

# Infraestructuras electorales basadas en blockchain

Rafer Cooley

*Departamento de Ciencias de la Computación*  
*Universidad de Wyoming*  
 Laramie, Wyoming  
 rcooley2@uwyo.edu

Lobo Shaya

*Departamento de Ciencias de la Computación*  
*Universidad de Wyoming*  
 Laramie, Wyoming  
 swolf4@uwyo.edu

mike borowczak

*Departamento de Ciencias de la Computación*  
*Universidad de Wyoming*  
 Laramie, Wyoming  
 mike.borowczak@uwyo.edu

**Resumen**—Estudiantes de la Universidad de Wyoming diseñaron dos sistemas de votación basados en blockchain durante una clase ofrecida solo una vez en la Universidad. El primer sistema (reutilización) ramificó Ethereum para aprovechar sus beneficios de seguridad y privacidad. El segundo sistema (reinventar) creó un nuevo sistema de votación blockchain que usaba dos cadenas separadas, una para validar votantes y otra para asegurar votos. Esta investigación analizó los beneficios y las fallas de los sistemas electorales actuales, así como los beneficios y las fallas de la tecnología blockchain para mejorar la infraestructura electoral actual. Estos sistemas tienen como objetivo proporcionar integridad, privacidad y seguridad a sus usuarios. Además, se esfuerzan por ser tolerantes a las fallas. Finalmente, estos sistemas podrían extenderse a plataformas de votación móvil y contratos inteligentes. Sobre la base de los servicios descentralizados actuales, esta investigación demuestra una prueba de concepto de que las elecciones podrían beneficiarse de los sistemas basados en blockchain. Este tipo de sistemas serían ideales en ciudades inteligentes para garantizar la confiabilidad del procedimiento de votación.

## INTRODUCCIÓN

Las ciudades inteligentes empoderan a los ciudadanos al brindar capacidades informáticas distribuidas a varios servicios a través de dispositivos de Internet de las cosas (IoT). Las administraciones de las ciudades benefician a sus electores con servicios inteligentes a través de sistemas ciberfísicos que permiten ecosistemas más inteligentes, tiempos de respuesta de emergencia más rápidos y redes de sensores más confiables y completas. Para aprovechar estos avances, los sistemas ciberfísicos requieren poder computacional. Los investigadores avanzan en estos avances al mejorar la computación en la nube/perimetral para permitir una interacción más fluida entre dispositivos y servidores. Como resultado, los diseños e implementaciones de ciudades inteligentes pueden evolucionar para adaptarse a las necesidades emergentes [2]. Esto significa nuevos sistemas y mejoras que sirvan mejor a los ciudadanos de las ciudades inteligentes. Los sistemas y métodos de votación actuales contienen muchas vías para posibles mejoras.

Para mejorar los métodos y sistemas actuales, se diseñó una prueba de concepto para un sistema de votación blockchain. Las cadenas de bloques son libros de contabilidad distribuidos donde los participantes mantienen y acuerdan un historial de transacciones. Las criptomonedas aprovechan la tecnología blockchain para crear monedas seguras, tolerantes a fallas y transparentes. De la misma manera, la tecnología blockchain se puede aprovechar para crear sistemas de votación que garanticen la integridad, la seguridad y la privacidad de los votantes. Este trabajo adopta dos enfoques para crear un sistema de votación basado en blockchain. El primer enfoque utiliza (reutiliza) la tecnología existente para crear un sistema de votación derivado de Ethereum. Esto aprovecha la

los mismos beneficios de los modelos de cadena de bloques existentes y lleva esos beneficios a un sistema de votación sin problemas. En segundo lugar, se creó (reinventó) un sistema de votación blockchain desde cero. Al reinventar una nueva cadena de bloques, el sistema se adapta a las preferencias exactas. Finalmente, los funcionarios electorales locales aportaron información sobre lo que los sistemas de votación actuales brindan a sus electores y estos beneficios se mantuvieron en cada uno de los sistemas de votación.

