IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Fecha de publicación xxxx 00, 0000, fecha de la versión actual xxxx 00, 0000.

Identificador de objeto digital 10.1109 / ACCESS.2020.DOI

Encuesta sobre contratos inteligentes basados en Blockchain: aspectos técnicos e investigación futura

Tharaka Mawanane Hewa [1], (Miembro estudiante, IEEE), Yining Hu [2], (Miembro estudiante, IEEE), Madhusanka Liyanage [3], (Miembro senior, IEEE), Salil Kanhare [4], (Miembro senior, IEEE) y Mika Ylianttila [5], (Miembro senior, IEEE)

[1,3,5] Centro de comunicación inalámbrica, Universidad de Oulu, Oulu, Finlandia, (correo electrónico: firstname.lastname@oulu. Fi)

[2] IBM Australia (correo electrónico: hulyric@gmail.com)

[3] Facultad de Ciencias de la Computación, University College Dublin, Irlanda, (correo electrónico: madhusanka@ucd.ie)

[4] Departamento de Ingeniería y Ciencias de la Computación, Universidad de Nueva Gales del Sur, Sydney, Australia, (correo electrónico: salil.kanhare@unsw.edu)

RESUMEN

El contexto de la investigación industrial e informática revolucionó en diversas direcciones durante las últimas décadas. El contrato inteligente basado en blockchain se adoptó como un interés de investigación significativo debido a sus características distintivas, como el almacenamiento descentralizado de transacciones, la ejecución autónoma de códigos de contrato y el establecimiento descentralizado del fideicomiso. Los contratos inteligentes basados en blockchain pueden transformar la arquitectura de trabajo de casi todas las industrias hacia estándares de servicio elevados. Los casos de uso de contratos inteligentes basados en blockchain van desde aplicaciones industriales como sistemas de criptomonedas hasta logística, agricultura, bienes raíces, comercio de energía, etc. El concepto de descentralización de blockchain es uno de los mayores avances en la investigación tecnológica desde que la informática del futuro obtuvo un gran impulso hacia el Internet de las cosas (IoT) y la informática de borde. Se está llevando a cabo una gran cantidad de investigaciones para investigar las oportunidades para la aplicabilidad de los contratos inteligentes y las tecnologías blockchain a diversas industrias. Es importante identificar los aspectos técnicos de los contratos inteligentes basados en blockchain para mejorar y agudizar aún más las capacidades que ya debían. Esta encuesta se realiza para identificar los aspectos técnicos significativos de los contratos inteligentes basados en blockchain con las futuras direcciones de investigación asociadas. Es importante identificar los aspectos técnicos de los contratos inteligentes basados en blockchain para mejorar y agudizar aún más las capacidades que ya debían. Esta encuesta se realiza para identificar los aspectos técnicos significativos de los contratos inteligentes basados en blockchain con las futuras direcciones de investigación asociadas. Es importante identificar los aspectos técnicos de los contratos inteligentes basados en blockchain para mejorar y agudizar aún más las capacidades que ya debían. Esta encuesta se realiza para identificar los

TÉRMINOS DEL ÍNDICE Blockchain, concurrencia, Ethereum, Hyperledger Fabric, IoT, contratos inteligentes, seguridad, escalabilidad

I. INTRODUCCIÓN

Los servicios de computación asociados que incluyen transacciones financieras, transmisión de video, correo electrónico y telecomunicaciones adoptaron en su mayoría una arquitectura centralizada [1] con la influencia de principios de diseño como la computación en nube. Los servidores de correo, los servidores de transmisión de vídeo y los sistemas de autorización de pago se han implementado en una infraestructura informática centralizada y los usuarios que consumen estos servicios adoptan la arquitectura cliente-servidor. Sin embargo, las futuras direcciones evolutivas de la investigación informática reflejan que el número de suscriptores de servicios informáticos se expande enormemente [2] - [4]. La revolución de la Industria 4.0 ha anticipado la contribución de la IoT industrial, la comunicación de máquina a máquina y la inteligencia artificial (IA). Los sistemas centralizados tienen limitaciones de escalabilidad con las futuras expansiones masivas de demanda de la informática.

La comunidad está muy motivada para investigar una estrategia arquitectónica novedosa para sostener la demanda computacional de la próxima generación [5]. Además, la privacidad, la disponibilidad, el control de acceso y la integridad de los datos son preocupaciones importantes en la investigación informática. Los contratos inteligentes basados en blockchain aumentan su empleabilidad como un avance tecnológico para la industria del futuro mediante la descentralización incorporada con integridad, ejecución autónoma y precisión [6].

La cadena de bloques es un libro mayor descentralizado e inmutable que se compone de una cadena de registros bloqueados enlazados criptográficamente. La colección de registros se denomina bloques y los registros generalmente se denominan transacciones o eventos. El libro mayor descentralizado se comparte entre todos los miembros contribuyentes en la red blockchain [7]. Las transacciones se agregan al libro mayor tras la verificación y el proceso de acuerdo entre las partes a bordo en la cadena de bloques. El enlace criptográfico es

la columna vertebral de blockchain. La asociación de palabras clave importantes con blockchain son los *descentralización, inmutabilidad* y *enlace criptográfico.*

Descentralización: La descentralización refleja la capacidad transaccional (almacenar y recuperar datos) de los contratos inteligentes basados en blockchain sin un solo punto de falla. El libro mayor está disponible en cada nodo y, a diferencia de los sistemas de gestión de bases de datos centralizados [8], el acceso a los datos no depende de un servicio centralizado.

Inmutabilidad: Los registros en el libro mayor son inmutables una vez registrados [9]. El intento de falsificar el registro del libro mayor en un bloque en particular lo descalificará y fallará la integridad de los datos de toda la cadena de bloques. La inmutabilidad del libro mayor garantizada mediante técnicas criptográficas como el hash y las firmas digitales que se explicarán en el papel. Las alteraciones del libro mayor es una tarea computacionalmente costosa.

Enlace criptográfico: El enlace criptográfico es la columna vertebral de la confianza de toda la cadena de bloques [10]. La inmutabilidad de blockchain se logra a través del enlace criptográfico establecido con hash y firmas digitales [11]. Ni la transacción ni el bloque se pueden alterar, ya que requiere alterar todos los bloques posteriores.

A. MOTIVACIÓN EN PAPEL

Los contratos inteligentes basados en blockchain tienen un contexto de aplicación inmenso, que va desde varias aplicaciones financieras [18] - [24], hasta aplicaciones de atención médica [25] - [32]. Sin embargo, se ha demostrado que programar correctamente los contratos inteligentes es un desafío. Por ejemplo, una pérdida financiera en la red Ethereum [33] fue causada por malas prácticas de programación.

Existen varias encuestas sobre contratos inteligentes basados en blockchain. Wright y col. [34] presentan los beneficios y desventajas de la tecnología descentralizada emergente y su requisito para la expansión de un nuevo subconjunto de la ley que se denominó Lex Cryptographia y destacó el requisito de la regulación de las organizaciones basadas en contratos inteligentes basados en blockchain. zations bajo la teoría jurídica. Wüst y col. [35] analizar críticamente la aplicabilidad de blockchain para un escenario de aplicación particular proponiendo una metodología estructurada para determinar las soluciones técnicas relevantes y evaluadas con algunas aplicaciones significativas del mundo real. Clack y col. [36] exploró el panorama del diseño de formatos potenciales para el almacenamiento y transmisión de acuerdos legales inteligentes en asociación con la tecnología blockchain específicamente para el contexto de servicios financieros. Wang y col. [37] también proporciona una descripción general completa de los contratos inteligentes impulsados por blockchain, destacando los desafíos distinguidos en los contratos inteligentes junto con las tendencias futuras. No obstante, los trabajos de investigación existentes no han estudiado a fondo los aspectos técnicos de los contratos inteligentes. Tampoco han explorado el potencial de integrar contratos inteligentes a otras tecnologías, como la inteligencia artificial y la teoría de juegos.

B. NUESTRA CONTRIBUCIÓN

En este documento, nuestro objetivo es realizar una encuesta exhaustiva que se centre en varios aspectos técnicos de los contratos inteligentes. Más específicamente, discutimos temas sobre la seguridad, la privacidad, el costo del gas, la concurrencia de los lenguajes de programación de contratos inteligentes existentes y hacemos las siguientes contribuciones:

- Primero discutimos los problemas existentes y las soluciones existentes sobre la seguridad, la privacidad, el costo del gas y la concurrencia de los contratos inteligentes.
- Luego, discutimos las lecciones aprendidas y las direcciones de investigación futuras para el desarrollo de contratos inteligentes para mejorar su seguridad, privacidad, costo del gas y
- simultaneidad. También discutimos temas de investigación futuros que involucran la integración de contratos inteligentes con otras tecnologías, incluida la inteligencia artificial y la teoría de juegos.

C. ESQUEMA DEL DOCUMENTO

El artículo consta de cinco secciones. La Sección I proporciona una breve introducción al artículo. La Tabla 1 consta de algunas encuestas importantes realizadas anteriormente en el contexto del contrato inteligente. La Sección II consta de importantes requisitos previos para comprender los contratos inteligentes. Se explican conceptos importantes de criptografía, incluido el hash y las firmas digitales. También se discuten los principios de blockchain y sus módulos centrales. Además, la evolución de blockchain hacia contratos inteligentes junto con importantes hitos históricos se examinan en el documento. La sección III contiene una parte significativa de la contribución principal de esta encuesta. La Tabla 2 contiene los componentes clave de algunas de las principales plataformas de contratos inteligentes del mercado. La Sección III incluye los aspectos técnicos significativos de los contratos inteligentes basados en blockchain. El contenido incluye los ataques de seguridad, las precauciones y las mejores prácticas para eliminar estos ataques, la optimización del rendimiento y las técnicas de mejora de la escalabilidad. Los conocimientos importantes de los aspectos técnicos del contrato inteligente basado en blockchain y las consideraciones importantes para dar forma a las direcciones de investigación futuras se desarrollaron en la Sección IV. Otras direcciones de investigación futura, como la combinación de contratos inteligentes con la teoría de juegos y la inteligencia artificial, se discuten más adelante en la Sección V. Finalmente, la Sección VI concluye la encuesta. Los conocimientos importantes de los aspectos técnicos del contrato inteligente basado en blockchain y las consideraciones importantes para dar forma a las direcciones de investigación futuras se desarrollaron en la Sección IV. Otras direcciones de investigación futura, como la combinación de contratos inteligentes con la teoría de juegos y la inteligencia artificial, se analizan más adelante en la Sección V. Finalmente, la Sección VI concluye la encuesta. Los conocimientos importantes de los aspectos té

II. ANTECEDENTES

El concepto de contratos inteligentes fue introducido por primera vez por Nick Szabo. Ethereum [20] es una de las plataformas de contratos inteligentes más destacadas con multitud de aplicaciones en diferentes contextos. Inicialmente, los contratos inteligentes estaban destinados únicamente a aplicaciones financieras como los tokens ERC20 [38]. Con el tiempo, la invención de plataformas de contratos inteligentes se diversificó debido a diversos requisitos industriales [39].

A. HISTORIA DE CONTRATOS INTELIGENTES

La Figura 1 ilustra los hitos importantes de la evolución histórica de los contratos inteligentes basados en blockchain. La introducción del concepto de contratos inteligentes fue realizada por Nick Szabo al mundo en 1994, es el nacimiento de los contratos inteligentes. La

TABLA 1. Encuestas anteriores sobre contratos inteligentes

Árbitro	Año	Descripción	Comparación con nuestra contribución
[12]	2019	Seguridad y privacidad en Blockchain: Una descripción general completa sobre la seguridad y la privacidad de blockchain, con técnicas para hacer cumplir la seguridad y la privacidad de los contactos inteligentes.	Ampliamos aún más la discusión sobre seguridad y privacidad y discutimos los aspectos técnicos adicionales como la optimización del rendimiento, la concurrencia, la escalabilidad y la verificación formal. Nuestro documento se
[13]	2019	Aplicaciones de las tecnologías de contabilidad distribuida a la Internet de las cosas: una encuesta: Proporciona un análisis de la cadena de bloques en la perspectiva de la aplicación.	ha centrado en los aspectos técnicos de la utilización de contratos inteligentes en diferentes aplicaciones, incluidas las IoT.
[14]	2019	Comunicación entre cadenas de bloques: una encuesta: Una discusión exhaustiva sobre las técnicas de comunicación entre cadenas de bloques.	Nuestro artículo analiza varios aspectos técnicos relevantes, sin limitarse a un tema específico.
[15]	2018	Una encuesta de aplicaciones de blockchain en diferentes dominios: Proporciona una descripción general de los contextos de aplicación de blockchain en dominios que incluyen moneda, atención médica, protección de derechos de autor y seguros.	Nuestro artículo se ha centrado principalmente en los aspectos técnicos de la utilización de contratos inteligentes en diferentes aplicaciones.
[dieciséis]	2018	Comprensión de las prácticas de desarrollo de software de los proyectos de blockchain: una encuesta: Incluye los resultados de una encuesta formal para identificar las prácticas de ingeniería de software, incluido el análisis de requisitos, la asignación de tareas, las pruebas y la verificación de proyectos de software blockchain.	Discutimos los aspectos técnicos en lugar de la perspectiva de la aplicación.
[17]	2018	Una encuesta sobre oportunidades y desafíos de la adopción de tecnología Blockchain para una innovación revolucionaria: Se analizó la adopción de blockchain en los sectores importantes de la Industria 4.0.	Discutimos los aspectos técnicos en general en lugar de centrarnos en aplicaciones individuales.

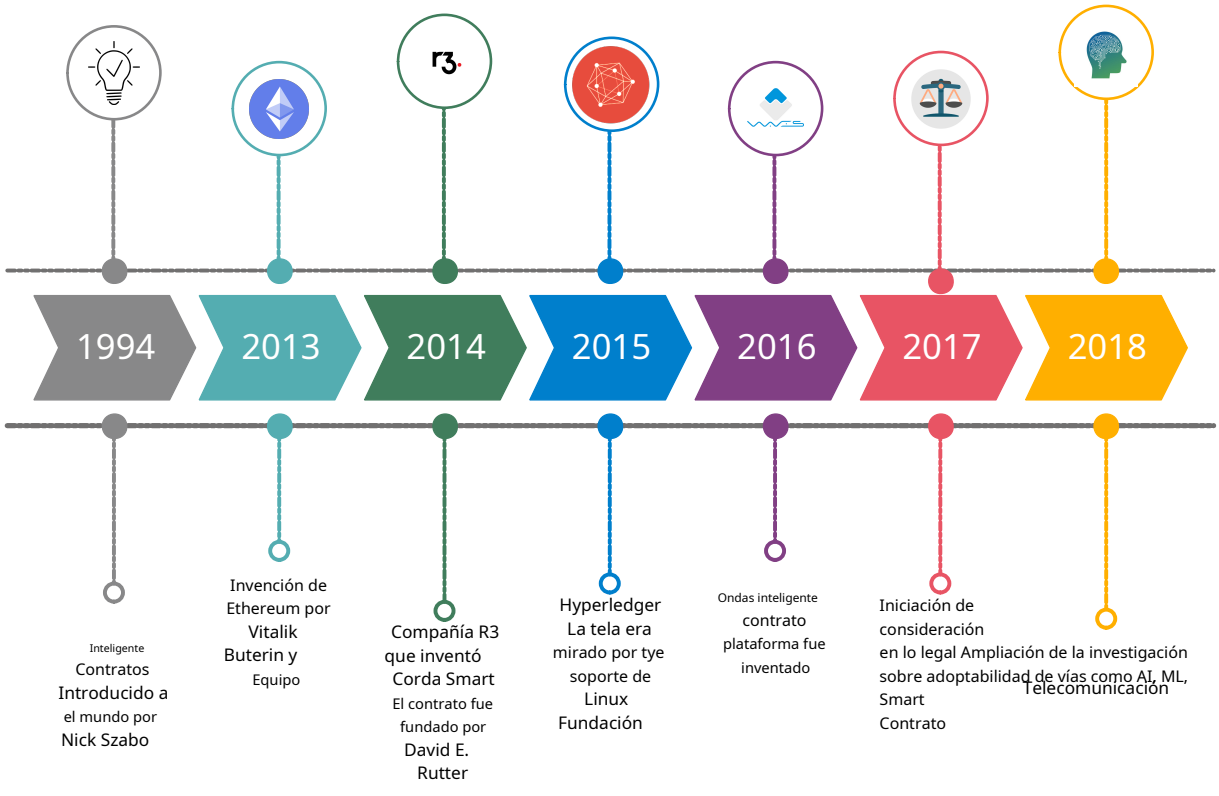


FIGURA 1. Cronología de la evolución de importantes plataformas blockchain [40] - [43].

La invención de Ethereum es uno de los saltos más importantes de la historia de los contratos inteligentes. La cadena de bloques pública de Ethereum permitió a los usuarios subirse a bordo e implementar aplicaciones de contratos inteligentes en las cadenas de bloques públicas. Ethereum fue el principal objetivo del cambio de divisas al principio. El proyecto Hyperledger Fabric se inició en colaboración con la Fundación Linux. La dirección de Hyperledger Fabric se ha desviado de la de Ethereum desde que Hyperledger fue concebida como una cadena de bloques empresarial. Muchas plataformas que se están desarrollando están dirigidas a los requisitos empresariales. La investigación se centró en la legalización de contratos inteligentes con la madurez del contexto de contratos inteligentes con múltiples plataformas y

diversos casos de uso. La próxima generación de investigación está muy centrada en la posición de los contratos inteligentes en los temas de investigación emergentes en informática.

