokens correspondiente a la energía transferida de la billetera del propietario del vehículo, y la suma a la billetera del propietario del estacionamiento.
3) Si el vehículo se descarga para suministrar potencia a la red, resta los tokens de la billetera del propietario del estacionamiento y los suma en la billetera del propietario del vehículo.
4) Actualiza estas transacciones en la red de *blockchain* de Ethereum.

# 3 AUTOCONSUMO SOLAR COLECTIVO CON *BLOCKCHAIN*

*Comenzar un camino nuevo da miedo. Pero a cada paso que damos, nos damos cuenta de que lo peligroso era quedarse quieto.*

*- Roberto Benigni -*

Blockchain puede ser utilizado para mejorar la eficiencia y seguridad de sistemas eléctricos, tal y como se ha expuesto en el capítulo anterior, especialmente en aplicaciones donde la operación descentralizada resulta ser más eficiente. Es el caso de las comunidades energéticas, donde *blockchain* puede facilitar la implementación de mecanismos de comercio de energía a nivel local y de operación descentralizada. Algunas de estas comunidades se conforman como microrredes autogestionadas o como otro tipo de organizaciones con diversos objetivos, como las comunidades de autoconsumo solar colectivo.

El autoconsumo solar colectivo consiste en un grupo de consumidores que utilizan infraestructuras de generación fotovoltaica comunes para su propio uso. Habitualmente los consumidores y las instalaciones de generación están situados dentro de un área geográfica cercana y utilizan la red de distribución para los intercambios de energía. Físicamente la energía solar es inyectada en la red. Para cada comunidad, la energía inyectada por las instalaciones de generación y el consumo energético de cada consumidor, son medidos mediante contadores inteligentes en periodos de tiempo determinados (normalmente horarios). Entonces, la energía generada total para cada periodo es agregada virtualmente y dividida entre todos los consumidores de la comunidad de acuerdo con unas reglas previamente pactadas.

El autoconsumo solar compartido presenta ciertas ventajas frente al autoconsumo solar individual [120]:

- Incrementa el ratio de energía efectivamente autoconsumida dentro de la comunidad frente a instalaciones individuales.
- Permite a varios participantes poner en común sus instalaciones para maximizar su beneficio.
- Permite el desarrollo de proyectos fotovoltaicos en las zonas comunes de urbanizaciones y bloques de viviendas.
- Permite a la comunidad elegir ubicaciones con configuraciones de la instalación que maximicen la producción solar.

El funcionamiento de las comunidades de autoconsumo solar compartido cumple con las condiciones necesarias para que la implementación de *blockchain* permita mejorar su eficiencia. Algunas de estas características, tal y como se vio en el Capítulo 2, son la existencia de varias partes involucradas, su operación descentralizada es más eficiente, es necesario mantener un historial de datos y no es necesaria una gran velocidad en el proceso.

En este capítulo se define el concepto de autoconsumo solar compartido y comunidad energética, tal y como

vienen recogidos en el marco regulatorio de la Unión Europea. A continuación, se desarrollan las condiciones administrativas, técnicas y económicas existentes en España para el autoconsumo solar colectivo, reguladas a través del Real Decreto 244/2019. Además, se propone un sistema para gestionar comunidades de autoconsumo colectivo basado en *blockchain*. Este modelo pretender aportar algunas mejoras al mecanismo recogido en el RD 244/2019, actualmente utilizado para gestionar este tipo de comunidades.

Por último, se simula el modelo propuesto, para ello se diseña una comunidad de autoconsumo colectivo formada por 10 hogares y una instalación fotovoltaica compartida. Se utiliza una red de *blockchain* local donde se programan y despliegan *smart contracts*, y se utilizan datos de consumo y producción eléctrica para probar el funcionamiento del modelo.

## 3.1 Definiciones

Junto con el desarrollo de nuevos sistemas de generación distribuida han surgido nuevas propuestas de organización, como las comunidades energéticas [121]. Estas propuestas permiten a los ciudadanos organizar colectivamente su participación en el sistema eléctrico y son una alternativa al sistema eléctrico tradicional. Este tipo de organizaciones están en una etapa temprana de su desarrollo y en ocasiones su marco normativo no está completamente definido.

En el contexto de la Unión Europea, el paquete de medidas *Clean Energy for All Europeans* introduce una serie de directivas que disponen el diseño y marco regulatorio para estas nuevas iniciativas energéticas [122]. Además, en estas directivas se dan definiciones básicas a los términos de comunidad energética y autoconsumo colectivo. La Directiva EU 2018/2001 (REDII), fomento uso de energía procedente de fuentes renovables, introduce los términos de *Renewable Energy Communities (*Comunidades de Energía Renovables) y *jointly acting renewable self-consumer* (autoconsumo colectivo). La Directiva EU 2019/944 (IEM), sobre normas comunes para el mercado interior de la electricidad, introduce el término de *Citizens Energy Communities* (Comunidades Ciudadanas de Energía).

El autoconsumo colectivo es definido en la Directiva REDII Art. 21 como un grupo de al menos dos autoconsumidores de energía renovable, localizados en el mismo edificio, que generan energía renovable para su propio uso, y que pueden almacenar o vender la energía producida, siempre que esto no constituya una actividad profesional. Adicional a su rol activo como prosumidores, los miembros de estos esquemas mantendrán sus derechos y obligaciones como consumidores finales. La Directiva especifica que los miembros pueden compartir la energía producida por sus plantas generadoras (que pueden ser propiedad de un tercero), estando estos sujetos al pago de las tasas e impuestos por el uso de la red, y que cada Estado miembro debe definir de una manera no discriminatoria.

El término Comunidad de Energía Renovable se define en la Directiva REDII Art. 22 como una entidad ciudadana colectiva basada en la participación abierta y voluntaria, autónoma, controlada por sus participantes o miembros que están situados cerca de un proyecto de energía renovable que es propiedad de la comunidad. Los miembros de la comunidad pueden ser personas, empresas o entidades públicas. Las actividades de la comunidad son producir, consumir, almacenar y vender la energía, compartir la energía producida entre sus miembros y participar en el mercado eléctrico (directamente o a través de agregadores). Su principal finalidad proporcionar beneficios económicos, sociales y medioambientales a sus participantes, en lugar de ganancias financieras.

Comparando la definición de los términos presentados, se puede entender el autoconsumo colectivo como una actividad específica, cuyo funcionamiento debe estar definido y reglado. Por ejemplo, debe regularse si es posible utilizar la red de distribución, la aplicación de peajes o como se bonifican los excedentes de generación vertidos a la red. Sin embargo, las comunidades energéticas se enfocan principalmente en los aspectos organizativos y de mercado, teniendo cabida dentro de su funcionamiento actividades como generación, distribución, suministro y consumo. Estas comunidades energéticas, por ejemplo, pueden materializarse en forma de microrredes con puntos de frontera físicos de la red de distribución y autogestionadas de forma comunitaria.

En la Tabla 3-1 se muestra un resumen de las legislaciones implementadas en algunos Estados miembro de la UE [122]. En el caso de España el autoconsumo compartido está regulado por el RD 244/19. Y, aunque no existe regulación específica para las comunidades energéticas, el RD 244/19 contempla el autoconsumo compartido entre distintos edificios, haciendo uso de la red de distribución de baja tensión.

Tabla 3-1. Marco regulatorio de autoconsumo compartido y comunidades energéticas en Europa. (PG es la abreviatura de *private grid* (red privada) [122]

| Country | Collective Self-consumption | Energy Communities |
|---|---|---|
| AT | ✓ ElWOG 2017 | Legislative process started (Renewables expansion law) |
| BE | ✓ Wallonia, decrees in 2018, 2019 | ✓ Wallonia, framework legislation; decree in 2019 |
| DE | ✓ Tenant power model 2017 | - |
| DK | PG only | - |
| EE | PG only, Electricity Market Act | - |
| ES | ✓ Royal Decree 244/19 | - (multi-building CSC) |
| FI | PG only | - |
| FR | ✓ Law 2017-227, decree 2017-676 | Legislative process started |
| GR | ✓ 2016 law on virtual net metering | ✓ Law N4513/2018 on energy communities 2018 |
| LU | Draft electricity market bill 2018 | Draft electricity market bill 2018 |
| NL | PG only | - |
| PT | Legislative process started | - |
| SI | ✓ Regulation on self-supply 2019 | ✓ Framework within regulation on self-supply 2019 |
| SE | PG only | - |
| UK | PG only | - |
| CH | ✓ Energy law and decree 2016/2017 | ✓ Energy law and decree 2016/2017 |

## 3.2 Regulación en España

En España, las condiciones administrativas, técnicas y económicas del autoconsumo de energía eléctrica están reguladas en el Real Decreto 244/2019 [123], que junto con la Ley 24/2013 del Sector Eléctrico [124], forma el marco normativo que regulan las actividades de autoconsumo.

En el RD 244/2019, se definen las figuras de consumidor asociado e instalación de producción próxima. Un consumidor asociado es un consumidor en un punto de suministro que tiene asociadas instalaciones de producción. Las figuras de consumidor asociado y productor, pueden ser la misma persona o no, y ser una persona física o jurídica. Una instalación de producción próxima a las de consumo asociadas puede ser de dos tipos:

- Instalaciones próximas de red interior: La instalación de producción está conectada a la red interior de los consumidores asociados, o están unidas mediante líneas eléctricas directas.
- Instalaciones próximas a través de la red: Hacen uso de la red de distribución y tanto las instalaciones de producción como los consumidores asociados cuentan con un punto frontera con la red de distribución. Se deben cumplir las siguientes condiciones:
  - Están conectadas a cualquiera de las redes de baja tensión derivadas del mismo centro de transformación.
  - Tanto la generación como los consumos se encuentran conectados en baja tensión y a una distancia entre ellos inferior a 500 metros. Se tomará como referencia la distancia entre los equipos de medida en proyección ortogonal en planta.
  - La generación y los consumos deben estar ubicados en una misma referencia catastral según sus primeros 14 dígitos.

En el RD 244/2019 se contemplan diferentes modalidades de autoconsumo:

- Autoconsumo sin excedentes. En esta modalidad debe instalarse un mecanismo antivertido que impida la inyección de energía excedentaria a la red de transporte o distribución.

- Autoconsumo con excedentes. En esta modalidad las instalaciones de producción y de consumo asociadas podrán, además de suministrar energía para autoconsumo, inyectar en la red eléctrica la energía excedentaria. A su vez, esta modalidad se divide en:
  - Acogida a compensación: Pertenecen a esta modalidad aquellos casos en los que voluntariamente el productor y consumidor opten por acogerse a un mecanismo de compensación de excedentes. El mecanismo de compensación, previsto en la Ley 24/2013, es un contrato mediante el cual se establece las condiciones de compensación entre los déficits de consumo y energía excedentaria generada. Esta opción sólo es posible si se cumplen unas condiciones, algunas de ellas son:
    - La fuente de energía primaria debe ser de origen renovable.
    - La potencia total de las instalaciones de producción asociadas no puede ser superior a 100 kW
    - El consumidor y productor asociado haya suscrito un contrato de compensación de excedentes de autoconsumo.
    - La instalación de producción no tenga otorgado un régimen retributivo adicional o específico.
  - No acogida a compensación: Pertenecen a esta modalidad, todos aquellos casos de autoconsumo con excedentes que no cumplan alguno de los requisitos para acogerse a mecanismo de compensación o que voluntariamente opten por no acogerse a esa modalidad.

Adicionalmente, el autoconsumo puede clasificarse en individual o colectivo en función de si se trata de uno o varios consumidores los que están asociados a las instalaciones de generación. En el caso de autoconsumo colectivo, todos los consumidores asociados a una misma instalación de generación deberán pertenecer a la misma modalidad de autoconsumo y deberán comunicar de forma individual a la empresa distribuidora como encargado de la lectura, un mismo acuerdo firmado por todos los participantes que recoja los criterios de reparto.

Con carácter general, los consumidores acogidos a cualquier modalidad de autoconsumo deberán disponer de un equipo de medida bidireccional en el punto frontera. Las instalaciones de generación deberán disponer de un equipo de medida que registre la generación neta cuando se realice autoconsumo colectivo y cuando la instalación de generación sea una instalación próxima a través de la red. Para los consumidores acogidos a las modalidades de sin excedentes o excedentes con compensación, el encargado de la lectura de los equipos de medida será la compañía distribuidora. La distribuidora deberá remitir la información desglosada para la correcta facturación a las empresas comercializadoras y aplicar, en su caso, el mecanismo de excedentes de compensación.