## BLOCKCHAIN VOTAR SERVICIOS

En su forma más básica, votar permite a los civiles inducir cambios en su gobierno. Este elemento básico de la democracia permite que se proporcionen controles y equilibrios eficientes a los ciudadanos para mantener un gobierno para el pueblo. La votación se extiende más allá de la educación cívica y llega a salas de juntas corporativas y reuniones de inversionistas. Los futuros dispositivos inteligentes pueden incluso votar para decidir en dilemas éticos que involucren interacciones entre humanos y máquinas autónomas. En las ciudades inteligentes, este sistema debería ser lo más fluido y eficiente posible para eliminar las barreras que impiden que los ciudadanos voten. Muchas elecciones que se llevan a cabo en todo el mundo hoy en día tienen fallas sistemáticas, donde la población distribuida debe confiar en una sola autoridad central para recopilar, contar y validar los votos. En muchos casos, estas agencias centrales luchan por brindar la integridad y la seguridad necesarias para garantizar una infraestructura electoral confiable y sucumbir al fraude y los errores. Los sistemas de votación basados en blockchain permiten sistemas confiables que no requieren confianza entre ninguna de las partes. La distribución de un libro mayor compartido común, o registro de votos, entre cientos o miles de partidos permite que la gente esté realmente a cargo de sus elecciones. La integridad, seguridad y privacidad que ofrece una cadena de bloques crea muchas oportunidades para cambiar la forma en que pensamos sobre los estándares de votación [7]. Con estos objetivos en mente, se crearon dos mecanismos de votación que mejoran nuestro sistema de votación centralizado actual. Este trabajo se centra en dos métodos diferentes para desarrollar un sistema de votación,

## DECENTRALIZADO SERVICIOS

Actualmente, muchas ciudades utilizan sistemas de confianza ciega en los que los ciudadanos intercambian la responsabilidad de mantener y proteger sus datos por muy poca tranquilidad. En los servicios centralizados, una brecha de seguridad afecta a todos los que usan ese servicio. El almacenamiento de datos centralizado permite una más fácil y

vector de ataque más rentable en los datos del consumidor. Por el contrario, la descentralización de los datos dispersa el foco de los atacantes y hace que una filtración de datos exitosa sea menos lucrativa [3]. Tomemos, por ejemplo, una situación en la que Alice y Bob quieren intercambiar bienes, pero no confían el uno en el otro. Normalmente, este problema se resuelve introduciendo a un tercero en el que tanto Alice como Bob deben confiar. Sin embargo, la selección del tercero central no debe tomarse a la ligera. Este tercero ahora tiene acceso a los bienes que provienen de ambos lados y puede ganar el doble de lo que Alice o Bob pueden ganar. Del mismo modo, en cualquier sistema centralizado, la agencia central crea un centro que permite a las partes hacer negocios, pero también reúne todos los productos básicos en un lugar conveniente para los atacantes.

Asimismo, los sistemas de votación actuales dependen de agencias electorales centrales para facilitar el proceso de votación y contar los votos. Esto requiere mucha confianza por parte de los electores y las agencias centrales experimentan vulnerabilidades de seguridad. En nuestros sistemas de votación, mejoramos estos sistemas centralizados con un servicio descentralizado. Al descentralizar los servicios de votación, los votantes no están obligados a confiar en una agencia electoral central. Debido a que cada máquina de votación tiene una copia del registro de votación, y todos están de acuerdo con el contenido del registro, los votos no se ven influenciados por los intereses de terceros. Ethereum, una de las criptomonedas más grandes y exitosas, brinda los mismos beneficios a los participantes a través de un libro mayor distribuido. Al ramificar Ethereum, el mecanismo de votación de reutilización aprovecha los servicios descentralizados al mantener el mismo libro mayor distribuido. El mecanismo de votación reinventado refleja este tipo de servicio descentralizado, pero en su lugar implementa una solución personalizada para lograr este objetivo. Cada máquina de votación se configuró con acceso a la cadena y almacenó una copia del libro mayor. Cada máquina mantuvo el consenso entre sí misma y todas las demás máquinas de votación. Esto permitió que los votos se registraran y contaran al mismo tiempo que se garantizaba el acuerdo sobre el recuento. Cada uno de estos sistemas aprovecha los beneficios de los servicios descentralizados sin requerir la confianza de los votantes. Esto permitió que los votos se registraran y contaran al mismo tiempo que se garantizaba el acuerdo sobre el recuento. Cada uno de estos sistemas aprovecha los beneficios de los servicios descentralizados sin requerir la confianza de los votantes.