B. CARACTERÍSTICAS DE LOS CONTRATOS INTELIGENTES BASADOS EN BLOCKCHAIN

Los contratos inteligentes son programas autoejecutables y autoejecutables que activan los términos y condiciones de un acuerdo particular utilizando códigos de software e infraestructura computacional. Los contratos inteligentes son programas descentralizados que amplían el uso de la red blockchain subyacente [44]. El programa es inmutable y se verifica criptográficamente para garantizar su confiabilidad.

Algunas características de los contratos inteligentes se heredan de la tecnología blockchain subyacente. Estas características permiten la empleabilidad de contratos inteligentes en diversos dominios [45]. En términos generales, los contratos inteligentes se ejecutan en modo peer to peer sin la intervención de un tercero centralizado. Proporcionan disponibilidad de servicio sin ninguna dependencia centralizada. Y permita la ejecución automatizada de transacciones cuando se alcancen las condiciones predefinidas [46]. A continuación, detallamos las características clave de los contratos inteligentes basados en blockchain.

1) Eliminación de terceros de confianza y ejecución autónoma

La ventaja más significativa de los contratos inteligentes basados en blockchain es la descentralización [47]. El requisito de intermediarios confiables, como corredores, agentes o proveedores de servicios, puede desalojarse cuando un sistema en particular se integra con contratos inteligentes basados en blockchain. La eliminación de un tercero de confianza reducirá los costos de transacción y la autoridad impuesta por las entidades centralizadas. Uno de los ejemplos más significativos es la criptomoneda, que adoptó contratos inteligentes para alterar el papel de terceros de confianza, como los bancos centrales [48]. Los terceros centralizados imponen altos costos de transacción y se comportan como los órganos de gobierno últimos. Los usuarios deben adherirse a las regulaciones impuestas por las autoridades centralizadas.

Por el contrario, los contratos inteligentes proporcionan el procedimiento de acuerdo que deben definir los propios participantes para maximizar la democracia [49]. Los participantes definen las reglas y regulaciones para el establecimiento de contratos inteligentes y se implementan de mutuo acuerdo. Se supone que la condición programada y el flujo de eventos se ejecutan una vez que la cadena de bloques alcanza un estado predefinido específico. El estado específico se definirá en el contrato inteligente con el acuerdo de todas las partes de la red blockchain. Este estado puede ser cualquier condición, como un saldo específico de fondos de la billetera, o un límite de tiempo específico, etc. La ejecución es entonces automática sin la intervención de un tercero centralizado. La disponibilidad del servicio está garantizada ya que la operación no depende de un tercero centralizado y ejecuta peer-to-peer. La ejecución autónoma según las condiciones asegura la precisión de la operación sin error humano o incluso sin acciones sesgadas. Por lo tanto, el contrato inteligente es una solución prometedora para la mayoría de las aplicaciones que requieren alternativas sin terceros confiables.

2) Resistencia e inmutabilidad de la forja

La integridad de los registros de transacciones en el libro mayor distribuido se verifica con firmas digitales [50]. Además, las transacciones individuales veri fi cadas y aprobadas antes de adjuntarlas al libro mayor. El libro mayor cada vez mayor consta de transacciones aprobadas que son inmutables. La alteración no puede ser cometida por un individuo. El código de contrato inteligente implementado en la cadena de bloques es inmutable. El código se puede implementar en cada nodo utilizando varias técnicas. Por ejemplo, como ejecutable incluido en el contenedor. El código de contrato inteligente es a prueba de manipulaciones y los contratos inteligentes manipulados no se pueden ejecutar. Sin embargo, los contratos inteligentes se pueden actualizar si es necesario mediante el acuerdo de los nodos en la red blockchain. Por lo tanto,

3) Transparencia

La transparencia [51] es una de las características distintivas significativas heredadas de los contratos inteligentes de blockchain [52]. La transparencia del contrato inteligente es doble. En primer lugar, el código definido en los contratos inteligentes es transparente tanto para las partes intervinientes como para el público. En segundo lugar, el conjunto de transacciones incluidas en los bloques también son transparentes para el público. Por lo tanto, las partes intervinientes de la red blockchain pueden confiar en la lógica y las transacciones en la red blockchain [53]. En un ejemplo más concreto, si la lógica del contrato inteligente de fi nida por una autoridad gobernante que es un participante de la red blockchain [54], la operación particular ejecutada sobre la lógica puede considerarse confiable e imparcial ya que el código es visible públicamente. Además, la transacción agregada al libro mayor también es visible públicamente para garantizar la confianza [55]. Por el contrario, la arquitectura de servicios centralizados no es transparente y es propensa a vulnerabilidades como los ataques man-in-the-middle. Las bases de datos centralizadas también son vulnerables e imposibles de rastrear si se produjo alguna modificación en los datos en reposo. La transparencia del código de contrato inteligente [56] garantiza que los miembros del ecosistema blockchain verifiquen públicamente la exactitud de su ejecución.

C. DESPLIEGUE Y EJECUCIÓN

La Figura 2 retrata hitos importantes de la inicialización y el procesamiento de transacciones de los contratos inteligentes basados en blockchain. El paso inicial (Paso 0) implica la inicialización de contratos inteligentes. Después de definir los términos y condiciones como un programa de software, el contrato inteligente debe instalarse en la red. El contrato inteligente implementado en cada nodo es idéntico en todos los aspectos para garantizar la equidad y cumplir con el requisito principal de los contratos inteligentes basados en blockchain. Existen muchas técnicas de interfaz en el mercado para cada red blockchain, cuando se requieren contratos inteligentes para conectarse con los sistemas comerciales externos. La API REST creada con aplicaciones basadas en Hyperledger Fabric SDK [57] o Ethereum SDK [58] son ejemplos significativos. La red blockchain recibe transacciones de la interfaz

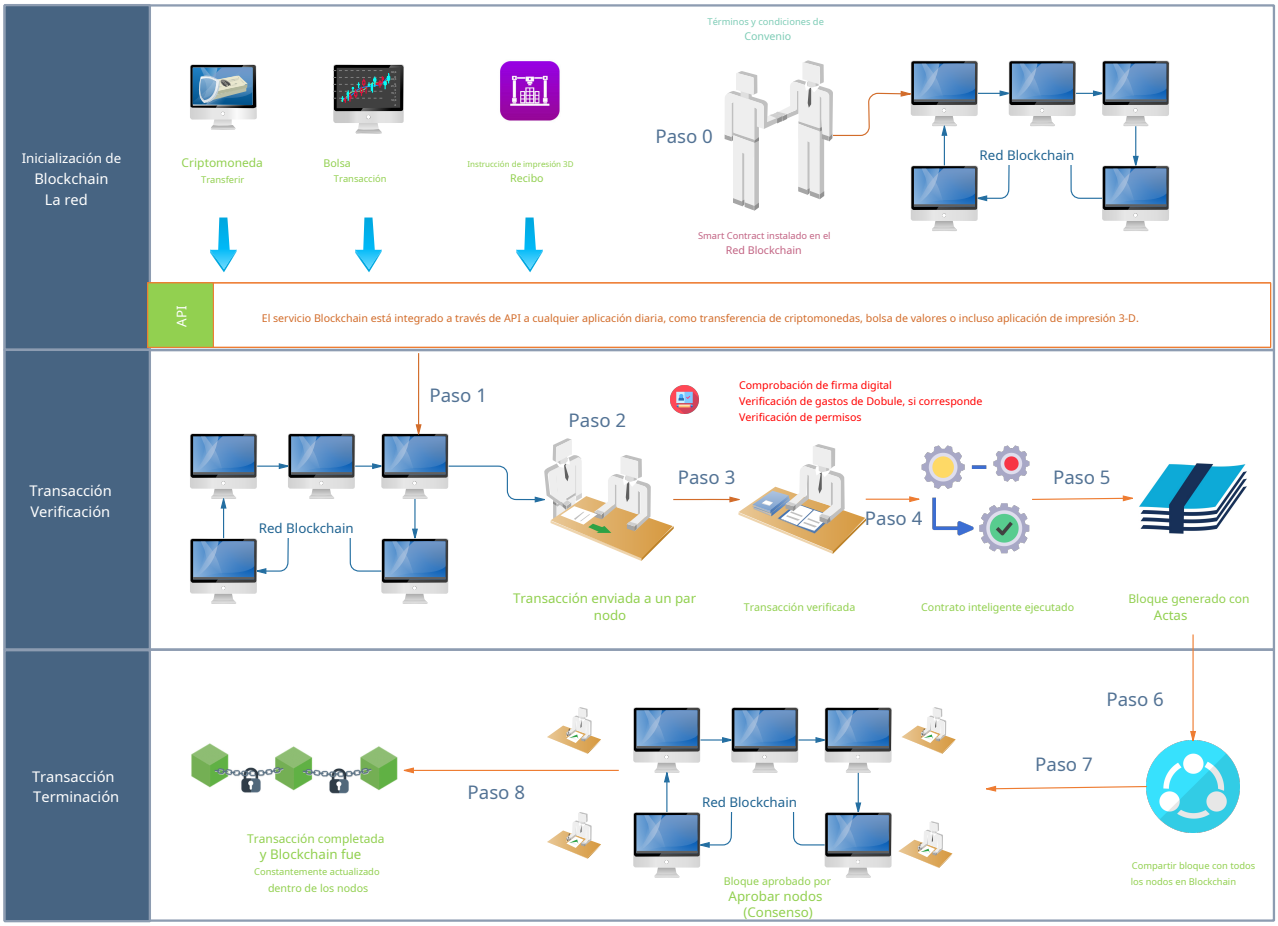


FIGURA 2. Flujo de transacciones de alto nivel de una integración típica de blockchain.

ing aplicaciones (Paso 1). Una vez que la red blockchain ha recibido la transacción, las transacciones se verifican para varias condiciones (Paso 2). La firma digital es esencial para autenticar que la transacción es legítima y es provocada por el miembro real de la red. Además, existen comprobaciones específicas de la plataforma en algunas redes blockchain. Por ejemplo, la plataforma Bitcoin comprueba el doble gasto en este paso [59]. Una vez que la transacción es legítima, la transacción se marca (Paso 3) como una transacción legítima y el contrato inteligente se ejecuta (Paso 4). La transacción se agrega al bloque y el bloque finalizado es generado por un nodo de minería (Paso 5). El bloque con fi rmado luego se disemina dentro de la red (Paso 6) y recibe las aprobaciones de cada nodo (Paso 7) según la regla de consenso predefinida.

III. ASPECTOS TÉCNICOS DE LOS CONTRATOS INTELIGENTES

La investigación científica sobre contratos inteligentes basados en blockchain hipnotizó las diferentes direcciones de la especialización técnica. Comenzó como un libro mayor inmutable descentralizado mínimo, la tecnología blockchain ha surgido con características vitales como seguridad mejorada, escalabilidad y funcionamiento óptimo gracias a la contribución de la investigación realizada a nivel mundial. Los aspectos técnicos significativos de los contratos inteligentes basados en blockchain se discuten en esta sección. La Figura 3 muestra una descripción general rápida de los aspectos técnicos de los contratos inteligentes.

A. ATAQUES DE SEGURIDAD, VULNERABILIDADES Y POSIBLES SOLUCIONES

Los contratos inteligentes están comenzando a ser ampliamente adoptados en muchos casos de uso de la industria. La seguridad es de vital importancia al considerar los contratos inteligentes, ya que afecta la funcionalidad de toda la cadena de bloques. Los diversos ataques a los contratos inteligentes, la investigación existente sobre estos ataques y las posibles soluciones se analizan en esta sección. Debido a la amplia adopción de los contratos inteligentes de Ethereum en casos de uso de la vida real y los ataques de seguridad ocurridos en los últimos años, en esta sección nos enfocamos solo en Ethereum para discutir los ataques y vulnerabilidades de los contratos inteligentes [72]. La Tabla 3 resume los ataques y las soluciones correspondientes.

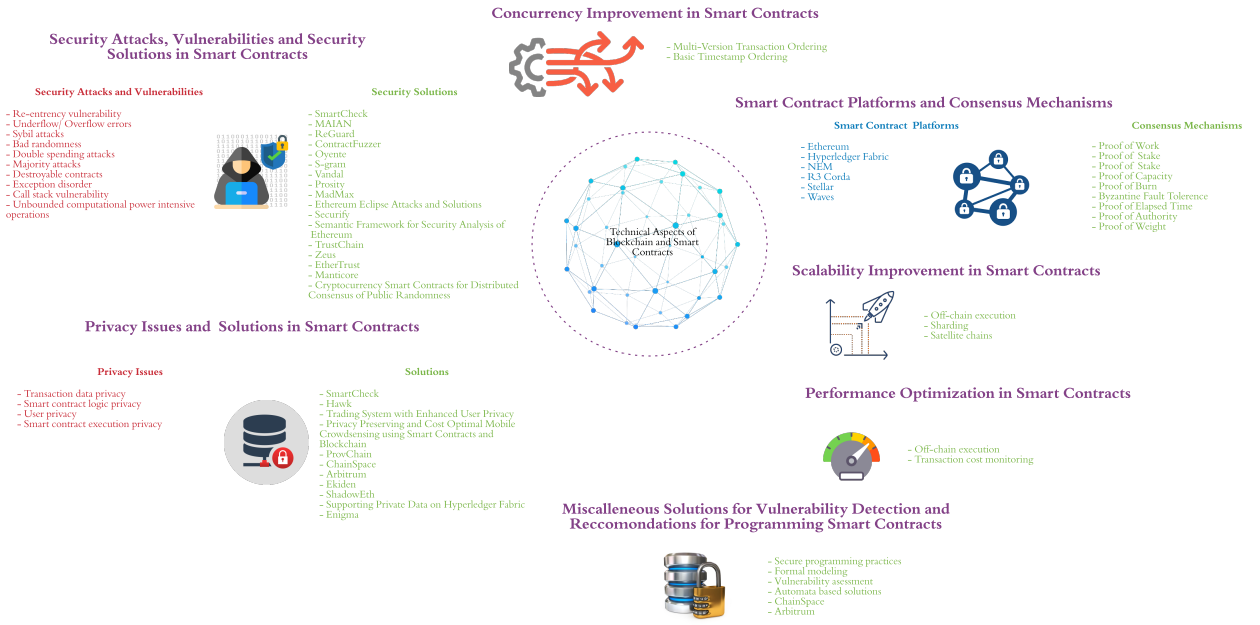


FIGURA 3. Descripción general de los aspectos técnicos de los contratos inteligentes

1) Diferentes ataques y vulnerabilidades

Existen multitud de ataques en el contexto de los contratos inteligentes [73]. Estos ataques se deben a numerosas razones, como errores de programación, restricciones en los lenguajes de programación y lagunas de seguridad. Los resultados de estos ataques consisten en muchas complicaciones para las redes blockchain y su precisión, pérdida de criptomoneda nativa y terminan la disponibilidad del sistema. Los ataques se pueden identificar en plataformas blockchain públicas y privadas. El papel de los contratos inteligentes y su precisión pueden ser más trascendentales en las cadenas de bloques públicas que en las cadenas de bloques privadas. La depuración o cualquier corrección es un proceso engorroso [74] ya que los contratos adoptan a todos los nodos de una red blockchain.

Vulnerabilidad de reentrada (A1): En términos generales, la La vulnerabilidad de reentrada se explota cuando un contrato inteligente invoca otro contrato inteligente de forma iterativa y el contrato inteligente que inicia la invocación es malicioso. Tales ataques fueron amplios en la plataforma Ethereum. Eventualmente, los Ethers del contrato inteligente que invoca se transfieren a la cuenta del contrato malicioso. Mehar y col. [33] describió el ataque DAO, un hacker anónimo robó 50MUSD de Ethers de los 168M invertidos a través de una recaudación de capital de riesgo virtual en 2016. Un codificador encontró una laguna, una vez que se invoca una función dividida, el código recupera Ether primero y actualiza el saldo más tarde y sin comprobar si se trata de una llamada recursiva. El atacante llama de forma recursiva a funciones divididas y recupera sus fondos antes de que el código verifique el saldo.

Errores de subflujo / desbordamiento (A2): Flujo insuficiente o desbordamiento Ocurrió cuando el resultado de una operación aritmética particular era menor o mayor que el tipo de datos numérico mínimo o máximo utilizado en la plataforma de contrato inteligente. La plataforma Ethereum utiliza uint256 [75]. Conceptualmente, el balance de Ether de 0 se puede transformar en el valor máximo de uint256 o el balance de Ether de valor máximo se puede transformar en 0. Sin embargo, los programadores deben considerar tales circunstancias al codificar el contrato [76]. Hay bibliotecas disponibles para eliminar los problemas conocidos, que se discutirán en las próximas secciones.