El mecanismo de compensación simplificada previsto en el RD 244/2019 consistirá en un saldo en términos económicos de la energía consumida en el periodo de facturación, según los siguientes casos:

- Si el consumidor dispone de un contrato de suministro con una comercializadora libre:
  - La energía horaria consumida de la red será valorada al precio horario acordado entre las partes.
  - La energía horaria excedentaria será valorada el precio horario acordado entre las partes.
- Si el consumidor dispone de un contrato de suministro al precio voluntario para el pequeño consumidor con una comercializadora de referencia:
  - La energía horaria consumida de la red será valorada al coste horario de la energía del precio voluntario para el pequeño consumidor en cada hora (TCUh), definido en el artículo 7 del Real Decreto 216/2014.
  - La energía horaria excedentaria, será valorada al precio medio horario (Pmh), obtenido a partir de los resultados del mercado diario e intradiario para cada hora, menos el coste de los desvíos CDSVh, definidos los artículos 10 y 11 del Real Decreto 216/2014.

Para la aplicación del mecanismo de compensación simplificada, los consumidores deben remitir a la empresa distribuidora, normalmente a través de su comercializadora, el acuerdo de compensación entre los sujetos participantes.

Para la liquidación de la energía horaria excedentaria vertida por instalaciones no acogidas a la modalidad de

mecanismo de compensación, se les aplicará la normativa general de la actividad de producción.

Para la determinación de los peajes de acceso a las redes de transporte y distribución y cargos del sistema eléctrico que se aplican a las modalidades de autoconsumo:

- La energía autoconsumida de origen renovable, cogeneración o residuos, está exenta de todo tipo de peajes.
- Para la determinación del término de potencia se utilizará el equipo de medida ubicado en el punto frontera de consumo.
- Para la determinación del término de energía activa, la energía a considerar será la energía horaria consumida de la red.

A efectos de facturación y liquidación, la cantidad de energía generada, consumida, autoconsumida, consumida de la red y excedentaria, para el caso de autoconsumo colectivo, se calculan según lo establecido en el Anexo I del RD 244/2019:

- Energía horaria neta generada individualizada ($ENG_{h,i}$): Es la energía bruta generada menos la consumida por los servicios auxiliares de producción en un periodo horario correspondiente a un consumidor acogido a la modalidad de autoconsumo colectivo. Se calcula así:

$$ENG_{h,i} = \beta_i \cdot ENG_h$$

Donde,

**$ENG_h$** es la energía neta horaria total producida por el generador o generadores.

**$\beta i$** es el coeficiente de reparto de la energía generada entre los consumidores que participan del autoconsumo colectivo. Para cada consumidor i participante del autoconsumo colectivo, este coeficiente tomará el valor que figure en un acuerdo firmado por todos los consumidores participantes y que debe ser notificado a la empresa distribuidora. El valor de estos coeficientes podrá determinarse en función de la aportación económica de cada uno de los consumidores a la instalación de generación, de la potencia de cada consumidor, o de cualquier otro criterio que los participantes consideren oportuno, siempre que exista consenso entre ellos y la suma de los coeficientes βi sea la unidad.

La empresa distribuidora, como encargada de la lectura, deberá aplicar los coeficientes de reparto $\beta_i$. Estos coeficientes deberán ser constantes y tener un valor fijo para todas las horas de facturación.

- Energía horaria consumida individualizada: Es la energía neta horaria consumida por un consumidor. Para el cálculo de esta, se utiliza el equipo de medida en el punto frontera.
- Energía horaria consumida de la red individualizada: Es el saldo neto de energía eléctrica recibida de la red no procedente de instalaciones de generación asociadas al punto de suministro del consumidor. Se calcula como la diferencia entre la energía horaria consumida individualizada y la energía horaria autoconsumida individualizada.

$$Econ\_red_{h,i} = Econ_{h,i} - Eaut_{h,i}$$

- Energía horaria autoconsumida individualizada (Eauth,i): Autoconsumo neto horario realizado por un consumidor. Se calcula como:
  - Si la energía horaria consumida individualizada del consumidor es superior en valor absoluto a la energía horaria neta generada individualizada, el autoconsumo horario individualizado será el valor de la energía neta generada individualizada:

$$Eaut_{h,i} = ENG_{h,i}$$

  - Si es inferior, el autoconsumo horario individualizado será, el valor de la energía horaria consumida individualizada del consumidor:

$$Eaut_{h,i} = Econ_{h,i}$$

- Energía horaria excedentaria individualizada: Es el saldo neto horario de energía horaria excedentaria correspondiente a un consumidor que participa en una instalación de autoconsumo colectivo. Se calcula como la diferencia entre la energía neta horaria generada individualizada y la energía horaria consumida individualizada por cada consumidor. Se considerará cero cuando el valor de esta operación sea negativo.

$$Eexc_{h,i} = ENG_{h,i} - Econ_{h,i}$$

En cualquier caso, la suma entre la energía horaria excedentaria y la energía horaria autoconsumida de todos los consumidores participantes del autoconsumo compartido debe ser igual a la energía neta horaria producida por el generador o generadores.

## 3.3 Autoconsumo solar colectivo con *blockchain*

### 3.3.1 Modelo propuesto

En este trabajo se propone una solución basada en *blockchain* para liquidar la cantidad de energía generada individualizada por cada consumidor en una comunidad de autoconsumo solar colectivo, aportando mejoras al mecanismo recogido en el RD 244/2019 expuesto anteriormente. La comunidad de autoconsumo solar colectivo estaría formada por varios consumidores que comparten los derechos de una o varias instalaciones fotovoltaicas, y que cumplen con los requisitos del RD 244/2019 para acogerse a esta modalidad de autoconsumo. Tanto los consumidores como las instalaciones de generación cuentan con contadores inteligentes en sus puntos frontera con la red de distribución.

La propuesta consiste en una red de *blockchain*, donde cada uno de los consumidores, junto con la instalación de generación, y la compañía distribuidora, son un nudo de la red. Los nodos de los consumidores y generadores se implementan en contadores inteligentes con funcionalidad IoT o en dispositivos IoT conectados a un puerto de los contadores inteligentes. En la Figura 3-1 se muestra un esquema del modelo de *blockchain* propuesto.

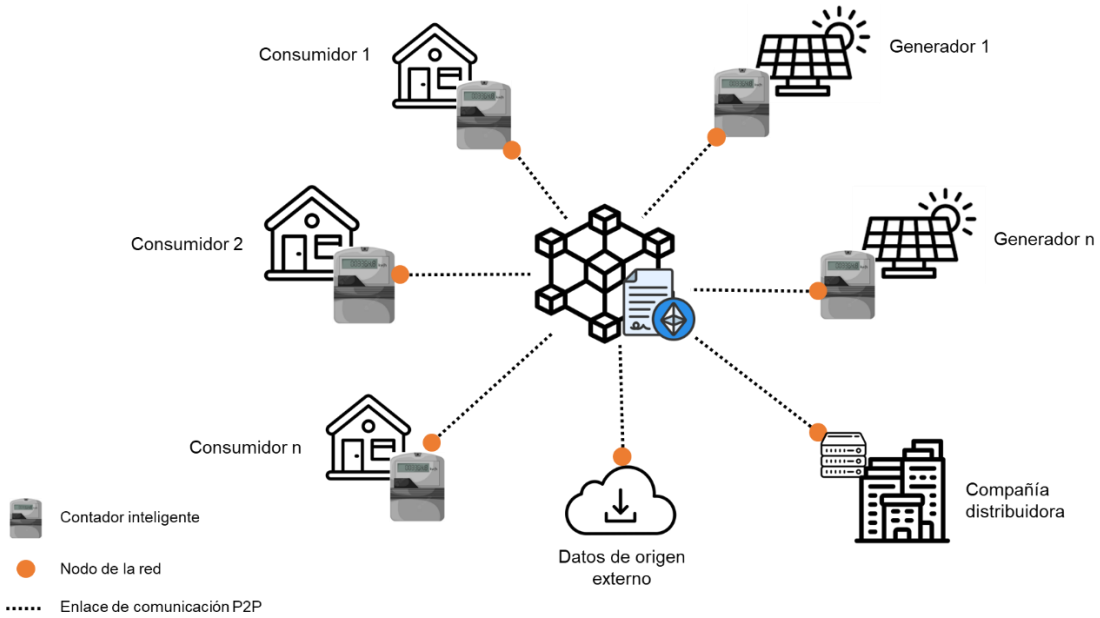


Figura 3-1. *Blockchain* propuesta para comunidades de autoconsumo solar colectivo [Elaboración propia]

Los datos de consumo y generación se envían a la *blockchain* desde los contadores inteligentes de forma horaria. Una vez que los datos se envían a la *blockchain*, mediante el uso de *smart contracts* y de unas reglas previamente definidas, se calcula la cantidad de energía generada individualizada que es imputada a cada consumidor. La compañía distribuidora, encargada de la medición, accede a los datos horarios de generación individualizada para cada usuario a través de la *blockchain*. Con estos datos, junto con la lectura de los

contadores a través de su infraestructura de medición convencional, calcula además los valores de energía autoconsumida, consumida de la red y excedentaria. Estos datos son enviados a las compañías comercializadoras para la facturación y liquidación de la energía eléctrica.

El tipo de *blockchain* que mejor se ajustaría a esta aplicación sería de tipo privada y *permisionless,* debido a que los nodos de la red son limitados y su ingreso en la comunidad y en la red puede ser controlado mediante algún mecanismo de acceso e identificación que normalmente sería llevado a cabo por la compañía distribuidora. Además, las *blockchain* de tipo privadas permiten implementar mecanismos de consenso con requisitos de cómputo bajos.

Dentro de la *blockchain* se implementan dos *smart contracts*, con las siguientes funciones:

- ***Smart contract* 1**: Se utiliza para dividir los derechos de uso de la instalación fotovoltaica utilizando *tokens*. Mediante este *smart contract*, se efectúa una emisión y reparto inicial de *tokens*, según la aportación de cada usuario en la promoción de la instalación fotovoltaica. El número de *tokens* de cada usuario será usado para calcular la cantidad de energía generada adjudicada a cada consumidor. Los *tokens* son fácilmente transferibles entre usuarios, pudiendo ser negociados posteriormente.
- ***Smart contract 2***: Donde se implementa el algoritmo con las reglas de la comunidad para distribuir y liquidar la energía generada por la instalación fotovoltaica (Figura 3-2). Se ejecuta automáticamente para cada periodo horario, y tiene como entradas los datos de generación y consumos horarios enviados desde las direcciones de consumidores y generadores, tomados de los contadores inteligentes. También puede tener otras entradas externas, como datos de precios del mercado eléctrico, usados para liquidaciones económicas internas dentro de la comunidad. La salida del *smart contract* son las cantidades de energía generada individualizada de cada consumidor. Los datos de salida sólo son accesibles desde la dirección asignada a la compañía distribuidora, que utiliza estos datos para su labor de medición de energía eléctrica y su posterior reporte a las compañías comercializadoras. Por último, este *smart contract* también ejecuta de manera automática la liquidación económica entre usuarios mediante criptomonedas, sumando o restando en el balance de cada usuario según corresponda.

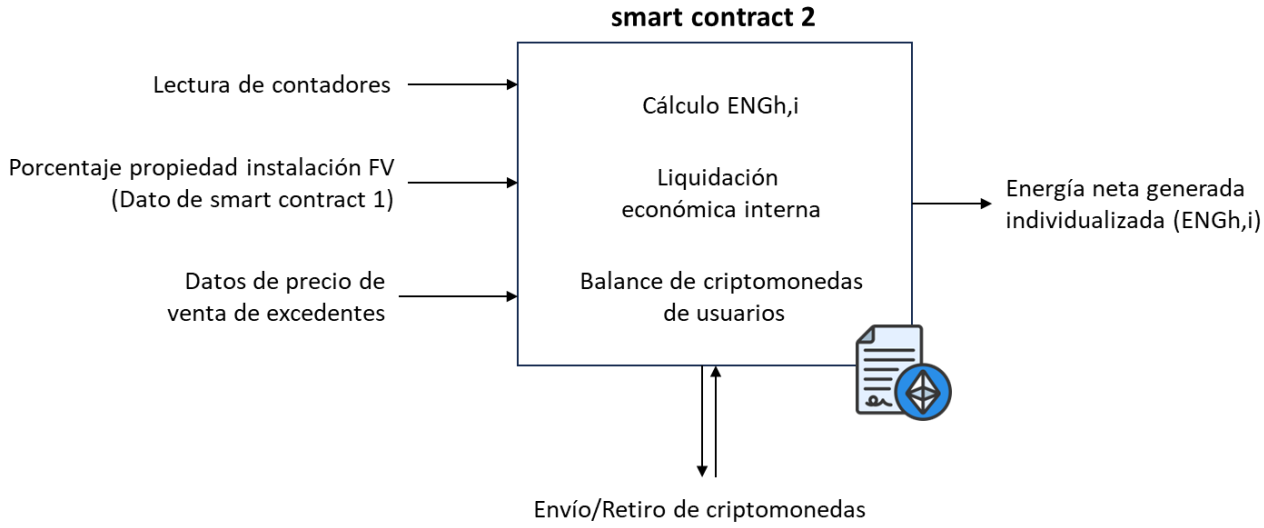


Figura 3-2. Esquema de *smart contract* propuesto [Elaboración propia]

Para la liquidación económica interna entre consumidores de la comunidad, se utilizará dentro de la *blockchain* una criptomoneda. Por el tipo de aplicación, es conveniente que esta criptomoneda sea de tipo *stablecoin*, de decir que su valor de mercado esté ligado a una moneda común, por ejemplo, el Euro.

