Privacidad en Smart Grid mediante Smart Contracts y agregación de datos

Joan Ferré-Queralt*, Carles Anglés-Tafalla*, Julián Salas†, Guillermo Navarro-Arribas‡,
Alexandre Viejo*, David Megías†, Jordi Castellà-Roca*

* Universitat Rovira i Virgili
Dept. d'Enginyeria Informàtica i Matemàtiques, CYBERCAT,
Av. Països Catalans 26, E-43007 Tarragona, Spain
{joan.ferreq, carles.angles, alex.viejo,jordi.castella}@urv.cat

† Universitat Oberta de Catalunya
Internet Interdisciplinary Institute (IN3), CYBERCAT,
Rambla del Poblenou, 154, 08018, Barcelona, Spain
{jsalaspi, dmegias}@uoc.edu

‡ Universitat Autonoma de Barcelona
Dept. d'Enginyeria de la Informació i les Comunicacions, CYBERCAT,
08193 Bellaterra, Catalonia, Spain
guillermo.navarro@uab.cat

***Resumen*—En este trabajo presentamos un sistema para la gestión de redes de distribución de energía inteligentes (*Smart Grids*) donde se preserva la seguridad y privacidad de los usuarios. La propuesta utiliza tecnología blockchain y *Smart Contracts* como componentes centrales, teniendo en cuenta la privacidad de los usuarios, la disponibilidad y la seguridad del sistema. Al mismo tiempo, ofrece medidas para identificar y tomar acciones punitivas contra usuarios maliciosos. El sistema proporciona, finalmente, información de consumo y producción de energía para su publicación o uso, donde se preserva el anonimato de los usuarios con el principio de k-anonimidad.**

***Index Terms*—Smart meter, privacidad de datos, blockchain, k-anonimidad, descentralización, Smart Contracts**

I. Introducción

Tradicionalmente, la generación y distribución de energía se han realizado mediante la instalación de centrales eléctricas que utilizan combustibles fósiles, como carbón y gas natural, o mediante la explotación de la energía nuclear. Estas soluciones presentan notables desventajas, como los elevados costes asociados a la construcción y mantenimiento de estos complejos y la infraestructura de transporte requerida, así como las emisiones de gases de efecto invernadero y la generación de residuos nucleares. Ante esta problemática, resulta evidente la necesidad de explorar alternativas y orientarse hacia otras fuentes principales de energía.

En los últimos años, el coste de implantación de las fuentes de energía renovable, como la eólica y la solar, ha disminuido significativamente, haciéndolas más competitivas y propulsando a la Unión Europea hacia un sector eléctrico más sostenible y libre de emisiones de carbono. A pesar de estos avances, la menor fiabilidad, disponibilidad y eficiencia de las energías renovables, en comparación con las fuentes tradicionales [1], han dificultado su transición desde los combustibles fósiles, impidiendo que la adopción de las energías renovables progrese al ritmo esperado[1].

Una estrategia efectiva para optimizar la disponibilidad y eficiencia del sistema de distribución de energía consiste en ubicar a los productores de energía más cerca de los consumidores, pudiendo así reducir significativamente los costes y pérdidas producidos por la transmisión de energía en largas distancias. La relevancia de esta estrategia se acentúa con la adopción de tecnologías de energía renovable distribuida, como paneles solares, que abre la posibilidad de un modelo de producción y consumo de electricidad local y descentralizado [2]. En este contexto, algunas propiedades están comenzando a integrar recursos energéticos distribuidos (*Distributed Energy Resources*, DER), como los paneles solares, para generar y consumir su propia electricidad, pudiendo vender el excedente de energía a la red principal en caso de producir mas energía de la necesaria. No obstante, los precios de venta de este excedente energético a menudo no son lo suficientemente atractivos debido a los impuestos o tarifas adicionales impuestas por gobiernos o compañías eléctricas.

A la luz de lo anterior, se puede concluir que la sociedad se beneficiaría claramente de la adopción de un nuevo modelo energético que ayude a satisfacer la creciente demanda, incorporando energía generada por productores locales que favorezca un paradigma más descentralizado. En este escenario, las *Smart Grids* se ha propuesto como una forma de modernizar y optimizar la distribución de energía, fomentando la contribución energética de propiedades con DER a la red principal. Contribuyendo a este paradigma, tecnologías como los *Smart Contracts* [3], junto con el subyacente *public digital ledger* conocido como Blockchain, se han establecido como herramientas robustas para el diseño de nuevos modelos descentralizados que permiten el acuerdo de transacciones

[1] IEA: Wholesale energy costs made simple, https://www.edfenergy.com

de recursos arbitrarios, como la producción y consumo de energía. No obstante, la integración de estas tecnologías en el sector eléctrico presenta nuevos desafíos en privacidad, dado que los datos publicados en el Blockchain son de dominio público y, por ende, requieren de medidas de protección adecuadas.