Ataques de Sybil (A3): El ataque Sybil [77] ocurre cuando un miembro intenta apoderarse de la red de pares al concebir identidades falsas explícitamente. Tales circunstancias [78] conducirán a un control desproporcionado de la red que puede conducir al secuestro del ecosistema de pares distribuido de blockchain. Por ejemplo, si el consenso se basa en la votación mayoritaria de una cadena de bloques en particular, los miembros creados explícitamente en el ataque pueden hacerse cargo del consenso de la red. El sistema es propenso a ese riesgo cuando el proceso de incorporación a la cadena de bloques es mínimo y está automatizado.

Mala aleatoriedad (A4): La aleatoriedad es necesaria en los contratos inteligentes, especialmente en el contexto de los juegos de azar y las apuestas. Además de eso, hay funciones de utilidad que requieren aleatoriedad [79]. Los enfoques para la generación de números aleatorios o pseudoaleatorios serán vulnerables en algunas circunstancias [80]. El uso de variables de bloque y hashes de bloque como fuentes de entropía puede ser vulnerable.

Ataques de doble gasto (A5): El gasto de los nativos token es común en casi todas las plataformas de contratos inteligentes [81]. En cada transacción, existe el riesgo de que el mismo usuario pueda gastar un token en particular dos o más veces [82]. Este tipo

TABLA 2. Algunas plataformas de contratos inteligentes líderes en el mercado

Plataforma	Árbitro	Descripción
Ethereum	[20]	Ethereum es una plataforma pública de blockchain que permite a los usuarios implementar contratos inteligentes públicamente. El consumo de recursos computacionales para la ejecución del contrato inteligente evaluado y la criptomoneda nativa es Ether.
Hyperledger	[42]	Hyperleder Fabric es una plataforma blockchain de código abierto inventada por la fundación Linux y algunas otras organizaciones. La plataforma se desarrolló como una plataforma de cadena de bloques empresarial y no hay una criptomoneda nativa adjunta a la plataforma Hyper-ledger.
NEM	[60]	NEM es una plataforma de cadena de bloques que se diseñó para la empresa y permite la de fi nición de activos que se pueden mapear como instrumentos industriales realistas, como artículos legales y documentos de envío.
R3 Corda	[41]	R3 Corda es una plataforma blockchain escalable que habilita funciones de privacidad y está diseñada para la integración industrial.
Estelar	[61]	Stellar es una plataforma de pago multidivisa basada en blockchain que es comparativamente eficiente en términos de consumo de recursos computacionales. La plataforma
Ondas	[43]	Waves es una plataforma de criptomonedas que también se integró con una pasarela de pago en dólares para que los usuarios de la billetera sean capaces de reabastecerse en dólares estadounidenses.
Ethereum Clásico	[62]	Ethereum Classic se formó mediante la bifurcación de Ethereum, que permite transacciones a un costo menor. Está evolucionando como una versión mejorada de Ethereum.
Tezos	[63]	Tezos se define como un libro mayor criptográfico auto-modificable, con criptomonedas nativas y dos tipos de cuentas como cuentas implícitas y cuentas originadas. Los contratos inteligentes se adjuntan a las cuentas originadas.
NEO	[64]	Neo se desarrolla con la intención de una economía inteligente. Neo se puede utilizar para digitalizar activos como certificados digitales.
Cardano	[sesenta y cinco]	La plataforma de contrato inteligente de Cardano es la primera plataforma respaldada por el estudio científico y de revisión por pares. Cardano ha introducido un nuevo lenguaje de programación llamado Plutus para desarrollar contratos inteligentes.
EOS	[66]	EOS se desarrolla principalmente con el objetivo de construir aplicaciones descentralizadas escalables horizontal y verticalmente. EOS ha abordado muchos aspectos, incluido el procesamiento paralelo, la gobernanza y la usabilidad mejorada.
Qtum	[67]	Qtum es una plataforma de contrato inteligente que se conoce como un híbrido de Bitcoin y Ethereum. Está adaptado al modelo UTXO de Bitcoin e incluye criptomoneda nativa.
Lisk	[68]	Lisk es una plataforma de contrato inteligente que habilita aplicaciones descentralizadas basadas en Javascript. Los autores han introducido el concepto de cadena lateral y SDK, que se pueden adjuntar a la cadena de bloques si es necesario.
ARCA	[69]	La plataforma ARK se desarrolló con un consenso y una escalabilidad mejorados. Los autores definieron la simplicidad mejorada que permite a un usuario implementar una nueva cadena de bloques y un token con solo presionar un botón.
RSK	[70]	RSK es una cadena de bloques escalable que permite pagos casi en tiempo real con la incorporación completa de contratos inteligentes de Turing a la cadena de bloques de
NXT	[71]	Bitcoin. NXT proporciona contratos inteligentes basados en plantillas que no están completos en Turing. Las plantillas de contratos inteligentes deben coincidir con el negocio.

de los ataques se conoce como ataques de doble gasto [83].

Ataques mayoritarios (A6): La mayoría de los ataques ocurren cuando algunos usuarios o grupos malintencionados toman el control para reescribir el historial de transacciones o evitar que se confirmen nuevas transacciones [84]. El ataque puede ocurrir cuando un consorcio de blockchain en particular lo adopta con el consenso de la mayoría de votos [85]. Dependiendo de los requisitos del usuario, a veces la verificación de transacciones y la minería de bloques se transfieren a algunos pares líderes dedicados de cada miembro del consorcio. Si la mayoría de los principales pares son secuestrados por el usuario malintencionado, ocurrió una circunstancia similar.

Contratos destruibles (A7): La vulnerabilidad de autodestrucción [86] elimina el contenido de un contrato inteligente al eliminar el código de bytes en las direcciones particulares. Además, envía todos los fondos del contrato a una dirección de destino específica, lo que hace que el contrato no sea funcional. Trastorno de excepción (A8):
El trastorno de excepciones se produce debido a que las excepciones conducen a una falla cuando no se manejaron adecuadamente [87]. El manejo de excepciones es una práctica importante en la programación, ya sea blockchain o en cualquier otro contexto. El manejo inadecuado de las excepciones, especialmente cuando un contrato invoca a otro, afecta la operatividad de toda la red [88]. Por lo tanto, el trastorno de excepción se destaca como una vulnerabilidad importante.

Vulnerabilidad de la pila de llamadas (A9): La profundidad de la pila de llamadas es limitado hasta un cierto valor en el entorno de ejecución del contrato inteligente. Por ejemplo, en Ethereum la profundidad de la pila de llamadas está limitada a 1024 fotogramas. La operación falla cuando la profundidad de la llamada alcanza el límite. Esto puede ocurrir debido a varias razones, como errores de programación [89].

Operaciones intensivas en energía computacional ilimitadas (A10): Cada operación de los contratos inteligentes requiere el consumo de potencia computacional [90]. Por ejemplo, el costo de la potencia computacional en Ethereum se llama Gas. El gas utilizado para evaluar el consumo de recursos computacionales de una operación particular en el contrato inteligente. Las operaciones intensivas en potencia computacional ilimitadas y no restringidas conducen a varios errores y eventualmente afectan al sistema [91].

2) Soluciones potenciales

Los problemas de seguridad causados por fallas semánticas pueden conducir a pérdidas financieras masivas. Destefanis y col. [109] presentó un estudio de caso sobre una biblioteca de contratos inteligentes denominada Parity. El problema se debió a prácticas de programación deficientes que causaron 500.000 Ethers para congelar en 2017. [1] Los autores analizaron la cronología de los eventos e identificaron que el problema ocurrió debido a prácticas de programación negligentes.

Dado que los programas de contratos inteligentes se implementan en cada nodo del sistema blockchain, el requisito de precisión del contrato inteligente es supremo. Se requiere que el contrato inteligente se agote por vulnerabilidades y errores de programación antes de ingresar a los miles de nodos de blockchain. Se han realizado varios trabajos de investigación para abordar varios ataques de seguridad sobre contratos inteligentes. Nosotros

[1] Equivale a 150M USD en el año 2017.

TABLA 3. Soluciones y ataques de seguridad

Árbitro	Descripción	Vulnerabilidad de reentrada (A1)	Errores de subflujo / desbordamiento (A2)	Ataques de Sybil (A3)	Mala aleatoriedad (A4)	Ataques de doble gasto (A5)	Ataques mayoritarios (A6)	Contratos destruibles (A7)	Trastorno de excepción (A8)	Vulnerabilidad de la pila de llamadas (A9)	Poder computacional ilimitado operaciones intensivas (A10)
[92]	SmartCheck: herramienta de análisis integral para detectar problemas de código en contratos inteligentes de Ethereum	X	X				X				
[93]	MAIAN: Análisis simbólico entre procedimientos y validación de Ethereu,		X		X						
[94]	ReGuard: analizador basado en Fuzzy para detectar vulnerabilidades de re-entrada en Ethereum	X									
[95]	ContractFuzzer: marco difuso para detectar vulnerabilidades en Ethereum	X		X						X	
[96]	Oyente: un marco para detectar errores en los contratos inteligentes	X			X					X	X
[97]	S-gram: herramienta de predicción de posibles vulnerabilidades mediante secuencias de tokens irregulares	X									
[98]	Vándalo: marco de análisis de seguridad para Ethereum con capacidad de conversión de código de bytes EVM en relaciones semáticas	X						X	X		
[99]	Prosity: Decompiler para Ethereum que genera sintaxis de solidez legibles a partir del código de bytes	X			X					X	
[100]	MadMax: técnica de análisis de programación estática para detectar gas vulnerabilidades enfocadas		X								X
[101]	Ataques y soluciones de Ethereum Eclipse: vulnerabilidades en consenso y sincronización de bloques y contramedidas					X					
[102]	Securify: analizador de seguridad escalable para Ethereum	X									
[103]	Marco de análisis semántico: análisis de seguridad semántica marco para Ethereum usando el lenguaje de programación F *	X							X		
[104]	TrustChain: estructura de datos a prueba de manipulaciones sin permisos con sybil resistencia			X		X					
[105]	Zeus: verificador de corrección y validador de equidad para contratos inteligentes	X									
[106]	EtherTrust: analizador estático automatizado para código de bytes EVM	X									
[107]	ManticCore: analizador binario para contratos inteligentes de Ethereum para detectar bombas lógicas	X									
[108]	Contratos inteligentes de criptomonedas para consenso distribuido de aleatoriedad pública: un generador de números aleatorios seguro				X						

discutir estos trabajos de investigación de las tres categorías principales debajo: *identificación de fallas semánticas, herramientas de control de seguridad* y *verificación formal.*

a: Identificación de fallas semánticas

Varios estudios de investigación han analizado estas fallas semánticas e identificado prácticas de programación para mitigarlas.

Por ejemplo, Atzei et al. [110] analizó las vulnerabilidades de Ethereum, que es popular en la industria. Las vulnerabilidades se agruparon en tres clases según el nivel en que se introduzcan, como Solidity, EVM bytecode o blockchain. Los autores destacaron que esperan que los lenguajes legibles por humanos completos que no son de Turing resuelvan algunos de los problemas identificados.

Delmolino y col. [111] documentó algunos conocimientos importantes sobre la enseñanza de la programación de contratos inteligentes a estudiantes de pregrado en la Universidad de Maryland. Los autores expusieron errores comunes en el diseño de contratos inteligentes seguros y protegidos, y destacaron la importancia de corregir estos errores en la programación.

Del mismo modo, Wöhrer et al. [112] presentó varios patrones de seguridad que son aplicables a los desarrolladores de Solidity para mitigar escenarios de ataque típicos en la plataforma Ethereum. Los patrones declarados incluían protección de ataques de reentrada, habilitación de mutex, etc. Los autores planearon crear un lenguaje de patrones de diseño estructurado e informativo para Solidity.

b: herramientas de control de seguridad

Además, también se han propuesto múltiples herramientas de control de seguridad para prevenir fallas semánticas de los contratos inteligentes.

Varios estudios han abordado la *Ataque de reentrada.* Liu y col. [94] presentó la herramienta ReGuard, que se puede utilizar para identificar errores de re-entrada en contratos inteligentes. Es un analizador de base difusa que detecta automáticamente los errores de re-entrada en los contratos inteligentes de Ethereum. ReGuard genera de forma iterativa diversas transacciones al azar para probar la vulnerabilidad. Del mismo modo, Jiang et al. [95] presentó ContractFuzzer, un marco de fuzzing integral para detectar siete tipos de vulnerabilidades en los contratos inteligentes de Ethereum. Los autores identificaron pocos tipos de ataques significativos, como el envío sin gas y la vulnerabilidad de reentrada. Los autores identificaron la tasa de falsos negativos optimizada al comparar con otras plataformas.

Otros trabajos de investigación investigados *Código de bytes de Ethereum.* Por ejemplo, Brent et al. [98] proporcionó un marco de análisis de seguridad para los contratos inteligentes de Ethereum. Proporciona una canalización de análisis para la conversión del código de bytes EVM de bajo nivel en relaciones lógicas semánticas. La evaluación transmitió que Vandal es rápido y robusto, además de superar a las herramientas líderes de última generación con un análisis exitoso de 95 de los 141,000 contratos únicos con un tiempo de ejecución promedio de 4.15 segundos. Suiche y col. [99] presentó Prosity, un descompilador que genera sintaxis de Solidity legibles a partir del código de bytes EVM. Los contratos descompilados pueden realizarse con análisis estático y dinámico según sea necesario. Grishchenko y col. [103] más tarde presentó una semántica completa de pequeños pasos del código de bytes EVM y formalizó un fragmento signi fi cativamente grande de EVM usando F *, que es un lenguaje de programación popular usado para un asistente de prueba programado de verificación similar. Los autores también lo validaron con éxito frente al conjunto de pruebas oficial de Ethereum. Los autores definieron además una serie de propiedades de seguridad destacadas para los contratos inteligentes. Más recientemente, Mossberg et al. [107] introdujo un marco de ejecución dinámica de código abierto llamado Manticore para analizar los binarios de los contratos inteligentes de Ethereum. El marco proporciona análisis para encontrar problemas que incluyen bombas lógicas. La API proporciona flexibilidad para personalizar la utilización del marco. Esto respalda la escalabilidad hasta contratos más grandes. Los autores probaron la herramienta con Oyente y observaron resultados superiores y EtherTrust mostró una mejor precisión en un punto de referencia en lugar de soluciones de vanguardia.

A medida que los contratos de Ethereum consumen *gas,* el costo del gas en la ejecución del contrato inteligente también se ha convertido en una preocupación vital. GRECH y col. [100] clasificó e identificó el gas enfocado en las vulnerabilidades encontradas en los contratos inteligentes de Ethereum. El gas es el costo de la ejecución de un contrato inteligente particular en la red pública de Ethereum y las vulnerabilidades centradas en el gas se refieren principalmente a los códigos con ejecución exhaustiva para consumir el gas asignado para el contrato inteligente. Además de eso, los autores presentaron MadMax, que son algunas técnicas de análisis de programación estática que se pueden utilizar para detectar vulnerabilidades relacionadas con el gas con una confianza significativamente alta. El enfoque incluyó análisis de bajo nivel para descompilación en técnicas de análisis de programa declerativo para análisis de nivel superior que se validó con 6,6 millones de contratos.

Nikolic 'y col. [93] implementó MAIAN, que emplea un análisis simbólico entre procedimientos y un validador concreto para identificar exploits reales. La herramienta identifica tres tipos principales de errores, incluidos *suicida* contratos que pueden matar a cualquiera, *pródigo* contratos que pueden enviar Ethers a cualquiera y contratos codiciosos que no permiten llevar Ether a nadie. La herramienta evaluó con análisis de un millón de contratos y marca 34.200 contratos vulnerables gastando 10 segundos por contrato.