Las ciudades inteligentes habilitan a los ciudadanos con altos niveles de conectividad y se esfuerzan por encontrar formas inteligentes de hacer negocios. Idealmente, las elecciones en una ciudad inteligente se distribuirían, de modo que ninguna agencia individual pueda efectuar la votación. Al distribuir el voto, hay menos posibilidades de corrupción y los electores pueden tener más fe en un sistema confiable. Un beneficio adicional de los procedimientos de votación digital es la nueva capacidad para aumentar la cantidad de ciclos de votación, donde los códigos y políticas municipales se pueden votar a medida que surgen en lugar de agrupar los problemas en una o dos elecciones por año.

## YOINTEGRIDAD

Las infraestructuras electorales válidas requieren un sistema fiable y digno de confianza para proporcionar el nivel de confianza que exigen los votantes. Para implementar dicho sistema, es necesario tener un sistema con integridad donde solo se permitan acciones autorizadas. La tecnología Blockchain proporciona un sistema descentralizado basado en una autenticación creíble. Dado que todos en la cadena tienen una copia del libro mayor, todos pueden detectar una acción fraudulenta. Esto proporciona una base ideal para un

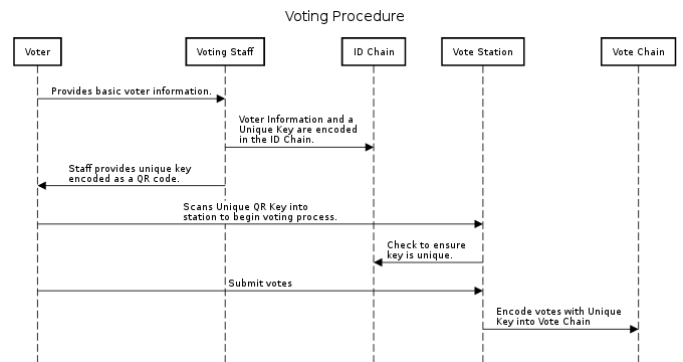


Figura 1. El procedimiento de votación seguido por el sistema Re-invent.

protocolo de elección segura [5]. Las elecciones requieren este nivel de integridad y las ciudades inteligentes pueden aprovechar la tecnología blockchain para brindar a sus ciudadanos un sistema de votación en el que puedan confiar. En nuestro sistema de reutilización, aseguramos el mismo nivel de integridad que Ethereum garantiza a sus usuarios. Mediante el uso de una cadena de bloques confiable y probada, el mecanismo de reutilización proporciona una gran integridad que garantiza una autenticación creíble a través de las mismas medidas modificadas de prueba de participación que usa Ethereum. Además, brinda un servicio confiable al garantizar que solo los votantes verificados puedan emitir un voto legítimo. Las llamadas API facilitan el paso de información del usuario a la cadena. La cadena requiere un número de identificación de votante para validar a un votante con una base de datos de votantes aprobada y solo proporciona a un votante legítimo su información de votación adecuada.