En este trabajo se propone un algoritmo sencillo, a implementar en el *smart contract* 2, que consiste en un reparto inicial de la energía generada en base a la participación de cada consumidor en la instalación fotovoltaica (de forma similar al mecanismo del RD 244/2019), y una posterior liquidación interna entre usuarios con excedentes y usuarios con déficits. De esta forma, se maximiza la cantidad de energía generada

por la instalación que es liquidada como autoconsumida frente a la que es liquidada como excedentaria. Debido a que normalmente la bonificación por energía excedentaria vertida a la red es inferior al precio de la energía consumida de la red, la maximización de energía liquidada como autoconsumida revierte en un beneficio económico para la comunidad. El algoritmo implementado se observa en la Figura 3-3, donde:

*ENG_h*: Energía neta generada por la instalación FV durante el periodo horario h.

*ENG_h,i*: Energía neta generada individual de un usuario i para el periodo horario h.

*Econ_h,i*: Energía consumida por un usuario i durante el periodo horario h.

*βi*: Porcentaje de participación del usuario i en la instalación FV

*E_exc_h,i* = Energía excedente de un usuario i para el periodo horario h

*sum_E_exc_h* = Sumatorio de energía excedentaria total

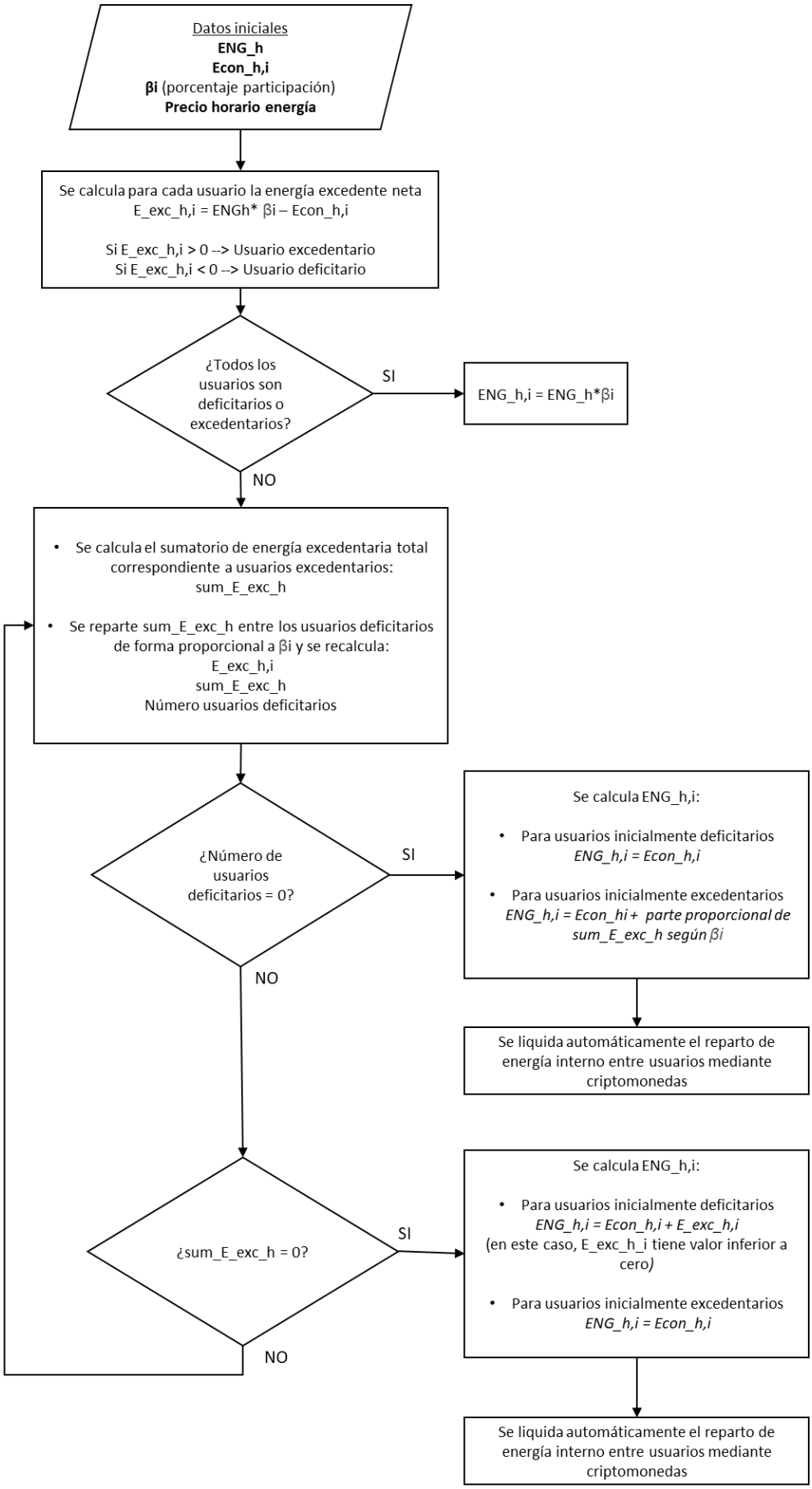


Figura 3-3. Algoritmo de reparto para calcular la energía neta generada individualizada implementado en *smart contract* [Elaboración propia]

Aunque en este trabajo se ha propuesto el algoritmo anterior, existe la posibilidad de explorar y desarrollar mecanismos más complejos. Por ejemplo, pueden implementarse algoritmos de optimización que controlen soluciones de almacenamiento o cargas controlables de los consumidores, tratando así de maximizar aún más la cantidad de energía que es producida y autoconsumida dentro de la comunidad. Podrían ponerse a disposición de la comunidad recursos de generación y almacenamiento particulares, a cambio de ciertas bonificaciones. También pueden desarrollarse mecanismos de mercados internos, o acuerdos de intercambios de energía entre miembros de la comunidad. Lo interesante de estas propuestas es que permiten a las comunidades implementar nuevas soluciones energéticas, con flexibilidad y autonomía, sin la necesidad sobrecargar con nuevos procesos y desarrollos a las compañías de distribución.

En general, las ventajas que la solución propuesta presenta con respecto al mecanismo propuesto en el RD 244/2019 son las siguientes:

- **Maximizar la energía liquidada como autoconsumida**. El mecanismo del RD 244/2019 calcula la energía generada neta individualizada para cada consumidor mediante el uso de unos coeficientes de reparto previamente notificados por la comunidad, y que son fijos para todos los periodos horarios (como se explica en el Apartado 3.2). Este sistema tan rígido provoca que en ocasiones no se maximice la energía computada como autoconsumida dentro de la comunidad. Por ejemplo, en ciertos periodos horarios algunos miembros de la comunidad pueden presentar superávit en la relación generación/consumo (computándose ese superávit como excedentes), mientras que otros pueden presentar déficit (su consumo se computa como consumido de la red). Con la solución propuesta, se permite que los consumidores liquiden internamente, con mejores condiciones, la energía generada individualizada. Con esto, se consigue que toda la energía generada sea liquidada como autoconsumida, excepto cuando la generación total es superior al consumo total de la comunidad, donde el exceso será liquidado como excedentes repartidos según el mecanismo implementado.
- **Evita que la compañía de distribución modifique su infraestructura**. Para lograr el objetivo anterior, donde para cada periodo horario las condiciones de liquidación varían, en lugar de ser fijas como en el mecanismo del RD 244/2019, sería necesario que la compañía distribuidora implementase nuevos procesos en su labor de liquidación, con cálculos y algoritmos adicionales. Mediante la solución propuesta, donde la liquidación se realiza automáticamente mediante un *smart contract*, la compañía de distribución sólo tiene que tomar el resultado de este *smart contract*, en lugar de utilizar los valores de coeficientes fijos para calcular la energía generada individualizada.
- **Desarrollo de nuevas soluciones dentro de la comunidad**. Además de para una simple liquidación más efectiva de la energía generada y autoconsumida, la red de *blockchain* propuesta puede utilizarse para diseñar nuevas soluciones energéticas. Aprovechando la capacidad de automatización de los *smart contracts*, y el uso de controladores inteligentes, pueden incorporarse a la comunidad sistemas de almacenamiento, carga de vehículo eléctrico y sistemas de gestión energética de hogar. Los *smart contracts* se encargarían del control automático de estos elementos, tratando de maximizar el beneficio de la comunidad, mediante algoritmos de optimización programados en éstos.
- **Desarrollo de nuevas funcionalidades de la comunidad**. Mediante la solución propuesta se establece una comunidad y un enlace de comunicación con la compañía distribuidora, que podría ser utilizado por ésta para otras finalidades más allá de simplemente tomar información para el proceso de liquidación y facturación de energía. La compañía distribuidora podría utilizar los recursos de generación, almacenamiento y control de la comunidad para las necesidades de la red. Así, tal y como se mostró en algunas propuestas en el capítulo anterior, podrían desarrollarse sistemas de respuesta de la demanda, control de voltaje y frecuencia, etc.

### 3.3.2 Desarrollo de aplicación

En este apartado se recoge el proceso de simulación de una red *blockchain* siguiendo el modelo expuesto anteriormente. Para ello, se diseña una comunidad de autoconsumo solar colectivo, formada por 10 viviendas y una instalación fotovoltaica de 25 kW de potencia nominal.

Se ha implementado una red de *blockchain* local, utilizando un emulador para pruebas basado en la red de Ethereum, sobre la que se han desplegado los *smart contracts*. Finalmente, utilizando curvas de carga y de

generación horarias, a modo de datos de lectura de los contadores inteligentes, se simula con Python el proceso de envío y consulta de datos. Finalmente se evalúan los resultados y el correcto funcionamiento de la simulación.

#### 3.3.2.1 Herramientas utilizadas

- **Ganache**

Ganache es un emulador de *blockchain* que permite crear una red de pruebas local. Es utilizado para desarrollar, desplegar y testear *smart contracts* y *DApps* en un entorno seguro sin necesidad de ejecutar un nodo en la red de Ethereum real [125]. Ganache está desarrollado en dos entornos, uno con interfaz de usuario y otra con interfaz de línea de comandos. La versión con interfaz de usuario, usada en este trabajo, es una aplicación de escritorio disponible para Windows, Mac y Linux.

- **Solidity**

Solidity es un lenguaje de programación de alto nivel orientado a objetos. Su sintaxis es similar a la de JavaScript y está enfocado a la programación de *smart contracts* que serán desplegados en la Ethereum Virtual Machine (EVM) [126].

- **REMIX IDE**

REMIX es un entorno integrado de desarrollo web de código abierto que permite la programación de *smart contracts* escritos en lenguaje de programación Solidity y su despliegue en la *blockchain* de Ethereum [127]. Cuenta con varios módulos para probar, compilar y desplegar *smart contracts* en una máquina virtual de prueba.

- **Metamask**

Metamask es una *wallet* de Ethereum, disponible en forma de extensión en un navegador web o en aplicación móvil. Metamask permite al usuario enviar transacciones y consultar su estado de cuentas [128].

- **Python**

Python es un lenguaje de programación de alto nivel, ampliamente utilizado en aplicaciones web, desarrollo de software, ciencia de datos y *machine learning*. Actualmente es uno de los lenguajes de programación más populares. Es administrado por Python Software Foundation y tiene una licencia de código abierto.

- **Visual Studio Code**

Visual Studio Code es un editor de código fuente desarrollado por Microsoft. Es gratuito y de código abierto y compatible con varios lenguajes de programación [129]. En este trabajo se ha utilizado para compilar el código de Python.