Más *propósitos generales* También se propusieron herramientas de control de seguridad. Por ejemplo, Tikhomirov et al. [92] propuso SmartCheck, una herramienta de análisis integral que detecta problemas de seguridad de los contratos inteligentes de Ethereum. Los autores evaluaron la herramienta en un conjunto de datos masivo de contratos de la vida real y obtuvieron resultados exitosos. También declararon la capacidad de desarrollo de la herramienta en direcciones futuras, incluida la mejora de la gramática. También se ha demostrado que Smartcheck es más eficaz en las pruebas de seguridad automatizadas que otras herramientas [113]. Otro ejemplo, Tsankov et al. [102] presentó Securify, un analizador de seguridad para contratos inteligentes Ethereum. Es escalable, totalmente automatizado y capaz de demostrar que los comportamientos del contrato son seguros o inseguros correspondientes a una propiedad determinada y se han probado con más de 18k contratos. El análisis es un proceso de dos pasos que incluye un análisis simbólico del gráfico de dependencia del contrato para extraer información semántica precisa y verificar los patrones de infracción de cumplimiento. Luu y col. [96] propuso una ejecución simbólica

herramienta denominada Oyente para encontrar posibles errores de seguridad. La herramienta marcó 8.833 contratos como vulnerables de los 19.366, incluido el error DAO que provocó una pérdida de 60 millones de dólares. Posteriormente, Kalra et al. [105] también presentó el marco Zeus, que se puede utilizar para verificar la exactitud y validar la equidad de los contratos inteligentes. También definieron la corrección como el cumplimiento de prácticas de programación seguras y la imparcialidad como el cumplimiento de la lógica empresarial acordada de nivel superior. El marco supera significativamente a Oyente con cero falsos negativos en su conjunto de datos. Mavridou y col. [114] introdujo FSolidM, que incluía una semántica meticulosa para diseñar contratos como máquinas de estado finito. Los autores presentaron una herramienta para crear Finite State Machine (FSM) en una interfaz gráfica fácil de usar que genera automáticamente contratos inteligentes Ethereum. Los autores también introdujeron un conjunto de patrones de diseño que se pueden implementar como complementos y se pueden integrar fácilmente para mejorar la seguridad y la funcionalidad. Liu y col. [97] propuso una técnica de auditoría de seguridad con conciencia semántica llamada S-gram para Ethereum. Los autores combinaron el modelado del lenguaje N-gram así como el etiquetado semántico estático ligero y para aprender los reguladores estadísticos de los tokens de contrato y para capturar la semántica de alto nivel, como la sensibilidad de flujo de una transacción. Los autores demostraron que S-gram se puede utilizar para predecir vulnerabilidades potenciales en la identificación de secuencias de tokens irregulares y es posible optimizar los analizadores en profundidad existentes. Los autores también introdujeron un conjunto de patrones de diseño que se pueden implementar como complementos y se pueden integrar fácilmente para mejorar la seguridad y la funcionalidad. Liu y col. [97] propuso una técnica de auditoría de seguridad con conciencia semántica llamada S-gram para Ethereum. Los autores combinaron el modelado del lenguaje N-gram así como el etiquetado semántico estático ligero y para aprender los reguladores estadísticos de los tokens de contrato y para capturar la semántica de alto nivel, como la sensibilidad de flujo de una transacción. Los autores demostraron que S-gram se puede utilizar para predecir vulnerabilidades potencia

c: Verificación formal

La verificación formal en general se refiere a la verificación formal de la corrección de un programa de computadora. La verificación formal es importante en el contexto de los contratos inteligentes, ya que los contratos inteligentes pueden tener valores financieros y, a menudo, se ponen a disposición de todos en una cadena de bloques. Varios estudios de investigación han investigado la verificación formal de contratos inteligentes y han aplicado la verificación formal en diferentes etapas durante el despliegue de contratos inteligentes. Por ejemplo, Bhagavan et al. [115] describió un marco para analizar y verificar la seguridad del tiempo de ejecución. Mientras que Abdellatif et al. [116] y Nehai et al. [117] propuso verificar los contratos inteligentes en su entorno de ejecución. Albert y col. [118] por otro lado propuso el marco EthIR para analizar el código de bytes Ethereum.

B. PROBLEMAS DE PRIVACIDAD Y SOLUCIONES

La descentralización es un principio fundamental de los contratos inteligentes basados en blockchain. La descentralización en blockchain hace que el libro mayor de transacciones y los contratos inteligentes sean transparentes para todos los pares en la red como una característica de seguridad. No se recomienda la transparencia en determinadas circunstancias. La transparencia incorporada es una preocupación de privacidad significativa en los contratos inteligentes basados en blockchain. La Tabla 4 refleja los trabajos relacionados y las correspondientes soluciones de privacidad.

TABLA 4. Problemas y soluciones de privacidad

Árbitro	Descripción	Privacidad de datos de transacciones (I1)	Privacidad de lógica de contrato inteligente (I2)	Privacidad del usuario (I3)	Privacidad en la ejecución de contratos inteligentes (I4)
[119]	Halcón	X		X	
[120]	Sistema de comercio con mayor privacidad del usuario			X	
[121]	Preservación de la privacidad y optimización del coste de la detección de masas móvil mediante contratos inteligentes y blockchain			X	
[122]	ProvChain			X	
[123]	ChainSpace	X			
[124]	Arbitrum			X	
[125]	Ekiden				X
[126]	TownCrier				X
[127]	ShadowEth				X
[128]	Soporte de datos privados en Hyper-ledger Fabric con computación segura de múltiples partes	X			
[129]	Enigma			X	
[130]	Zether		X		

1) Diferentes preocupaciones sobre la privacidad

La privacidad es un dominio más amplio en términos del contrato inteligente [131]. Debido a la naturaleza distribuida de los contratos inteligentes, existen pocas preocupaciones importantes sobre la privacidad [132]. Estas condiciones de privacidad cerns [133] deben abordarse con el fin de aumentar la empleabilidad de los contratos inteligentes en la industria [134].

Privacidad de los datos de la transacción (I1): En ciertas circunstancias [135], los miembros de la red no preferirán la transparencia, ya que revelará información sensible, como secretos comerciales, información sobre precios. A pesar de que el sistema está asociado con blockchain, las medidas necesarias para la preservación de la privacidad deben integrarse [136], [137].

Privacidad de la lógica del contrato inteligente (I2): El contrato inteligente desplegado públicamente en todos los nodos de la cadena de bloques [130]. Debido a algunos requisitos, la lógica empresarial de la organización requería incorporarse en la cadena de bloques. Las lógicas de negocio pueden incluir información sensible como comisiones, bonificaciones. La revelación de dicha información sensible a través del contrato inteligente será una preocupación de privacidad del

Organizaciones.

Privacidad del usuario (I3): La privacidad del usuario está muy preocupada en algunas aplicaciones importantes de contratos inteligentes basados en blockchain. Los usuarios que incorporan los contratos inteligentes deben ser privados en determinadas circunstancias. Por ejemplo, las soluciones como los sistemas de información de salud no prefieren los usuarios si la información de identidad personal se revela en el libro mayor. La privacidad de la identidad del usuario también es una preocupación importante en la implementación de contratos inteligentes basados en blockchain [138].

Privacidad en la ejecución de contratos inteligentes (I4): El inteligente los contratos son programas que se ejecutan en la infraestructura computacional [139]. En blockchain, los contratos inteligentes se ejecutan en los nodos. Se puede acceder a las instrucciones ejecutadas en la máquina utilizando varios enfoques [140], [141]. Por ejemplo, la contraseña ingresada por un usuario debe cargarse en la memoria y puede verse de forma clara utilizando herramientas de volcado de memoria. Este tipo de robos de datos de nivel inferior en la ejecución se consideran violaciones de la privacidad en determinadas circunstancias [142].

2) Soluciones potenciales

A continuación, discutimos y categorizamos varias posibles soluciones sobre cómo preservar la privacidad de los contratos inteligentes.

a: preservar la privacidad de los datos de las transacciones

Ibáñez et al. [143] presentó información significativa sobre diferentes aspectos de la tecnología blockchain, incluida la regulación general de protección de datos y su aplicabilidad en blockchain como facilitador de la protección de datos. Los autores discutieron la aplicación de contratos inteligentes en cadenas de bloques autorizadas y cadenas de bloques sin permiso en asociación con controladores de datos apropiados. Los autores categorizaron los dos tipos de soluciones para permitir el cumplimiento, como la integración de diferentes funciones criptográficas y esquemas de computación privados sin revelar el contenido de las transacciones y la aplicación de blockchains como máquinas de verificación descentralizadas.

Juels y col. [144] ilustró el surgimiento de los contratos inteligentes criminales que facilitarán la revelación de la información confidencial. Los autores ilustraron algunos problemas, incluido el robo de claves criptográficas por contratos inteligentes criminales. Sus resultados destacaron la creación de políticas y medidas técnicas de protección contra los contratos inteligentes delictivos para garantizar los objetivos beneficiosos de los contratos inteligentes.

Kosba et. al [119] presenta Hawk, un contrato inteligente que preserva la privacidad, que disipó el obstáculo de privacidad encontrado en Bitcoin y Ethereum como moneda. Los autores proponen un marco que permite a un programador no especializado redactar un contrato inteligente que preserve la privacidad. Hawk garantiza la privacidad en la cadena, que oculta criptográficamente el flujo de dinero y la cantidad a la vista del público.

b: Protección de la privacidad del usuario

Niya y col. [120] demostró un diseño e implementación de una aplicación comercial que utilizaba contratos inteligentes de Ethereum. La aplicación está desarrollada con fl exibilidad en solicitando la identidad del usuario directamente por el vendedor y el comprador. Se establece una cadena de bloques ligera para facilitar el intercambio de datos en los canales de dispositivo a dispositivo.

Chatzopoulos y col. [121] propuso una nueva arquitectura para las tareas de detección de multitudes espaciales basadas en eventos en asociación con la cadena de bloques y la tecnología con la preservación de la privacidad del usuario. La arquitectura utiliza contratos inteligentes para permitir que los proveedores de servicios de detección de multitudes envíen sus solicitudes, realicen subastas con un costo óptimo y manejen los pagos.

Liang y col. [122] diseñó e implementó ProvChain, que es una arquitectura descentralizada para la procedencia confiable de datos en la nube. Provchain proporciona características de seguridad importantes, como la procedencia a prueba de manipulaciones y la privacidad del usuario. Las principales fases operativas son la recopilación de datos de procedencia, el almacenamiento de datos de procedencia y la validación de datos de procedencia, que proporciona registros a prueba de manipulaciones para permitir la transparencia y la responsabilidad de los datos en la nube.

c: Privacidad en la lógica

Al Bassam y col. [123] presenta ChainSpace, que ofrece extensibilidad amigable con la privacidad en la plataforma de contrato inteligente. La plataforma ofrece una mayor escalabilidad que la plataforma existente lograda a través de la fragmentación entre nodos utilizando un novedoso protocolo de compromiso atómico distribuido denominado S-BAC. También es compatible con la auditabilidad y la transparencia.

Kalodner y col. [124] presentó Arbitrum, que es un sistema de criptomonedas con contratos inteligentes. El modelo de Arbitrum es compatible para contratos inteligentes privados que no revela el estado interno a los verificadores que participan en la validación de transacciones en determinadas circunstancias. Arbitrum incentiva a las partes a acordar fuera de la cadena sobre el comportamiento de VM, lo que significa que los mineros de Arbitrum solo requieren verificar las firmas digitales sin revelar el contrato para confirmar que las partes acordaron el comportamiento de VM.

d: entorno de ejecución de confianza (TEE)

Un entorno de ejecución de confianza como Intel SGX [145] garantiza la confidencialidad y la privacidad durante la ejecución del código.

Zhang y col. [126] presentó un sistema de alimentación de datos autenticado que se denomina Town Crier. Town Crier proporciona un puente entre los contratos inteligentes y los sitios web existentes en los que comúnmente se confía para aplicaciones que no son blockchain. El frontend y el backend de hardware se combinan con la solución que está habilitada con privacidad según sea necesario.

Cheng et al [125] presentaron Ekiden, que combina blockchain con TEE. Los autores aprovecharon una arquitectura novedosa que separa el consenso de la ejecución y permitió la confidencialidad preservando los contratos inteligentes en un entorno de ejecución confiable. Los autores planearon ampliar su trabajo para permitir la computación segura de múltiples partes en el futuro.

Yuan y col. [127] presentó ShadowEth, que es un sistema que aprovecha un enclave de hardware para garantizar la confidencialidad de los contratos inteligentes en cadenas de bloques públicas como Ethereum. El sistema también garantiza la integridad y la disponibilidad. Los autores implementaron el prototipo utilizando Intel SGX en

Red Ethereum para analizar la seguridad y vulnerabilidad del sistema.

e: Computación segura entre múltiples partes

Benhamouda y col. [128] presentó un método para hacer que la plataforma de cadena de bloques Hyperledger Fabric sea compatible con datos privados utilizando computación segura de múltiples partes. El protocolo se implementó utilizando el problema millonario de Yao [146] y la transferencia inconsciente. Los autores asociaron un servidor auxiliar, que separa la computación de múltiples partes en fuera de la cadena.

Zyskin y col. [129] presentó Enigma, que es un modelo computacional basado en una versión altamente optimizada de computación segura multipartita denominada Enigma que garantiza esquemas de intercambio de secretos verificables y asegura la confidencialidad. Los autores utilizaron una tabla hash distribuida modificada para almacenar datos compartidos en secreto con una cadena de bloques externa como controlador de la red para controlar el acceso y la gestión de identidad. Los componentes privados de los contratos inteligentes se ejecutan fuera de la cadena en la plataforma Enigma y se denominan contratos privados.

C. REDUCIR LOS GASTOS GENERALES DE COMPUTACIÓN DE LOS CONTRATOS INTELIGENTES

La ejecución de contratos inteligentes es un proceso que consume muchos recursos. Las partes interesadas del contrato inteligente deben compensar la ejecución de las partes relevantes. En Ethereum, el costo se evalúa en gas. Los contratos inteligentes que no son óptimos son costosos en el cálculo y eventualmente incurrirán en un costo adicional para los usuarios de los contratos inteligentes. Además, el consumo excesivo de recursos propios de los contratos inteligentes colapsará todo el sistema. Por lo tanto, la condición de ejecución óptima es muy esperada en el contexto de los contratos inteligentes.

1) Soluciones potenciales

Idelberger y col. [147] presentó información importante con las ventajas y desventajas técnicas de los contratos inteligentes basados en la lógica cuando se presentan los contratos ordinarios. Los autores demostraron que un enfoque basado en la lógica puede complementar ventajosamente su componente de procedimiento en pocas dimensiones, incluida la negociación, la formación y el almacenamiento. Los autores enfatizaron que los enfoques lógicos y procedimentales no son incompatibles en los contratos inteligentes. Chen y col. [148] desarrolló GASPER, una herramienta que localiza los patrones costosos del gas de contrato inteligente de Ethereum mediante el análisis del código de bytes del contrato inteligente. Los creadores pueden ser sobrecargados por contratos inteligentes sub optimizados por el consumo adicional de gas. En la evaluación, los autores descubrieron 3 patrones predefinidos representativos de 4.240 contratos inteligentes. Kothapalli y col. [149] implementó un protocolo compatible con incentivos llamado SmartCast que se ejecuta fuera de la cadena y depende de la criptomoneda existente para la implementación del mecanismo de recompensa y castigo. El enfoque creó un sistema que permite a los trabajadores hacer cumplir la integridad puede recompensar su participación correcta en el proceso que se hizo cumplir a través de contratos inteligentes de Ethereum. Los autores evaluaron la viabilidad del enfoque mediante la construcción de un implementación del prototipo que comprende el contrato inteligente de Ethereum y el protocolo de consenso fuera de la cadena.

D. MEJORAS DE CONCURRENCIA

Una vez que los contratos inteligentes se implementan en una cadena de bloques, se espera que se ejecuten en múltiples instancias. Para mejorar la e fi ciencia, varios estudios han propuesto enfoques para mejorar la concurrencia de contratos inteligentes. Se propusieron dos categorías principales de enfoques, incluido el ordenamiento básico de marcas de tiempo (BTO) y el ordenamiento de transacciones de múltiples versiones (MVTO). BTO asigna a cada transacción una marca de tiempo y determina el orden de serialización de las transacciones para la ejecución o el acceso a un recurso en función de las marcas de tiempo. MVTO garantiza que si se detecta una inconsistencia entre dos transacciones que acceden a elementos de datos relevantes, una de ellas abortará. Por ejemplo, Zhang et al. [150] propuso un esquema concurrente para ejecutar contratos inteligentes de manera concurrente que arrojó una velocidad de procesamiento 2.5 veces mayor en la validación de bloques con tres hilos de trabajo. Anjana y col. [151] desarrolló un marco eficiente basado en sistemas de memoria transaccional de software (STM) para permitir la ejecución concurrente de contratos inteligentes. El marco propuesto arrojó aumentos de velocidad de 3.6xy 3.7x sobre los mineros en serie bajo BTO y MVTO respectivamente.

IV. LECCIONES APRENDIDAS Y TRABAJOS FUTUROS

La sección anterior refleja los aspectos técnicos significativos de los contratos inteligentes basados en blockchain desde una perspectiva más amplia. Se analizan los inconvenientes y algunas soluciones a los contratos inteligentes existentes. Esta sección se elabora con conocimientos significativos de los aspectos técnicos de los contratos inteligentes y las direcciones de investigación para futuras mejoras.

A. ATAQUES DE SEGURIDAD, VULNERABILIDADES Y SOLUCIONES DE SEGURIDAD EN CONTRATOS INTELIGENTES

1) Lecciones aprendidas

Los lenguajes de programación de software ordinarios se pueden utilizar en los lenguajes de programación utilizados para contratos inteligentes, por ejemplo, Java, Javascript y GoLang. Estos lenguajes están diseñados para ser Turing completos para lograr una funcionalidad completa. La programación de contratos inteligentes estará expuesta a errores humanos como otros programas de software ordinarios. Los daños resultantes de los errores de programación son exponenciales ya que los contratos inteligentes se implementan en todos los nodos. Los contratos inteligentes se distinguen ya que una vez que se implemente el código, se distribuirán en toda la red, lo que dificulta la aplicación de parches como programas ordinarios. Por lo tanto, los programadores deben asegurarse de que se garantice que los programas de contratos inteligentes estén libres de errores. La investigación sobre la mejora de los errores de contratos inteligentes está evolucionando y se anima a los programadores a utilizar los resultados de la investigación. como bibliotecas mejoradas. Los programadores son capaces de utilizar una red privada para simular los ataques o pruebas formales de penetración para la evaluación de la respuesta en contratos inteligentes para el escenario de ataque. Los contratos inteligentes necesarios para actualizar con los parches sobre las vulnerabilidades de seguridad del contrato inteligente identificadas por la investigación y asegurarse

los programas desarrollados por ellos están libres de estas vulnerabilidades conocidas.