El sistema de reinversión utiliza dos cadenas de bloques separadas, una para la identificación de votantes y otra para almacenar los votos reales. Los votos se mantienen en una cadena separada de la información del votante para tratar la autenticación del voto por separado de la autenticación del votante y tomar las decisiones de diseño apropiadas para cada parte. Dado que los mecanismos de validación están separados, las cadenas de bloques se pueden adaptar para manejar las autorizaciones de manera adecuada en cada situación. Los votantes recibirían una identificación de un funcionario electoral en el momento de la votación. Luego, utilizando esta identificación, completan su boleta en una máquina de votación dedicada. Para validar que un votante es legítimo, debe usar su identificación de votante para acceder a la boleta y emitir su voto. Esto evita que se emitan votos que no estén asociados con un votante específico y evita que cualquier votante emita más de un voto. Además, se requieren votos para tener la identificación de votante asociada y para que el voto se valide y se agregue al libro mayor, esa identificación de votante no se puede asociar con ningún otro voto que ya esté en la cadena. El procedimiento de votación se puede ver en la Figura 1. Esto mantiene la integridad del sistema y mejora la confiabilidad del sistema actual.

Las ciudades inteligentes se benefician de estar en contacto con las nuevas tecnologías. La tecnología Blockchain ofrece a las ciudades inteligentes una forma de garantizar la integridad y confiabilidad en su infraestructura electoral. Es difícil confiar en una persona u organización, sin embargo, estos sistemas solo requieren confianza en las matemáticas y el código. Esto tampoco es un fideicomiso ciego. Con la tecnología blockchain, las ciudades inteligentes podrían implementar un sistema de votación de código abierto, en el que cualquiera podría buscar y ver cómo funcionan las matemáticas y el código. Por ser

transparente sobre cómo opera el procedimiento, y debido a que este procedimiento no requiere la confianza de un tercero, los civiles pueden confiar en el sistema de votación y estar seguros de la precisión del resultado.

#### SSEGURIDAD

Los sistemas de votación blockchain, cada vez más populares, garantizan una plataforma de votación electrónica segura que utiliza un libro mayor inmutable [4]. Al garantizar la privacidad y la protección contra el fraude electoral, la tecnología blockchain ofrece mucho para los sistemas de votación en línea que requieren transparencia. Además, las cadenas de bloques son difíciles de piratear y fáciles de auditar. Esto permite un sistema de votación más abierto que los civiles pueden usar con confianza. Más importante aún, los sistemas de votación blockchain superan a los sistemas de votación actuales que carecen de transparencia y seguridad. El sistema de votación de reutilización garantiza una plataforma segura al implementar protecciones contra el fraude electoral, como validar a los votantes y auditar la cadena de votación. Además, permite la transparencia a lo largo de la votación, lo que permite a los electores ver cómo se desarrolla una elección en tiempo real.

El sistema reinventado utiliza cadenas separadas para la identificación del votante y la información de la boleta para almacenar el voto de forma anónima y asegurar la identidad del votante. Además, ningún votante puede votar más de una vez ya que las identificaciones de los votantes también se mantienen en una cadena auditable. Se valida el DNI al igual que el voto. Este sistema utiliza firmas de anillo que permiten que los bloques sean firmados por un individuo en un grupo y que la identidad del firmante sea anónima, lo que agrega seguridad al sistema y al mismo tiempo proporciona un rastro de papel válido. Además, ambos sistemas son una mejora drástica con respecto a los sistemas de votación actuales que son probablemente pirateables y vulnerables al fraude electoral. Debido a que todos los colegios electorales tienen una copia del historial de votos, es difícil cuestionar los resultados de una elección. Un hacker no necesitaría piratear un sistema,

Las ciudades inteligentes ya manejan grandes preocupaciones de seguridad. Cuando todos están conectados, las vulnerabilidades se comparten fácilmente. Esto puede abarcar no solo a los usuarios, sino también a las plataformas. Estos problemas se abordan en estos sistemas de votación aprovechando los sistemas distribuidos y las implementaciones transparentes de blockchain. Actualmente falta seguridad electoral en los sistemas de votación que implementamos hoy, pero un sistema basado en blockchain aseguraría las identidades de los electores de las ciudades inteligentes, así como sus votos.