El artículo se organiza de la manera siguiente. En el apartado II se presentan varios artículos relacionados con este trabajo. El apartado III muestra una descripción general del sistema y en el IV se muestran los detalles del sistema relacionados con el uso de *Smart Contracts*. En el apartado V se presenta la agregación de datos y, finalmente, el apartado VI concluye el artículo.

II. Trabajos Relacionados

Los sistemas de redes inteligentes han sido ampliamente estudiados en los últimos años, con diversas implementaciones que se enfocan en diferentes aspectos. Nos centramos en los *prosumers*, usuarios que son capaces de producir y consumir energía, que comercian electricidad dentro de la *Smart Grid*.

El concepto de una *Smart Grid* fue presentado por primera vez por el Departamento de Energía de los Estados Unidos en 2007 [4]. Este informe esbozaba la visión de una red modernizada que pudiera integrar diversos recursos de energía distribuida, mejorar la fiabilidad y la eficiencia, y permitir la comunicación bidireccional entre las empresas de servicios públicos y los consumidores. Sin embargo, a medida que las *Smart Grid* evolucionan e incorporan más elementos distribuidos, las preocupaciones de seguridad respecto al control centralizado se vuelven cada vez más prominentes. Los sistemas distribuidos, con su redundancia inherente y su naturaleza a prueba de manipulaciones, ofrecen soluciones potenciales a estos desafíos de seguridad, como se discute en [5].

Un paso significativo hacia un sistema descentralizado de comercio de electricidad fue presentado en [6]. Los autores propusieron una moneda de energía basada en la tecnología blockchain [7]. Este enfoque allana el camino para la integración sin problemas de blockchain y contratos inteligentes dentro de la *Smart Grid*, permitiendo el comercio de energía entre pares de manera segura y transparente sin la necesidad de una autoridad central. Desde esta propuesta inicial, numerosos estudios han explorado diversas arquitecturas de blockchain para la implementación de *Smart Grid*, como se evidencia en los trabajos presentados en [8], [6], [9]. Estos estudios demuestran la versatilidad y el potencial de la tecnología blockchain para revolucionar el sector energético.

Sin embargo, las soluciones blockchain mencionadas emplean un mecanismo de consenso de *Proof of Work* (PoW). Aunque PoW ofrece fuertes garantías de seguridad, es conocido por su alto consumo de energía debido a la considerable potencia computacional requerida para validar transacciones [10]. Esta alta huella energética contradice los principios de una *Smart Grid*. Por lo tanto, explorar mecanismos de consenso alternativos que sean más eficientes energéticamente mientras mantienen la integridad y seguridad del sistema debería ser una prioridad.

Existen trabajos que no usan PoW y, en su luga, emplean otros mecanismos de consenso, como los presentados en [11], [12], que también exploran la integración de la tecnología blockchain en sistemas energéticos sin depender de PoW. Sin embargo, estas propuestas a menudo carecen de un fuerte enfoque en otros aspectos como el anonimato del usuario (ocultar la identidad de los participantes en las transacciones de energía) y la privacidad del usuario (proteger la información sensible como los patrones de consumo de energía). La falta de medidas de privacidad adecuadas puede llevar a vulnerabilidades de seguridad, ya que los datos sensibles de los usuarios podrían ser susceptibles de acceso no autorizado o perfilado, como se destaca en [13].

Las blockchains *permissioned*, como se implementan en [14], [15], ofrecen una solución parcial al requisito de privacidad al restringir la participación en la red a entidades autorizadas. Este enfoque puede mitigar el riesgo de que atacantes externos identifiquen a los usuarios a través del análisis de transacciones. Sin embargo, no aborda la preocupación de que los usuarios internos puedan deducir las identidades de los usuarios dentro de la red con permiso.

En respuesta a eso, han surgido recientemente otras propuestas como [16] y [17]. Las soluciones presentadas en estos trabajos tienen en cuenta el anonimato de los usuarios, pero no verifican si la producción o el consumo reclamado por los usuarios es realmente el especificado. Como resultado, un usuario deshonesto podría presentar un registro de producción de energía falso, lo que puede engañar al sistema y a otros usuarios, llevando a resultados indeseables.