Además, los principios de programación son aplicables a la programación de contratos inteligentes. Se requiere que los contratos inteligentes se programen con simplicidad para eliminar los gastos generales. Es necesario considerar las diferentes especificaciones de hardware de los nodos de la cadena de bloques. La integración de bucles debe minimizarse y las ejecuciones recursivas requieren eliminación y desarrollo. Cuando se manipulan los números, es fundamental evitar que los códigos se desborden aritméticos. Si existen bibliotecas específicas para eliminar tales errores, estas bibliotecas deben utilizarse en los contratos inteligentes. Los códigos que darán lugar a interbloqueos requieren identificación y eliminación antes de la implementación del contrato inteligente. En general, los contratos inteligentes deben diseñarse teniendo en cuenta la eficiencia de la memoria y la computación.

Además, a medida que se amplían las áreas de aplicación de los contratos inteligentes, los códigos deben verificarse formalmente. La veri fi cación formal requiere que el contrato inteligente particular, eventualmente un programa de computadora, se ejecute según la especificación formal anticipada por las partes interesadas. La especificación formal de los contratos inteligentes requiere una definición clara con el apoyo de expertos. Especialmente cuando las cadenas de bloques subyacentes se integran con sistemas de misión crítica como la gestión del tráfico aéreo y los sistemas de salud, la verificación formal será un requisito obligatorio. La verificación formal no debería requerir la intervención de terceros. Por ejemplo, la detección de vulnerabilidades requiere probadores de penetración expertos para simular ataques de seguridad y detectar vulnerabilidades. Las auditorías de seguridad pueden requerir la intervención de expertos. Pero la verificación formal solo requiere establecer especificaciones formales que pueden ser experiencia de los desarrolladores. Los desarrolladores de contratos inteligentes deben conocer los métodos formales de verificación para verificar los contratos inteligentes antes de la implementación. La verificación formal identifica vulnerabilidades importantes, como bloquear los fondos, enviar fondos a otras cuentas continuamente sin el consentimiento del propietario de la cuenta, etc. La verificación formal es una de las mejores prácticas obligatorias para los futuros desarrolladores de contratos inteligentes. enviar fondos a otras cuentas continuamente sin el consentimiento del propietario de la cuenta y así sucesivamente. La verificación formal es una de las mejores prácticas obligatorias para los futuros desarrolladores de contratos inteligentes. enviar fondos a otras cuentas continuamente sin el consentimiento del propietario de la cuenta y así sucesivamente. La verificación formal es una de las mejores prácticas obligatorias para los futuros desarrolladores de contratos inteligentes.

2) Trabajo futuro

Los lenguajes de programación de contratos inteligentes son Turing completos en la mayoría de las plataformas líderes. La integridad de Turing lleva a todo el sistema de contratos inteligentes a riesgos de seguridad según las investigaciones anteriores. Por lo tanto, algunas de las plataformas de contratos inteligentes como Stellar están diseñadas con el lenguaje de contratos inteligentes incompleto de Turing. Aunque los contratos inteligentes incompletos de Turing no proporcionan la funcionalidad completa como los contratos completos de Turing, se eliminan algunos de los riesgos de seguridad. La asignación de limitaciones de consumo de energía computacional, como el límite de gas, será una consideración de desarrollo prudente en los contratos inteligentes que eliminarán los desbordamientos del consumo de recursos. La evaluación de la corrección de los contratos inteligentes es una consideración esencial en el desarrollo futuro de los sistemas de contratos inteligentes.

soluciones según la Tabla 5. Los ataques Sybil (A3), los ataques mayoritarios (A6), los contratos destruibles (A7) y los trastornos de excepción (A8) requieren que se aborden más a fondo mediante las próximas soluciones de seguridad antes de que los ataques generen pérdidas financieras.

Además de eso, las bibliotecas de utilidades de terceros requieren que se desarrollen en paralelo. Por ejemplo, las operaciones criptográficas en cadena no son compatibles con la plataforma Hyperledger-Fabric. Si los contratos inteligentes se utilizan como una utilidad criptográfica, es necesario importar bibliotecas criptográficas. Es un requisito vital verificar que las bibliotecas de terceros importadas estén libres de vulnerabilidades. De lo contrario, la importación de las bibliotecas hará que todo el sistema blockchain sea vulnerable. Las mejoras de sintaxis sobre los contratos inteligentes también permitirán a las partes interesadas del negocio diseñar sus propios contratos inteligentes, con un conocimiento mínimo de programación. Además, los principios de diseño seguro de los contratos inteligentes evolucionarán como patrones de diseño recomendados como los principales lenguajes de programación ya definidos.

La verificación formal de los contratos inteligentes se prevé como un estándar global en el desarrollo futuro de contratos inteligentes. Los desarrolladores, proveedores de plataformas adoptarán la compatibilidad de verificación formal de las plataformas blockchain. Hay oportunidades para que los investigadores desarrollen marcos para diseñar convenientemente especificaciones formales que son los prerrequisitos para la verificación formal de contratos inteligentes. Las técnicas como la IA se pueden consolidar en las metodologías formales de verificación de la próxima generación. En el futuro, las plataformas de servicio para la verificación formal también pueden estar disponibles en línea para plataformas populares de contratos inteligentes. Este tipo de arquitectura de servicio se puede utilizar para respaldar la verificación formal asistida por IA de contratos inteligentes.

B. PROBLEMAS DE PRIVACIDAD Y SOLUCIONES

1) Lecciones aprendidas

La característica principal de la tecnología de contabilidad distribuida es la visibilidad de los datos de las transacciones para todos los pares de la red. La mayoría de las personas se muestran reacias a adoptar tecnologías blockchain debido a la falta de privacidad y visibilidad de los datos de las transacciones. Una plétora de investigaciones realizadas para mejorar la privacidad en tecnologías de contabilidad distribuida. La mejora de la privacidad es un requisito obligatorio cuando los contratos inteligentes se incorporan a los sistemas comerciales futuros. Dado que la transparencia es una fortaleza vital de blockchain, las técnicas de mejora de la privacidad no deben violar la transparencia del sistema blockchain. Una posible solución es almacenar datos fuera de la cadena. Para incorporar la privacidad y el cifrado con contratos inteligentes, se requiere un marco de gestión de claves sólido. A veces, el marco de gestión de claves requiere vincularse con los HSM para alinearse con los requisitos de cumplimiento. Según la Tabla 6, la privacidad de la lógica del contrato inteligente requiere mayor atención en la investigación como mejora de la privacidad. Además, las personalizaciones de los requisitos de privacidad también deben cumplir con el caso de uso comercial concreto.

2) Trabajo futuro

En el futuro, se puede esperar que los contratos inteligentes se integren con muchos sistemas comerciales con diferentes requisitos de privacidad. Por lo tanto, se pueden anticipar más técnicas de mejora de la privacidad a partir de la investigación. La naturaleza distribuida y transparente de los contratos inteligentes basados en blockchain se puede observar como una característica contradictoria desde una perspectiva de privacidad. Sin embargo, se utilizarán diferentes técnicas en los futuros sistemas de contratos inteligentes para equilibrar la privacidad y la descentralización. La gestión de claves de contratos inteligentes también será una dirección emergente de investigación en los futuros sistemas blockchain. La privacidad será un requisito de cumplimiento de seguridad de datos, como PCI-DSS / PA-DSS para sistemas financieros y HIPAA para sistemas de gestión de datos de atención médica. Si los contratos inteligentes basados en blockchain se van a adoptar con casos de uso de la industria, Es obligatorio diseñar los contratos inteligentes con disposiciones que se alineen con las regulaciones. Además de los datos de la transacción, la privacidad del usuario también es un requisito vital en las redes blockchain. Se requiere que las futuras redes blockchain estén diseñadas para el funcionamiento sinérgico de los sistemas de gestión de usuarios existentes. Los sistemas de contratos inteligentes deben ser compatibles con las soluciones de gestión de usuarios basadas en PKI existentes junto con los esquemas de autenticación asistidos por hardware, como tarjetas inteligentes o tokens de hardware. El diseño arquitectónico modular será un principio de diseño ideal en los futuros sistemas blockchain para simplificar la integración con las plataformas existentes. Para una computación segura utilizando datos de contratos inteligentes, también existen varias oportunidades en aplicaciones como la computación segura de múltiples partes.

C. REDUCIR LOS GASTOS GENERALES DE COMPUTACIÓN DE LOS CONTRATOS INTELIGENTES

1) Lecciones aprendidas

La optimización del rendimiento es un requisito importante de los contratos inteligentes. Los contratos inteligentes a menudo se integran con aplicaciones como finanzas, aviación, administración de identidades y control de acceso, donde se espera una operación en tiempo real con una latencia mínima y un mayor rendimiento. Dado que la cadena de bloques Ethereum ampliamente utilizada no admite la concurrencia, existen limitaciones para expandir el dominio de aplicación de Ethereum. El servicio de almacenamiento del libro mayor, el mecanismo de consenso y los lenguajes de programación de contratos inteligentes son las principales dependencias de la ejecución de los contratos inteligentes. Además, la verificación de transacciones de la cadena de bloques subyacente también afecta el rendimiento. Por ejemplo, la verificación de doble gasto es una verificación adicional realizada en los contratos inteligentes financieros. La optimización del contrato inteligente se puede lograr de diferentes formas. La optimización del protocolo de consenso es un enfoque eficaz. El ordenamiento de transacciones de múltiples versiones y el ordenamiento básico de marcas de tiempo son algunas de las técnicas de optimización de consenso. La integración del consenso de Ripple, la plataforma de contrato inteligente Stellar redujo el tiempo de procesamiento de transacciones en 3-5 segundos. La incorporación de un alto rendimiento de escritura también mejora el rendimiento de la base de datos distribuida. La estimación del consumo de gas antes de la implementación de los contratos inteligentes de Ethereum, se garantiza que la ejecución esté restringida dentro de los límites cuando se implementan en una red pública de blockchain.

2) Obras futuras

Dado que los contratos inteligentes se implementan en la cadena de bloques pública y afectan la eficiencia de todo el sistema de la cadena de bloques, es importante que los contratos inteligentes estén optimizados. La penalización de los contratos inteligentes en condiciones óptimas será una solución eficaz para eliminarlos en condiciones óptimas. Se puede desarrollar un mecanismo de calificación de desempeño global para plataformas de cadenas de bloques conocidas como Ethereum para evaluar de forma independiente el desempeño de los contratos inteligentes. Antes de implementar contratos inteligentes en la cadena de bloques, las partes interesadas deben aprobar la calificación de rendimiento. La evaluación se puede implementar como una plataforma de servicio. Sin embargo, los desarrolladores de contratos inteligentes ahora están predispuestos a implementar contratos inteligentes simplificados y transferir gastos generales computacionales a servicios fuera de la cadena. Si los gastos generales computacionales se transfieren fuera de la cadena, la privacidad y la integridad de los datos se vuelven vulnerables. Además, el servicio fuera de la cadena puede ser un factor adicional que limita el rendimiento. Para la integración fuera de la cadena, la API REST se puede utilizar para pasar los datos que se calcularán al exterior. Sin embargo, la API REST también tendrá ciertas limitaciones desde una perspectiva de rendimiento. Por tanto, se pueden utilizar técnicas de integración alternativas como gRPC. Si la sobrecarga computacional se transfiere a los nodos Edge en el futuro, se puede utilizar COAP para la integración. Se pueden utilizar técnicas de integración alternativas como gRPC. Si la sobrecarga computacional se transfiere a los nodos Edge en el futuro, se puede utilizar COAP para la integración. Se pueden utilizar técnicas de integración alternativas como gRPC. Si la sobrecarga computacional se transfiere a los nodos Edge en el futuro, se puede utilizar COAP para la integración.

D. MEJORAS DE CONCURRENCIA

1) Lecciones aprendidas

La concurrencia es esencial para que los contratos inteligentes puedan hacer frente a las demandas futuras. La ejecución de contratos inteligentes y los mecanismos de consenso deben mejorarse para cumplir con las demandas de concordancia. Las mejoras de simultaneidad no deben sacrificar las características de seguridad. La sincronización de bloques y el mantenimiento de la coherencia en el libro mayor deben tenerse en cuenta al diseñar los mecanismos de mejora de la concurrencia.

2) Obras futuras

Se espera que los contratos inteligentes jueguen un papel vital en el contexto de la IoT industrial en el futuro. Las mejoras de concurrencia deben alinearse con la naturaleza informática restringida de IoT. La concurrencia en los mecanismos de consenso debe ser eficiente para cumplir con los requisitos de IoT.

V. OTROS TEMAS DE INVESTIGACIÓN FUTUROS

A continuación, examinamos la posibilidad de aplicar otras teorías informáticas a los contratos inteligentes en diferentes aspectos. Se discute la aplicabilidad y trabajos relacionados de teorías significativas de la informática a los contratos inteligentes.

1) Contratos inteligentes y teoría de juegos

La teoría de juegos consiste en un conjunto de herramientas matemáticas para identificar las interacciones entre agentes. La combinación de contratos inteligentes y teoría de juegos se destaca como temas de investigación emergentes. Hay muchas aplicaciones que serán beneficiosas para los contratos inteligentes. Liu y col. [73] presentó una encuesta completa sobre la aplicación de la teoría de juegos a los contratos inteligentes. Los autores discutieron la aplicabilidad de la teoría de juegos para diferentes aspectos de los contratos inteligentes, como la seguridad y la gestión de la minería. Los autores también destacaron los desafíos existentes y las direcciones de investigación futuras. Piasecki [152] discutió la teoría de los juegos detrás de los casinos integrados con contratos inteligentes. El autor exploró que un atacante que sea financieramente fuerte puede engañar al sistema comprando potencia informática que es beneficiosa para él.

2) Contratos inteligentes e inteligencia artificial

La inteligencia artificial (IA) se puede aplicar a los contratos inteligentes de diferentes formas. Algunas técnicas de IA se pueden incorporar en los códigos de contratos inteligentes, otras se pueden utilizar para validar contratos inteligentes. Además, hay muchas aplicaciones emergentes de Tensor y otros conceptos de aprendizaje profundo para los contratos inteligentes basados en blockchain. La computación cognitiva es otro subconjunto de la IA que simula los pensamientos humanos sobre la infraestructura informática.

a: IA para pruebas y evaluación de contratos inteligentes

La IA es generalmente aplicable a la prueba de contratos inteligentes. Más específicamente, las pruebas se pueden centrar en direcciones como las pruebas de rendimiento, la detección de vulnerabilidades y la evaluación de la corrección de los contratos inteligentes. La contribución de la IA como un servicio de utilidad para la cadena de bloques es importante para mejorar los contratos inteligentes basados en cadenas de bloques y el rendimiento. Marwala y col. [153] presentó cómo utilizar la IA para la verificación de contratos inteligentes. Los autores señalaron aplicaciones importantes de la inteligencia artificial en el contexto del contrato inteligente basado en blockchain, como la mejora de la seguridad, la escalabilidad, etc. Los autores también destacaron la aplicabilidad de la verificación formal basada en IA para la evaluación de contratos inteligentes.

b: aprendizaje federado

El aprendizaje federado es un enfoque de aprendizaje descentralizado y colaborativo que está alineado con la capacidad de descentralización de la cadena de bloques. El aprendizaje federado funciona sin cargar los datos sin procesar como conjuntos de datos de entrenamiento. Especialmente, la información sensible distribuida, como la información de salud, se puede integrar con blockchain para lograr diferentes funcionalidades, como el control de acceso a datos y el aprendizaje federado. La combinación de aprendizaje federado y contratos inteligentes puede generar nuevas oportunidades de investigación. Lu y col. [154] propuso una cadena de bloques y un mecanismo de preservación de la privacidad basado en el aprendizaje federado para el IoT industrial. Los autores integraron el aprendizaje federado al consenso para mejorar la consumo de recursos informáticos y eficiencia en funcionamiento. Los problemas abiertos asociados con la infraestructura de computación con recursos restringidos también se discuten para resaltar los requisitos de privacidad de los datos. Kang y col. [155] propuso un sistema de aprendizaje federado basado en una cadena de bloques de consorcio. Los autores diseñaron un mecanismo de incentivos basado en la teoría del contrato para evaluar a los trabajadores de alta reputación en busca de una capacitación confiable para desarrollar el proceso de aprendizaje. Los autores también discutieron el requisito de mejora del cálculo de reputación.

c: contratos inteligentes y computación cognitiva

La computación cognitiva es un tema de investigación avanzada de inteligencia artificial que permite el pensamiento humano en la infraestructura informática. La computación cognitiva se adopta con el patrón de pensamiento humano y las limitaciones en la ejecución, lo que produce una precisión significativamente mayor en comparación con las otras técnicas de IA. Los contratos inteligentes basados en blockchain mejorarán los valores del servicio en los diferentes escenarios de aplicación de la computación cognitiva. La transparencia de los datos, la capacidad de control de acceso descentralizado y la confianza descentralizada son las características importantes de los contratos inteligentes basados en blockchain en la perspectiva de la computación cognitiva. Daniel y col. [156] realizó una encuesta sobre la aplicabilidad de la computación cognitiva en el dominio de la salud.

d: contratos inteligentes con redes tensoriales

Hay aplicaciones significativas en las redes de tensores para contratos inteligentes. Estas aplicaciones son relevantes para industrias como la financiera y el comercio minorista. El modelado predictivo, el análisis del patrón de compra del cliente se puede asociar con blockchain y redes de tensores. Charlie y col. [157] presentó un enfoque basado en tensores para predecir interacciones de contratos inteligentes en función de sus intercambios de criptomonedas. El modelado de tenor y el enfoque basado en el proceso estocástico utilizado para subrayar los intercambios reales entre contratos inteligentes. El enfoque propuesto también es capaz de predecir intercambios futuros.