- **Web3 librarys**

Web3 es una colección de librerías que permiten interactuar con un nodo local o remoto de Ethereum [130]. En este trabajo se ha utilizado la librería Web3.py para Python.

#### 3.3.2.2 *Smart contracts*

A continuación, se detalla el funcionamiento y las funciones implementadas en los dos *smart contracts* utilizados en el modelo.

- ***Smart contract* 1**

Mediante este *smart contract* se "tokeniza" la propiedad de la instalación fotovoltaica, es decir, se crean *tokens* de tipo fungible que representan el derecho de uso de la energía generada por la instalación. Los *tokens* son activos que se pueden transferir fácilmente entre usuarios.

Se ha utilizado el protocolo de ERC-20 que es un estándar utilizado para crear tokens dentro de la *blockchain* de Ethereum. Para ello, se ha empleado la librería de OpenZeppelin [131].

El *smart contract* está formado por una sola función, llamada *constructor*, que es una función especial en

Solidity, utilizada para inicializar variables cuando se crea el contrato. En esta función se declaran las direcciones de los usuarios participantes, y la cantidad de *tokens* que poseen inicialmente. En este caso cada uno de los diez usuarios tendrá 10 *tokens* (un 10% de participación en la instalación). En el protocolo ERC-20 y en general en los *smart contract* programados con Solidity, para evitar utilizar variables de punto flotante, las cantidades habitualmente se expresan multiplicadas por 18 (es decir una unidad equivale a 10^18).

El código del *smart contract* se puede consultar en el apartado A.1.1 del Anexo A.

- ***Smart contract* 2**

En este *smart contract* se recolectan los datos de mediciones eléctricas de consumo de usuarios y generación de la instalación fotovoltaica. Posteriormente, se efectúa el cálculo de energía generada individualizada de los usuarios, ejecutando el algoritmo propuesto en la Figura 3-3. Por otro lado, el *smart contract* ejecuta automáticamente la liquidación económica entre usuarios y gestiona el balance económico de cada usuario, incluyendo retiradas e ingresos de criptomonedas al *smart contract*.

Las funciones implementadas en este *smart contract* son:

- Función *Eh_con_input*: Recibe y almacena los datos de consumo horario de los usuarios. Los datos son enviados mediante transacciones realizadas desde la dirección de los usuarios. Sólo permite enviar transacciones a usuarios con participación en la instalación fotovoltaica.
- Función *E_gen_inst_input*: Recibe y almacena los datos de generación horaria. Igualmente, los datos sólo pueden enviarse mediante una transacción desde la dirección asignada a la instalación fotovoltaica.
- Función *Precioh_input*: Destinada a recibir los datos de precio horario de venta de excedentes de generación.
- Funciones *receive* y *withdraw*: Utilizadas para enviar y retirar criptomonedas al contracto.
- Función *consulta_balance*: Permite a los usuarios consultar su balance de criptomonedas.
- Función *resultado*: Es la función principal, implementa el algoritmo de reparto de la Figura 3-3 para cada periodo horario. Tiene como salida un *array* con la dirección de cada usuario y la energía generada individualizada para ese periodo horario. Sólo puede ser invocada desde la dirección de la compañía distribuidora.

El código completo del *smart contract* se puede consultar en el apartado A.1.2 del Anexo A.

#### 3.3.2.3 Simulación

Utilizando la plataforma Ganache, en su versión de aplicación de escritorio para Windows, se crea una *blockchain* local. Ganache permite crear *blockchains* basadas en la red de Ethereum, con el objetivo de testear los desarrollos en sus primeras fases. En este caso, al estar basada la *blockchain* utilizada en Ethereum, la criptomoneda utilizada es ETH, la propia de este ecosistema.

La red está formada por 13 direcciones, 10 para usuarios, una para la instalación fotovoltaica, una para la obtención de datos de precios de electricidad y otra para interactuar con la compañía distribuidora. Desde la pestaña *Accounts* de la interfaz de usuario puede consultarse la información de las direcciones, incluyendo el balance en ETH que tiene cada una de ellas (Figura 3-4). También puede visualizarse la clave privada de cada dirección, necesaria para enviar transacciones desde la dirección (Figura 3-5).

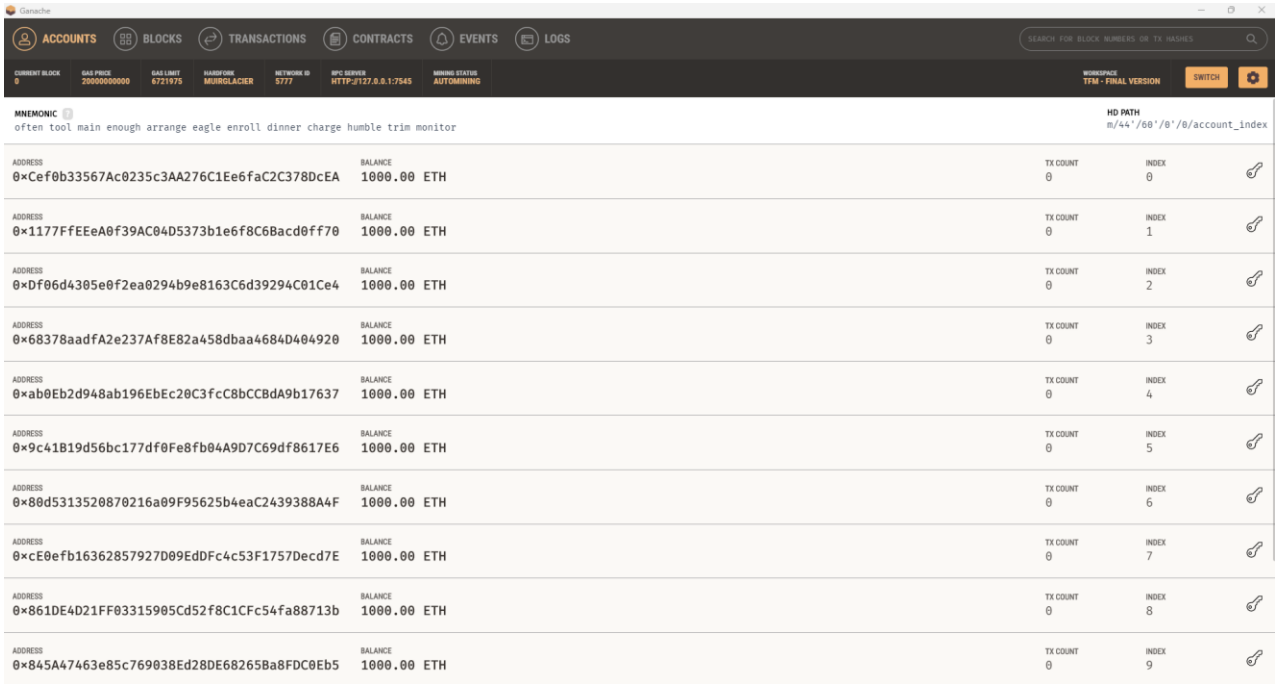


Figura 3-4. Listado de direcciones que forman la *blockchain* de Ganache [Captura pantalla Ganache]

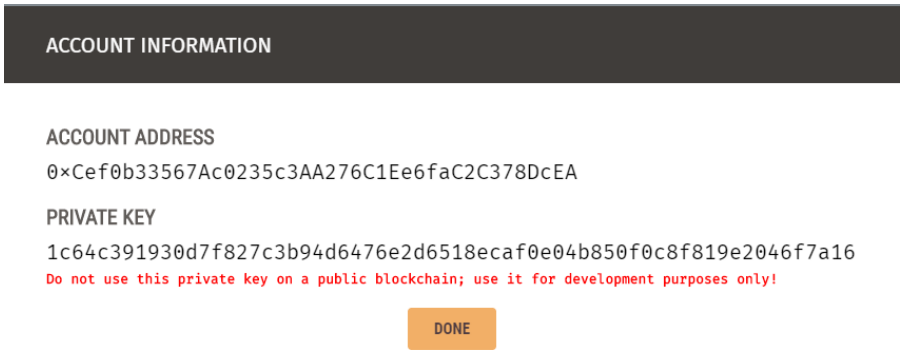


Figura 3-5. Información de una dirección en Ganache. Dirección pública y clave privada [Captura pantalla Ganache]

Los *smart contracts*, escritos en lenguaje Solidity, se han compilado en el entorno de programación web REMIX IDE. Con REMIX también es posible conectarse a la red de *blockchain* local creada y desplegar los contratos sobre ella (Figura 3-6). Así, se compilan y despliegan los dos *smart contracts* expuestos en el apartado anterior.

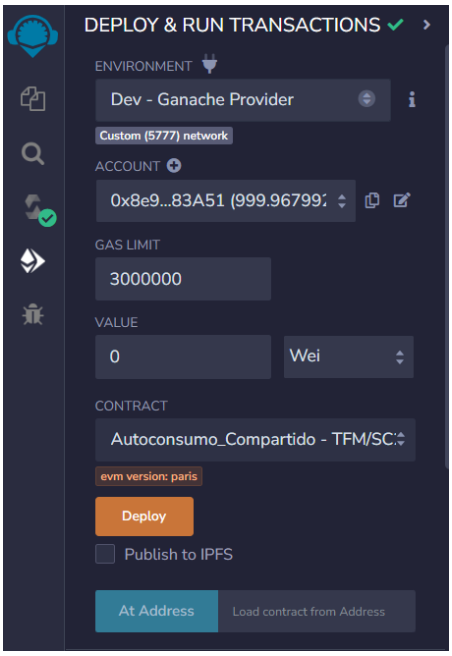


Figura 3-6. Entorno web de programación REMIX. Pantalla para despliegue de un *smart contract* en la *blockchain* creada con Ganache [Captura pantalla REMIX]

Las transacciones realizadas para crear los contratos pueden observarse desde la pestaña *Transactions* en Ganache:

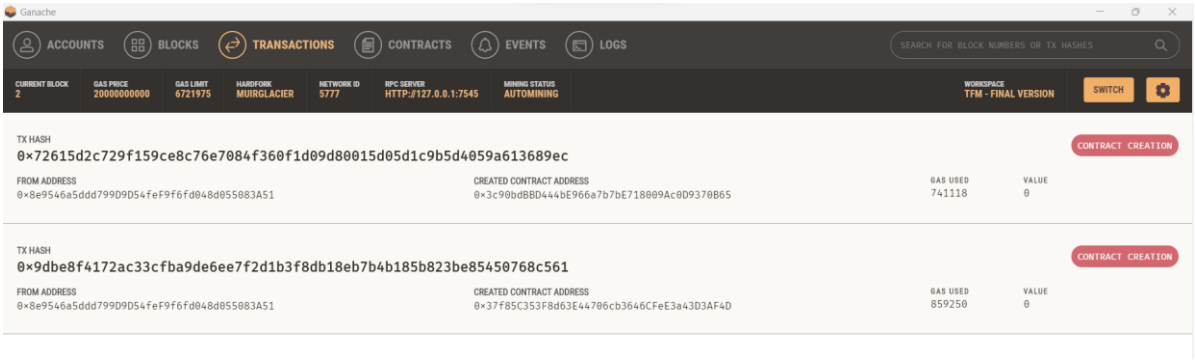


Figura 3-7. Listado de transacciones en Ganache [Captura pantalla Ganache]

En la pestaña *Blocks* puede consultarse la información de los bloques de la *blockchain*, por ahora solo existen dos, con una transacción cada uno:

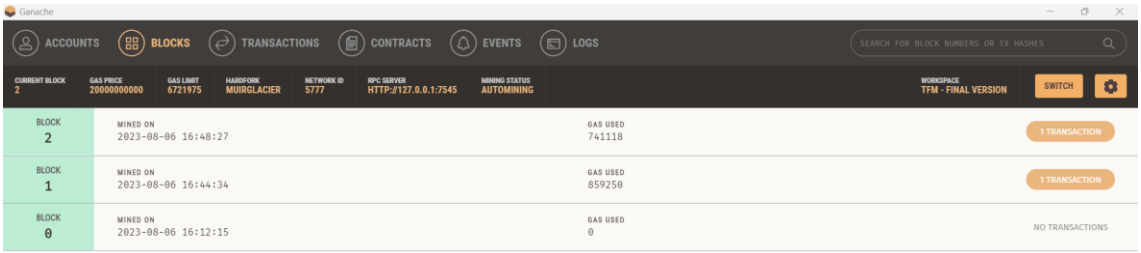


Figura 3-8. Listado de bloques de la cadena [Captura pantalla Ganache]

Para simular la transferencia de criptomonedas al *smart contract*, y la consulta del estado de cuentas de cada usuario, se utilizar la *wallet* Metamask, en su versión de extensión de navegador web. Se configura en Metamask la red local (Figura 3-9), y se accede a la cuenta de los usuarios mediante la clave privada que proporciona Ganache. Así, se puede consultar, para cada usuario, el balance en ETH (Figura 3-10), realizar envíos y retiros de ETH al *smart contract* (Figura 3-12), consultar el balance de *tokens* de propiedad de la instalación fotovoltaica (Figura 3-11), e incluso transferir estos *tokens* a otros usuarios.