Por otro lado, [18] utiliza un sistema de reputación para castigar a aquellos usuarios que se comportan de manera indebida. Sin embargo, en este esquema nadie posee la relación entre las cuentas de la red inteligente y la identidad real de los usuarios y, por lo tanto, no es capaz de aplicar medidas coercitivas de manera efectiva al usuario que se comporta mal.

El último problema también ocurre en trabajos como [19], [20], [21], donde los autores usan el anonimato para proteger las transacciones de microredes y las autoridades no pueden identificar a un usuario en caso de comportamiento indebido.

En trabajos como [22] y [23], se estudia la agregación de datos de consumo y producción de los *prosumers* utilizando técnicas de comunicación de datos mediante watermarking. Utilizando agregación de datos se evita el conocimiento del consumo y producción de un usuario concreto. De hecho, la agregación se ha utilizado directamente como método de protección de la privacidad en la publicación y uso de datos de *Smart Grid* [24], [25], [26].

En este trabajo presentamos una comparación de dos métodos de agregación para la publicación de datos con garantías de k-anonimato en un sistema para la gestión de redes de distribución de energía inteligentes basado en el uso de *Smart Contracts*, que extiende el trabajo de [27].

III. Descripción del sistema

La arquitectura propuesta se muestra en la Fig. 1. Consta de tres capas principales: *capa de Prosumers*, *capa de Smart Grid* y *capa de Main Grid*. Los siguientes actores/componentes están involucrados:

- *Smart Meters* (SM_i): dispositivos que registran el uso de energía de un *prosumer*.
- *Prosumers*: usuarios del sistema que potencialmente pueden producir y/o consumir energía. Atendiendo a su balance energético, el *prosumer* puede ser: *Consumidor*

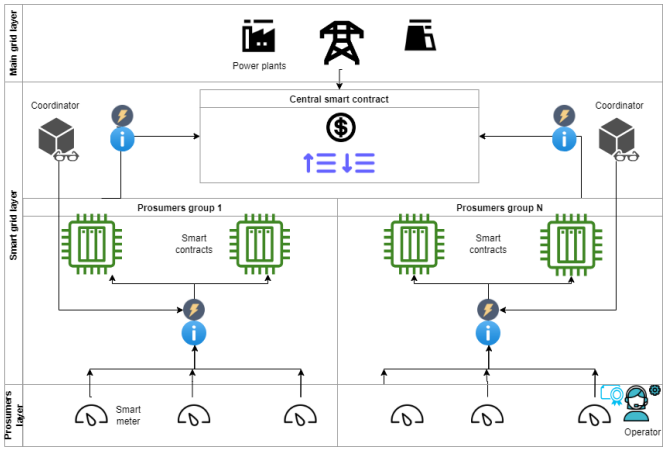


Figura 1. Esquema de la arquitectura

(C_i) si consume más energía de la que produce; o un *Productor* (P_i) si produce más energía de la que consume. Cada *prosumer* posee un *Smart Meter* e instalaciones de consumo y producción de energía en su propiedad.

- *Main Grid* (MG): conecta las principales fuentes de energía a la *Smart Grid* y se encarga de la distribución de electricidad. Es la responsable de la predicción del consumo de energía y de proporcionar la electricidad adicional necesaria.
- *Smart Grid*: gestiona las transacciones eléctricas y pagos entre *prosumers* y sus interacciones con la Main Grid.
- *Coordinadores* (Co_i): verifican las transacciones eléctricas de los usuarios. Son propietarios de los *Smart Meters* instalados en las propiedades de los *prosumers*, permitiéndoles verificar sus cantidades de consumo/producción eléctrico. El coordinador puede tomar las medidas en caso de impago, aunque queda fuera de las contribuciones de la propuesta.
- *Operadores* (O_i): encargados de registrar *prosumers* en la capa de *Smart Grid*, conectándolos y dándoles la autorización para enviar mensajes con la información comercial relevante a sus respectivos grupos.

La *capa de Prosumers* está compuesta por varios grupos de prosumers, geográficamente cercanos, que intercambian electricidad entre ellos para mejorar la eficiencia.

La *capa de Smart Grid* actúa como intermediaria entre la capa de Prosumers y la capa de Main Grid. Cada grupo de prosumers en esta capa está supervisado por un coordinador, quien es responsable de verificar las transacciones eléctricas dentro de su grupo. Esta capa también gestiona los datos sobre el uso de energía de cada grupo, lo que permite identificar déficit o excedentes eléctricos. En tales casos, la *capa de Smart Grid* se comunica con la capa de Main Grid para gestionar su compra o venta. Este proceso implica el registro meticuloso de todas las transacciones de energía entre los Prosumers de cada grupo.