3) Contratos inteligentes en ciencia de datos

Los contratos inteligentes son aplicables como técnica escalable en ciencia de datos. Especialmente, el control de un volumen de datos masivo en una arquitectura centralizada genera cuellos de botella en el rendimiento, riesgos de falla y riesgos de seguridad. El papel de los contratos inteligentes para la ciencia de datos es vital en diferentes aspectos. Las aplicaciones de los contratos inteligentes basados en blockchain para la ciencia de datos incluyen el control de acceso a los datos, la integridad de los datos, la garantía de una confianza descentralizada y la habilitación de mecanismos de intercambio de datos confiables. Kara fi loski [158] presentó una encuesta sobre soluciones basadas en blockchain para big data. Los autores revisaron diferentes casos de uso, como el control de acceso a registros médicos, IoT y la gestión de propiedades digitales. Abdullah y col. [159] técnicas de autenticación detalladas asociadas con blockchain para big data. Los autores discutieron la autenticación Kerberos y

cómo la cadena de bloques es capaz de abordar las limitaciones identificadas. Yue y col. [160] presenta una plataforma de intercambio de datos que garantiza la trazabilidad. Los contratos inteligentes se pueden utilizar para permitir el intercambio de datos. Xu y col. [161] presentó un sistema de almacenamiento inteligente basado en contratos, denominado Sapphire para respaldar el análisis de datos en IoT. Uchibeke y col. [162] desarrolló un sistema de control de acceso blockchain utilizando Hyperledger Fabric para controlar el acceso de grandes conjuntos de datos.

VI. CONCLUSIÓN

El documento comienza con los conceptos que son requisitos previos para los contratos inteligentes basados en blockchain. Los aspectos técnicos de la sección de contratos inteligentes proporcionan una amplia discusión sobre las características esenciales de los contratos inteligentes. Los contratos inteligentes y la investigación actual de temas importantes en informática también incluyeron la sección de aspectos técnicos. La sección de lecciones aprendidas y trabajos futuros se elaboró con una descripción general de las direcciones de investigación futuras junto con importantes conocimientos de los aspectos técnicos. Como podemos ver, los dominios de aplicación de los contratos inteligentes expandirán el futuro. La brecha entre los contratos humanos e inteligentes se eliminará en el futuro a través de la movilidad. Los contratos inteligentes deben mejorarse en forma de eficiencia y tiempo de procesamiento de transacciones y expondrá más oportunidades para los contratos inteligentes. La próxima generación de computación requiere una computación óptima y liviana. Por lo tanto, los mecanismos de consenso deben mejorar para respaldar el funcionamiento de la cadena de bloques en una infraestructura informática futura con recursos limitados. La reducción de la brecha del contrato humano-inteligente será una preocupación de investigación clave en el futuro para mejorar la usabilidad de los contratos inteligentes para resolver los problemas en los sistemas existentes.

RECONOCIMIENTO

Este trabajo se ha realizado bajo 5GEAR Menot CWC-NS (Grane No: 2430299111) y el marco de 6Genesis Flagship (Grant No: 318927).

REFERENCIAS

[1] M. Garriga, S. Dalla Palma, M. Arias, A. De Renzis, R. Pareschi y D. Andrew Tamburri, "Blockchain y criptomonedas: una clasificación y comparación de controladores de arquitectura", Concurrencia y computación: práctica y Experiencia, p. e5992, 2020.

[2] S. Cohen, A. Rosenthal y A. Zohar, "Razonamiento sobre el futuro en las bases de datos Blockchain", en la 36a Conferencia Internacional de Ingeniería de Datos (ICDE) de IEEE 2020. IEEE, 2020, págs. 1930–1933.

[3] G. Srivastava, RM Parizi y A. Dehghantanha, "El futuro de la tecnología blockchain en la seguridad del Internet de las cosas en la atención médica", en Ciberseguridad, confianza y privacidad de Blockchain. Springer, 2020, págs. 161–184.

[4] A. Bazarhanova, J. Magnusson, J. Lindman, E. Chou y A. Nilsson, "Identificación electrónica basada en blockchain: comparación entre países de seis opciones de diseño", 2019.

[5] T. Aste, P. Tasca y T. Di Matteo, "Tecnologías Blockchain: El impacto previsible en la sociedad y la industria", computadora, vol. 50, no. 9, págs. 18-28, 2017.

[6] SK Lo, X. Xu, YK Chiam y Q. Lu, "Evaluación de la idoneidad de la aplicación de blockchain", en 2017 22ª Conferencia Internacional sobre Ingeniería de Sistemas Computacionales Complejos (ICECCS). IEEE, 2017, págs. 158-161.

[7] M. Pilkington, "Tecnología Blockchain: principios y aplicaciones", en Manual de investigación sobre transformaciones digitales. Edward Elgar Publishing, 2016.

[8] MJM Chowdhury, A. Colman, MA Kabir, J. Han y P. Sarda, "Blockchain versus base de datos: un análisis crítico", en 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference Sobre ciencia e ingeniería de Big Data (TrustCom / BigDataSE). IEEE, 2018, págs. 1348-1353.

[9] F. Hofmann, S. Wurster, E. Ron y M. Böhmecke-Schwafert, "El concepto de inmutabilidad de las cadenas de bloques y los beneficios de la estandarización temprana", en 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE, 2017, págs. 1–8.

[10] M. Di Pierro, "¿Qué es la cadena de bloques?" Computación en ciencia e ingeniería, vol. 19, no. 5, págs. 92–95, 2017.

[11] A. Anjum, M. Sporny y A. Sill, "Estándares de blockchain para el cumplimiento y la confianza", IEEE Cloud Computing, vol. 4, no. 4, págs. 84–90, 2017.

[12] R. Zhang, R. Xue y L. Liu, "Seguridad y privacidad en blockchain", ACM Comput. Surv., Vol. 52, no. 3, págs. 51: 1–51: 34, julio de 2019. [En línea]. Disponible: http://doi.acm.org/10.1145/3316481

[13] Q. Zhu, SW Loke, R. Trujillo-Rasua, F. Jiang y Y. Xiang, "Aplicaciones de las tecnologías de contabilidad distribuida al Internet de las cosas: una encuesta", ACM Comput. Surv., Vol. 52, no. 6, págs. 120: 1–120: 34, nov. 2019. [En línea]. Disponible: http://doi.acm.org/10.1145/3359982

[14] IA Qasse, M. Abu Talib y Q. Nasir, "Comunicación entre cadenas de bloques: una encuesta", en Actas de la pista de investigación de la sexta conferencia internacional anual de ArabWIC, ser. ArabWIC 2019. Nueva York, NY, EE. UU .: ACM, 2019, págs. 2: 1–2: 6. [En línea]. Disponible: http://doi.acm.org/10.1145/3333165.3333167

[15] W. Chen, Z. Xu, S. Shi, Y. Zhao y J. Zhao, "Una encuesta de aplicaciones blockchain en diferentes dominios", en Actas de la Conferencia Internacional 2018 sobre Tecnología y Aplicación Blockchain, ser. ICBTA 2018. Nueva York, NY, EE. UU .: ACM, 2018, págs. 17–21. [En línea]. Disponible: http://doi.acm.org/10.1145/3301403.3301407

[dieciséis] P. Chakraborty, R. Shahriyar, A. Iqbal y A. Bosu, "Comprensión de las prácticas de desarrollo de software de los proyectos de blockchain: una encuesta", en Actas del 12º Simposio Internacional ACM / IEEE sobre Ingeniería y Medición de Software Empírico, ser. ESEM '18. Nueva York, NY, EE. UU .: ACM, 2018, págs. 28: 1–28: 10. [En línea]. Disponible: http://doi.acm.org/10.1145/3239235.3240298

[17] PT Duy, DTT Hien, DH Hien y V.-H. Pham, "Una encuesta sobre oportunidades y desafíos de la adopción de la tecnología blockchain para la innovación revolucionaria", en Actas del Noveno Simposio Internacional sobre Tecnología de la Información y la Comunicación, ser. SoICT 2018. Nueva York, NY, EE. UU .: ACM, 2018, págs. 200–207. [En línea]. Disponible: http://doi.acm.org/10.1145/3287921.3287978

[18] Btc, "Sí, Bitcoin puede hacer contratos inteligentes y Particl demuestra cómo". [En línea]. Disponible: https://bitcoinmagazine.com/articles/sí-bitcoin-puede-hacer-contratos-inteligentes-y-particl-demuestra-cómo /

[19] S. Lande y R. Zunino, "SoK: Unraveling Bitcoin Smart Contracts", Principios de seguridad y confianza LNCS 10804, p. 217, 2018.

[20] G. Wood, "Ethereum: A Secure Descentralized Generalized Transaction Ledger", documento amarillo del proyecto Ethereum, vol. 151, págs. 1–32, 2014.

[21] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne y ME Ylianttila, "Un esquema de pago tolerante al retraso basado en Ethereum Blockchain", CoRR, vol. abs / 1801.10295, 2018. [En línea]. Disponible: http://arxiv.org/abs/1801.10295

[22] D. Hopwood, S. Bowe, T. Hornby y N. Wilcox, "Especificación del protocolo Zcash", Tech. reps. 2016–1.10. Compañía de monedas eléctricas Zerocoin, Tech. Rep., 2016.

[23] E. Duffield y D. Diaz, "Dash: A Privacy-centric Cryptocurrency", No Publisher, 2015.

[24] MT Rosner y A. Kang, "Comprensión y regulación de los sistemas de pago del siglo XXI: el estudio de caso de Ripple", Mich. L. Rev., vol. 114, pág. 649, 2015.

[25] A. Azaria, A. Ekblaw, T. Vieira y A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", en 2016 2nd International Conference on Open and Big Data (OBD), agosto 2016, págs. 25-30.

[26] P. Nichol y J. Brandt, "Co-creación de confianza para la atención médica: el marco de criptociudadanos para la interoperabilidad con Blockchain", 07 de 2016.

[27] T. Kuo y L. Ohno-Machado, "ModelChain: Privacidad descentralizada - Preservación del marco de modelado predictivo de la atención médica en redes privadas de blockchain", CoRR, vol. abs / 1802.01746, 2018. [En línea]. Disponible: http://arxiv.org/abs/1802.01746

[28] GG Dagher, J. Mohler, M. Milojkovic y PB Marella, “Ancile: Marco de preservación de la privacidad para el control de acceso y la interoperabilidad de registros de salud electrónicos usando tecnología Blockchain”, Ciudades y sociedad sostenibles, vol. 39, págs. 283-297, 2018.

[29] X. Yue, H. Wang, D. Jin, M. Li y W. Jiang, “Puertas de enlace de datos sanitarios: inteligencia sanitaria encontrada en Blockchain con un novedoso control de riesgos de privacidad”, Journal of medical systems, vol. 40, no. 10, pág. 218, 2016.

[30] SP Novikov, OD Kazakov, NA Kulagina y NY Azarenko, “Blockchain y contratos inteligentes en una infraestructura de salud descentralizada”, en la conferencia internacional IEEE de 2018 “Gestión de calidad, transporte y seguridad de la información, tecnologías de la información” (TI, QM e IS). IEEE, 2018, págs. 697–703.

[31] S. Alexaki, G. Alexandris, V. Katos y EN Petroulakis, “Registros electrónicos de pacientes basados en blockchain para jurisdicciones de atención médica circulares reguladas”, en 2018 IEEE 23rd International Workshop on Computer Aided Model and Design of Communication Links and Networks (CAMAD). IEEE, 2018, págs. 1–6.

[32] T.-T. Kuo, H.-E. Kim y L. Ohno-Machado, "Tecnologías de libro mayor distribuido Blockchain para aplicaciones biomédicas y de atención médica", Revista de la Asociación Estadounidense de Informática Médica, vol. 24, no. 6, págs. 1211-1220, 2017.

[33] MI Mehar, CL Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanay- hie, HM Kim y M. Laskowski, "Comprensión de un gran experimento revolucionario y defectuoso en blockchain: el ataque dao", Journal of Casos de tecnología de la información (JCIT), vol. 21, no. 1, págs. 19–32, 2019.

[34] A. Wright y P. De Filippi, "Tecnología de cadena de bloques descentralizada y el auge de la criptografía Lex", disponible en SSRN 2580664, 2015.

[35] K. Wüst y A. Gervais, "¿Necesita una cadena de bloques?" en 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018, págs. 45–54.

[36] CD Clack, VA Bakshi y L. Braine, “Plantillas de contrato inteligente: requisitos esenciales y opciones de diseño”, preprint arXiv arXiv: 1612.04496, 2016.

[37] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin y F.-Y. Wang, "Una descripción general del contrato inteligente: arquitectura, aplicaciones y tendencias futuras", en el Simposio de vehículos inteligentes IEEE 2018 (IV). IEEE, 2018, págs. 108–113.

[38] N. Reiff, "¿Qué es ERC-20 y qué significa para Ethereum?" 2020. [En línea]. Disponible: https://www.investopedia.com/ news / what-erc20-and-what-does-it-mean-ethereum /

[39] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng y M. Imran, "Una descripción general de los contratos inteligentes: desafíos, avances y plataformas", Future Generation Computer Systems, vol. 105, págs. 475–491, 2020.

[40] V. Buterin et al., “Un contrato inteligente de próxima generación y una plataforma de aplicaciones descentralizadas”, informe técnico, vol. 3, pág. 37 de 2014.

[41] W. Corda, "Corda Técnico Papel blanco," https://www.corda.net/content/corda-technical-whitepaper.pdf.

[42] H. Fabric, “Hyperledger Fabric”, https://www.hyperledger.org/wp-content / uploads / 2018/07 /, 2018.

[43] R. Waves, "Waves", https://wavesplatform.com/files/whitepaper_v0.pdf.

[44] I. Bashir, Dominando Blockchain: Explicación de la tecnología de contabilidad distribuida, descentralización y contratos inteligentes. Packt Publishing Ltd, 2018.

[45] D. Macrinici, C. Cartofeanu y S. Gao, “Aplicaciones de contratos inteligentes dentro de la tecnología Blockchain: un estudio de mapeo sistemático”, Telemática e Informática, 2018.

[46] Z. Zheng, S. Xie, H. Dai, X. Chen y H. Wang, "Una descripción general de la tecnología Blockchain: Arquitectura, consenso y tendencias futuras", en el congreso internacional IEEE de 2017 sobre big data (congreso BigData). IEEE, 2017, págs. 557–564.

[47] A. Norta, "Diseño de una capa de aplicación de contrato inteligente para la transacción de organizaciones autónomas descentralizadas", en Conferencia internacional sobre avances en informática y ciencias de datos. Springer, 2016, págs. 595–604.

[48] T. Mancini-Griffoli, HSH Peria, I. Agur, A. Ari, J. Kiff, A. Popescu y C. Rochon, “Arrojando luz sobre la moneda digital del banco central”, Notas de debate del personal técnico del FMI, núm. 18-08, 2018.

[49] E. Shapiro, “Punto: Fundamentos de la democracia electrónica”, Comunicaciones de la ACM, vol. 61, no. 8, págs. 31–34, 2018.

[50] SS Gupta, Blockchain. John Wiley & Sons, Inc, 2017.

[51] F. Rizal Batubara, J. Ubacht y M. Janssen, “Desentrañar la transparencia y la responsabilidad en blockchain”, en Actas de la 20a Conferencia Internacional Anual sobre Investigación en Gobierno Digital, 2019, págs. 204–213.

[52] T. Nugent, D. Upton y M. Cimpoesu, "Mejora de la transparencia de datos en ensayos clínicos mediante contratos inteligentes de Blockchain", F1000Research, vol. 5, 2016.

[53] F. Yiannas, “Una nueva era de transparencia alimentaria impulsada por blockchain”, Innovaciones: tecnología, gobernanza, globalización, vol. 12, no. 1-2, págs. 46–56, 2018.

[54] M. Farnaghi y A. Mansourian, “Blockchain, una tecnología habilitadora para SIG participativos públicos descentralizados transparentes y responsables”, Cities, vol. 105, pág. 102850, 2020.

[55] N. Pokrovskaia, “Mecanismos reguladores fiscales, financieros y sociales dentro de la economía impulsada por el conocimiento. algoritmos blockchain y computación en niebla para la regulación eficiente ”, en 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). IEEE, 2017, págs. 709–712.