Figura 3-9. Configuración en Metamask de la red Ethereum local [Captura de pantalla Metamask]

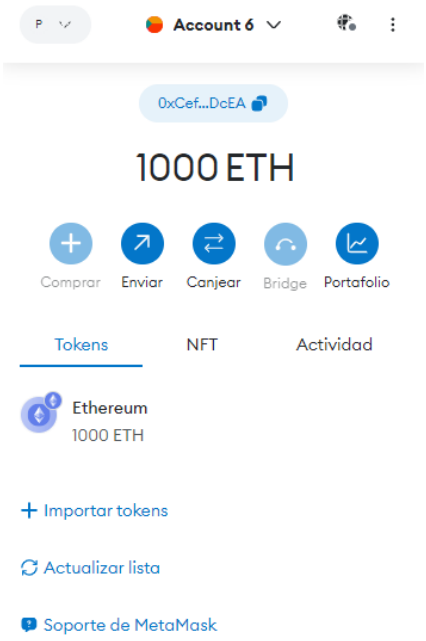


Figura 3-10. Consulta de balance de ETH [Captura de pantalla Metamask]


Figura 3-11. Balance de *tokens* de propiedad de la instalación [Captura de pantalla Metamask]

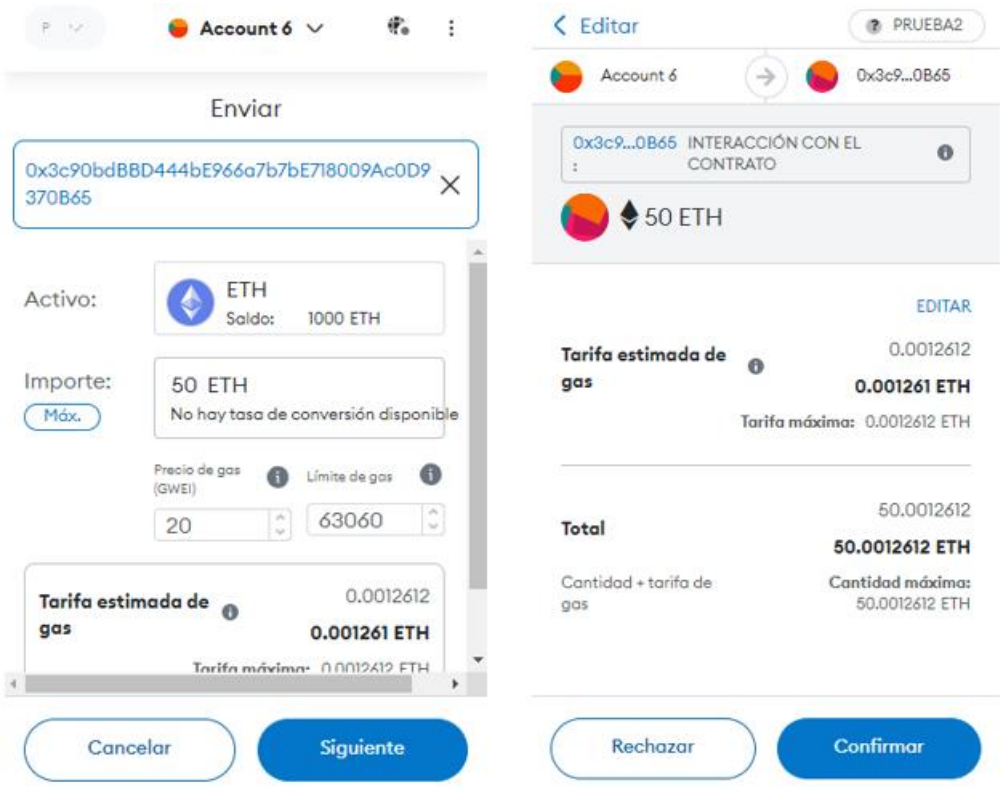


Figura 3-12. Envío de criptomonedas desde una cuenta de usuario al *smart contract* de la comunidad [Captura de pantalla Metamask]

Finalmente, se ha simulado el funcionamiento del modelo con datos de consumo y generación horarios correspondientes a un año completo. Se ha utilizado Python junto con la librería web3, para interactuar con el *smart contract*. Mediante el código desarrollado, se simula la transacción de datos horarios que se efectuaría por los contadores inteligentes y la respuesta que obtendría la compañía distribuidora con el resultado. La aplicación programada en Python incluye las siguientes etapas:

- Se conecta la aplicación a la red local de *Blockchain* utilizando la librería de Python web3.
- Se instancia el *smart contract* desplegado en la *blockchain* para poder interactuar con él.
- Se leen los datos horarios de generación y consumo desde archivos Excel. Se crean variables tipo *array* para almacenar los datos, y se tratan para que sean tipo enteros (*int*), debido a que los *smart contracts* programados en Solidity sólo funcionan correctamente con este tipo de variables.
- En un bucle, para cada periodo horario, se efectúan transacciones al *smart contract* desde la dirección asignada a cada uno de los consumidores y a la instalación fotovoltaica, conteniendo los datos de consumo y generación. También se efectúa una transferencia desde la dirección asignada para el envío de datos de precios de excedentes. Estas transferencias se efectúan llamando a las funciones del *smart contract* que corresponda según el caso.
- Dentro del mismo bucle, desde la cuenta de la compañía distribuidora, se invoca la función que calcula el reparto de energía, y se obtiene como resultado la energía generada individualizada para cada consumidor. Este resultado se escribe en un archivo Excel para su análisis.

El código de programación escrito en Python se puede consultar en el Apartado A.2 del Anexo A.

Los datos utilizados para la simulación han sido los siguientes:

- Datos de consumo horario: Los perfiles de consumo horario para los usuarios se han generado mediante el software LoadProfileGenerator [132].
- Datos de generación horaria: Los datos de producción fotovoltaica se han generado mediante la aplicación PVGIS desarrollada por la Comisión Europea [133]. Se ha simulado una instalación fotovoltaica de 25 kWp de potencia instalada, con paneles inclinados 30º y orientados al sur. La instalación está ubicada en latitud 40.40 y longitud -3.70.

- Datos de precio de excedentes de autoconsumo: Se ha tomado como datos de precios para la liquidación interna de la comunidad, el precio de la energía excedentaria de autoconsumo para el mecanismo de compensación simplificada (PVPC). Estos datos son accesibles desde la página web de REE [134].

Comparando el resultado obtenido en la simulación donde se implementa un reparto basado en el algoritmo de la Figura 3-3, frente al mecanismo propuesto por el RD 244/2019, se observa que la cantidad de energía total generada computada como excedentaria es inferior con el algoritmo (Tabla 3-2). Debido a que la bonificación por vertido de excedentes a la red es habitualmente es inferior al precio de la energía consumida de la red, esto revierte en un beneficio económico para la comunidad.

Tabla 3-2. Energía excedentaria de la comunidad simulada durante un año. Comparativa entre modelo *blockchain* propuesto con RD 244/2019.

| | |
|---|---|
| Energía excedentaria según RD 244/2019 | 25.861 kWh |
| Energía excedentaria con modelo y algoritmo propuesto | 22.429 kWh |

# 4 CONCLUSIONES

*Hace mucho tiempo, el hombre oía extrañado el sonido de un golpeteo regular dentro de su pecho y no tenía ni idea de su origen. […] El cuerpo era una jaula y dentro de ella había algo que miraba, escuchaba, temía, pensaba y se extrañaba; ese algo, ese resto que quedaba al sustraerle el cuerpo, eso era el alma.*

*Hoy, por supuesto, el cuerpo no es desconocido. […] Desde que sabemos denominar todas las partes, el cuerpo desasosiega menos al hombre. Ahora también sabemos que el alma no es más que la actividad de la materia gris del cerebro. La dualidad entre el cuerpo y el alma ha quedado velada por los términos científicos […]*

*Pero basta que el hombre se enamore como un loco y tenga que oír al mismo tiempo el sonido de sus tripas. La unidad del cuerpo y el alma, esa ilusión lírica de la era científica, se disipa repentinamente.*

*- Milan Kundera -*

Este trabajo pretende explorar las posibles aplicaciones de *blockchain*, una tecnología disruptiva y que ha tenido gran repercusión durante los últimos años, en el sector eléctrico. En primer lugar, se introduce *blockchain* como una tecnología que permite, gracias a la criptografía y a sistemas que aseguren el consenso entre partes que no tienen por qué confiar necesariamente entre sí, compartir una base de datos distribuida sin requerir una autoridad central de confianza. A continuación, se recogen potenciales usos de *blockchain* en sistemas eléctricos, incluyendo ejemplos con propuestas de aplicaciones concretas. En general, las potenciales aplicaciones tienen como marco general los cambios y nuevos desafíos en los que el sector eléctrico está actualmente inmerso. Por último, se hace un ejercicio de innovación y se presenta un sistema basado en *blockchain* para mejorar la gestión de comunidades de autoconsumo solar colectivo. Además, se desarrolla el modelo propuesto en una *blockchain* local de pruebas, simulando su funcionamiento para una comunidad de autoconsumo colectivo formada por 10 viviendas y una instalación fotovoltaica.

Después del trabajo realizado, se pueden sacar algunas conclusiones:

- La tecnología *blockchain* puede ser aplicada en diversos sectores, no sólo como base para crear criptomonedas.
- *Blockchain* aún se encuentra en una fase temprana de su desarrollo, aunque su funcionamiento esté basado en tecnologías ampliamente estudiadas como la criptografía y las redes de comunicación. Por eso, todavía no existe una estandarización de esta tecnología, necesaria para hacerla interoperable y fomentar su adopción.

- *Blockchain* tiene potencial para mejorar el desempeño y seguridad de los sistemas eléctricos y puede ser una herramienta útil en la implementación de nuevas soluciones. Especialmente en aplicaciones donde existen varias partes involucradas como mercados eléctricos o propuestas basadas en comunidades. También, en aplicaciones a nivel de redes eléctricas de distribución, donde cada vez más, existen muchos elementos a gestionar de propietarios distintos.
- Aunque existen numerosas propuestas de aplicación de *blockchain* en sistemas eléctricos, en su mayor parte todavía provienen del ámbito académico. Fuera de este ámbito, sólo existen algunos proyectos que aún están en fase de prueba de concepto, en general relacionados con aplicaciones de mercados eléctricos.
- El modelo propuesto en el Capítulo 3, evidencia como *blockchain* puede ser utilizado para mejorar procesos en el sector eléctrico, en este caso aplicándolo a la gestión de comunidades de autoconsumo solar colectivo. También, se demuestra que es relativamente sencillo simular el funcionamiento de aplicaciones concretas, creando una *blockchain* de pruebas y programando los *smart contracts* necesarios.

Por último, se sugieren algunas ideas para mejorar y continuar con el trabajo del modelo propuesto:

- Desarrollo de *smart contracts* para comunidades energéticas que incorporen, además de una instalación de generación compartida, sistemas de almacenamiento energético, estaciones de recarga de vehículo eléctrico y consumidores con sistemas de gestión energética automatizados. También, implementar la posibilidad de que los usuarios pongan a disposición de la comunidad instalaciones de generación privadas, más allá de la gestión de una sola instalación compartida como se ha propuesto en este trabajo. Por otro lado, se sugiere la implementación de algoritmos de optimización en los *smart contracts* que gestionan los recursos de la comunidad.
- Desarrollo de una interfaz de usuario para interactuar con los *smart contracts* y el entorno *blockchain*. Con una interfaz de usuario, mediante una aplicación móvil o web, cada usuario podría acceder fácilmente a sus datos de consumo y generación y configurar determinados parámetros.