Finalmente, la *capa de Main Grid* es el sistema tal como lo conocemos hoy, encargada de la distribución de energía y compuesta por las principales empresas eléctricas con sus generadores de electricidad a gran escala.

III-A. Visión general de la propuesta

Las cuatro fases principales del sistema propuesto son: *Inicialización*, *Cálculo de precios*, *Comercio de energía* y *Liquidación de deudas*.

En la fase de *Inicialización*, los Prosumers (es decir, consumidores y productores) deben registrarse con los operadores y deben estar autorizados para interactuar con la infraestructura de la *Smart Grid*.

El proceso de *Cálculo de precios* comienza el día anterior al comercio de energía, donde se realiza una predicción del consumo de energía esperado. La mayoría de los mercados energéticos emplean este sistema y su implementación queda fuera del ámbito de este trabajo. Durante esta fase, la Main Grid evalúa la demanda y establece comunicación con los principales productores de electricidad. Los productores se clasifican en función de sus precios, siendo el más caro el que determina el precio de negociación de la electricidad en cada franja horaria. Esto se hace de manera similar a como se realiza en la mayor parte de la UE [28].

La fase de *Comercio de energía* consiste en la comunicación entre los *Smart Meters* de los Prosumers con la capa de *Smart Grid*. Cada *Smart Meter*, situado en la propiedad del usuario, monitoriza el consumo y las transacciones de electricidad, almacenando periódicamente los datos de producción y consumo en la capa de *Smart Grid* a través de transacciones en el blockchain. Esto permite un seguimiento detallado del consumo eléctrico de cada usuario, facilitando así el cálculo de su deuda en función de la energía consumida o producida y el precio establecido por franja horaria. La infraestructura de la *Smart Grid* monitoriza las necesidades energéticas de cada grupo, gestionando la solicitud de electricidad adicional desde la Main Grid o la venta de excedentes. En esta propuesta, la Main Grid opera como un prosumer más, permitiendo una integración fluida en el mercado de energía. Los coordinadores, que son propietarios y disponen acceso a los *Smart Meters* de los Prosumers, verifican las transacciones y actúan como terceros de confianza (TTPs).

Finalmente, en la etapa de *Liquidación de deudas*, la *Smart Grid* recopila todas las transacciones de los usuarios y asigna una deuda correspondiente a cada una, dependiendo de si el usuario ha actuado como productor o consumidor. Esta deuda se notifica a los consumidores y, una vez saldada, la cantidad correspondiente se distribuye a los productores. De esta manera, no hay interacción directa entre los consumidores y los productores.

IV. El sistema propuesto en detalle

Esta sección explica primero los *Smart Contracts* basados en blockchain que son los componentes centrales de la solución propuesta. Después, detalla los cuatro pasos principales: *Inicialización*, *Cálculo de precios*, *Comercio de energía* y *Liquidación de deudas*.

IV-A. Smart Contract principal

El *Smart Contract* principal (SC_{MG}) actúa como intermediario entre los grupos de Prosumers (G_i) y la Main Grid. Su función principal es proporcionar un medio para que cada productor de la main grid (MG_k^P), registrado en el SC_{MG}, comunique su capacidad y precio de producción de energía. Los datos publicados por los MG_k^P permite al SC_{MG}

determinar los precios de la electricidad en cualquier momento del día y coordinar las necesidades de energía excedente o faltante entre los otros $SC_{i,j}$s de cada grupo de prosumers. Para ello, las $address$ de cada $SC_{i,j}$ (*smart contract* j del grupo G_i) y de cada MG_k^P deben estar registradas en SC_{MG}. El MG_k^P lleva un registro de todas las transacciones entre cada $SC_{i,j}$ y el MG. Cuando un grupo de prosumers necesita energía del MG, o desea vender un excedente, el SC_{MG} registra la transacción con la cantidad de energía y el precio. Este procedimiento es similar al seguido entre prosumers en cada $SC_{i,j}$.

IV-B. Smart Contracts del grupo de prosumers

Cada grupo de Prosumers (G_i) despliega varios $SC_{i,j}$s que son responsables de monitorizar el consumo y precio de la energía para cada usuario $U_{i,j}$, usuario j de G_i. El despliegue de $SC_{i,j}$s por grupo de prosumers busca priorizar el comercio local de energía. Para mejorar la privacidad, se implementan múltiples $SC_{i,j}$s por grupo, lo que permite a los Us fraccionar su consumo eléctrico en diferentes transacciones (Tx).