[56] F. Sander, J. Semeijn y D. Mahr, "La aceptación de la tecnología blockchain en la trazabilidad y transparencia de la carne", British Food Journal, 2018.

[57] C. Cachin et al., “Arquitectura de Hyperledger Blockchain Fabric”, en Taller sobre criptomonedas distribuidas y libros de contabilidad de consenso, vol. 310, no. 4, 2016.

[58] C. Dannen, Introducción a Ethereum y Solidity. Springer, 2017, vol. 1.

[59] GO Karame, E. Androulaki, M. Roeschlin, A. Gervais y S. Č apkun, “Mala conducta en Bitcoin: un estudio de doble gasto y responsabilidad”, ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 1, págs. 1–32, 2015.

[60] R. NEM, "NEM Técnico Referencia," https://nem.io/wp-contenido / temas / nem / archivos / NEM_techRef.pdf /.

[61] W. Stellar, "Documento técnico estelar", https://stellargold.net/whitepaper.pdf.

[62] E. Classic, "Ethereum Classic", Ethereum Classic (consultado el 16 de octubre 2017) https: // ethereumclassic. github. io.

[63] L. Goodman, “Tezos: un libro blanco de cripto-ledger auto-modificable”, URL: https: // www. tezos. com / static / papers / white_paper. pdf, 2014. "Documento técnico de

[64] Neo Blockchain". [En línea]. Disponible: https://docs.neo.org/ docs / en-us / index.html

[sesenta y] "Documento técnico de Cardano Blockchain". [En línea]. Disponible: https: // www. circle.com/marketing/pdfs/research/circle-research-cardano.pdf “EOS

[66] Blockchain Papel blanco." [En línea]. Disponible: https://github.com/BlockchainTranslator/EOS/blob/master/TechDoc/ EOS.IO-Technical-WhitePaper-v2.md

[67] "Documento técnico de Qtum Blockchain". [En línea]. Disponible: https: //old.qtum. org / user / pages / 03.tech / 01.white-papers / QtumWhitepaper.pdf

[68] "Libro blanco de Lisk". [En línea]. Disponible: https://github.com/slasheks/ lisk-whitepaper / blob / development / LiskWhitepaper.md

[69] "Libro blanco del arca".

[70] "Documento técnico de contrato inteligente impulsado por Bitcoin de la plataforma Rootstock". [En línea]. Disponible: https://www.rsk.co/wp-content/uploads/2019/02/ RSK-White-Paper-Updated.pdf

[71] "NXTWhitepaper". [En línea]. Disponible: https://www.rsk.co/wp-content/ uploads / 2019/02 / RSK-White-Paper-Updated.pdf

[72] T. Min y W. Cai, "Un caso de estudio de seguridad para juegos blockchain", en 2019 IEEE Games, Entertainment, Media Conference (GEM). IEEE, 2019, págs. 1–8.

[73] Z. Liu, NC Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang y DI Kim, "Una encuesta sobre Blockchain: una perspectiva teórica del juego", IEEE Access, vol. 7, págs. 47 615–47 643, 2019.

[74] Y. Zhang, S. Ma, J. Li, K. Li, S. Nepal, y D. Gu, "SMARTSHIELD: Automatic Smart Contract Protection Made Easy", en la 27a Conferencia Internacional de IEEE 2020 sobre análisis, evolución y reingeniería de software. neering (SANER). IEEE, 2020, págs. 23–34.

[75] CG Harris, "Los riesgos y desafíos de implementar contratos inteligentes de ethereum", en la Conferencia Internacional IEEE de 2019 sobre Blockchain y Criptomonedas (ICBC). IEEE, 2019, págs. 104–107.

[76] S. Kim y S. Ryu, "Análisis de contratos inteligentes de blockchain: técnicas y conocimientos", en 2020 IEEE Secure Development (SecDev). IEEE, 2020, págs. 65–73.

[77] P. Otte, M. de Vos y J. Pouwelse, “Trustchain: una cadena de bloques escalable resistente a la sibila”, Future Generation Computer Systems, vol. 107, págs. 770–780, 2020.

[78] Y. Cai y D. Zhu, “Detecciones de fraude para negocios en línea: una perspectiva desde la tecnología blockchain”, Innovación financiera, vol. 2, no. 1, pág. 20, 2016.

[79] M. Bellare, Z. Brakerski, M. Naor, T. Ristenpart, G. Segev, H. Shacham y S. Yilek, “Hedged public-key encryption: How to protect against bad

aleatoriedad ", en la Conferencia Internacional sobre Teoría y Aplicación de la Criptología y Seguridad de la Información. Springer, 2009, págs. 232–249.

[80] K. Chatterjee, AK Goharshady y A. Pourdamghani, "Contratos inteligentes probabilísticos: aleatoriedad segura en la cadena de bloques", en la Conferencia Internacional IEEE de 2019 sobre Blockchain y Criptomonedas (ICBC). IEEE, 2019, págs. 403–412.

[81] D. Efanov y P. Roschin, "La omnipresencia de la tecnología blockchain", Procedia Computer Science, vol. 123, págs. 116-121, 2018.

[82] UW Chohan, "El problema del doble gasto y las criptomonedas", disponible en SSRN 3090174, 2017.

[83] S. Zhang y J.-H. Lee, "Doble gasto con un ataque sybil en la red descentralizada de bitcoin", IEEE Transactions on Industrial Information, vol. 15, no. 10, págs. 5715–5722, 2019.

[84] S. Dey, "Asegurar el ataque mayoritario en blockchain mediante el aprendizaje automático y la teoría de juegos algorítmicos: una prueba de trabajo", en 2018, décima ciencia de la computación e ingeniería electrónica (CEEC). IEEE, 2018, págs. 7–10.

[85] J. Moubarak, E. Filiol y M. Chamoun, "Sobre la seguridad de la cadena de bloques y los ataques relevantes", en la Conferencia de Comunicaciones de IEEE Oriente Medio y África del Norte de 2018 (MENACOMM). IEEE, 2018, págs. 1–6.

[86] A. Groce, J. Feist, G. Grieco y M. Colburn, "¿Cuáles son los defectos reales en los contratos inteligentes importantes (y cómo podemos encontrarlos)?" en Conferencia Internacional sobre Criptografía Financiera y Seguridad de Datos. Springer, 2020, págs. 634–653.

[87] C. Liu, J. Gao, Y. Li, H. Wang y Z. Chen, "Estudiar las excepciones de gas en aplicaciones en la nube basadas en blockchain", Journal of Cloud Computing, vol. 9, no. 1, págs. 1–25, 2020.

[88] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho y M.-S. Kim, "Una encuesta sobre vulnerabilidades de seguridad cibernética de blockchain y posibles contramedidas", International Journal of Network Management, vol. 29, no. 2, pág. e2060, 2019.

[89] X. Li, P. Jiang, T. Chen, X. Luo y Q. Wen, "Una encuesta sobre la seguridad de los sistemas blockchain", Future Generation Computer Systems, vol. 107, págs. 841–853, 2020.

[90] A. Singh, RM Parizi, Q. Zhang, K.-KR Choo y A. Dehghantanha, "Formalización de contratos inteligentes de Blockchain: enfoques y desafíos para abordar vulnerabilidades", Computers & Security, vol. 88, pág. 101654, 2020.

[91] DK Tosh, S. Shetty, X. Liang, CA Kamhoua, KA Kwiat y L. Njilla, "Implicaciones de seguridad de la nube blockchain con análisis del ataque de retención de bloques", en 2017, 17º Simposio Internacional IEEE / ACM sobre Computación en Clúster, Nube y Grid (CCGRID). IEEE, 2017, págs. 458–467.

[92] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko e Y. Alexandrov, "Smartcheck: Análisis estático de contratos inteligentes de Ethereum", en el primer taller internacional IEEE / ACM 2018 sobre tendencias emergentes en ingeniería de software para blockchain (WET-SEB). IEEE, 2018, págs. 9–16.

[93] I. Nikolić´, A. Kolluri, I. Sergey, P. Saxena y A. Hobor, "Encontrar los contratos codiciosos, pródigos y suicidas a escala", en Actas de la 34ª Conferencia Anual de Aplicaciones de Seguridad Informática. ACM, 2018, págs. 653–663.

[94] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen y B. Roscoe, "ReGuard: Finding Reentrancy Bugs in Smart Contracts", en Actas de la 40ª Conferencia Internacional sobre Ingeniería de Software: Actas complementarias. ACM, 2018, págs. 65–68.

[95] B. Jiang, Y. Liu y W. Chan, "Contractfuzzer: Fuzzing Smart Contracts for Vulnerability Detection", en Actas de la 33ª Conferencia Internacional ACM / IEEE sobre Ingeniería de Software Automatizada. ACM, 2018, págs. 259–269.

[96] L. Luu, D.-H. Chu, H. Olickel, P. Saxena y A. Hobor, "Cómo hacer que los contratos inteligentes sean más inteligentes", en Actas de la conferencia ACM SIGSAC de 2016 sobre seguridad informática y de comunicaciones. ACM, 2016, págs. 254–269.

[97] H. Liu, C. Liu, W. Zhao, Y. Jiang y J. Sun, "S-gram: Hacia una auditoría de seguridad con conciencia semántica para contratos inteligentes de Ethereum", en Actas de la 33a Conferencia Internacional ACM / IEEE sobre automóviles - Ingeniería de software acoplada. ACM, 2018, págs. 814–819.

[98] L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz y B. Scholz, "Vandal: A Scalable Security Analysis Framework for Smart Contracts", preprint arXiv arXiv: 1809.03981, 2018.

[99] M. Suiche, "Porosity: A Decompiler for Blockchain Smart Contract Bytecode", DEF CON, vol. 25, pág. 11 de diciembre de 2017.

[100] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz e Y. Smaragdakis, "Madmax: Surviving Out-of-Gas conditions in Ethereum Smart Contratos ", Actas de la ACM sobre lenguajes de programación, vol. 2, no. OOPSLA, pág. 116, 2018.

[101] K. Wüst y A. Gervais, "Ethereum Eclipse Attacks", ETH Zurich, Tech. Rep., 2016.

[102] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli y M. Vechev, "Securify: Practical Security Analysis of Smart Contracts", en Actas de la Conferencia ACM SIGSAC 2018 sobre seguridad informática y de comunicaciones. ACM, 2018, págs. 67–82.

[103] I. Grishchenko, M. Maffei y C. Schneidewind, "Un marco semántico para el análisis de seguridad de los contratos inteligentes de Ethereum", en la Conferencia Internacional sobre Principios de Seguridad y Confianza. Springer, 2018, págs. 243–269.

[104] P. Otte, M. de Vos y J. Pouwelse, "TrustChain: una cadena de bloques escalable resistente a Sybil", Future Generation Computer Systems, 2017.

[105] S. Kalra, S. Goel, M. Dhawan y S. Sharma, "Zeus: Analizando la seguridad de los contratos inteligentes", en el 25º Simposio anual de seguridad de redes y sistemas distribuidos, NDSS, 2018, págs. 18–21.

[106] I. Grishchenko, M. Maffei y C. Schneidewind, "EtherTrust: análisis estático de sonido del código de bytes de Ethereum", Technische Universität Wien, Tech. Rep, 2018.

[107] M. Mossberg, F. Manzano, E. Hennenfent, A. Groce, G. Grieco, J. Feist, T. Brunson y A. Dinaburg, "Manticore: A User-Friendly Symbolic Execution Framework for Binaries and Smart Contracts", preprint arXiv arXiv: 1907.03890, 2019.

[108] P. Mell, J. Kelsey y J. Shook, "Contratos inteligentes de criptomonedas para el consenso distribuido de aleatoriedad pública", en Simposio internacional sobre estabilización, seguridad y protección de sistemas distribuidos. Springer, 2017, págs. 410–425.

[109] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali y R. Hierons, "Vulnerabilidades de contratos inteligentes: ¿un llamado a la ingeniería de software de cadena de bloques?" en 2018 Workshop Internacional sobre Ingeniería de Software Orientada a Blockchain (IWBOSE). IEEE, 2018, págs. 19-25.

[110] N. Atzei, M. Bartoletti y T. Cimoli, "Una encuesta sobre los ataques a los contratos inteligentes de Ethereum (sok)", en la Conferencia internacional sobre principios de seguridad y confianza. Springer, 2017, págs. 164-186.

[111] K. Delmolino, M. Arnett, A. Kosba, A. Miller y E. Shi, "Paso a paso hacia la creación de un contrato inteligente seguro: lecciones y conocimientos de un laboratorio de criptomonedas", en Conferencia internacional sobre criptografía financiera y seguridad de datos . Springer, 2016, págs. 79–94.

[112] M. Wohrer y U. Zdun, "Contratos inteligentes: patrones de seguridad en el ecosistema ethereum y solidez", en el Taller internacional de 2018 sobre ingeniería de software orientada a cadenas de bloques (IWBOSE), marzo de 2018, págs. 2–8.

[113] RM Parizi, A. Dehghantanha, K.-KR Choo y A. Singh, "Análisis empírico de vulnerabilidad de pruebas de seguridad de contratos inteligentes automatizados en cadenas de bloques", en Actas de la 28ª Conferencia Internacional Anual sobre Ciencias de la Computación e Ingeniería de Software. IBM Corp., 2018, págs. 103-113.

[114] A. Mavridou y A. Laszka, "Designing Secure Ethereum Smart Contracts: A Finite State Machine based Approach", arXiv preprint arXiv: 1711.09327, 2017.

[115] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, A. Rastogi, T. Sibut-Pinote, N. Swamy y S. Zanella-Béguelin, "Short Paper: Formal Veri fi cation of Smart Contracts", en Proceedings of the 11th ACM Workshop on Programming Languages and Analysis for Security (PLAS), junto con ACM CCS, 2016, págs. 91–96 .

[116] T. Abdellatif y K.-L. Brousmiche, "Verificación formal de contratos inteligentes basados en usuarios y modelos de comportamiento Blockchain", en 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2018, págs. 1–5.

[117] Z. Nehai, P.-Y. Piriou y F. Daumas, "Model-check of Smart Contracts", en IEEE International Conference on Blockchain, 2018, págs. 980–987.

[118] E. Albert, P. Gordillo, B. Livshits, A. Rubio e I. Sergey, "EthIR: A Framework for High-Level Analysis of Ethereum Bytecode", en el Simposio Internacional sobre Tecnología Automatizada para Verificación y Análisis. Springer, 2018, págs. 513–520.

[119] A. Kosba, A. Miller, E. Shi, Z. Wen y C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", en el Simposio sobre seguridad y privacidad (SP) del IEEE 2016, mayo 2016, págs. 839–858.

[120] SR Niya, F. Shüpfer, T. Bocek y B. Stiller, "Configuración de operaciones flexibles y ligeras con privacidad mejorada del usuario utilizando Smart

Contracts ", en el Simposio de Gestión y Operaciones de Red IEEE / IFIP de NOMS 2018-2018. IEEE, 2018, págs. 1–2.

[121] D. Chatzopoulos, S. Gujar, B. Faltings y P. Hui, "Preservación de la privacidad y Crowdsensing móvil con optimización de costos usando contratos inteligentes en Blockchain", en la 15a Conferencia Internacional IEEE de 2018 sobre sistemas móviles ad hoc y de sensores (MASS) . IEEE, 2018, págs. 442–450.

[122] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat y L. Njilla, "Provchain: una arquitectura de procedencia de datos basada en blockchain en un entorno de nube con mayor privacidad y disponibilidad", en Proceedings of the 17th Simposio internacional IEEE / ACM sobre computación en clúster, nube y grid. IEEE Press, 2017, págs. 468–477.

[123] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn y G. Danezis, "Chainspace: Una plataforma de contratos inteligentes fragmentados", preprint arXiv arXiv: 1708.03778, 2017.

[124] H. Kalodner, S. Goldfeder, X. Chen, SM Weinberg y EW Felten, "Arbitrum: Scalable, Private Smart Contracts", en el 27º Simposio de seguridad {USENIX} ({USENIX} Security 18), 2018, págs. 1353-1370.

[125] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller y D. Song, "Ekiden: una plataforma para contratos inteligentes que preservan la confidencialidad, son dignos de confianza y funcionan", 1804.

[126] F. Zhang, E. Cecchetti, K. Croman, A. Juels y E. Shi, "Town pregonero: un feed de datos autenticado para contratos inteligentes", en Actas de la conferencia 2016 aCM sIGSAC sobre seguridad informática y de comunicaciones. ACM, 2016, págs. 270–282.

[127] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang y J. Xie, "Shadoweth: Contrato inteligente privado en blockchain público", Revista de Ciencias de la Computación y Tecnología, vol. 33, no. 3, págs. 542–556, 2018.

[128] F. Benhamouda, S. Halevi y TT Halevi, "Soporte de datos privados en Hyperledger Fabric con computación segura entre varias partes", IBM Journal of Research and Development, 2019.

[129] G. Zyskind, O. Nathan y A. Pentland, "Enigma: plataforma de computación descentralizada con privacidad garantizada", preprint arXiv arXiv: 1506.03471, 2015.

[130] B. Bünz, S. Agrawal, M. Zamani y D. Boneh, "Zether: Hacia la privacidad en un mundo de contratos inteligentes", en la Conferencia internacional sobre criptografía financiera y seguridad de datos. Springer, 2020, págs. 423–443.