# ANEXO A. CÓDIGO DE PROGRAMACIÓN

## A.1 Código Solidity (*smart contracts*)

### A.1.1 *Smart contract* 1

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract InstalacionFV3 is ERC20("Owners_FV1", "PFV") {

    constructor() {
        _mint(0xCef0b33567Ac0235c3AA276C1Ee6faC2C378DcEA, 1000000000000000000);
        _mint(0x1177FfEEeA0f39AC04D5373b1e6f8C6Bacd0ff70, 1000000000000000000);
        _mint(0xDf06d4305e0f2ea0294b9e8163C6d39294C01Ce4, 1000000000000000000);
        _mint(0x68378aadfA2e237Af8E82a458dbaa4684D404920, 1000000000000000000);
        _mint(0xab0Eb2d948ab196EbEc20C3fcC8bCCBdA9b17637, 1000000000000000000);
        _mint(0x9c41B19d56bc177df0Fe8fb04A9D7C69df8617E6, 1000000000000000000);
        _mint(0x80d5313520870216a09F95625b4eaC2439388A4F, 1000000000000000000);
        _mint(0xcE0efb16362857927D09EdDFc4c53F1757Decd7E, 1000000000000000000);
        _mint(0x861DE4D21FF03315905Cd52f8C1CFc54fa88713b, 1000000000000000000);
        _mint(0x845A47463e85c769038Ed28DE68265Ba8FDC0Eb5, 1000000000000000000);
         }
}
```

### A.1.2 *Smart contract* 2

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract Autoconsumo_Compartido {

    mapping (address =>  int) Eh_con; //Energía horaria consumida. Lectura de
smart meter de consumidores.
    int E_gen_inst;  //Energía horaria generada por la instalación fotovoltaica
compartida. Lectura de smart meter de la instalación.
    int Precioh_excedentes; //Precio horario utilizado para la liquidación
interna de excedentes entre usuarios. Dato de origen externo.
```

```
    address[] addresses; //Array para almacenar las direcciones de los
participantes.
    uint counter_participants; //Contador del número de participantes.
    mapping (address =>  int) balance; //Balance en ETH de cada participante.

    IERC20 token1 = IERC20(0x37f85C353F8d63E44706cb3646CFeE3a43D3AF4D);
//Dirección del contrato SC1. Utilizado para asignar las participaciones de cada
usuario en la instalación fotovoltaica.

    //Función para recibir los datos de consumo horario.
    function Eh_con_input(int Datos_entrada) public {
          Eh_con[msg.sender] = Datos_entrada;
          addresses.push(msg.sender);
          counter_participants++;
          require(token1.balanceOf(msg.sender)>0, "Invalid sender
address");  //Esta función sólo puede ser llamada desde la dirección de un
usuario con participaciones en la instalación FV.
    }

     //Función para recibir los datos de generación horaria.
     function E_gen_inst_input(int Datos_entrada) public {
         E_gen_inst = Datos_entrada;
         require(msg.sender == 0xf00fFC43238F7c3f89D5883Fe75c32e99CEFB8F5,
"Invalid sender address");  //Esta función sólo puede ser llamada desde la
dirección de la compañía instalación FV.
    }

     //Función para recibir los datos de precio horario de excedentes.
    function Precioh_input(int Datos_entrada) public {
         Precioh_excedentes = Datos_entrada;
         require(msg.sender == 0x3dCc85457e3150D3A464b78955d2F64B0bEe603E,
"Invalid sender address");   //Esta función sólo puede ser llamada desde la
dirección encargada de incorporar estos datos externos al smart contract.
    }

     //Función para permitir a los usuarios enviar criptomonedas (ETH) al
contrato. La programación en Solididy convierte automáticamente las unidades de
ETH a wei (la división más pequeña posible de un ETH, siendo 1 ETH=10^18 wei)
     receive() external payable {
          balance[msg.sender] += int(msg.value);
     }

     //Función para permitir a los usuarios retirar criptomonedas (ETH) del
contrato.
     function withdraw(uint amount) external {
         require(balance[msg.sender] >= int(amount), "Insufficient balance.");
         balance[msg.sender] -= int(amount);
         payable(msg.sender).transfer(amount);
     }

     //Función para permitir a los usuarios consultar su balance.
```

```
     function consulta_balance() public view returns  (int) {
         return balance[msg.sender];
    }

     //Función donde se implementa el algoritmo de reparto de energía dentro de
la comunidad.
    function resultado() public returns (int[] memory, address[] memory) {

        require(msg.sender == 0x8e9546a5ddd799D9D54feF9f6fd048d055083A51,
"Invalid sender address"); //Esta función sólo puede ser llamada desde la
dirección de la compañía distribuidora.

        int[] memory shares = new int[](counter_participants); //Array para
almacenar el % de participación de cada usuario en la instalación FV.
        int[] memory Eh_gen = new int[](counter_participants); //Array para
almacenar la Energía horaria generada individualizada de cada usuario (resultado
de la función).
        int[] memory E_exc = new int[](counter_participants); //Array usado para
registrar energía excendentaria de los usuarios (diferencia entre energía
generada y consumida).
        int[] memory def = new int[](counter_participants); //Array para
identificar los usuarios que tienen déficit de energía. (Consumen más de lo que
generan)
        int[] memory def_ini = new int[](counter_participants);
        address[] memory addresses_temp = new address[](counter_participants);
//Array para almacenar las direcciones participantes en cada reparto horario de
energía.
        uint def_counter; //Contador de usuario deficitarios.
        int E_exc_nodef; //Sumatorio de energía excedente.
        int shares_def; //Participaciones de usuario deficitarios. Usado para
repartir energía excedente.
        int shares_def_aux; //Variable temporal
        int shares_nodef; //Participaciones de usuarios no deficitarios. Usado
para repartir energía excedente.
        int E_exc_aux; //Sumatorio de energía excedente. Variable temporal.

      //Se obtiene el porcentaje de participación de cada usuario en la
instalación FV.
        for (uint j=0;j<counter_participants;j++){
          addresses_temp [j] = addresses[addresses.length-j-1];
          shares[j] =
int(token1.balanceOf(addresses_temp[j])/100000000000000000);
        }

      //Se evalúa la energía excedente de cada usuario, y se etiquetan como
deficitarios o no deficitarios de energía.
        for (uint j=0;j<counter_participants;j++){
          E_exc[j] = E_gen_inst*shares[j]/100-Eh_con[addresses_temp[j]];
          if (E_exc[j]>=0) {def[j]=0; E_exc_nodef=E_exc_nodef+E_exc[j];
shares_nodef=shares_nodef+shares[j];} //Participante no deficitario
```

```
          else if (E_exc[j]<0)  {def[j]=1;def_ini[j]=1;def_counter++; shares_def
= shares_def + shares[j];}  //Participante
deficitario
      }
          shares_def_aux = shares_def;
      //En caso de que todos los participantes sean deficitarios o ninguno de
ellos lo sea, la energía generada individualizada es propocional a sus
participaciones en la instalación FV.
          if (def_counter==counter_participants||def_counter==0) {
               for (uint j=0;j<counter_participants;j++) {
                         Eh_gen[j] = E_gen_inst*shares[j]/100;
               }
          }
     //En caso contrario se efectúa un reparto y liquidación entre usuarios
excedentarios y deficitarios.
          else if(def_counter!=counter_participants) {
          while(E_exc_nodef!=0){    //Se repite el reparto hasta que la energía
excedentaria es cero, o no existen participantes deficitarios.
                E_exc_aux=0;
               for (uint
j=0;j<counter_participants;j++){
                    if (def[j]==1){
                         E_exc[j] =  E_exc[j] +
E_exc_nodef*shares[j]/shares_def; //Se reparte la energía excedentaria entre los
participantes deficitarios.
                         if (E_exc[j]>=0) {def[j]=0;def_counter--
;E_exc_aux=E_exc_aux+E_exc[j];shares_def_aux = shares_def_aux-shares[j];} //Se
evalúa si sigue siendo deficitario.
                         }
               }

               E_exc_nodef = E_exc_aux;
               shares_def = shares_def_aux;

               if(def_counter==0){   //Si no existen participantes deficitarios,
se finaliza el bucle. Se calcula la energía generada individualizada y se
efectúa automáticamente la liquidación de criptomonedas entre usuarios.
                    for(uint j=0;j<counter_participants;j++){
                         if(def_ini[j]==0){
                              Eh_gen[j] =
Eh_con[addresses_temp[j]]+E_exc_aux*shares[j]/shares_nodef;
                              balance[addresses_temp[j]] +=
((E_gen_inst*shares[j]/100-Eh_gen[j])*Precioh_excedentes)/100000;
                          }
                         else if(def_ini[j]==1){
                              Eh_gen[j] = Eh_con[addresses_temp[j]];
                              balance[addresses_temp[j]] +=
((E_gen_inst*shares[j]/100-Eh_gen[j])*Precioh_excedentes)/100000;
                          }
                    }
                    break;
```

```
                }
                else if(def_counter>0){
                     if(E_exc_nodef==0){ //Si la energía deficitaria es cero, se
finaliza el bucle. Igualmente, se calcula la energía generada individualizada y
se efectúa automáticamente la liquidación de criptomonedas entre usuarios.
                          for(uint j=0;j<counter_participants;j++){
                               if(def[j]==0){
                                    Eh_gen[j] = Eh_con[addresses_temp[j]];
                                    balance[addresses_temp[j]] +=
((E_gen_inst*shares[j]/100-Eh_gen[j])*Precioh_excedentes)/100000;
                               }
                               else if(def[j]==1){
                                    Eh_gen[j] =
Eh_con[addresses_temp[j]]+E_exc[j];
                                    balance[addresses_temp[j]] +=
((E_gen_inst*shares[j]/100-Eh_gen[j])*Precioh_excedentes)/100000;
                               }
                          }
                     }
                }
           }
     }
     counter_participants = 0;
     return (Eh_gen, addresses_temp); //La función devuelve un array con la
dirección de cada usuario, y su energía generada individualizada.
     }
}
```