Con el fin de garantizar que solo se publiquen Tx autorizadas en el blockchain, en el $SC_{i,j}$ se mantiene una lista actualizada de los $U_{i,j}$s con acceso a sus funcionalidades. Además, cada $SC_{i,j}$ debe poseer la identidad del coordinador (Co_i) a cargo del grupo, siendo este la única autoridad que puede validar las Tx de cada U. Finalmente, las $address$ de los $SC_{i,j}$s deben estar registradas en el SC_{MG} para recibir actualizaciones del precio de venta de la electricidad durante cada franja horaria.

Una vez que los $SC_{i,j}$ han sido desplegados y autorizados, pueden comenzar a recopilar las Tx de los Us de su grupo. Los $SC_{i,j}$ pueden comunicarse con el SC_{MG}. Por ejemplo, si un grupo tiene un excedente de energía, pueden comunicarse con el SC_{MG} para contactar con otro grupo que necesite energía con el fin de vender su excedente.

IV-C. Inicialización

Durante esta fase, la Main Grid (MG), Operadores (O_i), Coordinadores (Co_i) y Usuarios ($U_{i,j}$) realizan sus procesos de inicialización:

La autoridad del MG despliega el SC_{MG}, y registra los MG_k^P con el método del SC_{MG} designado para ello.

El Co_i de cada grupo de prosumers despliega los $SC_{i,j}$s del grupo y registra sus $address$ en el SC_{MG} por medio de un método del SC_{MG}. Como *owner* de los $SC_{i,j}$s, Co_i también registra los O_is autorizados.

Los O_is instalan un *Smart Meter* sellado $SM_{i,j}$ en la propiedad de cada $U_{i,j}$ al que ofrezca servicio, conectando el $SM_{i,j}$ a la toma de la red eléctrica de $U_{i,j}$ para que el $SM_{i,j}$ obtenga acceso a los datos de consumo y generación eléctrica. Finalmente, conecta los SMs al Co_i de cada grupo para que este sea capaz de acceder y validar los datos de consumo.

Finalmente, durante el registro, cada U se registra primero recibiendo una *wallet* con una clave privada y utiliza una Función de Derivación de Claves para crear n pares de claves/direcciones. Las claves privadas se almacenan en un almacenamiento seguro al cual solo $U_{i,j}$ tiene acceso.

A continuación, $U_{i,j}$ comunica cada clave pública al O_i, así como su identificación a través de un sistema de comunicación seguro y privado, el cual registra a $U_{i,j}$ en cada $SC_{i,j}$ utilizando la función *newUser*() y comunica la información de $U_{i,j}$ al Co_i para que el Co_i pueda identificar a $U_{i,j}$. Finalmente, O_i envía a $U_{i,j}$ cada dirección del $SC_{i,j}$

IV-D. Cálculo de precios

Durante la parte inicial de esta fase, todos los Ps disponibles publican sus ofertas por medio de una función del SC_{MG}, la cual es bloqueada cuando el MG determina en el SC_{MG} el inicio del periodo de subasta. En ese momento, la lógica del SC_{MG} ordena las ofertas desde la más barata hasta la más cara y, para cada franja horaria, selecciona los n MG_k^P más baratos hasta que los bloques de energía que ofertan suplen la demanda esperada para cada franja horaria. El precio en cada franja horaria es el de la oferta del MG_k^P más caro de los n seleccionados. Este método es similar a prácticas observadas en diferentes mercados de energía en la Unión Europea [28].

IV-E. Comercio de energía

Esta fase da comienzo cuando el MG llama al método *beginTrading*() del SC_{MG} que inicia la fase de comercio de energía en todos los $SC_{i,j}$s desplegados, permitiendo que los $U_{i,j}$s/SMs puedan publicar su producción/consumo de energía con fines de compraventa.

Una vez autorizados a publicar, los SM, al menos una vez por franja horaria, verifican su saldo eléctrico (excedente o déficit) para publicarlo en el blockchain. Por motivos de privacidad, el SM divide su saldo eléctrico en transacciones eléctricas más pequeñas cuyo añadido equipare su saldo. Después, usa el método *sellEnergy()/buyEnergy()* del $SC_{i,j}$ para publicar cada una de estas pequeñas transacciones. Como cada grupo de prosumers tiene desplegados varios $SC_{i,j}$s, el SM distribuye su publicación aleatoriamente entre su lista de $SC_{i,j}$s conocidos. La lógica del método hace que cada $SC_{i,j}$ almacene las transacciones recibidas a su lista de *Transacciones*, junto con el precio actual de la electricidad y un flag que las marca como no verificadas.