[131] H. Halpin y M. Piekarska, "Introducción a la seguridad y la privacidad en Blockchain", en el Simposio europeo de seguridad y privacidad del IEEE 2017 (EuroS & PW). IEEE, 2017, págs. 1-3.

[132] Z. Liehuang, G. Feng, S. Meng, L. Yandong, Z. Baokun, M. Hongliang y W. Zhen, "Encuesta sobre técnicas de preservación de la privacidad para la tecnología Blockchain", Revista de investigación y desarrollo informático, p. 2170, 2017.

[133] BK Mohanta, D. Jena, SS Panda y S. Sobhanayak, "Tecnología Blockchain: una encuesta sobre aplicaciones y desafíos de privacidad de seguridad", Internet de las cosas, vol. 8, pág. 100107, 2019.

[134] R. Henry, A. Herzberg y A. Kate, "Privacidad de acceso a Blockchain: desafíos y direcciones", IEEE Security & Privacy, vol. 16, no. 4, págs. 38–45, 2018.

[135] Q. Feng, D. He, S. Zeadally, MK Khan y N. Kumar, "Una encuesta sobre la protección de la privacidad en el sistema blockchain", Journal of Network and Computer Applications, vol. 126, págs. 45–58, 2019.

[136] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman y SW Kim, "Protección de privacidad de contrato inteligente usando inteligencia artificial en sistemas ciberfísicos: herramientas, técnicas y desafíos", IEEE Access , vol. 8, págs. 24 746–24 772, 2020.

[137] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke y T. Varvarigou, "Conozca la implementación de su cliente (kyc) con contratos inteligentes en una arquitectura descentralizada orientada a la privacidad", Future Internet, vol. 12, no. 2, pág. 41, 2020.

[138] A. Dorri, M. Steger, SS Kanhere y R. Jurdak, "Blockchain: una solución distribuida para la seguridad y privacidad automotriz", IEEE Communications Magazine, vol. 55, no. 12, págs. 119-125, 2017.

[139] S. Woo, J. Song y S. Park, "Un oráculo distribuido que utiliza intel sgx para aplicaciones de iot basadas en blockchain", Sensors, vol. 20, no. 9, pág. 2725, 2020.

[140] G. Ayoade, V. Karande, L. Khan y K. Hamlen, "Gestión de datos de iot descentralizada utilizando blockchain y un entorno de ejecución confiable", en la Conferencia Internacional IEEE de 2018 sobre Reutilización e Integración de la Información (IRI). IEEE, 2018, págs. 15–22.

[141] S. Felsen, Á. Kiss, T. Schneider y C. Weinert, "Evaluación de funciones seguras y privadas con intel sgx", en Actas de la Conferencia ACM SIGSAC de 2019 sobre el Taller de seguridad de la computación en la nube, 2019, págs. 165–181.

[142] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei y B. Chen, "Cuando blockchain se encuentra con sgx: una descripción general, desafíos y problemas abiertos", IEEE Access, 2020.

[143] L.-D. Ibáñez, K. O'Hara y E. Simperl, "Sobre Blockchains y el Reglamento General de Protección de Datos", 2018.

[144] A. Juels, A. Kosba y E. Shi, "The Ring of Gyges: Investigating the Future of Criminal Smart Contracts", en Actas de la Conferencia ACM SIGSAC de 2016 sobre seguridad informática y de comunicaciones. ACM, 2016, págs. 283–295.

[145] Intel, "Intel Software Guard Extensions (Intel SGX)", 2020. [En línea]. Disponible: https://www.intel.com.au/content/www/au/en/arquitectura-y-tecnología / software-guard-extensions.html

[146] WikiPedia, "El problema de los millonarios de Yao", 2020. [En línea]. Disponible: https://splash247.com/blockchain-roaming-in-the-maritime-industry/

[147] F. Idelberger, G. Governatori, R. Riveret y G. Sartor, "Evaluación de contratos inteligentes basados en lógica para sistemas Blockchain", en Simposio internacional sobre reglas y lenguajes de marcado de reglas para SemanticWeb. Springer, 2016, págs. 167–183.

[148] T. Chen, X. Li, X. Luo y X. Zhang, "Los contratos inteligentes sub optimizados devoran su dinero", en la 24ª Conferencia Internacional IEEE de 2017 sobre Análisis, Evolución y Reingeniería de Software (SANER). IEEE, 2017, págs. 442–446.

[149] A. Kothapalli, A. Miller y N. Borisov, "Smartcast: un protocolo de consenso compatible con incentivos utilizando contratos inteligentes", en la Conferencia internacional sobre criptografía financiera y seguridad de datos. Saltador, 2017, págs. 536–552.

[150] A. Zhang y K. Zhang, "Habilitación de la concurrencia en contratos inteligentes mediante pedidos de múltiples versiones", en la Conferencia internacional conjunta sobre Web y Big Data de Asia-Pacífico Web (APWeb) y Web-Age Information Management (WAIM). Springer, 2018, págs. 425–439.

[151] PS Anjana, S. Kumari, S. Peri, S. Rathor y A. Somani, "Un marco eficiente para la ejecución concurrente optimista de contratos inteligentes", en 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)). IEEE, 2019, págs. 83–92.

[152] PJ Piasecki, "Casinos de contratos inteligentes independientes y demostrablemente justos para juegos", Ledger, vol. 1, págs. 99-110, 2016.

[153] T. Marwala y B. Xing, "Blockchain and Arti fi cial Intelligence", preprint arXiv arXiv: 1802.04451, 2018.

[154] Y. Lu, X. Huang, Y. Dai, S. Maharjan y Y. Zhang, "Blockchain y aprendizaje federado para el intercambio de datos con privacidad preservada en iot industrial", IEEE Transactions on Industrial Informatics, 2019.

[155] J. Kang, Z. Xiong, D. Niyato, S. Xie y J. Zhang, "Mecanismo de incentivo para el aprendizaje federado confiable: un enfoque de optimización conjunta para combinar la reputación y la teoría de contratos", IEEE Internet of Things Journal, 2019.

[156] J. Daniel, A. Sargolzaei, M. Abdelghani, S. Sargolzaei y B. Amaba, "Tecnología Blockchain, computación cognitiva e innovaciones en el cuidado de la salud", Journal of Advances in Information Technology Vol. Vol. 8, no. 3, 2017.

[157] J. Charlier, S. Lagraa, J. Francois et al., "Perfiles de interacciones de contratos inteligentes con descomposición de tensor y minería de gráficos", 2017.

[158] E. Kara fi loski y A. Mishev, "Soluciones blockchain para desafíos de big data: una revisión de la literatura", en IEEE EUROCON 2017-17th International Conference on Smart Technologies. IEEE, 2017, págs. 763–768.

[159] N. Abdullah, A. Hakansson y E. Moradian, "Enfoque basado en blockchain para mejorar la autenticación de big data en entornos distribuidos", en la Novena Conferencia Internacional sobre Redes Ubicuas y Futuras de 2017 (ICUFN). IEEE, 2017, págs. 887–892.

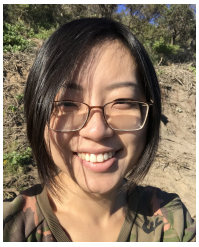
[160] L. Yue, H. Junqin, Q. Shengzhi y W. Ruijin, "Modelo de big data de intercambio de seguridad basado en blockchain", en la 3ª Conferencia Internacional de Computación y Comunicaciones de Big Data (BIGCOM) de 2017. IEEE, 2017, págs. 117–121.

[161] Q. Xu, KMM Aung, Y. Zhu y KL Yong, "Un sistema de almacenamiento basado en blockchain para el análisis de datos en el Internet de las cosas", en Nuevos avances en el Internet de las cosas. Springer, 2018, págs. 119-138.

[162] UU Uchibeke, KA Schneider, SH Kassani y R. Deters, "Ecosistema de control de acceso Blockchain para la seguridad de big data", en la Conferencia Internacional IEEE sobre Internet de las Cosas (iThings) 2018 e IEEE Green Computing and Communications (GreenCom) e IEEE Cyber, Computación física y social (CPSCom) e IEEE Smart Data (SmartData). IEEE, 2018, págs. 1373-1378.

THARAKA HEWA Actualmente trabaja como estudiante de doctorado en el Centro de Comunicaciones Inalámbricas de la Universidad de Oulu, Finlandia. Recibió su licenciatura en Ciencias de la Computación de la Escuela de Computación de la Universidad de Colombo, Sri Lanka en 2013, y la Maestría en Ciencias en Seguridad de la Información (Distinción) de la Escuela de Computación de la Universidad de Colombo en 2016. De 2012 a 2017, trabajó en un proveedor líder de soluciones de pago digital en Sri Lanka como Senior Ingeniero de software. Dentro de su carrera en la industria, contribuyó a muchos proyectos en banca móvil, banca por Internet, PKI, cajeros automáticos y participó en la integración y el soporte del sistema. Es ingeniero certificado por SafeNet Luna SA 6.0 HSM. En 2017, se incorporó a la Universidad Tecnológica de Nanyang como investigador asociado. Desempeñó un papel vital en muchos proyectos de investigación e implementación en diferentes contextos. Contribuyó a la ciberseguridad y los sistemas de pago digital y fue coautor de 2 publicaciones relacionadas con las aplicaciones de blockchain en la industria con contribución a 1 patente. Contribuyó a proyectos de investigación e implementación en curso que incluyen blockchain para impresión 3D, agricultura, relojes de lujo, monetización de activos musicales y aviación.

Los intereses de investigación de Hewa son Blockchain, PKI, 5G, Seguridad de sistemas bancarios, Seguridad de la atención médica y Ciudades inteligentes.



YINING HU Yining Hu recibió su título BE (Electricidad) con honores de primera clase de la Universidad de Sydney, Sydney, Australia, y el Instituto de Tecnología de Harbin, Harbin, China, en 2016 (programa conjunto). Recibió su Ph.D. en la Universidad de Nueva Gales del Sur, Sydney, Australia, en 2020. Durante su Ph.D. candidatura también estaba afiliada a Data61-CSIRO, Sydney, Australia. Se incorporó a IBMAustralia, Melbourne, Australia, como investigadora postdoctoral, en 2020. Sus principales áreas de interés de investigación son el análisis de transacciones de criptomonedas ilícitas, la mejora de la utilidad de las plataformas blockchain y la habilitación de la interoperabilidad blockchain.

MADHUSANKA LIYANAGE (Miembro principal, IEEE) es actualmente miembro de Ad Astra / profesor asistente en la Escuela de Ciencias de la Computación, University College Dublin, Irlanda. También es profesor adjunto en la Universidad de Oulu, Finlandia. Recibió su B.Sc. Licenciatura (con honores de primera clase) en ingeniería electrónica y de telecomunicaciones de la Universidad de Moratuwa, Moratuwa, Sri Lanka, en 2009, el M.Eng. grado del Instituto Asiático de Tecnología, Bangkok, Tailandia, en 2011, el M.Sc. título de la Universidad de Niza Sophia Antipolis, Niza, Francia, en 2011, y el Ph.D. Licenciado en ingeniería de comunicaciones de la Universidad de Oulu, Oulu, Finlandia, en 2016. También recibió la prestigiosa beca individual Marie Skłodowska-Curie Actions durante 2018-2020. De 2011 a 2012, trabajó como investigador científico en el laboratorio I3S e Inria, Sophia Antipolis, Francia. Ha sido investigador visitante en el Departamento de Ciencias de la Computación, Universidad de Oxford, Data61, CSIRO, Sydney, Australia, Infolabs21, Universidad de Lancaster, Reino Unido, y Ciencias de la Computación e Ingeniería, Universidad de Nueva Gales del Sur durante 2015-2018. En 2020, recibió el premio "2020 IEEE ComSoc Outstanding Young Researcher" otorgado por IEEE ComSoc EMEA.

Ha sido coautor de más de 90 publicaciones, incluidos dos libros editados con Wiley y una patente. Es el copresidente de demostración de WCNC 2019, presidente de publicidad de ISWCS 2019 y presidente de póster de 6G Summit 2020. Se desempeñó como miembro del comité de programa técnico en EAI M3Apps 2016, 5GU 2017, EUCNC 2017, EUCNC 2018, 5GWF 2018, MASA 2018, MCWN 2018, WCNC 2019, EUCNC 2019, EUCNC 2020, MASS 2020. Copresidente del programa técnico y conferencias ICBC 2021 en el taller SecureEdge en la conferencia IEEE CIT2017 y el taller Blockchain para IoT en IEEE Globecom 2018, IEEE ICC 2020 e IEEE 5GWF 2020. También se desempeñó como presidente de la sesión en una serie de otras conferencias, incluidas IEEE WCNC 2013, CROWNCOM 2014, 5GU 2014, IEEE CIT 2017, IEEE PIMRC 2017, 5GWF 2018, Bobynet 2018, Globecom 2018, WCNC 2019, ICC 2020. recibió dos premios al mejor artículo en las áreas de seguridad SDMN (en NGMAST 2015) y seguridad 5G (en IEEE CSCN 2017). Además, ha recibido tres becas de investigación y otros 22 premios / becas de prestigio durante su carrera investigadora.

El Dr. Liyanage ha trabajado para más de doce proyectos de la UE, internacionales y nacionales en el ámbito de las TIC. Ocupó responsabilidades como líder de paquetes de trabajo en varios proyectos nacionales y de la UE. Actualmente, es el coordinador nacional finlandés de la Acción COST CA15127 de la UE sobre servicios de comunicación resilientes. Además, se desempeña como miembro del comité de gestión de otros cuatro proyectos de acción de EU COST, a saber, EU COST Action IC1301, IC1303, CA15107 y CA16226. Liyanage tiene más de tres años de experiencia en gestión de proyectos de investigación, liderazgo de grupos de investigación, preparación de propuestas de proyectos de investigación, documentación del progreso del proyecto y co-supervisión / tutoría de estudiantes graduados, habilidades. En 2015, 2016 y 2017, ganó el Premio al Mejor Investigador en el Centro de Comunicaciones Inalámbricas de la Universidad de Oulu por su excelente contribución en la gestión de proyectos y actividades de difusión. Además, dos de los proyectos de investigación (proyectos MEVICO y SIGMONA) recibieron el Premio a la Excelencia CELTIC en 2013 y 2017 respectivamente.

Los intereses de investigación del Dr. Liyanage son 5G, SDN, IoT, Blockchain, MEC, seguridad de redes móviles y virtuales. http://madhusanka.com.

SALIL S. KANHERE recibió su MS y Ph.D. grados, ambos en Ingeniería Eléctrica de la Universidad de Drexel, Filadelfia. Es profesor en la Facultad de Informática e Ingeniería de la UNSW Sydney, Australia. También tiene afiliaciones con el Centro de Investigación Cooperativa de Ciberseguridad y Data61 de CSIRO. Ha ocupado puestos de visita en el Instituto de Investigación de Infocom de Singapur, la Universidad Técnica de Darmstadt, la Universidad de Zurich y la Universidad de Graz. de tecnología. Sus intereses de investigación incluyen Internet de las cosas, informática generalizada, sistemas ciberfísicos, blockchain, ciberseguridad y aprendizaje automático aplicado. Ha publicado más de 250 artículos revisados por pares y entregado más de 50 tutoriales y charlas magistrales sobre estos temas de investigación. Ha recibido 8 premios al Mejor Papel. Su investigación ha aparecido en ABC News Australia, Forbes, Wired, ZDNET, MIT Technology Review, Computer World, IEEE Spectrum y otros medios de comunicación. Participa regularmente en el comité organizador de una serie de conferencias internacionales IEEE y ACM. Es el Presidente General de la Conferencia Internacional IEEE sobre Blockchain y Criptomonedas (IEEE ICBC) en 2021. Salil es el Editor en Jefe de Ad Hoc Networks Journal y en el Consejo Editorial de IEEE Transactions on Network Management and Service, Computación móvil y generalizada y comunicaciones informáticas. Es miembro del Comité Ejecutivo del Comité Técnico de Comunicaciones Informáticas (TCCC) de la IEEE Computer Society. Salil es miembro senior tanto del IEEE como del ACM. Recibió la Beca de Investigación Alexander von Humboldt.

MIKA YLIANTTILA (Miembro principal, IEEE) es profesor asociado a tiempo completo (trayectoria permanente) en el Centro de Comunicaciones Inalámbricas (CWC), en la Facultad de Tecnología de la Información e Ingeniería Eléctrica (ITEE), Universidad de Oulu, Finlandia. Dirige un equipo de investigación y es director del programa de doctorado en ingeniería de comunicaciones. Anteriormente fue director del Center for Internet Excellence (2012-2015), subdirector del grupo de investigación MediaTeam Oulu (2009-2011), y profesor (pro tem) en Informática e Ingeniería, y director del programa de estudios de redes de información (2005-2010). Recibió su doctorado en Ingeniería de Comunicaciones en la Universidad de Oulu en 2005. Ha sido coautor de más de 150 artículos internacionales revisados por pares. Sus intereses de investigación incluyen informática de punta, seguridad de redes, virtualización de redes y redes de fi nidas por software. Es miembro senior de IEEE y editor de la revista Wireless Networks.