## A.2 Código Python

```
from web3 import Web3  #librería que permite interactuar con smart contracts
import simplejson as json #librería para manejar datos tipo json
import pandas as pd #libreria para tratamiento de datos
import numpy as np #librería para cálculo numérico

#Se leen desde archivos Excel los datos de consumo, generación y precios. Se
almacenan en variables locales para su uso.
#Los datos de energía se manejan en W*10^15 (Watios con quince ceros) debido que
la programación de smart contracs en Solidity no soporta variables float.
#Los datos de precios se manejan en €/MWh*100.

consumos =
pd.read_excel(r"C:\Users\Usuario\Desktop\aplicacion\Datos\LOAD_PROFILE_HOURLY.xl
sx")
generacion =
pd.read_excel(r"C:\Users\Usuario\Desktop\aplicacion\Datos\GENERATION_PROFILE_HOU
RLY.xlsx")
precio_excedentes =
pd.read_excel(r"C:\Users\Usuario\Desktop\aplicacion\Datos\PRECIO_PVPC_EXCEDENTES
_HOURLY.xlsx")

numero_datos = 8760 #número de datos usados en la simulación. 8760 horas (1
año).
datos_consumo = [[None] * 8760 for i in range(10)] #array para almacenar y
manejar los datos de consumo.
datos_reparto_Egen = [[None] * 8760 for i in range(10)] #array para almacenar
los datos resultantes del reparto efectuado por el algoritmo del smart contract.

#Se almacenan los datos en arrays:
datos_consumo[0] = consumos['CHR01'].values.tolist()
datos_consumo[1] = consumos['CHR05'].values.tolist()
datos_consumo[2] = consumos['CHR10'].values.tolist()
datos_consumo[3] = consumos['CHR15'].values.tolist()
datos_consumo[4] = consumos['CHR17'].values.tolist()
datos_consumo[5] = consumos['CHR27'].values.tolist()
datos_consumo[6] = consumos['CHR34'].values.tolist()
datos_consumo[7] = consumos['CHR44'].values.tolist()
datos_consumo[8] = consumos['CHR51'].values.tolist()
datos_consumo[9] = consumos['CHR52'].values.tolist()
generador_1 = generacion['Energy (Wh)'].values.tolist()
datos_precio_excedentes = precio_excedentes['value (€/MWh)'].values.tolist()

#Se tratan los datos para modificar su escala y forzar que sean de tipo int,
debido a que el smart contract no soporta variables tipo float.
for i in range(10):
    for j in range(numero_datos):
        datos_consumo[i][j] = int(datos_consumo[i][j]*10**18)

for i in range(numero_datos):
```

```
    generador_1[i] = int(generador_1[i]*10**15)

for i in range(numero_datos):
    datos_precio_excedentes[i] = int(datos_precio_excedentes[i]*100) #Se
multiplica por 100 para utilizar datos tipo int en lugar de float.


#Para poder interactuar con la blockchain y el smartcontract:
ganache_url = "HTTP://127.0.0.1:7545"           #Dirección de la blockchain
local implementada,
web3 = Web3(Web3.HTTPProvider(ganache_url))     #Se crea el objeto web3 que
permitirá interactuar con la blockchain.

print(web3.isConnected())  #Se verifica que la blockchain está funcionado.

#Datos del contrato que ejecuta el algoritmo, desplegado en la blockchain local.
abi =
json.loads('[{"inputs":[],"name":"E_gen_inst","outputs":[{"internalType":"int256
","name":"","type":"int256"}],"stateMutability":"view","type":"function"},{"inpu
ts":[{"internalType":"int256","name":"Datos_entrada","type":"int256"}],"name":"E
_gen_inst_input","outputs":[],"stateMutability":"nonpayable","type":"function"},
{"inputs":[{"internalType":"address","name":"","type":"address"}],"name":"Eh_con
","outputs":[{"internalType":"int256","name":"","type":"int256"}],"stateMutabili
ty":"view","type":"function"},{"inputs":[{"internalType":"int256","name":"Datos_
entrada","type":"int256"}],"name":"Eh_con_input","outputs":[],"stateMutability":
"nonpayable","type":"function"},{"inputs":[{"internalType":"uint256","name":"","
type":"uint256"}],"name":"Eh_gen_final","outputs":[{"internalType":"int256","nam
e":"","type":"int256"}],"stateMutability":"view","type":"function"},{"inputs":[{
"internalType":"int256","name":"Datos_entrada","type":"int256"}],"name":"Precioh
_input","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs"
:[{"internalType":"uint256","name":"","type":"uint256"}],"name":"addresses","out
puts":[{"internalType":"address","name":"","type":"address"}],"stateMutability":
"view","type":"function"},{"inputs":[{"internalType":"address","name":"","type":
"address"}],"name":"balance","outputs":[{"internalType":"int256","name":"","type
":"int256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"co
nsulta_balance","outputs":[{"internalType":"int256","name":"","type":"int256"}],
"stateMutability":"view","type":"function"},{"inputs":[],"name":"counter_partici
pants","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateM
utability":"view","type":"function"},{"inputs":[],"name":"resultado","outputs":[
{"internalType":"int256[]","name":"","type":"int256[]"},{"internalType":"address
[]","name":"","type":"address[]"}],"stateMutability":"nonpayable","type":"functi
on"},{"inputs":[{"internalType":"uint256","name":"amount","type":"uint256"}],"na
me":"withdraw","outputs":[],"stateMutability":"nonpayable","type":"function"},{"
stateMutability":"payable","type":"receive"}]')
address = web3.toChecksumAddress("0x3c90bdBBD444bE966a7b7bE718009Ac0D9370B65")

#Se instancia el contrato.
contract = web3.eth.contract(address=address, abi=abi)

#Bucle para evaluar el reparto de energía en cada hora.
```

```
for i in range(1,8760):

#Simulación de transacciones al smart contract por parte de los contadores
inteligentes de los consumidores:
    for j in range(10):
     web3.eth.defaultAccount = web3.eth.accounts[j] #Cuenta utilizada para
enviar la transacción. En la blockchain creada, las 10 primeras (de 0 a 9)
direcciones se han reservado para las mediciones de consumo de los usuarios.
     contract.functions.Eh_con_input(datos_consumo[j][i]).transact()

#Simulación de transacciones al smart contract por parte del contador de la
instalación FV
    web3.eth.defaultAccount = web3.eth.accounts[11] #Cuenta utilizada para
enviar la transacción. En la blockchain creada, la número 11 se ha reservado
para las mediciones de generación.
    contract.functions.E_gen_inst_input(generador_1[i]).transact()

#Simulación de envío de datos de precio de venta de excendetes para liquidación
interna en la comunidad.
    web3.eth.defaultAccount = web3.eth.accounts[10] #Cuenta utilizada para
enviar la transacción. En la blockchain creada, la número 10 se ha reservado
para el envío de datos de precios.
    contract.functions.Precioh_input(datos_precio_excedentes[i]).transact()

#Simulación de transacción solicitada por la compañía distribuidora para obtener
los valores de reparto de la energía generada por la instalación FV
    web3.eth.defaultAccount = web3.eth.accounts[12] #Cuenta utilizada para
enviar la transacción. En la blockchain creada, la número 12 se ha reservado
para las transacciones de la compañía distribuidora.
    resultado_reparto = contract.functions.resultado().call()
    contract.functions.resultado().transact()

    for k in range(10):
        datos_reparto_Egen[k][i] = resultado_reparto[0][k]/10**18 #Se almacena
en el array "datos_reparton_Egen" el resultado de energía generada
individualizada de cada participante, para su posterior evaluación.


#Se escriben los resultados obtenidos en un archivo Excel, para su análisis y
comprobación del buen funcionamiento del algoritmo.
reparto = pd.DataFrame(datos_reparto_Egen).T
reparto.to_excel(excel_writer="C:/Users/Usuario/Desktop/aplicacion/Datos/REPARTO
_GEN_HOURLY.xlsx"
```

# REFERENCIAS


[1] A. Preukschat, *Blockchain: La revolución industrial de internet*. Barcelona: Gestión 2000, 2017.

[2] D. Kavanagh and P. J. Ennis, "Cryptocurrencies and the emergence of blockocracy," *Information Society*, vol. 36, no. 5, pp. 290–300, Aug. 2020.

[3] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: www.bitcoin.org.

[4] *De Alan Turing al 'ciberpunk': la historia de blockchain.* [Online]. Available: https://www.bbva.com/es/historia-origen-blockchain-bitcoin/.

[5] W. Diffie, W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans Inf Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[6] R. C. Merkle, "A digital signature based on a convencional encryptation function," in *Proc. Conf. Theory Appl. Cryptograph*. Techn., 1987, pp. 369–378.

[7] R. L. Rivest, A. Shamir y L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, vol. 26, n.º 1, pp. 96–99, Jan. 1983.

[8] S. Haber y W. S. Stornetta, "How to time-stamp a digital document", J. Cryptol., vol. 3, n.º 2, pp. 99–111, Jan. 1991.

[9] Adam Back, *Hash cash postage implementation*. [Online]. Available: http://www.hashcash.org/papers/announce.txt.

[10] D. Chaum, "Blind Signatures for Untraceable Payments", en Advances in Cryptology. Boston, MA: Springer US, 1983, pp. 199–203.

[11] W. Dai, *b-money*. [Online]. Available: http://www.weidai.com/bmoney.txt

[12] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday*, vol. 2, no. 9, Sep. 1997.

[13] Ethereum documentation. [Online]. Available: https://ethereum.org/.

[14] H. Delfs y H. Knebl, *Introduction to Cryptography*. Berlin, Heidelberg: Springer Berl. Heidelb., 2015.

[15] *Lifetimes of cryptographic hash functions.* [Online]. Available: http://valerieaurora.org/hash.html.

[16] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of Used Cryptography in Blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.

[17] T. Kanstrén, *Merkle Trees: Concepts and Use Cases.* [Online]. Available: https://medium.com/coinmonks/merkle-trees-concepts-and-use-cases-5da873702318.

[18] S. Nakov, *Practical Cryptography for Developers*. [Online]. Available: https://cryptobook.nakov.com/symmetric-key-ciphers/ethereum-wallet-encryption.

[19] B. D. Geliot, *Introducción a la Criptografía en Blockchain.* [Online]. Available: https://medium.com/boske/criptograf%C3%ADa-f9bad85e072d.

[20] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," NIST, Gaithersburg, MD, USA, Tech. Rep. 8202, 2018.

[21] J. Garzik, *Public versus Private Blockchains Part 1: Permissioned Blockchains White Paper*. [Online]. Available: https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf

[22] J. Garzik, *Public versus Private Blockchains Part 2: Permissionless Blockchains White Paper*. [Online]. Available: https://bitfury.com/content/downloads/public-vs-private-pt2-1.pdf

[23] *What is a Consortium Blockchain & How Does it Work?* [Online]. Available: https://shardeum.org/blog/what-is-a-consortium blockchain/#How_Does_a_Consortium_Blockchain_Work.

[24] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, Canada, 2017, pp. 2567-2572.

[25] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," in *Concurrency: The Works of Leslie Lamport*, New York, NY, USA: Association for Computing Machinery, 2019, pp. 203–226.

[26] I. Bashir, *Mastering Blockchain: A Deep Dive into Distributed Ledgers, Consensus Protocols, Smart Contracts, DApps, Cryptocurrencies, Ethereum, and More*, *3rd Edition*. Packt Publ. Ltd., 2020.

[27] S. Ghimire and H. Selvaraj, "A survey on bitcoin cryptocurrency and its mining," in *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Feb. 2019.

[28] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 557–564.

[29] *Qué tanto contamina el bitcoin, la moneda que consume más electricidad que Finlandia, Suiza o Argentina.* [Online]. Available: https://www.bbc.com/mundo/noticias-56049826.

[30] Daniel Frumkin, Alex Dean, and Thomas Shaddox, *Nothing-at-stake problem*. [Online]. Available: https://golden.com/wiki/Nothing-at-stake_problem-639PVZA.

[31] S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, Jun. 2020.

[32] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc., 2015.

[33] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday*, vol. 2, no. 9, Sep. 1997.

[34] J. Stark, *Making sense of blockchain smart contracts.* [Online]. Available: https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts/.

[35] Delmolino Kevin, Arnett Mitchell, Kosba Ahmed, Miller Andrew, and Shi Elaine, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab", *Lecture Notes in Computer Science*, vol. 9604 LNCS, 2016, pp. 79-94.

[36] V. Morabito, "Smart contracts and licensing," in *Business Innovation Through Blockchain*. Cham, Switzerland: Springer, 2017, pp. 101 124.

[37] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Trans Syst Man Cybern Syst*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[38] K. Bhargavan et al., "Formal verification of smart contracts: Short paper," in *Proc. ACM Workshop Program. Lang. Anal. Security (PLAS)*, Vienna, Austria, Oct. 2016, pp. 91–96

[39] Wood, G. Ethereum: "A secure decentralised generalised transaction ledger". *Ethereum project yellow paper,* vol. 151, no 2014, p. 1-32.

[40] Documentación Hiperledger. [Online]. Available: https://hyperledger-fabric.readthedocs.io/

[41] Guillermo Araujo Riestra, *Hyperledger Fabric — Conceptos y Tipos de Nodos*. [Online]. Available: https://medium.com/babel-go2chain/hyperledger-fabric-conceptos-y-tipos-de-nodos-4f24ce1ec4fd

[42] Documentación Hiperledger, *Ledgers and Chaincode*. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.1/peers/peers.html#ledgers-and-chaincode

[43] S. Voshmgir, *Token Economy: How the Web3 reinvents the Internet*. Shermin Voshmgir, BlockchainHub Berl., 2020.

[44] P. Kasireddy, *The Architecture of a Web 3.0 application*. [Online]. Available:

https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application.

[45] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating Suitability of Applying Blockchain," in *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS*, Institute of Electrical and Electronics Engineers Inc., Feb. 2018, pp. 158–161.

[46] *¿Qué son las 'stablecoins' y para qué sirven*? [Online]. Available: https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/.

[47] *Cryptocurrency market capitalization charts*. [Online]. Available: https://coinmarketcap.com/charts/.

[48] *Qué es un 'token' y para qué sirve*. [Online]. Available: https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/.

[49] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?" in *Proc. Hamburg Int. Conf. Logistics (HICL)*, 2017, pp. 3–18.

[50] C. S. Sung and J. Y. Park, "Understanding of blockchain-based identity management system adoption in the public sector," *Journal of Enterprise Information Management*, vol. 34, no. 5, pp. 1481–1505, Nov. 2021.

[51] A. Takyar, *All about blockchain scalability solutions.* [Online]. Available: https://www.leewayhertz.com/blockchain-scalability solutions/#:~:text=Conclusion,What%20is%20blockchain%20scalability%3F,a%20huge%20amount%20of%20data.

[52] D. Geroni, *Blockchain Scalability Problem*. [Online]. Available: https://101blockchains.com/blockchain-scalability-challenges/.

[53] *What Is Blockchain Sharding: An Introduction To A Blockchain Scaling Solution.* [Online]. Available: https://101blockchains.com/blockchain-sharding/.

[54] *Blockchain Layer 1 VS Layer 2 Scaling Solution: Key Differences.* [Online]. Available: https://zipmex.com/learn/layer-1-vs-layer-2/.

[55] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger Approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019.

[56] G. Dileep, "A survey on smart grid technologies and applications," *Renew Energy*, vol. 146, pp. 2589–2625, Feb. 2020.

[57] S. Kakran and S. Chanana, "Smart operations of smart grids integrated with distributed generation: A review," *Renewable and Sustainable Energy Reviews*, vol. 81. Elsevier Ltd, pp. 524–535, Jan. 01, 2018.