Antes de finalizar la franja horaria, el Co_i a cargo de cada grupo de prosumers verifica el conjunto de transacciones que los SMs de los $U_{i,j}$s han publicado. Para ello, el Co_i, quien durante la franja horaria almacena información del consumo real de los $U_{i,j}$s, contrasta los datos de cada transacción con la información recopilada. Si los datos concuerdan, el Co_i cambia el estado de las transacciones en el blockchain a 'verificadas' llamando un método del $SC_{i,j}$ que actualiza dicho flag de estado.

Al final de la franja horaria, los Co_is y la MG cierran la franja horaria en los $SC_{i,j}$s y el SC_{MG}, respectivamente, llamando al método habilitado para ello. Una vez producido, el $SC_{i,j}$ calcula la diferencia entre la electricidad total producida y consumida por el grupo de prosumers G y publica una transacción en SC_{MG} indicando su superávit o déficit eléctrico, requiriendo la venta/compra de dicha cantidad de energía.

Una vez cerrado el cómputo de la franja horaria, se inicia la siguiente franja horaria, repitiendo el proceso descrito en esta fase. Al final del día, cuando se cierra la última franja horaria, la autoridad del MG cierra la fase de comercio, llamando al método *calculateDebt()* del SC_{MG}.

Una vez finalizadas todas las franjas horarias, los Co_is, que han registrado información del consumo real de los $U_{i,j}$s a lo largo del día, publican en el blockchain los datos de consumo y generación de energía de los grupos de prosumers bajo su cargo. Para preservar la privacidad de los patrones de generación y consumo de los $U_{i,j}$s, los datos subidos al *public ledger* se procesan mediante un proceso de agregación, descrito en la Sección V. La publicación de estos datos como open data proporciona una fuente de información adicional para el proceso de predicción de consumo de energía que se lleva a cabo durante la subasta eléctrica [28].

IV-F. Liquidación de deudas

La etapa comienza cuando la autoridad del MG llama al método *calculateDebt()* en el SC_{MG}, el cual llama recursivamente al mismo método de cada $SC_{i,j}$. Cada U que ha consumido más de lo que ha producido durante el día de negociación, consulta su deuda, los $SC_{i,j}$ de su G_i. Una vez que cada C tiene su deuda, debe pagarla a cada $SC_{i,j}$. El $SC_{i,j}$ paga a cada U que produjo más de lo que consumió y debe ser compensado. Cada $SC_{i,j}$ verifica si el G_i consumió más de lo que produjo en el SC_{MG}. Si el $SC_{i,j}$ debe fondos al SC_{MG}, debe pagar al MG por la electricidad adicional que necesitaba el G_i. Finalmente, el SC_{MG} paga a cada MG_k^P por la energía producida, terminando la tercera y última etapa.

V. Agregación de Datos y Resultados

Para poder publicar o distribuir los datos de consumo y producción de energía, optamos por agregar estos datos para preservar la privacidad de los patrones de consumo individuales. Esta es una práctica común en estos tipos de datos, ya que permite obtener estimaciones globales exactas (ver Sección II).

En esta sección llevamos a cabo un estudio de agregación de los datos utilizando datos reales de consumo y producción de electricidad de 50 hogares [29].

Consideramos que hay 5 coordinadores (Co_i) que agregan localmente los datos de 10 usuarios. Comparamos la agregación local con una agregación global que busca obtener el óptimo para diferentes valores de k-anonimidad y medimos la pérdida de información de ambos métodos de agregación.

La agregación local se obtiene promediando los valores de todos los usuarios que reportan su consumo y producción a cada coordinador local, que podemos ver como un punto de distribución o recolección de la *Smart Grid*.

La agregación global se obtiene aplicando microagregación. La microagregación [30], [31] es un método popular en privacidad de datos que se utiliza comúnmente para proporcionar k-anonimidad. Se crean pequeños grupos (microclusters) y luego se reemplaza cada uno de los registros o elementos del grupo por el centro del grupo. Dado que cada grupo tiene al menos k registros, cuando todos los registros son reemplazados por el mismo centro del grupo, se cumple la propiedad de k-anonimidad.

La microagregación, cuando se considera más de una variable, pasa a ser un problema NP-hard [32], por lo que se deben utilizar métodos heurísticos. MDAV [33] es uno de esos métodos y se ha utilizado ampliamente en la literatura. En este trabajo utilizamos MDAV para microagregación. Hemos utilizado valores de $k = 2, \ldots, 20$.

La Fig. 2 muestra la pérdida de información medida como el *Mean Square Error* (MSE) entre los datos originales y los datos protegidos. La línea horizontal verde muestra el MSE de la agregación local (que proporciona 10-anonimidad). La línea azul muestra los valores de MSE aplicando la agregación global para distintos valores del parámetro k. La línea roja muestra el valor en donde coinciden las garantías de privacidad de la agregación local y la global.