#### PAGSRIVACIDAD

La tecnología Blockchain prospera con la promesa de privacidad. Debido a su fortaleza contra los piratas informáticos, los sistemas de cadena de bloques garantizan la seguridad de los datos de los usuarios contra la manipulación. Además, las medidas de seguridad adicionales permiten que un sistema brinde privacidad y anonimato a un usuario [8]. Los sistemas de votación exigen un alto nivel de anonimato para evitar sobornos y extorsiones. La auditabilidad frecuentemente se compensa con el anonimato. ¿Cómo puede un sistema mantener a los usuarios anónimos mientras verifica el voto de cada persona? El sistema de votación perfecto le permite a un usuario ver por quién votó,

pero no les permite ver el voto de nadie más. La tecnología Blockchain proporciona ambos dentro de lo razonable. En el sistema de votación de reutilización, pudimos garantizar la privacidad mediante el uso de hashes de identificaciones de votantes para validar a un votante y asegurar su voto de forma anónima. Al hacer esto, validamos su voto y aseguramos su privacidad. Debido a que este sistema utiliza hashes de la identificación del votante, es fácil ver que una persona votó, pero no es tan trivial ver por quién votó. En cambio, el sistema muestra por quién votó cada hash.

En el mecanismo de reinversión, la privacidad no era tan sencilla ya que se compensa con la auditabilidad. Debido a que este sistema garantiza seguridad y confiabilidad, la oportunidad de mostrar un recibo del voto de una persona se vuelve factible. Después de votar, un elector podría ver por quién votó. Esto aumenta la confiabilidad y seguridad de la cadena ya que luego es auditable por cualquier votante. Sin embargo, mostrarle a un votante por quién votó después del hecho representa un riesgo para la privacidad y abre la puerta a sobornos y extorsión. Si alguien puede mirar hacia atrás en la cadena y ver por quién votó, la cadena se vuelve fácil de auditar pero también compromete la integridad del voto, ya que un votante podría probar que votó por una persona específica. Por lo tanto, el sistema de reinversión permite que un usuario vea que votó y que su bloque se agregó con éxito a la cadena, pero no permite que nadie vea el contenido de un voto. Hacemos esto encriptando el voto y codificando la identificación de votante de los usuarios. Esto prioriza la privacidad sobre la auditabilidad, pero mantiene la integridad del procedimiento electoral.

La privacidad no siempre se mantiene en muchas ciudades. Sin embargo, en las ciudades inteligentes, la privacidad se puede mantener durante una elección. Esto es vital para preservar los ideales democráticos de una votación y garantizar los medios por los cuales elegimos a los funcionarios. Al mantener la privacidad, las ciudades inteligentes permiten una gran conectividad sin temor a la agitación del adversario.

#### FAULTOTOLERANCIA

La tecnología Blockchain ofrece mecanismos de recuperación en caso de que haya problemas. Por esta razón, muchas aplicaciones de blockchain se están implementando en otros dominios, sobre todo en el campo de la medicina. Los sistemas utilizados en este campo deben poder llegar a un consenso. En otras palabras, todos deben estar de acuerdo en lo que es exacto. Al llegar a un consenso, todos los participantes entienden y están de acuerdo con los datos recopilados. La principal preocupación en muchos sistemas es la tolerancia a fallas bizantina. Una falla bizantina es una discrepancia en los datos que se presenta de manera diferente a diferentes usuarios. Las discrepancias que aparecen de manera diversa hacen que sea casi imposible llegar a un consenso. Por lo tanto, muchas aplicaciones de blockchain buscan evitar estas fallas. Blockchain se presta bastante bien a la tolerancia práctica a fallas y muchos sistemas en medicina han obtenido buenos resultados con aplicaciones de tolerancia a fallas [9]. En nuestros sistemas, nos esforzamos por la tolerancia a fallas. Esto brinda la oportunidad de corregir un voto incorrecto. Sin embargo, esto nos lleva de nuevo al equilibrio entre la auditabilidad y la privacidad.