[58] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *IEEE Access*, vol. 7, pp. 62962–63003, 2019.

[59] K. Wang *et al.*, "A survey on energy internet: Architecture, approach, and emerging technologies," *IEEE Syst J*, vol. 12, no. 3, pp. 2403–2416, Sep. 2018.

[60] K. Mahmud, B. Khan, J. Ravishankar, A. Ahmadi, and P. Siano, "An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview," *Renewable and Sustainable Energy Reviews*, vol. 127. Elsevier Ltd, Jul. 01, 2020.

[61] C. H. Lo and N. Ansari, "Decentralized controls and communications for autonomous distribution networks in smart grid," *IEEE Trans Smart Grid*, vol. 4, no. 1, pp. 66–77, 2013.

[62] Y. J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 58–65, Nov. 2010.

[63] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2886–2927, Jul. 2019.

[64] S. N. Islam, Z. Baig, and S. Zeadally, “Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures,” *IEEE Trans Industr Inform*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[65] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, Mar. 2020.

[66] M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100. Elsevier Ltd, pp. 143–174, Feb. 01, 2019.

[67] M. B. Mollah *et al.*, “Blockchain for Future Smart Grid: A Comprehensive Survey,” *IEEE Internet of Things Journal*, vol. 8, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 18–43, Jan. 01, 2021.

[68] *Electropedia: The World's Online Electrotechnical Vocabulary*. [Online]. Available: https://www.electropedia.org/.

[69] K. Kimani, V. Oduol, and K. Langat, “Cyber security challenges for IoT-based smart grid networks,” *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019.

[70] K. Thakur, M. L. Ali, N. Jiang, and M. Qiu, “Impact of Cyber-Attacks on Critical Infrastructure,” in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, Apr. 2016, pp. 183–186.

[71] P. Zhuang, T. Zamir, and H. Liang, “Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey,” *IEEE Trans Industr Inform*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[72] R. Deng, P. Zhuang, and H. Liang, “False Data Injection Attacks Against State Estimation in Power Distribution Systems,” *IEEE Trans Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[73] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, “Smart meter data privacy: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2820–2835, Jun. 2017.

[74] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 998–1010, 2012.

[75] P. Danzi, M. Angjelichinoski, Č. Stefanović and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Dresden, Germany, 2017, pp. 45-51.

[76] G. C. Lazaroiu and M. Roscia, "Blockchain and smart metering towards sustainable prosumers," *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM),* Amalfi, Italy, 2018, pp. 550-555.

[77] Z. Guan *et al.*, “Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities,” *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[78] M. del R. F. Jimeno and M. S. Cebrián, ‘El mercado eléctrico en España: La convivencia de un monopolio natural y el libre mercado’, Revista europea de derechos fundamentales, no. 25, pp. 257–297, 2015.

[79] D. Bowker et al., ‘Trading electricity with Blockchain systems’, 2023.

[80] D. Livingston, V. Sivaram, M. Freeman, and M. Fiege, “Council on Foreign Relations Applying Blockchain Technology to Electric Power Systems,” 2018.

[81] *Overview of blockchain for energy and commodity trading*. EY, USA, 2017.

[82] M. Merz, *Potential of the Blockchain Technology in Energy Trading*. [Online]. Available: https://www.ponton.de/downloads/mm/Potential-of-the-Blockchain-Technology-in-Energy-Trading_Merz_2016.en.pdf

[83] REE Procedimientos de Operación, [Online]. Available: https://www.ree.es/es/actividades/operacion-del-sistema-electrico/procedimientos-de-operacion

[84] M. Merz, *Enerchain Project Overview and Key Insights*. [Online]. Available: http://www.ponton.de

[85] *Blockchain Enigma. Paradox. Opportunity*. Deloitte, UK, 2016.

[86] *Blockchain-an opportunity for energy producers and consumers.* PwC, 2016.

[87] *Endesa y Gas Natural Fenosa realizan por primera vez en España una transacción de energía con la tecnología blockchain.* [Online]. Available: https://www.endesa.com/es/prensa/sala-de-prensa/noticias/transicion-energetica/digitalizacion/endesa-y-gas-natural-fenosa-realizan-primera-transaccion-energia-con-blockchain-en-espana.

[88] Tendermit documentation. [Online]. Available: https://tendermint.com/.

[89] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable and Sustainable Energy Reviews*, vol. 82. Elsevier Ltd, pp. 1675–1684, Feb. 01, 2018.

[90] H. Khajeh, A. A. Foroud, and H. Firoozi, "Robust bidding strategies and scheduling of a price-maker microgrid aggregator participating in a pool-based electricity market," *IET Generation, Transmission and Distribution*, vol. 13, no. 4, pp. 468–477, Feb. 2019.

[91] S. Talari, H. Khajeh, M. Shafie-khah, B. Hayes, H. Laaksonen, and J. P. S. Catalão, "Chapter 5 - The role of various market participants in blockchain business model," in *Blockchain-based Smart Grids*, M. Shafie-khah, Ed., Academic Press, 2020, pp. 75–102.

[92] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer-to-peer and community-based markets: A comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 104. Elsevier Ltd, pp. 367–378, Apr. 01, 2019.

[93] Y. Parag and B. K. Sovacool, "Electricity market design for the prosumer era", *Nature energy*, vol. 1, no. 4, pp. 1–6, 2016.

[94] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Appl Energy*, vol. 210, pp. 870–880, Jan. 2018.

[95] T. Samad and A. M. Annaswamy, "Controls for Smart Grids: Architectures and Applications," *Proceedings of the IEEE*, vol. 105, no. 11, pp. 2244–2261, Nov. 2017.

[96] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid - Challenges, issues, advantages and status," in *2011 IEEE/PES Power Systems Conference and Exposition, PSCE 2011*, 2011.

[97] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans Smart Grid*, vol. 1, no. 1, pp. 20–27, 2010.

[98] W. Saad, A. L. Glass, N. B. Mandayam, and H. V. Poor, "Toward a consumer-centric grid: A behavioral perspective," *Proceedings of the IEEE*, vol. 104, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 865–882, Apr. 01, 2016.

[99] L. T. Berger, A. Schwager, and J. J. Escudero-Garzás, "Power line communications for smart grid applications," *Journal of Electrical and Computer Engineering*. 2013.

[100] Y. T. Aklilu and J. Ding, "Survey on blockchain for smart grid management, control, and operation," *Energies*, vol. 15, no. 1. MDPI, Jan. 01, 2022.

[101] M. Asim Aftab, S. M. S. Hussain, and I. Ali, "ICT Technologies, Standards and Protocols for Active Distribution Network Automation and Management," in *Advanced Communication and Control Methods for Future Smartgrids*, IntechOpen, 2019.

[102] L. Shen *et al.*, "Blockchain-based Power Grid Data Asset Management Architecture," in *Proceedings - 2020 International Conference on Computer Science and Management Technology, ICCSMT 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 207–211.

[103] D. Zheng *et al.*, "The concept of microgrid and related terminologies," in *Microgrid Protection and Control*, Elsevier, 2021, pp. 1–12.

[104] A. Mnatsakanyan, H. Albeshr, A. Al Marzooqi, and E. Bilbao, "Blockchain-integrated virtual power plant demonstration," in *2020 2nd International Conference on Smart Power and Internet Energy Systems, SPIES 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 172–175.

[105] Q. Yang, H. Wang, T. Wang, S. Zhang, X. Wu, and H. Wang, "Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant," *Appl Energy*, vol. 294, Jul. 2021.

[106] A. Aderibole *et al.*, "Blockchain Technology for Smart Grids: Decentralized NIST Conceptual Model," *IEEE Access*, vol. 8, pp. 43177–43190, 2020.

[107] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain Applications in Smart Grid-Review and Frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.

[108] F. Rahimi *et al.*, "IEEE Blockchain-Enabled Transactive Energy Position Paper" 2021.

[109] Z. Li, S. Bahramirad, A. Paaso, M. Yan, and M. Shahidehpour, "Blockchain for decentralized transactive energy management system in networked microgrids," *Electricity Journal*, vol. 32, no. 4, pp. 58–72, May 2019.

[110] A. Brooks, E. Lu, D. Reicher, C. Spirakis, and B. Weihl, "Demand dispatch," *IEEE Power and Energy Magazine*, vol. 8, no. 3, pp. 20–29, May 2010.

[111] A. Hasankhani, S. Mehdi Hakimi, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *International Journal of Electrical Power and Energy Systems*, vol. 129. Elsevier Ltd, Jul. 01, 2021.

[112] C. Yapa, C. de Alwis, M. Liyanage, and J. Ekanayake, "Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research," *Energy Reports*, vol. 7. Elsevier Ltd, pp. 6530–6564, Nov. 01, 2021.

[113] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Computer Communications*, vol. 151. Elsevier B.V., pp. 395–418, Feb. 01, 2020.

[114] T. Cioara, C. Pop, R. Zanc, I. Anghel, M. Antal, and I. Salomie, "Smart grid management using blockchain: Future scenarios and challenges," in *Proceedings - RoEduNet IEEE International Conference*, IEEE Computer Society, Dec. 2020.

[115] "DOUE" núm. 119, de 4 de mayo de 2016, páginas 1 a 88 (88 págs.)

[116] M. L. DI Silvestre, P. Gallo, E. R. Sanseverino, G. Sciume, and G. Zizzo, "Aggregation and Remuneration in Demand Response with a Blockchain-Based Framework," *IEEE Trans Ind Appl*, vol. 56, no. 4, pp. 4248–4257, Jul. 2020.

[117] F. Wang, K. Li, C. Liu, Z. Mi, M. Shafie-Khah, and J. P. S. Catalao, "Synchronous pattern matching principle-based residential demand response baseline estimation: Mechanism analysis and approach description," *IEEE Trans Smart Grid*, vol. 9, no. 6, pp. 6972–6985, Nov. 2018.

[118] I. V. Lokshina, M. Greguš, and W. L. Thomas, "Application of integrated building information modeling, iot and," in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 497–502.

[119] G. M. Madhu, C. Vyjayanthi and C. N. Modi, "A Novel Framework for Monitoring Solar PV based Electric Vehicle Community Charging Station and Grid Frequency Regulation using Blockchain," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur,* India, 2019, pp. 1-7.

[120] C. Plaza, J. Gil, F. de Chezelles and K. A. Strang, "Distributed Solar Self-Consumption and Blockchain Solar Energy Exchanges on the Public Grid Within an Energy Community," *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Palermo, Italy, 2018, pp. 1-4.

[121] IDAE, *Comunidades energéticas*. [Online]. Available: https://www.idae.es/ayudas-y-financiacion/comunidades-energeticas.

[122] D. Frieden, A. Tuerk, J. Roberts, S. d'Herbemont, and A. Gubina, *Collective self-consumption and energy communities: Overview of emerging regulatory approaches in Europe*. Compile, 2019.

[123] BOE, "Real Decreto 244/2019, de 5 de abril, por el que se regulan las condiciones administrativas, técnicas y económicas del autoconsumo de energía eléctrica.," 2019.

[124] BOE, "Ley 24/2013, de 26 de diciembre, del Sector Eléctrico"

[125] Truffle Suite documentation. [Online]. Available: https://trufflesuite.com/docs/ganache/.

[126] Solidity documentation. [Online]. Available: https://docs.soliditylang.org/en/v0.6.1/index.html.

[127] Remix IDE documentation. [Online]. Available: https://remix-ide.readthedocs.io/en/latest/.

[128] Metamask documentation. [Online]. Available: https://docs.metamask.io/guide/.

[129] Visual Studio Code documentation. [Online]. Available: https://code.visualstudio.com/docs.

[130] Web3 library documentation. [Online]. Available: https://web3js.readthedocs.io/en/v1.3.4/getting-started.html.

[131] OpenZeppeling, *ERC20 library documentation*. [Online]. Available: https://docs.openzeppelin.com/contracts/4.x/erc20.

[132] N. Pflugradt, P. Stenzel, L. Kotzur, and D. Stolten, "LoadProfileGenerator: An Agent-Based Behavior Simulation for Generating Residential Load Profiles," *J Open Source Softw*, vol. 7, no. 71, p. 3574, Mar. 2022.

[133] European Commission, *Photovoltaic Geographical Information System*. [Online]. Available: https://re.jrc.ec.europa.eu/pvg_tools/en/.

[134] Esios red eléctrica, *Precio de la energía excedentaria del autoconsumo para PVPC*. [Online]. Available: https://www.esios.ree.es/es/pvpc.