Para los datos de consumo podemos observar que la pérdida de información de la agregación global sigue siendo menor que la pérdida de información de la agregación local, incluso para valores de privacidad más altos (hasta $k = 20$). Por otro lado, para los datos de producción esto es cierto únicamente para valores de k hasta 12. Cuando $k > 12$, la agregación global pierde más información que la agregación local.

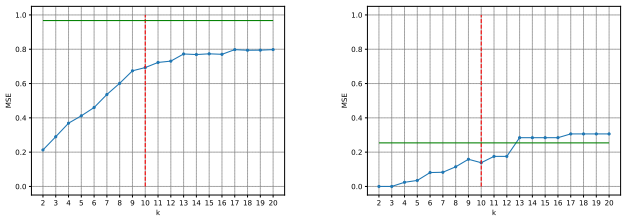


Figura 2. Comparativa de la pérdida de información (MSE) después de agregar los datos de consumo y producción de manera global y local.

Las Fig. 3 y 4 muestran los datos de consumo y agregación originales junto con los obtenidos después de agregarlos global y localmente. Podemos ver que los datos agregados globalmente tienen más variabilidad que los datos agregados localmente y representan más cercanamente los patrones de los datos originales. Este resultado es consistente con el hecho de que la pérdida de información sea menor para la agregación global que para la agregación local.

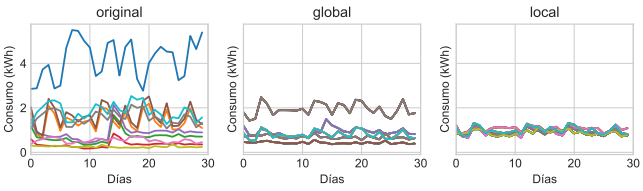


Figura 3. Datos de consumo originales y agregados de manera global (para $k = 10$) y local.

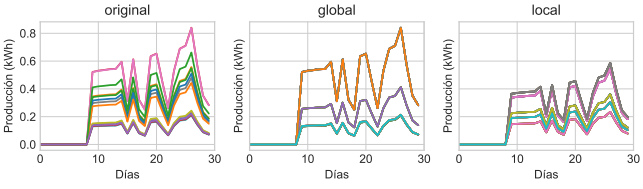


Figura 4. Datos de producción originales y agregados de manera global (para $k = 10$) y local.

VI. Conclusiones

En este artículo hemos presentado un sistema de gestión de *Smart Grids* que proporciona privacidad y seguridad a

los usuarios. Como se ha mostrado, el sistema permite el comercio de energía en un entorno seguro. Se promueve la participación de los usuarios sin riesgo a la privacidad y se pueden publicar datos de consumo y producción para el uso en estudios de predicción. Esta publicación permite preservar la privacidad de los usuarios a costa de perder un poco de información sobre patrones de consumo individuales, pero sin que las estimaciones globales se vean afectadas.

Como trabajo futuro, estamos considerando la implementación del sistema en dispositivos de bajo consumo y baja capacidad de cómputo. También consideramos interesante estudiar alternativas a la agregación de datos de consumo/producción para su publicación que puedan aportar alguna mejora respecto a la pérdida de información en agregaciones locales.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación mediante los proyectos PID2021-125962OB-C31 (SECURING/CYBER), PID2021-125962OB-C32 (SECURING/DATA), PID2021-125962OB-C33 (SECURING/NET). Por la Agencia de Gestión de Ayudas Universitarias y de Investigación (AGAUR) de Catalunya, mediante los proyectos SGR2021-00643, SGR2021-00115. Por el Plan de Recuperación, Transformación y Resiliencia financiado con fondos Next Generation EU mediante los proyectos DANGER INCIBE-C062/23, HERMES, y ARTEMISA: Cátedra internacional en ciberseguridad.

REFERENCIAS

[1] B. N. Stram, "Key challenges to expanding renewable energy," *Energy Policy*, vol. 96, pp. 728–734, 2016.

[2] M. K. Hoffacker and R. R. Hernandez, "Local energy: spatial proximity of energy providers to their power resources," *Frontiers in Sustainability*, vol. 1, pp. 585–110, 2020.

[3] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[4] U. Congress, "Energy independence and security act of 2007," *Public law*, vol. 2, pp. 110–140, 2007.

[5] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[6] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International Conference on the European Energy Market (EEM14)*, 2014, pp. 1–6.

[7] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[8] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, pp. 207–214, 2018.