Sería posible en cualquier mecanismo corregir un voto, sin embargo, hacerlo en cualquiera de los dos sistemas significa comprometer la identidad de un votante. Aunque no estamos mejorando en el

sistema actual de esta manera, estamos manteniendo la privacidad y la integridad. Además, ambos sistemas aún permiten un alto nivel de tolerancia a fallas. Si hay un problema con algunas de las máquinas de votación, el sistema continúa funcionando sin comprometer el proceso electoral. Esto permite que ocurran problemas técnicos y dificultades imprevistas sin dañar el procedimiento de votación y, por lo tanto, aumenta la integridad de la votación. Además, dado que todos los nodos tienen una copia del historial de votaciones, los votos no se pueden perder ni alterar. Debido a los niveles más altos de seguridad e integridad, la auditabilidad de la cadena se vuelve menos importante. Debido a la solidez del sistema, la posibilidad de que uno necesite auditar la cadena se reduce a ser muy escasa. Además, permitimos a los usuarios verificar dos y tres veces su voto antes de enviarlo a la cadena,

Dado que las ciudades inteligentes aprovechan muchos avances tecnológicos nuevos, es probable que haya problemas con la implementación de estos nuevos sistemas a medida que las personas comienzan a aprender nuevas formas de completar tareas. Sin embargo, gran parte de la nueva tecnología que se está implementando en las ciudades inteligentes tolera problemas. En un sistema de votación, esto significa que una elección no puede verse comprometida fácilmente y que los problemas que surjan durante la elección no afectarán el resultado.

#### METROOBILOVOTAR

Los avances tecnológicos nos permiten estar más conectados que nunca. En las ciudades inteligentes, las personas maximizan su tecnología. No solo nos esforzamos por conectarnos entre nosotros, sino que queremos conectividad entre nuestros dispositivos IoT. Esto crea sistemas ciberfísicos que nos conectan con el mundo. La tecnología Blockchain nos permite crear orden en los sistemas ciberfísicos. Basados en la tolerancia a fallas, el consenso y el intercambio de información, los registros distribuidos permiten a los usuarios conectar de manera confiable y transparente todos sus dispositivos [6]. Los sistemas ciberfísicos aumentan la funcionalidad de las ciudades inteligentes, lo que permite a los usuarios no solo conectar sus propios dispositivos, sino también conectarse con otras personas.

En un sistema de votación, esto plantea la cuestión del voto móvil. ¿Es factible pensar que alguien pueda votar de forma segura desde su teléfono? Descubrimos que podíamos muy factiblemente permitir esto. Usando nuestro sistema de reinversión, creamos múltiples interfaces que podrían servir como plataformas de votación. Esto permite flexibilidad en la forma en que los usuarios pueden emitir su voto e incluso permitiría que los superintendentes de tropas voten de forma anónima. Al permitir la votación móvil, se puede mejorar la participación de los votantes y aliviar los problemas comunes que tienen los electores al votar en filas tan largas y tener que ausentarse del trabajo. Sin embargo, la votación móvil tiene sus inconvenientes. El uso de máquinas de votación dedicadas y la limitación del personal de mantenimiento aprobado garantiza un mayor control sobre el sistema. Una aplicación de votación móvil requeriría un sistema para la descarga segura, así como una red segura. En el sistema de reinversión, la creación de redes se realizó a través del descubrimiento de pares. Esto podría extenderse a los dispositivos móviles, pero requeriría mayores niveles de seguridad.

#### SMERCADOCONTRATOS

Los sistemas implementados dan mucha confianza a las personas que instalan las cabinas de votación. La creación de nodos es

crucial para mantener un sistema viable. Esto reintroduce la confianza en el sistema que fue diseñado para no confiar. En futuras iteraciones de este trabajo, los contratos inteligentes pueden resolver este problema. Los contratos inteligentes son funciones autónomas que realizan transacciones en la cadena de bloques [1]. Una variación de estas funciones, un contrato inteligente que agregue un nuevo nodo con el permiso de la mayoría de la cadena, podría eliminar la amenaza de seguridad en los sistemas actuales. Esto podría permitir la votación móvil y garantizar que haya un control mínimo sobre la votación por parte de una agencia de votación central.