[9] B.-B. M. E. Trading, "Deal: Differentially private auction for blockchain-based microgrids energy trading."

[10] A. de Vries, "Bitcoin's energy consumption is underestimated: A market dynamics approach," *Energy Research & Social Science*, vol. 70, p. 101721, 2020.

[11] J. Hou, H. Wang, and P. Liu, "Applying the blockchain technology to promote the development of distributed photovoltaic in china," *International Journal of Energy Research*, vol. 42, no. 6, pp. 2050–2069, 2018.

[12] O. Samuel and N. Javaid, "A secure blockchain-based demurrage mechanism for energy trading in smart communities," *International Journal of Energy Research*, vol. 45, no. 1, pp. 297–315, 2021.

[13] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 3–19, 2021.

[14] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE network*, vol. 32, no. 6, pp. 184–192, 2018.

[15] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[16] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A blockchain-based load balancing in decentralized hybrid p2p energy trading market in smart grid," *IEEE Access*, vol. 8, pp. 47 047–47 062, 2020.

[17] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "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, 2018.

[18] O. Samuel and N. Javaid, "Garlichain: A privacy preserving system for smart grid consumers using blockchain," *International Journal of Energy Research*, vol. 46, no. 15, pp. 21 643–21 659, 2022.

[19] S. Khan and R. Khan, "Multiple authorities attribute-based verification mechanism for blockchain mircogrid transactions," *Energies*, vol. 11, no. 5, p. 1154, 2018.

[20] X. Lu, L. Shi, Z. Chen, X. Fan, Z. Guan, X. Du, and M. Guizani, "Blockchain-based distributed energy trading in energy internet: An sdn approach," *IEEE access*, vol. 7, pp. 173 817–173 826, 2019.

[21] Y.-B. Son, J.-H. Im, H.-Y. Kwon, S.-Y. Jeon, and M.-K. Lee, "Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption," *Energies*, vol. 13, no. 6, p. 1321, 2020.

[22] F. Kabir, D. Megías, and T. K. Araghi, "Watercrypt: Joint watermarking and encryption scheme for secure privacy-preserving data aggregation in smart metering systems," in *Proceedings of International Conference on Information Technology and Applications: ICITA 2022*. Springer, 2023, pp. 547–556.

[23] F. Kabir, T. K. Araghi, and D. Megías, "Privacy-preserving protocol for high-frequency smart meters using reversible watermarking and paillier encryption," *Computers and Electrical Engineering*, vol. 119, no. 109497, 2024.

[24] K. S. Adewole and V. Torra, "Dftmicroagg: a dual-level anonymization algorithm for smart grid data," *International Journal of Information Security*, vol. 21, pp. 1299–1321, 2022.

[25] M. Alsaid, T. E. Slay, N. Bulusu, and R. B. Bass, "K-anonymity applied to the energy grid of things distributed energy resource management system," *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*, 2022.

[26] C. Gerlitz, A. Eriksson, and C. Hansson, "Anonymisation score for time series consumption data," *27th International Conference on Electricity Distribution (CIRED 2023)*, 2023.

[27] J. Ferré-Queralt, J. Castellà-Roca, and A. Viejo, "Smart contracts for a secure and privacy-preserving smart grid," in *International Conference on Risks and Security of Internet and Systems*. Springer, 2023, pp. 103–118.

[28] I. PETCU, "How are eu electricity prices formed and why have they soared?" ., 2022. [Online]. Available: https://www.eurelectric.org/in-detail/electricity_prices_explained/

[29] C. Goncalves, R. Barreto, P. Faria, L. Gomes, and Z. Vale, "Dataset of an energy community's generation and consumption with appliance allocation," *Data in Brief*, vol. 45, p. 108590, 2022.

[30] J. Domingo-Ferrer and V. Torra, "Ordinal, continuous and heterogeneous k-anonymity through microaggregation," *Data Min. Knowl. Discov.*, vol. 11, no. 2, pp. 195–212, 2005.

[31] M. Laszlo and S. Mukherjee, "Minimum spanning tree partitioning algorithm for microaggregation," *IEEE Trans. on Knowl. and Data Eng.*, vol. 17, no. 7, pp. 902–911, 2005.

[32] A. Oganian and J. Domingo-Ferrer, "On the complexity of optimal microaggregation for statistical disclosure control," *Statistical journal of the United Nations economic commission for Europe*, vol. 18, pp. 345–354, 2001.

[33] J. Domingo-Ferrer and J. M. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control," *IEEE Trans. on Knowl. and Data Eng.*, vol. 14, no. 1, pp. 189–201, 2002.