#### CONCLUSIÓN

Las ciudades inteligentes conectan a las personas aprovechando las capacidades informáticas en la nube/de borde en los dispositivos IoT para brindar servicios más inteligentes a sus civiles. A través de la investigación de los sistemas de votación actuales, encontramos que estos sistemas primitivos se pueden mejorar para encajar mejor en el esquema de la ciudad inteligente. Las infraestructuras electorales deben ser confiables, seguras, privadas y tolerantes a fallas. Sin estas piedras angulares, no podemos proporcionar la integridad del sistema que esperan los constituyentes. Sin embargo, con un sistema distribuido, podemos continuar aprovechando las tecnologías emergentes para mejorar los sistemas electorales antiguos. A través de los sistemas de votación basados en blockchain, podemos atender mejor a los votantes con elecciones más legítimas.

Creamos dos sistemas de votación diferentes. El primero ramificó Ethereum y aprovechó esa tecnología para crear un sistema electoral confiable. Este sistema brinda seguridad y privacidad y cumple con los mismos estándares de blockchain que actualmente están floreciendo en las criptomonedas. Nuestro segundo sistema fue construido desde cero. Este sistema se esfuerza por equilibrar la auditabilidad y la privacidad. Este sistema también abre la puerta a las plataformas de votación móvil impulsadas por contratos inteligentes. Con el objetivo principal de mejorar el sistema actual, pudimos investigar el sistema actual y crear nuevos sistemas descentralizados que son más seguros y brindan una infraestructura electoral más viable.

#### REFERENCIAS

- [1] K. Christidis y M. Devetsikiotis. Blockchains y contratos inteligentes para el internet de las cosas. *Acceso IEEE*, 4:2292–2303, 2016.
- [2] Franco Cicerelli, Antonio Guerrieri, Giandomenico Spezzano y Andrea Vinci. Una plataforma basada en el borde para aplicaciones dinámicas de ciudades inteligentes. *Sistemas informáticos de generación futura*, 76:106–118, 2017.
- [3] Jan Thomas Frec y Thomas Selzam. Ecosistema tokenizado de datos personales ejemplificado en el contexto de la ciudad inteligente. *JeDEM - eJournal of eDemocracy and Open Government*, 9(2):110–133, 2017.
- [4] Darin Stanchfield. La tecnología Blockchain puede hacer que los sistemas de votación sean más seguros, 7 de noviembre de 2016. Copyright - Copyright Network Media Group DBA Network Alliance, LLC 7 de noviembre de 2016; Última actualización: 2016-11-08.
- [5] Jianjun Sun, Jiaqi Yan y Kem ZK Zhang. Servicios compartidos basados en blockchain: lo que la tecnología blockchain puede contribuir a las ciudades inteligentes. *Innovación financiera*, 2(1):26, diciembre de 2016.
- [6] de Lier Ben. ¿Pueden los sistemas ciberfísicos colaborar de manera confiable dentro de una cadena de bloques? *Metafilosofía*, 48(5):698–711.
- [7] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang y Ningxiao Lu. Elección a gran escala basada en blockchain. *Procedia Informática*, 129:234–237, 2018. 2017 Conferencia Internacional sobre Identificación, Información y Conocimiento en el Internet de las Cosas.
- [8] J. Wang, M. Li, Y. He, H. Li, K. Xiao y C. Wang. Un mecanismo de incentivos para preservar la privacidad basado en blockchain en aplicaciones de detección de multitudes. *Acceso IEEE*, 6:17545–17556, 2018.
- [9] Lijing Zhou, Licheng Wang y Yiru Sun. Mistore: un sistema de almacenamiento de seguros médicos basado en blockchain. *Revista de sistemas médicos*, 42(8):149, julio de 2018.